SOC FUNDAMENTALS

ALTAY TAKIMI

HAZIRLAYAN:**MUHAMMED ALİ ZENGİN**
22.02.2025

İçindekiler

1.GİRİŞ

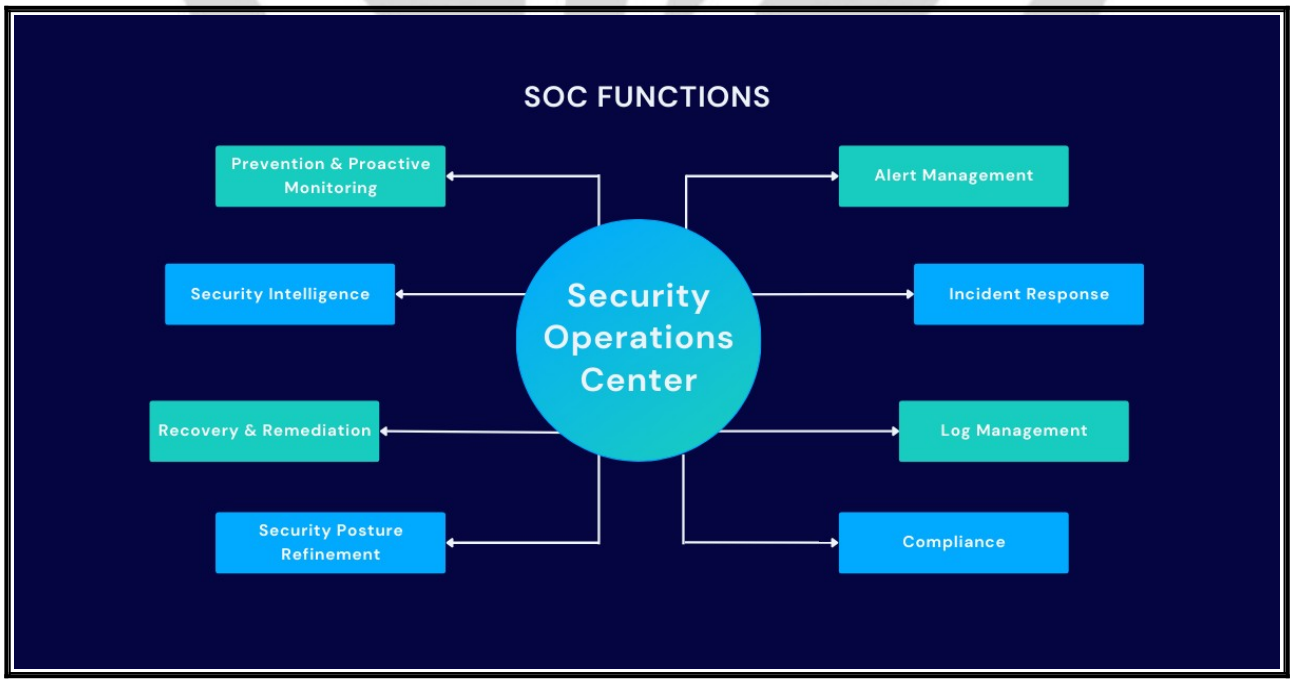
Bu rapor, Security Operations Center (SOC) kavramını, işlevlerini, organizasyon yapısını ve kullanılan güvenlik teknolojilerini detaylı bir şekilde incelemeyi amaçlamaktadır. Günümüzün dijital dünyasında, siber tehditler giderek daha karmaşık ve sofistike hale gelmektedir. Bu tehditlere karşı kuruluşların etkin bir savunma mekanizması oluşturabilmesi için SOC yapıları kritik bir rol oynamaktadır. Rapor, SOC'nin temel görevlerini, ekip yapısını ve kullanılan güvenlik araçlarını ele alarak, bir organizasyonun siber güvenliğini nasıl güçlendirebileceğini ortaya koymayı hedeflemektedir. Aynı zamanda, SOC'nin operasyonel süreçlerini, tehdit yönetimindeki önemini ve organizasyonların siber güvenlik stratejilerine olan etkisini değerlendirmektedir.

2.SOC Nedir?

