SOC FUNDAMENTALS

İREM GÜZEL
07.02.2025

İçindekiler

Giriş

Bu raporun amacı, Güvenlik Operasyonları Merkezi'nin (SOC) ne olduğunu, görevlerini, yapısını, olay yönetimi süreçlerini ve kullandığı temel araçları detaylı bir şekilde incelemektir. Bu sayede, kurumların SOC'un önemini anlamalarına ve kendi güvenlik stratejilerini geliştirmelerine yardımcı olmak amaçlanmaktadır.

SOC (Security Operation Center) Nedir?

SOC, bir kuruluşun güvenliğini devamlı olarak izleyen ve güvenlik olaylarının analizinden sorumlu bir bilgi güvenliği ekibinin bulunduğu yer veya tesistir. Bu ekip, teknolojik çözümleri kullanarak iyi bir süreç yönetimi yapar ve siber güvenlik olaylarının tespit edilmesini sağlayıp analizini sunar. Siber saldırılara karşı aksiyon alır.

SOC'un Görevleri :

- Sürekli Güvenlik İzleme ve Log Analizi
- Olay Tespiti, Analizi ve Sınıflandırma
- Olay Müdahale
- Tehdit Avcılığı
- Güvenlik Politikaları ve Uyum Süreçlerini Yönetme
- Adli Bilişim (Digital Forensics)
- Raporlama ve İyileştirme Çalışmaları

SOC EKİBİ

1) Seviye 1 Güvenlik Analisti

- Gelen alarmları inceler, doğruluğunu kontrol eder ve önceliklendirir.
- Saldırı sinyalleri içeren olaylar için ticket oluşturur ve Seviye 2 analistlerine iletir.
- Zafiyet taramaları yapar ve sonuçları değerlendirir.

2) Seviye 2 Güvenlik Analisti

- Seviye 1 analistlerinin oluşturduğu ticket'ları inceler ve olayın kaynağını araştırır.
- Tehdit istihbaratlarını analiz eder, saldırının kapsamını ve etkilenen sistemleri belirler.
- Gelecekte olası saldırılar için iyileştirme ve kurtarma planları oluşturur

3) Seviye 3 Güvenlik Analisti

- Veri görselleştirme araçlarını kullanarak saldırı örüntülerini analiz eder.
- Zafiyet değerlendirmesi yapar ve varlık envanterini gözden geçirir.
- Tehdit avcılığı gerçekleştirir ve SOC sistemlerini optimize eder.

4) SOC Yöneticisi (SOC Manager)

- SOC ekibinin faaliyetlerini yönetir ve operasyonları denetler.
- Ekip için eğitim süreçlerini ve işe alım süreçlerini planlar.
- Uyumluluk raporlarını hazırlar ve SOC' un iş dünyasındaki önemini anlatır.
- Olay yönetim süreçlerini ve kriz durumlarını koordine eder.

5) Siber Tehdit İstihbaratı Ekibi

- Saldırganların amaçlarını ve yöntemlerini analiz eder.
- Kurumun güvenliğini tehdit eden mevcut ve potansiyel saldırılar hakkında bilgi toplar.
- Büyük SOC ekipleri kendi tehdit istihbaratı birimlerini oluşturabilirken, küçük SOC ekipleri dış tehdit istihbarat hizmetlerinden faydalanabilir.

Olay Yönetim Süreçleri

İzleme (Monitoring):

SOC, kurumların ağlarını, sistemlerini ve uygulamalarını 7 gün 24 saat boyunca izler. Bu sürekli gözlem sayesinde, güvenlik olayları ve anormallikler tespit edilir. Güvenlik duvarları, saldırı tespit sistemleri (IDS), antivirüs yazılımları, sunucular, bulut hizmetleri gibi çeşitli kaynaklardan güvenlik olaylarına dair veriler toplanır. Bu veriler, "log" adı verilen kayıtlar halinde tutulur ve sistemlerdeki her türlü aktiviteyi kaydeder. Toplanan loglar ve güvenlik olayları, adı verilen özel yazılımlar tarafından merkezi olarak analiz edilir. SIEM, büyük miktardaki veriyi anlamlı hale getirerek güvenlik analistlerine yardımcı olur. İzleme sürecinde, normal dışı aktiviteler tespit edilmeye çalışılır.

