SECURITY OPERATION CENTER

SİBER GÜVENLİK OPERASYON MERKEZİ

07.02.2025

MEHMET MERMER

ALTAY SİBER VATAN

İÇİNDEKİLER

GİRİŞ

Günümüzde siber tehditler giderek karmaşıklaşmakta ve kurumların dijital varlıklarını koruma gereksinimi artmaktadır. Artan dijitalleşme ile birlikte, siber saldırıların hedefi olan organizasyonların, güvenlik tehditlerini hızlı ve etkili bir şekilde tespit edip müdahale edebilmesi büyük bir gereklilik haline gelmiştir. Bu kapsamda, şirketler ve kurumlar, tehditleri algılamak, analiz etmek ve bu tehditlere karşı zamanında müdahale edebilmek için Siber Güvenlik Operasyon Merkezleri (SOC - Security Operations Center) oluşturmaktadır. SOC, kurumların siber güvenlik stratejilerinin temel taşlarından biri olup, olay izleme, tehdit tespiti, olay yanıtlama ve risk azaltma gibi kritik işlevleri yerine getirir. Ayrıca, SOC ekipleri sürekli olarak sistemleri izleyerek, gelişen tehditlere karşı önleyici tedbirler almakta ve güvenlik açıklarını en aza indirmek için çalışmaktadır.

Bu rapor, SOC'un temel yapısını ve işleyişini ayrıntılı bir şekilde inceleyerek, SOC katmanları (L1, L2, L3) ve analist rollerinin sorumluluklarını ortaya koymaktadır. SOC içerisinde farklı seviyelerde görev alan analistler, güvenlik olaylarını sınıflandırarak ve ilgili aksiyonları alarak tehditlere karşı etkin bir savunma mekanizması oluştururlar. Ayrıca, olay yönetimi süreçleri ile SOC'da yaygın olarak kullanılan SIEM, IDS/IPS ve log yönetim sistemleri gibi temel araçlara da değinilecektir. Bu araçlar, tehdit istihbaratı toplamak, saldırıları analiz etmek ve güvenlik olaylarına hızlı bir şekilde müdahale etmek için kullanılmaktadır.

Bu raporun amacı, SOC'un siber güvenlik ekosistemindeki yerini ve önemini kavrayarak okuyuculara stratejik bir bakış açısı kazandırmaktır. Bunun yanı sıra, SOC'un işleyişine dair detaylı bilgiler sunularak, bu alanda kariyer yapmak isteyen bireyler için rehber niteliğinde bir kaynak oluşturulması hedeflenmektedir.

SECURITY OPERATION CENTER NEDİR?

Güvenlik Operasyonları Merkezi (Security Operations Center) siber güvenlik uzmanlarından oluşan ve bilişim sistemlerini 7/24 süreyle siber saldırılara karşı izleyip, aksiyon alan bir yapıdır. Bu ekip, teknolojik çözümleri kullanarak iyi bir süreç yönetimi yapar ve siber güvenlik olaylarının tespit edilmesini sağlayıp analizini sunar. Siber saldırılara karşı aksiyon alır.

Daha ayrıntılı tanımıyla ; SOC iyi tanımlanmış süreçlerin yardımı ile siber güvenlik olaylarını önlemeyi hedefleyen bir sistemdir. Siber güvenlik olayların gerçekleşmesi süreçlerinde tespit, analiz ve yanıtlama aşamalarında profesyonel bir ekip oluşturur. Kurumun güvenlik duruşunu sürekli olarak izleyen ve iyileştirmesi için organize olan bu ekip ayrıca ayrıntılı olarak belirlenmiş prosedürlerden oluşan iş süreçlerine sahiptir.

SOC ekipleri, sistemleri tehdit eden veya tehdit etme potansiyeli olan bütün unsurları en kısa sürede tespit ve aksiyonla yükümlüdür. Tespit ve aksiyon süreçleri elde edilen ham bilgilerin kademeli olarak alanında uzman kişiler tarafından filtrelerden geçirilerek gerçek verilere dönüştürülmesiyle oluşmaktadır. Veriyi toplayan veya tespit eden kişilerden verinin onaylanacağı yöneticilere kadar uzanan bu süreçlerde en can alısı nokta ise “zaman” ile yarışıyor olmaktır.

SOC’un amacı siber güvenlik tehditlerini belirleyerek , analiz ederek ve bunlara tepki vererek kurumu güvenlik ihlallerinden korumaktır.

Bir SOC, merkezi komuta merkezi gibi davranır; ağları, cihazları bilgi depoları dahil olmak üzere bir kuruluşun BT altyapısını göz önüne alarak hareket eder. Temel olarak, SOC, izlenen organizasyonda kaydedilen her olay için bir benzerlik noktasıdır. Bu olayların her biri için, SOC nasıl yönetileceği ve nasıl davranılacağına karar vermelidir. Bu kararların alınması ile saldırıların önceden tespit edilmesini sağlar.

