

# Siber Güvenlik

## Görev 1: Gölge Analist Raporu

Kadir Veysel Sayar

05.02.2026

### Bölüm A: Savunma Mimarisi ve Teknoloji Entegrasyonu

#### 1. Ağ ve Çevre Güvenliği (Sınır Hattı):

**Firewall & IDS/IPS:** Güvenlik duvarı, ağıda karşıımıza çıkan ilk duvardır. OSI modelinde Firewall 3. (Ağ) ve 4. (Taşıma) katmanında; IDS & IPS 7. (Uygulama) katmanına kadar çalışır.

Bir mektubumuz var diyelim ve bu mektubumuzun Erişim Kontrol Listesindeki kurallara uyuyorsa içeriğe bakmadan kabul eder. Sonrasında IDS & IPS ise bu mektubun içine bakar. IDS sadece içeriğe bakıp alarm üretirken; IPS içeriğe bakıp engelleyebilir. Eğer sadece IPS içeriğe bakarsa mektubun içeriği kötü olmamasına rağmen false positive olarak algılayabilir ve engeller. IDS ise gelen mektupların içlerini öğrenirken IPS bu öğrenmeye dayalı engellemeye yapar. Firewall ile IDS/IPS iş birliği ise, duvarın geçirdiği mektupları IPS ayrıntılı inceleyerek güvenli bir iletişim yolunu sağlanmasıdır.

**NDR (Network Detection and Response):** Firewall ve IPS'in atlatıldığı senaryolarda NDR, iç ağdaki trafiği inceler. Trafik şifreli olsa bile Metadata üzerinden analiz yapar ve yapay zeka ile inceler. Bir saldırgan yanal hareket ile yetkisi olmayan bir sunucudan diğer bir sunucuya geçiyorsa ve mesai saatleri dışında gerçekleşiyorsa bunu tespit eder.

#### 2. Uç Nokta Savunması (Son Kale)

**Antivirüs vs EDR:** Dosyasız saldırıları EDR yakalar çünkü diske herhangi bir dosya kaydetmeden Powershell üstünden çalışır ama bir dosya olmadığı için bunu antivirüs göremez. Antivirüs, imza tabanlı çalışır. Bu yüzden diğer kötü dosyalarla karşılaşılıyor. EDR, örnek verecek olursak kayıt defteri değiştirmesini tespit eder.

#### 3. Operasyon Merkezi ve Görünürlük (Beyin Takımı)

**SOC & SIEM:** Bir kullanıcı adını yanlış girdi ve sisteme bunun kaydı düşer fakat çok kez yanlış girerse SIEM bunu görerek kritik seviye olarak sisteme not geçer ve alarm üretir. SOC Analisti kritik uyarılar ekranında, saldırı ip, hedef ip, zaman ve tarih görür.

**SOAR:** İnsan sisteme bazen 7/24 aktif olmadığından insan gibi davranış gösterir.

#### 4. Genişletilmiş ve Yönetilen Hizmetler (Büyük Resim)

**XDR (Extended Detection and Response):** Gelen verileri tek bir yerde toplar. Bu yüzden verilerin analizi daha kolay olur.

**MDR (Managed Detection and Response):** Yetersiz hizmet olduğunda devreye girer. Bu bir hizmet. Müşteri ağını 7/24 izler. Tehdit avcılığı gibi olayları üstlenir.

### **Bölüm B: Teknik Sözlük ve Kavram Avı**

#### 1. Temel Yapıtaşları ve Ağ

**Transistor & Bilgisayar:** Transistorların 0 ve 1'leri bilgisayarın anadilini olan (binary) makine kodunun alfabetesidir. Bu elektriksel sinyallerin birleşmesiyle oluşan işlemci komutları, işletim sisteminin donanımı yönetebilmesini sağlayan katmanı oluşturur.

**OSI vs TCP/IP:** OSI modeli ağ iletişimini 7 katmanda temelini oluşturan mükemmel bir referanştır. TCP/IP ise bu katmanları 4'e düşürür. TCP/IP kuralları yerine protokollere önem verir.

**Kriptografi:** Şifreleme algoritmalarıyla veriyi yetkisiz kişilerden saklar. Hashlar sayesinde verinin iletim sırasında değiştirilip değiştirilmemiğini matematiksel olarak kanıtlanabilir.

#### 2. Saldırı Vektörleri (Offensive Terminology)

**Sosyal Mühendislik & Phishing:** Bir insanı kandırmak bir güvenlik duvarını aşmaktan daha kolaydır ve iş gücü daha azdır. Phishing bir saldırı yöntemi iken E-mail spoofing, bu amacı gerçekleştirmek için gerçekçi bir e-posta atılmasıdır.

**Malware Dünyası:** Malware veriyi çalmayı veya silmek olurken, Ransomware bu veriyi şifreler ve karşı taraftan fidye talep eder.

**Zero-Day (Sıfır Gün):** Bilinen bir saldırının olmadığından antivirüs ve güvenlik duvarının bu saldırıyı önleyemeyeceği anlamına gelir.

#### 3. Savunma Mekanizmaları (Defensive Terminology)

**Yama (Patch) Yönetimi:** Zamanında bir koda veya sisteme güncelleme yapılmazsa saldırıcı bu açığı yama gelmeden önce keşfedebilir. Yama dediğimiz açıkları kapatın bir geliştirme/yükseltme/güncellemedir.

**Kimlik ve Erişim:** Parola tek faktörlü doğrulamadır. 2FA ise ikinci bir doğrulama ekler. (Parmak izi, yüz tanıma). Matematiksel olarak iki sorunu çözmek bir sorunu çözmekten daha zor olduğundan iki faktör güvenliği artırır.

