

Rapor Başlığı: SOC Fundamentals

Hazırlayan: İlayda Hörgüşlüoğlu

Tarih: 07.02.2025

**SOC Fundamentals**

SOC kelimesinin kelime anlamı, Güvenlik Operasyon Merkezidir. Siber tehditlerin giderek arttığı günümüzde, tehdir tespiti, saldırı analizi ve olay müdahalesi kritik öneme sahiptir. Raporda çeşitli başlıklarla bu kavramın detaylarına inilecek ve önemi vurgulanacaktır.

1. SOC Tanımı ve Önemi

SOC, bir kuruluşun siber güvenlik altyapısını izleyen, tehditleri tespit eden ve olaylara müdahale eden merkezdir. 7/24 izleme ve analiz yapabilme yeteneğine sahiptir. Siber dayanıklılığını artırmayı hedefler. SOC'nin temel amacı, güvenlik tehditlerini minimum hasarla yönetmek ve sürekli gelişen saldırı tekniklerine karşı bir güvenlik duruşu sergilemektir.

SOC’nin en kritik unsurlarından biri, alanında uzmanlaşmış personellerdir. Uzmanlar; tehdit istihbaratı toplama, olay yönetimi ve müdahale, iyileştirme ve önleme stratejileri ile bu süreci ilerletmektedirler. Uzmanlar bu süreçlerde SIEM, EDR ve IDS/IPS gibi teknolojik araçlardan yararlanırlar.

1. SOC Süreçleri
   1. Tehdit İzleme ve Algılama: SIEM sistemleri kullanılarak anormalliklerin belirlenmesi.

* Günlük (Log) Analizi: SIEM (Security Information and Event Management) sistemleri, ağ cihazları, uç noktalar ve güvenlik duvarları gibi kaynaklardan gelen logları analiz eder.
* Anomali Tespiti: Makine öğrenimi ve davranışsal analiz araçları kullanarak olağan dışı davranışları belirleme.
* İmzaya Dayalı Tespit: IDS/IPS sistemleri ve antivirüs yazılımları, bilinen tehdit imzalarını kullanarak saldırıları tanımlar.
* Davranışsal Analiz: Kullanıcı ve varlık davranış analizleri (UEBA) ile şüpheli etkinlikleri belirleme.
* Tehdit Avcılığı (Threat Hunting): Proaktif olarak ağ içinde gizlenmiş tehditleri manuel veya otomatik analiz teknikleriyle keşfetme.
  1. Olay Yönetimi ve Müdahale: Olaylar tespit edildikten sonra, zararın en aza indirilmesi için müdahale edilmesi.
* Günlük (Log) Analizi: SIEM (Security Information and Event Management) sistemleri, ağ cihazları, uç noktalar ve güvenlik duvarları gibi kaynaklardan gelen logları analiz eder.
* Anomali Tespiti: Makine öğrenimi ve davranışsal analiz araçları kullanarak olağan dışı davranışları belirleme.
* İmzaya Dayalı Tespit: IDS/IPS sistemleri ve antivirüs yazılımları, bilinen tehdit imzalarını kullanarak saldırıları tanımlar.
* Davranışsal Analiz: Kullanıcı ve varlık davranış analizleri (UEBA) ile şüpheli etkinlikleri belirleme.
* Tehdit Avcılığı (Threat Hunting): Proaktif olarak ağ içinde gizlenmiş tehditleri manuel veya otomatik analiz teknikleriyle keşfetme.
  1. Adli Analiz (Forensics): Saldırının kaynağının belirlenmesi ve kanıtların toplanması.
  2. Raporlama ve İyileştirme: Olay sonrası süreçlerin analiz edilerek yeni önlemler geliştirilmesi.

