SOC Fundamentals

Hazırlayan: Saliha Polat

Tarih: 07.02.2025

İçindekiler

Giriş

Teknolojinin hızla gelişmesi ve dijitalleşmenin yaygınlaşmasıyla birlikte siber güvenlik, kurumlar için en önemli önceliklerden biri haline gelmiştir. Günümüzde şirketler, devlet kurumları ve diğer organizasyonlar, siber tehditlerin sürekli artan ve gelişen doğasıyla başa çıkabilmek için çeşitli güvenlik önlemleri almak zorundadır. Bu noktada, Güvenlik Operasyon Merkezleri (SOC – Security Operations Center), kurumların siber güvenliğini sağlamak, tehditleri tespit etmek ve olası saldırılara karşı hızlı müdahalede bulunmak amacıyla kritik bir görev üstlenir.

SOC, güvenlik olaylarını 7/24 izleyen, analiz eden ve gerekli aksiyonları alan bir yapıdır. Kurumların güvenlik açıklarını belirleyerek, veri ihlallerini önlemelerine ve sistemlerini güvende tutmalarına yardımcı olur. Bu merkezler, sadece tehdit tespiti yapmakla kalmaz, aynı zamanda olay müdahale süreçlerini yönetir, sistem güvenliğini sürekli olarak iyileştirmek için çalışmalar yürütür ve güvenlik politikalarını geliştirir.

Bu yazıda, SOC' un temel işlevleri, görevleri, yapısı, türleri ve çalışma süreci gibi konular ele alınacaktır. Ayrıca, SOC'larda kullanılan sistemler ve güvenlik olaylarının nasıl raporlandığına dair önemli bilgiler sunulacaktır. Siber güvenlik alanında etkili bir savunma mekanizması oluşturan SOC'ların çalışma prensipleri ve işleyişi hakkında kapsamlı bir bakış açısı kazanmanız amaçlanmaktadır.

SOC (Güvenlik Operasyon Merkezi) Nedir?

SOC (Güvenlik Operasyon Merkezi), bir kuruluşun güvenliğini devamlı olarak izleyen ve güvenlik olaylarının analizinden sorumlu bilgi güvenliği ekibinin bulunduğu yerdir. Bu ekip, siber güvenlik olaylarının tespiti, önlenmesi ve bunlarla ilgili olarak aksiyon alınmasını sağlayan, aynı zamanda kurumların güvenlik duruşunu sürekli olarak izlemek ve iyileştirmek için teknolojiyi, süreçleri ve insan gücünü kullanan merkezi bir fonksiyondur.

Ekip, tüm güvenlik sistemlerini gerçek zamanlı olarak taramaktan sorumludur. Bu ilk savunma hattı, bir organizasyonun güvenlik altyapısını olası siber tehditlerden korumak için günün her saati çalışır.

SOC (Güvenlik Operasyon Merkezi) Ne Yapar?

SOC, olası güvenlik olaylarını doğru bir şekilde tanımlamak, analiz etmek, savunmak, araştırmak ve raporlamaktan sorumludur. Ağ altyapısı, bilgisayar sunucuları, çok sayıda uç nokta, uygulamalar, web sayfaları ve diğer varlıklar, bir güvenlik tehdidi veya ihlaline işaret edebilecek olağandışı davranışları kontrol eden güvenlik operasyon merkezlerinde izlenir ve analiz edilir.

Çoğu SOC, kesintisiz çalışır ve çalışanlar, güvenlik araçları kullanarak faaliyetleri kaydeder, anormallikleri analiz eder ve siber tehditleri ve kötü amaçlı yazılımları ortadan kaldırır. SOC ekipleri diğer takımlar ve departmanlarla iş birliği yapabilir.

SOC' un Görevleri

SOC ekipleri ağlardaki, sunuculardaki, veri tabanlarındaki, uygulamalardaki, web sitelerindeki ve diğer sitemlerdeki etkinlikleri izler ve analiz eder, bir güvenlik olayı veya tavizinin göstergesi olabilecek anormal etkinlikleri tarar.

Temel SOC görevleri:

- **Yönetim ve Bakım:** Güncellemeler ve yamalar dahil olmak üzere araçlar izlenir ve yönetilir.
- **Sürekli İzleme:** SOC, güvenlik ihlallerine dair herhangi bir işaret aramak için bir organizasyonun BT altyapısını sürekli olarak izler. Güvenlik duvarları, saldırı tespit sistemleri (IDS) ve saldırı önleme sistemleri (IPS) gibi çeşitli kaynaklardan veri toplamak ve analiz etmek için gelişmiş izleme araçları ve teknolojilerinin kullanılmasını içerir.
- **Olay Algılama ve Müdahale:** Olası bir tehdit algılanırsa, SOC olayın ciddiyetini ve iş etkisini belirlemek için olayı araştırmaktan sorumludur. SOC ekibi daha sonra etkilenen sistemleri izole etmek, yamalar uygulamak veya daha derinlemesine düzeltme taktikleri uygulamak gibi tehdidi azaltmak için uygun önlemleri alır.

