SOC FUNDAMENTALS

&

CYBER KILL CHAIN RAPORU

Sema Nimet ÜNAL

07.02.2025

İÇİNDEKİLER

1. GİRİŞ

Bu raporda, SOC yani Güvenlik Operasyon Merkezi'nin (Security Operations Center) temel işleyişini ve önemini inceleyeceğiz. Siber saldırıları tespit etmek ve önlemek için geliştirilen **Cyber Kill Chain** modeli hakkında detaylı bilgi vereceğiz.

2. SOC FUNDAMENTALS

2.1. SOC Nedir ve Neden Önemlidir?

SOC, bir organizasyonun siber güvenlik tehditlerine karşı korunmasını sağlayan bir merkezdir. Sürekli olarak ağları, sistemleri ve cihazları izleyerek güvenlik açıklarını tespit etmeye çalışır. SOC sayesinde organizasyonlar, tehditlere karşı daha hızlı ve etkili bir şekilde tepki verebilirler.

2.2. SOC'un Yapısı ve İşleyişi

SOC ekipleri genellikle 7/24 çalışarak güvenlik tehditlerini analiz eder ve olay müdahalesi yapar. Çalışma süreci şu adımlardan oluşur:

- **Tehdit İzleme:** Ağ ve sistem aktiviteleri sürekli takip edilir.
- **Tehdit Tespiti:** Şüpheli olaylar analiz edilir.
- **Olay Müdahalesi:** Tespit edilen tehditlere karşı hızlı aksiyon alınır.
- **İyileştirme:** Zayıf noktalar belirlenir ve önlemler alınır.

2.3. SOC İçerisindeki Katmanlar ve Görevleri

SOC ekibi, genellikle 3 farklı seviyeden oluşur:

- **L1 :** İlk seviye analistlerdir, olayları inceler ve temel analiz yapar.
- **L2 :** Daha derin analiz yaparak olayları detaylandırır.
- **L3 :** Gelişmiş saldırıları tespit eder ve tehdit avcılığı (threat hunting) yapar.

2.4. Olay Yönetimi

Olay yönetimi, bir tehdit tespit edildiğinde nasıl hareket edileceğini belirler. SOC analistleri genellikle şu adımları izler:

1. **Olayın Tespiti** – Log ve ağ trafiği incelenir.
2. **Analiz ve Kategorilendirme** – Olayın ciddiyeti değerlendirilir.
3. **Müdahale** – Saldırının etkileri en aza indirilir.
4. **İyileştirme** – Olaydan dersler çıkarılarak güvenlik politikaları güncellenir.

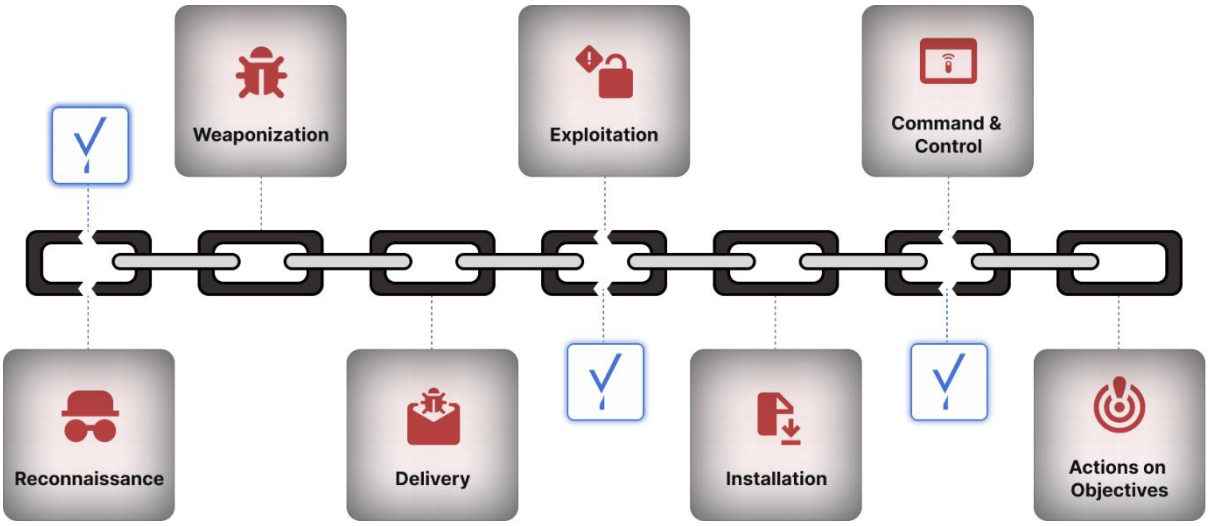
2.5. SOC'da Kullanılan Temel Araçlar

- **SIEM (Security Information and Event Management)** – Logları analiz etmek için kullanılır.
- **IDS/IPS (Intrusion Detection/Prevention Systems)** – İzinsiz girişleri tespit eder.
- **Firewall (Güvenlik Duvarı)** – Zararlı trafiği engeller.

3. CYBER KILL CHAIN

3.1. Cyber Kill Chain Nedir?

Cyber Kill Chain, siber saldırıları aşamalara ayırarak analiz etmeye yarayan bir modeldir.



3.2. Cyber Kill Chain Aşamaları

1. **Reconnaissance:** Hedef sistem hakkında bilgi toplanır.
2. **Weaponization:** Zararlı yazılım hazırlanır.
3. **Delivery:** Malware hedef sisteme ulaştırılır.
4. **Exploitation:** Açıklar kullanılarak sisteme giriş sağlanır.
5. **Installation:** Malware çalıştırılır.
6. **Command & Control:** Saldırgan sistemde kontrol sağlar.
7. **Actions on Objectives:** Veri çalınır veya sistemler zarar görür.

3.3. Cyber Kill Chain ile Saldırıları Analiz Etme

SOC analistleri, saldırının hangi aşamada olduğunu belirleyerek uygun savunma önlemleri alabilirler.

4. SONUÇ

Bu raporda SOC'un nasıl çalıştığını, Cyber Kill Chain ve MITRE ATT&CK Framework'ünü detaylıca inceledik. Siber tehditlere karşı nasıl önlem alabileceğimizi ve SOC analistlerinin olaylara nasıl müdahale ettiğini daha iyi anlamış olduk. Siber güvenlikte proaktif bir yaklaşım geliştirmenin önemini kavradık.

5. KAYNAKÇA

1. Cisco Networking Academy - Siber Güvenlik Temelleri.
2. MITRE ATT&CK Framework Documentation.
3. https://www.beyondidentity.com/collections/phishing-kill-chain-analysis
4. https://www.koenig-solutions.com/blog/all-about-soc-analyst