Security Operations Center ifadesinin kısaltması olan SOC ,bir kuruluşun siber güvenlik duruşunu geliştirmekten ve tehditlere karşı korumaktan, tehditleri algılamaktan ve tehditlere yanıt vermekten sorumlu merkezi bir işlev veya ekiptir. Çeşitli teknolojik çözüm kombinasyonları kullanarak kurumun siber güvenliğini sağlamaktır. Bu süreçte SOC ekipleri, ağlar, sunucular, veritabanları, uygulamalar ve diğer sistemlerdeki etkinliği izleyip analiz ederek bir güvenlik olayını veya tehdit unsuru sayılabilecek anormal etkinlikleri araştırır.

3.SOC Görevleri

SOC ekip üyeleri saldırıları önlemeye, yanıtlamaya ve saldırılardan kurtarmaya yardımcı olmak için aşağıdaki işlevleri üstlenir.



3.1. Önleme ve İzleme

Siber saldırılara karşı en iyi savunma, önleyici tedbirler almaktır. SOC ekibi, siber suç trendlerini takip ederek güncel tehditlere karşı hazırlıklı olur. Ayrıca, olay müdahale planları oluşturur, güvenlik açıklarını yamalar ve diğer önleyici önlemleri uygular.

3.2.Alarm Yönetimi

SOC'nin temel işlevlerinden biri, güvenlik izleme araçları tarafından oluşturulan alarmları toplamak ve yönetmektir. Bu süreçte güvenlik duvarları (firewalls), saldırı tespit ve önleme sistemleri (IDPS) ve güvenlik bilgi ve olay yönetimi sistemleri (SIEM) gibi teknolojiler kullanılır.

3.3. Güvenlik İstihbaratı

SOC, gerçek zamanlı veya gerçek zamana yakın tehdit bilgileri sağlayarak organizasyonun güvenliğini artırır. Kullanılan güvenlik araçları tarafından tespit edilen tehditler analiz edilir ve önleyici adımlar atılır.

3.4. Olay Müdahalesi

SOC'nin en kritik rollerinden biri, güvenlik olaylarına anında müdahale etmektir. Olay müdahale süreçleri şunlardır:
-Etkilenen cihazları ve sistemleri izole etmek,
-Tehditleri sınıflandırmak ve analiz etmek,
-Tüm olayları belgelerle kayıt altına almak ve gelecekte benzer tehditlere karşı referans oluşturmak.

3.5. Kurtarma ve Düzeltme (Remediation)

SOC, bir olay sonrasında sistemleri eski haline döndürmek ve kaybolan verileri kurtarmaktan sorumludur.
Veri ihlali gibi durumlarda sistemlerin yeniden yapılandırılması,
Ransomware (fidye yazılımı) saldırılarında yedeklerin kullanılması gibi süreçleri yönetir.

3.6.Log Yönetimi

SOC ekibi, kurum içindeki tüm aktiviteleri ve iletişimleri sürekli izler, saklar ve analiz eder. Bu süreç, Normal ve anormal aktiviteleri tespit etmek,
Siber tehditleri belirlemek ve engellemek amacıyla kullanılır.

3.7. Güvenlik Duruşunun Sürekli İyileştirilmesiSOC, organizasyonun güvenlik seviyesini sürekli olarak analiz eder ve geliştirir.
Yeni tehditlere karşı güvenlik politikaları güncellenir, Savunma mekanizmaları sürekli güçlendirilir.

3.8. Uyumluluk (Compliance)

Özellikle kamu ve özel sektör kuruluşları, siber güvenlik regülasyonlarına uyum sağlamak zorundadır. SOC, Güvenlik standartlarına uyumluluğu sağlar,
Denetim süreçlerini yönetir ve organizasyonun yasal gerekliliklere uygun çalışmasını garanti eder.

Bu fonksiyonlar sayesinde SOC ekipleri, siber tehditleri tespit ederek organizasyonun güvenliğini en üst seviyeye çıkarmayı hedefler.

4.SOC Ekibi ve Organizasyon Yapısı

SOC ekibindeki analistler üç temel seviyeye ayrılır:

