

REHBER

SOC/SIEM Projesine Başlarken

Merkezi log izleme ve SOC kurmayı düşünen kurumlar için: nereden başlanır, hangi sorular sorulur ve başarı nasıl ölçülür?



REHBER

YAKLAŞIK 7 DK OKUMA

SOC / SIEM

BU REHBERDE

1. SIEM, SOC ve EDR: fark nedir?
2. Başlamadan önce sorulacak sorular
3. Proje yol haritası
4. Log kaynağı önceliği
5. Kullanım senaryoları ve ayar
6. Başarı ölçütleri

01 SIEM, SOC ve EDR: fark nedir?

SIEM

Farklı kaynaklardan logları toplayıp ilişkilendiren ve uyarı üreten platform. Bir araçtır.

SOC

Uyarıları sürekli izleyen, inceleyen ve müdahale eden ekip ve süreçtir. İnsan ve süreçtir.

EDR / XDR

Uç noktalarda (XDR'da daha geniş kaynaklarda) tespit ve müdahale sağlar; SIEM'e veri besler.

Yönetilen hizmet

SIEM/SOC'un bir kısmını veya tamamını hizmet sağlayıcı işletir (MDR, yönetilen SOC).

Önemli: SIEM almak SOC kurmak değildir. Uyarıları izleyecek insan ve süreç yoksa araç değer üretmez.

02

Başlamadan önce sorulacak sorular

- Hangi tehditlere ve hangi kritik varlıklara karşı görünürlük istiyoruz?
- Hangi log kaynakları mevcut, hangileri açılmalı?
- Saklama süresi ve uyum gereksinimleri neler?
- 7/24 izleme için ekibimiz var mı, yoksa hizmet mi alacağız?
- Başarıyı nasıl ölçeceğiz?

03

Proje yol haritası

1

Kapsam ve kaynaklar

Hedefler, kritik varlıklar, log kaynakları

2

Mimari ve ürün

Mimari, boyutlandırma, ürün seçimi

3

Kurulum ve entegrasyon

Platform ve kaynak bağlantıları

4

Kural ve ayar

Korelasyon kuralları, yanlış alarm ayarı

5

Devreye alma

Süreçler, eğitim, devir

04

Log kaynağı önceliği

Her şeyi bir anda bağlamak yerine en çok değer üreten kaynaklarla başlayın:

- Kimlik sistemleri (Active Directory, kimlik sağlayıcı)
- Uç noktalar (EDR ve sunucu logları)
- Güvenlik duvarı, VPN ve proxy
- E-posta güvenliği
- Bulut hizmetleri
- Kritik iş uygulamaları

05

Kullanım senaryoları ve ayar

Kural yazımına tehdit odaklı senaryolarla başlanır; örneğin çok sayıda başarısız girişin ardından başarılı giriş, olağandışı saat veya konumdan oturum açma, yetki yükseltme. MITRE ATT&CK ile eşleştirmek kapsamı görünür kılar. İlk haftalarda yanlış alarmları ayıklamak, ekibin uyarılara güvenini korumak için kritiktir.

Başarı ölçütleri

- | | |
|---|--|
| ☐ Log kaynağı kapsama oranı (kritik varlıkların yüzdesi) | ☐ Ortalama tespit süresi (MTTD) ve müdahale süresi (MTTR) |
| ☐ Yanlış alarm oranı ve uyarı başına harcanan süre | ☐ Kural kapsamı (ATT&CK tekniklerine eşleme) |
| ☐ Olay sayısı ve çözülme oranı | |

SOC/SIEM projenizi birlikte planlayalım İhtiyacınıza uygun mimariyi ve yol haritasını birlikte belirleyelim.

// 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@troybilgiteknolojileri.com



Hizmet sayfası ve bilgi formu
için QR kodu okutun