Güvenlik operasyonları merkezleri genellikle güvenlik analistleri, güvenlik mühendisleri ve güvenlik işlemlerini denetleyen yöneticilerden oluşur ve güvenlik operasyonlarını denetleyen yöneticileriyle birlikte çalışır.

GÜVENLİK OPERASYON MERKEZİ AMACI

Güvenlik Operasyon Merkezi, kuruluşların siber güvenliğini sağlamak ve olası tehditlere karşı korunmasını garanti altına almak için kritik bir rol oynar. SOC'un temel amacı, güvenlik olaylarını tespit etmek, analiz etmek ve müdahale ederek zararı en aza indirmektir. Bu süreç iki temel aşamadan oluşur:

1. Aşama: Güvenlik Zafiyetlerini Keşfetmek ve Tanımlamak

SOC, organizasyonun ağ altyapısını, sistemlerini ve uygulamalarını sürekli olarak izleyerek güvenlik açıklarını tespit eder ve analiz eder. Bu aşamada temel hedef, tehditleri daha ortaya çıkmadan belirlemek ve önlem almaktır. SOC'un bu aşamada sağladığı merkezi izleme yetenekleri, aşağıdaki unsurları içerir:

- **Güvenlik İzleme ve Log Yönetimi**: SIEM (Security Information and Event Management) gibi araçlar kullanılarak sistemlerden ve ağ cihazlarından gelen günlük kayıtlar analiz edilir.
- **Anomali Tespiti**: Olağandışı kullanıcı aktiviteleri, şüpheli veri akışları veya kötü amaçlı yazılım izleri tespit edilir.
- **Sızma Testleri ve Zafiyet Yönetimi**: Sistemlerde mevcut güvenlik açıkları belirlenir ve bunların kapatılması için çözümler geliştirilir.
- **Tehdit İstihbaratı**: Yeni ve gelişen tehditlere karşı bilgi toplanarak organizasyonun savunma stratejileri güncellenir.

Bu aşama, olası saldırıları önlemek ve sistemleri güçlendirmek için kritik bir süreçtir. Güvenlik açıklarının erken tespit edilmesi, kuruluşun saldırılara karşı daha dayanıklı hale gelmesini sağlar.

2. Aşama: Güvenlik Olaylarına Müdahale Etmek

SOC'un ikinci temel aşaması, organizasyonun altyapısına, servislerine veya müşterilerine zarar verebilecek güvenlik olaylarına müdahale etmektir. Tehditlerin tamamen ortadan kaldırılması veya etkisinin en aza indirilmesi için hızlı ve etkili müdahale gereklidir. SOC'un bu aşamada gerçekleştirdiği başlıca faaliyetler şunlardır:

- **Gerçek Zamanlı Olay Tespiti ve Analiz**: Eş zamanlı izleme sayesinde şüpheli aktiviteler anında tespit edilir ve olası saldırılar daha gerçekleşmeden durdurulabilir.
- **Olay Müdahale Süreçleri**: SOC, güvenlik ihlallerini tespit ettiğinde hızlıca harekete geçerek tehditleri izole eder, saldırının yayılmasını önler ve sistemleri normale döndürmek için gerekli adımları atar.
- **Zararın Sınırlandırılması**: Saldırının organizasyon üzerindeki etkisini en aza indirmek için güvenlik önlemleri uygulanır ve gerekli düzeltmeler yapılır.
- **Adli Analiz ve Raporlama**: Saldırıların kaynağı, yöntemi ve etkileri analiz edilerek detaylı bir rapor hazırlanır. Bu raporlar, ilerleyen dönemlerde benzer tehditlerin önlenmesi için kullanılır.

- **İyileştirme ve Güçlendirme**: Yaşanan olaylardan ders çıkarılarak güvenlik sistemleri güncellenir ve kuruluşun savunma mekanizmaları güçlendirilir.

SOC'un hızlı ve etkili bir şekilde olaylara müdahale edebilmesi, saldırının oluşturabileceği potansiyel zararları ciddi şekilde azaltır. Eğer SOC, bir saldırıyı gerçekleşirken tespit edip durdurabilirse, kuruluşun finansal kayıplarını engelleyebilir, veri ihlallerinin önüne geçebilir ve markanın itibarını koruyabilir.

GÜVENLİK OPERASYON MERKEZİ GÖREVLERİ

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.

GÜVENLİK OPERASYON MERKEZİ EKİBİ

Siber güvenlik operasyon merkezleri , kurum içerisindeki başarısı ekibe bağlıdır. SOC ekibi ; seviye 1 , seviye 2 seviye 3 , seviye 4 pozisyonlarına sahiptir. Birde siber tehdit istihbarat ekibi vardır.