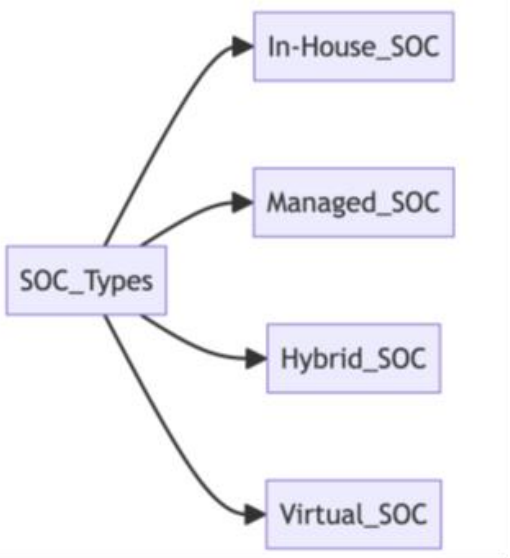
- **Tehdit İstihbaratı:** SOC analistleri, olası tehditlerin önünde kalmak için tehdit istihbaratından yararlanır. Bu, siber güvenlik haber akışları, tehdit istihbarat platformları ve bilgi paylaşım ve analiz merkezleri (ISAC'ler) gibi çeşitli dış kaynaklardan ortaya çıkan tehditler ve güvenlik açıkları hakkında bilgi toplamayı ve analiz etmeyi içerir.

- **Olay Yönetimi:** Etkili olay yönetimi, bir SOC'nin işlevi için kritik öneme sahiptir. Buna, olay müdahale planlarının geliştirilmesi ve izlenmesi, güvenlik olaylarından ders çıkarmak için olay sonrası analiz yapılması ve güvenlik protokollerinin ve süreçlerinin sürekli olarak iyileştirilmesi dahildir.

- **Kurtarma ve Düzeltme:** Hangi varlıkların saldırıya uğradığını inceler, kaybolan veya çalınan verileri kurtarır, uyarı araçlarını günceller ve prosedürlerin yeniden değerlendirilmesini sağlar.
  Ayrıca yedekleme sistemleri, güncellemeler ve yeniden yapılandırmalar yoluyla kaybolan veya güvenliği ihlal edilmiş verileri kurtarmayı amaçlar.

- **Uyumluluk ve Raporlama:** SOC ayrıca kuruluşların ilgili veri koruma düzenleyici gerekliliklerine uymasını ve sektör standartlarını sürdürmesini sağlama yükünü de taşır. Bu, denetimler ve düzenleyici uyumluluk için kritik öneme sahip olan güvenlik olayları ve bunları ele almak için alınan önlemler hakkında ayrıntılı raporlar oluşturmayı içerir.

SOC Türleri



In-House SOC (Şirket içi/Dahili SOC): Kuruluş tarafından yönetilen ve işletilen bu tür, güvenlik operasyonları üzerinde tam kontrol sağlar. Dahili bir SOC, kaynaklar ve yetenekli profesyoneller açısından oldukça talepkârdır. Bu nedenle, yalnızca büyük kuruluşlar veya kritik daha büyük ağları izlemekten sorumlu olanlar için uygulanabilirdir.

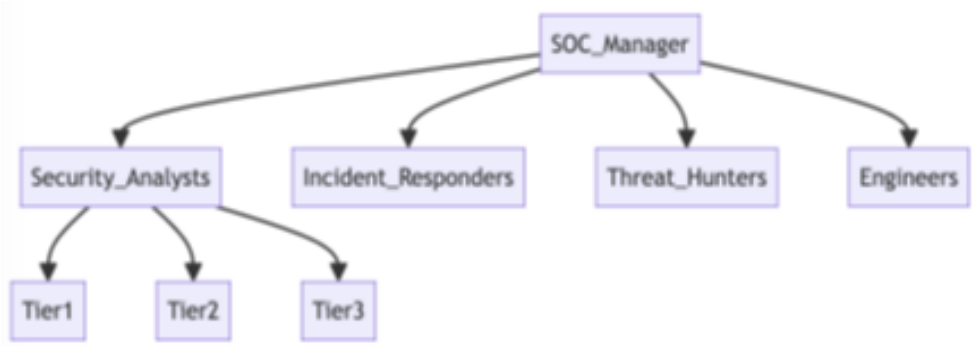
Managed SOC (Yönetilen SOC): Bu tür, tüm SOC işlemlerini yöneten bir Yönetilen Güvenlik Hizmet Sağlayıcısına (MSSP) dış kaynaklıdır. Bu seçenek, şirket içi bir SOC oluşturmak için daha fazla kaynağa ihtiyaç duyacak kuruluşlar için maliyet açısından etkilidir.