Analiz (Analysis):

İzleme sırasında şüpheli bir durum tespit edildiğinde, güvenlik analistleri olayı ayrıntılı bir şekilde incelemeye başlar. Bu aşamada, olayın gerçekleştiği zaman, yer ve yöntem gibi temel sorulara yanıt aramak için log kayıtları analiz edilir. Analistler, olayın bilinen bir siber saldırı türüyle bağlantılı olup olmadığını belirlemek amacıyla tehdit istihbaratı kaynaklarına başvururlar. Bu kaynaklar, mevcut saldırı teknikleri, kötü amaçlı yazılımlar ve siber suçlulara dair bilgiler sunar. Ayrıca, farklı veri kaynaklarından gelen loglar birleştirilerek olaylar arasındaki ilişkiler ortaya çıkarılır ve kapsamı daha iyi anlaşılır.

Olay Müdahalesi:

Olayın ciddiyetine göre, derhal bir müdahale süreci başlatılır. İlk olarak, saldırının daha fazla yayılmaması için etkilenen sistemler ağdan izole edilir ya da kapatılır. Kötü amaçlı yazılımlar veya diğer saldırı araçları temizlenerek sistemlerden uzaklaştırılır. Etkilenen sistemlerin işlevselliği tekrar sağlanır ve veriler eski haline getirilir. Olayın nedenleri detaylıca araştırılır, etkiler değerlendirilir ve benzer saldırıların önlenmesi için gerekli önlemler alınır. Son olarak, olayın tüm süreci ve sonuçları hakkında detaylı bir rapor hazırlanarak yönetime ve diğer ilgili birimlere sunulur.

SOC'da Kullanılan Temel Araçlar

1. **SIEM Sistemleri: Güvenlik Bilgileri ve Olay Yönetimi**

   Farklı kaynaklardan gelen log kayıtlarını toplar, analiz eder ve ilişkilendirir. IBM QRadar, Splunk

Özellikleri:

- Merkezi log yönetimi
- Gerçek zamanlı olay analizi
- Anormallik tespiti
- Olay korelasyonu

2. **IDPS: Saldırı Tespit ve Önleme Sistemleri**

Ağ trafiğini ve sistem aktivitelerini izleyerek kötü amaçlı aktiviteleri tespit eder ve engeller.

Örnekler: Snort, Suricata

Özellikleri:

- Gerçek zamanlı trafik analizi
- Kural tabanlı veya davranışsal analiz
- Saldırı imzası veritabanı
- Otomatik engelleme veya uyarı mekanizmaları

- IPS : Tespit edilen saldırıları otomatik olarak engeller.
- IDS :Saldırıları sadece tespit eder ve güvenlik analistlerini uyarır. Engelleme işlemi manuel olarak yapılır.

3. **Firewall :**

Firewall, gelen ve giden ağ trafiğini izleyen bir güvenlik aygıtıdır. Güvenlik duvarı, bir dizi güvenlik kuralına dayalı olarak veri paketlerine izin verir veya bunları engeller, dahili ağınız ile harici kaynaklardan gelen trafik arasında bir bariyer oluşturur. Güvenlik duvarı

yalnızca istenmeyen trafiği engellemekle kalmaz, aynı zamanda kötü amaçlı yazılımların bilgisayarınıza bulaşmasını engellemeye de yardımcı olabilir.

Örnekler: Cisco ASA, Palo Alto Networks Firewalls, Fortinet Firewalls

4. **Endpoint Security Araçları:**

Bilgisayarlar, ve mobil cihazlar gibi uç noktaları kötü amaçlı yazılımlara karşı korur.

Özellikleri:

- Antivirüs ve anti-casus yazılım
- Güvenlik duvarı
- Cihaz kontrolü
- Davranışsal analiz

Örnek: CrowdStrike Falcon, Kaspersky Endpoint Security

5. **Tehdit İstihbaratı Platformları :**

Siber tehditler hakkında bilgi toplar, analiz eder ve paylaşır.

Örnek: ThreatConnect, Recorded Future, Anomali

6. **Adli Bilişim Araçları :**

Siber güvenlik olaylarını araştırmak ve delil toplamak için kullanılır. FTK, Autopsy

Özellikleri:

- Disk imajı alma
- Veri kurtarma
- Log analizi
- Kötü amaçlı yazılım analizi

Sonuç

Bu rapor, SOC'un önemini ve işleyişini anlamak için bir rehber niteliğindedir. SOC, kurumların siber güvenlik duruşunu güçlendirmek ve siber saldırılara karşı daha dirençli hale gelmek için kritik bir öneme sahiptir.

KAYNAKÇA

https://chatgpt.com/

https://www.ibrahimaslanbakan.com/2019/07/soc-nedir-gorevi-nedir-bir-socnin.html

https://www.infinitumit.com.tr/guvenlik-operasyon-merkezi-soc-nedir/

https://bulutistan.com/blog/soc/