1) SEVİYE 1 GÜVENLİK ANALİSTİ :

En alt tabakadadır. Sistem yöneticisi yetkinliklerine, programlama ve güvenlik yeteneklerine sahiptir. Alarmların doğruluğunu kontrol eder ve önceliğini belirler. Saldırı sinyali veren alarmlar için ticket oluşturur ve bunu seviye 2 yani üst yöneticiye haber verir. Zafiyet taramaları yapar ve raporlarını değerlendirir. Güvenlik izleme araçlarını yönetir ve yapılandırır.

2) SEVİYE 2 GÜVENLİK ANALİSTİ :

Seviye 1 analistin yapması gereken görevlerin yanı sıra problemin asıl kaynağına inebilme ve baskı altında çalışabilme ve krizi yönetebilmelidir. Seviye 1 analistinin oluşturduğu ticket'ları inceler. Tehdit istihbaratlarını değerlendirerek etkilenen sistemleri ve saldırının kapsamını belirler. Saldırıya maruz kalabilecek sistemler üzerindeki bilgileri ileriki saldırılar için toplar, iyileştirme ve kurtarma planını belirleyip yönetir.

3) SEVİYE 3 UZMAN GÜVENLİK ANALİSTİ :

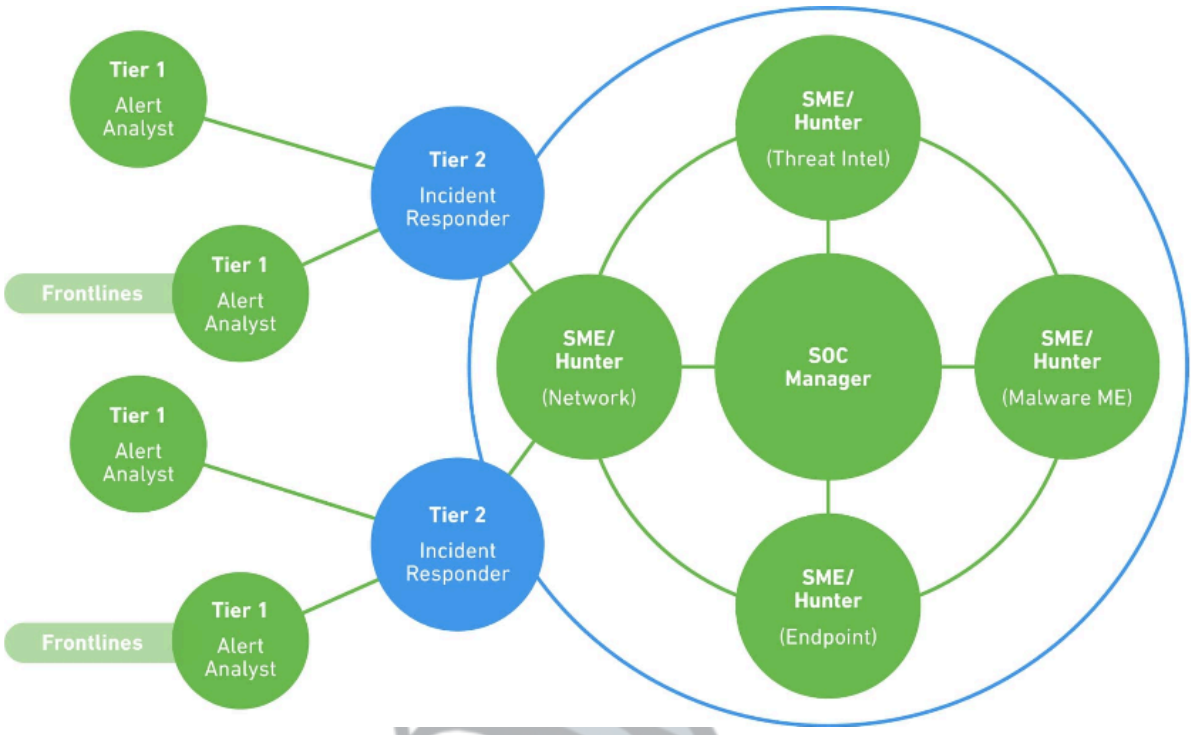
Seviye 1 ve 2 analistlerinin yetkinliklerinin yanında veri görselleştirme araçlarına hakim olmalıdır. Tanımlanan zafiyet değerlendirme ve varlık envanterini verilerini gözden geçirir. Tehdit istihbaratlarını göz önünde bulundurarak kurum ağı içerisinde yerleşmiş olan gizli tehditleri ve tespit yöntemlerini bulur. Sistemlere sızma testleri yaparak dayanıklılığını ve düzeltilmesi gereken açıklıkları bulurlar. Tehdit avcılığının yardımıyla güvenlik izleme araçlarını optimize ederler.

