# SOC FUNDEMENTALS

**HAZIRLAYAN: ALİ BERK CENGİZ**

**07/02.2025**

# İçindekiler

# Giriş

Security Operations Center (SOC), bir kuruluşun bilgi güvenliği altyapısını izlemek, analiz etmek, korumak ve iyileştirmek amacıyla kurulan merkezi bir birimdir. Günümüzde siber tehditlerin karmaşıklığı ve sıklığı arttıkça, kuruluşların dijital varlıklarını korumak için daha sofistike ve proaktif güvenlik önlemlerine ihtiyaç duyulmaktadır. SOC, bu ihtiyacı karşılamak üzere tasarlanmış bir yapıdır ve siber güvenlik operasyonlarının kalbi olarak kabul edilir.

SOC'un temel amacı, kuruluşun Information Technology altyapısını sürekli olarak izlemek, olası tehditleri tespit etmek, bu tehditlere hızlı bir şekilde müdahale etmek ve güvenlik ihlallerinin etkisini en aza indirmektir. Bunu yaparken, SOC ekipleri çeşitli güvenlik araçlarını ve teknolojilerini kullanır. Bu araçlar arasında SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems), SOAR (Security Orchestration, Automation, and Response) ve EDR (Endpoint Detection and Response) gibi sistemler bulunur.

# SOC Fundementals

## SOC'un Temel İşlevleri:

**Monitoring:** Ağ trafiği, sunucular, uç noktalar ve diğer kritik sistemler sürekli olarak izlenir.

**Threat Detection:** Anormal aktiviteler, olası saldırılar ve güvenlik ihlalleri tespit edilir.

**Incident Response:** Tespit edilen güvenlik olaylarına hızlı ve etkili bir şekilde müdahale edilir.

**Log Yönetimi:** Sistemlerden toplanan loglar analiz edilerek olası tehditler belirlenir.

**Güvenlik Açığı Yönetimi:** Sistemlerdeki güvenlik açıkları tespit edilir ve bu açıklıklar kapatılır.

**Raporlama ve Analiz:** Güvenlik olayları ve tehditler hakkında raporlar hazırlanır ve analizler yapılır.

## SOC'nin Bileşenleri:

SIEM (Security Information and Event Management): Güvenlik olaylarını toplar, analiz eder ve raporlar.

IDS/IPS (Intrusion Detection/Prevention Systems): Ağdaki anormal aktiviteleri tespit eder ve engeller.

SOAR (Security Orchestration, Automation, and Response): Güvenlik operasyonlarını otomatikleştirir ve olay müdahalesini hızlandırır.

Endpoint Detection and Response (EDR): Uç noktalardaki tehditleri tespit eder ve müdahale eder.

Threat Intelligence: Güncel tehdit bilgilerini toplar ve analiz eder.

## SOC Ekibi ve Rolleri:

**SOC Analisti:** Güvenlik olaylarını izler, analiz eder ve ilk müdahaleyi yapar.

**Incident Responder:** Güvenlik ihlallerine müdahale eder ve ihlallerin etkisini azaltır.

**Threat Hunter:** Proaktif olarak ağdaki olası tehditleri arar ve tespit eder.

**SOC Manager:** SOC operasyonlarını yönetir, stratejiler belirler ve raporlama yapar.

**Forensic Analyst:** Güvenlik ihlallerinin detaylı analizini yapar ve delil toplar.

## SOC'un Faydaları

**Proaktif Güvenlik:** Tehditler henüz zarar vermeden tespit edilir ve önlenir.

**Hızlı Müdahale:** Güvenlik olaylarına hızlı bir şekilde müdahale edilir, zarar minimize edilir.

**Uyumluluk:** Yasal düzenlemelere ve standartlara uyum sağlanır.

**Farkındalık:** Kuruluşun güvenlik duruşu sürekli olarak izlenir ve iyileştirilir.

## SOC'un Karşılaştığı Zorluklar

**Yüksek Hacimli Veri:** Büyük miktarda log ve olay verisini yönetmek zor olabilir.

**Yetersiz Kaynaklar:** SOC ekipleri genellikle yetersiz kaynaklarla çalışmak zorunda kalır.

**Sürekli Güncelleme:** Siber tehditler sürekli evrim geçirdiği için SOC'un sürekli güncellenmesi gerekir.

**Yanlış Pozitifler:** Yanlış alarmlar, ekiplerin zamanını alabilir ve gerçek tehditlerin gözden kaçmasına neden olabilir.

## SOC'un Geleceği

**Yapay Zeka ve Makine Öğrenmesi:** AI ve ML, tehdit tespiti ve olay müdahalesini otomatikleştirecek.

**Bulut Güvenliği:** Bulut tabanlı sistemlerin artmasıyla birlikte SOC'un bulut güvenliğine odaklanması gerekecek.

**Zero Trust Architecture:** Güvenilir olmayan her türlü erişimi engelleyen Zero Trust modelleri yaygınlaşacak.

**Otomasyon:** SOAR gibi araçlarla güvenlik operasyonları daha da otomatikleşecek.

## Sonuçlar

Güvenlik Operasyon Merkezi (SOC), siber tehditlere karşı savunmanın ön saflarında yer alır ve modern organizasyonların güvenlik stratejisinde kritik bir rol oynar. Özellikle dijital dönüşümün hızlandığı ve siber tehditlerin her geçen gün daha karmaşık hale geldiği bir dönemde, SOC'un etkinliği bir organizasyonun güvenlik duruşunu belirleyen temel faktörlerden biridir.

SOC, sürekli izleme, proaktif tehdit avcılığı ve hızlı olay müdahalesi sayesinde hem tehditlerin tespit edilmesini hem de güvenlik olaylarının etkisinin en aza indirilmesini sağlar. Olaylara erken müdahale edilmesi ve uygun iyileştirme adımlarının atılması, veri ihlallerinin ve operasyonel kesintilerin önlenmesine yardımcı olur.

SOC ekiplerinin başarısı, sadece teknolojiye değil, aynı zamanda insan kaynağına, süreçlerin etkinliğine ve sürekli gelişime bağlıdır. Eğitimli ve tecrübeli bir ekip, doğru araçlarla donatıldığında, siber güvenlik ekosisteminde proaktif bir yaklaşım benimseyebilir ve organizasyonların karşılaşabileceği riskleri büyük ölçüde azaltabilir.

Geleceğe yönelik olarak, yapay zeka (AI) ve makine öğrenimi gibi ileri teknolojilerin SOC süreçlerine entegrasyonu, tehditlerin daha hızlı ve daha doğru şekilde tespit edilmesini sağlayacaktır. Bunun yanı sıra, küresel tehdit istihbarat ağları ve otomatik olay müdahale araçları da SOC operasyonlarının verimliliğini artıracaktır.

## Kaynakça

https://iritt.medium.com/soc-fundamentals-cyber-security-101-defensive-security-tryhackme-walkthrough-82b1093bea59

https://www.ibm.com/think/topics/security-operations-center

SANS Institute, "Best Practices for Building a Security Operations Center (SOC)", 2021. https://www.sans.org