SOC Fundamentals & Cyber Kill Chain

Hazırlayan:Alperen Buğra AKCA

Tarih:07/02/2025

1. Giriş

Bu rapor, günümüz siber güvenlik dünyasında kritik bir rol oynayan SOC (Security Operations Center) temelleri ile siber saldırıların analizinde kullanılan Cyber Kill Chain modelini ele almaktadır.

Amaç:

- SOC'un işleyişini, temel bileşenlerini ve organizasyonlardaki rolünü açıklamak
- Cyber Kill Chain modelinin aşamalarını detaylandırarak, saldırı senaryolarını incelemek
- Her iki kavram arasındaki ilişkiyi değerlendirerek, siber güvenlik operasyonlarının etkinliğine dair çıkarımlarda bulunmaktır.

2. SOC Temelleri

2.1. SOC Nedir ?

SOC, bir organizasyonun siber güvenlik operasyonlarını 24/7 izleyen, analiz eden ve olaylara müdahale eden merkezdir. Bu yapı, potansiyel tehditlerin hızlı tespiti ve zararın minimize edilmesi amacıyla çeşitli teknolojik araçlar ve uzman ekipler tarafından desteklenir.

2.2. SOC Temel Bileşenleri Nelerdir ?

SOC (Security Operations Center) Fundamentals, bir güvenlik operasyon merkezi (SOC) içinde temel işleyişi, süreçleri ve kullanılan teknolojileri kapsayan konuları ifade eder. SOC, kuruluşların bilgi sistemlerini izleyen, tehditleri tespit eden, analiz eden ve müdahale eden bir güvenlik ekibidir.

SOC Fundamentals'ın Temel Bileşenleri

1. **SOC'un Amacı ve İşlevleri**
    a. Güvenlik olaylarını izleme ve yönetme
    b. Tehdit tespiti ve analizi
    c. Güvenlik ihlallerine müdahale
    d. Olay sonrası analiz ve raporlama
    e. Sürekli iyileştirme ve güvenlik stratejileri geliştirme
2. **SOC'un Yapısı ve Rolleri**
    a. **L1 (Tier 1) – SOC Analyst (Alert Analyst):** Güvenlik uyarılarını inceler, olası tehditleri belirler ve gerektiğinde L2'ye iletir.
    b. **L2 (Tier 2) – Incident Responder:** Güvenlik olaylarını daha derinlemesine analiz eder ve uygun müdahale prosedürlerini uygular.
    c. **L3 (Tier 3) – Threat Hunter & Forensic Analyst:** Gelişmiş tehdit avcılığı yapar, olayın kaynağını ve etkisini araştırır.
    d. **SOC Manager:** Tüm SOC operasyonlarını yönetir, güvenlik politikalarını belirler ve ekibin etkinliğini artırır.
3. **SOC Teknolojileri ve Araçları**
    a. **SIEM (Security Information and Event Management):** Logları toplar, korelasyon yapar ve tehditleri tespit eder (örn. Splunk, IBM QRadar, Elastic SIEM).
    b. **EDR (Endpoint Detection and Response):** Uç nokta tehditlerini analiz eder (örn. CrowdStrike, SentinelOne, Microsoft Defender ATP).
    c. **IDS/IPS (Intrusion Detection/Prevention Systems):** Ağ trafiğini izler ve şüpheli aktiviteleri tespit eder (örn. Snort, Suricata).
    d. **Threat Intelligence Platforms:** Tehdit istihbaratı sağlar (örn. MISP, Recorded Future).
    e. **SOAR (Security Orchestration, Automation, and Response):** Olaylara otomatik müdahale süreçleri uygular (örn. Palo Alto XSOAR, Splunk SOAR).
4. **SOC Süreçleri**
    a. Log toplama ve analizi
    b. Tehdit tespiti ve sınıflandırması
    c. Olay müdahale prosedürleri (Incident Response)
    d. Tehdit avcılığı (Threat Hunting)
    e. Olay sonrası analiz ve raporlama (Post-Incident Analysis)
5. **SOC Operasyonlarını Güçlendiren Çerçeveler**
    a. **MITRE ATT&CK Framework:** Saldırı teknikleri ve taktiklerini sınıflandırır.
    b. **NIST Cybersecurity Framework:** SOC için güvenlik kontrolleri sunar.
    c. **CIS Controls:** Temel güvenlik önlemlerini içerir.

