SOC Fundamentals

Hazırlayan: Esra Akteke
Tarih: 07.02.2025

Giriş

Siber dünyada artan tehditlerle mücadele etmek ve sistemlerin güvenliğini sağlamak için Güvenlik Operasyon Merkezleri (SOC) kritik bir role sahiptir. SOC, kurumların siber güvenlik operasyonlarını merkezi bir noktadan yönetmelerine ve anlık tehditlere karşı hızlı müdahale etmelerine olanak tanır. Bu rapor SOC'un temel yapı taşlarını, işleyişini ve siber güvenlik ekosistemindeki önemini anlamayı amaçlamaktadır.

SOC Nedir?

Security Operations Center (SOC), bir kurumun siber güvenliğini 7/24 izleyen, tehditleri analiz eden ve gerekli önlemleri alan stratejik bir savunma hattıdır. SOC'un temel görevi, kuruma yönelik tehdit ve saldırıları tespit etmek, loglamak ve bu tehditleri derinlemesine inceleyerek olası zararları önlemektir. Başarılı bir SOC ekibi, yalnızca kurum içi olayları takip etmekle yetinmez; sektör dinamiklerini, globalde ki yeni saldırı trendlerini ve ülkeye yönelik tehditleri de sürekli gözlem altında tutar. Bu yaklaşım potansiyel riskleri erken fark etmeyi ve kritik müdahalelerle saldırıları etkisiz hale getirmeyi sağlar.

SOC Analisti Nedir?

Bir organizasyonun siber güvenlik altyapısını sürekli olarak izleyen, güvenlik olaylarını tespit eden ve bu olaylara müdahale eden uzman kişidir. SOC analistleri, tehditleri belirlemek, değerlendirmek ve bunlara zamanında müdahale etmekten sorumludur. Farklı tecrübe seviyelerine göre L1, L2 ve L3 olarak üç katmana ayrılırlar.

SOC Analisti Rolleri

L1 Analisti:

SOC'un ilk savunma hattında görev yapar ve temel güvenlik olaylarının izlenmesi ve ilk değerlendirmesinden sorumludur. SIEM sistemi üzerinden gelen alarmları sürekli takip ederek olayların ön elemesini gerçekleştirir. Bu süreçte, öncelikle olayları kategorize edip önem derecelerine göre sıralar ve müdahale gerektiren durumları tespit eder. İlk değerlendirmede çözülmesi mümkün olmayan veya daha derinlemesine analiz gerektiren karmaşık olayları, ayrıntılı inceleme yapılması için L2 analistlerine iletir.

L2 Analisti:
L1'in ilettiği olayları derinlemesine analiz eder ve olay müdahalesini yönetir. Tehditleri doğrulamak, saldırı vektörlerini belirlemek ve olayın kapsamını anlamak temel görevlerindendir. Kök neden analizi yaparak tehdidin kaynağını tespit eder ve gerektiğinde zararlı yazılım analizine başvurur. Olay müdahale sürecinde aktif rol alır ve L1 analistlerine rehberlik eder.

L3 Analisti:
SOC'da en tecrübeli uzmandır. Proaktif tehdit avcılığı yaparak gizli tehditleri tespit eder ve APT saldırılarına karşı savunma stratejileri geliştirir. SIEM ve güvenlik sistemlerini optimize ederken adli bilişim süreçlerini de yönetir, olayların derinlemesine analizini yapar.

Incident Responder (Olay Müdahale Görevlisi):
Güvenlik olaylarına hızlıca müdahale eden ve tehditleri etkisiz hale getiren kişidir. Olayın kaynağını ve etkisini hızlı bir şekilde belirler, sistemleri tekrar güvenli hale getirir. Zararlı etkinlikleri durdurarak kurtarma süreçlerini yönetir ve olay sonrası raporlama yapar.

Threat Hunter (Tehdit Avcısı):
Sistemlerde gizlenen tehditleri proaktif olarak arayan uzmandır. Bilinen saldırıların ötesine geçerek yeni tehditleri ve anormal davranışları tespit eder. Proaktif tehdit avcılığı yapar, yeni saldırı yöntemlerini ve kötü niyetli aktiviteleri belirler, ileri düzey log ve ağ trafiği analizleri gerçekleştirir.

