

# HAFTA 1

## BÖLÜM A

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

Firewall sadece izler . IDS/IPS izler ve uyarı aralarındaki fark budur .Firewall görünümle ilgilenirken IDS/IPS içerikle ilgilenir gibi düşünebiliriz. IDS/IPS iyi görünümlü kötüleride tespit etme açısından firewallden daha iyi bir performans sergiliyor. Sanal saldırılar saniyeler içinde gerçekleşir sen saldırıyı anlam verip çözmeye çalışana kadar IDS/IPS şüpheliyi bulup engellemeye çalışır , firewall bu konuda yetersiz kalabilir. IDS/IPS bazen yanlış bir çözüm yolu olabilir çünkü şüpheliyi takip etmek sistemdeki açığı anlamamızı kolaylaştırır işte burda da firewall şüpheliyi tespit eder ama engellemez .Genellikle ağın en dışında firewall ondan sonra IDS/IPS yerleştirilir.

NDR(Ağ Tespit ve Yanıt) zeka gibi düşünebiliriz. Bir otel düşünün otele girişte firewallle karşılaştık ondan sonra IDS/IPS ile. NDR bizi otelin içinde bekler davranışlarımıza bakar her gün 1GB veri yolluyorsam niye bu sefer 50 GB yolladım diye beni sorguya alır yani otelin içindeki gizli dedektiftir. Kötü yazılım firewallle iyi görünerek otelin kapısından içeri girer.Bundan sonra yazılımın bütün hareketleri ,davranışları NDR tarafından gözlem altına alınır.En ufak bir garip davranışta yakalanır.

### 2)Uç Nokta Savunması (Son Kale)

Antivirüsün imza halinde olması elinde kötü yazılımların yani suçluların olduğu bir dosya olmasıdır. EDR suçluları yakalamayı dosyasız yapabiliyor eğer yazılım laptopunuza eriştiyse ve antivirüs imzasında böyle bir kötü yazılım yoksa EDR işinize yarar.

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

SIEM dijital beyin SOC ise beyine gelen verileri inceleyen operasyon merkezidir. SIEM ilk önce verileri toplar sonra hepsini aynı dile çevirir,olayları birbirleriyle ilişkilendirir en son uyarıları önceliklendirir.SOC ekranında alarm aciliyet listesi , dünya haritası , saldırı şiddet grafiği , varlık bilgisi gözüktür.

SOAR ilk önce şüpheliyi algılar sonra veri tabanlarında soruşturur eğer soruşturma sonucu iyiye bırakır kötü ise eyleme geçer.Otomatik müdahale gerçekleşir.

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

XDR ilk önce EDR , NDR,e-posta, bulut'tan aldığı verileri veri havuzunda toplar. Sonra farklı verileri ilişkilendirir analist böylece tek ekranda her şeye ulaşır

MDR toplu bir siber güvenlik hizmeti gibi düşünebiliriz. 7/24 çalışan , daha tecrübeli neye bakacağını bilen , kendi EDR/XDR teknoloji paketini kullanan proaktif bir hizmettir. SOC 'u olmayanlar MDR kullanarak toplu bir hizmet paketi alıyor.

## BÖLÜM B

### 1. Temel Yapıtaşları ve Ağ

Transistörler elektrik akımıyla 1 ve 0 durumlarını oluşturur ve mantık kapıları halinde birleştirilerek modern sonuçlar ortaya koyar.

OSI ağdaki yedi katmanda tanımlayan bir klavuzdur .TCP/IP ise daha sade ve uygulanabilir 4 katmanlı modern internetin pratik temelidir.

Kriptografi şifreleme ve doğrulama mekanizmasıdır. Dijital imzalar özet değerleriyle verinin yolda değişikliğe uğramadığını kanıtlamış olur

### 2. Saldırı Vektörleri (Saldırı Terminolojisi)

Sosyal mühendislik gerçek hayattaki hacker , insanda herhangi bir güvenlik yaması olmadığı için sistem hacklemekten daha kolaydır. Kimlik avı kullanıcıyı kandırıp veri çalmak e-posta sahtekarlığı sahte e-posta aracılığıyla insan kandırmaktır.

Malware tüm kötü yazılımların adıdır Ransomware ise daha özel bir kavram olup verileri şifreleyerek erişimi engelleyen, veriler karşılığında fidye isteyen kötü yazılımdır.

