SOC FUNDEMANTALS

HAZIRLAYAN

ADI: AYŞE

SOYADI: BALCI

TARİH: 04/02/2025

İçindekiler Tablosu

GİRİŞ

Günümüzde dijital dünya büyüdükçe, siber tehditler de giderek karmaşık hale gelmekte ve kuruluşlar için ciddi riskler oluşturmaktadır. Kurumların verilerini, ağ altyapısını ve sistemlerini korumak için siber güvenlik tehditlerini anlamak ve bunlara karşı etkili çözümler geliştirmek kritik bir öneme sahiptir. Malware, oltalama (phishing), hizmet dışı bırakma (DoS/DDoS), iç tehditler ve sosyal mühendislik gibi farklı siber saldırı yöntemleri, hem bireysel hem de kurumsal seviyede büyük zararlar verebilmektedir. Bu çalışma, yaygın siber tehdit ve saldırı türlerini açıklayarak, siber güvenlik alanında bilinç oluşturmayı ve etkili savunma stratejileri geliştirilmesine katkı sağlamayı amaçlamaktadır.

SOC Nedir?

SOC (Security Operations Center), işletmelerin güvenlik açıklarını izleyen, analiz eden ve tehditlere karşı savunma sağlayan siber güvenlik uzmanlarından oluşur. Ağ altyapısı, sunucular, uç noktalar, uygulamalar ve web siteleri gibi varlıkları izleyerek güvenlik tehditlerini tespit eder ve müdahale ekipleriyle işbirliği içinde çalışır. SOC'un temel görevleri, tehditleri tanımlamak, analiz etmek, savunmak, araştırmak ve raporlamaktır.

SOC (Güvenlik Operasyonları Merkezi) genellikle **CIA Üçgeni**'ni (Confidentiality, Integrity, Availability - Gizlilik, Bütünlük, Erişilebilirlik) korumayı amaçlar. SOC'nin temel görevi, organizasyonun dijital altyapısını ve verilerini korumak, güvenlik tehditlerini tespit etmek ve bu tehditlere karşı gerekli müdahaleleri yaparak CIA Üçgeni'ni sağlamak üzerinedir.

- **Gizlilik (Confidentiality):** Verilerin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlamak.
- **Bütünlük (Integrity):** Verilerin doğru, eksiksiz ve değiştirilmeden korunması.
- **Erişilebilirlik (Availability):** Verilerin ve sistemlerin yetkili kullanıcılar tarafından gerektiğinde erişilebilir olmasını sağlamak.

Şekil 1 CIA Üçgeni

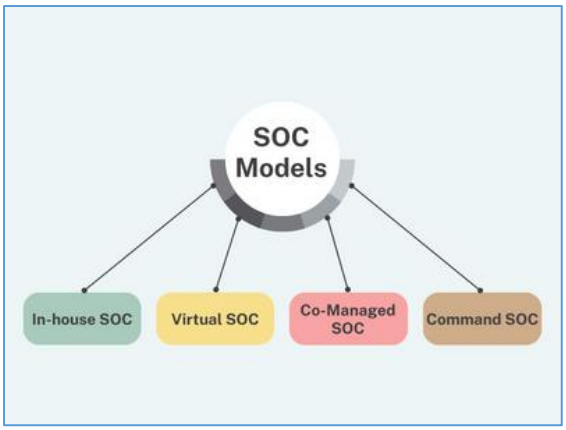
SOC Modelleri Nelerdir?

İç SOC (In-house SOC):
Bu ekip, bir organizasyon kendi siber güvenlik ekibini kurduğunda oluşur. İç bir SOC oluşturmayı düşünen organizasyonların, sürdürülebilirliğini destekleyecek bir bütçeye sahip olmaları gerekir.

Sanal SOC (Virtual SOC):
Bu tür SOC ekibi, sabit bir tesise sahip değildir ve genellikle farklı yerlerden uzaktan çalışır.

Ko-Yönetilen SOC (Co-Managed SOC):
Ko-Yönetilen SOC, iç SOC personelinin, dış bir Yönetilen Güvenlik Hizmet Sağlayıcısı (MSSP) ile birlikte çalıştığı bir yapıdır. Bu modelde koordinasyon çok önemlidir.

Komuta SOC (Command SOC):
Bu SOC ekibi, geniş bir bölgeyi kapsayan daha küçük SOC'ları denetler. Bu modeli kullanan organizasyonlar arasında büyük telekomünikasyon sağlayıcıları ve savunma ajansları yer alır.