Security Engineer:
Güvenlik altyapısını tasarlayan, kuran ve bakımını yapan kişidir. SIEM ve IDS/IPS gibi SOC araçlarının bakımını yapar, güvenlik politikaları geliştirir ve yeni güvenlik çözümleri entegre eder. Ayrıca sistem açıklarını analiz ederek güvenlik çözümleri oluşturur.

SOC Manager:
SOC operasyonlarını yöneten ve ekibin performansını denetleyen kişidir. Ekip koordinasyonunu sağlar, olay müdahale süreçlerini gözden geçirir ve iyileştirmeler önerir. Ayrıca üst yönetime raporlar hazırlayarak siber güvenlik stratejilerini geliştirir.

SOC'da Olay Yönetim Süreci Nedir?

Olay yönetimi, bir kuruluşun operasyonlarında kesintiye neden olabilecek tehditleri tespit etme, analiz etme ve bu tehditleri düzeltme sürecidir. Etkili olay yönetimi, olası zararın önlenmesi ve gelecekteki olayların tekrarını engellemeyi amaçlar. Bu süreç, genellikle bir olay müdahale ekibi veya olay yönetim ekibi tarafından yönetilir.

Yapılandırılmış bir olay yönetimi olmadan güvenlik ihlalleri, sistem arızaları veya hizmet kesintileri ciddi veri kaybına, düşük üretkenlik ve gelir kaybına yol açabilir. Ayrıca hizmet seviyesi sözleşmelerinin ihlali gibi sorumluluklar da ortaya çıkabilir. Etkili bir olay yönetimi süreci organizasyonun iş sürekliliğini sağlamak için kritik öneme sahiptir.

SOC'da Olay Yönetimi Süreçleri

Hazırlık:
Hazırlık aşaması, organizasyonun olası tehditlere karşı ne kadar hazır olduğunu belirlemeyi amaçlar. Bu süreçte olay müdahale planları oluşturulur ve ekipler potansiyel tehditlere karşı eğitim alır. Ayrıca gerekli güvenlik araçları ve kaynaklar sağlanarak, ekiplerin etkili müdahale yapabilmesi için altyapı oluşturulur. Hazırlık dediğimiz süreç olası olaylara karşı önceden plan yaparak etkili bir müdahale süreci için temel oluşturmayı amaçlar diyebiliriz.

Tespit:
Organizasyonun güvenlik altyapısı sürekli olarak izlenir ve potansiyel tehditler belirlenir. Ağ trafiği izleme, güvenlik alarmlarını yönetme ve tehdit avcılığı gibi faaliyetleri içerir. İzleme araçları şüpheli aktiviteleri gerçek zamanlı olarak takip eder, alarmlar oluşturur ve güvenlik ekibine bildirir. Tehdit avcıları ise bilinen tehditlerin ötesine geçerek, gizlenen veya yeni ortaya çıkan tehditleri proaktif şekilde arar.

Müdahale:
Tespit edilen tehditlere karşı hızlı bir şekilde aksiyon alınır. Soc ekibi olayın yayılmasını engellemek ve hasarı sınırlamak için gerekli adımları atar. Bu aşama etkin bir izolasyon, geçici çözümler ve güvenlik açığının kapatılması işlemlerini içermektedir. Olayın ne kadar genişlediği ve hangi sistemlerin etkilendiği belirlenerek öncelikli müdahaleler yapılır.

Kurtarma:
Olayın etkilerinin ortadan kaldırılmasını ve sistemlerin tekrar normal çalışır hale getirilmesini içerir. Kötü amaçlı yazılımlar temizlenir, sistemler yeniden yapılandırılır ve gerekirse yedeklemelerden geri yükleme yapılır. Ayrıca yamalar ve güncellemeler uygulanarak benzer bir olayın tekrar yaşanmaması için sistemlerin güvenliği güçlendirilir. Bu aşama, organizasyonun en kısa sürede eski işleyişine dönmesini sağlamayı amaçlamaktadır.

İnceleme ve Raporlama:
Olayın kök neden analizi yapılır. Ekip olayın kaynağını, nasıl yayıldığını ve etkilerini belirler. Bu analiz gelecekteki benzer olayları önlemek için önemli bilgileri sunuyor. Olayın raporlanması ise ilgili taraflara şeffaf bilgi sunar. Raporlama sürecinde olayın yönetimi sırasında yapılanlar ve alınan dersler ayrıntılı olarak belirtilir. Ayrıca olayın neden olduğu herhangi bir zararın telafisi için öneriler de sunulabilir.

