SOC kurulum maliyetleri,

Gerekli sertifikalar,

SIEM kuralları (örnekler)

SOC kurulumu, lisans ve donanım gibi başlangıç maliyetlerinin ötesinde, personel ve operasyon giderlerini de kapsayan büyük bir yatırımdır. Aşağıda maliyetler, sertifikalar ve SIEM kural örneklerini bulabilirsiniz.

1. SOC Kurulum Maliyetleri

TOP

Bir SOC kurmanın maliyeti, kurumun büyüklüğü, sektörü, kapsamı ve hizmetin şirket içi mi yoksa dış kaynaklı mı (MSSP) olacağına göre büyük ölçüde değişir.

A. **Genel Yatırım ve Zamanlama**

Küresel pazarda bir SOC kurmak için planlanan ortalama bütçe yaklaşık 2 milyon USD civarındadır. Ancak bu rakam şirketten şirkete değişir:

* Şirketlerin %55'i 1 milyon USD'nin altında bütçe planlarken, %24'ü 2.5 milyon USD'nin üzerinde yatırım yapmayı hedefler.

* Türkiye'de ise durum biraz farklıdır. Kurumların %35'i en büyük zorluğun yüksek başlangıç maliyetleri olduğunu belirtmektedir.

Zamanlama açısından:

* Şirketlerin %50'si SOC'lerini 6-12 ay içinde kurmayı hedeflerken, %41'i bu sürecin 2 yılı bulabileceğini öngörmektedir.

B. **Karşılaştırmalı Maliyet Tablosu (Yıllık)**

Aşağıdaki tablo, farklı büyüklükteki şirketler için yönetilen SOC (MSSP) hizmetleri ile şirket içi (In-house) SOC kurmanın karşılaştırmalı maliyetlerini göstermektedir. (Veriler 2026 yılına aittir).

Şirket Büyüklüğü	Yönetilen SOC (MSSP) Yıllık Tahmini	Şirket İçi SOC (In-house) Yıllık Tahmini
KOBİ (250 cihaz)	$15.000 - $90.000 arası (Sağlayıcıya göre değişir)	$500.000 - $800.000
Orta Ölçek (1.000 cihaz)	$50.000 - $360.000 arası	$1.2 Milyon - $2 Milyon
Kurumsal (5.000+ cihaz)	$200.000 - $1.8 Milyon arası	$2.5 Milyon - $4 Milyon+

Önemli Not: Tablodaki geniş fiyat aralıkları, hizmetin kapsamına (24/7 gözetim, tehdit avcılığı, uyumluluk raporlaması vb.) ve kullanılan teknolojilere göre değişir. Özellikle veri giriş ücretleri (data ingestion), entegrasyon danışmanlığı ve erken fesih cezaları gibi gizli maliyetlere dikkat edilmelidir.

C. **SOC 2 Uyumluluk Maliyeti**

Eğer SOC kurulumunuzun bir parçası olarak SOC 2 sertifikasyonu almayı planlıyorsanız (özellikle bulut bilişim ve SaaS şirketleri için), ek maliyetleri göz önünde bulundurmalısınız:

* Tip 1 (Anlık Görüntü) Denetim Ücretleri: $15.000 - $50.000
* Tip 2 (Belirli Süreç) Denetim Ücretleri: $30.000 - $100.000+
* Uyumluluk Araçları (GRC Platformları): Yıllık $10.000 - $150.000+
* İç Ekip Zamanı: Genellikle en büyük maliyet kalemidir. Mühendislik ve uyum ekiplerinin harcadığı zamana bağlı olarak $40.000 - $200.000 ek maliyet çıkarabilir.

2. Gerekli Sertifikalar (Kariyer Yol Haritası)

SOC ekibi kurarken veya bu alanda kariyer yapmak isteyenler için sertifikalar oldukça önemlidir. Sertifikalar genellikle Tier 1 (Giriş Seviyesi) , Tier 2 (Uzman) ve Tier 3 (Saldırı Avcısı/Yönetici) seviyelerine göre ayrılır.