4) SEVİYE 4 SOC YÖNETİCİSİ :

En üst tabakadır. Seviye 1,2 ve 3 analistlerinin yetkinliklerine ek olarak güçlü liderlik ve iletişim yeteneklerine sahip olmalıdır. Ekip ruhunu diri tutmalıdır. SOC yöneticisi, operasyonları ve ekibi yönetir. SOC ekibinin faaliyetlerini gözetler. Ekip için eğitim süreçlerini , işe alım ve değerlendirmelerini yapar. Saldırıların süreçlerini yönetir ve olay raporlarını gözden geçirir. Ekiple haberleşme için iletişim planını geliştirir ve uygular. Uyumluluk raporlarını yayınlar .Denetleme süreçlerini yakından takip eder ve destekler; SOC önemini iş dünyasına aktarır.

5) SİBER TEHDİT İSTİHBARATI EKİBİ :

Siber tehdit istihbaratı, kurumlarda güvenliğine zarar verebilecek tehditler hakkında tanımlanmış, toplanmış ve zenginleştirilmiş verilerin bir süreçten geçirilerek analiz edilmesi sonucu saldırganların amaçlarını ve metotlarını tespit etmeye yarayan bir istihbarat türüdür. Siber tehdit istihbaratı ,bir kurumun veya varlığın güvenliğini tehdit eden mevcut ve potansiyel saldırılar hakkındaki bilgilerin toplanmasına, analiz edilmesine odaklanan siber güvenlik alanıdır. Büyük SOC ekipleri tehdit istihbaratına özel görevlendirmeler yapabilirler.



SOC ANALİSTİ NE YAPAR?

SOC, Güvenlik Operasyon Merkezi, bir organizasyonun siber güvenlik sinir merkezi. SOC analistleri, bu merkezdeki uyanık nöbetçilerdir:

Güvenlik araçlarını izleme: Buna SIEM (Güvenlik Bilgileri ve Etkinlik Yönetimi) sistemleri, saldırı tespit sistemleri (IDS) ve olağandışı aktivite arayan güvenlik duvarları dahildir.

Güvenlik uyarılarını analiz etme: Potansiyel tehditleri araştırmak, meşruiyetlerini belirlemek ve potansiyel etkilerini anlamak.

Olay Yanıtı: Siber tehditleri kontrol altına almak ve azaltmak için planlar geliştirmek ve yürütmek.

Güvenlik Aracı Yönetimi: Çeşitli güvenlik araçlarının bakımı ve optimizasyonuna yardımcı olmak.

Raporlama ve Belgeler: Güvenlik olaylarının titiz kayıtlarını tutmak ve paydaşlar için raporlar oluşturmak.

SOC Analistleri için Temel Beceriler:

Bir SOC analisti olarak mükemmel olmak için, teknik uzmanlık ve yumuşak becerilerin bir karışımı çok önemlidir. İşte ihtiyacınız olan bazı temel beceriler:

Teknik Beceriler:

Ağ güvenliği: Ağ protokolleri (TCP / IP), güvenlik duvarları, VPN'ler ve izinsiz giriş algılama sistemlerinin güçlü bir şekilde anlaşılması.

İşletim Sistemleri: Güvenlik sertleştirme teknikleri de dahil olmak üzere Windows ve Linux gibi işletim sistemleri hakkında derinlemesine bilgi.

Güvenlik araçları: SIEM sistemleri (Splunk, QRadar), güvenlik açığı tarayıcıları (Nessus, OpenVAS) ve diğer güvenlik araçlarına aşinalık.

Komut Dosyası / Programlama: Görevleri ve veri analizini otomatikleştirmek için Python veya Bash gibi komut dosyası dillerinin temel olarak anlaşılması.

Günlük Analizi: Güvenlik olaylarını tanımlamak için çeşitli kaynaklardan günlük verilerini okuma ve analiz etme yeteneği.

Yumuşak Beceriler:

Analitik Düşünme: Eleştirel düşünme ve karmaşık güvenlik sorunlarını çözme yeteneği.

İletişim Becerileri: Olayları bildirmek ve ekip üyeleriyle işbirliği yapmak için mükemmel yazılı ve sözlü iletişim.

Problem çözme: Baskı altındaki güvenlik sorunlarını hızlı bir şekilde belirleme ve ele alma kapasitesi.

Uyarlanabilirlik: Siber güvenlik sürekli gelişmektedir, bu nedenle yeni teknolojilere ve tehditlere uyarlanabilir olmak esastır.

Takım çalışması: SOC analistleri genellikle bir ekibin parçası olarak çalışır ve işbirliği ve iletişimi çok önemli hale getirir.

