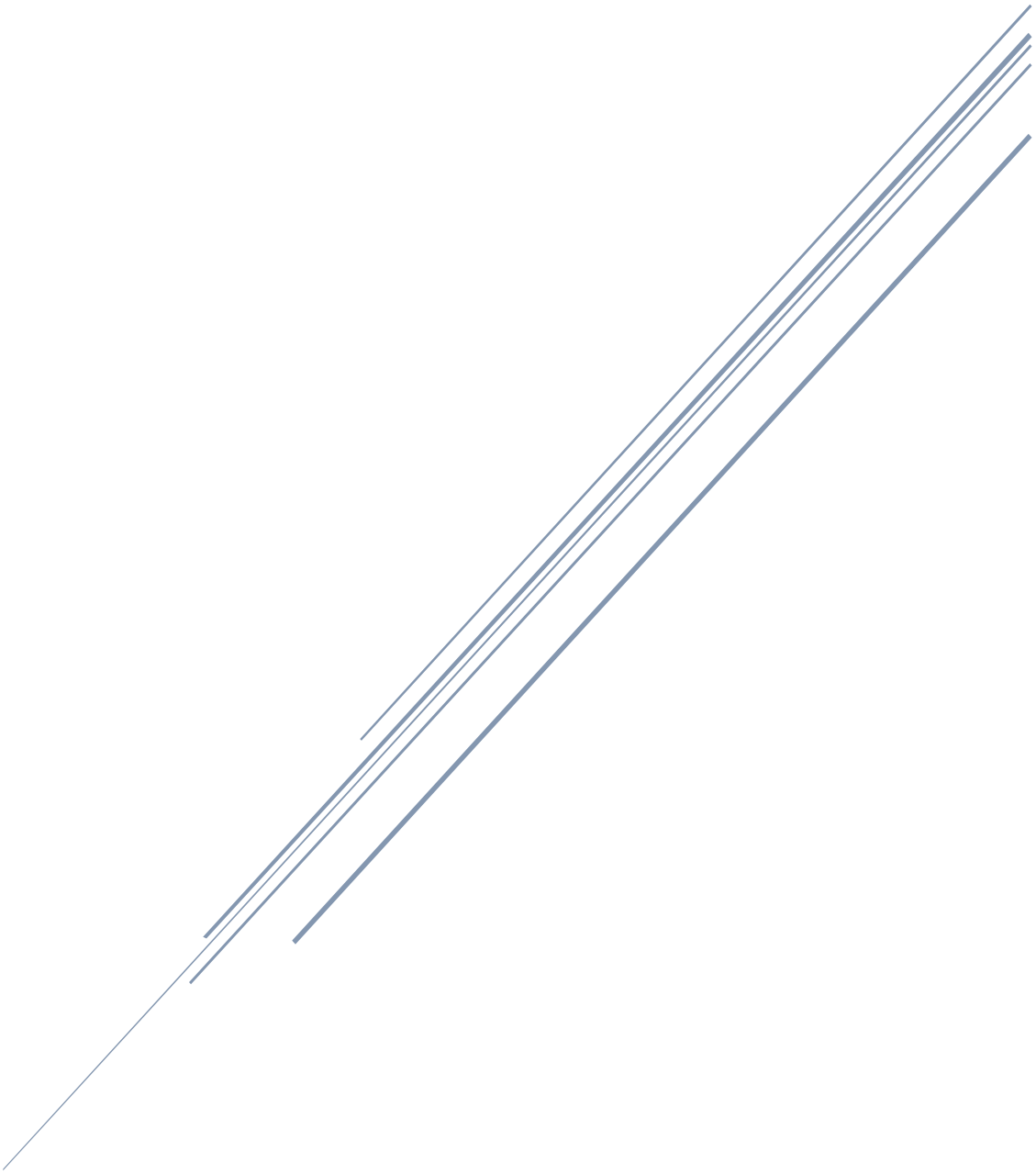
SOC Fundamentals

Hazırlayan: Sinan Kocagöz

Tarih: 26.01.2025



İçindekiler

1. Giriş **2**

2. SOC (Security Operation Center) Nedir? **3**

3. SOC' de Tespit ve Yanıt **3**

4. SOC' un Temel Bileşenleri **4**

4.1.İnsanlar **5**

4.2.Süreç **6**

4.3.Teknoloji **7**

5. SOC Modellerinin Türleri **9**

5.1.Şirket içi SOC **9**

5.2.Sanal SOC **9**

5.3.Ortak Yönetimli SOC **9**

5.4.Komuta SOC **9**

6. Sonuç **10**

Kaynakça **11**

1. Giriş

SOC ekibinin ana odağı Algılama ve Yanıtı sağlam tutmaktır. SOC ekibinin bunu başarmalarına yardımcı olan güvenlik çözümleri biçiminde bazı kaynakları mevcuttur. Bu çözümler, tüm şirketin ağını ve tüm sistemleri tek bir merkezi konumdan izlemek için entegre eder. Herhangi bir güvenlik olayını algılamak ve yanıtlamak için sürekli izleme gereklidir.

SOC, yalnızca tehditleri belirlemekle kalmaz, aynı zamanda siber güvenlikle ilgili en iyi uygulamaların uygulanmasında, organizasyonun uyumluluk gereksinimlerini karşılamasında ve olay yanıtının etkili bir şekilde gerçekleştirilmesinde de hayati bir rol oynar. Bu raporda, SOC'un temel işlevleri, yapısı ve önemine ilişkin temel bilgiler açıklanacak; bir SOC'un nasıl işlediği ve bir organizasyon için neden bu kadar önemli olduğu detaylı bir şekilde ele alınacaktır.

2. SOC (Security Operation Center) Nedir?

SOC (Security Operations Center) yani "Güvenlik Operasyonları Merkezi", uzmanlaşmış bir güvenlik ekibi tarafından işletilen özel bir tesistir. Bu ekip, bir organizasyonun ağını ve kaynaklarını sürekli olarak izlemeyi ve hasarı önlemek için şüpheli faaliyetleri tespit etmeyi amaçlar.