Hybrid SOC (Hibrit SOC): Bu tür, hem şirket içi hem de yönetilen SOC'lerin unsurlarını birleştirir. Kuruluş, belirli işlevler için harici uzmanlık ve kaynaklardan yararlanırken güvenlik operasyonları üzerinde bir miktar kontrole sahip olur.

Virtual SOC (Sanal SOC): Bu, analistlerin ve araçların tek bir fiziksel konumda bulunmadığı merkezi olmayan bir SOC' dur. Bu model, esneklik ve ölçeklenebilirlik sağlamak için bulut tabanlı araçlardan ve uzak ekiplerden yararlanır (Houghton, 2021).

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

SOC Yapısı



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.

Security Analysts: Sistemleri izleyen, uyarıları analiz eden ve olayları araştıran ön saflardaki savunuculardır. Genellikle deneyim ve uzmanlıklarına göre seviyelere (1., 2. ve 3. Kademe) ayrılırlar.

1.Seviye: Alert Analyst (Uyarı Analisti)

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.Seviye: Incident Responder (Olay Müdahale Görevlisi)

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.Seviye: Matter Expert/Hunter (Konu Uzmanı/Avcı)

Seviye 1 ve 2 analistlerinin yetkinliklerinin yanında veri görselleştirme araçlarına hâkim 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.

Threat Hunter: 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. Bu profesyoneller, otomatik araçların tespit edemediği tehditleri ararlar. Potansiyel riskleri şekillenmeden önce belirlemek ve azaltmak için gelişmiş teknikler ve tehdit istihbaratı kullanırlar.

SOC Engineers: SOC mühendisleri, SOC'nin teknik altyapısını/kaynaklarını sürdürmek ve optimize etmekten sorumludur. Bu, güvenlik araçlarını yapılandırmayı ve yönetmeyi, bunları güncellemeyi ve gerektiğinde yeni teknolojileri entegre etmeyi/uygulamayı içerir (Bykowski, 2023).

SOC' un Çalışma Süreci

1)Koruma: Önlem alınan adımdır. Bu aşamada öncelik dereceleri belirlenir. 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)Tespit: 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)Geri 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 da Kullanılan Sistemler

1)IDS (Intrusion Detection Systems):

Ağ trafiğiniz içerisindeki zararlı hareketleri veya zararlı bağlantıların tespiti için kullanılan sistemlere verilen addır. IDS güvenlik sistemlerinin amacı zararlı hareketi tanımlama ve loglama yapmaktır. Yani kısaca gelen saldırıyı algılamak ve loglamak için kullanılır.

2)IPS (Intrusion Prevention Systems):

Ağ trafiğiniz içerisindeki zararlı hareketleri veya zararlı bağlantıların tespitiyle birlikte önlenmesi için kullanılan güvenlik sistemleridir. 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 (Security Information Event Management):

SIEM sistemlerini, log üreten değil logları toplayan, anlamlandıran ve alarm üreten merkezi bir loglama ve log yönetimi bileşeni olarak tanımlayabiliriz.

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.

SOC Raporlaması

SOC Raporu Nedir?

SOC (Security Operations Center) raporu, bir güvenlik operasyonları merkezi tarafından ağ trafiği, güvenlik olayları ve tehdit tespitine ilişkin analizleri içeren bir belgedir. SOC raporları, bir organizasyonun siber güvenlik durumu hakkında bilgi sağlamak ve güvenlik açıklarını belirlemek amacıyla hazırlanır.

SOC Raporunda Seviyelere Göre Bulunması Gerekenler

L1 Raporu: Olay Tespiti ve Temel Müdahale

- Olay Özeti (Tarih, saat, olayın türü)
- Tespit Edilen Güvenlik Olayı (SIEM alarmları, etkilenen sistemler)
- İlk Analiz ve Tehdit Seviyesi
- Önerilen İlk Aksiyonlar (Hızlı müdahale adımları)
- Sonraki Adımlar (L2'ye aktarım gerekip gerekmediği)

L2 Raporu: Derinlemesine Analiz ve Olay Yönetimi

- Başlık ve Olay Özeti (L1'den gelen bilgiler)
- Detaylı Olay Analizi (Nasıl gerçekleşti? Kaynak ve hedef sistemler)
- Adli Bilişim Bulguları (Log analizi, zararlı IP'ler, dosya hash'leri)
- Alınan Müdahale Aksiyonları (Sistemin temizlenmesi, erişim kontrolü)
- Önerilen Güvenlik Önlemleri (Gelecekteki riskleri önleme)
- Sonraki Adımlar (L3'e yönlendirme gerekliliği)

