07.02.2025

Blue Team Fundamentals

SOC Fundamentals & Cyber Kill Chain

HALİL İBRAHİM KORKUDAN
ALTAY TAKIMI

İçindekiler

Giriş

Günümüz dijital dünyasında siber tehditler her geçen gün daha karmaşık ve sofistike hale gelmektedir. Kuruluşların güvenlik operasyonlarını etkin bir şekilde yönetebilmeleri ve bu tehditlere karşı hızlı ve doğru yanıt verebilmeleri için Güvenlik Operasyon Merkezi (SOC) kritik bir rol oynamaktadır. SOC, kurumların siber güvenlik tehditlerini tespit etmek, analiz etmek ve bu tehditlere karşı gerekli müdahaleleri gerçekleştirmek amacıyla yapılandırılmış bir merkezdir.

Bu rapor, SOC'un temel yapı taşlarını, işleyişini ve organizasyonel yapısını detaylı bir şekilde ele almaktadır. Ayrıca, SOC içerisinde farklı seviyelerde görev yapan analistlerin sorumluluklarını, olay yönetimi süreçlerini ve kullanılan temel araçları açıklayarak, siber güvenlik dünyasında sağlam bir uzmanlık kazanmak isteyen profesyoneller için rehber niteliği taşımaktadır.

Raporda ayrıca, SOC'un siber güvenlik ekosistemindeki önemi ve proaktif savunma stratejileri incelenerek, Cyber Kill Chain modeli kapsamında bir saldırının nasıl gerçekleştiği ve bu saldırılara karşı alınabilecek önlemler detaylandırılmıştır. Bu kapsamlı içerik sayesinde, SOC ekosistemine dair geniş bir bakış açısı kazanabilir, siber güvenlik operasyonlarını etkin bir şekilde yönetmek için gerekli bilgi ve becerileri geliştirebilirsiniz.

SOC Fundamentals

Siber tehditlerin giderek daha sofistike hale gelmesi, kurumların güçlü bir güvenlik operasyon merkezi (SOC) oluşturmalarını zorunlu kılmaktadır. SOC, kuruluşların siber güvenliğini sağlamak, tehditleri tespit etmek ve etkin bir şekilde müdahale etmek için kritik bir bileşendir. SOC'un temel amacı, sürekli izleme, analiz ve yanıt süreçlerini entegre ederek organizasyonun güvenlik seviyesini en üst düzeye çıkarmaktır.

Bu doküman, SOC'un temel yapı taşlarını, işleyişini ve siber güvenlik ekosistemindeki rolünü ayrıntılı olarak ele almaktadır. SOC'un organizasyonel yapısını, kullanılan teknolojileri ve analist rollerini öğrenerek, siber güvenlik dünyasında güçlü bir uzmanlık kazanabilirsiniz. SOC Fundamentals eğitimi, siber güvenlik alanında çalışmak isteyen profesyoneller için kapsamlı bir rehber niteliğindedir.

SOC'un Temel Yapı Taşlarını ve İşleyişini Öğrenmek

SOC, siber güvenlik operasyonlarının merkezinde yer alarak tehditleri tespit eder, analiz eder ve uygun müdahalelerde bulunur. Etkin bir SOC'un oluşturulması için üç temel unsurun bir araya gelmesi gerekmektedir:

1. İnsanlar (People)

SOC'un en kritik bileşeni, bu merkezde görev alan uzmanlardır. Farklı uzmanlık alanlarına sahip güvenlik profesyonelleri, SOC'un verimli ve etkin çalışmasını sağlar:

- SOC Analistleri: Tehditleri tespit edip analiz eden ve olaylara müdahale eden uzmanlardır. L1, L2 ve L3 seviyelerine ayrılarak farklı derecede sorumluluk alırlar.
- Tehdit Avcıları (Threat Hunters): Proaktif olarak tehditleri araştıran ve saldırganların tespit edilmeden önce faaliyetlerini engellemeye çalışan uzmanlardır.
- Olay Müdahale Uzmanları: Gerçekleşen siber saldırıları analiz eden, zarar tespiti yapan ve sistemleri eski haline döndürmek için adli bilişim tekniklerini kullanan uzmanlardır.
- Güvenlik Mühendisleri: SOC'un altyapısını yöneten ve SIEM, IDS/IPS gibi araçların yapılandırılmasını sağlayan mühendislerdir.
- SOC Yöneticileri: SOC operasyonlarını yöneten, olay müdahale planlarını hazırlayan ve ekibin etkinliğini artıran yöneticilerdir.