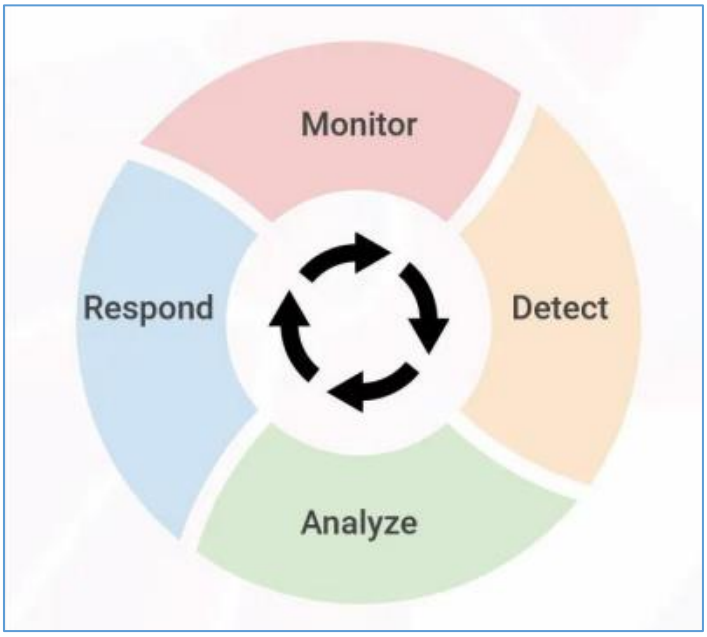


Şekil 2 SOC Modelleri

SOC Analisti Kimdir?

SOC Analisti (Security Operations Center Analyst), bir şirketin siber güvenlik bekçisi gibidir. Sistemleri izleyerek saldırı, kötü amaçlı yazılım ve şüpheli aktiviteleri tespit eder. Güvenlik uyarılarını analiz eder, tehditleri değerlendirir ve gerektiğinde müdahale ederek verileri korur.

SOC Görevleri Nelerdir?



Şekil 3 SOC Analisti temel görevleri

Monitor:

- Şirketin ağını, sistemlerini ve cihazlarını sürekli olarak şüpheli veya olağandışı aktiviteler için izler.
- Güvenlik duvarı, antivirüs ve diğer güvenlik araçlarından veri (log) toplayarak analiz yapar.
- **Önemi:** Tehditlerin erken tespiti, saldırıları gerçekleşmeden engellemeye yardımcı olur.

Tespit:

- Kötü amaçlı yazılım, oltalama girişimleri ve yetkisiz erişim gibi güvenlik tehditlerini belirler.
- Şüpheli web sitelerine yüksek trafik gibi olağandışı aktiviteleri tespit etmek için uyarılar oluşturur.
- **Önemi:** Hızlı tespit, SOC ekibinin saldırılara erken müdahale etmesini sağlar.

Analiz:

- Uyarıları inceleyerek gerçek tehditleri ve yanlış alarmları ayırt eder.
- Tehditlerin kaynağını, yöntemini ve hedefini anlamak için davranışlarını analiz eder.
- **Önemi:** Doğru analiz, tehdidin ciddiyetini belirleyerek uygun önlemlerin alınmasını sağlar.

Müdahale:

- Tehditleri etkisiz hale getirmek veya engellemek için aksiyon alır (örneğin, kötü amaçlı IP adreslerini engellemek).
- Zafiyetleri gidermek ve gelecekteki saldırıları önlemek için diğer ekiplerle işbirliği yapar.
- **Önemi:** Etkili müdahale, zararları en aza indirir, sistemlerin kesintisiz çalışmasını sağlar ve verileri korur.

SOC Rolleri Nelerdir?

Şekil 4 SOC Rolleri

Görselden hareketle SOC içindeki roller beş gruba ayrılabilir. Bunlar:

SOC Analisti; Bu rol, SOC yapısına göre LEvel 1, 2 ve 3 olarak kategorize edilebilir. Bir SOC analisti, alarmı sınıflandırır, nedeni araştırır ve düzeltme konusunda tavsiyelerde bulunur.

L1 (Seviye 1), SOC'nin ilk hattıdır, gelen güvenlik alarmlarını ve uyarılarını gözden geçirir, basit tehditleri tespit eder ve hızlıca sınıflandırır. Eğer sorun daha karmaşıksa, bunu L2 veya L3 seviyesine iletir. L2 (Seviye 2), Orta seviyedeki analisttir. L1 tarafından yönlendirilen olayları derinlemesine inceler, tehditlerin kaynağını araştırır ve olayı daha ayrıntılı analiz eder. Eğer olay daha karmaşıksa, L3'e danışabilir. L3 (Seviye 3) ise en deneyimli ve ileri seviyedeki analisttir. Kritik güvenlik olaylarıyla ilgilenir.. Ayrıca, SOC ekibine liderlik eder, güvenlik politikalarını oluşturur ve ekiplerin eğitimini üstlenir.

Incident Responder(olay müdahale görevlileri); Tehdit tespiti ile sorumlu bir kişidir. Bu rol, güvenlik ihlallerinin ilk değerlendirmesini yapar.

Threar Hunter; Bir organizasyonun ağındaki veya sistemindeki potansiyel tehditleri ve güvenlik açıklarını proaktif bir şekilde araştıran bir siber güvenlik profesyonelidir. Gelişmiş kalıcı tehditleri (APT'ler) ve diğer sofistike saldırıları tespit etmek, izole etmek ve hafifletmek için manuel ve otomatik tekniklerin bir kombinasyonunu kullanırlar.

Security Engineer; Güvenlik Bilgisi ve Etkinlik Yönetimi (SIEM) çözümleri ve güvenlik operasyonları merkezi (SOC) ürünlerinin güvenlik altyapısını sürdürmekten sorumludur. Örneğin, bir güvenlik mühendisi, SIEM ve Güvenlik Orkestrasyonu, Otomasyon ve Yanıt (SOAR) ürünleri arasındaki bağlantıyı kurar.

