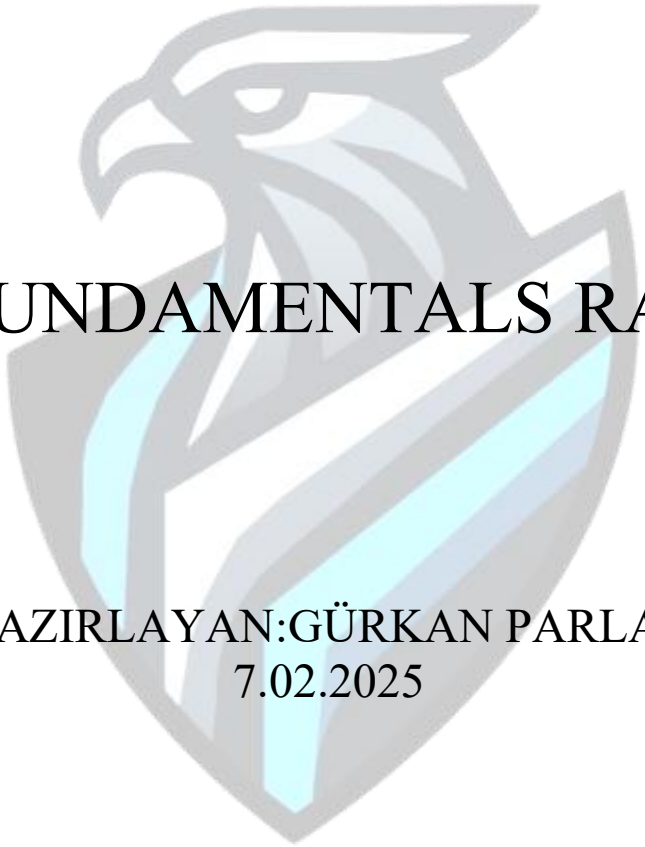
ALTAY TAKIMI



SOC FUNDAMENTALS RAPORU

HAZIRLAYAN:GÜRKAN PARLAK
7.02.2025

İçindekiler

SOC Nedir?

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.

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 Amaçları

SOC amacı,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.

Kısaca SOC'un amacı,Bir teknoloji çözümleri ve güçlü bir dizi süreç kombinasyonu kullanarak siber güvenlik olaylarını tespit etmek, analiz etmek ve bunlara yanıt vermektir.

SOC'un Görevleri

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.

SOC Analisti

SOC analistleri, güvenlik olaylarını tespit etmek, analiz etmek ve yanıtlamak için temel sorumluluğa sahiptir. Genellikle 3 seviyede sınıflandırılır:

Seviye 1 (L1) SOC Analisti

L1 SOC analistleri, sistemlerden gelen güvenlik olaylarını izleyen ve ön analiz yapan kişilerdir.

- Logları, uyarıları ve güvenlik olaylarını gerçek zamanlı olarak izler.
- Güvenlik izleme araçlarını yönetir, gelen uyarıları gözden geçirir ve olayların önem derecesini belirler.
-Saldırı sinyali veren alarmlar için ticket oluşturur ve bunu seviye 2 yani üst yöneticiye haber verir.

Seviye 2 (L2) SOC Analisti

L2 SOC analistleri, L1 tarafından yönlendirilen olayları detaylı bir şekilde analiz eden ve müdahale eden kişilerdir.

- Zararlı yazılım analizi yapmak.
- Logları ve sistem olaylarını detaylı incelemek.
- Ağ trafiği analizi yaparak şüpheli aktiviteleri belirlemek.
- IDS/IPS, EDR gibi araçları kullanarak saldırı vektörlerini anlamak.
- Saldırıyı doğruladıktan sonra olay müdahalesi başlatmak.

Seviye 3 (L3) SOC Analisti

L3 SOC analistleri, gelişmiş tehditleri analiz eden, saldırıların kök nedenini belirleyen ve tehdit avcılığı yapan kişilerdir.

- Tehdit avcılığı (Threat Hunting) yapmak.
- MITRE ATT&CK çerçevesine uygun saldırı analizleri gerçekleştirmek.
- Siber tehdit istihbaratı kullanarak olası saldırıları tahmin etmek.
- SIEM üzerinde özel algılama kuralları yazmak.
- Olay müdahale süreçlerini SOAR ile otomatikleştirmek.

Tehdit İstihbaratı Analisti

Bu analistler, dünyadaki siber tehditleri takip eden ve kurumun güvenlik stratejisini buna göre belirleyen kişilerdir.