Ağ altyapısı, bilgisayar sunucuları, çok sayıda uç nokta, uygulamalar, web sayfaları ve diğer varlıklar; bir güvenlik tehdidi veya ihlaline işaret edebilecek olağandışı davranışları kontrol eden güvenlik operasyon merkezlerinde izlenir ve analiz edilir. SOC, olası güvenlik olaylarını doğru bir şekilde tanımlamak, analiz etmek, savunmak, araştırmak ve raporlamaktan sorumludur.

3. SOC' de Tespit ve Yanıt

a) Tespit

Güvenlik açıklarını tespit edin: Bir güvenlik açığı, bir saldırganın izin düzeyinin ötesinde şeyler yapmak için kullanabileceği bir zayıflıktır. Bir güvenlik açığı, bir sunucu veya bilgisayar gibi herhangi bir cihazın yazılımında (işletim sistemi ve programlar) keşfedilebilir. Örneğin, SOC, belirli bir yayınlanmış güvenlik açığına karşı yamalanması gereken bir dizi MS Windows bilgisayarı keşfedebilir. Kesin olarak konuşursak, güvenlik açıkları mutlaka SOC' nin sorumluluğunda değildir; ancak, düzeltilmemiş güvenlik açıkları tüm şirketin güvenlik düzeyini etkiler.

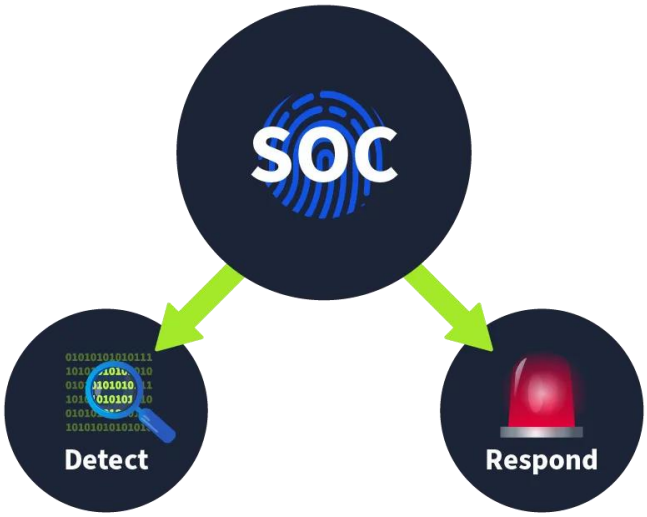
Yetkisiz etkinliği tespit edin: Bir saldırganın çalışanlardan birinin kullanıcı adını ve parolasını keşfedip bunları şirket sistemine giriş yapmak için kullandığı durumu düşünün. Bu tür yetkisiz etkinlikleri herhangi bir hasara yol açmadan önce hızlıca tespit etmek çok önemlidir. Coğrafi konum gibi birçok ipucu bunu tespit etmemize yardımcı olabilir.