SOC EKİBİNDE BULUNMASI GEREKEN ÖZELLİKLER

SOC ekiplerin de aranması gereken özellikler de NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından belirlenen CSF (Siber Güvenlik Çerçevesi/Standartları) referans gösterilerek şu şekilde özetlenebilir:

Belirleme (Identify): Kişilerden, yazılımlardan veya donanımlardan oluşan bütün sistem envanterini belirleyip, belirlenen envanter haritası üzerinden siber güvenlik risklerinin tespit edilmesine olan sağlar. SOC ekipleri, sistemleri izlemeye almadan önce envanteri iyi belirlemeli ve atak yüzeyine hakim olmalıdır. Gözden kaçan herhangi bir sistem, yazılım veya kişi, ilerleyen süreçte ufak bir zafiyetle başlayan tedarik zinciri saldırısına dönüşebilmektedir. Bu süreçte şirket için yazılım, donanım ve kişilerin tespitiyle birlikte paydaşların, hizmet alınan satıcıların da sisteme erişimleri olan noktaları belirlemek ve izlemeye almak "Envanter Oluşturma" isimini de verebileceğimiz bu adım, SOC ve güvenlik ekipleri için sistemin büyük resmini oluşturmaya yaramaktadır ve ilk temel adımdır. Bu adımı özetlemek gerekirse şu şekilde özetlenebilir:

- Fiziksel ve yazılım varlıklarını belirle,
- İş ortamlarını ve tedarik zinciri rolünü belirle,
- Yerleşik siber güvenlik politikalarını ve bu politikalra özgü yasal veya düzenleyici gereksinimleri belirle,
- Envanterde yer alan yazılım, donanım veya personele ait zafiyetleri belirle ve Risk Değerlendirme programı oluşturma (Risk Değerlendirme programı, risk yönetim stratejisi belirleme ve toleransları hesaplamaya katkı sağlayacaktır.),
- Önceliklere, risklere ve toleranslara göre karar vermeye olanak sağlayan risk yönetim stratejisini oluşturup, uygulama.

Koruma (Protection): Saldırı yüzeyi bir önceki fazda belirlenen sistemi tehdit eden veya edebilecek bütün unsurlara karşı koruma adımıdır. SOC ekipleri, izleme yaptıkları sistemde herhangi bir anomali durumunda veriyi hızlı bir şekilde doğrulayıp gerekli ve doğru aksiyonu alarak koruma adımını gerçekleştiriş olur. Örneğin: Mail güvenliği ve sandbox çözümleri olmayan bir sistemde mesai saatleri dışında personele e-posta yolu ile iletilen bir zararlı yazılım, SOC ekipleri tarafından algılanır ve kullanıcıya ait hesap sıfırlanırken (gerektiğinde askıya alınır), kullanmış olduğu bilgisayar internetten ve sistemden izole edilir. Koruma adımı özetlenirse:

- Envanterde bulunan yazılım, donanım ve kişilerden kaynaklanabilecek bütün zafiyetlerin sürekli ve düzenli yönetimi,
- Fiziksel ve uzaktan erişimler için kimlik doğrulama ve kimlik yönetimi,
- Personellere, siber tehdit farkındalık eğitimi verme,
- Envanterde yer alan bütün verilerin sınıflandırılarak düşük seviyeden kritik seviyeye kadar derecesi olan bütün verilere ayrı koruma politikaları düzenleme, uygulama ve uygulandığını kontrol etme.

Tespit Etme (Detection): Envanteri oluşturulup atak yüzeyi belirlenen ve veri koruma politikaları oluşturulan sistemi tehdit eden veya edebilecek bütün unsurların tespit edilip değerlendirmeye alınması gereken aşamadır. Değerlendirme sürecini kısa tutarken sonraki aşama olan "Yanıtlama" ya geçilir. SOC ekipleri sistemlerin atak yüzeylerine hakim olmaları gerektiği için tehditleri tespit etme aşamasında zorlanmamaları gerekmektedir. Tespit edilen tehditler için gerekli kural, korelasyon ve alarmların oluşturulması adına sonraki aşama olan "Yanıtlama" aşaması ekiplerine gerekli bilgileri sağlar. Tespit etme adımları kısaca:

- Anomali olayların tespit edildiğinden ve uygun yanıt için tehditlerinin kategorize edildiğini kontrol etme,
- Uygulanan önlemleri değerlendirmek ve siber tehditleri izlemek için sürekli güvenlik izleme yetenekleri geliştirme,
- Yeni siber saldırı göstergelerini belirlemek için süreçleri en son tehdit istihbaratına göre güncelleme,

Yanıt/Müdahale (Response): Tehditlerin tespit edilmesinin ardından yine en kısa sürede yanıtlama sürecini işletilmesi gerekmektedir. Tehditlere karşı önlemlerin alınma prosesleri bu süreçte gerçekleştirilir.