- Güncel tehdit istihbarat raporlarını takip etmek.
- Dark web üzerinde tehdit araştırmaları yapmak.
- Yeni tespit edilen zararlı yazılımları analiz etmek.
- Tehdit istihbaratı platformlarını kullanarak saldırıları önceden tahmin etmek.

Adli Bilişim Analisti

Bu analistler, siber olayların sonrasında dijital kanıtları inceleyerek saldırının nasıl gerçekleştiğini ortaya çıkarır.

- Ele geçirilen sistemlerin adli analizini yapmak.
- Memory ve disk analizleri gerçekleştirmek.
- Zararlı dosyaların Hash ve imzalarını incelemek.
- Saldırganın kimliğini belirlemeye yönelik çalışmalar yapmak.

Olay Müdahele Uzmanı

SOC içinde olaylara müdahale eden uzmanlardır.

- Güvenlik olaylarına anında müdahale etmek.
- Etkilenen sistemleri izole etmek ve karantinaya almak.
- Ağ trafiğini analiz ederek saldırı vektörünü belirlemek.
- Siber kriz yönetimi süreçlerini yürütmek.

SOC Yöneticisi

SOC yöneticisi, ekibin verimli çalışmasını sağlar ve güvenlik stratejilerini belirler.

- SOC'un işleyişini denetlemek.
- Yeni güvenlik araçlarını ve politikalarını belirlemek.
- Üst yönetime güvenlik durumu hakkında rapor vermek.
- Siber güvenlik olaylarında kriz yönetimi yapmak.

SOC Modelleri

Ekipte hangi iş rollerinin yer alacağına karar vermenin yanı sıra, bir kuruluşun uygulayabileceği birkaç SOC modeli vardır. Bunlar ;

Dedicated or self-managed (Internal) SOC: Bu model, kurum içi personelin bulunduğu bir şirket içi tesise sahiptir.

Virtual SOC: Bu modelin özel bir şirket içi tesisi yoktur. Bir sanal SOC, kuruluş tarafından çalıştırılabilir veya tamamen yönetilebilir. Kuruluş tarafından işletilen bir SOC'de genellikle şirket içi çalışanlar veya şirket içi, talep üzerine ve bulut tarafından sağlanan çalışanlar bulunur. Dış kaynaklı SOC veya hizmet olarak SOC (SOCaaS) olarak da bilinen tam olarak yönetilen bir sanal SOC'nin şirket içi personeli yoktur.

Distributed (Hybrid) SOC: Ortak yönetilen bir SOC olarak da bilinen bu model, üçüncü taraf bir yönetilen güvenlik hizmeti sağlayıcısı (MSSP) ile birlikte çalışmak üzere şirket içinde işe alınan yarı adanmış tam zamanlı veya yarı zamanlı ekip üyelerine sahiptir.

Managed SOC: Bu model, bir işletmeye tüm SOC hizmetlerini sağlayan MSSP'lere sahiptir. Yönetilen algılama ve yanıt (MDR) ortakları, yönetilen SOC'nin başka bir biçimidir.

Command SOC: Bu model, diğer, tipik olarak ayrılmış güvenlik operasyon merkezlerine tehdit istihbaratı içgörüleri ve güvenlik uzmanlığı sağlar. Bir komut SOC'si, gerçek güvenlik operasyonlarına veya süreçlerine dahil değildir, sadece istihbarat tarafıdır.

Fusion Center: Bu model, diğer SOC türleri veya BT departmanları dahil olmak üzere herhangi bir güvenlik odaklı tesisi veya girişimi denetler. Fusion merkezleri, gelişmiş SOC'ler olarak kabul edilir ve BT operasyonları, DevOps ve ürün geliştirme gibi diğer kurumsal ekiplerle birlikte çalışır.

Multifunction SOC: Bu modelin özel bir tesisi ve kurum içi personeli vardır, ancak rolleri ve sorumlulukları, ağ operasyon merkezleri (NOC'ler) gibi BT yönetiminin diğer kritik alanlarına kadar uzanır.

SOCaaS: Bu abonelik tabanlı veya yazılım tabanlı model, SOC işlevlerinin bir kısmını veya tamamını bir bulut sağlayıcısına dış kaynak olarak sunar.

