Fundamental of The Security Operations Center (SOC)

Sebahattin Gökcen Özden

09/02/2025

İNDEX

GİRİŞ

Teknoloji sürekli değişiyor. Yani siber saldırılar da evrimleşiyor. Yeni güvenlik açıkları ve saldırı yöntemleri sürekli olarak keşfedilir. Güvenlik ihlallerinden kaynaklanan itibar ve mali etki nedeniyle güvenlik önemli bir iş kaygısı haline geliyor. Saldırılar kritik ağları ve hassas verileri hedefliyor. Kuruluşların bir güvenlik ihlaline hazırlanma, bunlarla başa çıkma ve bu ihlallerden kurtulma planları olmalıdır.

Güvenlik ihlaline hazırlanmanın en iyi yollarından biri de bunu önlemektir. Sistemler, varlıklar, veriler ve yetenekler için siber güvenlik riskinin belirlenmesi, güvenlik önlemleri ve personel eğitimi ile sistemi korumak ve siber güvenlik olayını mümkün olan en kısa sürede tespit etmek konusunda rehberlik edilmelidir.

AMAÇ

Bu çalışma Güvenlik Operasyonları Merkezi Temelleri tanıtımı ve anlaşılması amacıyla hazırlanmıştır. Siber Dünya üstünde kendi yapılarını inşa etmiş firmaların ,şirketlerin veya devletlerin Siber güvenliklerini sağlamak amacıyla oluşturulan bu özel ekibin tanımı ve üstüne tanımlanan görevleri nelerdir bunlara değinilmesi amaçlanmıştır.

1. GÜVENLİK OPERASYONLARI MERKEZİ (SOC) NEDİR ?

Güvenlik operasyon merkezi (SOC), tüm siber güvenlik teknolojilerini ve operasyonlarını birleştirerek ve koordine ederek bir organizasyonun tehdit algılama , yanıt verme ve önleme yeteneklerini iyileştirir.

Bir SOC—genellikle "sock" olarak telaffuz edilir ve bazen bir bilgi güvenliği operasyon merkezi veya ISOC olarak adlandırılır ,bir organizasyonun tüm BT altyapısını 7/24 izlemeye adanmış, şirket içi veya dış kaynaklı bir BT güvenlik uzmanları ekibidir. Görevi, güvenlik olaylarını gerçek zamanlı olarak tespit etmek, analiz etmek ve bunlara yanıt vermektir. Siber güvenlik işlevlerinin bu şekilde düzenlenmesi, SOC ekibinin organizasyonun ağları, sistemleri ve uygulamaları üzerinde uyanık kalmasını sağlar ve siber tehditlere karşı proaktif bir savunma duruşu sağlar.(3)

SOC ayrıca kuruluşun siber güvenlik teknolojilerini seçer, işletir ve bakımını yapar ve kuruluşun güvenlik duruşunu iyileştirmenin yollarını bulmak için tehdit verilerini sürekli olarak analiz eder.

SOC Modelleri

Bir kurumdaki olgunluğa ve iş akışlarının yoğunluğuna göre 4 çeşit model vardır bu alanda.

- **Internal SOC:** Genellikle 7/24 izlemeyi destekleyecek için bütçeye sahip olan büyük ölçekli firmalar tarafından kullanılır. Kurum ağını tüm detayları ile analiz etme imkanı sağlar.
- **Fusion SOC:**Internal SOC'un gelişmiş halidir. Kuruluşların büyük BT ekiplerinin performanslarını denetlemek için kullanılır. Amaçları , BT ekiplerine yardım etmektir.CIRT ve OT fonksiyonları SOC çatısı altında entegreli çalışır.
- **Virtual SOC:** Virtual SOC, izleme ve tespit etme alanında gelişmiş, yüksek teknoloji ve yetenekli elemanlara sahip SOC hizmeti veren firmaların yardımı ile yapılan SOC işletmesidir.

