

TEST VE İZLEME

SOC / SIEM Kurulumu

Ağ, sistem ve uygulama kayıtlarınızı merkezi olarak toplayan, ilişkilendiren ve anlamlı uyarılara dönüştüren izleme altyapısını kurmanıza destek oluyoruz.



6

kapsam alanı

5

adımlı yöntem

6

teslim edilen çıktı

// NEDEN ÖNEMLİ?

Neden önemli?

Saldırıların çoğu önce iz bırakır; ancak bu izler dağınık kayıtlar arasında kaybolur. SIEM ve SOC yaklaşımı olayları tek merkezden görmenizi ve zamanında müdahale etmenizi sağlar.



Marka bağımsız çalışırız: ihtiyacınıza, bütçenize ve mevcut altyapınıza uygun çözümü birlikte seçeriz.

// KİMLER İÇİN?

Bu hizmet kimler için uygun?



Merkezi log ve olay izlemesi olmayan kuruluşlar



Mevcut SIEM'inden yeterli verim alamayanlar



Düzenlemeler gereği kayıt tutma ve izleme yükümlülüğü olanlar



Kendi SOC'unu kurmak isteyen kuruluşlar

// KAPSAM

Neleri kapsıyor?



Log kaynaklarının belirlenmesi

Hangi sistemlerin hangi kayıtlarının izlenmesi gerektiğini önceliklendiririz.



SIEM kurulumu

Platform seçimine, kurulumuna ve log entegrasyonlarına destek oluruz.



Korelasyon kuralları

Kullanım senaryolarını MITRE ATT&CK ile eşleştirerek tespit kuralları geliştiririz.



Uyarı ayarı

Yanlış alarmları azaltır, gerçek tehditleri öne çıkarırız.



Pano ve raporlama

Operasyon ve yönetim için anlamlı panolar ve düzenli raporlar kurarız.



SOC süreçleri

Olay sınıflandırma, eskalasyon ve müdahale iş akışlarını tanımlarız.

Saldırgan gibi düşünür, savunmacı gibi inşa ederiz.

// ÇALIŞMA YÖNTEMİ

Nasıl ilerliyoruz?

1

İhtiyaç ve kaynak analizi

Hedefleri, kritik varlıkları ve mevcut log kaynaklarını çıkarırız.

2

Mimari ve ürün seçimi

Ürün bağımsız olarak size uygun mimariyi ve çözümü belirleriz.

3

Kurulum ve entegrasyon

Platformu kurar, log kaynaklarını bağlarız.

4

Kural geliştirme ve ayar

Kullanım senaryolarını devreye alır, uyarıları ayarlarız.

5

Devreye alma ve devir

Ekibinizi eğitir, operasyon süreçlerini devrederiz.

// ÇIKTILAR

Neler teslim ediyoruz?



