

Siber Güvenlik Operasyon Hizmeti (SOC)

Kurumların siber güvenlik olaylarını 7/24 izleyen, analiz eden ve müdahale süreçlerini yöneten merkezi operasyon hizmetidir. SOME süreçleri, tehdit analizi ve olay müdahale operasyonlarının tek merkezden yürütülmesini sağlar.

Kurumların Siber Güvenlik Zorlukları

Kurumlar; gelişmiş tehditler, fidye yazılımları, veri sızıntıları ve iç tehditler nedeniyle sürekli izleme ihtiyacı duyar. Dağınık log yapıları ve manuel analiz süreçleri kritik olayların geç fark edilmesine neden olur. SOC hizmeti; farklı güvenlik sistemlerinden gelen verileri merkezi olarak analiz eder, tehditleri önceliklendirir ve hızlı aksiyon alınmasını sağlar.

- ⚠ Hangi Ekiplere Yardımcı olur?
- Güvenlik olaylarını geç fark eden kurumlar için
 - Manuel log analizi yapan operasyon ekipleri için
 - Yanlış alarm yönetiminde zorlanan SOC ekipleri için
 - 7/24 izleme ve müdahale ihtiyacı olan kurumlar için

Temel İlkeler

			
Doğruluk	Hızlı Müdahale	Sürekli İzleme	Görünürlük
Yanlış alarm azaltımı	Kritik olaylara hızlı aksiyon	7/24 kesintisiz olay takibi	Merkezi log ve olay görünürlüğü

SOC Hizmeti Nasıl Çalışır?

SOC hizmeti; güvenlik ürünlerinden gelen logları merkezi SIEM altyapısında toplar. Olaylar korelasyon kuralları ve tehdit istihbaratı ile analiz edilir, kritik alarmlar önceliklendirilerek müdahale süreçleri yönetilir.

Teknik Özellikler

Log Toplama ve İzleme

- ✓ Farklı kaynaklarda SIEM analizi
- ✓ Bütünleşik log entegrasyonu
- ✓ Aktif log sürekliliği takibi
- ✓ Hata ve erişilebilirlik takibi

SIEM ve Olay Yönetimi

- ✓ Anomali tehdit analizi
- ✓ Dinamik tehdit korelasyonu
- ✓ IP ve kullanıcı görünürlüğü
- ✓ Risk odaklı alarm optimizasyonu

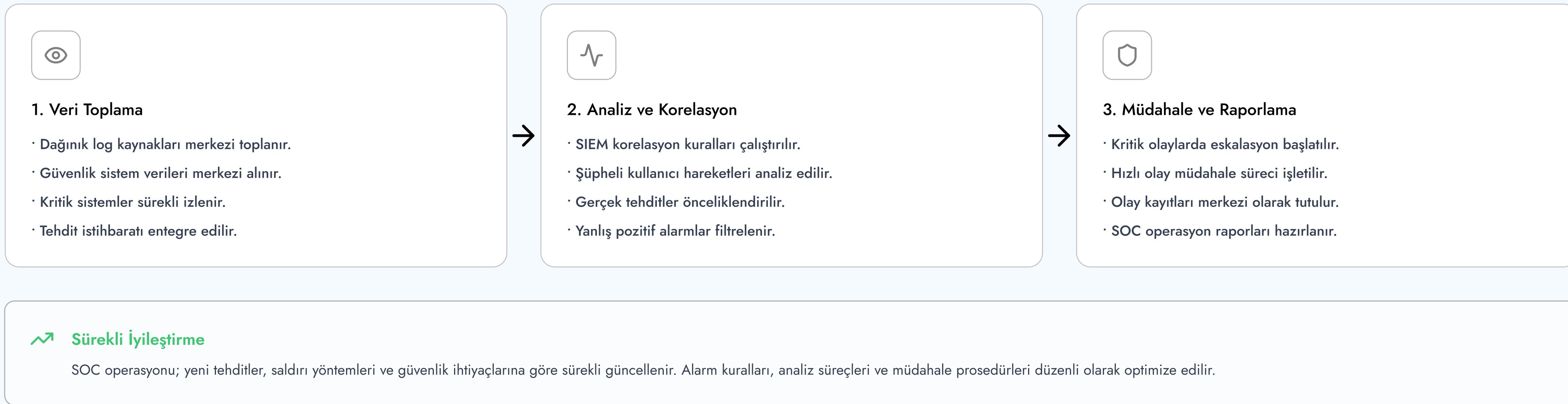
Tehdit İstihbaratı

- ✓ Zararlı IP ve hash takibi
- ✓ Güncel IOC entegrasyonu
- ✓ Kuruma özel tehdit avcılığı
- ✓ Saldırı trend analizleri

Raporlama ve Operasyon

- ✓ Merkezi SOC olay raporları
- ✓ SLA bazlı müdahale takibi
- ✓ Denetim ve kayıt desteği
- ✓ 7/24 SOC operasyon desteği

Çalışma Akışı



Avantajlar

 7/24 Güvenlik İzleme Güvenlik olayları merkezi SOC operasyon yapısında 7/24 izlenir, değerlendirilir ve kritik alarmlar anlık takip edilir.	 Olay Müdahale Yönetimi Kritik olaylarda SOME süreçleri kapsamında hızlı müdahale, eskalasyon yönetimi ve olay koordinasyonu sağlanır.
 SIEM Log Analizi Farklı güvenlik sistemlerinden gelen loglar merkezi SIEM altyapısında ilişkilendirilir, analiz edilir ve raporlanır.	 Tehdit İstihbaratı Tehdit analizi süreçlerinde güncel IOC, zararlı IP ve güvenlik istihbaratı verileri aktif olarak kullanılır.