SOC

GökBörüTİM

SOC Nedir, Nasıl Çalışır?

Güvenlik operasyonları merkezi, İngilizce **Security Operations Center** (**SOC**) bir kuruluşun güvenliğinin takibi, analizi ve güvenliğin sağlanması için oluşturulan yapıya denir. Temelde amaç kuruma yapılan saldırıların loglanması ve analiz edilmesi olmakla beraber, kurumun bulunduğu sektörü hedef alan veya global alanda yeni çıkan önemli saldırı vektörlerini de takip eder ve bu saldırılardan zarar görmemek için önlemler alır. Yani SOC ekibi yalnızca kendi kurumunu değil, sektördeki diğer kurumları, globali ve ülkesini hedef alan saldırıları da sürekli olarak takip ederse başarılı olur.

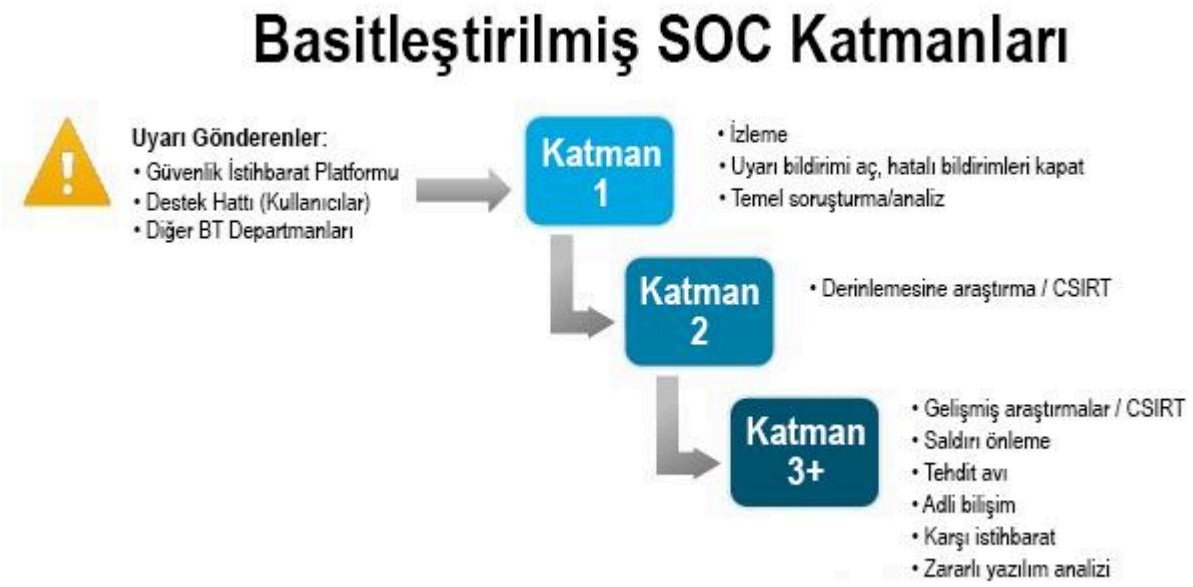
- **İzleme**
- **Tespit**
- **Analiz**
- **Müdahale**
- **Raporlama**

Ayrıca bazı ekiplere verilen ünvanlar :

- **CSIRT**: Bilgisayar Güvenliği Olay Müdahale Ekibi
- **CIRT**: Bilgisayar Olayları Müdahale Ekibi
- **CIRC**: Bilgisayar Olayları Müdahale Merkezi
- **CSIRC**: Bilgisayar Güvenliği Olay Müdahale Merkezi
- **CSOC**: Siber Güvenlik Operasyonları Merkezi(SOC, yalnızca siberi değil tüm güvenlik tehditlerini ele alır.)
- **CERT**: Bilgisayar Acil Durum Cevap Ekibi

SOC ekiplerinin, saldırı anı ve genel süreci şekillendirmek için önceden belirlediği politikalar (Security Operations Policy – SOP) ve tasarladığı mimariler vardır. Böylece kritik bir saldırı ele

alınırken dahi her şey planlı gerçekleşir. Bir SOC ekibi üç katmana ayrılır. Zaman zaman katman 4 eklenebilir.