Sıfır gün savunma tarafı adına açığı kapatmak için verilen süredir. Süresi çok olursa savunma için daha iyi bir strateji gerçekleştirilebilir.

### 3. Savunma Mekanizmaları (Savunma Terminolojisi)

Güvenlik güncellenmesini zamanında yapmazsan güvenlik açığı oluşturursun açığı kapatmak içinde yama yaparsan açık ile yama arasındaki süre senin için riskli olur.

2FA herhangi bir çalınma karşısında engel olabilecek bir faktördür , Sadece parola çok kolay çalınabildiği için 2FA uygulanmalıdır. Şifrenin yanına mobil onay, e-posta , sms vb. eklemek bizim açımızdan iyi olur.

VPN size şifreli bir tünel oluşturur , SSL/TLS ise tünelin içindeki trafiği şifreleyerek veri gizliliğini ve bütünlüğünü garantiler.

### 4. Standartlar ve İşlemciler

Zafiyet taraması otomatik olarak güvenlik açığı arar , sızma testi ise bu açıklardan sızarak ne olabileceğini gösterir.

ISO 27001, NIST ve GDPR gibi standartları teknik araç değil tüm süreçleri kapsayan yönetim stratejisidir. Bir mühendisin bunları bilmesi yasal ve teknik açıdan güvenli olmasını sağlar.

## BÖLÜM C

### 1.ADİM

45.128.232.67 nolu IP adresi Rusya merkezli olup AS202425 (Chang Way Technologies Co.Limited) isimli organizasyonu (ASN) tarafından kullanılıyor. Sicilinde kaba kuvvet ve port tarama sızma sonrası veri sızdırma Cobalt Strike komutları vardır. İlgili raporlamalar son 24 saat olup şu an aktif saldırı halinde olduğunu gösterir.

### 2.ADİM

Temel IOC 45.128.232.67 IP adresi ama sadece IP adresi değil bir .exe dosyasının SHA-256 hash değeri ya da saldırganın kullandığı zararlı alan adı (C2 Domain) da birer IOC haline gelir.Bunu istihbarata dönüştüren bağlamdır,şirketin rusya ile bağlantısı olmayıp portlar bağlantısıyla veri sızıntısı olduğunu söyler. IP adresini farklı platformlarda paylaşmak saldırı engelleyebilir ve siber dünyada sürü bağışıklığını anlatır.

### 3.ADİM

Karar: Engelle

Yapılan istihbarat sonucunda 45.128.232.67 IP adresinin Chang Way Technologies altyapısını kullanarak aktif bir SSH Brute Force saldırısını yaptığı ve son 24 saatte aktif olarak yüksek bir kötüye kullanım skoru elde etmiştir. Sunucunun bu IP ile kurduğu bağlantı, iş akışlarının dışında ve bir C2 (Komuta Kontrol) iletişimi riski taşımaktadır. Olası bir veri sızıntısını veya yanlamasına yayılmayı (Lateral Movement) önlemek amacıyla IP'nin uç nokta ve ağ seviyesinde acilen izole edilmesi gerekmektedir.

## BÖLÜM D

### SENARYO.1

İlk olarak ağ izolasyonu ile karantina altına alırım sonra EDR kullanarak bütün şüpheli işkemleri durdururum en son tüm yedekleme sunucularını ağdan koparır ve erişime engellerim. Malwarenin nasıl girdiğini bulmak için e-posta güvenlik ağ geçidi , windows olay günlükleri, Event ID 4688, VPN ve uzak masaüstü , EDR/AV loglarını kullanırım.

### SENARYO.2

Öncelikle başlık yapısını kontrol etmektir.Linkin üzerine gelerek gidilecek adrese uygunluğuna bakarım.Genellikle harf oyunları ve kısaltılmış linkler saldırının kanıtıdır. Mails Gateway (SEG) Kuralı ile kara listeye alırım firewall ve Web Proxy üzerinden linki engellerim.

### *SÜREÇ ve İLETİŞİM.3*

Pratik ve teknik süreçler için yani stratejileri kullanırken NIST , kurumun risk yönetim politikası için ISO 27001 standartını kullanırım. Saldırı altındayken karışıklık olmaması için olay komuta zinciri oluştururum ve her belirli sürede bir durum kontrol raporu veririm. Böylece herhangi bir yanlışlık oluşmasını önlerim.

### *VİZYON.4*

BleepingComputer, CVE Mitre / NIST NVD, The Hacker News (THN) kaynaklarını siber dünyada güncel kalmak için kullanıyorum.