Politika ihlallerini tespit edin: Bir güvenlik politikası, bir şirketi güvenlik tehditlerine karşı korumaya ve uyumluluğu sağlamaya yardımcı olmak için oluşturulmuş bir dizi kural ve prosedürdür. İhlal olarak kabul edilen şey şirketten şirkete değişir; örnekler arasında korsan medya dosyalarının indirilmesi ve gizli şirket dosyalarının güvenli olmayan bir şekilde gönderilmesi yer alır.

Saldırıları tespit edin: Saldırılar, sistemlere ve ağlara yetkisiz erişimi ifade eder. Bir senaryo, bir saldırganın web uygulamamızı başarıyla istismar etmesi olabilir. Bir diğeri ise bir kullanıcının kötü amaçlı bir siteyi ziyaret etmesi ve bilgisayarının enfekte olması olabilir.

b) Yanıt

Olay yanıtında destek: Bir olay tespit edildiğinde, buna yanıt vermek için belirli adımlar atılır. Bu yanıt, olayın etkisini en aza indirmeyi ve olayın kök neden analizini yapmayı içerir. SOC ekibi ayrıca olay yanıt ekibinin bu adımları gerçekleştirmesine yardımcı olur.



4. SOC' un Temel Bileşenleri

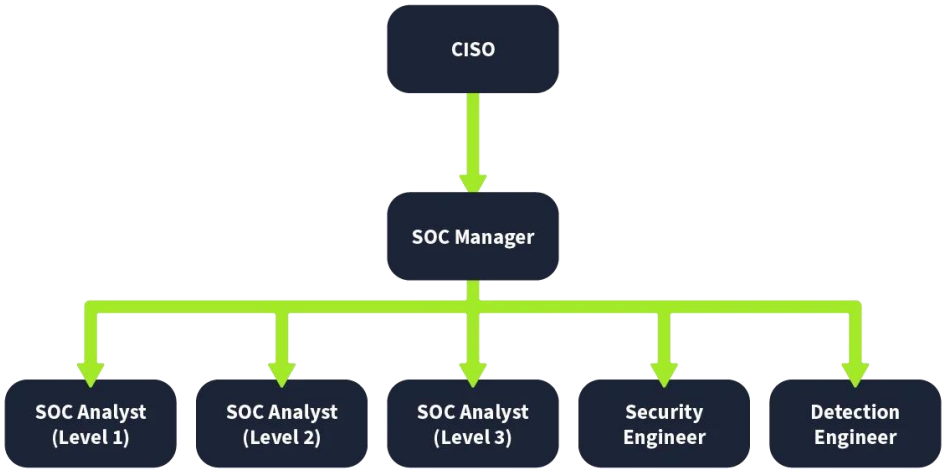
Bir SOC'nin üç ayağı vardır. Tüm bu ayaklarla bir SOC ekibi olgunlaşır ve farklı olayları etkili bir şekilde tespit edip yanıt verir. Bu ayaklar **İnsanlar**, **Süreç** ve **Teknoloji**'dir.

4.1. İnsanlar

Güvenlik görevlerinin çoğunun otomatikleştirilmesinin evrimi ne olursa olsun, bir SOC'deki İnsanlar her zaman önemli olacaktır. Bir güvenlik çözümü, bir SOC ortamında çok sayıda kırmızı bayrak üretebilir ve bu da büyük bir gürültüye neden olabilir.

Bir SOC'de, insan müdahalesi olmadan güvenlik çözümleri mevcut olduğunda, daha alakasız konulara odaklanırsınız. Güvenlik çözümünün gerçekten zararlı aktiviteleri belirlemesine ve hızlı bir yanıt sağlamasına yardımcı olan İnsanlar her zaman vardır.

