SOC TEMELLERİ

Hazırlayan: Berra SÖYLER

Tarih: 07.02.2025

Giriş **3**
1. SOC Temelleri **4**
a) SOC Nedir? 4
b) SOC Katmanları ve Analist Rolleri 4
c) Olay Yönetimi Süreçleri 4
i) Tehdit İzleme ve Tespit: 5
Örnek Senaryo: Brute-Force Saldırısının Tespiti 5
SOC'un Yanıtı: 5
ii) Olay Müdahale (Incident Response) 5
Örnek Senaryo: Ransomware Saldırısı 5
SOC'un Yanıtı: 6
iii) Güvenlik Analizleri: 6
Örnek Senaryo: Veri Sızıntısı Tespiti 6
SOC'un Yanıtı: 6
iv) Raporlama ve Dokümantasyon: 7
Örnek Senaryo: İç Denetim ve Uyum Gereklilikleri 7
SOC'un Yanıtı: 7
v) Güvenlik Politikaları ve Prosedürlerinin Uygulanması: 7
Örnek Senaryo: Çalışanların Phishing (Kimlik Avı) Saldırılarına Karşı Eğitilmesi 7
SOC'un Yanıtı: 7
2. Yanlış Pozitif(False Positive) Nedir? **8**
a. Yanlış Pozitiflerin Riskleri 8
b. Yanlış Pozitifleri Azaltma Yöntemleri 8
3.SOC'ta Kullanılan Teknolojiler **9**
a. SIEM (Security Information and Event Management): 9
b. IDS/IPS (Intrusion Detection/Prevention Systems): 9
c. EDR (Endpoint Detection and Response): 10
d. DLP (Data Loss Prevention): 10
e. SOAR (Security Orchestration, Automation and Response): 10
f. Tehdit İstihbarat Platformları: 10
g. Log Yönetimi ve Ağ Trafik Analizi Araçları: 10
5. Sonuç ve Öneriler **11**
● Güçlü ve Entegre Teknoloji Altyapısı: 11
● Süreç ve Operasyonel Verimlilik: 11
● Nitelikli Personel ve Sürekli Eğitim: 11
● İç ve Dış İletişimin Güçlendirilmesi: 11
● Sürekli İyileştirme ve Değerlendirme: 11
6. Kaynakça **12**

Giriş

Günümüzün sürekli evrilen siber tehdit ortamında, kuruluşların dijital varlıklarını koruma altına almak ve olası saldırılara anında yanıt verebilmek hayati önem taşımaktadır. Bu bağlamda, Güvenlik Operasyon Merkezleri (SOC), kurumların siber güvenlik stratejilerinde temel bir yapı taşı olarak öne çıkmaktadır. Raporumuz, "SOC Tehdit Tespit Yöntemleri ve Olay Müdahale Stratejileri" başlığı altında, SOC'lerin ne olduğu, hangi temel görevleri üstlendikleri ve bu görevlerin nasıl yapılandırıldığı konularını detaylandırmaktadır.

İlk bölümde, SOC'nin tanımı, yapısı (L1, L2, L3 analist rollerinin yanı sıra olay yönetimi süreçleri) ve temel işlevleri; sürekli izleme, olay müdahalesi, güvenlik analizi ile raporlama ve mevzuata uygunluk açısından ele alınmıştır. Devam eden bölümlerde, SOC süreçlerinde karşılaşılabilecek en kritik kavramlardan biri olan "yanlış pozitif"lerin oluşturduğu riskler ve bu risklerin azaltılması için kullanılan yöntemler (algılama kurallarının optimize edilmesi, makine öğrenimi ve bağlamsal analiz gibi) ayrıntılı olarak incelenmiştir.

Ayrıca, SOC'ta kullanılan teknolojik altyapı – SIEM, IDS/IPS, EDR, DLP, SOAR, tehdit istihbarat platformları ve log yönetimi araçları – entegrasyonları ve bu teknolojilerin SOC'nin 7/24 izleme, anında müdahale ve proaktif tehdit avcılığı gibi kritik işlevleri nasıl desteklediği de raporun önemli başlıklarını oluşturmaktadır.