**Tünelleme ve Gizlilik:** VPN bizi tamamen görünmez yapmaz. Sadece internet servis sağlayıcımızda gözükmektedir. Ağ trafiğinde bize ait şifreli bir tünel oluşturur. SSL/TLS, VPN tünelini şifreleyen protokoldür ve bu tünelin her yeridir.

#### 4. Standartlar ve Süreçler

**Zafiyet Taraması:** Zafiyet taraması otomatik yapılan kapsamlı bir zafiyet taramasıdır. Sızma testi ise bu zafiyet taramasındaki zafiyetlerin sömürülmemesidir.

**Regülasyonlar:** ISO 27001, NIST, GDPR ve KVKK gibi standartlar yasal bir zorunluluktur. Siber Güvenlik mimarı sistemi bu yasalara uyarak yanı hukuksal açıdan illegal olmadan kurması gereklidir.

### **Bölüm C: CTI ve İstihbarat Odaklı Vaka Analizi Taslağı**

#### 1. Adım: Pasif İstihbarat Toplama

**Kimlik Tespit:** Hollanda merkezli bir ip olarak görülmektedir.

**Sicil Kaydı:** Yoğunlukla SSH Brute Force ve Port Scanning aktivitelerinde bulunmuş. Mirai Botnet ve Cobalt Strike araçlarını kullanmış.

**Zaman Çizelgesi:** IP bir tehdit değil ve son 1 gün içinde hiçbir işlem gerçekleştirilmemiş.

#### 2. Adım: Terminoloji ve Yapılandırma (Applied Concepts)

**IOC (Indicator of Compromise):** Burada IOC fingerprint yerine geçer. Aslında IP değil bir URL veya dosya hash'i de olabilir.

Type: IPv4 Address

Value: 45.128.232.67

Tag: Mirai\_Botnet, SSH\_Brute\_Force

**CTI (Cyber Threat Intelligence):** Veriye bağlam katarak açıklarsak, 45.128.232.67 IP'si Hollanda'dadır cümlesi sadece bir veridir. Bu IP kurumumuzun veritabanı sunucularına yönelik SSH Brute Force saldırıları yapan Mirai Botnet ağının bir parçasıdır ve aktif olarak 22. portu zorlamaktadır demek bir istihbarattır.

**MISP (Malware Information Sharing Platform):** Bunu MISP üzerinden paylaşmam gereklidir çünkü aynı IP adresi bir başka kuruluşlara ve kurumlara da aynı saldırılardan yapabilir. Eğer saldırılardan önce savunma yapılsrsa kale daha güvenilir olur.

### 3. Adım: Karar ve Aksiyon (Actionable Intelligence)

**Karar:** Engelle ve İzle

**Gerekçe:** Yapılan trafik analizi ve pasif tarama sorgularında hedef IP adresinin (45.128.232.67) SSH Brute Force saldırıları ve Port Scanning faaliyetleri yürüten bir botnet ağının parçası olduğu tespit edilmiştir. Sunucumuzun bu IP ile kurduğu bağlantı, saldırganın sisteme bir backdoor oluşturma veya yetkisiz erişim denemesinde olduğu görülmektedir. Olası bir Yanal Hareket riskini önlemek adına IP adresi Firewall derecesinde engellenmeli yani güvenlik cihazlarında kara listeye alınmalıdır.

## Bölüm D: Kriz Yönetimi ve Olay Müdahale Refleksleri

### 1. Senaryo: Fidye Yazılımı (Ransomware) Kıyameti

**Acil Müdahale:** Fişi çekmek RAM'daki geçici bilgilerin kaybolmasına neden olur kesinlikle yapılmamalıdır. İlk olarak ağları izole ederek riskli cihazın Wifi bağlantısını keserim. Böylece yanal hareket yapmasını önerim. İkinci olarak RAM 'in bir kopyasını alırmış. Son olarak ise ağları kontrol edip diğer cihazlarda bir sorun var mı diye bakarım.

**LOG:** E-mail ve indirilen dosyalara bakarım. Eğer cihaz Windows ise Windows Olay Günlüğünden RDP üzerinden saldırı yapılmış mı diye bakarım. Firewall'ın görmediği arka planda bir script çalıştırılmış mı diye kontrol ederim.

### 2. Senaryo: Oltalama (Phishing) Dedektifliği

**Teknik İnceleme:** Mail adres yapısına ve IP adresi konumuna bakarım.

**Önlem:** Bir başkasına gönderilmemesi için IP adresini direkt kara listeye alınır. Eğer çalışanlara mail gönderilmiş ise otomatik olarak mailler silinir.

### 3. Süreç ve İletişim: "Mavi Takım" Ruhu

**Standartlar:** Olay müdahale sürecimi, uluslararası geçerliliği olan ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standartlarına dayandırıyorum.

**Kriz İletişimi:** İlk olarak önemli olduğunu düşündüğüm belirsizliği yönetirim. Kısa ve net cevaplar vererek. Örnek olarak işlem devam ediyor şu kadar süre

kaldı veya şu kadar sürecek diye. İkinci önemli olan net olan bilgilerin paylaşırıım. Emin olmadıklarımı baktıktan sonra eminken söylerim. Ve kriz anında herkesin bir şey söylemesi değil bu bilgilerin karşı tarafa karışıklık olmaması adına ve ekibin büyülüğüne göre bir veya iki kişinin aktarmasını tercih ederim.

#### 4. **Vizyon: Güncel Kalma Sanatı**

NIST NVD & CVE Details, The Hacker News, BleepingComputer