İnsanlar SOC ekibi olarak bilinir. Bu ekibin aşağıdaki rolleri ve sorumlulukları vardır.



- **SOC Analisti (Seviye 1):** Alarmları inceleyerek doğruluğunu ve önceliğini belirlemek, saldırı sinyali veren alarmlar için ticket oluşturmak ve üst yöneticiye (Seviye 2) duyurmak, zafiyet taramaları yapmak ve zafiyet değerlendirme raporlarını gözden geçirmek, güvenlik izleme araçlarını yönetmek ve yapılandırmak gibi görevleri vardır. Sistem yöneticisi yekinliklerine, programlama ve güvenlik yeteneklerine sahiptir.
- **SOC Analisti (Seviye 2):** Seviye 1 analistinin oluşturduğu ticket'ları denetlemek, ortaya çıkan tehdit istihbaratlarını değerlendirerek etkilenen sistemleri ve saldırının kapsamını tanımlamak, saldırıya maruz kalabilecek sistemler üzerindeki bilgileri ileriki araştırma aşamaları için toplamak, iyileştirme ve kurtarma planını belirleyip yönetmek. Seviye 1 analistin sahip olması gereken özelliklerin yanı sıra problemin asıl kaynağına inebilme ve baskı altında çalışabilme özelliklerine sahiptir.
- **SOC Analisti (Seviye 3):** Seviye 3 Analistleri, herhangi bir tehdit göstergesini proaktif olarak arayan ve olay müdahale faaliyetlerinde destek sağlayan deneyimli profesyonellerdir. Seviye 1 ve Seviye 2 Analistleri tarafından bildirilen kritik önem tespitleri, genellikle kontrol altına alma, ortadan kaldırma ve kurtarma gibi ayrıntılı müdahaleler gerektiren güvenlik olaylarıdır. Seviye 3 analistlerinin deneyiminin işe yaradığı yer burasıdır.
- **Güvenlik Mühendisi:** Tüm analistler güvenlik çözümleri üzerinde çalışır. Bu çözümlerin dağıtımı ve yapılandırması gerekir. Güvenlik Mühendisleri,

sorunsuz çalışmasını sağlamak için bu güvenlik çözümlerini dağıtır ve yapılandırır.

- **Algılama Mühendisi:** Güvenlik kuralları, zararlı aktiviteleri algılamak için güvenlik çözümlerinin arkasında oluşturulan mantıktır. Seviye 2 ve 3 Analistleri genellikle bu kuralları oluştururken, SOC ekibi bazen bu sorumluluk için algılama mühendisi rolünü bağımsız olarak da kullanabilir.
- **SOC Yöneticisi:** SOC Yöneticisi, SOC ekibinin takip ettiği süreçleri yönetir ve destek sağlar. SOC Yöneticisi ayrıca, SOC ekibinin mevcut güvenlik duruşu ve çabaları hakkında güncellemeler sağlamak için kuruluşun CISO' suyla (Baş Bilgi Güvenliği Sorumlusu) iletişim halinde kalır.

4.2. Süreç

Her rolün kendi Süreçleri vardır, tıpkı Seviye 1 SOC Analistlerinin uyarı sınıflandırmasını gerçekleştiren ve zararlı olup olmadığını belirleyen ilk müdahaleciler olarak rolünü gördüğümüz gibi.
Bir SOC' de yer alan bazı önemli süreçleri.

- **Uyarı Triyajı:** Uyarı triyajı, SOC ekibinin temelidir. Herhangi bir uyarıya verilen ilk yanıt triyajı gerçekleştirmektir. Triyaj, belirli uyarıyı analiz etmeye odaklanır. Bu, uyarının ciddiyetini belirler ve önceliklendirmemize yardımcı olur. Uyarı triyajı, 5N'yi yanıtlamakla ilgilidir. Bu 5N nedir?