Katman 1: 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 sahibi olunması gerekir.

> **False positive**: Bire bir çevirisi hatalı pozitif diyebiliriz. Loglarda saldırı olarak görünen ancak normalde saldırı olmayan durumlara denir.
> **Monitoring**: Genel anlamda sistemde yapılan tüm hareketlerin belirli bir kurala göre kaydedilip/loglanıp takip etmemizi sağlayan sistemler.
> **IDS**: Intrusion Detection Systems, kuruma yapılan saldırıların tespit edilmesi için oluşturulan sistemler.
> **IPS**: Intrusion Prevention System, IDS'ten farklı olarak tespit ettiği saldırı girişimini önler. İki sistem de genelde log tabanlı çalışır.
> **SIEM**: Monitoringten farklı olarak belirlenen politikalara göre yazılan kurallarla, logları filtreleyerek olası saldırıları tespit eden sistemler. (Security Informatin and Event Management)

Katman 2: Tehdit Yanıtlayıcı (Incident Responder)

Katman 1'den gelen bildirimleri, gelen temel verilerle beraber ele alarak saldırıdan hangi sistemlerin etkilendiğini, kimin, neden ve nasıl yaptığını derinlemesine araştırarak iyileştirme çalışmalarına danışmanlık yapan kişi veya sistemler burada yer alır.
İyi düzeyde adli bilişim, tehdit istihbaratı, log incelemeleri ve temel zararlı yazılım değerlendirmelerini yapan kaynaklar burada yer alır.

Katman 3: Tehdit Avcısı

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

Tüm bu sistem ve personelin yönetiminden, stratejik planlar ve güvenlik operasyonları politikasından sorumlu olan yöneticidir.
SOC'un zorlandığı ve olayları cevaplamakta geciktiği bazı durumlar olabilir. Bunlara sebep olan meseleler ise:

- SOC, masum hareketleri/kullanıcıları engellemediğinden emin olmak ister. False positive durumundan bahsetmiştik.
- Bazen saldırıya müdahale etmek, saldırının kendisinden daha fazla zarara sebep olabilir. Bazı durumlarda kurumun itibarını daha olumsuz etkileyebilir veya müdahale etmek, daha büyük maddi giderler gerektirebilir.
- Saldırganın ne yapmak istediğini, kim olduğunu ve kapsamını anlamak için saldırı evresinin bir noktaya kadar devam etmesine izin verilebilir. Haliyle riskli bir seçenektir.

Loglama Zamanı!

Toplanan loglarda olmazsa olmaz veri zaman damgasıdır. Kaldı ki hukuken de zaman verisi bulunmayan logların geçerliliği olmuyor. Diğer yandan saldırgan IP adresi, saldırıya uğrayan makinenin ve ana makinenin adı ve IP adresi log kayıtlarında yer almalıdır. Aynı zamanda saldırının analizi için gönderilen paketin veya isteğin de takip edilmesi gerekir. Logları toplayabileceğimiz önemli kaynaklar:

- **Network paketleri**

- **Apache, IIS gibi web sunucuları**
- **Web sitelerine yapılan istekler**
- **FTP, SSH ve RDP gibi servislere gelen talepler**
- **Kurumdaki bilgisayarlar ve ağa bağlı diğer cihazlar**
- **İşletim sistemleri**
- **Veri tabanları**
- **Mail sunucuları**

SOC Türleri

Güvenlik Ekibi

Tehdit durumlarını tespit etme ve karşılama politikaları yoktur. Bir saldırı sonrasında soruna çözüm bulur, sistemi yeniden kurar ve sornasında saldırıyı analiz eder. Genelde bir monitoring ve saldırıları ele alma politikaları/süreçleri bulunmaz.