Sürekli İzleme ve İyileştirme:
Olaso tehditlerin belirli aralıklarla değerlendirilmesini ve sistemlerin güvenliğinin sürekli kontrol edilmesini sağlar. Organizasyonun daha önce yaşanan olaylardan ders çıkarmasına yardımcı olur. İyileştirme çalışmaları elde edilen veriler doğrultusunda güvenlik süreçlerinin güçlendirilmesi için yapılır. Yeni güncellemeler, yazılım yamaları ve süreç iyileştirmeleri, güvenlik altyapısının sürekli olarak daha dayanıklı hale gelmesini sağlar.

SIEM (Security Information and Event Management) Nedir?

Güvenlik olaylarını toplamak, analiz etmek ve yönetmek için kullanılan bir yazılım sistemidir. SIEM, ağ ve sistemlerden gelen logları merkezi bir platformda toplar ve analiz eder. Şüpheli etkinlikler veya güvenlik tehditleri tespit edildiğinde güvenlik ekiplerine uyarılar gönderir. Bu araç olay yönetimini kolaylaştırarak hızlı müdahaleyi ve uyumluluk raporlamasını destekler. Aynı zamanda geçmişteki güvenlik olaylarını inceleyerek organizasyonların güvenlik duruşlarını güçlendirmelerine yardımcı olabiliyor.

Temel Güvenlik İzleme
Sistem ve ağ aktiviteleri sürekli izlenir, güvenlik olayları tespit edilip kaydedilir.

Gelişmiş Tehdit Algılama
Şüpheli davranışlar ve karmaşık tehditler tespit edilerek daha derinlemesine analiz yapılır.

Adli Bilişim ve Olay Müdahalesi
Olaylar detaylı şekilde incelenir, güvenlik ihlallerinin kaynağı belirlenir ve uygun müdahale gerçekleştirilir.

Günlük Toplama
Çeşitli sistemlerden gelen günlük verileri toplanarak merkezi bir sisteme aktarılır.

Normalleştirme
Farklı formatlardaki veriler tek bir standarda dönüştürülerek analiz için hazır hale getirilir.

Bildirimler ve Uyarılar: Tespit edilen tehditler hakkında güvenlik ekibine bildirimler gönderilir, hızlı müdahale sağlanır.

Splunk, IBM QRadar, ArcSight, LogRhythm, AlienVault, Graylog ve SolarWinds Security Event Manager gibi araçlar popüler SIEM çözümlerine örnek olarak gösterilebilir.

SOAR (Security Orchestration, Automation, and Response) Nedir?

SOAR, güvenlik olaylarına hızlı ve etkili bir şekilde yanıt vermek amacıyla kullanılan yazılım platformudur. Güvenlik süreçlerini otomatikleştirir, olay yönetimini entegre eder ve güvenlik ekiplerinin olaylara daha hızlı müdahale etmesini sağlar. Farklı güvenlik araçlarını ve süreçlerini birleştirerek tehditlerin otomatik olarak algılanmasını, sınıflandırılmasını ve yanıtlanmasını mümkün kılar. Ayrıca bu platformlar güvenlik olaylarının yönetimi sırasında zaman kazandırarak insana dayalı müdahale ihtiyacını en aza indirmeyi amaçlar diyebiliriz.

Otomatikleştirilmiş İşlemler
SOAR güvenlik süreçlerini otomatikleştirir ve olaylara anında yanıt verir. Böylece manuel müdahaleyi azaltıyor.

İş Akışı Orkestrasyonu
Farklı güvenlik araçları ve sistemleri arasında sorunsuz bir iş akışı oluşturur. Bu şekilde işlemler hızlı ve verimli bir şekilde yürütülüyor.

Olay Yanıtı ve Müdahale
Olayları hızlı bir şekilde tespit eder ve önceden belirlenmiş yanıt prosedürlerine göre müdahale eder.

Entegre Güvenlik Araçları
Farklı güvenlik sistemleri ve uygulamaları bir araya getirerek tüm güvenlik altyapısını merkezi bir noktadan yönetir.

Raporlama ve Analiz Süreci
Güvenlik olaylarının analizini yapar ve raporlar sunarak organizasyonların güvenlik duruşlarını güçlendirir.