4.1.Tier 1 SOC Analisti

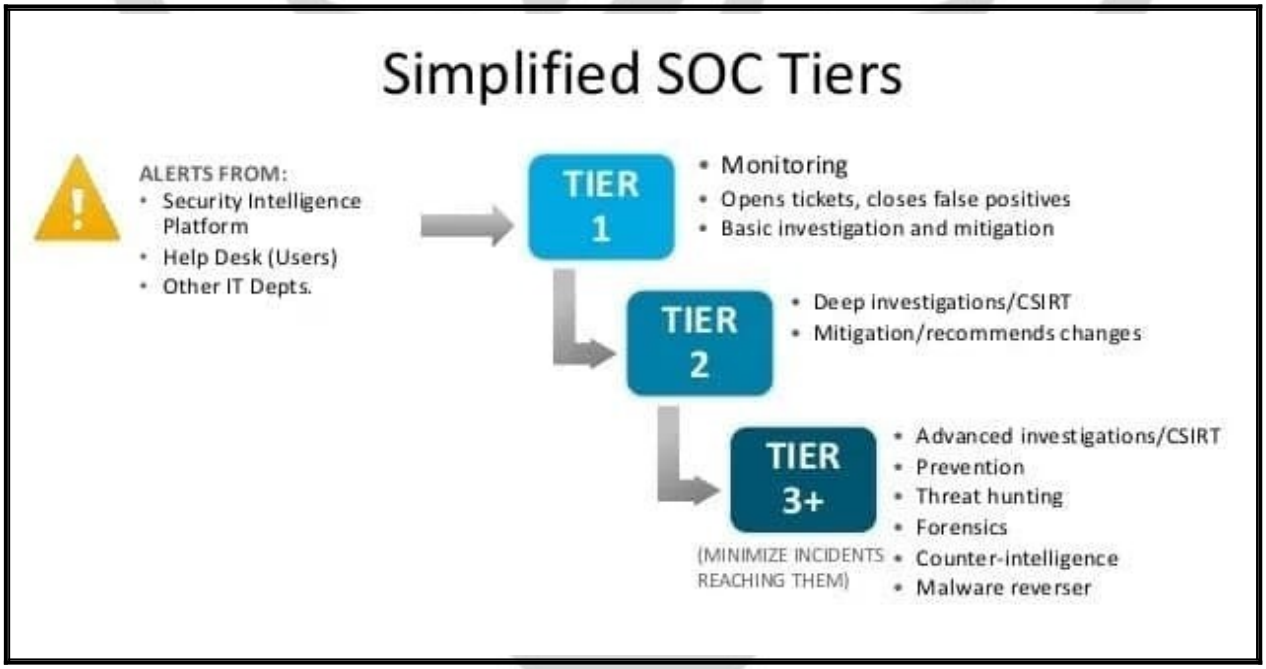
Tier 1 analistleri, SOC ekibinin ilk savunma hattıdır. Gündelik izleme ve alarmlara ilk yanıt verme görevini üstlenirler. Gelen alarmları analiz eder ve kritik olanları bir üst seviyeye aktarırlar.

4.2.Tier 2 SOC Analisti

Tier 2 analistleri, Tier 1 tarafından iletilen olayların derinlemesine analiz edilmesinden sorumludur. Alarmların teknik detaylarını inceler, olayın kaynağını belirler ve gereken aksiyonları planlar.

4.3.Tier 3 SOC Analisti

Tier 3 analistleri, SOC ekibinin en deneyimli üyeleridir. Ağ içerisinde henüz tespit edilmemiş tehditleri belirler, ileri seviye zararlı yazılım analizleri yapar ve organizasyonun uzun vadeli güvenlik stratejilerini geliştirir.



4.4.SOC Yöneticisi :

En üst tabakadır. Seviye 1,2 ve 3 analistlerinin yetkinliklerine ek olarak güçlü liderlik ve iletişim yeteneklerine sahip olmalıdır. Ekip ruhunu diri tutmalıdır. SOC yöneticisi, operasyonları ve ekibi yönetir. SOC ekibinin faaliyetlerini gözetler. Ekip için eğitim süreçlerini , işe alım ve değerlendirmelerini yapar. Saldırıların süreçlerini yönetir ve olay raporlarını gözden geçirir. Ekiple haberleşme için iletişim planını geliştirir ve uygular. Uyumluluk raporlarını yayınlar .Denetleme süreçlerini yakından takip eder ve destekler; SOC önemini iş dünyasına aktarır.

4.5.Siber Tehdit İstihbaratı Ekibi :

Siber tehdit istihbaratı, kurumlarda güvenliğine zarar verebilecek tehditler hakkında tanımlanmış, toplanmış ve zenginleştirilmiş verilerin bir süreçten geçirilerek analiz edilmesi sonucu saldırganların amaçlarını ve metotlarını tespit etmeye yarayan bir istihbarat türüdür. Siber tehdit istihbaratı ,bir kurumun veya varlığın güvenliğini tehdit eden mevcut ve potansiyel saldırılar hakkındaki bilgilerin toplanmasına, analiz edilmesine odaklanan siber güvenlik alanıdır. Büyük SOC ekipleri tehdit istihbaratına özel görevlendirmeler yapabilirler. Daha küçük SOC ekipleri ise güvenilir bir tehdit istihbaratı hizmet sağlayıcısından bilgi almak gibi bir yöntem uygulayabilirler.