2. Süreçler (Processes)

SOC'un etkili çalışması için belirli süreçlerin oturtulması gerekmektedir. Bu süreçler, güvenlik olaylarının yönetimini sistematik hale getirerek olaylara daha hızlı ve etkili müdahale edilmesini sağlar:

- Olay İzleme: SIEM ve ağ izleme araçları ile sistemlerin sürekli olarak izlenmesi sağlanır.

- Tehdit Tespiti: Anormal aktiviteler analiz edilerek, tehdit içeren olaylar belirlenir ve kritik seviyeye göre sınıflandırılır.
- Olay Müdahalesi: Tespit edilen güvenlik olaylarına hızlı yanıt verilir. Saldırgan aktiviteleri analiz edilir ve uygun aksiyonlar alınır.
- Adli Analiz: Gerçekleşen olayların detaylı incelenmesi, sistemlere verilen zararın belirlenmesi ve kanıtların toplanmasını kapsar.
- İyileştirme ve Önleme: Olay sonrası değerlendirme yapılır, güvenlik açıkları kapatılır ve gelecekte benzer olayların yaşanmaması için önleyici tedbirler alınır.

3. Teknoloji (Technology)

SOC'un etkili bir şekilde çalışabilmesi için gelişmiş güvenlik araçları ve teknolojiler kullanılmalıdır:

- SIEM (Security Information and Event Management): Logları toplayarak olayların ilişkilendirilmesini ve anomali tespitini sağlar.
- IDS/IPS (Intrusion Detection/Prevention Systems): Ağ trafiğini analiz ederek saldırı girişimlerini tespit eder ve engeller.
- EDR (Endpoint Detection and Response): Uç noktalardaki şüpheli aktiviteleri izleyerek zararlı yazılım bulaşmalarını tespit eder.
- SOAR (Security Orchestration, Automation and Response): Olay yönetimi süreçlerini otomatikleştirerek tehditlere daha hızlı müdahale edilmesini sağlar.
- Threat Intelligence (Tehdit İstihbaratı): Siber tehditlerle ilgili dış kaynaklardan bilgi toplayarak SOC analistlerine rehberlik eder.
- Gelişmiş Adli Analiz Araçları: Zararlı yazılımların incelenmesi, olayların geriye dönük analizi ve saldırganların izlerinin sürülmesi için kullanılır.

Bu üç temel bileşenin etkin bir şekilde entegrasyonu, SOC'un güçlü ve proaktif bir güvenlik yapısı oluşturmasını sağlar. SOC'un başarısı, uzman kadro, etkin süreçler ve gelişmiş teknolojilerin uyum içinde çalışmasına bağlıdır. Tehditlerin sürekli değiştiği günümüz siber güvenlik ortamında, SOC'un dinamik bir yapıya sahip olması ve sürekli olarak gelişmesi kritik öneme sahiptir.

SOC İçerisindeki Katmanlar (L1, L2, L3) ve Analist Rollerinin Sorumlulukları

SOC yapısı, olay yönetiminin etkin bir şekilde yürütülmesini sağlamak için üç temel analiz seviyesine ayrılmıştır. Her seviyenin kendine özgü sorumlulukları ve teknik uzmanlık gereksinimleri vardır.

Seviye 1 (L1) Analist - İlk Savunma Hattı

Seviye 1 analistler, SOC'un en temel savunma hattıdır ve olay yönetim sürecindeki ilk değerlendirme ve yönlendirme görevlerinden sorumludur.