  Birçok kuruluş için Virtual SOC'lar, bütçe kısıtlaması ve sınırlı çalışma alanından dolayı dahili SOC kurulamadığı durumlarda önerilir. Dezavantajları ise; bu hizmeti alan firmalar, tehditin ne pozisyonda olduğunu bilemeyebilir ve daha önemli kısmı ise organizasyon yapısından dolayı SOC hizmeti veren üçüncü bir firma tarafından bazı gizli bilgiler bilinebilir. Fakat yine de bu gizli bilgiler sözleşmeler aracılığıyla güvence altına alınır. Sanal SOC modelinde izleme ve tespit alanında uzman kişiler tarafından yapılır.

  Bu model de kendi arasında ikiye ayrılabilir;

  - ***Internal Virtual SOC:*** Uzaktan çalışan yarı zamanlı güvenlik ekiplerinden oluşur. Ekip üyeleri bir uyarı tehditi aldıklarında tepki vermekle yükümlüdürler.
  - ***Outsourced Virtual SOC:*** Uzaktan çalışan güvenlik ekipleridir. Doğrudan kuruluş için çalışmak yerine dış kaynaklı üçüncü taraf hizmeti sunar. Kendi bünyesinde SOC ekibi görevlisi olmayan kurumlara güvenlik hizmetleri sunar.

- **Hybrid SOC:** Her iki modelin birlikte kullanılmasıyla oluşur. Kurumun kendi personelleri, dışarıdan SOC hizmeti aldıkları firmadaki uzmanlar ile beraber çalışarak en güvenli çözümü sunarlar.

Bir SOC ekibi ise 3 temel yapı taşından oluşur ve bu bileşenlerin uyumlu çalışmasıyla hayata geçer:

1.İnsan:

SOC'de görev yapan analistler, mühendisler, yöneticiler ve diğer uzmanlar; güvenlik olaylarının tespitinden müdahalesine kadar tüm süreçlerde aktif rol alırlar. Her seviyede uzmanlık, olayların doğru sınıflandırılması ve müdahale sürecinin etkin yürütülmesi için kritik öneme sahiptir.

2.Süreçler:

Olay yönetim süreçleri, izleme, tespit, analiz, müdahale ve iyileştirme gibi adımları içerir. Bu süreçlerin tanımlanması ve sürekli iyileştirilmesi, SOC'un başarısının temelidir.

3.Teknoloji:

SOC'un verimli çalışması için SIEM, IDS/IPS, EDR, Firewall, Threat Intelligence, Sandbox ve DLP gibi çeşitli teknolojik araçların entegrasyonu gereklidir. Bu araçlar, büyük miktarda verinin gerçek zamanlı olarak işlenmesini, korelasyon kurallarının uygulanmasını ve güvenlik olaylarının otomatik olarak raporlanmasını sağlar.

1.1GÖREVLERİ

Siber güvenlik operasyon merkezleri; ağlardaki, sunuculardaki, bitiş noktalarındaki, veri tabanlarındaki, uygulamalardaki, web sitelerindeki ve diğer sistemlerdeki etkinlikleri izler ve analiz eder, bir güvenlik olayı veya tavizinin göstergesi olabilecek anormal etkinlikleri tarar. Olası güvenlik sorunlarının doğru bir şekilde tanımlanması, analiz edilmesi, araştırılması ve rapor edilmesi siber güvenlik operasyon merkezinin sorumluluğundadır. Daha detaylı bakarsak;

- İzlenmesi gereken önemli bilişim sistemlerine ait logların analiz araçlarına gönderilmesini sağlayacak sıkıntısız bir altyapı kurmak ve bunun için güvenlik izleme cihazlarını ve araçlarını çok iyi bir şekilde yapılandırmak ve öğrenmek.
- SOC kurallarını düzenlemek ve gözden geçirmek, saldırı bildirimlerini araştırmak, alarmları araştırmak, alarmların kritiklik derecesini belirleyerek önemine göre sıralamak, saldırı kaynaklarını belirlemek gibi zararlı aktiviteleri tespit için gereken önemli süreçleri güvenlik izleme cihazlarının yardımıyla en iyi şekilde yönetmek.
- Olay adımlarını planlamak ve ona göre davranmak.
- Yapılan saldırılarla ilgili inceleme ve çalışmalar yapmak ve kurtarmak.
- Adli analiz süreçlerini yapmak.