SOC Süreçlerinin Temel Aşamaları

SOC'un işleyişi belirli aşamalar üzerinden ilerler. Genel SOC süreç akışı şu adımlardan oluşur:

1.Olay Tespiti (Detection & Monitoring)
2.Olay Analizi ve Sınıflandırma (Analysis & Triage)
3.Olay Müdahalesi (Incident Response & Containment)
4.Olay Kurtarma ve İyileştirme (Recovery & Remediation)
5.Kök Neden Analizi (Root Cause Analysis - RCA)
6.Dokümantasyon ve Raporlama (Documentation & Reporting)
7.Sürekli İyileştirme ve Tehdit Avcılığı (Continuous Improvement & Threat Hunting)

1.Olay Tespiti (Detection & Monitoring)

Olay Tespiti (Detection & Monitoring), SOC operasyonlarının temel bileşenlerinden biridir.Bu süreçte, SIEM, EDR, IDS/IPS ve diğer güvenlik araçları kullanılarak sistemlerdeki anormal aktiviteler sürekli izlenir. Log verileri, tehdit istihbaratı ve korelasyon kuralları ile analiz edilerek saldırılar erken aşamada tespit edilir. Gerçek zamanlı uyarılar sayesinde SOC analistleri, şüpheli olaylara hızla müdahale edebilir

ve olası güvenlik ihlallerini önleyebilir. Etkili olay tespiti, proaktif savunma stratejileriyle kurumsal ağ güvenliğini güçlendirir.

2.Analizi ve Sınıflandırma (Analysis & Triage)
SOC analistleri, tespit edilen olayları detaylı bir şekilde analiz eder ve olayın ciddiyetini belirler.

- Olayın gerçek bir tehdit olup olmadığını belirleme (False Positive / True Positive ayrımı).
- Logları ve sistem olaylarını inceleyerek olayın kaynağını analiz etme.
- Olayın etki seviyesini belirleme:
  - Düşük (Low): Bilgi amaçlı loglar, zararsız aktiviteler.
  - Orta (Medium): Yetkilendirme hataları, şüpheli davranışlar.
  - Yüksek (High): Aktif saldırılar, kötü amaçlı yazılım tespiti.
  - Kritik (Critical): Veri sızıntısı, büyük çaplı saldırılar.

3.Olay Müdahalesi (Incident Response & Containment)
Tehdit onaylandıktan sonra, saldırının yayılmasını önlemek için müdahale süreci başlatılır.

- Etkilenen sistemleri izole etmek (karantinaya almak).
- Zararlı süreçleri ve bağlantıları sonlandırmak.
- Erişim kontrol politikalarını güncellemek.
- Güvenlik duvarı (Firewall) veya IDS/IPS ile kötü amaçlı IP'leri engellemek.
- Kullanıcı hesaplarını devre dışı bırakmak.
- Güvenlik ekipleriyle koordinasyon sağlamak.

4.Olay Kurtarma ve İyileştirme (Recovery & Remediation)
Saldırı durdurulduktan sonra, sistemlerin güvenli bir şekilde eski durumuna getirilmesi gerekir.

- Yedeklerden sistemleri geri yükleme.
- Güncellenmiş güvenlik yamaları ve konfigürasyonları uygulama.
- Kullanıcı şifrelerini sıfırlama ve erişim politikalarını gözden geçirme.
- SIEM ve diğer güvenlik araçlarında yeni algılama kuralları oluşturma.

5.Kök Neden Analizi (Root Cause Analysis - RCA)
Bir olay yaşandıktan sonra, tekrar yaşanmaması için kök neden analizi yapılır.

- Olayın nasıl gerçekleştiğini belirlemek (Saldırgan hangi yöntemi kullandı?).
- Kullanılan zafiyetleri ve güvenlik açıklarını tespit etmek.
- Saldırıya neden olan güvenlik ihlallerini belirlemek.
- Uzun vadeli iyileştirme planları oluşturmak.

6.Dokümantasyon ve Raporlama (Documentation & Reporting)
Olay müdahalesinden sonra, SOC ekibi yaşanan olayı belgeleyerek üst yönetime ve diğer ekiplerle paylaşır.

- Olayın zaman çizelgesini (Timeline) oluşturma.

- Kullanılan saldırı tekniklerini (MITRE ATT&CK ile eşleştirme).
- Alınan aksiyonları ve sonuçları detaylı şekilde yazma.
- Üst yönetime ve diğer birimlere raporlama.

7.Sürekli İyileştirme ve Tehdit Avcılığı (Continuous Improvement & Threat Hunting)
SOC ekibi, gelecekte benzer saldırıları önlemek için sistemlerini sürekli olarak geliştirir.