SOC Manager; Bir SOC yöneticisi, bütçeleme, strateji geliştirme, personel yönetimi ve operasyonları koordine etme gibi yönetim sorumluluklarını üstlenir. Teknik sorunlardan çok operasyonel sorunlarla ilgilenir.

Tespit Sonuçları Neler Olabilir?

False Positive: Sistem veya analist zararsız bir unsuru veya olayı tehdit olarak algılar.

True Positive: Sistem veya analist gerçek bir zararlı unsuru veya olayı zararlı olarak algılar.

False Negative: Sistem veya analist gerçek bir zararlı unsuru veya olayı zararsız olarak algılar.

True Negative: Sistem veya analist gerçek bir zararsız unsuru veya olayı zararsız olarak algılar.

SOC Metrikleri Nelerdir?

SOC metrikleri, SOC'nin güvenlik tehditlerini ne kadar iyi tespit ettiğini, yanıt verdiğini, hafiflettiğini ve yanıt sürecini nasıl yönettiğini değerlendirmede yardımcı olurlar.

- **Mean Time To Detect (MTTD) - Ortalama Tespit Süresi:** Bir güvenlik olayının tespit edilme süresini ölçer. Daha düşük MTTD, tehditlerin daha hızlı bir şekilde tespit edildiğini gösterir.

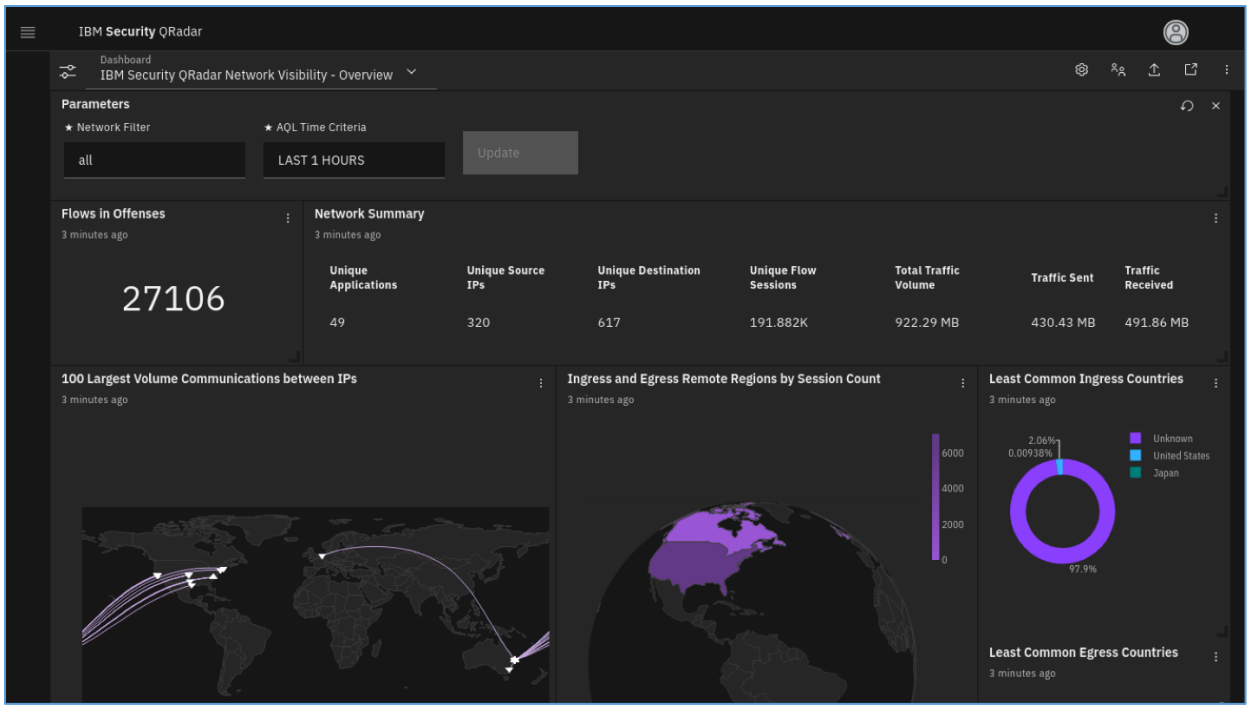
- **Mean Time To Resolution (MTTR) - Ortalama Çözüm Süresi**: Bir güvenlik olayının tespitinden çözülmesine kadar geçen ortalama süreyi ölçer. Daha düşük MTTR, olayların daha verimli bir şekilde çözüldüğünü gösterir.
- **Mean Time To Attend 4 Analysis (MTTA4A) - Ortalama Analize Katılma Süresi**: Bir olayın analize başlanmasından önceki süreyi ölçer. Daha düşük MTTA4A, olaylara daha hızlı müdahale yapıldığını gösterir.
- **Incident Detection Rate - Olay Tespiti Oranı:** SOC'nin tespit ettiği güvenlik olaylarının oranını ifade eder. Yüksek oran, daha iyi izleme ve olay tespiti anlamına gelir.
- **False Positive Rates (FPR) - Yanıltıcı Pozitif Oranı:** Yanıltıcı pozitifler, gerçek bir tehdit olmayan olayların alarm olarak işaretlenmesidir. Daha düşük oran, daha doğru tespitler yapıldığını gösterir.
- **False Negative Rate (FNR) - Yanıltıcı Negatif Oranı:** Yanıltıcı negatifler, gerçek bir tehdit olduğu halde alarmın tetiklenmemesidir. Daha düşük oran, tespit sistemlerinin doğruluğunun arttığını gösterir.
- **Key Risk Indicator (KRI) - Anahtar Risk Göstergesi:** Riskleri değerlendirmek için ölçülebilir değerlerdir.
  KRI'lar, bir organizasyonun karşı karşıya olduğu riskleri ölçmek ve izlemek için kullanılır.
- **Service Level Agreements (SLAs) - Hizmet Düzeyi Anlaşmaları**: SOC ekibi ile SOC müşterisi arasındaki anlaşmadır, bireysel yanıt süreleri, hizmet seviyesi ve performans gibi faktörleri içerir.
  SLAs, SOC'nin sağladığı hizmetlerin kalitesini, zamanında müdahale ve performans düzeyini belirleyen sözleşmelerdir.