- Yapılan saldırılardan yada olaylardan ders çıkarıp çalışmalar yapmak ve daha sonraki saldırılar için güvenlik almak.
- İzleme , tespit sistemlerinden çıkan sonuçlara göre önlem almak ve politikaları güncellemek.
- Ekipteki tüm üyeler, siber güvenlik operasyon merkezinin misyonu ve stratejisi hakkında farkındalığa sahip olmalıdır. Bu nedenle, etkili bir liderlik çok önemlidir. Siber güvenlik operasyon merkezinin yöneticisi, ekibi kurabilecek, üyeleri motive edebilecek bir kişi olmalıdır. Yapının 7 gün 24 saat çalışmak zorunda olması kolay bir iş değildir ve bu nedenle stres olası bir risk faktörü olacaktır.

2. SOC TAKIMININ ANAHTAR ÜYELERİ

Genel olarak, bir SOC ekibindeki başlıca roller şunlardır:

SOC yöneticisi: SOC yöneticisi ekibi yönetir, tüm güvenlik operasyonlarını denetler ve kuruluşun CISO'suna (Baş Bilgi Güvenliği Sorumlusu) rapor verir.
Güvenlik mühendisleri: Bu kişiler kuruluşun güvenlik mimarisini oluşturur ve yönetir. Bu işin büyük kısmı güvenlik araçlarını ve teknolojilerini değerlendirmeyi, test etmeyi, önermeyi, uygulamayı ve sürdürmeyi içerir. Güvenlik mühendisleri ayrıca kuruluşun güvenlik mimarisinin uygulama geliştirme döngülerine dahil edildiğinden emin olmak için geliştirme veya DevOps/ DevSecOps ekipleriyle birlikte çalışır.
Güvenlik analistleri: Güvenlik araştırmacıları veya olay müdahalecileri olarak da adlandırılan güvenlik analistleri, esasen siber güvenlik tehditlerine veya olaylarına ilk müdahale edenlerdir. Analistler tehditleri tespit eder, araştırır ve öncelik sırasına koyar; ardından etkilenen ana bilgisayarları, uç noktaları ve kullanıcıları belirler. Daha sonra tehdidi veya olayı azaltmak ve sınırlamak için uygun eylemlerde bulunurlar.)Bazı kuruluşlarda, araştırmacılar ve olay müdahalecileri sırasıyla 1. Kademe ve 2. Kademe analistler olarak sınıflandırılan ayrı rollerdir.)
Tehdit avcıları: Uzman güvenlik analistleri veya SOC analistleri olarak da adlandırılan tehdit avcıları, gelişmiş tehditleri tespit etme ve engelleme konusunda uzmanlaşmıştır; otomatik savunmaları aşmayı başaran yeni tehditleri veya tehdit türlerini avlarlar .
SOC ekibi, organizasyonun büyüklüğüne veya endüstri türüne bağlı olarak diğer uzmanları içerebilir. Daha büyük şirketler, olay müdahalesini iletmek ve koordine etmekten sorumlu bir Olay Müdahale Müdürü içerebilir. Ve bazı SOC'ler, bir siber güvenlik olayında hasar gören veya tehlikeye giren cihazlardan veri (ipuçları) alma konusunda uzmanlaşmış adli araştırmacıları içerir.

2.1.SOC'de iş Rolleri:

Genellikle SOC 'de iş rolleri gerektirdiği uzmanlık ve sorumluluklara göre kategorilendirilir.

- ***Alert Analyst (Tier 1):*** Analistler gelen uyarıları izler, gerçek bir olayın meydana geldiğini doğruladıktan sonra gerektiğinde Ticketleri Tier 2 'ye iletmekten sorumludurlar.

  Görev tanımları kısaca:
  - Gelen alarmları ve uyarıları sürekli izler.
  - Alarmın Doğruluğunu (false positive / true positive) belirler.
  - Düşük riskli olayları değerlendirir ve eğer karmaşıklık artarsa, vakayı Tier 2 'ye eskale eder.

Özellik: Hızlı yanıt verebilme, temel analiz yetkinliği ve log verilerini yorumlama becerisi önemlidir

- ***Incident Responser (Tier 2):*** Meydana gelen olayların derinlemesine araştırılmasından ve düzeltilmesini veya alınacak önlemlerden sorumludur.

