

**SOC Fundamentals**

**Hazırlayan:** Hilal ŞAHİN

**Tarih:** Şubat 2025

1. **Giriş**

Teknolojinin hızla gelişmesiyle siber güvenlik tehditleri de artmaktadır. Dijital varlıkların korunumu için etkili siber güvenlik stratejilerine ihtiyaç duyulmaktadır. Security Operations Center (SOC), güvenlik olaylarını izlemek ve bu olaylara müdahale etmek için önem arz etmektedir. SOC, bir organizasyonun siber güvenliğini yöneten, olay izleme-tespit, analiz ve müdahale aşamalarını takip etmektedir.

Bu rapor, SOC’nin temellerini, işleyişini ve önemini ele alarak siber güvenlikteki rolünü açıklayacaktır. Amacımız, SOC’nin siber güvenlikteki yerini vurgulayarak, organizasyonların etkili güvenlik çözümleri geliştirmesine katkıda bulunmaktır.

1. **Ana Bölümler**

Bu raporda, Security Operations Center (SOC) modeli detaylı bir şekilde ele alınacaktır. Siber güvenlik tehditlerine karşı organizasyonların nasıl savunma sağladığını anlamak adına SOC’nin temel işleyişi incelenecektir. SOC’nin olay izleme, tespit, analiz ve müdahale süreçleri açıklanarak, organizasyonların siber güvenlik stratejilerini nasıl güçlendirebileceği değerlendirilecektir. Ayrıca, SOC’nin sağladığı avantajlar ve kurumlar için neden kritik bir öneme sahip olduğu ele alınacaktır.

* 1. **SOC Nedir?**

SOC (Güvenlik Operasyonları Merkezi), bir sistemin güvenliğini sürekli olarak izleyen ve güvenlik olaylarını analiz eden bilgi güvenliği ekibinin bulunduğu merkez olarak adlandırılır. Teknolojik çözümleri kullanarak etkili bir süreç yönetimi gerçekleştirir. Siber güvenlik olaylarını tespit eder ve siber saldırılara karşı aksiyon alır. Ayrıca, siber güvenlik olaylarının tespit, analiz ve yanıtlama aşamalarında profesyonel bir ekip oluşturur. Bir kurum veya kuruluşun güvenliğini sürekli olarak izleyen bu ekip, ayrıntılı olarak belirlenmiş prosedürlerden oluşan iş süreçlerine sahiptir. SOC, merkezi bir komuta merkezi gibi davranır ve ağlar ile cihazların bilgi depoları da dahil olmak üzere bir kuruluşun BT altyapısını göz önüne alarak aksiyon alır.Güvenlik operasyon merkezleri, genellikle güvenlik analistleri, güvenlik mühendisleri ve güvenlik süreçlerini denetleyen yöneticilerden oluşur. Güvenlik operasyonunu denetleyen yöneticiler ekip ile koordineli bir şekilde çalışmaktadır.

* 1. **SOC Temelleri**

SOC işlemlerinin temelleri, kuruluşun sahip olduğu cihaz veya sistemlerden gönderilen log kayıtları, sistemin dijital hareket verileri ve bu verileri analiz ederek uygun sonuçlar ve tepkiler üreten SIEM ve SOAR sistemleridir.

* 1. **SOC Çalışma Adımları**
     1. **Birinci adım:**

Kurumun sahip olduğu donanım, sistem ve yazılımlar tespit edilir.

* + 1. **İkinci adım:**

Tespit edilen envanterin zafiyet değerlendirmesi yapılır.

* + 1. **Üçüncü adım:**

Sistemde gerçekleşen herhangi bir hareket belirlenir.

* + 1. **Dördüncü adım:**

IDS, IPS ve DLP gibi teknolojiler kullanılarak sızma ve sıra dışı hareketler tespit edilir.

* + 1. **Beşinci adım:**

SOAR ve SIEM sistemleri kullanılır.

* + 1. **Altıncı adım:**

Gerçekleşen saldırıya müdahale için analiz yapılır ve bu analizlerin raporu hazırlanır.

* + 1. **Yedinci adım:**

Hazırlanan raporlara göre güvenlik önlemleri alınarak sistem, önceki durumuna kıyasla daha güvenli hale getirilir.