SOC Araçları Nelerdir?

SOC ekipleri kurumların güvenlik durumlarını izleyip gelen alarmlara karşı önlem almak için çeşitli araçlar kullanırlar. Bu araçlardan bazıları gelen saldırılara veya sistemde bulunan bir açıklığa karşı sadece alarm üretirken, bazıları ise bu alarmlara karşı aksiyon alma görevini de üstlenebilir.

SIEM: SIEM (Security Information and Event Management) bir ağda 7/24 olarak izleme yapmayı sağlar. Ağdaki anomali tespitinde yardımcı olur. "Güvenlik Bilgi Yönetimi" (SIM) ve "Güvenlik Olay Yönetimi" (SEM) sistemlerinin birleşimi olan SIEM, büyük miktarda log verisi toplayarak bunları kategorize eder, düzenler ve erişilebilir hale getirir. Ağdaki logları toplayarak bunlar üzerinde gelen anormal bir davranışta alert üreterek aksiyon alınmasında yardımcı olur.

IBM QRadar, Splunk, FortiSIEM, McAfee ESM ücretli siem çözümlerine örnek olabilecekken, wazuh, splunk gibi araçlar da açık kaynak siem ürünlerine örnektir. Siem üzerinde kendi konfigürasyon ve korelasyonlarınızı yapabilir ve alertlerini bu koreleasyonlara göre alabilirsiniz.



Şekil 5 IBM Qradar ekran görüntüsü

SOAR: SOAR (Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı), güvenlik operasyonlarını optimize etmek için tehdit istihbaratı, olay yönetimi ve müdahale süreçlerini birleştiren bir güvenlik teknolojisidir. SIEM sistemlerinin bir adım ötesine geçerek, tehdit tespiti sonrası müdahale süreçlerini otomatikleştirmeye ve güvenlik ekiplerinin iş yükünü azaltmaya odaklanır.

Orkestrasyon, farklı güvenlik araçlarını (SIEM, EDR, IDS/IPS, Firewall) entegre ederek koordineli bir çalışma ortamı oluşturur. Otomasyon, tekrarlayan süreçleri (zararlı dosya analizi, IP engelleme, olay yanıtı) otomatik hale getirerek analistlerin iş yükünü azaltır ve müdahale süresini kısaltır. Yanıt (Response) ise olaylara hızlı ve tutarlı müdahale edilmesini sağlayarak tehditlere karşı daha etkin bir güvenlik duruşu oluşturur.

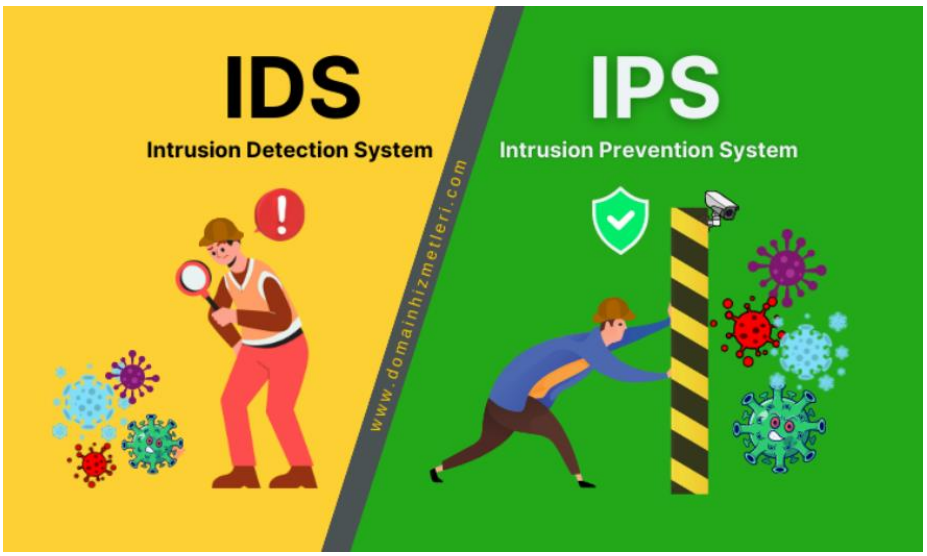
Bilinen bazı SOAR araçları arasında Palo Alto XSOAR (Demisto), Splunk SOAR (Phantom), IBM Resilient, Swimlane ve D3 Security bulunmaktadır.