- **Raporlama:** Tespit edilen zararlı uyarıların zamanında yanıt ve çözüm için daha üst düzey analistlere iletilmesi gerekir. Bu uyarılar bilet olarak iletilir ve ilgili kişilere atanır. Rapor, kapsamlı bir analizle birlikte tüm 5N'yi ele almalı ve etkinliğin kanıtı olarak ekran görüntüleri kullanılmalıdır.
- **Olay Müdahalesi ve Adli Bilimler:** Bazen, bildirilen tespitler kritik olan son derece kötü niyetli faaliyetlere işaret eder. Bu senaryolarda, üst düzey

ekipler bir olay yanıtını başlatır. Olay yanıt süreci, Olay Yanıtlama odasında ayrıntılı olarak tartışılır. Birkaç kez, ayrıntılı bir adli tıp faaliyeti de gerçekleştirilmesi gerekir. Bu adli tıp faaliyeti, bir sistem veya ağdan gelen eserleri analiz ederek olayın temel nedenini belirlemeyi amaçlar.

4.3. Teknoloji

Doğru İnsanlar ve Süreçlere sahip olmak, tespit ve yanıt için güvenlik çözümleri olmadan asla yeterli olmazdı. SOC sütunlarındaki Teknoloji bölümü, güvenlik çözümlerine atıfta bulunur. Bu güvenlik çözümleri, SOC ekibinin tehditleri tespit etmek ve yanıtlamak için yaptığı manuel çabayı etkili bir şekilde en aza indirir.

Bir organizasyonun ağı birçok cihaz ve uygulamadan oluşur. Bir güvenlik ekibi olarak, her cihaz veya uygulamadaki tehditleri ayrı ayrı tespit etmek ve bunlara yanıt vermek önemli çaba ve kaynak gerektirir. Güvenlik çözümleri, ağda bulunan cihazların veya uygulamaların tüm bilgilerini merkezileştirir ve tespit ve yanıt yeteneklerini otomatikleştirir.

Güvenlik çözümlerinden bazılarını inceleyelim:

- **SIEM:** Güvenlik Bilgi ve Olay Yönetimi (SIEM), hemen hemen her SOC ortamında kullanılan popüler bir araçtır. SIEM, güvenlik bilgilerini ve olay yönetimini birleştiren, bir ortamda olayların gerçek zamanlı olarak kaydedilmesini içeren bir güvenlik çözümüdür. Olay kaydının nihai amacı güvenlik tehditlerini tespit etmektir.
  Şüpheli etkinliği belirlemek için mantık içeren SIEM çözümünde algılama kuralları yapılandırılır. SIEM çözümü, bunları birden fazla günlük kaynağıyla ilişkilendirdikten sonra bize algılamaları sağlar ve kurallardan herhangi biriyle eşleşme olması durumunda bizi uyarır.
  SIEM çözümlerinin birçok özelliği olmasına rağmen, SOC analistleri genellikle yalnızca uyarıları izler. Yapılandırmaları ve kural korelasyonlarını geliştirmekten sorumlu başka gruplar/kişiler vardır.
  Uyarılar filtrelerden geçen verilerden üretilir. Uyarılar önce bir SOC analisti tarafından analiz edilir. Güvenlik operasyon merkezindeki bir SOC analistinin işi burada başlar. Esasen, üretilen uyarının gerçek bir tehdit mi yoksa yanlış bir uyarı mı olduğunu belirlemeleri gerekir.
- **EDR:** Uç Nokta Algılama ve Yanıtlama (EDR), Uç Nokta Tehdit Algılama ve Yanıtlama (ETDR) olarak da bilinir, sürekli, gerçek zamanlı izleme ve uç nokta verilerinin toplanmasını, kurallara dayalı otomatik yanıt ve analiz yetenekleriyle birleştiren entegre bir uç nokta güvenlik çözümüdür. Endpoint Detection and Response (EDR), SOC ekibine cihazların aktivitelerinin ayrıntılı gerçek zamanlı ve geçmiş görünürlüğünü sağlar. Uç nokta düzeyinde çalışır ve otomatik yanıtlar gerçekleştirebilir. EDR, uç noktalar için kapsamlı algılama yeteneklerine sahiptir ve bunları ayrıntılı olarak araştırmanıza ve birkaç tıklamayla yanıt vermenize olanak tanır.