İzleme mimarisi dokümanı



Korelasyon kuralları ve kullanım senaryoları listesi



SOC süreç ve olay müdahale iş akışları



Log kaynak envanteri



Operasyon ve yönetim panoları



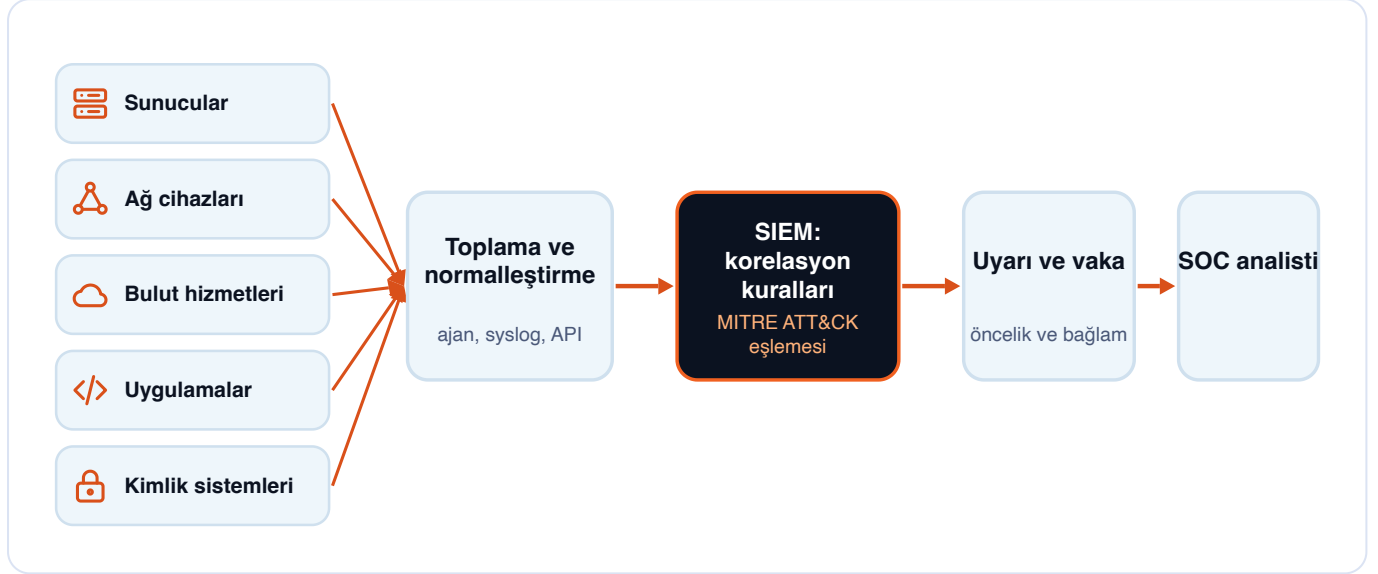
Eğitim ve devir dokümanları

// GÖRSEL ANLATIM

Konuya özel görseller

Log kaynaklarından müdahaleye: SOC/SIEM veri akışı

Dağıtık kayıtlar merkezde toplanır, kurallarla ilişkilendirilir ve analistin önüne anlamlı uyarı olarak gelir.

**Tek görünüm**

Tüm kaynaklardaki olaylar merkezde, ortak formatta incelenir.

Anlamlı uyarı

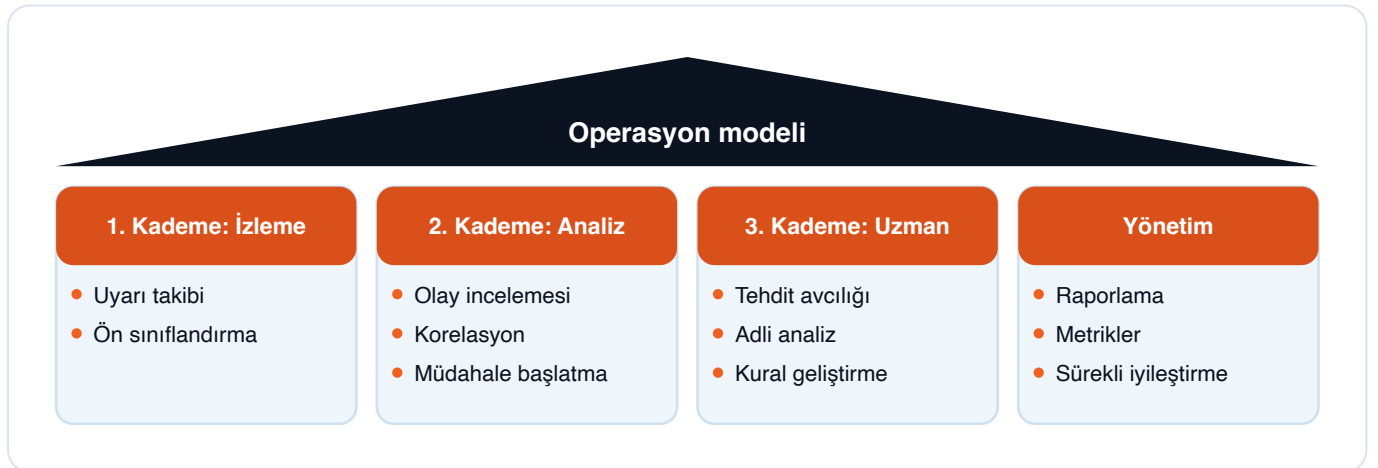
Korelasyon kuralları tekil olayları gerçek tehdit senaryolarına bağlar.

Gürültü ayarı

Kural ayarı yanlış alarmı azaltır, analistin zamanını korur.

SOC kademeleri ve görev dağılımı

Kademeli yapı, uyarıların doğru kişiye doğru derinlikte ulaşmasını sağlar.

**Doğru derinlik**

Basit uyarılar 1. kademede kapanır, karmaşık olaylar yukarı taşınır.

Proaktif avcılık

3. kademe uyarı beklemeden tehdit arar.

Ölçülür operasyon

Metrikler SOC performansını ve iyileşmesini gösterir.

// GÖRSEL ÖZET

Hizmete genel bakış

KAPSAM HARİTASI



UYGULAMA DÖNGÜMÜZ



// TEK ÇATI ALTINDA

Diğer hizmetlerimiz

- | | | |
|----------------------------------|------------------------------------|--------------------------------------|
| ISO 27001 Danışmanlığı | ISO 22301 Danışmanlığı | ISO 14298 Danışmanlığı |
| KVKK Uyum Danışmanlığı | Siber Güvenlik Danışmanlığı | Risk Yönetimi Danışmanlığı |
| Sızma Testi | Düzenli Zafiyet Tarama ve Yönetimi | DoS, DDoS Testleri ve Koruma Hizmeti |
| Endpoint Security İzleme Hizmeti | Güvenli Yazılım Geliştirme | Bilgi Güvenliği Farkındalık Programı |
| Olay Müdahale Hazırlığı | | |

// İLETİŞİM

Bize ulaşın

İhtiyacınızı ve mevcut durumunuzu paylaşın; size uygun kapsamı ve yol haritasını birlikte belirleyelim. Bilgi formumuzu doldurabilir veya doğrudan bize ulaşabilirsiniz.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul

T 0-216-575 5222 **E** info@troybilgiteknojileri.com

Hizmet sayfası ve bilgi formu
için QR kodu okutun