

# DİJİTAL SAVAŞ ALANI VE CTI(TEHDİT İSTİHBARATI)

## GÖLGE ANALİST RAPORU

### BÖLÜM A: SAVUNMA MİMARİSİ VE TEKNOLOJİ ENTEGRASYONU

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

**Firewall & IDS/IPS:** Firewall IP ve PORT ‘a bakar. IP ve PORT numarası yasaklı değilse geçiße izin veren yasaklısa erişimi engeller. IDS bir sorun tespit ederse sadece uyarı verir , müdahale etmez. IPS bir şüpheli durumda sadece uyarı vermez , o paketi düşürür(drop) ve bağlantıyı keser. IPS herhangi bir şüpheli durumda bağlantıyı keser. Bağlantının kesilmesi yanlış bir işlemde ağır sonuçlar doğurabilir bu yüzden IDS sadece şüpheli bir durumda onun sadece bir kopyasını (Mirroring/SPAN port üzerinden) alır. Orijinal paket hiç duraksamadan yoluna devam eder. IDS analizi 10 saniye bile sürse, ağdaki akışı yavaşlatmaz.

**NDR(Ağ Tespit ve Yanıt):** Firewall statik sorular sorular sorar . NDR ise dinamik sorular yani durumlara göre sorular sorarak şüpheli durumları analiz eder. Saldırganlar genellikle bir kullanıcı bilgisayarından (Phishing ile) içeri girer. Firewall bunu kaçırabilir çünkü paket “içerinden “ geliyor. Saldırganlar içinde sunucudan sunucuya atlamaya (Lateral Movement) başlar.

#### 2. Uç Nokta Savunması (Son Kale)

**Antivirüs vs EDR:** AV, diskteki dosyaya bakar. Eğer saldırgan, zararlı kodu diske hiç kaydetmeden doğrudan RAM'e enjekte edebilirse, AV tamamen kör kalır. EDR, dosyanın ne olduğuna değil, **işletim sistemi üzerinde ne yaptığına** bakar. EDR ajanları genellikle Kernel seviyesine "Hook" atar ve sistem çağrılarını (System Calls) izler. AV başarısız olur çünkü taranacak dosya yok! Her şey RAM 'de gerçekleşir. EDR , diskte dosya aramıyor. İşletim sistemindeki olayları inceleyerek şüpheli durumu anlıyor. Bu durumda EDR başarılı oluyor, AV ise başarısız oluyor.

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

**SOC & SIEM:** Binlerce log tek başına anlamsızdır. SIEM, Korelasyon Kuralları (Correlation Rules) adı verilen mantıksal sorgularla noktaları birleştirir. SOC analisti ekranda “Event” (Olay) değil, “Incident(Vaka/Olay Kaydı) düşer. İşlenmiş ve özet çıkarılmış bir raporu görür.

**SOAR:** Gelen veriyi (Email Header, Body, Sender IP, Attachments) JSON formatında parse eder ve bir "Vaka" (Case) nesnesi oluşturur. Otomatik API sorgularını sorarak bu yanıtları toplar ve vaka nesnesine ekler. Artık elinde şüphe değil kanıtlar vardır. Firewall den başlayarak sırasıyla diğer operatörlerden geçirir. Koşullar sağlandıysa ,SOAR insan onayı beklemeden diğer güvenlik cihazlarına API çağrıları göndererek savaşı başlatır.

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

##### **XDR (Genişletilmiş Tespit ve Yanıt):**

XDR, verileri birleştirmek için "**Pivot Noktaları**" (Anahtar Değerler) kullanır. Bu noktalar genellikle şunlardır:

- Kullanıcı Kimliği (User Identity)
- IP Adresi
- Dosya Hash'i
- Zaman Damgası (Timestamp)

##### **MDR (Yönetilen Tespit ve Yanıt):**

MDR, bir ürün değil, bir **hizmettir**. XDR veya EDR gibi araçları kullanan **insan gücüdür**.

MDR; "**Benim EDR aracım var ama onu kullanacak pilotum yok**" diyen şirketler için **kiralık pilottur**.

