SOC Fundamentals

Hasan Karaca

5.02.2025

İÇİNDEKİLER

SOC Nedir

SOC, Güvenlik Operasyonları Merkezi (Security Operations Center) bir kuruluşun güvenliğini devamlı olarak izleyen ve güvenlik olaylarının analizinden sorumlu bir bilgi güvenliği ekibinin bulunduğu yer veya tesistir. Bu ekip, teknolojik çözümleri kullanarak iyi bir süreç yönetimi yapar ve siber güvenlik olaylarının tespit edilmesini sağlayıp analizini sunar. Siber saldırılara karşı aksiyon alır.

Bu rapor, SOC'un temel bileşenlerini, işlevlerini ve organizasyonlar için önemini açıklamayı amaçlamaktadır.

SOC Katmanları

L1 Uyarı Analisti (Alert Analyst):

Takip ettiği loglarda izinsiz bir giriş veya müdahale görmesi halinde ilk aşamayı başlatır ve bir güvenlik tehdidi olduğunu katman 2'ye iletir. Bu sırada katman 2'nin kullanabileceği verileri toplamaya başlar. Bu katmanda daha çok monitoring ekibi yer alır. IDS/IPS'ler, SIEM sistemleri bu analistlere yardımcı olur. False positive durumlarını önlemeye çalışır.

Temel düzeyde bilgi güvenliği, network, log yönetimi ve SIEM konusunda bilgi sahibidir.

L2 Tehdit Yanıtlayıcı (Incident Responder) :

SOC L2 analisti, güvenlik olaylarını daha derinlemesine inceleyen ve L1 analistlerinden gelen alarmları değerlendirerek gerçek tehditleri belirleyen uzmanlardır. SIEM araçlarını kullanarak olay korelasyonu yapar, tehdit avcılığı gerçekleştirir ve olay yanıt süreçlerinde aktif rol oynar. Yanlış pozitifleri filtreleyerek kritik güvenlik ihlallerini tespit eder ve gerektiğinde L3 analistlerine veya diğer güvenlik ekiplerine eskalasyon yapar. IDS/IPS, EDR ve güvenlik duvarları gibi sistemleri analiz ederek siber tehditlere karşı etkin savunma sağlar.

L3 Tehdit Avcısı (Threat Hunter):

Katman 2'de yeterince veri elde edilemeyen durumlarda ve katman 2'nin gerekli önlemi alamaması halinde bu katman devreye girer. Tersine mühendislik ve zararlı yazılım analizi, tehdit istihbaratı, adli bilişim ve network konusunda iyi seviyede bilgi sahibi kişiler burada yer alır. Aynı zamanda belirli uygulamaların alt yapısında da bilgi sahibidirler. Tehditleri derinlemesine analiz ederler.

SOC Yöneticisi:

SOC yöneticisi, bir kuruluşun Güvenlik Operasyon Merkezi'ni (SOC) yöneten ve siber güvenlik stratejilerini belirleyen üst düzey bir yöneticidir. SOC ekibinin çalışmalarını koordine eder, olay yanıt süreçlerini denetler ve güvenlik politikalarının uygulanmasını sağlar. Güvenlik olaylarının etkili bir şekilde yönetilmesi için L1, L2 ve L3 analistleriyle iş birliği yapar, tehdit istihbaratını değerlendirir ve üst yönetime raporlama yapar. Ayrıca, bütçe yönetimi, yeni güvenlik teknolojilerinin entegrasyonu ve siber güvenlik farkındalığının artırılması gibi konular da SOC yöneticisinin sorumlulukları arasındadır.

SOC'da kullanılan temel araçlar

SIEM:

(Security Information and Event Management) Türkçe olarak Güvenlik Bilgileri ve Olay Yönetimi olarak çevrilir. SIEM çözümleri, bir ağda real time olarak neler olduğuna dair bütünsel bir görünüm sağlar ve BT ekiplerinin güvenlik tehditlerine karşı mücadelesinde daha proaktif olmalarını sağlar. SIEM, açılımları "Güvenlik Bilgi Yönetimi" olan SIM ve "Güvenlik Olay Yönetimi" olan SEM'in birleştirilmiş halidir.