1. SOC Mimarisi ve Teknolojileri

SOC'nin etkin bir şekilde çalışmasını sağlayan en önemli unsurlardan biri, kullanılan güvenlik teknolojileridir. Bu teknolojiler, tehditlerin tespiti, analiz edilmesi, müdahale süreçlerinin hızlandırılması ve olay yönetiminin otomatikleştirilmesi gibi kritik işlevleri yerine getirir. Aşağıda, SOC operasyonlarını destekleyen başlıca teknolojiler detaylandırılmıştır:

* 1. SIEM (Security Information and Event Management)

(Güvenlik Bilgi ve Olay Yönetimi)

SIEM sistemleri, ağdaki cihazlardan ve güvenlik araçlarından gelen logları ve olayları merkezi bir yerde toplayarak analiz eder. Temel işlevleri şunlardır:

* Gerçek Zamanlı Olay İzleme: Güvenlik olaylarını anlık olarak takip eder ve anormallikleri belirler.
* Korelasyon Analizi: Farklı sistemlerden gelen verileri ilişkilendirerek karmaşık saldırıları tespit eder.
* Tehdit Avcılığı (Threat Hunting): SIEM, tehdit istihbaratı ile entegre çalışarak SOC analistlerine derinlemesine araştırma imkanı sunar.
* Uyumluluk Yönetimi: Regülasyonlara (GDPR, ISO 27001, PCI-DSS vb.) uygunluk sağlamak için raporlar oluşturur.

Örnek SIEM çözümleri: Splunk, IBM QRadar, ArcSight, Microsoft Sentinel

* 1. UEBA (User and Entity Behavior Analytics)

(Kullanıcı ve Varlık Davranış Analitiği)

UEBA, kullanıcı ve sistem davranışlarını analiz ederek olağan dışı aktiviteleri belirleyen bir teknolojidir. SIEM’den farklı olarak, davranışsal analiz ve makine öğrenimi kullanarak tehditleri belirler.

* Normal ve Anormal Davranışın Belirlenmesi: Kullanıcının alışılmış aktiviteleriyle kıyas yaparak anormal hareketleri (örneğin bir kullanıcının normalde erişmediği bir sistemde işlem yapması) tespit eder.
* İç Tehditlerin Tespiti: Kötü niyetli çalışanlar veya ele geçirilmiş hesaplarla ilgili şüpheli aktiviteleri ortaya çıkarır.
* Gelişmiş Makine Öğrenimi Algoritmaları: Kullanıcı oturum açma alışkanlıklarını, veri erişimlerini ve sistem içi hareketleri analiz eder.

Örnek UEBA çözümleri: Exabeam, Varonis, Microsoft Defender for Identity, Splunk UEBA

* 1. SOAR (Security Orchestration, Automation, and Response)

(Güvenlik Orkestrasyonu, Otomasyon ve Müdahale)

SOAR çözümleri, güvenlik olaylarının otomatik olarak değerlendirilmesini ve müdahale süreçlerinin hızlandırılmasını sağlar.

* Olay Müdahalesini Otomatikleştirme: Örneğin, bir oltalama (phishing) saldırısı algılandığında ilgili e-posta otomatik olarak karantinaya alınabilir.
* Farklı Güvenlik Araçlarını Entegre Etme: SIEM, IDS/IPS, EDR ve tehdit istihbaratı kaynaklarını bir araya getirerek olay müdahalesini hızlandırır.
* Olaylara Müdahale Çalışma Akışları (Playbooks): Önceden tanımlı senaryolar kullanarak olayları değerlendirme ve aksiyon alma sürecini sistematik hale getirir.

Örnek SOAR çözümleri: Palo Alto Cortex XSOAR, Splunk Phantom, IBM Resilient, Microsoft Sentinel SOAR

* 1. IDS/IPS (Intrusion Detection / Prevention Systems)

(Saldırı Tespit ve Önleme Sistemleri)

IDS/IPS sistemleri, ağa yönelik saldırıları algılamak ve önlemek için kullanılır.