- Tespit edilen bulguları paydaşlar ve kolluk kuvvetleri arasında iletişim prosedürleri kurularak paylaşma,
- Müdahale etkinliğinin raporlanmasını sağlama ve sonrasındaki benzer vakalarda sonraki süreçlerin daha verimli atlatılmasını sağlama,
- Müdahale süreçlerinde iyileştirmeleri belirleme,
- SOC ekip yeteneklerinin geliştirmek için tespit ve müdahale eylemleri arasında belirlenen iyileştrimeleri uygulama,

adımları müdahale sürecini kısaca özetleyebilmektedir.

Kurtarma (Recovery): Tespit edilemeyen tehditlerin sistemi olumsuz etkilemesi halinde işletilecek olan prosestir. SOC ekipleri bu fazda, etkilenen yetenekleri, sistemleri veya hizmetleri en hızlı şekilde geri yüklemek için gerekli önlemlere odaklanmalıdır. Yine zamanla yarışması gereken SOC ekipleri sistemi etkilenen operasyonları normal haline gelmesi için en kısa sürede bu fazı tamamlamalıdır. Bu süreçte SOC ekiplerinin izlemesi gereken adımlar ise şunlardır:

- Sistemleri, varlıkları ve hizmetlere erişimi geri yüklerken kuruluşunuzun planlı Kurtarma süreçlerinin düzgün şekilde yürütülmesini sağlama,
- Yeni iyileştirmeleri uygulamak için mevcut stratejileri ve mevcut siber tehdit istihbaratını gözden geçirme,
- Olay kurtarma süreçleri sırasında ve sonrasında, dahili ve harici tüm iletişimleri koordine etme.

GÜVENLİK OPERASYON MERKEZİ ROLLERİ

Güvenlik Operasyonları Mühendisi: SOC'da kullanılan tüm güvenlik ürünlerinin kurulum ve işletim faaliyetlerini gerçekleştirir.

Güvenlik Mimarı: Güncel güvenlik tehditlerini ve saldırıları takip ederek ,bunları önlemek için strateji ve çözümleri sistemlere uygulanmasını sağlar. Yani kurumdaki güvenlik riskini azaltır ve doğru güvenliğin tasarımını yapar.

Güvenlik Analisti: Güncel saldırıları araştırır. Şüpheli durumları analiz eder ve saldırıları tespit eder. Güvenlik ve ağ cihazları , uygulamalardaki log kayıtlarını inceler.

Olay Müdahale Uzmanı: Güvenlik analisti tarafından şüpheli görülen olayların detaylı analizini yapar. Gerekli durumlarda SOC ekibini yönlendirir ve koordinasyonu sağlar. Sistemlerde meydana gelmiş veri sızıntılarını ve değişiklikleri tespit eder.

Sızma Testi Uzmanı: Web , ağ ve sistem uygulamalarındaki zafiyetleri bulur ve inceler. Bu zafiyetler üzerindeki tehditlere göre riskleri belirler ve iyileştirmeler yapar.

Adli Bilişim Mühendisi: Olay yeri incelemesi yapar. Delilleri bulur , saklar ve bilgileri toplar. Sonrada inceler ve rapor yazar. Analist ve uzmanlardan aldığı bilgilerle saldırı ile ilgili araştırma yapar.

Yazılım Güvenliği Mühendisi: Kurum içerisinde geliştirilen uygulamaları güvenlik yöntemleriyle gözden geçirir ve geliştirir. Sızma testi uzmanlarına test yaptırırlar ve çıkan sonuçları değerlendirir.

Siber Güvenlik Denetçisi: Kurumun güvenlik risk seviyelerini inceler. SOC'un kabul edilen risk seviyelerine , standartlarına ve süreçlere olan uygunluğunu ölçer ve raporlar.

Hukuk Danışmanı: Adli durumlarda kurum ve hukuk arasındaki süreçlerini koordine eder. Adli bilişim ve siber hukukundaki yasaları takip eder.

Eğitim Koordinatörü: Personelin eğitim ve yeterlilik seviyelerinin ölçülmesi için gerekli süreçleri oluşturur ve işletir.

Zararlı Yazılım Uzmanı: Zararlı yazılımları inceleyerek nasıl çalıştığını anlar ve kurum içinde ne gibi riskler oluşturacağını araştırır, önlem alır.

SİBER GÜVENLİK OPERASYON MERKEZLERİ NASIL ÇALIŞIR

Bir SOC ekibinin çalışabilmesi için donanımsal ve yazılımsal uygun altyapıya sahip olması gerekmektedir. Bazı SOC ekiplerinde, olayları analiz etmek için gelişmiş adli analiz, kriptanaliz, ters mühendislik ve zararlı yazılım analizi teknik kabiliyetlerini içermektedir.

