06.02.2025

SOC Fundamentals

Şerif GÜL

Altay Takımı

Giriş

Güvenlik Operasyon Merkezi (Security Operations Center - SOC), bir organizasyonun bilgi güvenliği altyapısını korumak için tasarlanmış birimlerdir. SOC ekipleri, siber tehditleri tespit etmek, analiz etmek ve bunlara yanıt vermek için çeşitli teknolojiler ve prosedürler kullanır. Modern şirketler için siber güvenliğin hayati önemi nedeniyle SOC, organizasyonların siber saldırılara karşı korunmasında kritik bir rol oynar.

SOC'un Temel Bileşenleri

SOC, farklı katmanlardan ve bileşenlerden oluşur. Ana bileşenler şunlardır:

1. **Personel**
    - SOC analistleri, mühendisler ve olay yanıt ekiplerinden oluşur.
    - Tehdit avcıları ve tehdit istihbarat uzmanları.
    - Adli bilişim ve olay yanıt ekipleri.
2. **Süreçler**
    - Olay tespit ve yanıtlama prosedürleri.
    - Tehdit avcılığı ve tehdit istihbarat işlemleri.
    - Raporlama ve olay kayıt yönetimi.

3. **Teknolojiler**

SIEM (Güvenlik Bilgi ve Olay Yönetimi), organizasyonların ağlarındaki güvenlik olaylarını ve tehditleri tespit etmek, analiz etmek ve raporlamak için kullanılan bir güvenlik çözümüdür.

Özellikleri:

- Farklı kaynaklardan (firewall, antivirüs, IDS/IPS, sunucular vb.) log toplar.
- Logları analiz eder ve tehdit tespiti yapar.
- Otomatik uyarılar ve olay yanıt mekanizmaları sağlar.
- Güvenlik olaylarını merkezi bir sistemde toplayarak inceleme ve adli bilişim süreçlerini kolaylaştırır.

Örnek SIEM Çözümleri:

- **Splunk**
- **IBM QRadar**
- **Elastic Security**
- **Wazuh** (Açık kaynak)
- **Microsoft Sentinel**

IDS/IPS (Intrusion Detection and Prevention Systems)

IDS/IPS sistemleri, ağ veya sistem seviyesinde güvenlik tehditlerini tespit etmek ve bunlara karşı önlem almak için kullanılır.

IDS (Intrusion Detection System - Saldırı Tespit Sistemi)

IDS, ağ trafiğini veya sistem aktivitelerini analiz ederek şüpheli hareketleri belirler ve güvenlik ekiplerine bildirim gönderir. Ancak, IDS yalnızca uyarı verir ve doğrudan saldırıyı engelleyemez.

IPS (Intrusion Prevention System - Saldırı Önleme Sistemi)

IPS, IDS'e benzer şekilde çalışır ancak farkı, saldırıyı otomatik olarak engelleyebilmesidir. Şüpheli trafiği algıladığında bağlantıyı kesebilir veya paketi düşürebilir.

Örnek IDS/IPS Çözümleri:

- **Snort** (Açık kaynak IDS/IPS)
- **Suricata**
- **Cisco Firepower**
- **Palo Alto Networks IDS/IPS**
- **Trend Micro TippingPoint**

EDR & NDR (Gelişmiş Güvenlik Çözümleri) 🔍

EDR (Endpoint Detection and Response - Uç Nokta Tespit ve Yanıt)

EDR sistemleri, uç noktalarda (bilgisayarlar, sunucular vb.) şüpheli aktiviteleri tespit etmek ve tehditleri önlemek için kullanılır. Antivirüs çözümlerinin ötesine geçerek gelişmiş saldırıları analiz eder ve tehdit istihbaratı ile ilişkilendirir.

Özellikleri:

- Gerçek zamanlı tehdit tespiti ve analizi.
- Uç noktalar arasında bağlantılı olay incelemesi.
- Otomatik tehdit yanıt mekanizmaları (kötü amaçlı yazılımı karantinaya alma, süreçleri sonlandırma vb.).
- Siber tehdit avcılığı (Threat Hunting).

Örnek EDR Çözümleri:

- **CrowdStrike Falcon**
- **Microsoft Defender for Endpoint**
- **SentinelOne**
- **Trend Micro Apex One**

NDR (Network Detection and Response - Ağ Tespit ve Yanıt)

NDR, ağ trafiğini sürekli izleyerek şüpheli aktiviteleri tespit etmeye odaklanır. Geleneksel IDS/IPS çözümlerinin daha gelişmiş ve yapay zeka destekli versiyonlarıdır.

Özellikleri:

- Ağ trafiğini analiz eder ve anomali tespiti yapar.
- İç tehditleri ve gelişmiş siber saldırıları belirler.
- Şifrelenmiş trafiği analiz ederek tehditleri ortaya çıkarabilir.
- SIEM ve EDR çözümleriyle entegre çalışabilir.