Bu rapor, SOC'lerin nasıl daha etkili yapılandırılabileceğini, olay müdahale stratejilerinin nasıl geliştirilebileceğini ve siber güvenlik operasyonlarının sürekli olarak iyileştirilmesi için uygulanabilecek yöntemleri detaylı bir şekilde ele alıyor. bu çalışma, yöneticiler, analistler ve IT alanına ilgi duyan herkes için, dijital güvenlik seviyelerinin yükseltilmesi, iş süreçlerinin aksamadan devam etmesi ve kurumsal itibarın korunması adına kazanılması gereken temel yaklaşımları ortaya koymayı amaçlamaktadır.

1. SOC Temelleri

a) SOC Nedir?

SOC, bir kuruluşun siber güvenlik tehditlerine karşı korunmasını sağlayan birimdir. Bu merkezler güvenlik olaylarını sürekli izler, analiz eder ve müdahalede bulunur. SOC, genellikle vardiyalı çalışan birimlerdir . Bu birimler hem iç hem de dış tehditlere karşı proaktif ve reaktif güvenlik önlemleri alarak kuruluşların bilgi güvenliğini sağlamaya yönelik kritik bir rol oynar. Çünkü SOC ekipleri, güvenlik açıklarını belirleyerek bu açıkların kötüye kullanılmasını önlemek için oldukça önemli bir birimdir. SOC bu analizleri çeşitli güvenlik araçları ve teknikleri kullanarak yaparlar. Aşağıda bu araçlar ve tekniklerden bahsedilmektedir. Tehditleri tespit etmek için SIEM (Security Information and Event Management), IDS (Intrusion Detection System), IPS (Intrusion Prevention System) gibi teknolojileri kullanır. Bir SOC'un temel görevleri kısaca şunlardır:

Sürekli İzleme: SIEM ve IDS gibi sistemler aracılığıyla ağ trafiğinin ve olayların analiz edilmesi
Olay Müdahalesi: Saldırıları tespit edip etkisini en aza indirerek yanıt verme
Güvenlik Analizi: Log yönetimi ve tehdit avcılığı yaparak saldırıları daha iyi anlamak
Raporlama ve Uygunluk: Güvenlik olaylarını dokümante etmek ve mevzuat uyumluluğunu sağlamak

b) SOC Katmanları ve Analist Rolleri

SOC, genellikle üç ana katmandan oluşur:

L1 Analist (Olay İzleme ve Sınıflandırma): Gelen alarmları değerlendirir, önceliklendirir ve basit saldırıları analiz eder.

L2 Analist (Derinlemesine Analiz ve Müdahale): Daha karmaşık tehditleri değerlendirir, tehdit istihbaratını kullanarak olayları detaylandırır.

L3 Analist (Tehdit Avcılığı ve İleri Seviye Müdahale): Gelişmiş saldırıları analiz eder, tehdit avcılığı yapar ve SOC süreçlerini geliştirir.

c) Olay Yönetimi Süreçleri

SOC ekiplerinin güvenlik tehditlerini tespit etmek, analiz etmek ve engellemek için uyguladığı süreçler bu başlıkta açıklanmıştır. Bu süreçler, tehditlerin erken aşamada fark edilmesini ve olası saldırıların önüne geçilmesini sağlar. SOC ekiplerinin en kritik görevlerinden biri olan olay yönetimi süreci beş temel adımdan oluşur:

i) Tehdit İzleme ve Tespit:

SOC ekipleri, organizasyonun ağ trafiğini, sistem günlüklerini ve güvenlik olaylarını sürekli olarak izleyerek anormal davranışları tespit eder. Bu süreçte kullanılan temel araçlar arasında SIEM (Security Information and Event Management), IDS (Intrusion Detection System) ve IPS (Intrusion Prevention System) yer alır. Bu araçlar hakkında ayrıntılı bilgi “” başlığı altındadır.

Örnek Senaryo: Brute-Force Saldırısının Tespiti

Bir SOC, bir sistemde belirli bir zaman dilimi içinde aynı IP adresinden çok fazla başarısız giriş denemesi yapıldığını tespit edebilir. Bu durum, bir brute-force saldırısının işareti olabilir. SIEM sistemi, sistem günlüklerini analiz ederek belirli bir hesaba yüzlerce başarısız giriş denemesi yapıldığını raporlar.

