SOC FUNDAMENTALS

MELİKE TAŞDELEN

07.02.2025

GİRİŞ

Günümüzde siber güvenlik tehditleri her geçen gün daha karmaşık hale gelmekte ve organizasyonlar için büyük bir risk oluşturmaktadır. Veri ihlalleri, kimlik avı saldırıları, kötü amaçlı yazılımlar ve gelişmiş kalıcı tehditler (APT'ler), güvenlik ekiplerinin sürekli olarak yeni saldırı vektörlerine karşı tetikte olmasını gerektirmektedir. Bu noktada, Güvenlik Operasyon Merkezi (SOC - Security Operations Center), kurumların siber tehditlere karşı korunmasını sağlamak için kritik bir rol üstlenmektedir.

SOC, siber güvenlik olaylarını sürekli olarak izlediği, analiz ettiği ve bunlara müdahale ettiği merkezi bir birimdir. Güvenlik olaylarını tespit etmek, tehditleri engellemek ve olası saldırılara karşı önlem almak için kesintisiz çalışır.

Bu rapor, SOC'un temel yapı taşlarını, işleyişini ve siber güvenlikteki yerini ele almayı amaçlamaktadır.

İÇİNDEKİLER

SOC NEDİR?

SOC (Security Operations Center) yani "Güvenlik Operasyonları Merkezi", siber güvenlik olaylarını önlerken, tespit ederken, analiz ederken ve bunlara yanıt verirken, bir kuruluşun güvenlik duruşunu sürekli olarak izlemek ve iyileştirmek için insanları, süreçleri ve teknolojiyi kullanan bir kuruluş içindeki merkezi bir işlevdir.

SOC'nin İŞLEVLERİ

1. **Tehdit Algılama ve İzleme:** SOC, ağ trafiğini, log kayıtlarını ve diğer güvenlik verilerini sürekli olarak izleyerek potansiyel tehditleri tespit eder. Bu, anormallikleri ve belirgin saldırı işaretlerini saptama yeteneğini içerir.
2. **Olay Yanıtı ve Müdahale:** SOC, tespit edilen tehditlere hızlı bir şekilde müdahale eder. Bu, saldırıları durdurmak, sistemleri korumak ve veri kayıplarını önlemek için önleyici önlemleri içerir.
3. **Analiz ve Araştırma:** Güvenlik analistleri, SOC içinde tespit edilen tehditleri ayrıntılı bir şekilde analiz eder. Bu, saldırıların karmaşıklığını anlamak ve gelecekte benzer tehditlere karşı daha iyi hazırlıklı olmak için önemlidir.
4. **Güvenlik Politika ve Süreç Geliştirme:** SOC, güvenlik politikalarını ve süreçlerini sürekli olarak gözden geçirir ve iyileştirir. Bu, organizasyonun güvenlik stratejilerini güncel tutmak ve yeni tehditlere uyum sağlamak için gereklidir.

SİBER GÜVENLİK İÇİN SOC NEDEN ÖNEMLİDİR?

Potansiyel tehditler gözlenir ve siber saldırıların büyük zararlara yol açmadan önce algılanmasını ve müdahale edilmesini sağlar. Böylece veri ihlallerinin olasılığını azaltır ve saldırganların güvenlik açıklarını istismar etmek için sahip olduğu süre en aza indirgenir. Hızlı bir şekilde müdahale sağlanır. Siber saldırılar her an gerçekleşebilir ve bir SOC, mesai saatleri dışında da güvenlik tehditlerinin sürekli olarak izlenmesini ve ele alınmasını sağlayarak 7/24 çalışır.

SOC AMAÇLARI

SOC'un temel amacı, bir organizasyonun siber güvenlik duruşunu güçlendirmek, siber tehditlere karşı korunmasını sağlamak ve güvenlik olaylarını etkili bir şekilde yönetmek için 7/24 izleme ve müdahale süreçlerini yürütmektir.

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 MODELLERİ NELERDİR?