5.SOC araçları ve teknolojileri

5.1.SIEM (Security Information and Event Management)

SIEM çözümleri, organizasyon genelinde ağ, sistem ve uygulamalardan toplanan logları analiz ederek güvenlik olaylarını tespit etmeye yardımcı olur. Anormal aktivitelerin belirlenmesi, gerçek zamanlı tehdit analizi yapılması ve detaylı log yönetimi gibi kritik işlevleri yerine getirir. Splunk, IBM QRadar ve Microsoft Sentinel gibi araçlar, en yaygın kullanılan SIEM çözümleri arasındadır.

5.2.IDS & IPS (Intrusion Detection & Prevention Systems)

IDS sistemleri, ağ trafiğini analiz ederek şüpheli aktiviteleri tespit ederken, IPS sistemleri ise bu tehditleri engelleyerek saldırıların gerçekleşmesini önler. Yetkisiz erişimleri tespit edip engelleyen bu sistemler, organizasyonun siber güvenlik altyapısının korunmasına büyük katkı sağlar. Snort ve Palo Alto Networks, yaygın kullanılan IDS/IPS çözümlerindendir.

5.3.EDR (Endpoint Detection and Response) ve XDR (Extended Detection and Response)

EDR ve XDR çözümleri, uç noktalarda gerçekleşen şüpheli aktiviteleri tespit eder ve tehdit avcılığı yaparak güvenlik açıklarını belirler. Kullanıcı cihazları, sunucular ve mobil sistemlerde gelişmiş analizler gerçekleştirerek tehditlere karşı otomatik müdahale mekanizmaları oluşturur. CrowdStrike

Falcon, Microsoft Defender for Endpoint ve SentinelOne, bu alanda en çok kullanılan araçlardır.

5.4.SOAR (Security Orchestration, Automation, and Response)

SOAR çözümleri, güvenlik operasyonlarını otomatikleştirerek tehditlere daha hızlı müdahale edilmesini sağlar. Tehdit istihbaratı ile entegre çalışarak alarm yönetimini otomatize eder ve olay müdahalesi için önceden tanımlanmış aksiyon planlarını devreye sokar. Splunk Phantom ve Palo Alto Cortex XSOAR, yaygın kullanılan SOAR araçları arasında yer almaktadır.

5.5.NDR (Network Detection and Response)

NDR çözümleri, ağ trafiğini sürekli olarak analiz ederek hem bilinen hem de bilinmeyen tehditleri tespit etmeye yardımcı olur. Anormal ağ hareketlerini algılayarak iç tehditleri belirleyen bu sistemler, SIEM ve SOAR çözümleriyle entegre çalışarak tehditlerin tespit edilmesini ve önlenmesini sağlar. Darktrace, Vectra AI ve Cisco Stealthwatch, NDR alanında kullanılan başlıca çözümlerdir.

6.SONUÇ

Bu rapor, Security Operations Center (SOC) yapısını, işlevlerini, organizasyonel yapısını ve kullanılan güvenlik teknolojilerini kapsamlı bir şekilde incelemiştir. Araştırma sürecinde, SOC'nin siber güvenlikte kritik bir rol oynadığı, yalnızca saldırıları tespit etmekle kalmayıp proaktif önlemlerle tehditleri önlemeye de odaklandığı görülmüştür.SOC'nin yalnızca olay müdahalesiyle sınırlı kalmayıp, organizasyonların güvenlik politikalarını sürekli iyileştirdiği ve regülasyonlara uyumu sağladığı görülmüştür. Bu araştırma, SOC'nin günümüz siber tehditlerine karşı nasıl etkin bir savunma mekanizması oluşturduğunu ve güvenlik süreçlerinin nasıl daha verimli hale getirilebileceğini anlamak açısından önemli bilgiler sağlamıştır.

7.KAYNAKÇA:

https://www.ibm.com/think/topics/security-operations-center
https://www.comptia.org/content/articles/what-is-a-security-operations-center
https://berqnet.com/blog/soc
https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir
https://www.infinitumit.com.tr/guvenlik-operasyon-merkezi-soc-nedir/