Bir kuruluşun SOC'unu kurmanın ilk adımı, çeşitli departmanlardan işletmeye özgü hedeflerin yanı sıra yöneticilerin girdisi ve desteğini içeren bir stratejiyi açıkça tanımlamaktır. Strateji geliştirildikten sonra, gereken altyapı uygulanmalıdır. Tipik bir SOC altyapısı güvenlik duvarları, IPS / IDS, DLP, Endpoint Security ve SIEM sistemi içerir. SOC personeli tarafından veri etkinliklerinin ilişkilendirilebilmesi ve analiz edilebilmesi için veri akışlarının, network kayıtlarının, cihaz loglarının ve ihtiyaca göre gerekli görülen kayıtların toplanması gerekmektedir. SOC işlemlerinin temeli, kurumun sahip olduğu cihaz ve sistemlerden gönderilen log kayıtlarını yani sistemin dijital hareket verilerini ve bu verileri analiz edip, uygun sonuçlar ve tepkiler üreten SIEM ve SOAR sistemleridir. SOC ayrıca ISO 270001, HIPAA, SOC2 gibi çeşitli yönetmeliklere uyum sağlamak için için de çalışmalar yapmaktadır.

SOC merkezi bir organizasyonun, kurumun bilgi güvenliği sistemlerini kontrol ve analiz ederek siber güvenlik tehditlerine karşı korur. Bir SOC ekibinde yönetici, güvenlik analistleri, güvenlik mühendisleri bulunur ve diğer tüm BT personeliyle koordineli olarak çalışırlar.

Soc'un kısaca çalışma adımları;

1. Kurumun sahip olduğu sistemlerin , yazılımların ve donanımların tespit edilmesi.
2. Tespit edilen envanterin zafiyet değerlendirmesini yapılması.
3. Sistemin sıradan hareketlerini ve sıradan dışı hareketlerini belirlenmesi.
4. IPS , IDS ,DLS gibi teknolojileri kullanarak sızma ve sıradan dışı hareketlerin tespitinin yapılması.
5. SIEM ve SOAR sistemleri kullanılması.
6. Saldırı varsa müdahale etmek ve analiz yapmak. Analiz sonuçlarını raporlanması.
7. Raporlara göre güvenlik önlemi almak ve sistemi eskisinden daha güvenilir hale getirilmesi.

GÜVENLİK OPERASYON MERKEZİ SÜREÇLERİ

1) KORUMA:
Önlem alınan adımdır. Bu aşamada öncelik dereceleri belirlenir . Bu çok önemlidir. Seviye 1 SOC analistleri en son tespit edilen ve en yüksek önemlilik derecesine sahip olan olayları kontrol ederler. Bu olayların daha ileri analizlere ihtiyaç olduğunu anladıklarında sorunu Seviye 2 analistlere bildirirler. Bu aşamada raporlandırma çok önemlidir. Alarmlar oluşturulur. Alarm türleri;

- **Keşif ve Araştırma (Probe):** Öncelik seviyesi düşük olan alarmdır. Saldırgan kurum hakkında bilgi topladığı çalışmadır. Pasif bilgi toplama yapar. Seviye 1 analistin tehdit istihbarat ekiplerinin duyuru ve hareketlerini takip etmesi gerekir.

- **İstismar Kodunun Gönderilmesi:** Öncelik seviyesi düşük ile orta arasında olan alarmdır. Phishing ‘deki e-postalara gönderilen zararlı yazılım yükleyen linklerin gelmesi gibi örnekler verilebilir. Seviye 1 analistin tehdit istihbarat ekiplerinin duyuru ve hareketlerini takip etmesi gerekir.

- **İstismar Kodunun Aktifleştirilmesi/Kurulması:** Öncelik seviyesi orta ile yüksek arasında olan alarmdır. Phishing ‘deki e-postalara gönderilen zararlı yazılım yükleyen linklerin tıklanması sonucunda açık oluşması ve sömürülmesi veya Backdoor/RAT kurulması gibi örnekler verilebilir. Doğrulama ve analiz yapıldıktan sonra Seviye 2’ye haber verilmesi gerekir.

- **Sistemin Ele Geçirilmesi:** Öncelik seviyesi yüksek olan alarmdır. Doğrulama ve analiz yapıldıktan sonra Seviye 2’ye haber verilmesi gerekir.

2) TESPİT:
Bu aşamada kuruma yapılan saldırı girişimine işaret eden durumlar analiz edilir ve uygun aksiyon alınması çok önemlidir. Denetime alınması gereken saldırı göstergeleri arasında mevcut bir açıklığı istismar eden saldırganın bıraktığı izleri bulup tespit ederiz.

3) MÜDAHALE:
Saldırının tespit edilip hemen müdahale edilmesi gerekir. Saldırı önlendikten sonra raporlara göre açıklıkları ve riskleri araştırılır. Saldırı hukuk işlemleri yapılması hakkında karar verilir. Saldırıyı kontrol altına almak için alınan adımlar; sistemlerin imajı alınır , sistem açıkları kapanır , ağ ve sistem erişimlerini yapılandırmak , zafiyet taramaları yapılır.

