CYBER KILL CHAİIN

Hazırlayan

Neslihan Aslan

14/02/2025

İçindekiler

Giriş

Gün geçtikçe bireylerden büyük şirketlere, devlet kurumlarından kritik altyapılara kadar herkes, giderek karmaşıklaşan siber saldırıların hedefi olabilmektedir. Tehditler sadece veri ihlalleriyle sınırlı kalmamakla beraber finansal kayıplara, operasyonel aksaklıklara, ulusal güvenliği tehlikeye atan geniş çaplı krizlere kadar yol açabiliyor.

Güvenlik sektörü, uzun yıllar boyunca saldırılara savunmacı bir yaklaşımla yanıt verdi Ancak tehdit aktörleri, gelişen teknolojileri kullanarak her geçen gün daha tespit edilmesi zor yöntemler geliştirdikçe, savunma stratejilerinin de geliştirilmesi kaçınılmaz hale geldi. Artık yalnızca saldırı gerçekleştiğinde müdahale etmek yeterli olmuyor; saldırıları erken aşamalarda tespit etmek ve engellemek en önemli nokta haline geldi.

Bu durumda, tehditlerin daha iyi anlaşılmasını ve etkili karşı önlemler geliştirilmesini sağlayan modeller ortaya çıktı. Modellerden biri de Cyber Kill Chain'dir. Siber saldırı süreçlerini aşamalara ayırarak analiz eden bu yaklaşım, tehditleri kaynaklarında durdurmayı, saldırganların ilerlemesini engellemeyi ve güvenlik önlemlerini proaktif bir yapıya kavuşturmayı amaçlar.

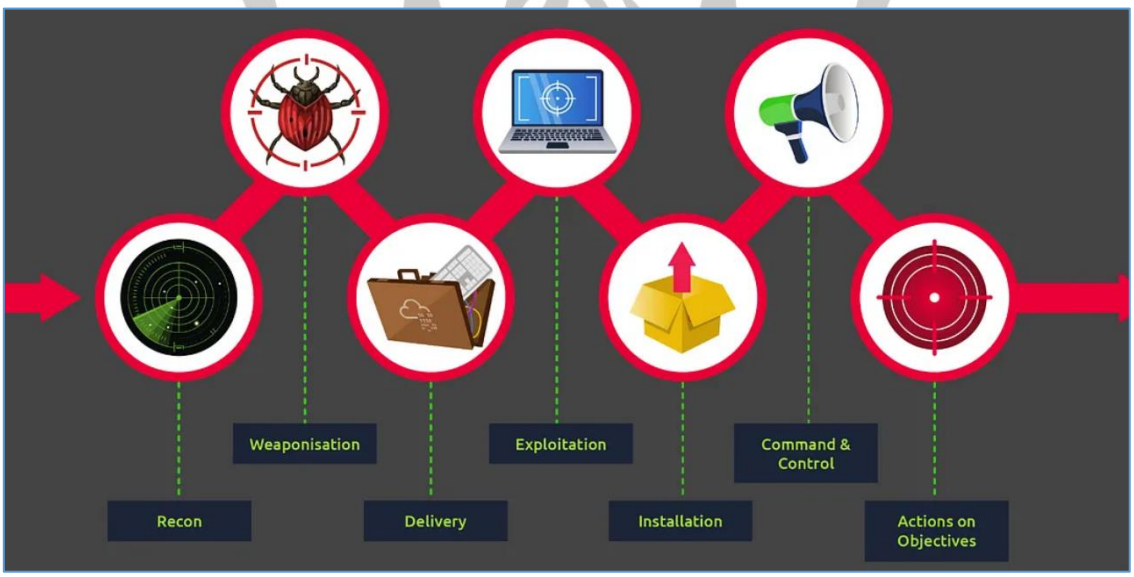
Cyber Kill Chain Nedir?

Cyber Kill Chain, siber saldırıları analiz ederek savunma stratejilerinin oluşturulmasına yardımcı olan sistematik bir güvenlik metodolojisidir. Bu model, bir saldırının keşif aşamasından başlayarak hedefin ele geçirilmesine kadar izlediği süreci aşamalara ayırarak, tehditlerin erken tespit edilmesini ve engellenmesini sağlar.

Saldırganlar, başarılı bir saldırı gerçekleştirebilmek için belirli aşamalardan geçmek zorundadır. Cyber Kill Chain, bu aşamaları detaylı bir şekilde tanımlayarak saldırı zincirinin her halkasında önlem alma imkânı sunar.

