SOC FUNDAMENTALS

Hazırlayan

Neslihan ASLAN

12/02/2025

İçindekiler Tablosu

Giriş

Teknoloji, hayatımızın ayrılmaz bir parçası haline gelirken siber tehditler de giderek karmaşık ve tehlikeli bir boyut kazanmaya devam ederek hayatımızda yerini almaktadır. İlerleyen teknoloji ile beraber verileri ve sistemleri korumak bu noktada önemli bir konumda yer alıyor. İşte tam da burada, Security Operations Center (SOC) devreye giriyor.

SOC, siber tehditleri tespit etmek, analiz etmek ve bertaraf etmek için sürekli çalışan bir savunma hattıdır. Güvenlik olaylarını anlık olarak izleyerek proaktif müdahaleler gerçekleştiren SOC ekipleri, tehdit avcılığı, olay yönetimi ve adli bilişim analizleri gibi kritik süreçleri yönetir. Böylece verilerini ve sistemlerini korumak isteyen yapılar saldırılara karşı daha dirençli hale gelir ve olası veri ihlallerinin önüne geçebilir.

Etkili bir SOC yalnızca teknolojiye değil, aynı zamanda insan ve süreç yönetimine de dayanmaktadır. Güçlü bir siber güvenlik altyapısı oluşturmanın anahtarı, bütüncül bir bakış açısıyla çalışan, uyum içinde hareket eden bir ekip ve iyi tasarlanmış süreçleri kapsar. Tıpkı bir zincirin gücünün en zayıf halkasına bağlı olması gibi, güvenlik ekosisteminin başarısı da parçaların bir araya gelerek oluşturduğu bütüne dayanır.

Security Operations Center (SOC) Nedir?

Siber güvenlik operasyon merkezi (SOC), bir organizasyonun güvenlik olaylarını sürekli olarak izleyen, analiz eden ve bu olaylara müdahale eden merkezi bir birimdir. SOC, güvenlik tehditlerini tespit etmek, etkisiz hale getirmek ve sistemleri koruyarak organizasyonun siber güvenliğini sağlamaktan sorumludur. Bu süreçler, gelişmiş güvenlik teknolojileri, tehdit istihbaratı ve alanında uzman güvenlik analistlerinden oluşan ekipler tarafından yürütülür.

Şekil 1

SOC'nin temel amacı, organizasyonun bilgi varlıklarını koruyarak siber saldırılara karşı proaktif ve hızlı bir savunma mekanizması oluşturmaktır. Bu doğrultuda, anlık tehdit izleme, olay analizi, zararlı aktivitelerin tespiti ve önlenmesi gibi kritik görevleri yerine getirir. Ayrıca, güvenlik politikalarının uygulanması, güvenlik ihlallerinin kayıt altına alınması ve olay sonrası adli analiz süreçlerinin yürütülmesi de SOC'nin sorumlulukları arasındadır.

Soc Modelleri

Oluşumun siber güvenlik operasyonlarını nasıl yönettiğini belirleyen yapıdır. Operasyonel gereksinimler, bütçe, güvenlik stratejileri, organizasyonun büyüklüğü gibi ihtiyaçlara göre çeşitli SOC modelleri bulunmaktadır.

Merkezi SOC

Tüm güvenlik operasyonlarının tek bir merkezden yönetildiği yapıdır. Tüm güvenlik izleme, tehdit avcılığı, olay müdahalesi ve raporlama süreçleri, belirli bir fiziksel lokasyonda bulunan ekipler tarafından yürütülür.

Dağıtık SOC

Dağıtık SOC, birden fazla lokasyona yayılmış ancak koordineli çalışan SOC yapılarıdır. Genellikle büyük ölçekli organizasyonlar tarafından tercih edilir. Farklı coğrafi bölgelerde bulunan SOC merkezleri, belirli bir organizasyonun güvenlik operasyonlarını yönetmek için iş birliği yapar.

Sanal SOC

Bulut tabanlı çözümler kullanılarak uzaktan yönetilen SOC modelidir. Geleneksel fiziksel SOC merkezlerinden farklı olarak, tamamen bulut ortamında çalışır ve güvenlik operasyonlarını sanal araçlar üzerinden yürütür.