L3 Raporu: İleri Düzey Tehdit Avcılığı ve Stratejik Güvenlik Önlemleri

- Başlık ve Yönetici Özeti
- Kök Neden Analizi (RCA) (Saldırının nasıl başladığı)
- Tehdit Avcılığı ve Adli Bilişim Bulguları (Hafıza analizi, PCAP verileri)
- Saldırganın Taktikleri (MITRE ATT&CK)
- Stratejik Güvenlik Önerileri (Altyapı değişiklikleri, tehdit istihbaratı)
- Sonuç ve Yönetim İçin Öneriler (İş süreçlerine etkisi, finansal risk analizi)

Sonuç

Siber tehditlerin giderek arttığı günümüz dijital dünyasında, Güvenlik Operasyon Merkezleri (SOC) kurumların veri güvenliğini sağlamak, siber saldırıları tespit etmek ve bu tehditlere karşı hızlı müdahalede bulunmak için kritik bir rol oynamaktadır. SOC, sürekli izleme, tehdit analizi, olay müdahalesi ve güvenlik iyileştirmeleriyle organizasyonların siber savunmasını güçlendiren önemli bir yapı olarak öne çıkar.

Doğru bir şekilde uygulandığında, Güvenlik Operasyon Merkezi (SOC) bir kuruluşa birçok avantaj sunabilir. Bu avantajlar arasında sürekli güvenlik izleme ve şüpheli aktivitelerin analizi, güvenlik olaylarına daha hızlı ve etkili müdahale, ihlal anından tespit edilene kadar geçen sürenin kısaltılması, yazılım ve donanım varlıklarının merkezi bir sistem altında toplanması yer alır. Bu merkezler, iletişim ve iş birliğini geliştirirken, siber güvenlik olaylarından kaynaklanan maliyetleri de minimize eder. Ayrıca, müşteriler ve çalışanlar hassas bilgi paylaşımında daha rahat ederken, güvenlik operasyonları üzerinde daha fazla şeffaflık ve kontrol sağlanır. Eğer kuruluş, siber suçlarla ilgili hukuki süreç başlatmayı planlıyorsa, verilerin kontrol zinciri de burada kurulmuş olur.

Başarılı bir SOC yönetimi, yalnızca güvenlik olaylarını tespit etmekle kalmaz, aynı zamanda tehditleri önceden belirleyerek proaktif bir güvenlik yaklaşımı benimser. Bu süreçte kullanılan gelişmiş güvenlik sistemleri, tehdit istihbaratı ve detaylı raporlama mekanizmaları, siber saldırılara karşı daha etkin bir koruma sağlamaya yardımcı olur.

Sonuç olarak, güvenlik operasyon merkezleri, siber güvenlik stratejisinin ayrılmaz bir parçasıdır ve kurumların güvenlik risklerini minimize etmek için sürekli olarak gelişmeye devam etmesi gereken bir alandır. Güçlü bir SOC yapısı, organizasyonlara yalnızca savunma sağlamakla kalmaz, aynı zamanda güvenlik açıklarını önceden tespit ederek uzun vadeli siber güvenlik politikalarının oluşturulmasına da katkıda bulunur.

Kaynakça

Şahin, A. B. (2021). *SOC Nedir?*. Medium. Erişim Linki

BGA Security. (2021). *SOC Ekipleri İçin Kullanıma Hazır Açık Kaynak Çözümler*. Erişim Linki

KoçSistem. (2021). *Güvenlik Operasyon Merkezi (SOC)*. Erişim Linki

Berqnet. (2021). *SOC (Security Operations Center) Nedir?*. Erişim Linki

Hosting.com.tr. (2021). *SOC Nedir ve Nasıl Çalışır?*. Erişim Linki

İHS Teknoloji. (2021). *Güvenlik Operasyon Merkezi (SOC) Nedir?*. Erişim Linki

Bulutistan. (2021). *SOC – Güvenlik Operasyon Merkezi Nedir?*. Erişim Linki

Secromix. (2021). *SOC Başlangıç Kılavuzu*. Erişim Linki

Gais Security. (2021). *SOC Nedir ve SOC Merkezleri Nasıl Çalışır?*. Erişim Linki

Microsoft. (2021). *What is a Security Operations Center (SOC)?*. Erişim Linki

EC-Council. (2021). *What is SOC (Security Operations Center)?*. Erişim Linki

GBHackers. (2021). *How to Build and Run a Security Operations Center?*. Erişim Linki