2025

SOC FUNDAMENTALS

BİLGEHAN BAYRAK

07/02/2025

İçindekiler

GİRİŞ

Security Operations Center (SOC), kuruluşların bilgi güvenliğini sağlamak ve siber tehditleri izlemek için oluşturduğu merkezi bir birimdir. Günümüz dijital dünyasında, artan siber tehditler nedeniyle SOC'un önemi giderek artmaktadır. Bu rapor, SOC'un temel bileşenlerini, analist seviyelerini, tehdit avcılığı sürecini, SIEM ve log analizinin önemini, olay müdahale süreçlerini ve genel işleyişi açıklamayı amaçlamaktadır. Siber güvenliğin sağlamlaştırılmasında SOC'un etkin yönetimi kritik bir rol oynar ve bu raporda SOC'un bileşenleri detaylı bir şekilde ele alınacaktır.

1. SOC'un İşleyişi ve Önemi

Günümüz dijital çağında, siber güvenlik tehditleri her ölçekteki işletme için büyük bir endişe kaynağıdır. Siber saldırılar giderek daha sofistike hale geldikçe, kuruluşların hassas verilerini ve altyapılarını korumak için sağlam güvenlik önlemleri alması gerekmektedir. Etkili bir siber güvenlik stratejisinin önemli bileşenlerinden biri de **Security Operations Center (SOC)**'tur.

- **Olay Müdahalesi:**
  Güvenlik olayı meydana geldiğinde SOC, olayla ilgili müdahale sürecini koordine eder. Bu, olayın triage edilmesi, tehdidin izole edilmesi ve etkiyi azaltmak için müdahalede bulunulması aşamalarını içerir. Olay müdahale prosedürleri genellikle resmi bir olay müdahale planında dokümante edilir.

- **Tehdit İstihbaratı:**
  SOC analistleri, çeşitli kaynaklardan tehdit istihbaratını toplayarak sürekli olarak yeni siber tehditlere karşı hazırlıklı olurlar. Bu, yeni zararlı yazılımlar, güvenlik açıkları ve siber suçluların kullandığı saldırı tekniklerinin izlenmesini içerir. En son tehditlerle ilgili bilgileri takip ederek, SOC potansiyel saldırılara karşı proaktif bir savunma geliştirir.

- **Ağ ve Sistem İzleme**
  SOC, sürekli ağ trafiğini izleyerek anormal hareketleri tespit eder. Sistemlere yetkisiz erişimlerin veya olağandışı aktivitelerin izlenmesi, güvenliği artırır.

- **Zafiyet Yönetimi:**
  SOC takımları, kuruluşun sistemlerinde ve altyapısında bulunan güvenlik açıklarını belirler ve düzeltme işlemlerini gerçekleştirir. Bu, düzenli zafiyet değerlendirmeleri yapmak, risklere göre düzeltme öncelikleri belirlemek ve bilinen güvenlik zayıflıklarını ele almak için yamalar ve güncellemeler uygulamakla ilgilidir.

- **Güvenlik Farkındalık Eğitimi:**
  Çalışanların siber güvenlik en iyi uygulamaları konusunda eğitilmesi, kuruluşun güvenlik duruşunun güçlendirilmesi için önemlidir. SOC takımları, insan kaynakları departmanı ile işbirliği yaparak, çalışanların güvenlik tehditlerini tanımasını ve etkin bir şekilde yanıt vermesini sağlayacak güvenlik farkındalığı eğitim programları hazırlar.

2. SOC Analist Seviyeleri ve Görevleri

SOC ekibi genellikle üç seviyeden oluşur ve her seviyenin farklı görev ve sorumlulukları vardır:

- **L1 (Seviye 1) - SOC Analisti:**
    - Güvenlik olaylarını izler ve temel analizleri gerçekleştirir.
    - Şüpheli etkinlikleri belirleyerek ilgili ekipleri bilgilendirir.
    - Güvenlik uyarılarını değerlendirerek yanlış pozitifleri filtreler.
- **L2 (Seviye 2) - Olay Müdahale Analisti:**
    - Daha karmaşık tehditleri analiz eder ve detaylı araştırmalar yapar.
    - Olay müdahale süreçlerini yönetir ve güvenlik önlemleri alır.
    - Tehdit aktörlerini ve saldırı tekniklerini anlamak için analiz yapar.
- **L3 (Seviye 3) - Tehdit Avcısı ve Uzman Analist:**
    - Tehdit avcılığı yaparak henüz tespit edilmemiş saldırıları belirler.
    - SOC'un stratejisini belirleyerek iyileştirmeler önerir.
    - Yeni saldırı vektörlerine karşı koruma mekanizmaları geliştirir.

---

4. Tehdit Avcılığı (Threat Hunting)

Tehdit avcılığı, güvenlik altyapısındaki potansiyel tehditleri proaktif bir şekilde tespit etmek amacıyla kullanılan bir tekniktir. Bu süreç, genellikle güvenlik bilgi ve olay yönetimi (SIEM) sistemleri, ağ izleme araçları, son nokta güvenlik çözümleri gibi araçlarla desteklenir. Tehdit avcılığının amacı, saldırıları tespit etmenin ötesine geçmek ve henüz algılanmamış, gizli tehditleri (örneğin, APT'ler) proaktif olarak belirlemektir.

Tehdit avcılığına yönelik kullanılan bazı teknikler ve yaklaşımlar şunlardır:

- **Hipotez Tabanlı Avcılık (Hypothesis-Driven Hunting):**
  Bu yaklaşımda, önceden belirlenen tehdit hipotezleri doğrultusunda arama yapılır. Hipotezler, önceki güvenlik olaylarından, tehdit istihbaratından ya da deneyimlerden elde edilen bilgilerle oluşturulur. Hipotezler, bir saldırı tekniği ya da yöntemi hakkında bir öngörüde bulunur ve bu öngörü doğrultusunda ağda, loglarda veya güvenlik araçlarında derinlemesine analiz yapılır.
- **Davranışsal Analiz (Behavioral Analysis):**
  Davranışsal analiz, kullanıcıların ve sistemlerin normal davranışlarını anlamayı ve anormallikleri tespit etmeyi amaçlar. Bu yöntemde, belirli bir süre boyunca normal kullanım davranışları izlenir. Davranışsal analiz araçları, belirli bir kullanıcı ya da sistem davranışındaki anormallikleri tespit etmek için kullanılır. Bu tür anormallikler, potansiyel bir iç tehdit veya dışarıdan gelen bir saldırının belirtisi olabilir.

- **Anomali Tespiti (Anomaly Detection):**
  Anomali tespiti, normalden sapmaları belirlemek için istatistiksel yöntemler ve makine öğrenme algoritmalarını kullanır. Bu yöntem, bir sistemin veya ağın zaman içindeki normal çalışma davranışını modelleyerek, o davranıştan sapmalar arar. Anomali tespiti, dinamik tehditler karşısında etkili olabilir çünkü tehditler genellikle alışılmadık, öngörülemeyen yollarla ortaya çıkar. İstatistiksel analiz ve makine öğrenme algoritmaları, örüntüleri öğrenebilir ve anormal olayları uyarı olarak işaretleyebilir. Bu teknik, özellikle sıfırıncı gün saldırıları ve henüz keşfedilmemiş tehditler için faydalıdır.

5. Olay Müdahale Süreçleri

Olay müdahale süreci, güvenlik olaylarını etkili bir şekilde yönetmek için beş aşamadan oluşur:

1. **Tanımlama (Detection):**
   - Güvenlik olayının tespit edilmesi için güvenlik araçları (SIEM, IDS/IPS vb.) kullanılır.
   - Anormal etkinlikler, tehditlerin ilk belirtileri, şüpheli ağ trafiği veya diğer güvenlik ihlalleri bu aşamada tespit edilir.
2. **Sınıflandırma (Classification):**
   - Olayın türü (örneğin, veri sızıntısı, yetkisiz erişim, zararlı yazılım enfeksiyonu) belirlenir.
   - Olayın ciddiyeti ve potansiyel etkisi değerlendirilerek, önceliklendirme yapılır. Bu aşama, müdahale sürecinin ne kadar acil olduğunu belirler.
3. **İzolasyon ve Müdahale (Containment and Eradication):**
   - Olayın yayılmasını önlemek için etkilenen sistemler veya ağ segmentleri izole edilir.
   - Saldırının kaynağına müdahale edilir, kötü amaçlı yazılımlar temizlenir ve güvenlik önlemleri artırılır.
   - Bu aşama, tehdidin hızlıca ortadan kaldırılması için kritik öneme sahiptir.
4. **Kurtarma (Recovery):**
   - Etkilenen sistemler normale döndürülür, yedekler veya güvenli durumdan geri yükleme işlemleri yapılır.
   - Sistemler güvenli hale getirilir ve operasyonel devamlılık sağlanır.
   - Kurtarma sürecinde, kullanıcıların ve hizmetlerin normal şekilde erişime açılmasına dikkat edilir.

5. **Analiz ve İyileştirme (Lessons Learned):**
    - Olay sonrası, saldırının nasıl gerçekleştiği ve hangi güvenlik açıklarının kullanıldığı analiz edilir.
    - Süreçler gözden geçirilir, eksiklikler belirlenir ve güvenlik politikaları, prosedürleri veya altyapısı güçlendirilir.
    - Bu aşama, gelecekteki tehditlere karşı savunma mekanizmalarının iyileştirilmesi için önemlidir.

6. SONUÇ

SOC, her tür kuruluş için kritik bir güvenlik bileşenidir. Hem büyük ölçekli şirketler hem de küçük işletmeler için, olası tehditlere karşı korunma ve hızlı yanıt verme, güvenli dijital operasyonların sürdürülebilirliğini sağlar. SOC'un etkin çalışması, doğru fonksiyonların uyum içinde işlemesi ve analistlerin uzmanlıkları ile mümkün olmaktadır. Bu bağlamda, SOC'un organizasyonlardaki rolü her geçen gün daha da önemli hale gelmektedir.

KAYNAKÇA

1. https://chatgpt.com/
2. https://www.linkedin.com/pulse/soc-security-operations-center-fundamentals-functions-responsibilities-oknof/
3. https://www.ibm.com/think/topics/security-operations-center
4. https://www.infinitumit.com.tr/guvenlik-operasyon-merkezi-soc-nedir
5. https://www.vodafone.com.tr/vodafone-business/is-dunyasi/soc-security-operations-center-nedir-ve-soc-nasil-calisir
6. https://www.microsoft.com/tr-tr/security/business/security-101/what-is-a-security-operations-center-soc?utm_source=chatgpt.com