Hibrit SOC

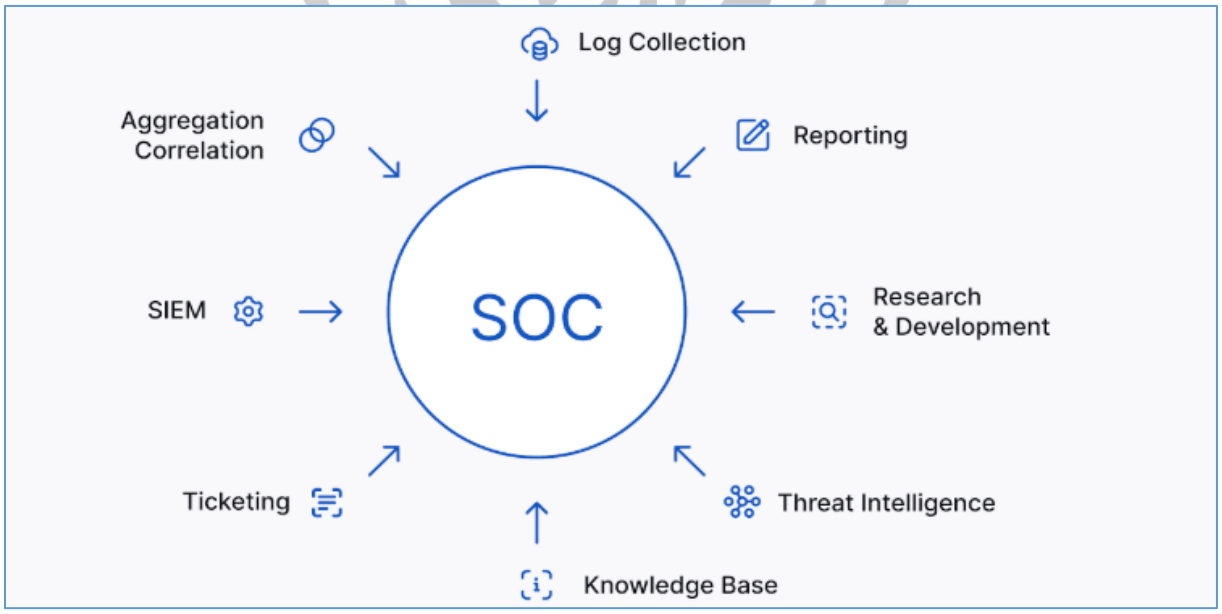
Hibrit SOC, merkezi ve dağıtık SOC modellerinin birleşimi olan yapıdır. Büyük organizasyonlar hem yerel hem de küresel tehditleri daha etkin yönetebilmek için hibrit SOC modelini tercih edebilir.

Komuta SOC (Command SOC)

Komuta SOC (Command SOC), geniş ölçekli oluşumlar için geliştirilen, SOC operasyonlarının üst düzeyden yönetildiği bir yapıdır. Büyük ve karmaşık güvenlik operasyonları merkezi bir komuta merkezi aracılığıyla koordine edilir. Genellikle hükümetler, çok uluslu şirketler ve büyük finansal kurumlar tarafından tercih edilir.

SOC Ne Yapar?

SOC (Security Operations Center), organizasyonların siber güvenlik tehditlerine karşı korunmasını sağlamak amacıyla birçok önemli görevi yerine getirir. Bu görevler, tehditlerin tespit edilmesi, analiz edilmesi, önlenmesi ve güvenlik açıklarının yönetilmesini kapsayan geniş bir yelpazeye yayılır. Bu süreçler sayesinde güçlü bir siber savunma hattı oluşturulur.



Şekil 2

Monitoring (İzleme)

Oluşumun bilişim altyapısını sürekli izleyerek güvenlik olayları takip edilir. Bu süreçte ağ trafiği, uç nokta aktiviteleri, güvenlik cihazları ve kullanıcı davranışları sürekli olarak analiz edilir. SIEM, EDR ve NDR gibi güvenlik araçları kullanılarak loglar toplanarak anormallikler belirlenir. Bu aşamada şüpheli aktiviteler tespit edilerek olası olumsuz etkiler en düşük seviyeye indirilebilir ve saldırılara karşı erken önlem alınabilir.

Threat Detection (Tehdit Algılama)

Tehdit algılama süreci, sistemlere yönelik anormal hareketlerin belirlenmesini ve olası saldırıların erken tespit edilmesini kapsar. Bu süreçte kural tabanlı algılama, davranışsal analiz ve yapay zekâ destekli tehdit tespit yöntemleri kullanılır. Yetkisiz erişim girişimleri, kimlik avı saldırıları, kötü amaçlı yazılım aktiviteleri gibi tehditler belirlenerek, güvenlik olayları hakkında hızlı aksiyon alınması sağlanır.