  Görev tanımı:
  - L1'den gelen vakaları detaylı inceleyerek kök neden analizini yapar.
  - Tehdit istihbaratı eve ek log analizi yaparak saldırının kapsamını belirler.
  - Gerekirse müdahale prosedürlerini başlatır(firewall veya EDR ile engelleme).

  Özellik: Daha derinlemesine teknik bilgi, baskı altında çalışabilme ve olay yanıtı süreçlerini yönetme becerisi öne çıkar.
- ***Threat Hunter (Tier 3):*** Ağ, endpoint, tehdit istihbaratı ve malware reverse engineering konularında uzman beceriye sahiptir. Sistemdeki etkilerini ve nasıl yok edileceğini belirlemek amacıyla malware süreçlerini izleme konusunda uzmandırlar. Ayrıca, potansiyel tehditleri avlamak ve tehdit algılama araçlarını uygulamakla da yakından ilgilenirler. Tehdit avcıları, ağda bulunan ancak henüz tespit edilmemiş siber tehditleri arar.

  Görev tanımı:
  - Karmaşık saldırı senaryolarını ve gelişmiş tehditleri analiz eder.
  - Adli analiz ,tersine mühendislik ve threat hunting faaliyetlerini yönetir.
  - Gelişmiş tehditlere karşı stratejik savunma çözümleri geliştirir.

  Özellik: En ileri düzey uzmanlık, analitik düşünce ve detaylı teknik inceleme becerileri.

- ***SOC Manager :*** SOC ekibinin tüm kaynaklarını yönetir ve daha büyük kuruluş veya müşteriler için iletişim noktası konumundadır.

  Görev tanımı:
  - Tüm SOC ekibinin operasyonlarını denetler.
  - Eğitim, kaynak yönetimi ve süreçlerin sürekliliğini sağlar
  - Olay raporlarını değerlendirir ve stratejik güvenlik planlarını geliştirir.

3. Olay Yönetim Süreçleri

SOC içerisinde olay yönetimi, genellikle şu aşamalardan oluşur:

1. **Tespit (Detection):**
   Tüm log ve veri akışları SIEM gibi araçlarla toplanır. Anormallikler, imza tabanlı veya davranış tabanlı analiz yöntemleriyle tespit edilir.
2. **Analiz (Analysis):**
   Tespit edilen uyarılar, L1 analistleri tarafından önceliklendirilir ve doğrulanır. Gerekli durumlarda vakalar L2'ye eskale edilerek detaylı analiz yapılır.

3. **Müdahale (Response):**
   Olayın etkisini minimize etmek için, saldırının izole edilmesi, engellenmesi veya sistemlerin kurtarılması gibi adımlar atılır.
4. **İyileştirme (Recovery & Lessons Learned):**
   Olay sonrası raporlamalar yapılır, süreçler güncellenir ve gelecekteki saldırılara karşı savunma stratejileri geliştirilir.

Bu döngü, SOC'un sürekli olarak siber tehditlere karşı güncel ve hazırlıklı kalmasını sağlar.(5)

4.SOC'UN ALTYAPISINDA BULUNAN SİSTEMLER

1)IDS :

Ağ trafiğiniz içerisindeki zararlı hareketleri veya zararlı bağlantıların tespiti için kullanılan sistemlere verilen addır. Intrusion Detection Systems kelimelerinin kısaltması olarak kullanılır. IDS güvenlik sistemlerinin amacı zararlı hareketi tanımlama ve loglama yapmaktır. Yani kısaca gelen saldırıyı algılamak ve loglamak için kullanılır.

2)IPS :

Ağ trafiğiniz içerisindeki zararlı hareketleri veya zararlı bağlantıların tespiti ile birlikte önlenmesi için kullanılan güvenlik sistemleridir. Intrusion Prevention Systems kelimelerinin kısaltması olarak kullanılır. IPS sistemlerinin amacı zararlı bağlantıların veya hareketlerin ağ trafiği üzerinde durdurulması ve önlenmesidir. Yani kısaca algılanan saldırıyı önlemek için kullanılır.