- **Güvenlik Duvarı:** Bir güvenlik duvarı yalnızca ağ güvenliği için işlev görür ve dahili ve harici ağlarınız (örneğin İnternet) arasında bir bariyer görevi görür. Gelen ve giden ağ trafiğini izler ve yetkisiz trafiği filtreler. Güvenlik duvarında ayrıca, şüpheli trafiği dahili ağa ulaşmadan önce tanımlamamıza ve engellememize yardımcı olan bazı algılama kuralları da dağıtılmıştır.
- **IDS/IPS (Saldırı Tespit/Önleme Sistemleri):** IDS (Saldırı Tespit Sistemi) ve IPS (Saldırı Önleme Sistemi), ağ trafiğini sürekli izleyen ve potansiyel güvenlik tehditlerini tespit eden sistemlerdir. IDS, şüpheli aktiviteleri tespit edip raporlarken, IPS bir adım daha ileri giderek tehditleri otomatik olarak engelleme yeteneğine sahiptir.
    - IDS özellikleri:
      Ağ trafiğini gerçek zamanlı olarak analiz eder.
      Anormal davranışları ve bilinen saldırı kalıplarını tespit eder.
      Detaylı log ve raporlama sağlar.
      Yöneticilere uyarılar gönderir.

    - IPS özellikleri:
      IDS'in tüm özelliklerine sahiptir.
      En önemlisi Tespit edilen tehditlere otomatik müdahale edebilir.
      Zararlı trafiği engelleyebilir.
      Ağ güvenlik politikalarını aktif olarak uygular.
- **SOAR (Security Orchestration, Automation and Response):** SOAR, güvenlik operasyonlarını otomatikleştiren ve orkestrasyon sağlayan gelişmiş bir çözümdür. SOAR platformları, güvenlik olaylarına yanıt sürecini otomatikleştirerek SOC ekiplerinin verimliliğini artırır.
    - SOAR'ın temel özellikleri:
      Olay yönetimi süreçlerini otomatikleştirir.
      Farklı güvenlik araçları arasında entegrasyon sağlar.
      Tekrarlayan görevleri otomatize eder.
      Tehdit istihbaratı verilerini toplar ve analiz eder.
      Olay müdahale süresini kısaltır.
      İnsan hatasını minimize eder.

Bu sistemler birbirleriyle entegre çalışarak SOC'un etkinliğini artırır. Örneğin, SIEM'den gelen bir uyarı SOAR tarafından değerlendirilip, gerekli aksiyonlar otomatik olarak alınabilir veya EDR çözümü üzerinden uç noktalarda gerekli önlemler devreye sokulabilir.

5. SOC Modellerinin Türleri

5.1. Şirket içi SOC

Bu ekip, bir organizasyon siber güvenlik ekibini kurduğunda oluşturulur. Dahili bir SOC düşünen organizasyonlar, sürekliliğini desteklemek için bir bütçeye sahip olmalıdır.

5.2. Sanal SOC

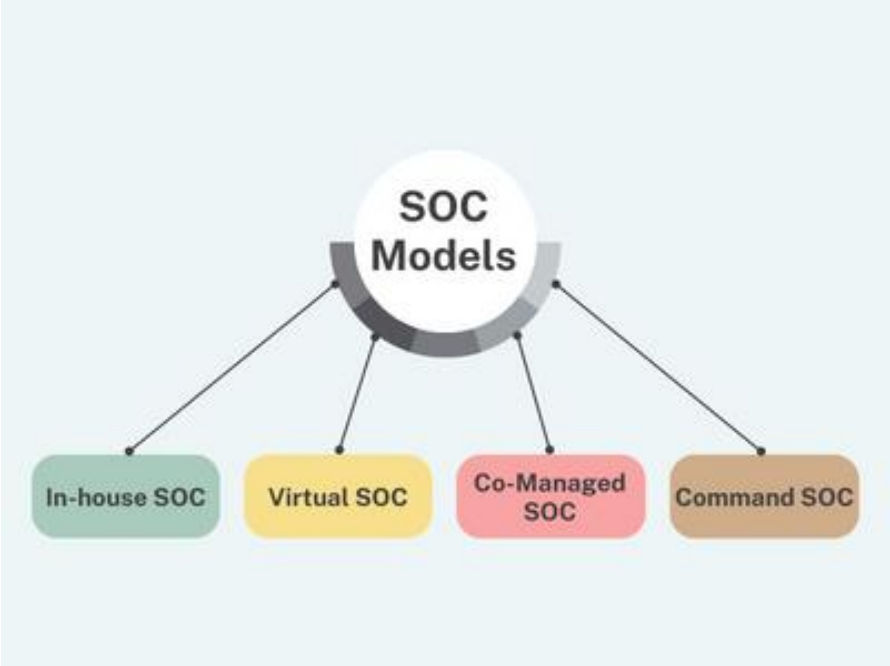
Bu tip SOC ekiplerinin kalıcı bir tesisi yoktur ve sıklıkla çeşitli lokasyonlarda uzaktan çalışırlar.