Incident Response (Olay Müdahalesi)

SOC ekipleri, tespit edilen güvenlik olaylarına hızlı ve etkili bir şekilde müdahale eder. Olay müdahale süreci, tehdidin tespit edilmesiyle başlar etkilenen sistemlerin izole edilmesi, saldırının kaynağının belirlenmesi, zararlı süreçlerin sonlandırılması, güvenlik açıklarının kapatılması ve sistemin normal çalışma sürecine devam etmesi aşaması ile sonlanır. Müdahale sonrası analizlerin yapılmasıyla beraber olası bir diğer benzer saldırıların yaşanmaması için bir dizi önlemler alınır.

Threat Hunting (Tehdit Avcılığı)

Tehdit avcılığı, pasif izleme ve algılama süreçlerinden farklı olarak proaktif bir yaklaşımla tehditleri araştırmayı içerir. SOC analistleri, MITRE ATT&CK çerçevesi gibi metodolojileri kullanarak gelişmiş saldırıları tespit etmeye çalışır. Bilinmeyen veya henüz gerçekleşmemiş saldırıları belirlemek analizler, TTP (Tactics, Techniques, and Procedures) incelemeleri ve anomali tespit yöntemleri kullanılır.

Reporting (Raporlama)

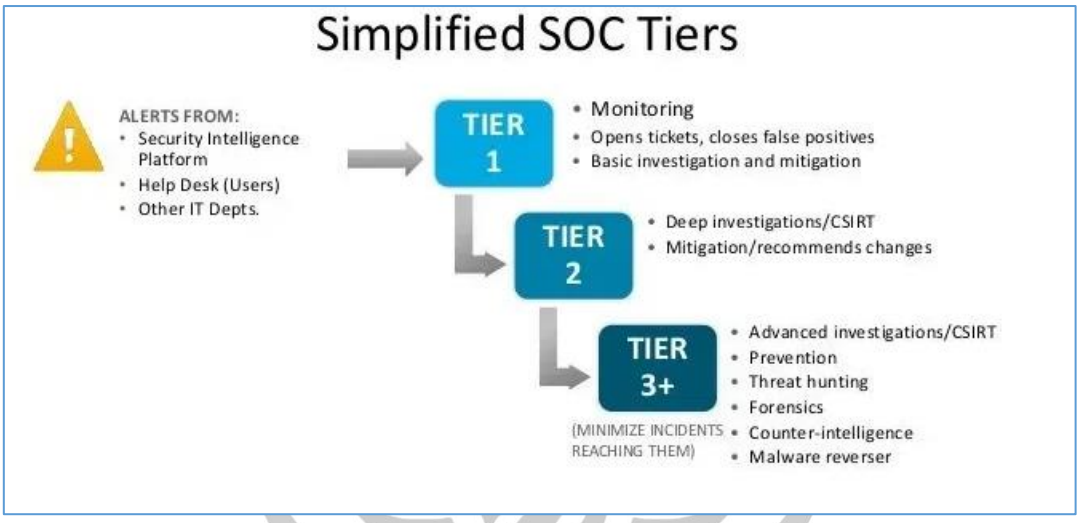
Güvenlik olayları, tehdit analizleri ve alınan önlemler düzenli olarak raporlanarak oluşumun güvenlik durumu değerlendirilir. Günlük olay raporları, haftalık/aylık analiz raporları ve yönetim seviyesinde sunulan teknik raporlar, SOC'un etkinliğini artırır. Raporlar sayesinde saldırı trendleri belirlenir, güvenlik açıkları analiz edilir ve organizasyonun siber güvenlik stratejisi güçlendirilmeye çalışılır.

Continuous Improvement (Sürekli Gelişim)

Siber tehditler sürekli geliştiği için SOC ekipleri de kendilerini geliştirmek zorundadır. Daha önce yaşanan saldırılar analiz edilerek sistem güvenliği konusunda iyileştirmeler yapılır. Düzenli zafiyet testleri ve simülasyonlar gerçekleştirilir. Red Team/Blue Team tatbikatları, yapay zekâ tabanlı tehdit tespit sistemlerinin entegrasyonu gibi yöntemler kullanılarak SOC'un siber tehditlere karşı dayanıklılığı arttırılmaya çalışılır.