A. **Yeni ve Güncel Sertifikalar (2026)**

* INE eSOC (Security Operations Certified - Level 1): 2026'da piyasaya sürülen bu yeni sertifika, Tier 1 SOC Analisti olmak için gereken temel becerileri ölçmeyi hedefler. SIEM analizi, olay triyajı, false positive tespiti ve vaka yönetimi gibi konulara odaklanır.

B. **Sektörde Tanınan Klasik Sertifikalar**

Seviye	Önerilen Sertifikalar	Açıklama
Giriş (Tier 1)	CompTIA Security+, CEH, eSOC	Siber güvenliğe giriş, ağ güvenliği, tehdit tespiti ve temel SOC süreçleri için idealdir.
Orta/İleri (Tier 2/3)	CySA+, GCIH, GCIA	Daha derinlemesine olay müdahalesi, tehdit avcılığı ve gelişmiş log analizi için uygundur.
Uzman (Yönetici/Mimari)	CISSP, CISM, SANS GPEN	SOC yönetimi, strateji geliştirme ve ekip koordinasyonu için tercih edilir.

3. SIEM Kuralları Örnekleri (Korelasyon Mantığı)

SIEM (Security Information and Event Management) yazılımı, farklı cihazlardan gelen logları toplar ve belirli kurallara göre ilişkilendirerek (korelasyon) alarm üretir. İşte gerçek hayattan basit SIEM kural mantığı örnekleri:

Örnek 1: **Brute Force (Kaba Kuvvet) Saldırısı Tespiti**

Amaç: Bir kullanıcı hesabına kısa sürede çok fazla başarısız giriş yapılıp, ardından başarılı giriş yapıldığında alarm vermek.

* Koşul 1: Aynı kullanıcı için 5 dakika içinde 10 veya daha fazla `Başarısız Giriş (Event ID 4625)` olayı var mı?

* Koşul 2: Bu başarısız girişlerin ardından, aynı kullanıcı için 2 dakika içinde bir `Başarılı Giriş (Event ID 4624)` olayı var mı?

* Sonuç: Eğer iki koşul da sağlanıyorsa, "Olası Brute Force Saldırısı ve Takip Eden Yetkisiz Erişim" alarmı oluştur.

Örnek 2: **Ayrıcalık Yükseltme (Privilege Escalation) Şüphesi**

Amaç: Normal bir kullanıcının yetkisi olmayan bir dosyaya veya kayda erişmeye çalıştığını ve ardından bir yönetici aracı çalıştırdığını tespit etmek.

* Koşul 1: Bir kullanıcı, erişim yetkisi olmayan bir kaynağa erişmeye çalıştığında `Erişim Engellendi (Access Denied)` hatası alıyor.

* Koşul 2: Bu hatadan sonraki 10 dakika içinde, aynı kullanıcı `Yönetici Yetkisi Gerektiren` bir işlem başlatıyor (örn: Yeni kullanıcı oluşturma, registry düzenleme).

* Sonuç: "Ayrıcalık Yükseltme Denemesi" alarmı oluştur.

Örnek 3: **Kötü Amaçlı Yazılım (Malware) Tespiti**

Amaç: Bir cihazın bilinen bir kötü amaçlı yazılım sunucusuna (Command & Control - C2) bağlanma girişimini tespit etmek.

* Koşul 1: Ağ trafiğinde bir cihazdan dışarıya giden bir `HTTP/HTTPS` isteği var.

* Koşul 2: Hedef IP adresi veya domain adı, Tehdit İstihbaratı (Threat Intelligence) veri tabanında "Kötü Amaçlı" veya "C2" olarak işaretlenmiş durumda.

* Sonuç: "Kötü Amaçlı Yazılım C2 İletişimi Tespit Edildi" alarmı oluştur (Bu alarm genellikle yüksek önceliklidir).