* IDS (Intrusion Detection System): Ağ trafiğini izleyerek şüpheli aktiviteleri ve potansiyel saldırıları tespit eder. Ancak pasif bir sistemdir ve sadece uyarı verir.
* IPS (Intrusion Prevention System): IDS’ye ek olarak saldırıları engelleyebilir. Örneğin, bir DDoS saldırısını algıladığında saldırgan IP’lerini otomatik olarak engelleyebilir.
* İmza ve Anomali Tabanlı Analiz: IDS/IPS sistemleri, bilinen tehditlere karşı imza tabanlı tespit yaparken, bilinmeyen tehditleri makine öğrenimi ve anomali tespiti ile ortaya çıkarabilir.

Örnek IDS/IPS çözümleri: Snort, Suricata, Cisco Firepower, Palo Alto Networks IPS

* 1. EDR/XDR (Endpoint Detection and Response / Extended Detection and Response)

(Uç Nokta Tespit ve Müdahale / Genişletilmiş Tespit ve Müdahale)

* EDR (Endpoint Detection and Response): Uç noktalarda (bilgisayarlar, sunucular, IoT cihazları vb.) derinlemesine tehdit analizi yapar, zararlı aktiviteleri tespit eder ve otomatik yanıt mekanizmaları sunar.
* XDR (Extended Detection and Response): EDR’nin bir üst versiyonu olup, yalnızca uç noktaları değil, e-posta güvenliği, ağ trafiği ve bulut ortamları gibi farklı bileşenleri de kapsar.
* Davranışsal Analiz: Kötü niyetli yazılımların (malware) veya fidye yazılımlarının (ransomware) aktivitelerini analiz eder ve otomatik aksiyon alır.
* Tehdit Avcılığı (Threat Hunting): SOC analistlerine proaktif tehdit avcılığı yapmaları için detaylı analiz imkanları sunar.

Örnek EDR/XDR çözümleri: CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne, Palo Alto Cortex XDR

* 1. Sandbox Teknolojileri

(Zararlı Yazılım Analiz Ortamları)

Sandbox teknolojileri, şüpheli dosyaları ve zararlı yazılımları (malware) izole bir ortamda çalıştırarak analiz eder.

* Gerçek Zamanlı Zararlı Yazılım Analizi: Dosyanın veya kodun davranışı analiz edilir ve kötü amaçlı olup olmadığı belirlenir.
* Dinamik Analiz: Statik analiz yerine, dosyanın sanal bir makinede çalıştırılmasıyla gerçek etkileri incelenir.
* Sıfırıncı Gün Saldırılarını Tespit Etme: Yeni çıkan ve imzası bilinmeyen tehditleri analiz ederek korunma imkanı sunar.

Örnek Sandbox çözümleri: FireEye AX, Palo Alto WildFire, Cuckoo Sandbox, VMware NSX Advanced Threat Analyzer

1. Sonuç

SOC, siber tehditleri tespit etmek, analiz etmek ve bu tehditlere yanıt vermek için gelişmiş teknolojiler ve süreçler kullanır. Tehdit istihbaratı, olay izleme ve tespit, güvenlik açığı yönetimi ve olay müdahale gibi temel süreçlerle SOC, sistemleri koruma görevini üstlenir. SOC'un başarısı, SIEM, SOAR, IDS/IPS, yapay zeka destekli analizler gibi modern araçlarla etkin bir şekilde çalışmasına bağlıdır. Ayrıca, kullanıcı farkındalığını artırmak ve güvenlik açıklarını minimize etmek için eğitim ve denetim süreçleri de kritik öneme sahiptir. Otomasyon ve orkestrasyon çözümleri, süreçlerin hızını ve verimliliğini artırarak tehditlere karşı daha etkin bir savunma sağlar. Sonuç olarak, SOC, siber güvenlik tehditleriyle mücadelede merkezi bir rol oynar ve tehdit ortamının sürekli değişmesi nedeniyle sürekli olarak güncellenmesi ve iyileştirilmesi gereken dinamik bir yapıya sahiptir.