# SOC FUNDAMENTALS

**HAZIRLAYAN:** MURAT GÜRSOY
**TARİH:** 29/01/2025

# İçindekiler

# Giriş

Günümüzde siber tehditler hızla artmakta ve kurumsal yapıları ciddi anlamda tehdit etmektedir. Bu tehditlere karşı koyabilmek için, Security Operations Center (SOC) yapılandırılmakta ve aktif olarak kullanılmaktadır. SOC, siber sızma ve siber sıkıntıların önlenmesi, tespit edilmesi ve zamanında müdahale edilmesi konusunda kritik bir rol oynar.

Bu raporda SOC yapısının temel bölümleri, işlemleri ve siber güvenlik stratejileri detaylı olarak ele alınacaktır.

## Security Operations Center (SOC)

SOC, kurumların siber tehditlere karşı korunmasını sağlayan merkezi bir güvenlik birimidir. Temel amacı, ağ trafiğini, sistemleri ve uygulamaları izleyerek siber sızma girişimleri ve tehditleri zamanında tespit edip müdahale etmektir.

### SOC'nin Temel Bileşenleri

SOC'nin etkili çalışabilmesi için üç temel bileşene ihtiyacı vardır:

#### *1. İnsan Kaynağı (SOC Ekibi)*

SOC ekibi farklı rollerde uzmanlardan oluşur:

- **Layer1 Analist:** Olay izleme ve analizini yapar.
- **Layer2 Analist:** Daha derin analiz ve olay müdahalesi gerçekleştirir.
- **Layer3 Analist (Threat Hunter):** Gelişmiş tehditleri proaktif olarak tespit eder.
- **SOC Yöneticisi:** SOC operasyonlarının tamamını yönetir.

#### *2. Teknoloji ve Araçlar*

SOC operasyonlarını destekleyen başlıca teknolojiler:

- **SIEM (Security Information and Event Management)**
- **IDS/IPS (Intrusion Detection/Prevention Systems)**
- **EDR (Endpoint Detection and Response)**
- **Threat Intelligence (Tehdit İstihbarat Araçları)**

#### *3. Süreçler ve Prosedürler*

SOC'nin verimli çalışabilmesi için aşağıdaki prosedürler kritik öneme sahiptir:

- **Olay Müdahale Süreci:** Tehditlerin tespiti ve müdahalesi.
- **İzleme ve Analiz Süreci:** Sistemlerin 7/24 gözetlenmesi.
- **Tehdit Avcılığı (Threat Hunting):** Gizli tehditleri belirleme.

### SOC Operasyonları ve Güvenlik Stratejileri

SOC, hem reaktif hem de proaktif olarak tehditleri engellemek için çeşitli stratejiler uygular:

- **Olay Tespiti ve Müdahale**: Anomali tespiti ve hızlı aksiyon alma.
- **Tehdit İstihbaratı**: Saldırganların kullandığı yöntemleri analiz etme.
- **Proaktif Güvenlik Yaklaşımı**: Sızma testleri ve çalışan eğitimleri.

### SOC'nin Önemi

SOC, kurumların siber sızma ve veri kaybı gibi büyük tehditlerden korunmasında kritik bir role sahiptir. Gelişen yapay zekâ ve otomasyon teknolojileri sayesinde SOC operasyonlarının daha etkin hale gelmesi beklenmektedir.

## Sonuç

SOC, siber güvenliğin temel taşlarından biridir. Doğru teknoloji ve uzman kadro ile çalıştığında, siber tehditleri etkili bir şekilde tespit ve müdahale edebilir.

# Kaynakça


1. https://blog.defarch.com/blue-team/01-soc-fundamentals
2. https://attack.mitre.org
3. https://medium.com/@aykutbayram/soc-fundamentals-letsdefend-8f5d4151b9d8
4. https://www.nist.gov/cyberframework