Bu model, askeri operasyonlardaki "öldürme zinciri" (kill chain) kavramına dayanmaktadır. Bu yaklaşımda, bir tehdidin belirlenmesi, izlenmesi ve ortadan kaldırılması için sistematik bir şekilde ilerlenir. Lockheed Martin tarafından 2011 yılında siber güvenlik alanına uyarlanan Cyber Kill Chain modeli, saldırganların hareketlerini anlamayı ve saldırıları daha başlamadan engellemeyi amaçlamaktadır.

Cyber Kill Chain metodolojisi, siber saldırıların karmaşıklığını anlaşılır ve yönetilebilir hale getirerek tehditlerin etkili bir şekilde analiz edilmesine, saldırıları erken aşamada durdurulmasına olanak tanır.



Şekil 1 Cyber Kill Chain Modeli

Cyber Kill Aşamaları

Her aşama, saldırının ilerlediği bir adımı temsil eder ve aynı zamanda saldırganın hangi süreçlerden geçtiğini anlamayı kolaylaştırarak savunma için müdahale edilebilecek kritik noktalar sunar.

1. Reconnaissance

İlk basamak olan bu aşamada saldırgan, hedef sistem, ağ yapısı ve kullanıcılar hakkında bilgi toplar. Açık kaynak istihbaratı (OSINT), pasif keşif yöntemleri ve ağ taramaları bu aşamada yaygın olarak kullanılır. Saldırganlar, genellikle sosyal mühendislik taktiklerinden ve sistemin zafiyetlerini ortaya çıkaran araçlardan yararlanır.

2. Weaponization

Saldırgan, keşif aşamasında elde ettiği bilgiler kullanılarak bir saldırı aracı veya zararlı yazılım hazırlar. Bu süreçte exploit kitleri kullanılarak hedefin zafiyetlerinden faydalanılacak saldırı senaryoları oluşturulabilir. Genellikle kimlik avı e-postaları**,** zararlı yazılım yükleyicileri ve sistem açıklarını istismar eden araçlar geliştirilir. Özetle bu aşama saldırı silahının belirlendiği aşamadır diyebiliriz.

3. Delivery

Bu aşamada saldırgan, hazırladığı zararlı yazılımı hedef sisteme ulaştırmaya çalışır. Teslimat genellikle oltalama e-postaları (phishing), kötü amaçlı web siteleri, zararlı bağlantılar veya taşınabilir medya aygıtları (USB gibi) aracılığıyla gerçekleştirilir. Saldırganın amacı, kurbanın bu zararlı içeriği açmasını veya çalıştırmasını sağlamaktır.

4. Exploitation

Teslim edilen zararlı yazılım, hedef sistemdeki güvenlik açıklarını kullanarak saldırıyı başlatır. Bu aşamada genellikle uzaktan kod yürütme (RCE), kötü amaçlı script çalıştırma veya sistem konfigürasyonlarının kötüye kullanılması gibi yöntemler uygulanmaktadır.

5. Installation

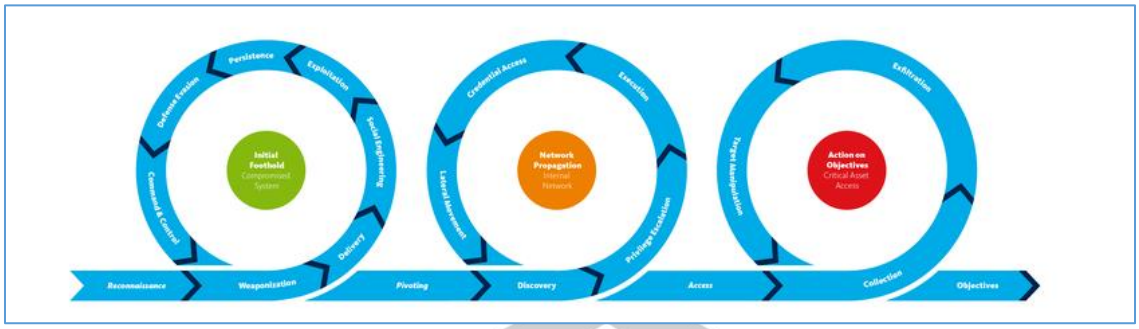
Saldırgan, sistemde kalıcı erişim sağlamak için zararlı yazılımı kurar. Bu aşamada rootkitler, uzaktan erişim truva atları (RAT) veya sistem yapılandırmalarında yapılan değişiklikler kullanılarak saldırının tespit edilmesi zorlaştırılır. Bu aşama saldırgan kontrolü ele alabileceği için saldırının yaşam döngüsünde bir dönüm noktasıdır.

