SOC Fundamentals

Tarih: *06.02.2025*

Hazırlayan: *Muhammed Barış Güven*

Altay

Giriş

Günümüzde sıkça yaşanan veri ihlalleri, siber saldırganlar tarafından analiz edilen hedef kurum ve kuruluşların sunucu veya sistemlerindeki açıkların sömürülmesi nedeni ile oluşuyor. Bu durum yeni olmadığı gibi ilk değil ve son olmayacak, İnternet var oldukça hep bir tehdit olacak. Bu tehdidin önüne geçmek açısından bir Güvenlik Operasyon Merkezi (Security Operation Center) kurulmuş ve bu merkezin içerisinde çalışan analiz ekibine de saldırıları anbean takip edebilecekleri bir sistem kurulmuştur. Bu merkezin temel amacı, siber güvenlik olaylarını 7/24 izleyecek, analiz edecek ve tehditlere karşı önlem alacak kişileri bir arada tutup; saldırı esnasında önlem almalarını sağlamaktır. SOC Fundamentals (temelleri) konusu, Siber Vatan bünyesinde bulunan Altay Takımı'nın ödevi olarak hazırlanmıştır.

SOC Fundamentals

SOC (Security Operations Center) yani Güvenlik Operasyon Merkezi, bir işletmedeki güvenlik tehditlerini izlemek, tespit etmek, analiz etmek ve bunlara yanıt vermekten sorumlu merkezi bir birim olarak görev yapar. Gerçek zamanlı olarak güvenliği tehdit edebilecek durumları izler, izinsiz girişleri tespit etmek veya önlemek için güvenlik duvarları, güvenlik bilgileri ve olay yönetimi (SIEM[1]) çözümleri gibi çeşitli güvenlik teknolojileri kullanır.

1. SOC Nasıl Çalışır?

1.1. İzleme

Güvenlik duvarlarından, saldırı tespit sistemlerinden ve sunuculardan gelen günlükler gibi çeşitli kaynaklardan veri ve bilgileri toplayıp analiz eder.

1.2. Tehdit Tespiti

Potansiyel güvenlik tehditlerini belirlemek ve bunlara karşı uyarıda bulunmak için SIEM çözümleri gibi çeşitli güvenlik araçları kullanır.

1.3. Analiz

Tespit edilen güvenlik olaylarının önem derecesini önceliklendirir, değerlendirir ve uygun eylem planını belirler.

1.4. Yanıt

Etkilenen sistemleri izole etme, tehdidi kontrol altına alma ve normal operasyonları geri yükleme gibi görevleri içerebilen güvenlik olaylarına yönelik yanıtı koordine eder ve yürütür.

1.5. Raporlama

Yönetim, denetçiler ve düzenleyiciler gibi paydaşlara güvenlik durumu ve güvenlik olayları hakkında düzenli raporlar sunar.

1.6. Sürekli iyileştirme

Yeni ve gelişen güvenlik tehditlerini tespit etmede ve bunlara yanıt vermede etkili olmasını sağlamak için süreç ve prosedürleri sürekli olarak gözden geçirir ve geliştirir.

SOC Türleri

- **Kendi Kendini Yöneten SOC:** Dahili personeli olan şirket içi bir modeldir.
- **Dağıtılmış SOC:** Harici bir hizmet sağlayıcıyla birlikte çalışan kısmi ve tam zamanlı çalışanlarla birlikte yönetilen bir modeldir.

---

[1] *SIEM: Security Information and Event Management yani Güvenlik Bilgileri ve Olay Yönetimi, bir ağda gerçek zamanlı olarak neler olduğunu inceler. Ağ ortamından çok büyük miktarda veri toplar, toplanan bu verilere log denir. Bu verileri birleştirerek insanlar tarafından erişilebilir hale getirir. Bkz: https://siberci.com/siem-nedir/*

- **Yönetilen SOC:** Üçüncü taraflar tarafından yönetilen bir modeldir.
- **Command SOC:** Bu model sadece istihbarat içgörüleri sağlar ve gerçek güvenlik operasyonlarını diğer SOC'lere bırakır.

SOC Seviyeleri

SOC seviyelerini çok katlı bir binaya benzetmek yanlış olmaz. Seviye 1'i zemin kat ve Seviye 2'yi bir üst kat olarak düşünürsek her seviye, siber tehditlere karşı savunmada çok önemli rollere sahip olsalar da odak noktaları ve sorumlulukları farklıdır.

a. SOC level 1

Sistemdeki şüpheli faaliyetlerin loglarını izler, temel güvenlik önlemlerine odaklanırlar. Şüpheli bir aktivite tespit ederlerse, aktivite hakkında mümkün olduğunca fazla bilgi toplarlar. Olayın zamanı, sistemi ihlal etmek için kullanılan IP adresi, sömürülen veya sömürülmeye açık olan güvenlik açığı gibi detaylar bir üst kademedeki sorumluya raporlar.

b. SOC level 2

Bu alanda çalışanlar genellikle veri güvenliği alanında birkaç yıllık deneyime sahiptirler. Bir alt kademedeki analistten gelen rapora göre, zararı değerlendirmek için olay araştırılır ve saldırganın sisteme verdiği/verebileceği zarara göre eylem alırlar.

c. SOC level 3

Açık kaynaklardan, DarkWeb'den istihbarat toplarlar. Güvenliği istismar edebilecek tehditleri araştırırlar. Bu şekilde veri korsanlarına, virüslere karşı daha bilinçli hareket ederler.

Sonuç

Bir SOC analisti, kademesine göre aldığı sorumlulukları gerçek zamanlı bir şekilde yerine getirir. Kullandığı yardımcı SIEM ürünleri ile izleme, tespit ve önleme gibi eylemleri gerçekleştiren SOC analisti, olası bir saldırı durumunda Cyber Kill Chain modelindeki adımlara göre saldırı aşamalarının tespiti ve önlenmesi konusunda bilinçli hareket eder. Bu aşamalardaki saldırı yöntemlerine göre alınabilecek önlemlerle saldırı erken aşamada tespit edilebilir, gerekli önlemler veri ihlali yaşamadan alınabilir.

Kaynakça

https://www.hosting.com.tr/blog/soc/

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

https://legendsof.tech/2021/06/24/soc-analyst-types-explained-tier-1-2-3/

https://24solutions.com.tr/soc-nedir-ve-soc-merkezleri-nasil-calisir/