SOC Fundamentals

Hazırlayan
Burak Ali DÜZÜN

07.02.2025

İÇİNDEKİLER

SOC Fundamentals 1

SOC'un Temel Yapı Taşları ve İşleyişi 1

SOC Katmanları (L1, L2, L3) ve Analist Rolleri 1

Olay Yönetimi Süreçleri 2

SOC'da Kullanılan Temel Araçlar 2

SOC'un Siber Güvenlik Ekosistemindeki Rolü 2

Kaynakça 3

SOC Fundamentals

Siber güvenlik operasyon merkezi (Security Operations Center - SOC), bir organizasyonun dijital varlıklarını tehditlerden korumak, veri ihlallerini önlemek ve siber olaylara etkili bir şekilde müdahale etmek için oluşturulmuş merkezi bir yapıdır. SOC, modern organizasyonlarda sadece bir savunma hattı değil, aynı zamanda iş sürekliliğini ve operasyonel verimliliği sağlamak için stratejik bir öneme sahiptir. SOC Fundamentals, bu merkezin temel yapısı, katmanları, analistlerin rollerini ve kullandığı teknolojileri kapsamaktadır. Bu raporda, SOC'un temel işlevleri ve bileşenleri detaylı bir şekilde ele alınacak ve siber güvenlik ekosistemindeki rolü üzerine odaklanılacaktır.

---

1. SOC'un Temel Yapı Taşları ve İşleyişi:

SOC, organizasyonların siber tehditlere karşı etkili bir şekilde savunma yapmasını sağlamak üzere çeşitli bileşenlerden oluşur:

- **Tehdit Tespiti**:

  Siber tehditlerin ve potansiyel saldırıların erken tespiti, organizasyonun zarar görmesini önler.

- **Olay Yanıtı**:

  Tespit edilen tehditlere hızlı yanıt verilerek sistemlerin korunması sağlanır.

- **Log ve Veri Analizi**:

  Sistemlerden toplanan log verileri analiz edilerek, anormal davranışların belirlenmesi ve raporlanması sağlanır.

- **Proaktif Savunma**:

  Gelecekteki tehditlerin etkisini azaltmak için politika ve prosedürler geliştirilir.

2. SOC Katmanları (L1, L2, L3) ve Analist Rolleri:

SOC, çoğunlukla işlevsel olarak üç temel katmana ayrılır ve her katmanda farklı uzmanlıklar gerektiren roller bulunur:

- **L1 (Seviye 1 - Tehdit Tespiti ve Alarm Değerlendirme)**:

  L1 analistleri, SOC'un ilk savunma hattını oluşturur. Gelen alarmları izler, olayın öncelik düzeyini belirler ve gerekirse üst seviyeye aktarır. Bu seviyede, SIEM gibi temel izleme sistemleri aktif olarak kullanılır.

- **L2 (Seviye 2 - Olay Analizi ve Müdahale)**:

  L2 analistleri, L1 seviyesinden gelen olayların kök nedenini araştırarak daha ayrıntılı bir analiz yapar. Aynı zamanda, gerektiğinde siber olaylara müdahale ederek sistemlerin normal durumuna geri dönmesini sağlar.

- **L3 (Seviye 3 - Uzman Desteği ve Proaktif Savunma)**:

  L3 analistleri, SOC'un en teknik seviyesini temsil eder. Sıkça karmaşık tehdit analizi yapar, ileri düzeyde tehdit istihbaratı toplar ve uzun vadeli savunma stratejileri geliştirir.

3. Olay Yönetimi Süreçleri:

SOC'un etkinliği, olay yönetimi süreçlerinin verimli bir şekilde yürütülmesine bağlıdır. Bu süreçler üc ana başlıkta incelenir:

- **İzleme**:

  SOC, 7/24 çalışan izleme sistemleriyle ağ trafiğini, kullanıcı etkinliklerini ve sistem davranışlarını gözetler. SIEM (Security Information and Event Management) sistemleri ve IDS/IPS teknolojileri, bu aşamada kritik rol oynar.

- **Analiz**:

  Tespit edilen anomaliler ve olaylar detaylı bir şekilde incelenir. Bu aşama, L1 analistlerinden başlayarak L2 analistlerinin derinlemesine analiz yapmasını gerektirir.

- **Olay Müdahalesi**:

  Kritik bir tehdit tespit edildiğinde, SOC analistleri müdahaleye geçer. Bu süreç, hem teknik hem de operasyonel adımları içerir; örneğin, enfekte sistemlerin izole edilmesi ve zararlı yazılımların temizlenmesi gibi.