6. Command & Control- C2

Bu aşamada saldırgan, ele geçirdiği sistemle uzaktan iletişim kurarak onu kontrol altına alır. Genellikle şifrelenmiş komut ve kontrol (C2) kanalları, DNS tünelleme veya proxy bağlantıları gibi teknikler kullanılarak saldırganın varlığı gizlenmeye çalışılır.

7. Actions on Objectives

Saldırganın nihai amacına ulaştığı aşamadır. Bu aşamada saldırgan hem veri sızdırma, fidye yazılımı saldırıları, sistem bozulması veya kritik altyapılara zarar verme gibi faaliyetler gerçekleştirilir hemde ağ boyunca yanal olarak hareket etmek, erişimini genişletmek ve ilerisi için daha fazla giriş noktası oluşturmak için de çabalayabilir.



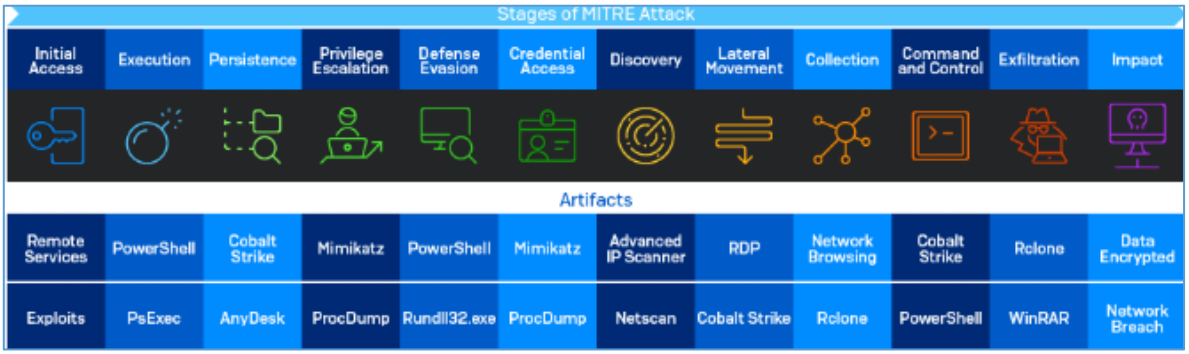
Şekil 2

Cyber Kill Chain ve Diğer Tehdit Modellerinin Karşılaştırılması

Cyber Kill Chain, saldırı sürecini aşamalara ayırarak tehditleri anlamaya yardımcı olan yaklaşımlardan biridir. Siber güvenlikte tehditlerin tespiti ve analizi için farklı modeller geliştirilmiştir. Siber tehditlerin giderek daha karmaşık hale gelmesiyle birlikte, MITRE ATT&CK, NIST Cybersecurity Framework (CSF) ve Diamond Model gibi farklı analiz yöntemleri de kullanılmaktadır. Her model, tehditlerin farklı yönlerini ele alarak daha kapsamlı bir bakış açısı sunar.

MITRE ATT&CK

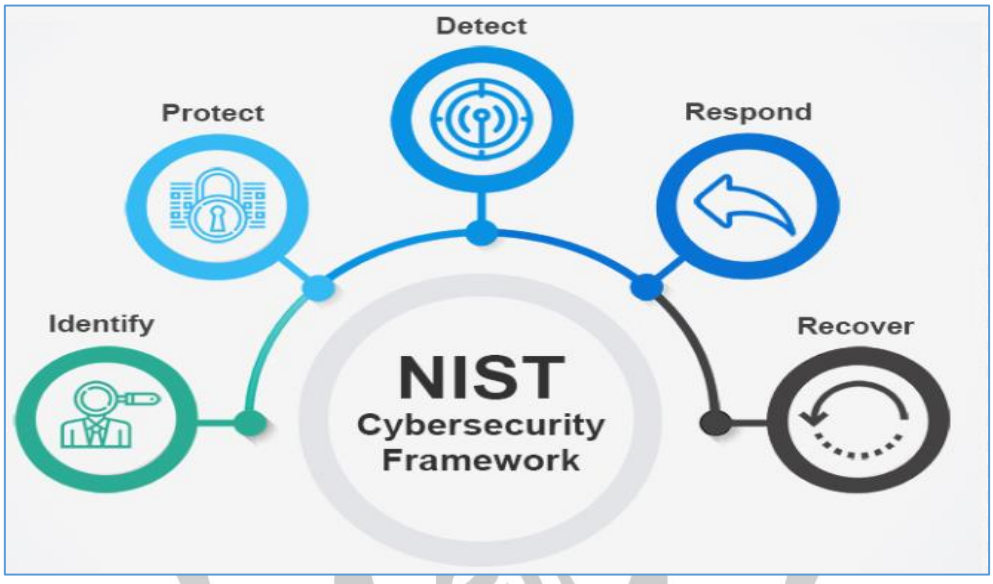
MITRE ATT&CK, en yaygın kullanılan modellerden biridir. Saldırganların çeşitli adımlarda kullandığı taktik, teknik ve prosedürleri (TTP) detaylandıran bir bilgi tabanıdır. Cyber Kill Chain modelinden farklı olarak, ATT&CK saldırının nasıl gerçekleştiğine ve hangi tekniklerin kullanıldığına odaklanır.



