Cyber Kill Chain

Hasan Karaca

4.02.2025

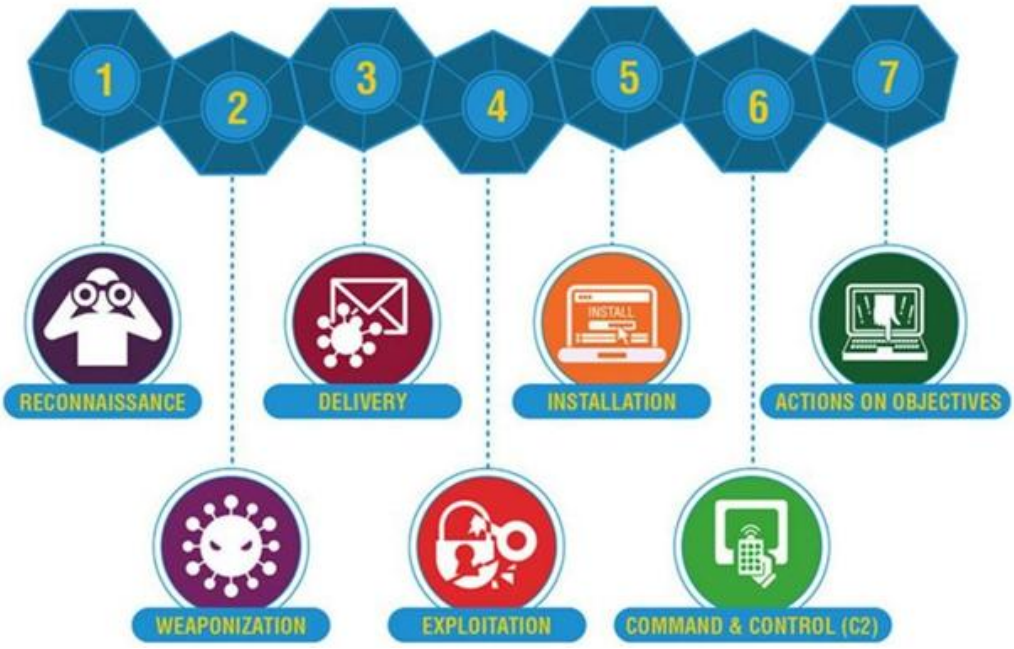
İÇİNDEKİLER

Cyber Kill Chain Nedir

Siber güvenlik modeli, siber saldırıların aşamalarını belirleyerek savunma stratejilerini daha etkin şekilde planlamaya yardımcı olur. Cyber Kill Chain, askeri terminolojiden esinlenerek siber saldırıları çeşitli aşamalarda tanımlayarak her aşamada saldırganın faaliyetlerini tespit edip durdurmak için savunma mekanizmaları oluşturulmasını önerir. Cyber Kill Chain, güvenlik ekiplerinin saldırıları daha iyi anlamalarına, önlemelerine veya karşılık vermelerine yardımcı olur.

Bu rapor, **Cyber Kill Chain** modelinin temel bileşenlerini, işlevlerini ve organizasyonlar için önemini açıklamayı amaçlamaktadır.

Cyber Kill Chain Aşamaları



1. Keşif (Reconnaissance):

Saldırı gerçekleşmeden veya bir istismar yaratılmadan önce keşif ve bilgi toplama aşamasıdır. Saldıran taraf; hedef sistem veya sistemler üzerinde çeşitli taramalar gerçekleştirerek zafiyetleri tespit etmeye çalışır ayrıca çalışanların isimleri, görevleri, e-mail adresleri, ip adresleri, ağ haritası çıkarma gibi eylemleri aktif ve pasif bilgi toplama araçlarıyla yapabildiği gibi, iş ilanları , linkedln , twitter , facebook , instagram gibi sosyal medya aracılığıyla hedef hakkında sosyal mühendislik yöntemleri ile bilgiler toplayabilir.