SOC’un Yanıtı:

- IDS, anormal giriş denemelerini fark ederek bir alarm üretir.
- SIEM, farklı sistemlerden gelen logları analiz eder ve saldırının belirli bir kaynaktan geldiğini tespit eder.
- SOC analistleri, saldırıyı doğrulamak için şüpheli IP adresini engelleyerek giriş denemelerini durdurur.
- Kullanıcı hesapları kilitlenir ve parola sıfırlama politikaları devreye alınır.

ii) Olay Müdahale (Incident Response)

SOC ekipleri, tespit edilen güvenlik olaylarına hızlı bir şekilde müdahale ederek saldırının yayılmasını önler. Olay müdahalesi sürecinde L2 ve L3 SOC analistleri, olayın kaynağını belirler, saldırının etkisini analiz eder ve saldırıyı durdurmak için uygun önlemleri alır. Bu önlemler; tehditlerin tespit edilmesi, izole edilmesi, analiz edilmesi ve ortadan kaldırılması aşamalarını içerir. Ayrıca, olay sonrası adli incelemeler ve güvenlik politikalarının iyileştirilmesi gibi süreçler de olay müdahalesi (incident response) kapsamında değerlendirilir. Etkili bir olay müdahalesi süreci, bir saldırının neden olduğu zararları en aza indirerek organizasyonun güvenliğini güçlendirmeye yardımcı olur.

Örnek Senaryo: Ransomware Saldırısı

Bir çalışanın e-posta yoluyla aldığı zararlı ek dosyayı açması sonucunda fidye yazılımı (ransomware) şirketin ağında yayılmaya başlar. Kullanıcı dosyaları şifrelenir ve saldırganlar fidye talep eden bir mesaj bırakır.

SOC'un Yanıtı:

- SIEM sistemi, şüpheli ağ etkinliklerini raporlar ve belirli bir bilgisayardan anormal dosya şifreleme işlemlerinin başladığını tespit eder.
- L2 analistleri, sistemin izole edilmesi gerektiğine karar vererek etkilenen makineleri ağdan ayırır.
- L3 analistleri, saldırının kökenini araştırarak zararlı yazılımın hangi güvenlik açığından yararlandığını tespit eder.
- Fidye yazılımının yayılmasını önlemek için tüm ağ cihazlarına güncellemeler uygulanır.
- Son olarak, güvenlik açıklarının düzeltilmesi ve çalışanların farkındalık eğitimleri ile gelecekte benzer saldırıların önlenmesi sağlanır.

iii) Güvenlik Analizleri:

SOC ekipleri, tespit edilen tehditleri ve olayları derinlemesine analiz ederek saldırıların nasıl gerçekleştiğini, hangi tekniklerin kullanıldığını ve saldırganların niyetlerini belirler.

Örnek Senaryo: Veri Sızıntısı Tespiti

Bir şirket, hassas müşteri bilgilerinin dark web üzerinde satışa sunulduğuna dair bir tehdit istihbaratı alır. SOC ekibi, bu veri sızıntısının kaynağını tespit etmek için derinlemesine analiz yapar.

SOC'un Yanıtı:

- DLP (Data Loss Prevention) sistemleri incelenerek verinin nasıl dışarı sızdırıldığı belirlenir.
- Proxy ve güvenlik duvarı logları kontrol edilerek, hassas verilerin hangi IP adresine gönderildiği tespit edilir.
- SIEM üzerinden tüm iç ve dış veri akışları analiz edilir.
- Bir çalışan veya kötü amaçlı yazılım tarafından sistemden veri sızdırıldığı anlaşılırsa, olayın adli incelemesi başlatılır.
- Şirketin güvenlik politikaları gözden geçirilerek veri şifreleme ve erişim kontrolleri sıkılaştırılır.

iv) Raporlama ve Dokümantasyon:

SOC ekipleri, gerçekleşen her güvenlik olayını detaylı bir şekilde raporlar veileride benzer saldırıların önlenebilmesi için ilgili departmanlarla paylaşır.

Örnek Senaryo: İç Denetim ve Uyum Gereklilikleri

Bir finans şirketi, KVKK (Kişisel Verilerin Korunması Kanunu) ve ISO 27001 gibi standartlara uymak zorundadır. SOC ekibi, her güvenlik olayını detaylandırarak yetkili mercilere sunulabilecek şekilde raporlar hazırlar.