- Gelen alarmları ve olayları inceler, önceliklendirir ve gerektiğinde L2'ye yönlendirir.
- SIEM, IDS/IPS ve diğer güvenlik izleme araçlarını kullanarak şüpheli aktiviteleri tespit eder.
- Otomatikleştirilmiş alarmların yanlış pozitif olup olmadığını değerlendirir.
- Zafiyet taramaları gerçekleştirerek riskli varlıkları belirler.
- Küçük ölçekli olaylara müdahale eder ve önleyici aksiyonlar alır.

Seviye 2 (L2) Analist - Olay Müdahale ve Derinlemesine Analiz

Seviye 2 analistler, Seviye 1 analistlerinden gelen olayları detaylı bir şekilde inceleyerek daha karmaşık olay yönetimi süreçlerini yürütür.

- Gelişmiş analiz yaparak saldırının kökenini ve yayılma yöntemlerini belirler.
- Tehdit istihbaratı verilerini değerlendirerek olası saldırı vektörlerini belirler.
- Kötü amaçlı yazılım analizi ve tersine mühendislik işlemlerini gerçekleştirir.
- Adli analiz yöntemleri ile saldırıların kaynağını ve etkilerini tespit eder.
- Siber güvenlik politikalarına uygun şekilde sistemleri güçlendirme planları oluşturur.
- Ağ trafiği analizleri yaparak anormal aktiviteleri belirler.

Seviye 3 (L3) Analist - Gelişmiş Tehdit Avcılığı ve Stratejik Güvenlik

Seviye 3 analistler, SOC'un en üst düzeyde uzmanlaşmış güvenlik profesyonelleridir. Olay yönetiminin ötesinde, stratejik güvenlik operasyonlarına odaklanırlar.

- Gelişmiş tehdit avcılığı (Threat Hunting) yaparak önceden tespit edilmemiş tehditleri belirler.
- Kurum içi güvenlik altyapısını optimize etmek için yeni güvenlik politikaları geliştirir.
- SOC ekibi için güvenlik analizleri yaparak en iyi güvenlik uygulamalarını belirler.
- Karmaşık siber saldırıları modelleyerek saldırganların olası hareketlerini öngörmeye çalışır.
- SOC tarafından kullanılan SIEM, SOAR ve diğer güvenlik araçlarının yapılandırılmasını yönetir.
- Sızma testi ve red teaming faaliyetlerine katılarak sistemlerin güvenliğini test eder.

SOC Yöneticisi - Operasyonel ve Stratejik Yönetim

SOC yöneticisi, operasyonların etkili ve verimli bir şekilde yürütülmesini sağlamakla yükümlüdür. Teknik bilgiye sahip olmasının yanı sıra operasyonel süreçleri yönetecek liderlik becerilerine de sahip olmalıdır.

- SOC ekibinin yönetiminden, işe alımlardan ve eğitim süreçlerinden sorumludur.
- Güvenlik olaylarını üst yönetime raporlar ve stratejik karar alma sürecine katkıda bulunur.
- SOC bütçesini yönetir ve yeni güvenlik çözümlerinin yatırım kararlarını alır.
- Uyumluluk ve düzenleyici gereksinimlerin yerine getirilmesini sağlar.
- SOC içindeki farklı ekipler arasında iletişim ve işbirliğini teşvik eder.
- SOC'un etkinliğini artırmak için otomasyon çözümleri ve süreç iyileştirmeleri geliştirir.

Bu katmanlı yapı sayesinde SOC, tehditleri daha etkili bir şekilde yönetebilir ve sürekli gelişen siber tehditlere karşı proaktif bir savunma sağlayabilir.

Bu rollerin her biri, SOC'un verimli çalışmasını sağlamak için kritik öneme sahiptir.