Şekil 3

NIST Cybersecurity Framework

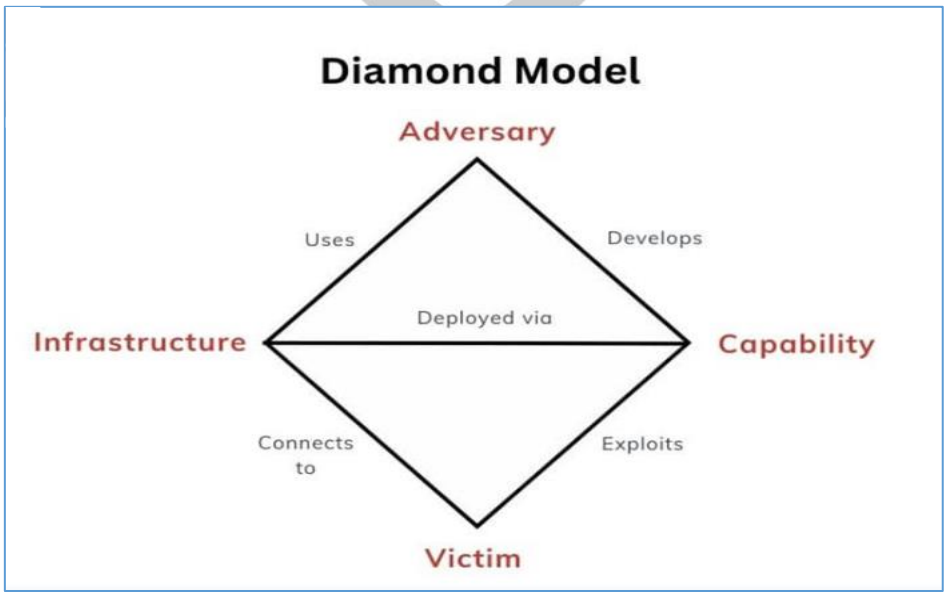
NIST, saldırıların teknik detaylarından ziyade daha çok siber güvenlik risk yönetimi üzerine yoğunlaşan bir çerçevedir. Cyber Kill Chain gibi saldırı aşamalarına odaklanmaz; bunun yerine, organizasyonların güvenlik süreçlerini geliştirmesi ve tehditlere karşı daha hazırlıklı olması için temel fonksiyonlar tanımlar. Oluşumun özel ihtiyaçlarına göre uyarlanabilir.



Şekil 4

Diamond Model

Bu model, saldırıları takım çalışmasıyla analiz etmeyi ve böylece saldırganın hareketlerini daha iyi anlamayı sağlar. Cyber Kill Chain ile saldırıları zaman içinde nasıl ilerlediğini görebilirken, bu model ile saldırının bileşenleri arasındaki ilişkileri görebiliriz.



Şekil 5

Özellikler	Cyber Kill Chain	Mitre Attack	Nist	Diamond
Odak Noktası	Saldırı aşamaları	Saldırı teknikleri	Risk yönetimi	Tehdit analizi ve ilişkilendirme
Yaklaşım	Lineer saldırı modeli	Taktik ve teknik odaklı	Çerçeve bazlı yönetim	Saldırgan, hedef, altyapı ve yetenek ilişkisi
Kapsam	Saldırı sürecini analiz eder	Gerçek saldırı tekniklerine odaklarınır	Organizasyonel güvenlik süreçlerini yönetir	Tehdit aktörlerini ve saldırı altyapısını değerlendirir
Avantajları	Saldırıları belirli aşamalara ayırır ve analiz eder	Gerçek saldırı tekniklerine dayalı güncellemeler içerir	Riskleri azaltmaya yönelik yönetim ve politika odaklı	Tehdit istihbaratı güçlenir ve saldırılar ilişkilendirilir
Zayıf Yönleri	Güncel saldırı karmaşıklığını yansıtmaması	Teknik detayları fazla olabilir ve uygulaması zor	Uygulaması zaman alabilir	Saldırılar arası ilişkilendirme bazen zor olabilmektedir