Palo Alto Networks Cortex XSOAR, IBM Resilient, Splunk Phantom, Swimlane, D3 Security gibi araçlar SOAR çözümlerine örnek olarak gösterilebilir.

IDS Nedir?

Ağda veya sistemde gerçekleşen şüpheli etkinlikleri veya güvenlik ihlallerini tespit etmek için kullanılan bir güvenlik teknolojisidir. Genellikle veri trafiğini izler, ağda olağandışı bir davranış veya tehdit algıladığında güvenlik ekiplerine uyarılar gönderir. Burada ki önemli nokta IDS sadece tespit yapmakla sınırlıdır ve herhangi bir müdahalede bulunmaz. Temel amacı potansiyel tehditleri erken aşamalarda fark ederek, bu konuda önlem alınabilmesi için bilgi sağlamaktır.

Snort, Suricata, Zeek, Cisco Secure IDS, McAfee Network Security Platform gibi araçlar IDS çözümlerine örnek olarak gösterilebilir.

IPS Nedir?

Ağdaki veya sistemdeki güvenlik tehditlerini tespit eden ve aynı zamanda bu tehditlere karşı aktif olarak müdahale eden bir güvenlik teknolojisidir. IDS den farklı olarak ağda veya sistemdeki şüpheli etkinlikleri tespit etmekle kalmaz, aynı zamanda bu tehditlere karşı aktif olarak müdahale de eder. Sadece güvenlik ihlalleri konusunda uyarı vermekle kalmaz, aynı zamanda tehditleri engellemek için otomatik aksiyonlar alır. Bu aksiyonlar arasında ağ trafiğini engellemek, şüpheli bağlantıları sonlandırmak veya zararlı paketleri durdurmak gibi işlemler bulunur.

Palo Alto Networks, Cisco Firepower, Snort, Suricata, Check Point IPS gibi araçlar, IPS çözümlerine örnek olarak gösterilebilir.

Log Management Nedir?

Bir organizasyonun ağındaki sistemlerindeki ve uygulamalarındaki tüm log verilerini toplama, depolama, analiz etme ve raporlama sürecini ifade ediyor. Bu süreç güvenlik olaylarının izlenmesi, sistem hatalarının tespiti ve uyumluluk gereksinimlerinin karşılanması için kritik bir öneme sahiptir.

Log management araçları verileri merkezi bir noktada toplar, normalize eder ve analiz edilmesini sağlar. Aynı zamanda logların uzun vadeli depolanması, erişilebilir olması ve gerektiğinde denetim amaçlı sorgulanabilir olması sağlanır. Bu araçlar organizasyonların güvenlik tehditlerini erken tespit etmelerine, sistem performansını optimize etmelerine ve yasal uyumluluk gereksinimlerini karşılamalarına yardımcı olur.

Log Yönetimi Süreçleri

Veri Toplama: Farklı sistemlerden, uygulamalardan ve ağ cihazlarından log verileri toplanıyor. Sistemde ki her türlü etkinliği ve güvenlik olayını kapsar.

Veri Normalleştirme: Farklı kaynaklardan gelen log verileri tutarlı ve analiz edilebilir bir formata dönüştürülür. Veri çeşitliliğini azaltarak daha verimli analiz yapılmasını sağlar.

Veri Depolama: Toplanan loglar uzun süreli depolama ve erişilebilirlik sağlamak amacıyla güvenli bir ortamda saklanır. Veriler gerektiğinde sorgulanabilir olmalıdır.

Analiz ve İzleme: Log verileri sürekli izlenir ve analiz edilir. Şüpheli etkinliklerin tespit edilmesi ve güvenlik tehditlerine karşı hızlı tepki verilmesi için kritik öneme sahiptir diyebiliriz.

Raporlama: Log verileri uyumluluk gereksinimlerini karşılamak veya olaylara dair raporlar hazırlamak amacıyla düzenli olarak raporlanır.

İzleme ve Uyarılar: Log verilerindeki anormallikler sistemdeki olası tehditleri veya hataları izlemek için sürekli olarak denetlenir. Belirli eşiklerin aşılması durumunda uyarılar gönderilir.

Arşivleme ve Yedekleme: Log verileri belirli bir süre saklanarak gerektiğinde geçmişe dönük analiz ve denetim yapılabilmesi için arşivlenir.