Olay Yönetimi Süreçlerini Kavramak

SOC'un en kritik süreçlerinden biri olay yönetimidir. Olay yönetimi, siber saldırıların etkilerini minimize etmek, olayları hızlı bir şekilde tespit edip müdahale etmek ve sistemleri daha dayanıklı hale getirmek için geliştirilmiş bir çerçevedir. SOC'daki olay yönetimi süreci, dört ana aşamadan oluşur:

1. İzleme (Monitoring)

SOC, SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems), uç nokta güvenlik çözümleri ve ağ trafiği izleme araçları gibi sistemler kullanarak 7/24 sürekli bir izleme gerçekleştirir. İzleme aşamasında yapılan işlemler:

- Log Toplama: SIEM sistemleri, ağ cihazlarından, güvenlik duvarlarından, uç noktalardan ve sunuculardan logları toplar.
- Tehdit Avcılığı: SOC analistleri, bilinen saldırı modellerine göre anormallikleri tespit etmek için tehdit istihbaratı ve makine öğrenimi destekli analizler yapar.
- Anomali Tespiti: Davranış analizi araçları kullanılarak, sistemlerde olağan dışı aktiviteler belirlenir.

2. Tespit (Detection)

Tehditlerin tespit edilmesi, SOC'un en önemli görevlerinden biridir. SIEM kuralları, ağ izleme araçları ve güvenlik analistlerinin manuel incelemeleri sayesinde zararlı aktiviteler belirlenir. Tespit aşamasında şu adımlar uygulanır:

- Alarm Yönetimi: SIEM ve IDS/IPS tarafından üretilen alarmlar değerlendirilerek önceliklendirilir.
- False Positive Ayıklama: Yanlış pozitif alarmlar elenerek gerçek tehditler belirlenir.
- Zafiyet Analizi: Olayın kaynağı, saldırı vektörleri ve potansiyel etkileri analiz edilir.

3. Yanıt Verme (Response)

Tespit edilen tehditlere karşı hızlı ve etkili bir şekilde müdahale edilmelidir. Yanıt süreci şu adımlardan oluşur:

- Olay İzolasyonu: Etkilenen sistemler ağdan izole edilerek saldırının yayılması engellenir.
- Zararlı Yazılım Analizi: Tespit edilen kötü amaçlı yazılımlar incelenerek bulaşma yöntemi ve etkileri belirlenir.
- Müdahale Planının Uygulanması: Önceden belirlenmiş olay müdahale planları devreye sokularak tehditlerin etkisi minimize edilir.
- Geri Yükleme (Recovery): Etkilenen sistemler temizlenir, güncellenir ve operasyonlar normale döndürülür.

4. İyileştirme ve Önleyici Tedbirler (Post-Incident Analysis & Prevention)

Olay sonrası süreçte, saldırının tekrar yaşanmaması için önleyici adımlar atılmalıdır. Bu aşamada şunlar gerçekleştirilir:

- Kapsamlı Olay Analizi: Olayın kök nedenleri incelenerek sistem açıkları belirlenir.
- Politika Güncellemeleri: Güvenlik politikaları, tespit edilen açıkları giderecek şekilde güncellenir.
- Personel Eğitimi: SOC analistleri ve diğer çalışanlar, olayın türüne göre bilgilendirilerek benzer tehditlere karşı daha iyi hazırlanmaları sağlanır.
- Yeni Güvenlik Önlemleri: IDS/IPS kurallarının güncellenmesi, ek güvenlik çözümlerinin devreye alınması ve SIEM sisteminde yeni korelasyon kurallarının oluşturulması gibi iyileştirmeler uygulanır.

Bu süreçlerin tamamı, olaylara hızlı ve etkili bir şekilde müdahale edilmesini sağlamakla birlikte, kuruluşun genel siber güvenlik olgunluğunu artırarak gelecekteki tehditlere karşı daha dirençli hale gelmesini sağlar.

SOC'da Kullanılan Temel Araçları Tanımak

SOC analistleri, tehditleri tespit etmek ve analiz etmek için çeşitli güvenlik araçlarını kullanır:

- SIEM (Security Information and Event Management): Ağdaki olayları merkezi olarak toplar, analiz eder ve korelasyon yaparak tehditleri belirler. SIEM sistemleri, büyük veri analitiği ile geçmişte yaşanan olayları da göz önünde bulundurarak anomali tespiti yapabilir.

