aa teknoloji

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
Yanlış alarm azaltımı

Hızlı Müdahale
Kritik olaylara hızlı aksiyon

Sürekli İzleme
7/24 kesintisiz olay takibi

Görünürlük
Merkezi log ve olay görünürlüğü

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

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.

Çalışma Akışı

1. Veri Toplama
- Dağınık log kaynakları merkezi toplanır.
- Güvenlik sistem verileri merkezi alınır.
- Kritik sistemler sürekli izlenir.
- Tehdit istihbaratı entegre edilir.

→

2. Analiz ve Korelasyon
- SIEM korelasyon kuralları çalıştırılır.
- Şüpheli kullanıcı hareketleri analiz edilir.
- Gerçek tehditler önceliklendirilir.
- Yanlış pozitif alarmlar filtrelenir.

→

3. Müdahale ve Raporlama
- Kritik olaylarda eskalasyon başlatılır.
- Hızlı olay müdahale süreci işletilir.
- Olay kayıtları merkezi olarak tutulur.
- SOC operasyon raporları hazırlanır.

Sürekli İyileştirme
SOC operasyonu; yeni tehditler, saldırı yöntemleri ve güvenlik ihtiyaçlarına göre sürekli güncellenir. Alarm kuralları, analiz süreçleri ve müdahale prosedürleri düzenli olarak optimize edilir.

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.

aa teknoloji

AA Teknoloji, modern haber merkezleri için geliştirilen yapay zekâ destekli medya teknolojileri platformudur. Haber akış sistemlerinden dijital arşiv çözümlerine, gerçek zamanlı yayın altyapılarından çok kanallı içerik yönetimine kadar uzanan entegre çözümlerimiz; medya kuruluşlarının dijital dönüşüm süreçlerini hızlandırır ve ölçeklenebilir yayın operasyonları sunar.

Daha fazla bilgi için, aateknoloji.tr'yi ziyaret edin veya @aateknoloji LinkedIn hesabını takip edin.