- Geçmiş olaylardan ders çıkarmak ve yeni güvenlik politikaları oluşturmak.
- SOC çalışanlarına düzenli eğitimler vermek (Red Team & Blue Team tatbikatları).
- Tehdit avcılığı (Threat Hunting) yaparak yeni tehditleri tespit etmek.
- Olay müdahale süreçlerini otomatikleştirmek (SOAR kullanımı).

Sonuç olarak SOC merkezi, tespit, analiz, müdahale, kurtarma, raporlama ve tehdit avcılığı aşamalarını içeren kapsamlı bir süreç takip eder. Bu süreçlerin doğru uygulanması, kurumların siber tehditlere karşı daha dirençli hale gelmesini sağlar.

Olay Müdahele (Incident Response) Nedir?

SOC (Security Operations Center) süreçlerinde olay müdahale (Incident Response), güvenlik olaylarının tespiti, analiz edilmesi, kontrol altına alınması ve etkisinin en aza indirilmesi için izlenen bir yöntemdir. Bu süreç genellikle NIST Cybersecurity Framework veya benzeri bir metodolojiye dayandırılarak uygulanır.

1.Hazırlık (Preparation)
Olası bir güvenlik olayına etkin müdahale etmek için önceden gerekli hazırlıkların yapılmasını kapsar. Bu hazırlıklar hem teknik hem de organizasyonel unsurları içerir.
- Politika ve prosedürler oluşturulur.
- Şirketin veri koruma, kullanıcı erişimi ve sistem yönetimine dair politikaları belirlenir.
- Saldırı senaryoları üzerinden ekipler tatbikata tabi tutulur (örneğin, phishing saldırısı veya ransomware vakası).
- Güvenlik açıklarını en aza indirmek için işletim sistemleri, uygulamalar ve ağ cihazları üzerinde gerekli yapılandırmalar yapılır.

2.Tespit ve Analiz (Detection and Analysis)
Güvenlik olaylarının belirlenmesi ve etkilerinin analiz edilmesi sürecidir:
-Alarm Tetiklenmesi: SIEM, IDS veya antivirüs sistemleri anormal aktiviteleri tespit eder.
-İlk Analiz: Loglar incelenerek olayın kaynağı, zaman çizelgesi ve etkilenen sistemler belirlenir.
-Etkilenen Varlıkların Belirlenmesi: Kullanıcı hesapları, dosyalar, ağ trafiği ve zararlı yazılım belirtileri araştırılır.

3.Müdahale (Containment, Eradication, and Recovery)
Olayın etkilerini sınırlandırma, zararlı unsurları temizleme ve sistemleri eski haline döndürme aşamasıdır:

Sınırlama (Containment)
- Etkilenen sistemler ağdan izole edilir.
- Kötü amaçlı dosyalar ve IP adresleri karantinaya alınır.
- Kullanıcılara olay hakkında bilgilendirme yapılır.

Temizleme (Eradication)
- Zararlı yazılım ve dosyalar sistemden kaldırılır.
- Yetkisiz erişim sağlanan arka kapılar kapatılır.
- Güvenlik açıkları giderilir (örneğin, yamalar yüklenir).

Kurtarma (Recovery)
- Yedeklerden temiz sistemler geri yüklenir.
- Sistem testleri yapılarak saldırının tekrar olup olmadığı kontrol edilir.
- İş sürekliliği sağlanarak operasyonlar normale döndürülür.

4.Öğrenim ve İyileştirme (Post-Incident Activity)

Yaşanan olaydan ders çıkarmak ve güvenlik süreçlerini geliştirmek için yapılan çalışmalar:

Olay İncelemesi: Kök neden analizi yapılarak güvenlik açıkları belirlenir.

Politika Güncellemeleri: E-posta filtreleri, erişim kontrolleri ve güvenlik kuralları güncellenir.

Eğitim ve Tatbikatlar: Çalışanlara saldırı farkındalık eğitimleri verilir, siber tatbikatlar düzenlenir.

Raporlama: Üst yönetime detaylı olay raporu sunulur.

SOC ve Kullanılan Teknolojiler

SIEM Nedir?

SIEM (Security Information and Event Management), bir kurumun bilgi sistemlerinden gelen güvenlik verilerini toplayan, analiz eden ve raporlayan bir yazılım çözümüdür. SIEM, güvenlik olaylarını gerçek zamanlı olarak izleyerek tehditleri tespit etmek ve müdahale etmek için kullanılır. Splunk, IBM QRadar, Microsoft Sentinel yaygın kullanılan SIEM ürünleridir

Temel İşlevleri:

1.Veri Toplama:
- Ağ cihazları, sunucular, uygulamalar ve güvenlik araçlarından gelen logları toplar.
- Farklı kaynaklardan gelen verileri merkezileştirir.