- IDS/IPS (Intrusion Detection/Prevention Systems): İzinsiz giriş tespit ve önleme sistemleri, ağ trafiğini analiz ederek potansiyel saldırıları belirler. IDS yalnızca algılama yaparken, IPS aktif olarak saldırıları engeller.
- EDR (Endpoint Detection and Response): Uç nokta güvenliği sağlar ve uç noktalarda gerçekleşen şüpheli hareketleri analiz eder. EDR, kötü amaçlı yazılım bulaşmalarını tespit edebilir ve otomatik olarak zararlı süreçleri sonlandırabilir.
- SOAR (Security Orchestration, Automation and Response): SOC süreçlerini otomatik hale getirerek güvenlik analistlerinin olaylara daha hızlı müdahale etmesini sağlar. SOAR, tehdit istihbarat kaynakları ile entegre çalışarak saldırıların daha etkili bir şekilde tespit edilmesine yardımcı olur.
- DLP (Data Loss Prevention): Veri kaybını önleme sistemleri, hassas bilgilerin yetkisiz erişimini ve sızdırılmasını engellemek için kullanılır. DLP, e-posta trafiğini, bulut hizmetlerini ve uç noktaları denetleyerek veri ihlallerini tespit eder.
- XDR (Extended Detection and Response): SIEM, EDR ve SOAR gibi teknolojileri birleştirerek daha kapsamlı bir tehdit tespiti ve yanıt mekanizması sunar. XDR, tehditlerin daha geniş bir bağlamda ele alınmasını sağlar.
- UTM (Unified Threat Management): Güvenlik duvarı, antivirüs, antispam, IPS/IDS ve VPN gibi güvenlik çözümlerini tek bir sistemde birleştiren kapsamlı bir güvenlik çözümüdür.

Bu araçlar, SOC'un tehditlere hızlı ve etkili yanıt vermesini sağlamakla birlikte, güvenlik olaylarının daha hızlı tespit edilmesini ve minimize edilmesini mümkün kılar.

Siber Güvenlik Ekosisteminde SOC'un Önemini Kavramak

SOC, siber güvenlik dünyasında hayati bir rol oynar. SOC sayesinde kuruluşlar aşağıdaki faydaları elde eder:

- Tehditleri daha erken tespit eder: Sürekli izleme sayesinde saldırılar erken aşamada yakalanır.
- Veri ihlallerini önler: Kritik sistemler korunarak veri sızıntıları engellenir.
- Güvenlik operasyonlarını optimize eder: Tehdit avcılığı, analiz ve olay yönetimi süreçleriyle organizasyon daha güvenli hale gelir.
- Yasal ve düzenleyici gerekliliklere uyum sağlar: SOC, güvenlik politikalarının uygulanmasını sağlayarak organizasyonun yasal zorunluluklara uyumunu destekler.

Cyber Kill Chain: Siber Saldırılarının Yaşam Döngüsü ve Proaktif Savunma Stratejileri

Cyber Kill Chain Nedir?

Cyber Kill Chain, Lockheed Martin tarafından geliştirilen ve siber saldırıların aşamalarını sistematik bir şekilde analiz eden bir güvenlik modelidir. Bu model, saldırının her aşamasını tanımlayarak tehditlerin anlaşılmasını ve engellenmesini sağlar. SOC (Security Operations Center) analistleri ve siber güvenlik uzmanları, bu model sayesinde saldırıları tespit edip durdurabilir ve proaktif savunma stratejileri geliştirebilirler.

Bu modelin temel amacı, bir saldırının hangi aşamada olduğunu belirleyerek, her aşamaya yönelik uygun güvenlik önlemleri almaktır. Böylece tehditleri erken tespit etmek ve saldırıların ilerlemesini engellemek mümkün hale gelir.