SOC'un Yanıtı:

- Her olay için incident report (olay raporu) oluşturulur.
- Saldırının kaynağı, saldırı süreci ve alınan önlemler raporda belirtilir.
- İlgili mevzuat ve uyumluluk gerekliliklerine göre raporlar düzenlenir.
- Yönetim ve hukuk ekipleriyle iş birliği yapılarak yasal bildirimler yapılır.

Bu süreç organizasyonun güvenlik politikalarının geliştirilmesine ve uyumluluk gerekliliklerinin yerine getirilmesi için oldukça önemlidir.

v) Güvenlik Politikaları ve Prosedürlerinin Uygulanması:

SOC ekipleri, organizasyonun güvenlik standartlarını belirleyerek uyulması gereken politikaları uygular. Bu politikalar, erişim kontrolleri, şifreleme standartları, güvenlik yamaları ve güvenlik farkındalık eğitimlerini kapsar.

Örnek Senaryo: Çalışanların Phishing (Kimlik Avı) Saldırılarına Karşı Eğitilmesi

Bir şirketin çalışanlarından biri, kendisini banka yetkilisi olarak tanıtan bir saldırgana şifrelerini verdiğinde SOC ekibi bu olayı analiz eder ve çalışanların bu tür saldırılara karşı eğitilmesi gerektiğini belirler.

SOC'un Yanıtı:

- Çalışanlara yönelik siber güvenlik farkındalık eğitimleri düzenlenir.
- Phishing simülasyonları yapılarak çalışanların saldırılara nasıl tepki vereceği ölçülür.
- Çok faktörlü kimlik doğrulama (MFA) zorunlu hale getirilerek güvenlik artırılır.

- Güvenlik politikaları güncellenerek, şüpheli e-postalara nasıl yanıt verileceği konusunda kılavuzlar oluşturulur.

Bu tür politikalar sayesinde organizasyonun genel güvenlik seviyesi artırılmış olur ve çalışanların bilinçlendirilmesi sağlanır.

2. Yanlış Pozitif(False Positive) Nedir?

Tüm bu süreçlerde karşılaşılabilecek en kritik kavramlardan biri de "Yanlış Pozitif"lerdir. Yanlış pozitif (false positive), bir güvenlik olayının veya tehdidin varmış gibi algılanması ancak gerçekte bir tehdit olmaması durumudur. Yanlış pozitifler, SOC ekipleri tarafından yapılan yanlış yorumlamalar veya güvenlik çözümleri (EDR, DLP, IDS/IPS, güvenlik duvarları vb.) tarafından yanlış değerlendirmeler sonucu oluşabilir. Örneğin, güvenli bir ağ trafiğinin zararlı olarak algılanması, meşru bir web sitesinin zararlı kabul edilmesi veya bir çalışanın yasal bir e-posta iletisinin spam olarak işaretlenmesi gibi durumlar yanlış pozitif örnekleridir.

a. Yanlış Pozitiflerin Riskleri

Yanlış pozitifler, organizasyonun tüm işleyişini olumsuz etkileyebilir ve bilgi güvenliği karar mekanizmalarında çeşitli sorunlara yol açabilir:

- **İş Süreçlerine Etkisi:** Yanlış pozitifler nedeniyle tetiklenen otomatik güvenlik önlemleri, hizmet kesintilerine neden olabilir. Yanlış analiz edilen bir olay nedeniyle bir sistemin erişime kapatılması veya bir uygulamanın çalışmasının durdurulması, çalışanların işlerini yapamamasına sebep olabilir.
- **Güvenlik Çözümlerine Duyulan Güvenin Azalması:** Sürekli yanlış pozitif üreten güvenlik çözümleri, çalışanlar ve SOC analistleri tarafından güvenilirliğini yitirebilir. Çalışanlar, güvenlik çözümlerini devre dışı bırakmaya veya görmezden gelmeye başlayabilir, bu da gerçek tehditlerin fark edilmemesine neden olabilir.
- **Zaman ve Kaynak İsrafı:** Yanlış pozitifleri doğrulamak için harcanan zaman ve efor, SOC ekiplerinin kritik tehditleri analiz etmesini zorlaştırır. Yanlış önceliklendirme nedeniyle kritik tehditlerin gözden kaçması, güvenlik olaylarının fark edilmeden ilerlemesine yol açabilir.

b. Yanlış Pozitifleri Azaltma Yöntemleri

Yanlış pozitifleri en aza indirmek için güvenlik çözümlerinin hassasiyet seviyeleri dengeli bir şekilde ayarlanmalı ve organizasyonun çalışma ortamına uygun hale getirilmelidir.