EDR: EDR (Endpoint Detection and Response- Uç nokta Tehdit Algılama ve Yanıt) Son kullanıcı cihazları üzerine kurulur. EDR araçları antivirüs öğelerine ek olarak gerçek zamanlı anomali algılama, uyarma, uç noktalarda çalışan işlemlerin takibi ve kayıtlarının tutulması gibi özellikler ile tehditlerin görünürlüğünü arttırır, adli analizi kolaylaştırır.

EDR, her dosya çalıştırma ve modifikasyonunu, kayıt defteri değişikliğini, ağ bağlantısını ve çeşitli işlemleri kaydeder, tehditlerin görünürlüğünü arttırır.

IPS/IDS: Bir siber saldırı önleme sistemi olan IPS (Intrusion Prevention System), tehlikeli, şüpheli ve risk oluşturabilecek aktiviteleri izleyerek engellenmesini sağlar. IPS, sürekli olarak ağ üzerindeki trafiği takip eder ve kontrol eder. Normal dışı bir durum belirlediğinde ise veri akışını kısıtlar ve ağ yöneticisine uyarı iletir.

Bir ağı sürekli olarak izleyerek ve tarayarak güvenlik açıkları, potansiyel saldırılar, şüpheli aktiviteler gibi durumlara karşı kullanılan yazılım ya da donanım güvenlik sistemidir. IDS sistemi temel olarak meydana gelen saldırıları tespit etmenin yanı sıra karantinaya almak, raporlamak, kaydetmek gibi farklı işlevleri de bulunmaktadır. Ayrıca IPS sistemi ile entegre bir şekilde kullanılabilir.



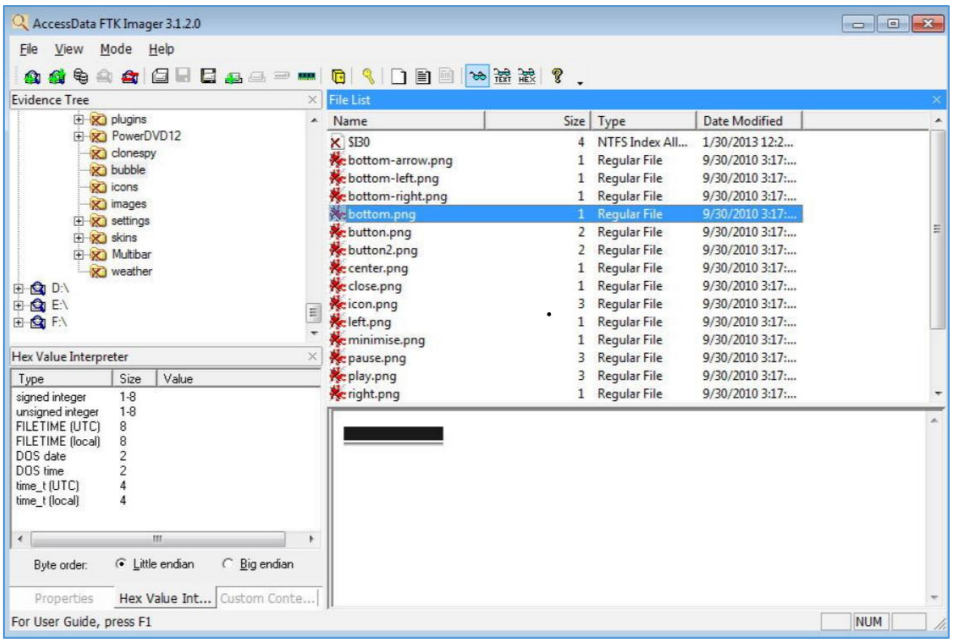
Şekil 6 IDS ve IPS temsili

NSM: NSM (Network Security Monitoring - Ağ Güvenliği İzleme), ağ trafiğini sürekli olarak analiz ederek tehditleri tespit etmeye ve güvenlik olaylarını izlemeye odaklanan bir güvenlik yaklaşımıdır. Bu sistemler, ağdaki anormal aktiviteleri belirleyerek saldırıları tespit eder, olay müdahale süreçlerine destek sağlar ve tehdit avcılığı için gerekli verileri sunar. NSM çözümleri, paket yakalama (PCAP), akış analizi (NetFlow) ve derin paket analizi (DPI) gibi teknikleri kullanarak ağ üzerindeki şüpheli faaliyetleri tespit eder. En yaygın kullanılan NSM araçları arasında Zeek (Bro), Suricata, Snort, Security Onion ve Arkime (Moloch) bulunur.