4. SOC'da Kullanılan Temel Araçlar:

SOC'un etkinliğini sağlamak için çeşitli yazılım ve donanım çözümleri kullanılır:

- **SIEM (Güvenlik Bilgi ve Olay Yönetimi)**:

  SOC'un temel taşı olarak kabul edilen bu sistemler, farklı kaynaklardan gelen log verilerini toplar, analiz eder ve tehditleri önceliklendirir.

- **IDS/IPS (Saldırı Tespit ve Önleme Sistemleri)**:

  Anormal ağ hareketlerini ve potansiyel tehditleri belirler. IDS, saldırıyı tespit ederken IPS, bu saldırıların aktif olarak engellenmesini sağlar.

- **Tehdit İstihbaratı Araçları**:

  Yeni ve gelişen tehditlerin önceden tespit edilmesi ve buna uygun önlemler alınmasını sağlar.

- **Log Yönetim Sistemleri**:

  Organizasyon genelinde oluşan log verilerini anlamlı raporlar ve şablonlar haline getirir. Bu sistemler, anormalliklerin daha hızlı tespit edilmesine yardımcı olur.

- **Endpoint Detection and Response (EDR) Sistemleri:**

  EDR sistemleri, uç noktalarda (bilgisayarlar, mobil cihazlar vb.) meydana gelen şüpheli etkinlikleri izler. Bu sistemler, SOC ekiplerine detaylı analiz ve tehdit algılama için görüş sağlar.

- **Olay Biletleme Sistemleri:**

  SOC ekiplerinin çalışma süreçlerini düzenleyen biletleme sistemleri, tehditlerin hangi seviyede olduğunu ve kim tarafından çözüleceğini takip etmeye yarar. Bu sistemler, olay yönetimini daha organize hale getirir.

5. SOC'un Siber Güvenlik Ekosistemindeki Rolü:

SOC, modern siber güvenlik ekosisteminin vazgeçilmez bir bileşenidir. Organizasyonun dijital varlıklarını korurken aynı zamanda operasyonel devamılılığı sağlar. SOC, sadece saldırılara karşı bir savunma hattı değil, aynı zamanda uzun vadeli bir siber strateji geliştirme aracıdır. Regülasyonlara uyum, veri gizliliği ve operasyonel şeffaflık açısından SOC'un katkıları büyüktür.

Sonuç olarak; SOC Fundamentals bilgisini edinmek, birey ve kurumlar için çok yönlü avantajlar sağlar. Bireysel anlamda, SOC yapısını ve işleyişini kavrayan bir analist, siber güvenlik alanında daha etkin rol alabilir, sorunlara çözüm odaklı yaklaşımlar geliştirerek kariyerinde ilerleme kaydedebilir. Organizasyonel düzeyde ise SOC, tehditleri önceden tespit ederek operasyonel sürekliliği sağlar, veri ihlallerini minimize eder ve çalışan verimliliğini artırır.

SOC'un temel işlevlerini ve bileşenlerini anlamak, bir kurumun dijital ekosisteminde güvenli bir altyapı oluşturmasına olanak tanır. Bunun yanında, regülasyonlara uyum ve risk yönetimi açısından da önemli avantajlar sağlar. Bu bilgiler ışığında, SOC'un sadece bir savunma mekanizması değil, aynı zamanda stratejik bir varlık olarak ele alınması gerektiği açıktır.

Son olarak, SOC'a dair bilgi ve beceriler, siber tehditlerin karmaşıklığının arttığı bir dönemde hem bireyler hem de kurumlar için kritik bir fark yaratır. Bu kazanımlar, siber güvenlik alanında daha bilinçli, etkin ve dirençli bir yaklaşımı mümkün kılar.

KAYNAKÇA

- https://iritt.medium.com/soc-fundamentals-cyber-security-101-defensive-security-tryhackme-walkthrough-82b1093bea59
- https://www.youtube.com/watch?v=XZHJphBJN_U
- https://www.cover6solutions.com/courses/socanalystprep/lessons/soc-analyst-fundamentals/#:~:text=A%20Security%20Operation%20Center%20is,identify%20and%20mitigate%20network%20threats.
- https://www.trellix.com/security-awareness/operations/what-is-soc/
- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/#:~:text=The%20function%20of%20the%20security,business%20systems%2C%20and%20brand%20integrity.