3)DLP :

Data Loss/Leak Prevention Veri Kaybı/Sızıntısı Önleme sistemidir. Network güvenlik alanında nispeten yeni sayılan ve gittikçe kullanımı artan bir veri koruma çeşididir. DLP yazılımları ile sisteminizden istenmeyen verinin çıkışını önleyebilir ya da belirlediğiniz dosyaların kullanım durumlarını izleyebilirsiniz.

4)ENDPOINT SECURITY :

Uç nokta güvenliği , istemci cihazlara uzaktan köprülenmiş bilgisayar ağlarının korunmasına yönelik bir yaklaşımdır . Laptoplar , tabletler , cep telefonları ,IOT vb. şeylerin kurumsal ağlara cihazlar ve diğer kablosuz cihazlar güvenlik tehditlerine karşı saldırı yolları oluşturur. Uç nokta güvenliği, bu tür cihazların standartlara belirli bir uyumluluk düzeyini takip etmesini sağlamaya çalışır .
Uç nokta güvenlik alanı, son birkaç yılda sınırlı antivirüs yazılımından uzaklaşarak daha gelişmiş, kapsamlı bir savunmaya dönüşmüştür. Bu, yeni nesil antivirüs, tehdit algılama, araştırma ve yanıt, cihaz yönetimi, veri sızıntısı koruması (DLP) ve gelişen tehditlerle yüzleşmek için diğer hususları içerir.

5)SIEM :

SIEM sistemlerini, log üreten değil logları toplayan, anlamlandıran ve alarm üreten merkezi bir loglama ve log yönetimi bileşeni olarak tanımlayabiliriz. Bu amaç için üretilmiş ürünlere Security Information Event Management (SIEM) denilmektedir.
SIEM, yerel ağda veya farklı kaynaklarda bulunan cihaz, sistem ve uygulamalarda, oluşan anormalliklerden haberdar olmak ve bu anormalliklere karşı önlem veya tedbir almak için alarm üretmeye yarayan sistemler bütünüdür. Üretilen alarmlar NOC ve SOC ekipleri tarafından değerlendirilip uygulanacak aksiyonlar belirlenerek gerekli tedbirler alınmaktadır.

6)SOAR:

SOAR (Güvenlik Düzenleme Otomasyon ve Yanıt), bir kuruluşun güvenlik tehditleri hakkında veri toplamasına ve küçük güvenlik olaylarına insan yardımı olmadan yanıt vermesine olanak sağlayan sistemdir.
SIEM olayların analizini yapıp sonuçları söylerken SOAR olayları anlayıp karşı hamle yapmaktadır. Sürekli devam eden tehditlere karşı ağda toplanan verilerin artması sonucunda elde edilen verilerin düzenlenmesi ve raporlanması zorlaşmaktadır. SOAR veri çeşitliliğinin ve miktarının artması karşısında tehdit müdahale yeteneklerinin artmasını sağlamakta ve iş süreçlerini kolaylaştırmaktadır. On kişiden fazla elemanın çalıştığı NOC ve SOC ekiplerinin SIEM yanında SOAR da kullanma gerekliliği de ortaya çıkmaktadır.
SOAR için önemli iki şey tanım otomasyon ve orkestrasyondur. Elle yapılacak işlemlerin otomasyon ortamında hızlıca ve hatasız yapılması ve farklı güvenlik uygulama ve servislerinin birlikte çalıştırılması ve birbirine entegre edilmesidir.
Daha hızlı bilgi edinme ve cevap vermek için SOAR çok önemlidir. SOAR şüpheli hareketlerin algılanmasını kolaylaştırmakta ve cevap verme süresini azaltmaktadır. Veri kaynaklarından gelen bilgileri birleştirerek işlemlerin verimliliği arttırmakta ve cevapları otomatikleştirmektedir.

7)GRC SİSTEMLERİ:

Kurumsal risklerin sistematik bir şekilde yönetilmesini sağlar. Risk göstergeleri ve erken uyarı sistemiyle saldırılara hemen müdahale etmemize olanak sağlar.