Threat Intelligence (Tehdit İstihbaratı) Platformları: Threat Intelligence (Tehdit İstihbaratı) araçları, siber tehditleri tespit etmek, analiz etmek ve önlem almak için kullanılan sistemlerdir. Bu araçlar, kötü amaçlı yazılım kampanyaları, saldırgan teknikleri ve tehdit aktörleri hakkında gerçek zamanlı veri sağlayarak SOC ekiplerinin proaktif güvenlik önlemleri almasını sağlar. Virustotal, alienvault, MISP, ThreadConnect bu platformlara örnek verilebilir.

Firewall: Güvenlik duvarı veya güvenlik duvarı yazılımı, bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir. Birçok farklı filtreleme özelliği ile bilgisayar ve ağın gelen ve giden paketler olmak üzere İnternet trafiğini kontrol altında tutar. IP filtreleme, port filtreleme, Web filtreleme, içerik filtreleme bunlardan birkaçıdır.

Adli Bilişim Araçları: Adli bilişim araçları, siber suçların araştırılması, dijital kanıtların toplanması ve analiz edilmesi için kullanılan yazılım veya donanımlardır. Bu araçlar, veri kurtarma, disk inceleme, bellek analizi, zararlı yazılım tespiti ve ağ trafiği analizi gibi işlemlerde kullanılır. Sistemin birebir kopyasını alarak sistem üzerinde inceleme yapma işini kolaylaştırır. Bu araçalara örnek olarak Autopsy, FTK, x-Ways, Oxygen verilebilir.



Şekil 7 FTK Imager

SOC ekipleri tüm bu araçlardan gelen logları toplayıp analiz ederek, potansiyel tehditleri ortaya çıkarır. Bu yüzden SOC analistlerinin log analizi konusunda bir bilgileri olması gerekir. Sistemde toplanan log türlerini ve bu logların analiz adımlarını iyi bilmelidir.

Özellikle Windows sistemlerde bu tür loglar Event ID denilen ID'ler ile toplanır ve bu ID'ler SOC analistlerinin sistemde olan biten davranışları anlamaları için büyük önem taşır.

LOG Türleri Nelerdir?

Sistem Logları: sistem başlatma, kapatma, güncelleme gibi işletim sistemi loglarıdır.

Uygulama Logları: Uygulama ve yazılımlarla ilgili loglardır.

Güvenlik Logları: sistem girişleri, politika değişimleri gibi sistem güvenliğiyle ilgili loglardır.

Network Logları: Ağ trafiğinde yakalanan loglardır.

Veritabanı Logları: SQL sorguları, error işlemleri gibi veritabanı loglarıdır.

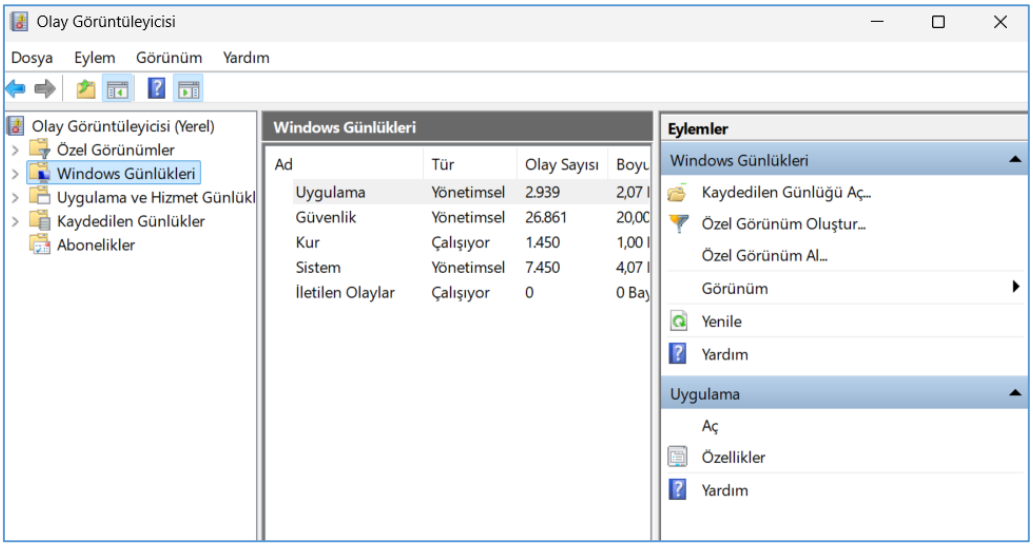
Email Logları: SMTP gibi email protokolleri, mail server, email, Transaction gibi loglardır.

Protokol Loglaro: HTTP/HTTPS, DNS, FTP gibi prokoller üzerinde yapılan işlemlerle ilgili loglardır.

Windows Sistemlerde Yaygın Event ID'ler ve Anlamları

Windows işletim sistemleri, sistem olaylarını kaydetmek için Olay Görüntüleyici (Event Viewer) aracını kullanır. Her olay, benzersiz bir Event ID (Olay Kimliği) ile tanımlanır.