5.3. Ortak Yönetimli SOC

Ortak Yönetimli SOC, harici bir Yönetilen Güvenlik Hizmet Sağlayıcısı (MSSP) ile çalışan dahili SOC personelinden oluşur. Bu tür modelde koordinasyon anahtardır.

5.4. Komuta SOC

Bu SOC ekibi, geniş bir bölgedeki daha küçük SOC'leri denetler. Bu modeli kullanan kuruluşlar arasında büyük telekomünikasyon sağlayıcıları ve savunma ajansları yer alır.



6. Sonuç

Günümüzün sürekli gelişen ve karmaşıklaşan siber tehdit ortamında, Security Operations Center (SOC), organizasyonların siber güvenlik savunmasının vazgeçilmez bir parçası haline gelmiştir. Bu raporda detaylı olarak incelediğimiz üzere, SOC'un üç temel bileşeni olan insan, süreç ve teknoloji, birbirleriyle uyum içinde çalışarak etkin bir siber güvenlik yapısı oluşturmaktadır.

SOC'un kritik önemi, özellikle şu noktalarda belirginleşmektedir:

- **Proaktif Tehdit Yönetimi:** SOC ekipleri, sadece mevcut tehditlere yanıt vermekle kalmayıp, potansiyel tehditleri önceden tespit ederek önleyici tedbirler alabilmektedir. SIEM, EDR, IDS/IPS ve SOAR gibi gelişmiş teknolojik araçların entegre kullanımı, bu proaktif yaklaşımı mümkün kılmaktadır.
- **Sürekli İzleme ve Hızlı Müdahale:** 7/24 çalışma prensibiyle faaliyet gösteren SOC, organizasyonun dijital varlıklarını sürekli gözetim altında tutarak, herhangi bir güvenlik ihlali durumunda hızlı ve etkili müdahale imkanı sağlamaktadır. Farklı seviyelerdeki SOC analistlerinin uzmanlıkları ve iş bölümü, bu müdahalelerin profesyonel bir şekilde yönetilmesini sağlamaktadır.
- **Kurumsal Uyumluluk ve Risk Yönetimi:** SOC, organizasyonların yasal düzenlemelere ve endüstri standartlarına uyumluluğunu sağlamada önemli bir rol oynamaktadır. Aynı zamanda, sürekli risk değerlendirmesi ve yönetimi yaparak, organizasyonun güvenlik olgunluk seviyesinin artmasına katkıda bulunmaktadır.

Gelecekte SOC'ların önemi daha da artacaktır. Özellikle yapay zeka ve makine öğrenimi teknolojilerinin gelişmesiyle birlikte, tehdit tespiti ve yanıt süreçleri daha da otomatikleşecek, ancak insan faktörünün kritik önemi devam edecektir. Bu nedenle, organizasyonların SOC yapılarına yatırım yapması ve bu yapıları sürekli geliştirmesi, siber güvenlik stratejilerinin vazgeçilmez bir parçası olmalıdır.

Sonuç olarak, modern bir organizasyonun siber güvenlik stratejisinde SOC'un varlığı, artık bir tercih değil, bir zorunluluk haline gelmiştir. Sürekli değişen tehdit ortamında ayakta kalabilmek için, organizasyonların güçlü bir SOC yapısı kurmaları ve bu yapıyı sürekli olarak güncel tutmaları gerekmektedir.

Kaynakça

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

https://app.letsdefend.io/training/lesson_detail/soc-types-and-roles

https://iritt.medium.com/soc-fundamentals-cyber-security-101-defensive-security-tryhackme-walkthrough-82b1093bea59

https://tryhackme.com/r/room/socfundamentals

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

https://bulutistan.com/blog/soc/