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

##### **1.Temel Yapıtaşları ve Ağ**

###### **Transistör ve Bilgisayar:**

**Transistör:** Alfabeteki harftir. (Anlamsızdır).

**Mantık Kapısı:** Kelimedir. (Ve, Veya, Değil).

**Modül (Adder/Memory):** Cümledir. (Bunu topla, şunu sakla).

**İşlemci (CPU):** Bir paragrafı okuyup anlayan kişidir.

**Yazılım:** O kişiye ne okuması gerektiğini söyleyen romandır.

**OSI vs TCP/IP:** OSI, ağın **anatomisini** anlamak için kullandığımız en iyi haritadır. TCP/IP ise o haritada arabayı sürmemizi sağlayan **motorun** kendisidir. Teoride OSI konuşuruz, pratikte TCP/IP kullanırız.

### Kriptografi:

- **Şifreleme (Encryption):** Veriyi bir **kasaya** koymaktır. (Gizlilik).
- **Hash/HMAC (Integrity):** Kasanın üzerine kırılabilir bir **mühür** vurmaktır. (Mühür kırıksa, içindenkine güvenilmez - Bütünlük).

Veri bütünlüğünü olmadan, gizliliğin hiçbir anlamı yoktur; çünkü yanlış veya manipüle edilmiş bir sırrı saklıyor olursunuz.

## 2. Saldırı Vektörleri (Saldırı Terminolojisi)

### Sosyal Mühendislik ve Kimlik Avı:

Yazılımın deterministik (belirlenebilir) olduğunu bilirsiniz. Input A her zaman Output B'yi verir. Ancak insan **deterministik değildir**, duygusaldır. Spoofing, göndericinin kimliğini taklit etme **tekniğidir**. İçerik zararlı olmak zorunda değildir (şaka amaçlı da yapılabilir). Phishing, kurbanı kandırarak hassas bilgi alma veya eylem yapırma **girişimidir**.

### Malware Dünyası:

Her Ransomware bir Malware'dir, ancak her Malware bir Ransomware değildir. **Malware** bilgisayarınızın "hasta" olduğunu söyler; **Ransomware** ise bilgisayarınızın "kaçırıldığını" ve fidye ödemeden serbest bırakılmayacağını söyler.

### Sıfır Gün (Sıfır Gün):

Savunma tarafı için kural şudur: "**Yama varsa operasyonel bir iştir, yama yoksa (Zero-Day) gerçek bir krizdir.**" Çünkü düşmanınızın elinde görünmezlik pelerini vardır.

## 3. Savunma Mekanizmaları (Savunma Terminolojisi)

### Yama (Patch) Yönetimi:

Yama yayınlandığı an, o açığın sömürülmeye olasılığı (Probability of Exploitation) %1'den %99'a fırlar.

Eğer siz yamayı, saldırganın "Binary Differencing" yapıp exploit geliştirmesinden daha kısa sürede (MTTR - Mean Time To Remediate) uygulayamazsanız, güvenlik açığı sizin için teorik bir risk olmaktan çıkıp, kesinleşmiş bir ihlale dönüşür.

### Kimlik ve Erişim:

Parola, kapının altına saklanmış bir anahtardır; bulan herkes girebilir. 2FA ise, o anahtarı kullandıktan sonra kapının açılması için aynı anda retin taraması yapılması ve o saniye üretilen bir kodun girilmesi zorunluluğudur.

### Tünelleme ve Gizlilik:

VPN, trafiği ISP'den gizleyen bir tüneldir. SSL/TLS ise bu tünelin içinden geçen zırhlı araçtır. Biri **kimliğinizi ve rotanızı** (Anonimlik), diğer **verinizin içeriğini** (Bütünlük ve Gizlilik) korur.

## 4. Standartlar ve İşlemciler

### Zafiyet Taraması:

Zafiyet Taraması "Genişlik" (Breadth) odaklıdır, Pentest ise "Derinlik" (Depth) odaklıdır. Zafiyet taraması, "**Kapı açık mı?**" sorusunun cevabıdır. Pentest ise, "**O kapıdan girip yatak odasındaki kasayı açabilir miyim?**" sorusunun cevabıdır.

### Regülasyonlar:

Regülasyonlar teknik değildir, **politiktir**. Ancak bu politikaların **uygulanması (enforcement)** %100 tekniktir.