- Algılama Kurallarının Optimize Edilmesi: IDS/IPS ve SIEM gibi sistemlerde kullanılan algılama kurallarının düzenli olarak gözden geçirilmesi ve organizasyonun gerçek operasyonel yapısına uygun hale getirilmesi gerekir.

- Makine Öğrenimi ve Yapay Zeka Kullanımı: Gerçek zamanlı ağ trafiği ve güvenlik olayları analiz edilerek tehdit algılama kurallarının dinamik olarak güncellenmesi sağlanabilir.

- Bağlamsal Analiz ve Telemetri Verilerinin Kullanımı: Sistemlerin oluşturduğu uyarılar, organizasyonun spesifik iş süreçleri göz önüne alınarak değerlendirilmelidir. Örneğin, bir bakım çalışmasının oluşturduğu ağ trafiği anomali olarak algılanmamalıdır.

- İç İletişimin Güçlendirilmesi: SOC ekipleri ile diğer IT ve operasyon ekipleri arasında etkili bir iletişim mekanizması kurulmalıdır. Özellikle sistem bakımı ve güncellemeler gibi olaylar SOC ekiplerine önceden bildirilerek gereksiz alarmların oluşması önlenebilir.

- MITRE ATT&CK Gibi Çerçevelerin Kullanımı: Siber saldırı tekniklerini daha iyi anlamak ve tehdit modellemesi yapmak için MITRE ATT&CK gibi frameworkler kullanılmalıdır.

Yanlış pozitifleri azaltmak, siber güvenlik sistemlerinin etkinliğini artırarak hem çalışanlar hem de güvenlik ekipleri için daha verimli bir çalışma ortamı oluşturur.

3.SOC'ta Kullanılan Teknolojiler

Modern bir SOC'nin etkin çalışabilmesi için, insan gücü kadar teknolojik altyapı da büyük önem taşır. SOC ekipleri, siber tehditleri tespit etmek, analiz etmek ve olaylara müdahale etmek için aşağıdaki temel teknolojik araç ve çözümleri entegre bir şekilde kullanır:

a. SIEM (Security Information and Event Management):

Farklı kaynaklardan (sunucular, ağ cihazları, uygulamalar, log sistemleri vb.) gelen verileri toplayarak normalleştirir, korele eder ve gerçek zamanlı uyarılar üretir. SIEM, SOC analistlerinin anormal aktiviteleri ve potansiyel tehditleri hızlıca tespit etmesinde kritik rol oynar.

b. IDS/IPS (Intrusion Detection/Prevention Systems):

Ağ trafiğini sürekli izleyerek, şüpheli aktiviteleri tespit eder ve gerektiğinde otomatik müdahale ile saldırıların önlenmesine yardımcı olur.

c. EDR (Endpoint Detection and Response):

Uç nokta cihazlarda meydana gelen anormal davranışları tespit eder; tehditlerin analizi ve yanıt süreçlerini hızlandırır. Böylece, uç nokta bazında gelişen saldırılar etkili biçimde izlenir.

d. DLP (Data Loss Prevention):

Kuruluş içindeki hassas verilerin yetkisiz erişim ve dışarı sızmasını önlemek amacıyla çalışır. DLP çözümleri, veri sızıntılarını erken aşamada engelleyerek iş sürekliliğini destekler.

e. SOAR (Security Orchestration, Automation and Response):

Olay müdahale süreçlerini otomatikleştirir ve SOC ekiplerinin farklı güvenlik araçları arasında koordinasyonu sağlar. Böylece, manuel iş yükü azalır ve müdahale süreleri kısalır.

f. Tehdit İstihbarat Platformları:

Güncel saldırı teknikleri ve zararlı yazılım örüntülerini sürekli olarak güncelleyerek, SOC ekiplerine siber tehditler hakkında zengin istihbarat sağlar. MITRE ATT&CK gibi çerçeveler, bu süreçte rehber niteliğindedir.

g. Log Yönetimi ve Ağ Trafik Analizi Araçları:

Tüm sistem ve ağ loglarının merkezi olarak toplanması, analiz edilmesi ve uzun vadeli korelasyonların yapılabilmesi için kullanılır. Bu sayede, geçmişte yaşanan olayların detaylı incelenmesi ve benzer saldırıların önceden tespit edilmesi mümkün olur.