SOC Seviyeleri (SOC Analyst Tier'ları)

SOC (Security Operations Center) analistleri, farklı uzmanlık seviyelerine göre sınıflandırılarak görev yapar. Bu seviyeler ile olayların ilk tespitinden ileri düzey tehdit avcılığına kadar uzanan bir hiyerarşi oluşturulmuş olur. Her seviye, oluşumun siber güvenliğini sağlamak için belirli sorumluluklar üstlenir ve tehditlere karşı proaktif savunma mekanizmaları geliştirir**.** Tier 1 analistleri ilk savunma hattı olarak güvenlik olaylarını izlerken, Tier 2 analistleri daha karmaşık tehditleri analiz eder ve olaylara müdahale eder. Tier 3 analistleri ise ileri seviye tehdit avcılığı yaparak saldırganların yöntemlerini ortaya çıkarır. SOC Manager ise tüm süreçlerin etkili bir şekilde yürütülmesini, ekip koordinasyonunun sağlanması ve stratejik planlamanın yapılmasını sağlar.



Şekil 3

Tier 1: Olay İzleme ve İlk Müdahale

Bu seviye ilk savunma hattıdır ve güvenlik olaylarını sürekli izleyen analistlerden oluşmaktadır.

SIEM (Security Information and Event Management) araçlarını kullanarak olayları analiz eder ve ardından sistemlerden gelen güvenlik uyarılarını (alert) inceleyerek ön eleme yapar. False positive alarmları ayıklayarak gereksiz müdahaleleri önler.

Özetle bu seviye, büyük ölçüde izleme, olayları sınıflandırma, önceliklendirme ve ön değerlendirme yapma sürecine odaklanır. Şüpheli aktivitelerin daha detaylı analizi için Tier 2'ye yönlendirilir.

Tier 2: Derinlemesine Analiz ve Olay Yönetimi

Tier 2 analistleri, Tier 1'den gelen olayları daha derinlemesine inceleyerek saldırı kapsamını tespit eder.

Olay günlüklerini (logs) detaylı analiz ederek saldırı vektörlerini belirlemek, kötü amaçlı yazılım tespiti ve sistem ihlallerini araştırmak, saldırının kaynağını belirlemek ve olay müdahale süreçlerini yönetmek, Firewall, IDS/IPS, WAF ve antivirüs gibi güvenlik

çözümlerini kullanarak tehditleri engellemek, saldırıya uğrayan sistemleri izole etmek ve etkilenen bileşenleri belirlemek gibi detaylı incelemeleri yaparlar.

Özetle Tier 2 analistleri, olay yönetimi süreçlerini koordine eder ve tehditlerin daha fazla yayılmasını önlemek için hızlı aksiyon alırlar.

Tier 3: Tehdit Avcılığı ve Gelişmiş Analiz

SOC içindeki en deneyimli analistlerden oluşmaktadır. Gelişmiş tehdit avcılığı (threat hunting) ve saldırı analizi gerçekleştirir.

Şüpehli durumları veya anormallik tespiti için ileri seviye tehdit avcılığı yöntemlerini kullanmak, güvenlik araçlarını yapılandırarak yeni tehditlere karşı savunma mekanizmaları geliştirmek, siber tehdit istihbaratı (Threat Intelligence) kullanarak saldırı trendlerini analiz etmek, saldırganların kullandığı teknikleri, taktikleri ve prosedürleri (TTPs) belirlemek, APT (Advanced Persistent Threat) gibi gelişmiş saldırıları tespit etmek ve analiz etmek gibi incelemeler yaparlar.

Özetle Tier 3 analistleri, organizasyonun güvenliğini bir adım daha ileri götürmek amacıyla saldırganların yöntemlerini anlamaya ve önlemek için stratejiler geliştirmeye odaklanır.

SOC Manager:

SOC Manager, SOC operasyonlarını denetlemek ve ekip koordinasyonunu sağlamak, SOC analistleri arasındaki görev dağılımı yaparak iş sürecini optimize etmek, güvenlik olaylarının raporlanmasını ve sunulmasını sağlamak, düzenleyici kurallara uyumluluğu sağlamak gibi görevleri vardır.

Özetle SOC Manager, ekibin verimli çalışmasını sağlamak, olay müdahale süreçlerini yönetmek, organizasyon genelinde güvenlik politikalarının uygulanmasını denetlemek sorumlu ve organizasyonun siber güvenlik stratejilerini geliştirmeye katkıda bulunan güvenlik lideridir.

SOC Teknolojileri ve Araçları

SOC operasyonlarının etkili ve sürekli bir şekilde ilerlemesi için gelişmiş güvenlik teknolojileri ve araçlar kullanılır. Bu araçlar ile tehditlerin tespit edilmesi, analiz edilmesi, engellenmesi ve olay sonrası inceleme süreçleri yönetilir.