Sanal SOC

Daimi bir SOC ekibi bulunur fakat temel amacı SOC olmayan kişilerden oluşur. Genellikle BT ve güvenlik alanında çalışan personellerden oluşur. Personeller rutin işlerinin yanında aynı zamanda SOC işlemlerini gerçekleştirir. Bir kişi veya küçük bir grup, güvenlik operasyonlarını koordine eder.

Merkezi SOC / Adanmış SOC

Yalnızca bu amaç için çalışan personelleri, bu amaç için ayrılan bütçesi, tesisi ve kaynakları bulunur.

Dağıtık SOC

SOC faaliyetlerini kurumun bu amaç için bulundurduğu personellerin yanı sıra bu alanda uzman, anlaşma yapılan başka firmalar da uzaktan yürütür.

Sanal ve Merkezi SOC

Temelde SOC için ana bir ekip bulunmakla beraber kurumun belirli departmanlarında esas işi SOC olmayan BT ve güvenlik elemanlarını da bünyesinde bulundurur. Ana SOC ekibi ve departmanlardaki elemanlar arasında senkron bir çalışma söz konusudur. Hiyerarşik bir yapı gibi düşünebilirsiniz.

SOC Olgunluk Modeli

Her kurum aynı güvenlik önlemlerine ihtiyaç duymaz. Kurumun büyüklüğü veya yaptığı işin kritikliğine göre farklı güvenlik önlemleri gerekir. Bütçeleri, personelleri, bilginin kritikliği, ağdaki cihazlarının sayısı, envanter durumu, fiziksel alanın genişliği gibi kriterler farklı farklı önlemler gerektirir. Bu durumda eksikliklerin tespit edilmesi ve düzeltilmesi için SOC olgunluk modeli kullanılır.

1.Seviye: Başlangıç

Halihazırda bir SOC ekibi bulunur fakat gerek teknoloji gerek personel sayısı ve teknik beceri yeterliliği noktasında yetersizdir. Güvenlik ürünleri eskidir ve önlemler yetersizdir. Bir tehdit anında belirli bir politikaları yoktur. Durum vahim anlayacağınız.

2.Seviye: Yönetilen

Temel güvenlik ürünlerini temin etmişlerdir ancak yeterli seviyede kullanamıyorlardır. SOC için mevcut personelleri bulunur fakat yaptıkları tek iş güvenlik değildir. Aynı zamanda BT işlerini gerçekleştirir. Yazılı olmayan politikaları bulunur ve bunlar kısmen uygulanır.

3.Seviye: Tanımlı

Söz konusu güvenlik araçları temin edilmiş ve doğru şekilde kullanılıyordur. Önceden belirlenen yazılı politikaları tehdit anında doğru şekilde uygulanıyordur. Personellerin görevleri önceden belirlenmiştir. Güvenlik elemanları aynı zamanda BT elemanı olabilir fakat güvenlik alanında eğitimli ve yetkindir.

4.Seviye: Ölçülebilen

Gerekli güvenlik araçları temin edilmiştir, bakımı düzenli olarak yapılır ve ürünler arasındaki entegre sağlanır. Tüm süreç politikası oluşturulmuş ve düzgün biçimde uygulanır. Kontrol listesi ve iş akışı planlanmıştır. Perosneller BT elemanlarından ayrı olarak bu iş için ayrılmıştır, herkesin rolü detaylı olarak planlanmıştır ve aksilik olması durumunda yedek kişi bellidir.

5.Seviye: İyileştirici

Tüm güvenlik ürünleri temin edilmiş ve entegre şekilde çalışır. Etkin biçimde çalışıp çalışmadığı süreki değerlendirilir. Teknolojiler ve süreç arasında entegrasyon sağlanır.

Oluşturulan süreç politikaları ve personeller de sürekli olarak değerlendirilir. Personeller kendi içerisinde iyi organize şekilde çalışır ve aksi durumlarda sürekli yedekleri bulunur.

Bir Sonraki Yazımızda Görüşmek Üzere...