Cyber Kill Chain Aşamaları

1. Reconnaissance (Keşif)

Saldırganın hedef hakkında bilgi topladığı aşamadır. Bilgi toplama yöntemleri şu şekilde ikiye ayrılır:

- Pasif Bilgi Toplama: Hedef sistemle doğrudan temas kurmadan yapılan bilgi toplama faaliyetleridir. Açık kaynak istihbaratı (OSINT), sosyal medya taramaları, halka açık veriler ve iş ilanları gibi kaynaklar bu süreçte kullanılır.
- Aktif Bilgi Toplama: Hedefle doğrudan temas gerektiren bilgi toplama faaliyetleridir. Port taramaları, ağ analiz araçları ve phishing saldırıları gibi yöntemlerle hedefin güvenlik açıkları belirlenir.

Savunma Mekanizmaları:

- Honeypot sistemleri kullanarak saldırganların keşif aşamasında belirlenmesi
- Çalışanların sosyal mühendislik saldırılarına karşı eğitilmesi
- OSINT izleme araçları ile saldırgan faaliyetlerin tespiti

2. Weaponization (Silahlanma)

Saldırgan, keşif aşamasında elde ettiği bilgiler doğrultusunda saldırıyı gerçekleştirmek için zararlı araçlar hazırlar. Bu aşamada kullanılan bazı yöntemler şunlardır:

- Özel olarak hazırlanmış zararlı yazılımlar (malware, rootkit, trojan, ransomware vb.)
- Sosyal mühendislik saldırılarına uygun phishing içerikleri ve sahte web siteleri
- Güvenlik açıklarını istismar eden özel exploitler ve payloadlar

Savunma Mekanizmaları:

- Tehdit istihbarat sistemleri ile yeni zararlı yazılımların takibi
- Exploit koruma sistemlerinin (IPS/IDS) aktif edilmesi

- Şirket içi güvenlik politikalarının belirlenmesi ve uygulamaya konulması

3. Delivery (İletim)

Hazırlanan zararlı yazılımın veya saldırı aracının hedef sisteme ulaştırıldığı aşamadır. Saldırganlar bu aşamada şu yöntemleri kullanabilir:

- Phishing e-postaları ile zararlı bağlantı veya ek dosya gönderme
- Sahte web siteleri ile kullanıcıları kimlik bilgilerini paylaşmaya yönlendirme
- USB bellek gibi fiziksel medya kullanarak zararlı yazılım yayma

Savunma Mekanizmaları:

- E-posta filtreleme sistemleri ile phishing e-postalarının engellenmesi
- Web filtreleme teknolojileri kullanarak zararlı sitelere erişimin kısıtlanması
- Çalışanlara siber güvenlik farkındalık eğitimlerinin verilmesi

4. Exploitation (Sömürme)

Bu aşamada saldırgan, hedef sisteme erişim sağlamak için zararlı yazılımı çalıştırır veya güvenlik açıklarını istismar eder. Saldırının başarılı olması için aşağıdaki yöntemler kullanılır:

- Hedef sistemdeki güncellenmemiş yazılımlar üzerinden exploit çalıştırma
- Kullanıcıları zararlı bağlantılara tıklamaya yönlendirerek kod yürütme
- Güvensiz sistem yapılandırmalarını kötüye kullanma

Savunma Mekanizmaları:

- Güncellemelerin ve yamaların düzenli olarak uygulanması
- Antivirus ve EDR (Endpoint Detection and Response) çözümlerinin kullanılması
- Güvenlik açıklarının düzenli olarak taranması
-

5. Installation (Yükleme)

Saldırgan, hedef sistem üzerinde kalıcı bir tehdit oluşturmak için zararlı yazılımı sisteme entegre eder. Bu aşamada saldırganlar şunları yapabilir:

- Arka kapılar (backdoors) oluşturarak kalıcı erişim sağlama
- Rootkit gibi araçlarla zararlı yazılımları gizleme
- Kullanıcı haklarını yükselterek sistemde daha fazla kontrol elde etme

Savunma Mekanizmaları:

- Uygulama beyaz listeleme ve kara listeleme politikalarının uygulanması

- Yetkisiz yazılım yüklemelerinin engellenmesi
- Güvenlik denetimlerinin ve log analizlerinin yapılması