3.CYBER KİLL CHAİN

3.1. Tanım ve Genel Bakış

Cyber Kill Chain, Lockheed Martin tarafından geliştirilen ve siber saldırıların aşamalarını sistematik olarak sınıflandıran bir modeldir. Bu model, saldırganların saldırı planlama sürecini anlamak ve savunma stratejilerini belirlemek açısından önemli bir çerçeve sunar.

3.2. Cyber Kill Chain Aşamaları

1. **Keşif (Reconnaissance):**
2. Saldırganın hedef hakkında bilgi toplaması; örneğin, ağ yapısı, açıklar ve zayıf noktalar hakkında araştırma yapılması.
3. **Silahlandırma (Weaponization):**

Toplanan bilgiler ışığında, saldırıda kullanılacak zararlı yazılım veya exploit'lerin hazırlanması.

4. **Teslimat (Delivery):**

Zararlı içeriğin hedefe ulaştırılması (e-posta eki, kötü amaçlı bağlantı, vb.).

5. **İstismar (Exploitation):**

Hedef sistemdeki açık veya zayıf noktalardan yararlanılarak zararlı yazılımın aktive edilmesi.

6. **Kurulum (Installation):**

Zararlı yazılımın sistemde kalıcı hale getirilmesi için gerekli dosya ve süreçlerin yerleştirilmesi.

7. **Komut ve Kontrol (Command and Control):**

Saldırganın, bulaşan sistem üzerinde uzaktan kontrol sağlayarak, ek saldırılar düzenlemesi.

8. **Eylem (Actions on Objectives):**

Nihai hedefe ulaşmak için veri hırsızlığı, sistem zarar verme veya diğer zararlı eylemlerin gerçekleştirilmesi

4. SOC ile Cyber Kill Chain İlişkisi

4.1. Saldırı Tespiti ve Müdahale

SOC, Cyber Kill Chain modelinin her aşamasında gerçekleşebilecek anormallikleri tespit edebilmek için tasarlanmıştır. Özellikle teslimat ve istismar aşamalarında, SIEM sistemleri ile erken uyarı mekanizmaları devreye girer. Böylece, saldırının ilerlemeden önlenmesi ve zararın minimize edilmesi sağlanır.

4.2. Operasyonel İyileştirme

Cyber Kill Chain'in analizi, SOC'un operasyonel süreçlerini optimize etme imkânı tanır. Saldırı adımlarının sistematik olarak incelenmesi, olay müdahale süreçlerinde eksikliklerin belirlenmesine ve iyileştirmelerin yapılmasına olanak verir. Bu da, organizasyonun genel siber güvenlik savunmasını güçlendirir.

5.Sonuç

Bu raporda, SOC temelleri ve Cyber Kill Chain modelinin siber güvenlik operasyonları üzerindeki önemi ele alınmıştır. SOC, siber tehditlere karşı proaktif ve reaktif müdahaleler sunarken Cyber Kill Chain modeli, saldırıların sistematik olarak anlaşılmasını ve savunma stratejilerinin geliştirilmesini sağlamaktadır. Yapılan analiz, siber güvenlik alanında hem teknolojik altyapının hem de süreçlerin sürekli güncellenmesi ve geliştirilmesinin gerekliliğini ortaya koymaktadır.

6.Kaynakça

https://www.ihsteknoloji.com/blog/guvenlik-operasyon-merkezi-soc-nedir/#Guvenlik_Operasyon_Merkezi_%E2%80%93_SOC_Nedir

https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir

https://chatgpt.com/

https://www.securefors.com/cyber-kill-chain-nedir/

https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu