Tarih 4/02/2025

Security Operations Center (SOC)

Hazırlayan

Kaan Akdeniz

İçindekiler

Giriş

Günümüzün dijital dünyasında siber saldırılar her geçen gün artmakta ve kurumlar için büyük tehditler oluşturmaktadır. **Security Operations Center (SOC)**, bu tehditlere karşı kurumların güvenliğini sağlamak amacıyla çalışan kritik bir güvenlik operasyon merkezidir. SOC, siber saldırıları önlemek, tespit etmek ve zamanında müdahale etmek için gelişmiş güvenlik araçlarını ve yöntemlerini kullanır.

Security Operations Center (SOC)

SOC, kurumsal ağların, sistemlerin, uygulamaların ve verilerin 7/24 izlenmesi, analiz edilmesi ve korunmasını sağlayan merkezi bir güvenlik birimidir. SOC ekipleri, siber tehditleri belirleyerek zamanında müdahale etmeyi amaçlar.

SOC'nin temel işlevleri şunlardır:

- Tehdit tespiti ve izleme
- Olay müdahale süreçlerinin yönetilmesi
- Güvenlik açıklarının analizi
- Adli bilişim (Digital Forensics) çalışmaları
- Güvenlik politikalarının oluşturulması ve uygulanması

1. SOC'nin Temel Bileşenleri

SOC'nin etkili çalışabilmesi için çeşitli bileşenlerden oluşan bir yapıya sahip olması gerekir. Başlıca bileşenler şunlardır:

1. **İnsan Kaynağı (SOC Ekibi)**
2. **Teknoloji ve Araçlar**
3. **Süreçler ve Prosedürler**

1.1 İnsan Kaynağı (SOC Ekibi)

SOC ekibi, siber güvenlik uzmanlarından oluşur ve farklı roller üstlenir. Temel SOC rolleri şunlardır:

- **Tier 1 Analist (Olay İzleme ve Analiz Uzmanı):** Güvenlik olaylarını izler, ilk analizleri yapar ve gerektiğinde üst seviyeye yönlendirir.
- **Tier 2 Analist (Olay Müdahale Uzmanı):** Tehditleri detaylı olarak analiz eder ve gerekli müdahaleleri gerçekleştirir.
- **Tier 3 Analist (Tehdit Avcısı – Threat Hunter):** Gelişmiş tehditleri proaktif olarak tespit eder ve olay sonrası incelemeler yapar.
- **SOC Müdürü:** Tüm SOC operasyonlarını yönetir ve güvenlik stratejilerini belirler.

1.2 Teknoloji ve Araçlar

SOC operasyonlarını yürütmek için çeşitli güvenlik araçları kullanılır. Başlıca araçlar şunlardır:

- **SIEM (Security Information and Event Management):** Güvenlik bilgilerini toplar, analiz eder ve anormallikleri tespit eder.
- **IDS/IPS (Intrusion Detection/Prevention Systems):** Şüpheli ağ trafiğini tespit eder ve önler.
- **EDR (Endpoint Detection and Response):** Uç nokta cihazlarını koruyarak tehditleri tespit eder ve müdahale eder.
- **Threat Intelligence (Tehdit İstihbaratı):** Güncel tehditleri ve saldırı yöntemlerini analiz eder.

1.3 Süreçler ve Prosedürler

SOC'nin etkin çalışmasını sağlamak için belirlenen standart prosedürler şunlardır:

- **Olay Müdahale Süreci:** Tehdit tespiti, değerlendirme, müdahale ve iyileştirme aşamalarından oluşur.
- **İzleme ve Analiz Süreci:** Sistemlerden gelen logların analiz edilmesi ve anormalliklerin belirlenmesi.
- **Tehdit Avcılığı (Threat Hunting):** Bilinen tehditler dışında kalan siber saldırıları proaktif olarak araştırma.

2. SOC Operasyonları ve Güvenlik Stratejileri

1. **Olay Tespiti ve Müdahale**
2. **Siber Tehdit İstihbaratı (Threat Intelligence)**
3. **Proaktif Güvenlik Yaklaşımı**

2.1 Olay Tespiti ve Müdahale

SOC, güvenlik olaylarını tespit ederek hızlı müdahale sağlar. Olay yönetimi aşağıdaki aşamalardan oluşur:

1. **Tespit:** Güvenlik olaylarının SIEM ve diğer araçlarla tespit edilmesi.
2. **Değerlendirme:** Olayın kritikliği ve etkisinin belirlenmesi.
3. **Müdahale:** Tehditin ortadan kaldırılması için aksiyon alınması.
4. **İyileştirme:** Olay sonrası sistemlerin güçlendirilmesi ve tekrar yaşanmaması için önlemler alınması.

2.2 Siber Tehdit İstihbaratı (Threat Intelligence)

Tehdit istihbaratı, SOC ekiplerinin saldırıları önceden tespit etmesine yardımcı olur. SOC, bu istihbarat sayesinde saldırganların kullandığı teknikleri analiz ederek korunma stratejileri geliştirir.

2.3 Proaktif Güvenlik Yaklaşımı

SOC, sadece reaktif bir şekilde saldırılara yanıt vermekle kalmaz, aynı zamanda proaktif olarak tehditleri önceden belirleyerek güvenliği artırır. Bu yaklaşım şunları içerir:

- **Sızma Testleri (Penetration Testing):** Sistemlerdeki güvenlik açıklarını tespit etmek için düzenli testler yapılması.
- **Güvenlik Farkındalık Eğitimleri:** Çalışanların sosyal mühendislik saldırılarına karşı bilinçlendirilmesi.
- **Otomatik Yanıt Mekanizmaları:** Anormal davranışlara otomatik yanıt verecek sistemlerin geliştirilmesi.

3. Arka Plan ve İlgili Çalışmalar

Güvenlik Operasyon Merkezleri (SOC) için olgunluk ve yetkinlik ölçümleri üzerine yapılan araştırmalar oldukça sınırlıdır. Bazı şirketler, bilgi güvenliği olay yönetimi olgunluk ölçümleri için çerçeveler geliştirmiştir. Ancak, SOC'lerin genel organizasyon yapısına yönelik olgunluk ve yetkinlik değerlendirme modelleri eksiktir. Bu nedenle, mevcut metodolojilerin incelenmesi ve SOC'ler için sistematik iyileştirme yöntemleri geliştirilmesi gerekmektedir.

3.1. Sürekli İyileştirme Modelleri

Sürekli İyileştirme (CI), süreçlerin, hizmetlerin veya ürünlerin aşamalı ve köklü değişimlerle iyileştirilmesini sağlayan bir süreçtir. Çeşitli iyileştirme metodolojileri vardır, bunlardan bazıları:

- PDCA (Plan-Do-Check-Act): Basit ve etkili bir süreçtir ancak büyük ölçekli değişiklikler için yetersiz olabilir.
- DMAIC (Define-Measure-Analyze-Improve-Control - Altı Sigma Yaklaşımı): Veriye dayalı bir modeldir ve iyileştirme süreçleri için güçlü bir temel sunar.
  Bu metodolojilerin SOC'lerde nasıl uygulanabileceği incelenmektedir.

3.2. SOC’de Olgunluk ve Yetkinlik Değerlendirme

SOC’lerin mevcut olgunluk seviyesini ölçmek için çeşitli çerçeveler geliştirilmiştir. Ancak, SOC’ye özel olgunluk ve yetkinlik modelleri sınırlıdır. Yapılan araştırmalar, birçok SOC'nin hedeflenen olgunluk seviyelerinin altında olduğunu göstermektedir. Bu yüzden, olgunluk ve yetkinlik değerlendirme modelleri SOC’lerdeki zayıflıkları belirleyerek iyileştirme sürecine katkı sağlayabilir.

3.3. Olay Yönetimi ve Yanıt Değerlendirmesi

SOC'lerde en kritik süreçlerden biri olay yönetimi ve yanıt mekanizmalarının etkinliğidir. Araştırmalara göre, olay yönetimi süreçlerinin olgunluk seviyelerini ölçmek için çeşitli çerçeveler kullanılmaktadır. Bunlardan bazıları, bilgi güvenliği olay yönetimi olgunluk ölçüm modelleri ve olay yanıt hizmetleri için değerlendirme araçlarıdır. SOC’lerin bu süreçleri iyileştirmesi için belirli metodolojiler önerilmektedir.

3.4. Olay Yönetimi ve Yanıt Hizmetinin Geliştirilmesi

SOC ekiplerinin olay yönetimi süreçlerini geliştirmesi için bazı yöntemler önerilmektedir:

- **Otomasyon**: Tekrarlayan görevlerin otomatikleştirilmesi, olayların daha hızlı tespit edilmesine ve analiz edilmesine yardımcı olur.
- **Orkestrasyon**: İnsan gücünün ve süreçlerin daha etkin yönetilmesini sağlar.
- **Metriklerin Kullanımı**: Olay yönetimi süreçlerinde başarıyı ölçmek için çeşitli metriklerin kullanılması gereklidir.

4. SOC’nin Önemi

SOC, kurumlar için siber saldırılara karşı en kritik savunma mekanizmalarından biridir. Günümüzde saldırıların daha karmaşık hale gelmesiyle birlikte SOC ekipleri gelişmiş analitik yöntemler ve yapay zeka destekli güvenlik çözümleri kullanarak tehditleri daha hızlı tespit etmektedir. Yani bir oalyın baştan sona içinde olan bir görev denebilir.

Sonuç

Günümüzün dijital dünyasında siber tehditlerin giderek daha karmaşık hale gelmesi, kurumların güvenliğini sağlamak için güçlü bir güvenlik operasyon merkezi (SOC) oluşturmalarını zorunlu kılmaktadır. SOC, siber tehditleri tespit etmek, analiz etmek ve hızlı müdahale sağlamak için kritik bir yapı olarak konumlanmaktadır.

SOC’nin temel bileşenleri olan insan kaynağı, teknoloji ve süreçler, etkin bir güvenlik yönetimi için uyum içinde çalışmalıdır. Olay tespiti ve müdahale süreçleri, siber tehdit istihbaratı ve proaktif güvenlik yaklaşımları sayesinde, SOC ekipleri saldırıları en aza indirerek kurumların siber dayanıklılığını artırmaktadır.

Sonuç olarak, SOC’nin önemi gün geçtikçe artmakta ve siber güvenlik stratejilerinin ayrılmaz bir parçası haline gelmektedir. Kurumların, modern tehditlere karşı güçlü bir savunma mekanizması oluşturabilmeleri için gelişmiş SOC operasyonlarını benimsemeleri büyük bir gereklilik haline gelmiştir.

Kaynakça

1-) Antonucci, D. (2020). Implementing an Effective Security Operations Center. Wiley.

2-) **SOC Nedir ve SOC Merkezleri Nasıl Çalışır?**