Cyber Kill Chain'e Karşı Savunma

Siber saldırılar, belirli aşamalardan oluşan bir süreç izler ve bu süreci kesintiye uğratmak, savunma mekanizmalarının temel hedeflerinden biridir. Cyber Kill Chain modeli, saldırganların hangi aşamalardan geçtiğini anlamayı sağlarken, savunma ekiplerinin de etkili önlemler almasına yardımcı olur. Cyber Kill Chain modelini anlamak, savunma stratejilerinin geliştirilmesi için kritik öneme sahiptir.

- Proaktif Tehdit Avcılığı
- Güvenlik Farkındalığı Eğitimleri
- Olay Müdahale Planları
- Ağ Segmentasyonu
- Tehdit İstihbaratı

Tehdit istihbaratından faydalanarak saldırganların yöntemleri analiz edilebilir, ağ ve erişim denetimleriyle yetkisiz girişler önlenebilir, çalışanlar güvenlik farkındalığı konusunda eğitilmeli ve güçlü bir olay müdahale planı uygulanmalıdır. Böylece, siber saldırılar başlangıç seviyesinde durdurulabilir ve gerekli önlemler alınarak güvenlik seviyesi artırılabilir.

Sonuç

Siber güvenlik, teknolojinin gelişimiyle birlikte sürekli değişen ve dönüşen bir alan olmaya devam etmektedir. Saldırı teknikleri her geçen gün daha karmaşık hale gelirken, savunma stratejileri de bu değişime ayak uydurmalıdır.

Saldırganların kullandığı yöntemler çeşitlenirken, güvenlik yaklaşımları da tek bir modelle sınırlı kalmaktan çıkmış, farklı çerçeveler ve metodolojiler ortaya çıkmıştır. Cyber Kill Chain, saldırı süreçlerini aşamalara ayırarak tehditleri daha iyi analiz etmeye yardımcı olurken, farklı güvenlik çerçeveleri ise saldırganların taktiklerini, tekniklerini ve prosedürlerini daha ayrıntılı bir şekilde anlamamızı sağlamaktadır. Bu sayede, tehditlere karşı daha hazırlıklı hale gelinir ve saldırıları henüz başlangıç aşamasındayken durdurabilir.

Güçlü bir güvenlik anlayışı, sürekli izleme, bilinçlendirme çalışmaları, güvenlik politikalarının sıkılaştırılması ve olay müdahale süreçlerinin etkin bir şekilde yönetilmesini gerektirir. Oluşumların güvenliğini artırmak için sadece teknik önlemler değil, aynı zamanda insan faktörünü ve süreçleri de göz önünde bulundurmak büyük önem taşır. Eğitim ve farkındalık bu noktada daha da önemli konumdadır.

Sonuç olarak, siber güvenlik dünyası sürekli gelişmeye devam edecek ve yeni tehditlerle birlikte yeni savunma yöntemleri de ortaya çıkacaktır. Bu nedenle, değişime ayak uydurabilen, güncel tehditleri takip eden ve çok katmanlı bir savunma anlayışını benimseyen oluşumlar, siber saldırılara karşı daha dirençli hale gelecektir.

Kaynakça

1. **https://bbsteknoloji.com/cyber-kill-chain-nedir/**
2. **https://www.securefors.com/cyber-kill-chain-nedir/**
3. **https://cyberartspro.com/en/cyber-kill-chain-nedir/**
4. **https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html**
5. **https://www.netskope.com/security-defined/cyber-security-kill-chain**
6. **https://berqnet.com/blog/cyber-kill-chain**
7. **https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/cyber-kill-chain/**
8. **https://abusix.com/blog/cybersecurity-frameworks-in-2024-explained-mitre-attck-cyber-kill-chain-diamond-and-nist/**
9. **https://berqnet.com/blog/cyber-kill-chain**
10. **https://medium.com/@AbhijeetSingh4/cyber-kill-chain-soc-level-1-tryhackme-walkthrough-ac77efd6425a**
11. **https://en.m.wikipedia.org/wiki/File:The_Unified_Kill_Chain.png**
12. **https://cyberwatching.eu/nist-cybersecurity-framework**
13. **https://kravensecurity.com/diamond-model-analysis/**
14. **https://docs.sophos.com/central/mdr/help/en-us/welcomeGuides/MDR/mitre/index.html**