2.Veri Analizi:
- Toplanan verileri analiz ederek anormal aktiviteleri tespit eder.
- Korelasyon kuralları kullanarak ilgili olayları birleştirir.

3.Tehdit Tespiti:
- Bilinen tehdit imzalarını (signature-based detection) ve anormal davranışları (behavior-based detection) tespit eder.
- Gerçek zamanlı uyarılar üretir.

4.Olay Müdahalesi:
- Güvenlik ihlallerine hızlı bir şekilde müdahale etmek için bilgi sağlar.
- Otomatik müdahale senaryolarını destekler.

5.Raporlama ve Uyumluluk:
- Güvenlik olayları ve performans metrikleri hakkında raporlar hazırlar.
- Yasal ve düzenleyici gerekliliklere uyum sağlamak için gerekli bilgileri sunar.

Sonuç olarak SIEM, SOC'un en önemli araçlarından biridir ve güvenlik operasyonlarının merkezinde yer alır. Veri toplama, analiz, tehdit tespiti ve raporlama gibi işlevleriyle, kurumların siber tehditlere karşı proaktif bir şekilde korunmasını sağlar. Splunk, IBM QRadar, ArcSight gibi popüler SIEM araçları, farklı ihtiyaçlara uygun çözümler sunar.

SOAR Nedir?

SOAR (Security Orchestration, Automation, and Response), güvenlik operasyonlarını düzenlemek, otomatikleştirmek ve olay müdahalesini hızlandırmak için kullanılan bir teknolojidir. SOAR, farklı güvenlik araçlarını ve süreçlerini bir araya getirerek, SOC ekiplerinin daha verimli çalışmasını sağlar. Palo Alto Networks Cortex XSOAR, Splunk Phantom, IBM Resillient yaygın olarak kullanılan SOAR ürünleridir.

Temel İşlevleri:
1.Orkestrasyon (Orchestration):
- Farklı güvenlik araçlarını ve sistemlerini entegre eder.
- Araçlar arasında veri akışını sağlar ve iş birliği yaratır.

2.Otomasyon (Automation):
- Tekrarlayan ve manuel görevleri otomatikleştirir.
- Güvenlik olaylarına otomatik müdahale senaryoları oluşturur.

3.Olay Müdahalesi (Response):
- Güvenlik ihlallerine hızlı ve etkili bir şekilde müdahale etmek için süreçleri yönetir.
- Olay müdahale süreçlerini standartlaştırır ve iyileştirir.

Sonuç olarak SOAR, SOC'un modern siber güvenlik operasyonlarında kullandığı kritik bir araçtır. Orkestrasyon, otomasyon ve olay müdahalesi özellikleriyle, güvenlik süreçlerini hızlandırır ve ekiplerin iş yükünü hafifletir. Palo Alto Networks Cortex XSOAR, Splunk Phantom, IBM Resilient gibi popüler SOAR araçları, farklı ihtiyaçlara uygun çözümler sunar.

EDR Nedir?

EDR (Endpoint Detection and Response), bir kurumun uç noktalarındaki (bilgisayarlar, sunucular, mobil cihazlar gibi) tehditleri tespit etmek, analiz etmek ve müdahale etmek için kullanılan bir güvenlik çözümüdür. EDR, geleneksel antivirüs yazılımlarının ötesine geçerek, gelişmiş tehditlere karşı proaktif bir savunma sağlar. Crowdstrike Falcon, Microsoft Defender for Endpoint yaygın kullanılan EDR ürünleridir.

Temel İşlevleri:
1.Tehdit Tespiti:

- Uç noktalardaki anormal aktiviteleri tespit eder.
- Gelişmiş tehdit avcılığı (Threat Hunting) teknikleri kullanır.

2.Veri Toplama ve Analiz:
- Uç noktalardan güvenlik verilerini toplar ve analiz eder.
- Saldırıların kök nedenini belirlemek için detaylı analiz yapar.

3.Olay Müdahalesi:
- Tehditlere hızlı ve etkili bir şekilde müdahale eder.
- Otomatik müdahale senaryoları oluşturur.