3 farklı çalışma modeli mevcuttur.

Dedicated or self-managed (Internal) SOC: kurumun kendi bünyesinde bulundurduğu tesis denebilir.

Virtual SOC: Şirketin kendi bünyesinde bir SOC ekibi olmaksızın bulut veya hizmet üzerinden, şirketin kendi talepleri doğrultusunda hizmet veren bir modeldir.

Distributed (Hybrid) SOC: MSSP üzerinden şirket içinde işe alınan yarı zamanlı veya tam zamanlı ekiptir.

SOC BİLEŞENLERİ:

1.İNSAN

SOC' nin en önemli bileşenlerinden biri eğitimli güvenlik uzmanları ve analistleridir. Tier 1(Uyarı Analisti)(SOC-L1), 2(Olay Müdahalecisi)(SOC-L2), 3 (Tehdit Avcısı)(SOC-L3) Analistleri ve Soc Managerdir.

L1 (Tier 1) – Olay İzleme ve İlk Yanıt Analistleri:

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.

L2 (Tier 2) – Olay Müdahale ve Tehdit Analistleri:

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.

L3 (Tier 3) – Tehdit Avcıları ve Güvenlik Mühendisleri:

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.

SOC Yöneticisi (SOC Manager):

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.

2.TEKNOLOJİ

Teknoloji SIEM, EDR, Firewall, SOAR, WAF, IPS, IDS gibi teknolojiler olabilir. Birkaçını örnek vermek gerekirse ;

- **SIEM (Güvenlik Bilgi ve Olay Yönetimi):** Güvenlik ortamının kapsamlı bir görünümünü sağlamak için çeşitli kaynaklardan gelen güvenlik verilerini toplar ve analiz eder.
- **UBA (Kullanıcı Davranış Analizi):** Bir güvenlik tehdidine işaret edebilecek anormal kullanıcı davranışlarını tespit eder.
- **XDR (Genişletilmiş Algılama ve Müdahale):** İsteğe bağlı veri toplama ve analiz yetenekleri sağlayarak tehdit avcılığını ve olay müdahalesini mümkün kılar.
- **SOAR (Güvenlik Orkestrasyonu, Otomasyonu ve Müdahalesi):** Olay müdahale iş akışlarını otomatikleştirerek verimliliği artırır ve müdahale sürelerini kısaltır.

3.SÜREÇ

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.

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.

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 TÜRLERİ

SOC türleri vardır ve organizasyonun ihtiyaçlarına, bütçesine ve güvenlik stratejisine göre farklı yapılar benimsenebilir. SOC türleri genellikle sahiplik modeli, yönetim şekli ve operasyonel kapsamına göre sınıflandırılır.

DEDICATED SOC:

Özel bir SOC yalnızca kuruluşun güvenlik operasyonlarına odaklanır. Gerçek zamanlı izleme, olay müdahalesi ve devam eden tehdit analizinden sorumlu özel bir güvenlik analistleri ve uzmanları ekibine sahiptir.

- Organizasyonun kendi altyapısında bulunur.
- İç tehditler ve kritik altyapılar için maksimum güvenlik sağlar.
- Gerçek zamanlı müdahale mümkündür.

MANAGED SOC:

Yönetilen bir SOC, işletmeleri siber tehditlere karşı korumak için bütünsel bir çözüm sunar. Bu dış kaynaklı hizmet, güvenlik duvarları, saldırı tespit ve önleme sistemleri ve diğer güvenlik araçları gibi bileşenleri kapsayan bir kuruluşun güvenlik çerçevesinin sürekli gözetimini ve kontrolünü sağlar.

- Güvenlik olayları üçüncü taraf MSSP firmaları tarafından yönetilir.
- SOC analistleri ve olay müdahale ekipleri dış kaynaklıdır.