4) GERİ DÖNÜŞ:
Adli bilişim mühendisleri tarafından saldırı detaylı bir şekilde analiz edilir ve rapor oluşturulur. Sızma testi uzmanları tarafından zafiyet taraması gerçekleştirilir. Bu sonuçlar dahilinde sistem kontrol edilir. Açıklık varsa kapanır. Sistemi eskisinden daha güvenilir hale getirilir.

SOC'NİN ALT YAPISINDA 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) EDR (Endpoint Detection and Response) :
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.

GÜVENLİK OPERASYON MERKEZİ FAYDALARI

Bir SOC birimine sahip olmanın en önemli yararı, sürekli izleme ve veri etkinliğinin analizi yoluyla güvenlik olaylarının tespitinin iyileştirilmesidir. Bir kuruluşun ağları, uç nokta cihazları, sunucuları ve veritabanları ile veri etkinliği analiz edilerek; SOC ekipleri, güvenlik olaylarının zamanında tespit edilmesi ve aksiyon alınmasını sağlamak için kritik öneme sahiptir. SOC tarafından sağlanan 7/24 izleme, organizasyona, kaynağa, günün saatine veya saldırı türüne bakılmaksızın, olaylara ve saldırılara karşı savunma yapma avantajı sağlar. Saldırganların aktif saldırı süreleri ve işletmelerin tespit etme süreleri arasındaki fark Verizon'un yıllık Veri İhlali Araştırması raporunda iyi bir şekilde belgeleniyor ve bir güvenlik operasyon merkezine sahip olmak, kuruluşların bu boşluğu kapatmasına ve çevrelerine yönelik tehditlerin üstünden kalkmasına yardımcı olur.

SOC'nin sağladığı temel faydalar şunlardır;

- Tehdit, ihlal tespiti ve olay müdahalesi için ağların, donanımın, yazılımın proaktif olarak gözetimi.
- Güvenlik sorunlarının kolayca çözülebilmesini sağlamak için kuruluşların kullandığı tüm araçlar hakkında uzmanlık.
- Güvenlik duvarı ve saldırı önleme sistemlerinin izlenmesi ve yönetimi.
- Saldırıların temel nedenini anlamak ve gelecekteki ihlalleri önlemek için güvenlik ihlallerinin araştırılması.
- Güvenlik olaylarıyla ilişkili maliyetlerin azaltılması.
- Güvenlik Operasyonları üzerinde daha fazla şeffaflık ve kontrol.
- Tüketici ve müşteri güveninin korunması.

SONUÇ

Bu rapor kapsamında, Siber Güvenlik Operasyon Merkezleri (SOC) ve bunların işleyişi ayrıntılı bir şekilde ele alınmıştır. Günümüzde giderek artan siber tehditler karşısında, kurumların etkin bir güvenlik stratejisi oluşturması kaçınılmazdır. SOC, tehditleri tespit etme, analiz etme ve zamanında müdahale etme yetenekleriyle güvenlik ekosisteminin vazgeçilmez bir parçası olmuştur.

Raporun içeriğinde SOC'un temel yapısı, katmanları (L1, L2, L3) ve analist rollerinin sorumlulukları incelenmiştir. Her katman, olay yönetimi süreçleri kapsamında belirli görevleri yerine getirerek güvenlik operasyonlarının sürekliliğini sağlamaktadır. Ayrıca, SOC içerisinde kullanılan temel araçlar olan SIEM, IDS/IPS ve log yönetim sistemlerinin önemi vurgulanarak, bu teknolojilerin tehdit istihbaratı toplama ve olay müdahalesindeki kritik rolü açıklanmıştır.

Sonuç olarak, SOC'un etkin kullanımı, siber güvenlik ekosistemindeki tehditlere karşı güçlü bir savunma mekanizması oluşturmada önemli bir rol oynamaktadır. Kurumlar, SOC yapılarını stratejik bir şekilde geliştirerek, siber tehditlere karşı daha hazırlıklı hale gelebilirler. Bu bağlamda, SOC'un sürekli gelişen siber güvenlik tehditlerine karşı uyum sağlayabilmesi için yenilikçi çözümlerle desteklenmesi ve analistlerin bilgi birikimlerini artırmaları kritik bir gerekliliktir.

KAYNAKÇA

- https://bulutistan.com/blog/soc/
- https://www.infinitumit.com.tr/guvenlik-operasyon-merkezi-soc-nedir/
- https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir
- https://www.bgasecurity.com/2018/11/soc-nedir-calisma-yapisi-ve-faydalari/
- https://www.gaissecurity.com/blog/soc-nedir-ve-firmalar-icin-neden-onemlidir
- https://www.cadosecurity.com/wiki/how-to-become-a-soc-analyst-a-complete-guide
- https://www.beyaz.net/tr/guvenlik/makaleler/soc_nedir_ve_soc_da_hizmet_surekligi_nasil_saglanir.html