Örnek NDR Çözümleri:

- **Darktrace**
- **Cisco Secure Network Analytics** (Stealthwatch)

- **Corelight**
- **Vectra AI**

SOC'un Temel Fonksiyonları

SOC, siber güvenlik dünyasında birden fazla kritik fonksiyon üstlenir. Bu fonksiyonlar şunlardır:

1. **Tehdit Tespiti ve Analizi**
    - Sistemlerden gelen log verilerinin analiz edilmesi.
    - Anormalliklerin tespit edilmesi ve potansiyel tehditlerin belirlenmesi.
2. **Olay Yanıtlama**
    - Saldırının tespit edilmesi ve etkisinin azaltılması.
    - Adli bilişim analizleri ve olay üzerinde derinlemesine araştırma yapılması.
3. **Tehdit Avcılığı (Threat Hunting)**
    - Aktif olarak tehditleri araştırmak ve belirlemek.
    - Daha önce bilinmeyen saldırı tekniklerini ortaya çıkarmak.
4. **Sürekli İyileştirme ve Zafiyet Yönetimi**
    - Zafiyet taramaları ve yamalama süreçlerinin yönetilmesi.
    - Saldırı örüntülerinin belirlenerek SOC'un sürekli geliştirilmesi.

SOC Seviyeleri

SOC ekipleri genellikle seviyelere ayrılır ve her seviye farklı bir sorumluluğa sahiptir:

1. Kademe:Olay Tespiti	**1. kademe SOC analisti, olayları sınıflandırmaktan ve uygun şekilde ele alınmalarını sağlamaktan sorumludur. Hangi olayların daha fazla araştırmaya ihtiyaç duyduğuna ve hangilerinin hızla çözülebileceğine karar verirler.**
2. Kademe: Olay Müdahalecileri	**2. seviye bir SOC analisti, soruşturmalar ve azaltma faaliyetleri gerçekleştirerek olaylara yanıt vermekten sorumludur. Ayrıca, saldırı altındaki sistem sorunlarını çözmek için güvenlik mühendisleri gibi diğer paydaşlarla da iş birliği yaparlar.**

3. Kademe: Tehdit Avcıları	**3. seviye bir SOC analisti, bir organizasyonun ağındaki veya altyapısındaki tehditleri avlar. Tehdit istihbarat bilgilerini kullanarak tehditlerin kaynağını belirler, tehlikelerini değerlendirir ve hasara yol açmadan önce onları durdururlar.**
SOC Mühendisi	**Bir SOC mühendisi, bir güvenlik operasyon merkezi (SOC) tasarlar, yönetir ve bakımını yapar. Hem günlük aktivitelerde hem de olaylar sırasında SOC'nin sorunsuz çalışmasını sağlamak için diğer ekip üyeleriyle yakın bir şekilde çalışırlar.**
SOC Yöneticisi	**Önceki rollerine bağlı olarak 10 ila 20 yıllık deneyime sahip bir SOC yöneticisi, SOC ekibinin günlük operasyonlarını yönetir ve tüm yönetim gereksinimlerini karşıladığından emin olur.**

SOC analistlerinin sorumluluklarından birkaçı şunlardır:

- **Bir Kuruluşun Ağ ve Sistemlerinin Gözetimi** : SOC analistleri, olası bir ihlali veya saldırıyı gösteren düzensizlikleri tespit etmek için güvenlik sistemleri, uygulamalar ve ağlar dahil olmak üzere bir kuruluşun BT altyapısını izler.
- **Güvenlik Tehditlerini Gerçek Zamanlı Olarak Belirler, Değerlendirir ve Azaltır** : Bir tehdit tanımlandıktan sonra, SOC analistleri ekipleriyle birlikte anormalliğin nedenini belirlemek ve gelecekte tekrarlanmasını önlemek için önleyici tedbirler almak üzere çalışır.
- **Olay Müdahalesi ve Soruşturma** : Daha fazla soruşturma veya kolluk kuvvetlerinin dahil olması gerekiyorsa, SOC analistleri, gerekirse yetkililere bildirmeden önce olayları iyice araştırmak için ekip üyeleriyle iş birliği yapar. Ayrıca, gelecekteki olayları önlemek için mevcut tehditler veya güvenlik açıkları hakkında edinilen yeni bilgileri de belgelendirirler.
- **Güvenlik Prosedürlerini, Çözümlerini ve En İyi Uygulamalarını Uygulamak İçin Diğer Ekip Üyeleriyle İş Birliği Yapar** : SOC analistleri, kuruluş içinde devam eden güvenli ve emniyetli operasyonları sağlamak için ekipleriyle birlikte güvenlik sistemlerini ve prosedürlerini uygulamak ve güncellemek için çalışır.
- **En Son Güvenlik Tehditleri Hakkında Güncel Kalın** : SOC analistleri, kimlik avı girişimleri ve yeni saldırı araçları gibi ortaya çıkan siber tehditler hakkında bilgi sahibi olarak olası sorunlara karşı hızlı bir şekilde harekete geçebilirler.
- **Güvenlik Denetimlerine Katılır** : SOC analistleri, verilerin hazırlanması ve incelenmesine yardımcı olarak güvenlik denetimlerine katılır ve güvenlik açıklarının istismar edilmeden önce belirlenmesine yardımcı olur.

SOC'un Karşı Karşıya Olduğu Zorluklar

SOC ekipleri birçok zorlukla karşı karşıya kalabilir:

- **Sinyal gürültüsü (Noise):** Yanlış pozitif alarmların fazla olması.
- **Tehditlerin Evrimi:** Yeni siber saldırı tekniklerinin ortaya çıkması.
- **Personel Eksikliği:** Kalifiye SOC personeli bulmakta zorluklar.
- **Otomasyon ve Yapay Zeka Kullanımı:** SOC işlemlerini hızlandırmak için yeni teknolojilere adaptasyon.

Kaynakça:

Gaissecurity.com

splunk.com

springboard.com

sans.org

chatgpt.com