4.Raporlama ve İyileştirme:
- Güvenlik olayları hakkında raporlar hazırlar.
- Süreçleri iyileştirmek için öneriler sunar.

Sonuç olarak EDR, SOC'un modern siber güvenlik operasyonlarında kullandığı kritik bir araçtır. Uç noktalardaki tehditleri tespit etmek, analiz etmek ve müdahale etmek için kullanılır. CrowdStrike Falcon, Microsoft Defender for Endpoint, Symantec Endpoint Detection and Response gibi popüler EDR araçları, farklı ihtiyaçlara uygun çözümler sunar.

MDR Nedir?

MDR, bir kurumun siber güvenlik operasyonlarını yönetmek ve tehditlere karşı proaktif bir savunma sağlamak için kullanılan bir hizmettir. MDR, genellikle bir üçüncü taraf güvenlik şirketi tarafından sunulur ve kurumun güvenlik operasyonlarını dış kaynak kullanarak yürütmesini sağlar.

Temel İşlevleri:
1.Tehdit Tespiti:
- Kurumun ağ, sistem ve uç noktalarındaki tehditleri tespit eder.
- Gelişmiş tehdit avcılığı (Threat Hunting) teknikleri kullanır.

2.Olay Müdahalesi:
- Tespit edilen tehditlere hızlı ve etkili bir şekilde müdahale eder.
- Olay müdahale süreçlerini yönetir.

3.Sürekli İzleme:
- Kurumun bilgi sistemlerini 7/24 izler.
- Anormal aktiviteleri gerçek zamanlı olarak analiz eder.

4.Raporlama ve İyileştirme:
- Güvenlik olayları hakkında raporlar hazırlar.
- Süreçleri iyileştirmek için öneriler sunar.

Sonuç olarak MDR (Managed Detection and Response), kurumların güvenlik operasyonlarını dış kaynak kullanarak yönetmesini sağlayan bir hizmettir. 7/24 izleme, olay müdahalesi ve tehdit avcılığı gibi hizmetleri kapsar. Özellikle kendi SOC ekibi bulunmayan veya ek destek almak isteyen kuruluşlar için etkili bir çözümdür.

XDR Nedir?

XDR, farklı güvenlik katmanlarındaki (ağ, uç nokta, bulut, e-posta gibi) verileri birleştirerek tehditleri tespit etmek, analiz etmek ve müdahale etmek için kullanılan bir teknolojidir. XDR, geleneksel güvenlik çözümlerinin ötesine geçerek, kurumun tüm güvenlik ekosistemini entegre eder.

Temel İşlevleri:
1.Veri Entegrasyonu:
- Farklı güvenlik katmanlarındaki verileri birleştirir.
- Ağ, uç nokta, bulut, e-posta gibi kaynaklardan gelen verileri analiz eder.

2.Tehdit Tespiti:
- Entegre edilen verileri analiz ederek anormal aktiviteleri tespit eder.
- Gelişmiş tehdit avcılığı (Threat Hunting) teknikleri kullanır.

3.Olay Müdahalesi:
- Tespit edilen tehditlere hızlı ve etkili bir şekilde müdahale eder.
- Otomatik müdahale senaryoları oluşturur.

4.Raporlama ve İyileştirme:
- Güvenlik olayları hakkında raporlar hazırlar.
- Süreçleri iyileştirmek için öneriler sunar.

Sonuç olarak XDR (Extended Detection and Response), uç nokta, ağ, bulut ve e-posta gibi farklı güvenlik katmanlarını entegre ederek tehditleri tespit etmeyi ve müdahale etmeyi sağlayan gelişmiş bir çözümdür. Geleneksel güvenlik çözümlerine kıyasla daha kapsamlı tehdit analizi ve otomatik müdahale mekanizmaları sunar.

IDS/IPS nedir?

IDS (Intrusion Detection System): Ağ trafiğini izleyerek olası saldırıları tespit eder ve uyarı üretir. Ancak saldırıyı engellemez.

IPS (Intrusion Prevention System): IDS'nin bir adım ötesine geçerek, tespit edilen saldırıları engeller. IPS, ağ trafiğini gerçek zamanlı olarak analiz eder ve tehditleri önler. Snort, Suricata, Palo Alto Networks yaygın kullanılan IDS/IPS ürünleridir.

Temel İşlevleri:
1.Tehdit Tespiti:
- Ağ trafiğindeki anormal aktiviteleri tespit eder.
- Bilinen saldırı imzalarını (signature-based detection) ve anormal davranışları (behavior-based detection) tanır.