8)UTM:

Yeni nesil güvenlik duvarıdır. Günümüzdeki güvenlik duvarları da sadece port kapatmak amaçlı kullanılmıyor. Yeni nesil güvenlik duvarları da UTM (Unified Threat Management) güvenlik duvarı, antivirüs, antispam, IDS/IPS, VPN, router gibi özellikleri olan tümleşik cihazlardır. Bilinen UTM cihaz markaları ; Palo Alto, Checkpoint, Cisco ASA, Fortinet, Labris, Juniper, NetSafe-Unity, Netscreen ve Symantec serisidir. Bu cihazlar üzerinde port , protokol bazısında kısıtlama yapabilir. Web filtrelemesi(terör, şiddet, silah gibi kategorilerine göre yasaklama) yapabilir. Dosya indirme gibi işlemleri durdurabilir.

9)NGFW:

Yeni nesil güvenlik duvarı, geleneksel güvenlik duvarını, sıralı derin paket denetimi kullanan bir uygulama güvenlik duvarı, saldırı önleme sistemi gibi diğer ağ cihazı filtreleme işlevleriyle birleştiren üçüncü nesil güvenlik duvarı teknolojisinin bir parçasıdır.

5.SOC'UN KURUMLAR İÇİN FAYDALARI VE ÖNEMİ

Kurumların yönetilmesi gün geçtikçe daha da zorlaşmaktadır. Kurumlara yapılan hizmet dışı bırakma, malware gibi saldırıları her gün yeni boyut kazanarak artmaktadır. Bu da kurumların ve müşterilerinin için kritik sorundur ve risklidir. Hatta kurumun adı için bu çok kötü bir şeydir. Kurumların itibarını düşürür, bunun sonucunda da kurumların kapanmasına veya paylarının küçülmesine sebep olabilir.

Kurumların güvenli kalması için sürekli gözlenmeli ve olası saldırı anında müdahale edilmesi gerekmektedir bu yüzden SOC kavramı ortaya çıkmıştır. SOC kurumlar için kritik derecede önemlidir. Artık her kurumda da bulunuyorlar.

Gerçekten başarılı siber güvenlik operasyon merkezleri, faydalı ve etkili olmak için güvenlik otomasyonundan yararlanır. Kurumlar, son derece yetenekli güvenlik analistleri ile güvenlik otomasyonunu birleştirerek güvenlik önlemlerini geliştirir. Veri ihlallerine ve siber saldırılara karşı daha iyi savunma sağlamak için analitik gücünü artırır. Bunu gerçekleştirecek kurum içi uzmanlığa ve kaynaklara sahip olmayan birçok kurumlar, siber güvenlik operasyon merkezi hizmetleri sunan kurumlara başvururlar.

SOC kurumlar için faydası çoktur. SOC ekibine sahip olmanın en önemli yararı, sürekli izleme ve veri etkinliğinin analizi yoluyla güvenlik olaylarının tespitinin iyileştirilmesidir. Kurumun ağları, uç nokta cihazları, sunucuları ve veritabanları ile veri etkinliği vb. şeyleri analiz edilerek; SOC ekipleri, güvenlik olaylarının zamanında tespit edilmesi ve aksiyon alınmasını sağlamak için kritik öneme sahiptir. SOC tarafından sağlanan sürekli denetim sayesinde kurumlar; kaynak, zaman ve saldırı türü fark etmeksizin olaylara ve saldırılara karşı savunma yapma avantajı sağlarlar.

SOC'lar siber tehdit istihbaratı ekibi, hızlı analiz ve SOC teknolojilerini kullanır. Saldırıları bu yüzden hızlı bir şekilde tespit eder ve müdahale eder. Saldırılardan verilen maddi manevi kayıpların önüne geçer. SOC kurmak masraflı olsa da uzun vadede geçici güvenlik önlemlerinin maliyetlerini ve güvenlik ihlallerin yol açtığı hasarı engeller. Saldırılara karşı soruşturmaların karmaşıklığını çözer.

REFERANSLAR:

1: https://www.beyaz.net/tr/guvenlik/makaleler/soc_ekibi_ozellikleri.html
2: ConnectWise
3: IBM
4: https://alpbatursahin.medium.com/soc-1-soc-nedir-32d28d7f0383
5: https://learn.microsoft.com/tr-tr/azure/sentinel/migration-security-operations-center-processes