SIEM, özünde bir veri toplayıcı, arama ve raporlama sistemidir. SIEM, ağ ortamından çok büyük miktarda veri toplar(log), bu verileri birleştirir ve insanlar tarafından erişilebilir hale getirir. Verileri kategorilere ayırır ve düzenleyerek , güvenlik kuralları yazmaya uygun hale getirir. Örneğin IBMQRadar, Splunk

IDS :

Bir çeşit saldırı önleme sistemidir. IDS'in açılımı Intrusion Detection System yani saldırı algılama sistemi olarak açıklanabilir ve IDS, tespit ettiği saldırıların engellenmesini sağlar. Ayrıca IDS bu saldırılara anlık olarak müdahale edebilir. Saldırı olarak tanımlanmış bir eyleme otomatik olarak müdahale eder ve ağda daha fazla zarara yol açmasını önler. Ağda tespit ettiği potansiyel saldırıların log kayıtlarını tutar. Ağ trafiğini düzenli olarak analiz eder. Tespit ettiği anomalileri kaydeder.

IPS:

IPS bir ağa gerçekleştirilen izinsiz girişleri tespit eden ve olası kötü amaçlı etkinlikleri izleyen ağ güvenlik aracıdır. Bu araçlar bir donanım veya yazılım olabilir. (Intrusion Prevention System) yani Saldırı Önleme Sistemi'dir. IPS, IDS'den farklı olarak tespit edilen saldırıları önleme yeteneğine de sahiptir. "IPS nedir?" sorusuna "saldırılara gerçek zamanlı olarak müdahale eden sistem" şeklinde cevap verilebilir. IPS sistemi bir saldırı tespit ettiğinde aksiyon alarak saldırıların ağa zarar vermesini engeller. Bu sayede iki sistem bir arada kullanıldığında IDS, saldırıları tespit ederken IPS ise saldırıları önleyerek kapsamlı bir koruma sağlar.

SOC Süreçler ve Prosedürler

SOC Etapları

Etap 1- Olay Sınıflandırma ve Öncelik Belirleme (Triage):

Kullanıcı aktiviteleri, sistem olayları(system events), güvenlik duvarı izin ve ret bilgilerinin yanı sıra belirli bir paterne sahip belirli olay dizileri ve kombinasyonları asıl saldırı göstergeleri arasında sayılabilir. Bu nedenle bu kritik olaylara ilişkin log verilerinin toplanması, korelasyonu ve analizi büyük önem taşımaktadır. Bu etapta her bir olayın hızlı bir şekilde sınıflandırılarak ilave araştırmalar gerektiren kritik olayların önceliklendirilip ilk sıralara alınması büyük önem arz etmektedir.

Bunun için Seviye 1 SOC Analistleri en son tespit edilen ve en yüksek kritiklik derecesine sahip olan olayları gözden geçirirler. Bu olayların daha ileri analizlere ihtiyaç duyduğunu belirlemeleri durumunda sorunu Seviye 2 Analistlere bildirirler. Bu aşamada tüm aktivitenin belgelendirilmesi önem taşımaktadır.

Atakların hassas bilgilere ve sistemlere zarar verecek bir seviyeye yükselmeden erken evrede tespit edilmesi bu etapta alınacak aksiyonları önemli kılmaktadır.

Etap 2- Önceliklendirme ve Analiz:

Önceliklendirme aşamasında iş sürekliliğini en kötü etkileyecek olaylara odaklanılması gerekir. Bunun belirlenebilmesi için hangi bilişim varlıklarının daha kritik olduğu saptanmış olmalıdır.

Bu etapta kurumunuza yapılan herhangi bir sızma girişimine işaret eden durumlar incelenip uygun aksiyon alınması önem taşımaktadır. Denetime alınması gereken saldırı göstergeleri arasında mevcut bir açıklığı istismar ederek sistemde kurulan rootkit/uzaktan erişim trojanları (RAT), iç ağdaki bir makine ile bilinen kötü bir IP adresi arasındaki ağ iletişimi gibi kritik işlemler sayılabilir.