2. Silahlandırma (Weaponization):

Keşif sırasında bulunan zafiyetlerin sömürülmesi için kullanılacak yöntemlerin belirlenmesi ve uygun araçları hazırlama olarak tanımlanan aşamadır. Bu aşamada zafiyete uygun exploitler, zafiyetin istismar edilmesi için kullanılabilecek payloadlar olabileceği gibi zararlı dosyalar ve dokümanlar, oltalama saldırısında kullanılabilecek sahte epostalar gibi birçok yöntem kullanılarak sızma işlemi gerçekleştirilebilir.

3. Teslimat (Delivery):

Hazırlanan zararlının ve belirlenen yöntemle hedefe iletilmesi bu aşamadadır. Çeşitli açık kaynak kodlu yazılımlar, phishing, sosyal networkler veya tünellemeler gibi yöntemler kullanılabilir.

4. İstismar (Exploitation):

Oluşturulan zararlı ve belirlenen atak vektörünü kullanarak hedefin zafiyetinin sömürüldüğü aşamadır. Exploit hazırlanıp hedefe iletildikten sonra bu aşamada zararlı kod çalıştırılır.

5. Kurulum (Installation):

Hedefin sömürülmesi ardından, kalıcı bir tehdit haline gelmek, güvenlik sisteminin ötesinde sistem başarılı bir şekilde kontrol edilebilmesi için hedefe asıl zararlı yazılımın indirilmesi, zararlı yazılımın sistemde kalacağı süreyi mümkün olduğunca arttırmayı hedefleyen aşamadır.

6. Komuta ve Kontrol (Command and Control):

Saldırgan, hedef sistemi uzaktan kontrol edebilmek için bir komuta ve kontrol (C2) kanalı oluşturur. Bu kanal, saldırganın sistem üzerinde tam kontrol sahibi olmasını sağlar.

7. Hedeflere Ulaşma (Actions on Objectives):

Bütün aşamaları gerçekleştiren saldırgan kuruma erişim sağlamıştır ve bu aşamada, veri çalma, veri değiştirme , veri silme , veri şifreleme, sisteme zarar verme gibi eylemleri gerçekleştirebilir.

Cyber Kill Chain Kullanarak Tehditleri Önleme

Cyber Kill Chain modelini kullanarak tehditleri önlemek, her aşamada uygun savunma mekanizmaları oluşturarak mümkündür. Model, güvenlik ekiplerinin saldırının farklı aşamalarında saldırganın faaliyetlerini tespit ederek durdurmasına yardımcı olur. Ağ trafiği izleme ve analiz araçları kullanarak saldırganların bilgi toplama faaliyetlerini tespit edebilirsiniz. Şüpheli etkinlikleri belirlemek için anormal trafiği izlemeniz yeterlidir. E-posta filtreleme ve kötü amaçlı yazılım analiz araçları, zararlı içerikleri tespit edip engellemek için kullanılabilir.

SOC ve Cyber Kill Chain

Cyber Kill Chain, SOC analistleri için olay tespit ve müdahale süreçlerinde kritik bir rehber görevi görür. Bu model, bir siber saldırının keşif aşamasından hedef gerçekleştirme aşamasına kadar geçen yedi adımı tanımlayarak saldırganların izlediği yolu anlamayı sağlar. SOC analistleri, bu aşamaları takip ederek saldırıları erken tespit edebilir ve zamanında müdahale edebilir. Örneğin, keşif ve silahlandırma aşamalarında tehdit istihbaratı kullanılarak saldırı girişimleri belirlenebilir, teslimat ve istismar aşamalarında güvenlik duvarları, IDS/IPS ve SIEM sistemleri aracılığıyla zararlı aktiviteler engellenebilir. Kurulum ve komuta-kontrol aşamalarında ise anormal ağ trafiği ve şüpheli erişimler izlenerek tehditler durdurulabilir. Cyber Kill Chain modeli, SOC analistlerine tehditleri aşama aşama analiz etme ve uygun yanıt stratejileri geliştirme imkânı sunarak siber saldırılara karşı proaktif bir savunma sağlar

Kaynakça

- https://www.securefors.com/cyber-kill-chain-nedir/
- https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu
- https://berqnet.com/blog/cyber-kill-chain
- https://bbsteknoloji.com/cyber-kill-chain-nedir/
- ChatGPT