CO-MANAGED SOC:

Ortak yönetilen bir SOC, bir organizasyonun siber güvenlik gereksinimlerini ele almak için iş birliğine dayalı bir stratejiyi temsil eder. Bu ortak yönetilen SOC çerçevesi içinde, organizasyon güvenlik açıklarını izleme, tanımlama ve bunlara yanıt verme görevlerini ortaklaşa ele almak için üçüncü taraf bir güvenlik sağlayıcısıyla iş birliği yapar; organizasyonların dahili gözetim ve şeffaflığı korurken özel bir güvenlik sağlayıcısının uzmanlaşmış bilgisinden ve varlıklarından yararlanmalarını sağlar.

- Organizasyon, kritik güvenlik süreçlerini kendi içinde yönetir.
- MSSP firması ise destekleyici hizmetler sunar.

VIRTUAL SOC:

Sanal bir SOC, siber güvenlik olaylarını izlemek, tespit etmek ve bunlara yanıt vermek için bulut tabanlı teknolojilerden ve uzak ekiplerden yararlanarak dijital bir alanda faaliyet gösterir. Bu yaklaşım, etkili tehdit yönetimi ve olay yanıtlama yeteneklerini korurken esneklik ve ölçeklenebilirlik sunar.

- SIEM, tehdit istihbaratı ve olay yönetimi gibi hizmetler kullanılır.
- Uzaktan çalışma esnekliği sağlar.

- Düşük maliyetlidir, altyapı yatırımı gerektirmez.

COMMAND SOC:

Bir Komuta SOC, belirli bir organizasyon veya kurum içindeki güvenlik operasyonlarını denetlemek ve gözetlemek için merkezi bir sinir merkezi görevi görür. Birincil amacı, yetenekli güvenlik personelinin, son teknoloji izleme teknolojilerinin ve kapsamlı bir iletişim yolları ağının konuşlandırılmasını düzenleyerek bireylerin, bilgilerin ve değerli varlıkların korunmasını garanti altına almaktır.

- SOC'lar bölgesel bazda faaliyet gösterir, ancak merkezi bir Command SOC tüm operasyonları yönetir.
- Küresel tehdit istihbaratı ve saldırı analizleri yapılabilir.

SONUÇ

Günümüzde siber tehditler yalnızca bireyleri değil, büyük organizasyonları, finansal kurumları, devlet kurumlarını ve kritik altyapıları da hedef almaktadır. Bu nedenle, tehditleri erken aşamada tespit etmek ve saldırılara karşı proaktif önlemler almak hayati önem taşımaktadır. İşte bu noktada, Güvenlik Operasyon Merkezleri (SOC), organizasyonların siber saldırılara karşı ilk savunma hattını oluşturur.

Bu raporda, SOC'un temel yapı taşları, bileşenleri, modelleri , analist rollerinin görevleri ve kullanılan teknolojiler ele alınmıştır. Sonuç olarak, gelişen siber tehdit ortamına karşı güçlü bir güvenlik operasyon merkezi oluşturmak, organizasyonlar için bir seçenek değil, bir zorunluluk haline gelmiştir. Etkili bir SOC yönetimi, sadece saldırıları tespit etmek ve engellemekle kalmaz, aynı zamanda organizasyonun siber dayanıklılığını artırarak iş sürekliliğini sağlar.

KAYNAKÇA

https://nureddineraslan.medium.com/soc-nedir-73e2647a8206

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

https://www.fortinet.com/resources/cyberglossary/what-is-soc

https://medium.com/@fraudas/soc-security-operations-center-tan%C4%B1mlaalari-e03819446781#:~:text=What%20is%20SOC%3F,ve%20teknolojiyi%20kullanan%20bir%20merkezdir.

https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir#:~:text=SOC'un%20amac%C4%B1%20siber%20g%C3%BCvenlik,g%C3%B6z%20%C3%B6n%C3%BCne%20alarak%20hareket%20eder.

https://medium.com/@fraudas/soc-security-operations-center-tan%C4%B1mlaalari-e03819446781#:~:text=What%20is%20SOC%3F,ve%20teknolojiyi%20kullanan%20bir%20merkezdir.