**Şekil 1** SOC adımları

* 1. **SOC’nin Altyapısında Bulunan Sistemler**
     1. **IPS**

Ağ trafiği içerisindeki zararlı hareketlerin veya zararlı bağlantıların tespit edilerek engellenmesi için kullanılan bir güvenlik sistemidir. IPS sisteminin asıl amacı, zararlı bağlantıları ağ trafiği üzerinde tespit etmek ve engellemektir.

* + 1. **IDS**

Ağ trafiği içerisindeki zararlı hareketlerin tespiti için kullanılan sistemlere verilen bir addır. IDS’in amacı, güvenlik sistemlerinde zararlı hareketleri tanımlamak ve loglamaktır.

* + 1. **DLP**

Veri Kaybı Önleme (Data Loss/Leak Prevention) sistemidir. Network güvenlik alanında yeni sayılan ve kullanımı artan veri koruma çeşididir. Sistemde istenmeyen verilerin çıkışını önleyen veya belirli dosyaların kullanım durumlarını izler.

* + 1. **SOAR**

SOAR (Güvenlik Düzenleme Otomasyon ve Yanıt), bir kurumun güvenlik tehditleri hakkında veri toplamasına ve küçük güvenlik olaylarına insan müdahalesi olmadan yanıt vermesine olanak tanıyan sistemdir.

* + 1. **Endpoint Security**

Uç nokta güvenliği, istemci cihazlara uzaktan bağlı bilgisayar ağlarının korunmasına yönelik bir yaklaşımdır. Güvenlik tehditlerine karşı koruma sağlamak amacıyla çeşitli önlemler alır.

* + 1. **SIEM**

SIEM sistemi log toplayan, anlamlı hale getiren ve alarm üreten merkezi bir loglama ve log yönetimi bileşeni olarak tanımlanır. Yerel ağda veya farklı kaynaklarda bulunan cihaz, sistem ve uygulamalarda oluşan anormalliklere karşı önlem veya tedbir almak için alarm üretmeye yarayan sistemlere denir. Üretilen alarmlar NOC ve SOC ekipleri tarafından değerlendirilip uygulanacak aksiyonlar belirlenerek gerekli tedbirler alınır.

* 1. **SOC Modelleri**

SOC, güvenlik açığını tespit etmek için merkezi izlemenin yanında bir organizasyon yapısına zarar verebilecek güvenlik olaylarına müdahale eder. Bu yüzden model seçimi büyük önem taşır. SOC modeli belirlenirken; kurumun büyüklüğü, daha önceden yaşanmış güvenlik problemleri, faaliyet gösterdiği endüstriye, IT departman bütçesine, kurum içinde oluşan günlük trafik kriterlerine bakılarak uygun model seçilir.

* + 1. **Fusion SOC**

Internal SOC’un gelişmiş halidir. BT ekiplerinin performanslarını denetlemek için kullanılır. Asıl amacı BT ekiplerine yardım etmektir.

* + 1. **Internal SOC**

Güvenlik ve BT uzmanlarından oluşan kurum içi ekiptir. Şirket içindeki ağı belirgin bir şekilde görmeyi sağlar. SOC ekibinin içerdeki cihazları, log kaynaklarını izlemesini ve tehdit oluşturabilecek herhangi bir olaylara karşı perspektif kazanmasını sağlar.

* + 1. **Virtual SOC**

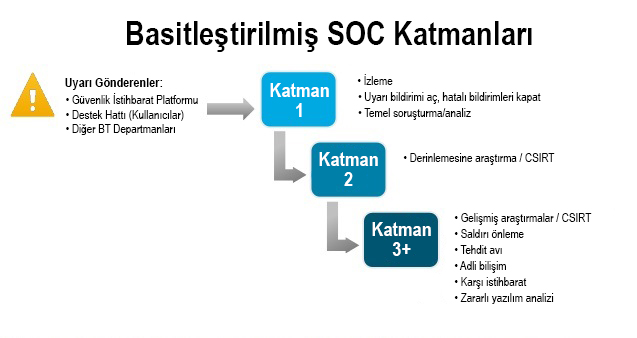
Tespit ve izleme alanında gelişmiş, yüksek teknoloji ve yetenekli elemanlara sahip SOC hizmeti veren kuruluşların yardımı ile yapılan SOC işletmesidir.