Şekil 4

SIEM (Security Information and Event Management)

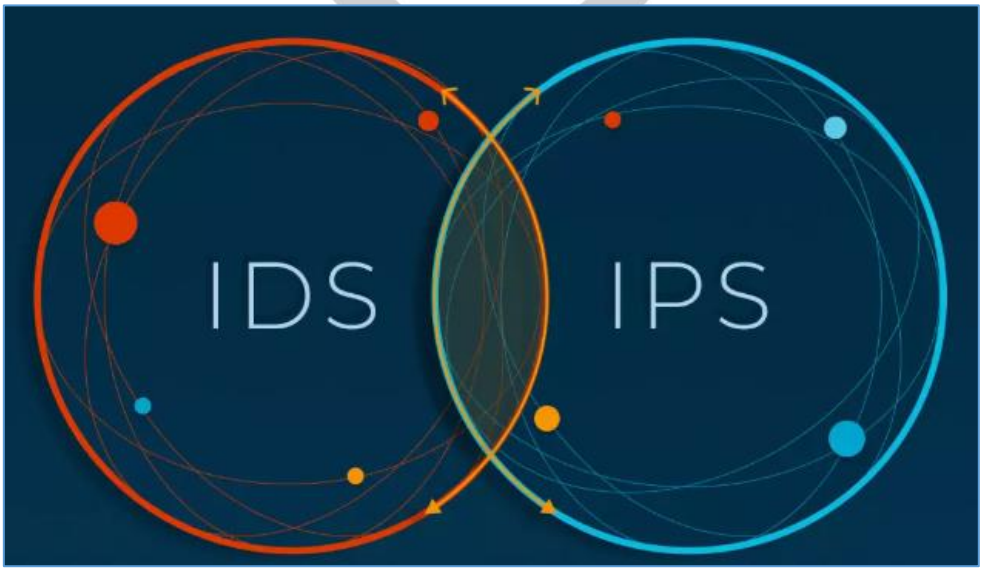
SIEM sistemleri, güvenlik olaylarını izlemek, analiz etmek ve korelasyon kurarak anlamlandırmak için kullanılan merkezi log yönetim platformlarıdır. SIEM, çeşitli kaynaklardan gelen logları toplayarak (sunucu, firewall vb) gerçek zamanlı analiz yapar ve anormal aktivitelerin tespiti konusunda yardım eder. SOC analistleri, SIEM' den gelen uyarıları değerlendirir.

Şekil 5

Splunk, IBM Qradar, Achsight, bilenen siem sistemleridir.

IDS/IPS (Intrusion Detection/Prevention Systems)

Saldırı Tespit ve Önleme Sistemleri (IDS/IPS), ağ trafiğini analiz ederek kötü amaçlı faaliyetleri belirlemek için kullanılır. IDS sistemleri yalnızca tehditleri tespit edip uyarı verirken, IPS sistemleri bu tehditleri aktif olarak engelleyerek güvenlik ihlallerini önler.

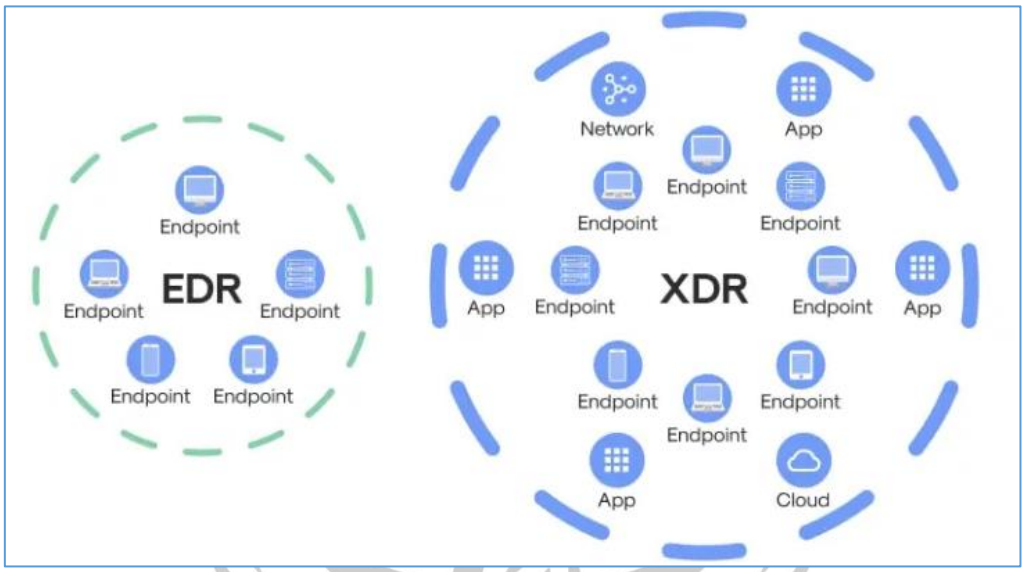


Şekil 6

Örnek olarak Snort, Palo Alto Networks Ngfw, Suricata ve Cisco firepower verilebilir.