6. Command & Control (Komuta ve Kontrol)

Hedef sistem ele geçirildikten sonra saldırgan, sistemle uzaktan iletişim kurarak komutlar gönderebilir. Bu aşamada şu teknikler kullanılır:

- C2 (Command & Control) altyapısı oluşturarak saldırıyı yönetme
- Şifrelenmiş trafik ile zararlı faaliyetleri gizleme
- DNS veya HTTP tabanlı gizli iletişim kanalları kullanma

Savunma Mekanizmaları:

- Ağ izleme ve anormal trafik tespit sistemlerinin kullanılması
- Şüpheli IP ve domain adreslerinin engellenmesi
- Proxy ve firewall kurallarının sıkılaştırılması

7. Actions on Objectives (Eylem)

Bu aşamada saldırgan, asıl amacını gerçekleştirmek için sistem üzerinde zararlı faaliyetlerde bulunur. Bu faaliyetler şunları içerebilir:

- Hassas verilerin çalınması (veri sızıntısı)
- Fidye yazılımları ile dosyaların şifrelenmesi
- Sistemleri çökertme veya hizmet dışı bırakma (DDoS saldırıları)

Savunma Mekanizmaları:

- Veri kaybı önleme (DLP) sistemlerinin kullanılması
- Hassas verilerin yedeklenmesi ve şifrelenmesi
- Anormal kullanıcı aktivitelerinin izlenmesi

Örnek Saldırı Senaryosu: Bir Finans Kuruluşuna Yönelik Siber Saldırı

1. Reconnaissance (Keşif)

- Saldırgan, büyük bir finans kuruluşunu hedef alır ve açık kaynak istihbarat (OSINT) tekniklerini kullanarak kurum hakkında bilgi toplar. Şirketin çalışanlarının LinkedIn hesaplarını analiz eder, e-posta adreslerini bulur ve şirketin güvenlik açıklarını tespit edebilmek için halka açık sistemlerini inceler. Aynı zamanda, phishing saldırısı düzenlemek için çalışanların e-posta adreslerini ve sosyal medya alışkanlıklarını değerlendirir.

2. Weaponization (Silahlanma)

- Saldırgan, elde ettiği bilgiler doğrultusunda özel bir phishing e-postası hazırlar. Bu e-posta, şirketin IT ekibinden geliyormuş gibi gösterilir ve içeriğinde "güvenlik güncellemesi" adı altında bir zararlı yazılım içeren sahte bir bağlantı bulunur. E-posta, hedef çalışanları kandırarak zararlı yazılımı indirmeye yönlendirecek şekilde tasarlanmıştır.

3. Delivery (İletim)

- Saldırgan, hazırladığı phishing e-postasını şirket çalışanlarına gönderir. E-posta içeriği oldukça ikna edici olduğu için birkaç çalışan bağlantıya tıklar ve zararlı yazılımı indirir. Aynı zamanda, saldırgan USB bellek yoluyla da zararlı yazılımı içeri sokmayı planlamaktadır.

4. Exploitation (Sömürme)

- Çalışanlardan biri, sahte güvenlik güncellemesini çalıştırır. Yazılım, şirketin iç sistemlerinde kritik bir güvenlik açığını kullanarak uzaktan kod yürütülmesine izin verir. Böylece saldırgan, sistemde yönetici ayrıcalıkları elde eder ve iç ağdaki diğer makineleri taramaya başlar.

5. Installation (Yükleme)

- Saldırgan, sistemde kalıcı bir tehdit oluşturmak için bir arka kapı (backdoor) yerleştirir. Aynı zamanda, bir keylogger yükleyerek çalışanların giriş bilgilerini kaydeder. Erişimini genişletmek için kötü amaçlı yazılımı diğer cihazlara da yaymaya çalışır.