2.Uyarı Üretme (IDS):
- Tespit edilen tehditler hakkında uyarılar üretir.
- SOC ekibine saldırı hakkında bilgi verir.

3.Saldırı Engelleme (IPS):
- Tespit edilen saldırıları otomatik olarak engeller.

- Örneğin, zararlı trafiği bloke eder veya saldırganın IP adresini engeller.

4.Loglama ve Raporlama:
- Ağ trafiği ve tespit edilen tehditler hakkında loglar tutar.
- Güvenlik olayları hakkında raporlar hazırlar.

Sonuç olarak IDS/IPS, SOC'un ağ güvenliğini sağlamak için kullandığı kritik araçlardır. Ağ trafiğini izleyerek olası saldırıları tespit eder ve engeller. Snort, Suricata, Cisco Firepower gibi popüler IDS/IPS araçları, farklı ihtiyaçlara uygun çözümler sunar.

CTI VE SOC

CTI Nedir?

CTI, siber tehditler hakkında bilgi toplama, analiz etme ve bu bilgileri kullanarak önlemler alma sürecidir. CTI, kurumların siber tehditlere karşı proaktif bir şekilde korunmasını sağlar ve güvenlik operasyonlarını iyileştirir.

CTI'nin Temel İşlevleri

1.Tehdit Bilgisi Toplama:
- Siber tehditler hakkında bilgi toplar.
- Açık kaynaklar (OSINT), karanlık ağ (Dark Web) ve özel kaynaklardan bilgi toplar.

2.Tehdit Analizi:
- Toplanan bilgileri analiz eder.
- Tehditlerin kaynağını, hedefini ve yöntemini belirler.

3.Tehdit Paylaşımı:
- Analiz edilen bilgileri SOC ekibi ve diğer paydaşlarla paylaşır.
- Tehditler hakkında uyarılar ve öneriler sunar.

4.Önlem Alma:
- Tehditlere karşı önlemler alır.
- Güvenlik stratejilerini ve süreçlerini iyileştirir.

CTI ve SOC ilişkisi

CTI, SOC'un siber tehditlere karşı proaktif bir savunma sağlamak için kullandığı kritik bir araçtır.

1.Tehdit Avcılığı (Threat Hunting):
- CTI, SOC ekibine tehdit avcılığı süreçlerinde rehberlik eder.
- Gizli tehditleri ortaya çıkarmak için bilgi sağlar.

2.Olay Müdahalesi (Incident Response):
- CTI, SOC ekibine olay müdahalesi süreçlerinde bilgi sağlar.
- Saldırıların kök nedenini belirlemek için analiz yapar.

3.Güvenlik Stratejileri:
- CTI, SOC'un güvenlik stratejilerini iyileştirmek için bilgi sağlar.
- Tehditlere karşı önlemler alınmasını sağlar.

4.Uyumluluk ve Raporlama:
- CTI, SOC'un yasal ve düzenleyici gerekliliklere uyum sağlamasına yardımcı olur.
- Güvenlik olayları hakkında raporlar hazırlar.

Sonuç olarak CTI, SOC'un siber tehditlere karşı proaktif bir savunma sağlamak için kullandığı kritik bir araçtır. Tehdit bilgisi toplama, analiz etme ve paylaşma süreçleriyle, kurumların siber tehditlere karşı daha güçlü bir savunma oluşturmasını sağlar. Recorded Future, ThreatConnect, Anomali ThreatStream gibi popüler CTI araçları, farklı ihtiyaçlara uygun çözümler sunar.

Log Nedir?

Log (kayıt dosyası), bir sistemin, uygulamanın veya ağ cihazının gerçekleştirdiği işlemleri kaydettiği metin tabanlı verilerdir. Siber güvenlikte loglar, olayları takip etmek, tehditleri tespit etmek ve olay müdahalesi yapmak için kritik öneme sahiptir.

Log Türleri

Sistem Logları
- İşletim sistemleri tarafından oluşturulur.
- Örnek: Windows Event Viewer veya Linux /var/log/ dizini altında bulunan loglar.

Ağ Logları
- Güvenlik duvarı (Firewall), IDS/IPS, yönlendiriciler (Router) ve anahtarlar (Switch) tarafından üretilir.
- Örnek: Cisco Firewall, Suricata, Snort logları.

Uygulama Logları
- Web sunucuları, veritabanları ve özel yazılımlar tarafından üretilir.
- Örnek: Apache Access Log, MySQL Error Log.