Bu teknolojilerin entegrasyonu, SOC'nin 7/24 izleme, anında müdahale ve proaktif tehdit avcılığı görevlerini yerine getirmesini sağlar. Her araç, belirli bir güvenlik açığına odaklanırken, birlikte çalışarak kapsamlı bir savunma mekanizması oluştururlar.

5. Sonuç ve Öneriler

Bu raporda, SOC'lerin temel işlevleri, olay yönetimi süreçleri, yanlış pozitiflerin yaratabileceği riskler ve SOC'ta kullanılan teknolojiler detaylı olarak ele alınmıştır. Elde edilen veriler ışığında şu sonuç ve öneriler öne çıkmaktadır:

- **Güçlü ve Entegre Teknoloji Altyapısı:**

  SOC'lerin etkin çalışabilmesi için SIEM, IDS/IPS, EDR, DLP, SOAR ve tehdit istihbarat platformlarının entegrasyonu şarttır. Bu teknolojik araçlar, anlık veri toplama, analiz ve otomatik müdahale yetenekleriyle siber saldırılara karşı güçlü bir savunma sağlar.

- **Süreç ve Operasyonel Verimlilik:**

  Olay tespiti ve müdahale süreçlerinin sürekli olarak güncellenmesi, standartlaştırılması ve otomasyonun artırılması gerekmektedir. Etkili bir SOC yapısında, yanlış pozitiflerin minimize edilmesi, acil müdahale planlarının uygulanması ve olay sonrası raporlamaların eksiksiz yapılması, sistemin genel verimliliğini artırır.

- **Nitelikli Personel ve Sürekli Eğitim:**

  Teknolojik altyapının yanında, deneyimli ve sürekli eğitilen güvenlik analistleri de SOC'nin başarısında kritik rol oynar. Personel eğitimlerinin düzenli olarak yapılması, güncel tehditler ve saldırı teknikleri hakkında bilgi sahibi olmalarını sağlar.

- **İç ve Dış İletişimin Güçlendirilmesi:**

  SOC ile diğer BT ve operasyon ekipleri arasında sürekli ve etkili bir iletişim kurulması, olayların doğru analiz edilmesi ve gereksiz müdahalelerin önlenmesinde fayda sağlar. Ayrıca, olay sonrası alınan derslerin tüm organizasyona aktarılması, benzer saldırıların önüne geçilmesi açısından önemlidir.

- **Sürekli İyileştirme ve Değerlendirme:**

  SOC altyapısının ve süreçlerinin düzenli olarak gözden geçirilmesi, performans değerlendirmeleri yapılması ve yeni teknolojik gelişmelerin entegre edilmesi gerekmektedir. Bu, sadece mevcut tehditlere karşı değil, gelecekte ortaya çıkabilecek saldırılara karşı da organizasyonun savunma seviyesini artıracaktır.

Sonuç olarak, SOC'ler, kuruluşların dijital varlıklarını korumada hayati bir rol oynar. Teknolojik araçların, süreçlerin ve nitelikli personelin uyum içinde çalıştığı güçlü bir SOC yapısı, siber saldırıların etkilerini minimuma indirerek iş sürekliliğini ve kurumsal itibarını korur. Bu nedenle, kurumların SOC yapılarını kendi iş ihtiyaçlarına uygun olarak düzenlemeleri, sürekli eğitim ve iyileştirme süreçlerini uygulamaları önerilir.

6. Kaynakça

1. https://www.karyabt.com/soc-nedir-bilmeniz-gereken-her-sey/

2. https://www.beyaz.net/tr/guvenlik/makaleler/soc_ekibi_ozellikleri.html