6. Command & Control (Komuta ve Kontrol)

- Saldırgan, hedef sistemle uzaktan iletişim kurabilmek için bir komuta ve kontrol (C2) altyapısı kurar. Sisteme yerleştirdiği zararlı yazılım, saldırganın belirlediği uzak bir sunucuya bağlanarak veri göndermeye başlar. Bu aşamada, saldırgan şirketin ağ trafiğini izleyebilir ve sistemlere müdahale edebilir.

7. Actions on Objectives (Eylem)

- Saldırganın nihai amacı finansal verilere ulaşmak ve bunları çalmaktır. Erişimini kullanarak müşteri hesaplarına ait hassas bilgileri kopyalar ve şifreli bir kanal üzerinden dışarıya sızdırır. Aynı zamanda, sistemlerin çökmesine neden olabilecek fidye yazılımını devreye alarak şirketten fidye talep edebilir.

Sonuç

SOC Fundamentals eğitimi, SOC'un yapı taşlarını ve işleyişini anlamak isteyenler için kapsamlı bir yol haritası sunar. Katılımcılar, SOC organizasyonunu, analist rollerini, olay yönetimi süreçlerini ve kullanılan araçları öğrenerek, bu alanda daha bilinçli ve yetkin hale gelirler. Siber güvenlik dünyasında başarılı bir kariyer için SOC'un temel prensiplerini kavramak büyük bir avantaj sağlar.Cyber Kill Chain modeli, siber saldırıların her aşamasını tanımlayarak savunma stratejilerinin geliştirilmesine yardımcı olur. SOC ekipleri ve güvenlik uzmanları, bu modeli kullanarak tehditleri erken tespit edebilir ve saldırıları daha başlangıç aşamalarında engelleyebilir. Güçlü siber savunma mekanizmaları ile saldırganların her aşamadaki ilerleyişi durdurulabilir ve organizasyonların güvenliği artırılabilir. Bu rapor, Güvenlik Operasyon Merkezi (SOC) kavramının temel yapı taşlarını, işleyişini ve siber güvenlik ekosistemindeki kritik rolünü detaylı bir şekilde ele almıştır. Siber tehditlerin sürekli geliştiği bir ortamda, SOC'un etkin bir şekilde çalışması, kuruluşların güvenlik seviyelerini artırmak ve tehditlere hızlı müdahale edebilmek için hayati önem taşımaktadır. Raporda, SOC'un organizasyonel yapısı, olay yönetimi süreçleri, kullanılan güvenlik araçları ve farklı seviyelerdeki analist rollerinin sorumlulukları açıklanmıştır. Ayrıca, Cyber Kill Chain modeli kapsamında bir saldırının aşamaları detaylandırılmış ve olası bir saldırı senaryosu üzerinden bu aşamaların nasıl işlediği değerlendirilmiştir. Bu araştırma sonucunda, SOC'un etkili çalışması için insan, süreç ve teknoloji bileşenlerinin uyum içinde olması gerektiği anlaşılmıştır. SOC analistlerinin görev tanımlarını net bir şekilde anlamak, doğru güvenlik araçlarını kullanmak ve olay yönetimi süreçlerini iyi kavramak, başarılı bir güvenlik operasyonunun temel taşlarını oluşturmaktadır.

Sonuç olarak, SOC ekiplerinin proaktif tehdit avcılığı yaparak siber saldırıları daha erken tespit edebilmesi ve güçlü savunma stratejileri oluşturabilmesi, kurumların siber güvenliğini sağlamak için kritik bir gerekliliktir. Bu rapor, siber güvenlik alanında çalışmak isteyen profesyoneller için kapsamlı bir rehber niteliğinde olup, SOC dünyasında başarılı bir kariyer inşa etmek isteyenler için önemli bir kaynak sunmaktadır.

Kaynakça

https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/cyber-kill-chain/

https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html

https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu

https://docs.yavuzlar.org/web-guvenligi/cyber-kill-chain

https://app.letsdefend.io/training/lesson_detail/introduction-to-soc

https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir

https://tryhackme.com/room/socfundamentals

Cyber Security Analysis of Turkey - Hakan Şentürk, C. Zaim Çil, Şeref Sağıroğlu