EDR/XDR (Endpoint Detection and Response / Extended Detection and Response)

EDR çözümleri, uç noktalarda (bilgisayarlar, sunucular, mobil cihazlar) gerçekleşen güvenlik olaylarını izleyerek tehditleri tespit eder ve yanıt verir. Şüpheli davranışlar analiz edilerek uç noktalara yönelik saldırılar etkisiz hale getirilir. XDR ise EDR'in daha geniş kapsamlı versiyonu olup, ağ, e-posta ve bulut güvenliği gibi farklı güvenlik katmanlarını entegre bir şekilde analiz eder.

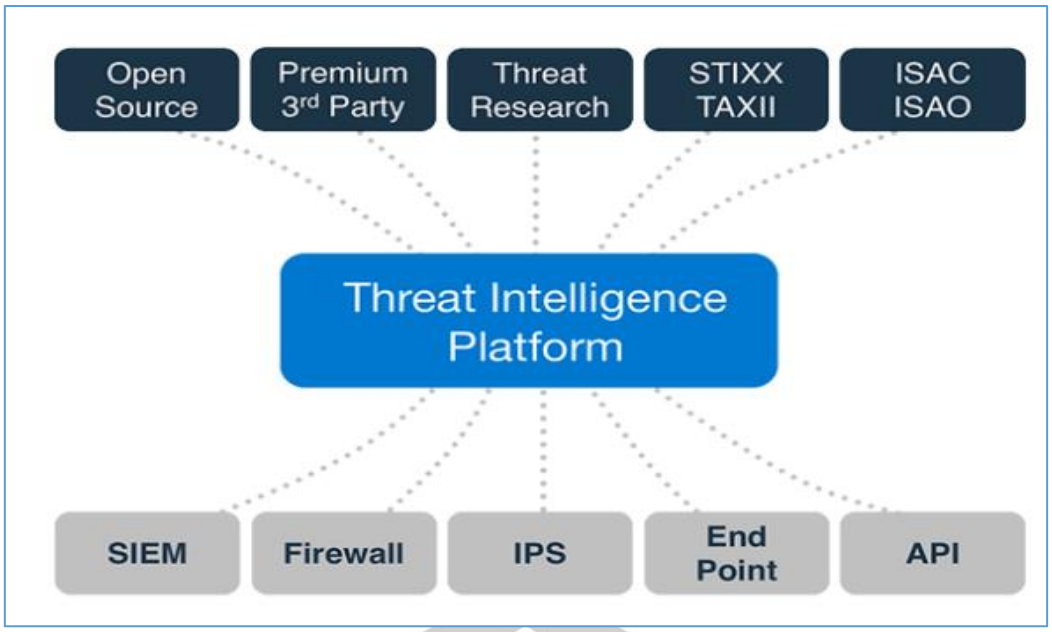


Şekil 7

Örnek olarak Micrsoft Defender for Endpoint, Synmantec endpoint security, Crowstrike Falcon verilebilir.

Threat Intelligence Platformları

Tehdit istihbaratı platformları, güncel siber tehditleri izlemek, analiz etmek ve bu tehditlere karşı proaktif savunma önlemleri geliştirmek için kullanılır. Bu platformların aktif bir şekilde kullanılması ile, zararlı IP adresleri, kötü amaçlı yazılım imzaları, saldırganların kullandığı yöntemler ve diğer tehdit bilgilerini toplayarak SOC süreci daha etkili ilerlemektedir. Tehdit istihbaratı sayesinde, güçlü savunma stratejileri oluşturabilir.



Şekil 8

Örnek olarak Virustotal, IBM X-Force, MISP (Malware information sharing platform) verilebilir.

Forensic ve Log Analiz Araçları

Adli bilişim (forensic) ve log analiz araçları, olay sonrası incelemelerde kritik bir rol oynar. Bir güvenlik ihlali meydana geldiğinde, bu araçlar sayesinde saldırının nasıl gerçekleştiği, hangi sistemlerin etkilendiği ve saldırganın izlediği yöntemler detaylı bir şekilde analiz edilir.

Log analiz araçları, sistemler tarafından üretilen kayıtları inceleyerek saldırının izlerini sürmeyi sağlar. Adli bilişim çözümleri ise, verilerin bütünlüğünü koruyarak hukuki süreçlerde delil olarak kullanılabilecek incelemeler yapmaya olanak tanır.