- Event ID 41: Sistem beklenmedik şekilde yeniden başlatıldı (Kernel-Power hatası)
- Event ID 7023: Hizmet beklenmedik şekilde sonlandı.
- Event ID 4624: Başarılı oturum açma.
- Event ID 4625: Başarısız oturum açma (Yanlış parola).
- Event ID 4720: Kullanıcı hesabı oluşturuldu.
- Event ID 4726: Kullanıcı hesabı silindi.
- Event ID 4738: Kullanıcı hesabı değiştirildi.
- Event ID 6005: Windows Güvenlik Duvarı devre dışı.
- Event ID 5156: Ağ bağlantısı engellendi (Güvenlik Duvarı).
- Event ID 903: PowerShell komut hatası.
- Event ID 11: Disk yazma hatası (Bad Sector)
- Event ID 2003: Yüksek CPU kullanımı.
- Event ID 4688: Yeni işlem oluşturuldu.
- Event ID 4700: Zamanlanmış görev değiştirildi.
- Event ID 4719: Sistem denetim ilkesi değişti.
- Event ID 8198: RPC (Remote Procedure Call) hatası.



Şekil 8 Windows Event viewer

Yaygın Tehditler ve Ataklar

Siber güvenlik tehditleri ve saldırıları, bir kuruluşun altyapısındaki farklı bileşenleri hedef alabilir ve çeşitli şekillerde gerçekleşebilir. Aşağıda en sık karşılaşılan türlerden bazıları bulunmaktadır:

Yaygın tehditler

Malware:

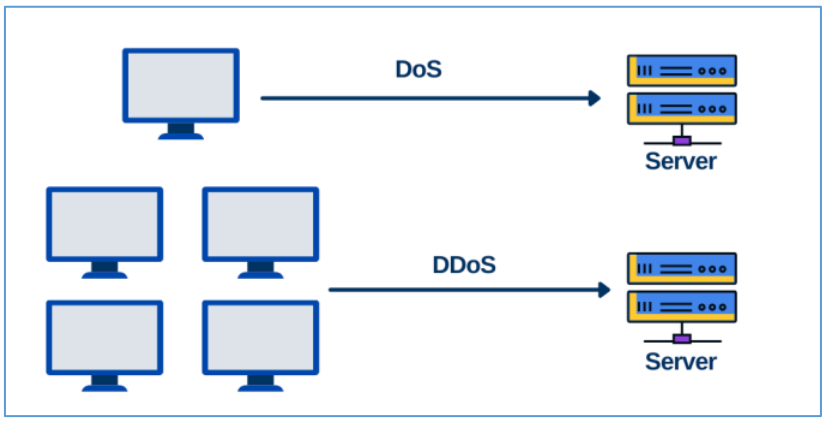
- **Virüsler:** Temiz dosyalara kendini ekleyerek yayılan ve diğer dosyalara zarar veren kötü amaçlı kodlar.
- **Solucanlar (Worms):** Ağlar üzerinde kendini kopyalayarak yayılan ve sistem açıklarını kullanan kötü amaçlı yazılımlar.
- **Truva Atları (Trojan Horses):** Meşru bir yazılım gibi gizlenmiş, kullanıcıları kandırarak yüklenmesini sağlayan kötü amaçlı yazılımlar.
- **Fidye Yazılımları (Ransomware):** Dosyaları şifreleyerek, şifre çözme anahtarı karşılığında fidye talep eden kötü amaçlı yazılımlar.
- **Casus Yazılımlar (Spyware):** Kullanıcıların farkında olmadan faaliyetlerini izleyen ve verilerini toplayan kötü amaçlı yazılımlar.

Oltalama (Phishing):

- **E-posta Oltalama (Email Phishing):** Kullanıcılardan kişisel bilgileri almaya veya kötü amaçlı bağlantılara tıklamalarını sağlamaya yönelik sahte e-postalar.
- **Hedefli Oltalama (Spear Phishing):** Belirli bireyleri veya kuruluşları hedef alan özel oltalama saldırıları.
- **Whaling:** Üst düzey yöneticiler gibi yüksek profilli kişileri hedef alan oltalama saldırıları (CEO dolandırıcılığı).

Hizmet Dışı Bırakma (DoS) ve Dağıtılmış Hizmet Dışı Bırakma (DDoS) Saldırıları:

- **DoS (Denial of Service):** Bir sistemi aşırı trafikle yükleyerek çökmesine ve kullanıcılar için erişilemez hale gelmesine neden olan saldırı.
- **DDoS (Distributed Denial of Service):** Genellikle ele geçirilmiş birçok cihazın kullanılmasıyla hedefe aşırı trafik göndererek hizmeti devre dışı bırakmayı amaçlayan saldırı.



Şekil 9 DOS ve DDOS temsili

Man In The Middle(ortadaki adam saldırıları) Attack:

Man in the middle saldırısı ağda, iki bağlantı arasındaki iletişimin dinlenmesi ile çeşitli verilerin ele geçirilmesi veya iletişimi dinlemekle kalmayıp her türlü değişikliğin yapılmasını da kapsayan bir saldırı yöntemidir. MITM'de iki taraf arasındaki iletişim kesilebilir ya da yanıltıcı bir iletişim oluşturulabilir. Bu saldırı ağ üzerindeki paketleri yakalayarak manipüle etmek olarak özetlenebilir.

Advanced Persistance Threads:

Uzun vadeli ve hedef odaklı saldırılar olup, saldırganlar bir ağa sızarak fark edilmeden kalır ve hassas verileri uzun bir süre boyunca çalmaya devam eder.