Etap 3- İyileştirme ve Kurtarma:

Saldırının hızlıca tespit edilip müdahale edilmesi oluşacak zararın etkilerinin azaltılmasını ve benzer saldırıların gelecekte gerçekleşmesinin önlenmesini kolaylaştırmaktadır. Saldırının etkilerini azaltma, kurtarma planını uygulama veya bu saldırının bir suç olarak araştırmaya açılıp açılmayacağını kararlaştırma gibi konuları değerlendirmek için SOC ekibi yönetim ekibi ile irtibat halinde olmalı ve her şeyi dokümanlaştırmalıdır.

Saldırıyı kontrol altına almak için alınan aksiyonlar genelde şu adımları kapsar:

- Sistemlerin imaj bazında yedeğinin alınması
- Sistemleri yamalamak ve güncellemek

- Sistem erişimlerini yeniden yapılandırmak (Hesap ve parolalar)
- Ağ erişimlerini yeniden yapılandırmak (VPN, güvenlik duvarları ve erişim kontrol listeleri)
- Sunucular ve diğer varlıklar üzerindeki izleme araçlarını yapılandırmak (HIDS)
- Zafiyet taramaları yaparak yama süreçlerini ve diğer güvenlik kontrollerini denetlemek

Etap 4- Durum Tespiti ve Denetim:

Kurumların siber saldırıya maruz kalmadan önce açıklıklarının tespit edilip kapatılması ve gerekli önlemlerin alınması için periyodik zafiyet değerlendirmesi yapılması ve bulguların rapor edilmesi güvenliğin yüksek düzeyde tutulmasına katkı sağlayacaktır. SOC süreçlerine en iyi şekilde adapte olarak zafiyetlerin kapatılması işlemlerinin geciktirilmeden zamanında yapılması gerekmektedir.

SOC Önemi ve Faydaları

Günümüzde siber tehditlerin giderek artması, kurumların dijital varlıklarını koruma ihtiyacını daha da önemli hale getirmiştir. **Güvenlik Operasyon Merkezi (SOC)**, organizasyonların siber tehditlere karşı 7/24 izleme, analiz ve müdahale süreçlerini yöneten kritik bir güvenlik yapısıdır. SOC, gelişmiş tehdit tespiti ve olay yanıt mekanizmaları ile saldırıları erken aşamada durdurarak veri ihlallerini ve finansal kayıpları önler. SIEM, EDR ve XDR gibi güvenlik çözümleriyle entegre çalışarak log yönetimi, tehdit avcılığı ve adli analiz süreçlerini yürütür. Kurumların siber güvenlik stratejilerinde merkezi bir rol oynayan SOC, hem uyumluluk gereksinimlerini karşılamaya hem de siber riskleri minimize etmeye yardımcı olur.

Rapor Kazanımları

Bu rapor, Güvenlik Operasyon Merkezi (SOC) kavramını detaylı bir şekilde ele alarak, SOC'un organizasyonlar için neden kritik bir yapı olduğunu ortaya koymaktadır. Araştırma sürecinde, SOC'un temel bileşenleri, işleyişi ve katmanları hakkında kapsamlı bilgi edinilmiş, L1, L2 ve L3 analistlerinin rollerinin yanı sıra SOC yöneticisinin stratejik görevleri incelenmiştir. Ayrıca, SIEM, IDS ve IPS gibi temel güvenlik araçlarının işlevleri anlaşılmış, SOC süreçleri ve olay yönetim aşamaları değerlendirilmiştir. Bu bilgiler, siber tehditlere karşı daha etkili güvenlik önlemleri geliştirme konusunda önemli bir farkındalık sağlamıştır. Rapor sonucunda, SOC'un 7/24 izleme, tehdit avcılığı ve olay müdahale süreçlerinde oynadığı kritik rolün önemi vurgulanmış, organizasyonların siber güvenlik stratejilerini güçlendirmesi gerektiği sonucuna ulaşılmıştır.

Kaynakça

- https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir
- https://servanalkan.medium.com/letsdefend-soc-fundamentals-bdaddcbe8e24
- https://caglar-celik.com/siber-guvenlik/soc-ekibi-nedir-nasil-calisir/
- https://www.beyaz.net/tr/guvenlik/makaleler/siem_nedir_lider_siem_urunleri_nelerdir.html
- https://www.techcareer.net/blog/ips-ve-ids-nedir?
- https://www.beyaz.net/tr/guvenlik/makaleler/soc_surecler_ve_prosedurler.html
- ChatGPT