Kimlik Doğrulama Logları
- Kullanıcı oturum açma ve yetkilendirme işlemlerini kaydeder.
- Örnek: Active Directory Logları, Linux auth.log.

Olay Logları (Security Logs)
- Şüpheli aktiviteleri (brute force saldırıları, yetkisiz erişimler vb.) kaydeder.
- Örnek: SIEM tarafından toplanan loglar.

Log Nasıl Analiz Edilir?

Log Toplama:
- SIEM (Security Information and Event Management) çözümleri kullanılarak loglar merkezi bir sistemde toplanır.
- Örnek SIEM araçları: Wazuh, Splunk, Elastic SIEM, QRadar.

Ön İşleme:
- Loglar formatlanır, filtrelenir ve gereksiz bilgiler temizlenir.

Korelasyon:
- Farklı log kaynaklarından gelen veriler birleştirilerek anormal olaylar tespit edilir.
- Örneğin, bir kullanıcı birçok başarısız giriş denemesi yaptıktan sonra oturum açmayı başarırsa, bu bir brute force saldırısı olabilir.

Anomali ve Tehdit Tespiti:
- Şüpheli işlemler tespit edilerek analistler tarafından incelenir.
- SIEM kurallarına ve tehdit istihbaratına dayanarak otomatik uyarılar (alarmlar) oluşturulabilir.

Olay Müdahalesi ve Raporlama:
- Şüpheli loglar incelenir, saldırının kaynağı belirlenir ve gerekli güvenlik önlemleri alınır.

Sonuç Olarak
- Loglar, siber güvenlik olaylarını tespit etmek ve analiz etmek için kritik veriler sağlar.
- SOC ekipleri, log toplama, analiz etme, korelasyon oluşturma ve tehdit tespiti yaparak saldırıları önlemeye çalışır.
- SIEM araçları ve tehdit istihbaratı kullanılarak otomatik log analizi süreçleri oluşturulabilir.

Sonuç

SOC (Security Operations Center), siber güvenlik operasyonlarının yürütüldüğü merkezi bir yapıdır ve tehditlerin tespiti, analizi ve müdahalesinde kritik bir rol oynar. SOC'un temel amacı, organizasyonun bilgi sistemlerini koruyarak saldırılara karşı hızlı ve etkili bir savunma sağlamaktır. Bu süreçte SOC analistleri, SIEM, SOAR, EDR, MDR ve XDR gibi teknolojileri kullanarak olay müdahalesi gerçekleştirir, güvenlik tehditlerini analiz eder ve saldırıların etkisini en aza indirmek için stratejiler geliştirir.

SOC'un temel süreçleri arasında olay müdahale (incident response), tehdit avcılığı (threat hunting) ve tehdit istihbaratı (CTI) ile entegre çalışmalar yer alır. SIEM gibi log yönetimi ve analiz araçları, SOC operasyonlarının merkezinde bulunur ve sistemlerden gelen verilerin anlamlandırılmasını sağlar. IDS/IPS sistemleri ile tehdit tespiti ve engelleme mekanizmaları devreye alınırken, sürekli izleme ve iyileştirme süreçleriyle SOC'un etkinliği artırılır.

Günümüz tehdit ortamında siber güvenlik ekipleri, sadece reaktif önlemler almak yerine proaktif savunma mekanizmaları geliştirerek saldırıları önceden engellemeye odaklanmaktadır. Bu nedenle, SOC'un gelişmiş analiz yetenekleri ve otomasyon teknolojileriyle desteklenmesi, güvenlik operasyonlarının daha verimli ve etkili hale gelmesini sağlar. Siber tehditlerin her geçen gün arttığı bir ortamda, SOC merkezlerinin stratejik önemi giderek artmakta ve organizasyonların siber dirençlerini güçlendirmede hayati bir rol üstlenmektedir.

Kaynakça

https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir
https://www.beyaz.net/tr/guvenlik/makaleler/soc_nedir_ve_soc_da_hizmet_surekligi_nasil_saglanir.html
https://www.infinitumit.com.tr/guvenlik-operasyon-merkezi-soc-nedir/
https://www.vodafone.com.tr/vodafone-business/is-dunyasi/soc-security-operations-center-nedir-ve-soc-nasil-calisir
https://bizcom.com.tr/blog/soc-nedir-ne-ise-yarar
https://www.microsoft.com/tr-tr/security/business/security-101/what-is-siem
https://www.kaspersky.com.tr/resource-center/definitions/threat-intelligence