İç Tehditler (Insider Threats):
Mevcut veya eski çalışanlar ya da kurumca güvenilen kişilerin sistemlere veya verilere erişerek gerçekleştirdiği kötü niyetli faaliyetler.

Yaygın Ataklar

SQL Enjeksiyonu (SQL Injection):
Saldırganlar, giriş alanlarına kötü niyetli SQL sorguları ekleyerek veritabanlarını manipüle eder ve hassas bilgilere erişim sağlayabilir.

Siteler Arası Betik Çalıştırma (XSS):
Kötü amaçlı betikleri web sayfalarına enjekte ederek, saldırganların çerezleri ve oturum bilgilerini çalmasına veya kullanıcıları zararlı sitelere yönlendirmesine olanak tanır.

Brute Force Attacks:
Otomatik araçlar kullanarak şifreleri, şifreleme anahtarlarını veya PIN kodlarını deneme yanılma yöntemiyle tahmin etmeye çalışır.

Credential Stuffing:
Saldırganlar, ele geçirilmiş giriş bilgilerini kullanarak farklı platformlarda oturum açmaya çalışır ve yetkisiz erişim sağlar.

Zero Day Exploits:
Yazılımın henüz üretici tarafından bilinmeyen ve düzeltme yaması bulunmayan güvenlik açıklarını istismar eden saldırılar.

Sosyal Mühendislik:
Bireyleri kandırarak gizli bilgileri ifşa etmelerini sağlamak için psikolojik manipülasyon teknikleri kullanılır.

- **Pretexting:** Özel bilgileri elde etmek için sahte bir senaryo oluşturma.
- **Baiting:** Ücretsiz teklifler veya sahte ödüllerle kullanıcıları kandırarak kimlik bilgilerini ele geçirme veya zararlı yazılım indirtme.

Şifre Saldırıları (Password Attacks):

- **Sözlük Saldırıları (Dictionary Attacks):** Yaygın olarak kullanılan şifreleri deneyerek erişim sağlamaya çalışma.
- **Keyloggers:** Kullanıcının klavye girdilerini izleyerek şifreleri ve hassas bilgileri ele geçirme.

Sahte Yazılım (Rogue Software):
Güvenilir bir yazılım gibi görünen, ancak aslında sisteme zarar veren veya veri çalan kötü amaçlı yazılımlar.

Session Hijacking:
Saldırganın, web tarayıcısında kullanıcı kimliğini doğrulamak için kullanılan oturum belirteçlerini çalarak bir oturumu ele geçirmesi ve yetkisiz erişim sağlaması.

SONUÇ

Siber güvenlik tehditleri her geçen gün daha sofistike hale gelmekte ve kurumların güvenliğini tehlikeye atmaya devam etmektedir. Bu nedenle, organizasyonların hem teknik hem de stratejik olarak bu tehditlere karşı hazırlıklı olmaları gerekmektedir. SIEM, SOAR, EDR ve NSM gibi güvenlik teknolojileri, tehditleri tespit etmek ve etkili bir şekilde müdahale etmek için kritik öneme sahiptir. Bunun yanı sıra, farkındalık eğitimleri, güçlü kimlik doğrulama yöntemleri ve en iyi siber güvenlik uygulamalarını benimsemek, tehditlerin etkisini en aza indirmenin temel yollarındandır. Bu bağlamda, siber güvenlik ekiplerinin tehditleri tanıması ve doğru stratejiler geliştirmesi, dijital varlıkları korumanın en etkili yolu olmaya devam edecektir.

KAYNAKÇA

1. https://media.licdn.com/dms/document/media/v2/D4D1FAQHkOwBj1bHY3A/feedshare-document-pdf-analyzed/feedshare-document-pdf-analyzed/0/1729345131332?e=1738800000&v=beta&t=YxQ3DwyyjA3YsETopYuhJDOp7__9ywDbQZ3wDmyG984
2. https://media.licdn.com/dms/document/media/v2/D561FAQFLe-Whd1sD5Q/feedshare-document-pdf-analyzed/B56ZQXQq4GGQAY-/0/1735557054792?e=1738800000&v=beta&t=3-E2kCPnR4hCaPmUa_iTvfwmQiZHoRcIl2iGtqiP9yU
3. https://media.licdn.com/dms/document/media/v2/D4D1FAQEnGcMpFljmDg/feedshare-document-pdf-analyzed/feedshare-document-pdf-analyzed/0/1718448479994?e=1739404800&v=beta&t=31TB50DidHsbAdtfpzajnM79RCNZGYa0l14aARg6tq8
4. https://www.beyaz.net/tr/guvenlik/makaleler/edr_cozumu_nedir.html
5. https://www.beyaz.net/tr/guvenlik/makaleler/soc_araclari.html
6. https://bulutistan.com/blog/soc/
7. https://www.turk.net/blog/ips-ve-ids-nedir-nasil-calisir/
8. https://berqnet.com/blog/firewall-nedir
9. https://www.gaissecurity.com/blog/adli-bilisim-digital-forensic-nedir
10. https://tahsinmete.com/windows-event-id-rehberi-en-yaygin-100-olay-kimligi-ve-anlamlari/
11. https://app.letsdefend.io/training/lessons/soc-fundamentals