Şekil 9

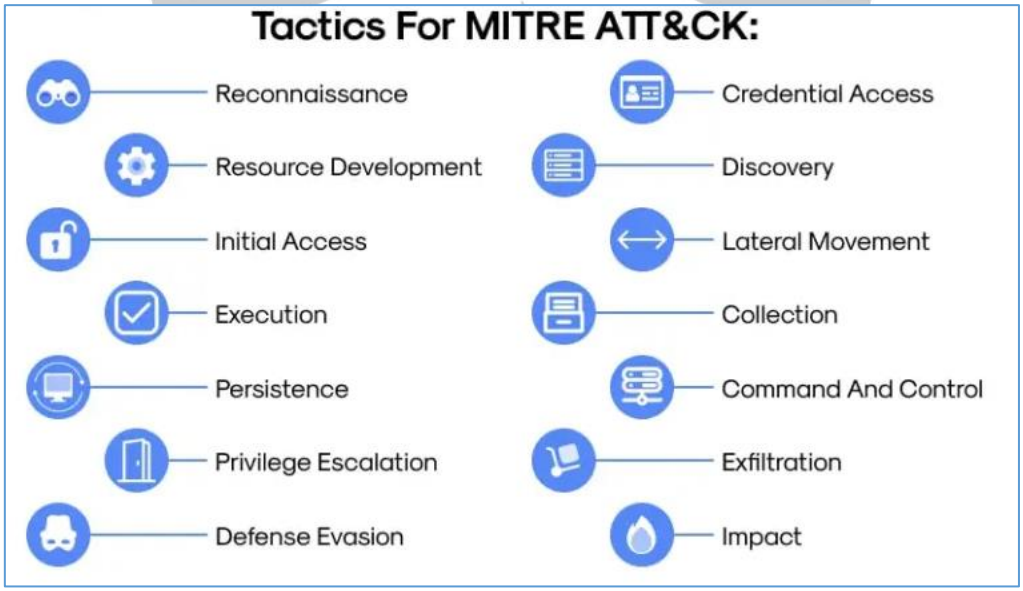
Örnek olarak Autopsy, Volatility, Wireshark, Splunk verilebilir.

SOC İçin Kullanılan Metodolojiler

SOC sürecinde, tehditlerin tespit edilmesi, analiz edilmesi ve olay müdahale süreçlerinin etkili bir şekilde yönetilmesi için kullanılan metodolojiler ve çerçeveler, saldırıların nasıl gerçekleştiğini anlamaya, tehdit aktörlerinin izlediği yolları analiz etmeye ve güvenlik önlemlerini stratejik bir şekilde uygulamaya yardımcı olmakla birlikte gün sonunda olay müdahale süreçlerinin standartlaştırılması ve iyileştirilmesine rehberlik eder. Bazı temel metodolojiler ve çerçeveler:

MITRE ATT&CK Framework

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), tehdit aktörlerinin sistemlere nasıl sızdığını, hangi yöntemleri kullandığını ve saldırılarını nasıl gerçekleştirdiğine dair taktik ve teknikleri detay konusunda yardımcı olan bir çerçevedir.



