SOC FUNDAMENTALS

HAZIRLAYAN: UMUT EMRE KARACAER
TARİH: 07.02.2025

İÇERİK

GİRİŞ:

Günümüz dijital dünyasında kurumlar ve işletmeler, siber tehditlere karşı sürekli bir savunma halinde olmak zorundadır. Bu ihtiyacın bir sonucu olarak ortaya çıkan Güvenlik Operasyonları Merkezi (SOC - Security Operations Center), kuruluşların güvenliğini sağlamak ve siber saldırılara karşı etkin bir savunma hattı oluşturmak amacıyla kritik bir rol üstlenmektedir.

SOC, iyi tanımlanmış süreçler ve gelişmiş teknolojiler yardımıyla güvenlik olaylarını tespit etmeyi, analiz etmeyi ve yanıtlamayı hedefleyen bir yapıdır. Merkezi bir komuta merkezi gibi hareket eden SOC ekipleri, ağlar, cihazlar, veri depoları ve uygulamalar gibi BT altyapısını izleyerek anormal aktiviteleri tespit eder ve güvenlik ihlallerine müdahale eder.

Bu rapor kapsamında, SOC'un tanımı, amaçları, görevleri, ekip yapısı ve çalışma prensipleri ele alınarak, siber güvenlik operasyon merkezlerinin önemi ve organizasyonların güvenlik yapısına sağladığı katkılar detaylı bir şekilde incelenecektir.

SOC NEDİR?

SOC, Güvenlik Operasyonları Merkezi (Security Operations Center) bir kuruluşun güvenliğini devamlı olarak izleyen ve güvenlik olaylarının analizinden sorumlu bir bilgi güvenliği ekibinin bulunduğu yer veya tesistir. 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'un amacı siber güvenlik tehditlerini belirleyerek , analiz ederek ve bunlara tepki vererek şirketi 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.

SOC'UN AMAÇLARI:

Günümüz dünyasında, bilişim teknolojileri akıl almaz derecede birbirine bağlı. Tabi, bu bağlılık yanında birçok bedeli de beraberinde getiriyor. Hemen her kuruluşun bir parçasının siber alanlarda olması, onlara ekstra bir risk getiriyor. Saldırganların hedefi olmak ise; kurumun itibarını, çalışma disiplinlerini ve hatta sızdırılan bilginin önemi ve saldırının tipine göre maaş bilgilerini bile etkileyebilir. Bunca kuruluşun oluşabilecek riskleri göze alıp siber alana girmesiyle birlikte, artık bilgi teknolojileri teriminden çok siber güvenlik terimleri daha kullanılır oldu.

Bu tür kuruluşlar iş ve siber güvenlik hedeflerini karşılamak için siber güvenlik risk yönetimi bilgilerine ihtiyaç duyarlar. İşte tam da bu sebeple SOC ortaya çıkmıştır.

SOC'un amacı iki aşamalıdır;

- **Birinci aşama:** güvenlik zafiyetlerini keşfetmek ve tanımlamak için merkezi izleme yetenekleri sağlamak.

- **İkinci aşama:** bir organizasyonun yapısına, servislerine ve hatta müşterilerine zarar verebilecek güvenlik olaylarına müdahale etmektir. SOC genel olarak, izleme ve müdahale hizmeti verdiği kuruluşa (kendi kuruluşu da olabilir) gerçekleşen atak ve sızma olaylarını en kısa sürede tespit etmeyi hedefler. Bu amaçla, eş zamanlı izleme ve şüpheli olayların analizi ile bir olayın oluşturabileceği potansiyel etki ve hasarı sınırlandırır. Eğer SOC bir saldırıyı devam ederken durdurabilirse, zaten hizmet verdiği organizasyonun zamanını, parasını kurtarmış, veri kaybının önüne geçmiş ve hatta markanın itibarını korumuş olur.

SOC'UN 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.

SOC EKİBİ:

Siber güvenlik operasyon merkezleri , kurum içerisindeki başarısı ekibe bağlıdır. SOC ekibi; seviye 1, seviye 2, seviye 3, seviye 4 pozisyonlarına sahiptir. Bir de 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. Daha küçük SOC ekipleri ise güvenilir bir tehdit istihbaratı hizmet sağlayıcısından bilgi almak gibi bir yöntem uygulayabilirler.

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

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.


LOG
COLLECTION
AGGREGATION
CORRELATION
REPORTING
SOC
SIEM
RESEARCH &
DEVELOPMENT
THREAT
INTELLIGENCE
TICKETING
KNOWLEDGE
BASE

SOC MODELLERİ:

SOC, güvenlik açıklarını tespit etmek için merkezi izleme yetenekleri sağlamanın yanında bir organizasyonun yapısına, servislerine ve hatta müşterilerine zarar verebilecek güvenlik olaylarına müdahale eder. O yüzden model seçimi çok önemlidir.

SOC modeli seçerken; kurumun büyüklüğüne, kurumun daha önce yaşadığı güvenlik problemlerine, kurumun içinde bulunduğu endüstriye , IT departman bütçesine ve personellerin kabiliyetlerine , kurum içinde oluşan bir günlük trafik kriterlerine bakılarak uygun model seçilir.