Bir mühendis olarak bu standartları bilmek, sizi "kod yazan eleman" seviyesinden, "şirketin riskini yöneten **Çözüm Mimarı (Solutions Architect)**" seviyesine taşıır. Kodunuzun sadece çalışmasını değil, **yasal ve güvenli** kalmasını sağlar.

## Bölüm C: CTI ve İstihbarat Odaklı Vaka Analizi

**Burası yok hocam bende 😊**

## Bölüm D: Kriz Yönetimi ve Olay Müdahale Refleksleri

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

#### Acil Müdahale:

**Ben şöyled yapardım:** Bilgisayarı kapatma, sadece internet kablosunu çek veya Wi-Fi'yi kapatırım.

**Neden Ağ Kesiyorum?** Ransomware bir "Solucan" (Worm) gibi ağdaki dosya sunucularına (File Server) ve diğer PC'lere sıçramaya (Lateral Movement) çalışır. Bağlantıyı keserek şirketin geri kalanını kurtarırmı.

**Ben şöyled yapardım:** Finans kullanıcısının bilgisayarının erişebildiği ortak klasörleri (Z:, X: sürücüler gibi File Server paylaşımıları) ve yedekleme (Backup) sunucularını kontrol ederim.

**Gerekçe:** Modern fidye yazılımları, sadece yerel diski değil, ağıda yazma yetkisi olan (Write Access) her yeri şifreler. Eğer dosya sunucusunda .encrypted uzantılı dosyalar oluşmaya başlamışsa, sunucunun SMB servisini durduram veya onu da izole etmem gereklidir. **Yedeklerin şifrelenmesi, şirketin iflası demektir.**

**Ben şöyle yapardım:** İzole edilmiş ve halen çalışan bilgisayara (USB üzerinden veya EDR aracıyla) bir Adli Bilişim (Forensics) aracı ile bağlanıp **RAM imajını** alırırm.

**Gerekçe:** Saldırının nasıl gerçekleştiğini (Phishing mi, RDP mi?), zararlı yazılımın kodlarını ve iletişim kurduğu C2 (Komuta Kontrol) sunucusunu bulmak için RAM en değerli kaynaktır. Bilgisayar yeniden başlatılırsa bu veriler uçar. Analiz aşamasında "Bu virüs nereden girdi?" sorusunun cevabı buradadır.

#### Analiz:

1. İşlem ve EDR Logları (Process Lineage) - "Tetiği Kim Çekti?"
2. Windows Güvenlik Logları (Event ID 4624/4625) - "Kapıyı Zorlayan Oldu mu?"

## 2.Senaryo: Oltalama (Phishing) Dedektifliği

#### Teknik İnceleme:

Header (Başlık) Analizi ve Reply-To Uyumsuzluğuna bakarım. Sonuçta yanıtlaya bastığımızda adres saldırgan cevabı kendine yönlendirmek zorundadır.

#### Önlem:

**Ben şöyle yapardım:** Email Gateway (SEG - Secure Email Gateway): İlk Savunma

- **Kural:** Göndericinin "Envelope Sender" (Zarf Adresi) ve "Header From" adresini kara listeye (Blocklist) alırırm.

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

#### Standartlar:

**Ben şöyle yapardım:** Olay müdahale sürecimi (Incident Response Lifecycle) kesinlikle **NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide)** standardına dayandırıyorum.

#### Kriz İletişimi:

Teknik ekibi fiziksel veya sanal bir odaya toplarım ve dışarıdan giriş-çıkışı yasaklarım.

Yönetime şunu söylerim: "*Şu an analizdeyiz. Size her 30 dakikada bir (veya saat başı) durum raporu vereceğiz. Lütfen bu süreler dışında ekibi aramayın/bölmeyin.*"

İletişimde asla "*Sanırım Ruslar saldırıyor*" veya "*Galiba veriler silindi*" gibi belirsiz ifadeler kullanmam.

Ekibe "*Hızlı olun*" yerine "*Doğru olun*" mesajını veririm. "Hata yapma lüksümüz var ama yalan söyleme lüksümüz yok" prensibini hatırlatırım.

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

LinkedIn,github repoları, web siteleri, Instagramda alanında uzman kişileri takip etmek.