Şekil 10

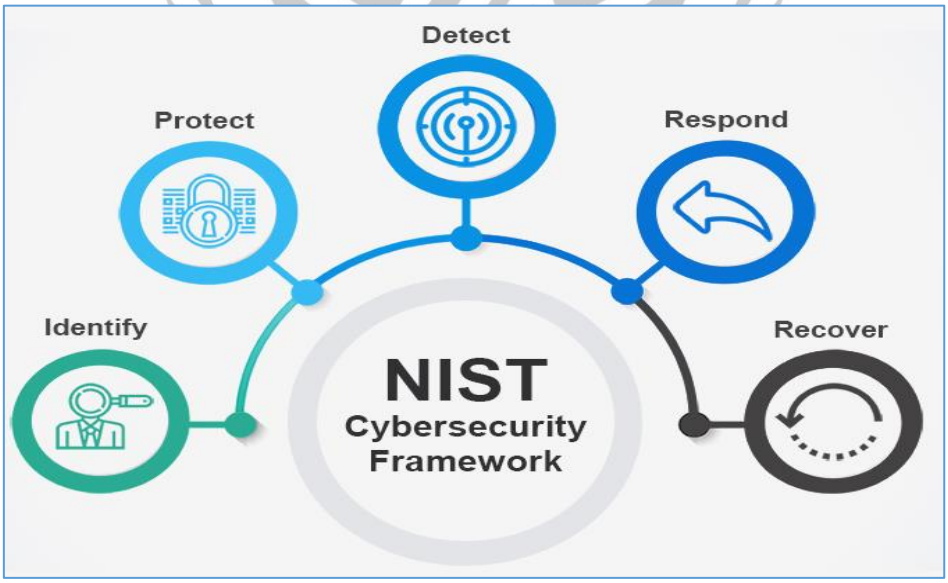
Cyber Kill Chain

Cyber Kill Chain, saldırıların aşamalarını anlamak ve bu aşamalara uygun güvenlik önlemleri geliştirmek için kullanılan bir metodolojidir. Lockheed Martin tarafından geliştirilmiş olan bu model, bir saldırının başlangıcından başarılı bir şekilde gerçekleştirilmesine kadar geçen süreci aşamalar halinde tanımlar. SOC sürecinde, saldırının hangi aşamasında olunduğunu belirlenerek, tehditleri erken aşamada durdurmak için gerekli önlemleri alınabilir.

Şekil 11

NIST Incident Response Framework

NIST (National Institute of Standards and Technology) tarafından geliştirilen Olay Müdahale Çerçevesi, güvenlik olaylarına müdahale sürecinin nasıl yürütülmesi gerektiğine dair kapsamlı bir rehberdir.



Şekil 12

ISO 27001

ISO 27001, bilgi güvenliği yönetim sistemleri (ISMS - Information Security Management System) için uluslararası bir standarttır. Bu standart, kuruluşların bilgi güvenliği süreçlerini etkin bir şekilde yönetmesini sağlayarak, veri gizliliği, bütünlüğü ve erişilebilirliğini korumaya yönelik politikalar ve kontroller belirler. SOC ekipleri için ISO 27001 uyumluluğu, güvenlik operasyonlarının standartlara uygun bir şekilde yürütülmesi ve sürekli iyileştirilmesi sağlanır.

Sonuç

Günümüz dijital dünyasında SOC (Security Operations Center), kurumların siber tehditlere karşı en önemli savunma hattıdır. Sürekli izleme, tehdit algılama ve olay müdahalesi gibi kritik süreçleri yöneterek saldırıları önceden tespit edip etkisiz hale getirir.

Ancak etkili bir SOC sadece teknolojiyle değil, bilgi güvenliği farkındalığı ve sürekli gelişim ile güçlenir. Kurumların, SOC yapılarını güçlendirerek siber güvenliği stratejik bir öncelik haline getirmesi hem kendi güvenliklerini sağlamalarına hem de daha güvenli bir dijital ekosistem oluşturmalarına katkı sağlar.

Siber tehditler her geçen gün daha gelişmiş ve karmaşık hale gelirken, SOC ekiplerinin tehdit avcılığı, olay yönetimi ve analiz yetkinliklerini geliştirmesi büyük önem taşımaktadır. Bu nedenle, güvenlik operasyon merkezleri yalnızca savunma yapmakla kalmamalı, aynı zamanda proaktif yaklaşımlar benimseyerek tehditlere karşı bir adım önde olmayı hedeflemelidir.

Kaynakça

1. https://www.gaissecurity.com/blog/soc-nedir-ve-soc-merkezleri-nasil-calisir
2. https://www.ibm.com/think/topics/security-operations-center
3. https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/security-operations-center-soc/
4. https://cyberartspro.com/security-operations-center-soc/
5. https://www.micromindercs.com/blog/soc-operations-and-processes
6. https://www.fortinet.com/resources/cyberglossary/what-is-soc
7. udemy
8. https://business.ewe.de/telekommunikation/it-security/soc
9. https://alpbatursahin.medium.com/soc-1-soc-nedir-32d28d7f0383
10. https://letsdefend.io/blog/soc-analyst-levels-description-requirements-career
11. https://www.netova.com.tr/soc-consultancy.php
12. https://secromix.com/blog/siber-guvenlikte-siem-neden-onemli-avantajlari-neler/
13. https://amnafzar.ir/en/Intrusion-detection-and-prevention-systems-IDS-IPS
14. https://lab.wallarm.com/what/what-is-xdr/
15. https://www.linkedin.com/pulse/cyber-threat-intelligence-platforms-tips-forensics-
16. https://www.infinitumit.com.tr/dijital-adli-bilisim-computer-forensic/
17. https://lab.wallarm.com/what/what-is-the-mitre-attck-framework/
18. https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu
19. https://cyberwatching.eu/nist-cybersecurity-framework