* + 1. **Hybrit SOC**

Kurumlar ile beraber eş zamanlı olarak çalışır. İzleme, alarm ve tespit etmede etkili çözümler sunar ve her iki taraftan da izlenir, çift taraflı kontrol yapmış olur.

* 1. **SOC Katmanları**

SOC ekiplerinin, saldırı anı ve genel süreci şekillendirmek için önceden belirlenmiş politikalar ve tasarladığı mimariler vardır. Kritik bir saldırı anında ele alınan her şey planlı gerçekleşir. Bir SOC ekibi 3 katmana ayrılır.



**Şekil 2** SOC katmanları

* + 1. **Katman 1: Uyarı Analisti (Alert Analyst)**

Takip edilen loğlarda izinsiz bir giriş ya da müdahale görmesi halinde ilk aşama başlatılır. Bir tehdit olduğunu Katman 2’ye bildirir. Tehdidi bildirdikten sonra Katman 2’nin kullanabileceği verileri toplamaya başlar. Bu katmanda daha çok monitoring ekibi çalışır. IPD/IDS’ler, SIEM sistemleri kullanılır. False positive durumları önlemeye çalışır.

**False positive;** logları saldırı olarak gören ancak normalde saldırı olmayan durumlara denir.

**Monitoring;** sistemde yapılan tüm hareketlerin belirli bir kurala göre loglanıp takip etmeye yarar.

* + 1. **Katman 2: Tehdit Yanıtlayıcı (Incident Responder)**

Katman 1’de gelen bildirimleri, gelen temel veriler ile beraber ele alarak saldırıdan hangi sistemlerin etkilendiğini, saldırının nasıl yapıldığını derinlemesine araştırarak çalışmalara danışmanlık yapan kişi veya sistemler burada yer alır.

* + 1. **Katman 3: Tehdit Avcısı**

Katman’2 de yeterince veri elde edilemediği durumlarda ya da katman 2’nin gerekli önlemleri almaması halinde katman 3 devreye girer. Adli bilişim, tersine mühendislik ve zararlı yazılım analizi ve network konusunda iyi seviyede bilgi sahibi kişiler burada yer alır. Tehditleri derinlemesine analiz ederler.

* 1. **Sonuç**

Günümüz dijital dünyasında, siber güvenlik tehditleri her geçen gün artmakta ve kurumların güvenlik stratejilerini sürekli olarak geliştirmesi gerekmektedir. Bu noktada, Security Operations Center (SOC), organizasyonların güvenlik olaylarını tespit etmesi, analiz etmesi ve bunlara hızlı bir şekilde müdahale etmesi açısından kritik bir rol oynamaktadır. Bu raporda, SOC’nin temel işleyişi, altyapısında bulunan sistemler, çalışma adımları, modelleri ve katmanları detaylı bir şekilde ele alınmıştır. SOC’nin sağladığı merkezi güvenlik yönetimi sayesinde, siber saldırılar etkin bir şekilde izlenmekte, tespit edilmekte ve önleyici tedbirler alınarak sistemlerin güvenliği artırılmaktadır. Kurumların ihtiyaçlarına göre farklı SOC modellerinin tercih edilmesi, güvenlik operasyonlarının etkinliğini artırarak tehditlere karşı daha güçlü bir savunma oluşturulmasını sağlamaktadır.

Sonuç olarak, SOC’nin etkin bir şekilde kullanılması, organizasyonların siber güvenlik alanında daha dayanıklı hale gelmesini sağlamakta ve potansiyel tehditlere karşı daha hazırlıklı olmalarına yardımcı olmaktadır. Güvenlik süreçlerinin sürekli iyileştirilmesi ve gelişmiş teknolojilerin entegre edilmesi, siber tehditlere karşı başarılı bir savunma mekanizması oluşturmanın temel unsurları arasında yer almaktadır.

1. **Kaynakça**

<https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir>

<https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir#:~:text=SOC%20i%C5%9Flemlerinin%20temeli%2C%20kurumun%20sahip,%C3%BCreten%20SIEM%20ve%20SOAR%20sistemleridir>.

https://caglar-celik.com/siber-guvenlik/soc-ekibi-nedir-nasil-calisir/