Uyumluluk Sağlama: Yasal düzenlemelere ve endüstri standartlarına uygunluk sağlamak için log yönetimi süreçleri uyumlu olmalıdır. Organizasyonların denetimlere hazır olmasını sağlar.

Sonuç

Bu raporda SOC ve siber güvenlik alanındaki çeşitli bileşenler incelenmiştir. Yapılan araştırmalar SOC'un bir organizasyonun siber güvenlik altyapısındaki kritik rolünü vurgulamaktadır. Özellikle SOC'un gerçek zamanlı tehdit izleme, saldırı tespiti ve olay müdahalesi süreçlerindeki etkinliği, kurumların güvenlik duruşunu büyük ölçüde güçlendirmektedir. Bu anlamda çok önemlidir.

SIEM, IDS/IPS, SOAR gibi araçların SOC içinde nasıl kullanıldığı ve bu araçların kurumların güvenlik stratejilerini aslında nasıl desteklediği detaylandırılmıştır diyebiliriz. Bu araçlar organizasyonların güvenlik tehditlerine hızlı ve etkili bir şekilde yanıt vermesini sağlayarak olası güvenlik açıklarının en aza indirilmesine yardımcı olmaktadır.

Araştırmada elde edilen bilgiler SOC'un yalnızca savunma amacı taşımadığını, aynı zamanda proaktif tehdit avcılığı, güvenlik stratejilerinin geliştirilmesi ve sürekli iyileştirme konularında stratejik bir rol oynadığını göstermektedir. Aynı zamanda güvenlik yönetimi ve olay müdahale süreçlerinin etkin bir şekilde yönetilmesi organizasyonların uzun vadeli siber güvenlik hedeflerine ulaşmalarını sağlamaktadır. Bu tür organizasyonlarda sistemin güvenliğinin sağlanması her şeyden önemlidir. Organizasyon çeşitliliğine bağlı olarak verilerin korunması ve güvenliğinin sağlanması önceliklidir.

Siber güvenlik ekosisteminde SOC'un önemi giderek artmaktadır ve bu yapının verimli çalışabilmesi için doğru araçlar, beceriler ve süreçlerin entegre edilmesi, kullanılan teknolojilerin güncel olması ve süreklilik bakımından bakımı yapılarak düzenli kontrol edilmesi gerekmektedir. Bu rapor SOC'un etkinliğini artırmak ve kurumların siber güvenlik stratejilerini güçlendirmek için gerekli olan unsurların altını çizmektedir.

Kaynakça

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

https://www.inosas.com.tr/2023/05/29/olay-yonetimi-nedir-2/#:~:text=Olay%20y%C3%B6netimi%20s%C3%BCre%C3%A7leri%2C%20olaylara%20m%C3%BCdahale,ve%20hangi%20ara%C3%A7lar%C4%B1n%20kullan%C4%B1ld%C4%B1%C4%9F%C4%B1n%C4%B1%20i%C3%A7erir.

BTK Akademi - Siber Olaylara Müdahale (Kurs)

https://www.beyaz.net/tr/guvenlik/makaleler/soc_araclari.html

https://www.hackthebox.com/blog/soc-analyst-tools-essentials-for-blue-teams

https://www.microsoft.com/tr-tr/security/business/security-101/what-is-siem

https://www.fortinet.com/resources/cyberglossary/what-is-siem

https://www.fortinet.com/resources/cyberglossary/what-is-soar

https://www.paloaltonetworks.com/cyberpedia/what-is-soar

https://medium.com/@tahirbalarabe2/what-is-a-soar-security-orchestration-automation-response-13c7460ec493

https://www.ibm.com/think/topics/security-orchestration-automation-response

https://www.servicenow.com/products/security-operations/what-is-soar.html

https://www.techcareer.net/blog/ips-ve-ids-nedir?gad_source=1&gclid=Cj0KCQiA-5a9BhCBARIsACwMkJ4n85G56SCj-Uur6QltK9anNLfAbIOMFR2KQj2B6dDF8wdt6KH6dwcaAksMEALw_wcB

https://www.exabeam.com/explainers/log-management/log-management-process-tools-and-tips-for-success/

https://www.cloudpanel.io/blog/log-management/

https://www.turk.net/blog/ips-ve-ids-nedir-nasil-calisir/

https://www.techcareer.net/en/blog/ips-ve-ids-nedir

https://www.okta.com/identity-101/ids-vs-ips/