1) INTERNAL SOC (DAHİLİ SOC) :

Kurum içinde çalışan güvenlik ve BT uzmanlarından oluşan kurum içi ekiptir. İç ekip üyeleri diğer bölümlere yayılabilirler. Ayrıca , güvenlik için kendi bölümlerini oluşturabilirler.

Dahili SOC kurmayı düşünen firmaların devamlı izlemeyi desteleyecek bir bütçeye sahip olması gerekir. Büyük ölçekli şirketlerin dahili SOC kurması önerilir.

Internal SOC'un avantajlarından biri, şirket içindeki ağı belirgin bir şekilde görmeyi sağlar. SOC ekibinin içerdeki cihazları, log kaynaklarını görmesini ve tehdit oluşturacak olaylara karşı perspektif kazanmasını sağlar. Bu avantajlarının yanında bazı önemli dezavantajları da ; bazı olayların tespiti gözden kaçabilir, uzman personel yetiştirmede sıkıntı yaşanabilir ve başlangıçtaki yatırım maliyeti çok yüksektir. Ayrıca, bu modelin etkili olması ve yeterli düzeye gelmesi çok fazla zaman alır.

2) 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.

3) VIRTUAL SOC (SANAL 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;

1. **Internal Virtual SOC:** Uzaktan çalışan yarı zamanlı güvenlik ekiplerinden oluşur. Ekip üyeleri bir uyarı tehditi aldıklarında tepki vermekle yükümlüdürler.

2. **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.

4) HYBRID SOC :

Saydığımız modellerin en etkili bir şekilde birlikte kullanılmasından oluşur. Kurumla birlikte eş zamanlı olarak çalışılır. İzleme, tespit ve alarm üretmede daha etkili çözümler sunar. Bu modelde sistemler, alarmalar, tehditler her iki taraftan da izlenir ve çift taraflı kontrol yapılmış olur. Bu modeli seçen kurumlar genel olarak bu iş için kendi ekiplerini kurabilecek kadar gelişmişlerdir ama bütçe ve uzman ve kaynak eksikliğinden sürekli izleme yapılacak bir Internal SOC kuracak bir kapasitede değildirler. Avantaj olarak önleme ve tespit açısından en güvenli model olmasının yanı sıra dezavantajı ise ,kurumsal bilgileri üçüncü bir firma tarafından da bilinir ve ekstra donanım gerektirir.

SOC'UN KARŞILAŞTIĞI ZORLUKLAR:

1) ARTAN GÜVENLİK UYARI SAYISI:

Artan güvenlik uyarı sayısı, analistlerin zamanını ciddi derecede alır. Uyarıların doğruluğu bulmaya çalışırken acil olmayan güvenlik uyarısıyla da uğraşırlar bu yüzden ciddi uyarıları kaçırarak sisteme saldırı yapılabilir.

2) GÜVENLİK ARAÇLARININ YÖNETİMİ:

SOC tarafından ; çeşitli güvenlik paketleri kullanıldığından , veri noktaları ve kaynaklardan ve kullandığı teknolejilerden tüm verileri izlemek zor olabilir.

3) KAYNAK VE PERSONEL TAHSİSİ:

Yetenekli personel ve kaynak problemleri basit olsa da çözümü olmadığında çok büyük problemlere sebep olabilir. Bir kurum dış kaynak kullanımına karar verebilir fakat uzak çalışma koşullarıyla meydana gelen daha fazla güvenlik açığı çıkabilir.

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.

SONUÇ:

Güvenlik Operasyonları Merkezleri (SOC), günümüz siber tehdit ortamında kurumların güvenliğini sağlamada kritik bir role sahiptir. SOC yapıları, proaktif izleme, tehdit tespiti ve hızlı müdahale süreçleri ile kuruluşların bilgi varlıklarını korumalarına olanak tanır.

Bu raporda incelenen SOC'un yapısı, işleyişi ve güvenlik operasyonlarındaki önemi, dijital güvenliğin sadece teknoloji değil, aynı zamanda süreçler ve uzman insan kaynağı ile desteklenmesi gerektiğini ortaya koymaktadır. SOC ekiplerinin tehdit istihbaratı kullanımı, gelişmiş tehdit analizi ve otomasyon teknolojilerinden yararlanarak operasyonel verimliliği artırması, organizasyonların siber tehditlere karşı daha dirençli hale gelmesini sağlar.

Sonuç olarak, kurumların güvenlik operasyonlarında daha etkin olmaları için SOC yapılarına yatırım yapmaları, güvenlik stratejilerini sürekli olarak güncellemeleri ve uzman SOC analistleriyle iş birliği içinde çalışmalarının önemi büyüktür. Siber tehditlerin sürekli evrildiği bir ortamda SOC, dijital güvenliğin geleceğine yön veren vazgeçilmez bir unsurdur.

KAYNAKÇA:

https://www.trellix.com/security-awareness/operations/what-is-soc/
https://bulutistan.com/blog/soc/
https://www.bgasecurity.com/2018/11/soc-nedir-calisma-yapisi-ve-faydalari/
https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir
https://www.infinitumit.com.tr/guvenlik-operasyon-merkezi-soc-nedir/
https://www.ibm.com/think/topics/security-operations-center