ALTAY TAKIMI

CYBER KILL CHAIN RAPORU

Hazırlayan : Efe Körün

Tarih : 07.02.2025

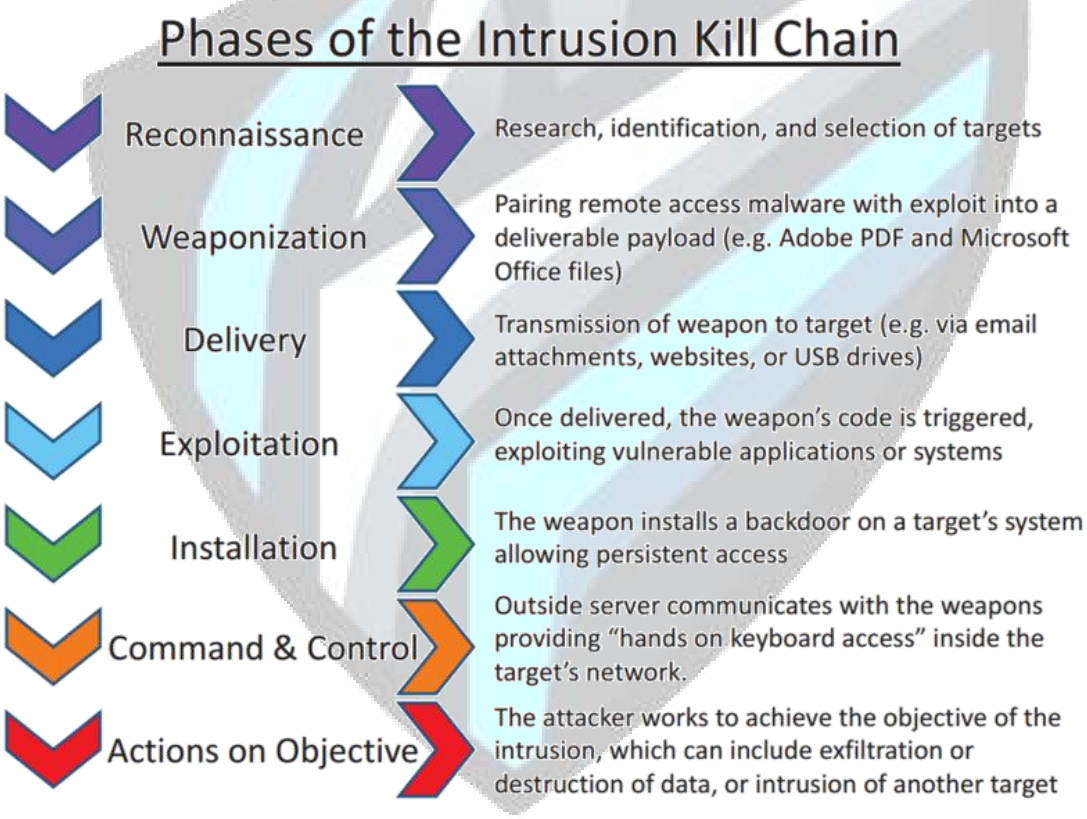
İÇİNDEKİLER

1. GİRİŞ

Siber saldırılar günümüzde kurumlar ve bireyler için ciddi bir tehdit oluşturmaktadır. Bu saldırıların tespit edilmesi ve önlenmesi için çeşitli güvenlik çerçeveleri geliştirilmiştir. Bunlardan biri de Cyber Kill Chain modelidir. Lockheed Martin tarafından geliştirilen bu model, bir siber saldırının yaşam döngüsünü aşamalara ayırarak analiz etmeye ve saldırılara karşı önleyici tedbirler geliştirmeye yardımcı olur.

Cyber Kill Chain modeli, saldırganların bir hedefi nasıl keşfettiğini, saldırıyı nasıl gerçekleştirdiğini ve sistemlere nasıl sızdığını anlamak için yapılandırılmıştır. Bu modelin anlaşılması, SOC (Security Operations Center) analistleri başta olmak üzere siber güvenlik uzmanları için kritik bir öneme sahiptir.

Bu rapor, Cyber Kill Chain'in kazanımlarını detaylandırarak saldırıların tespit edilmesi, analiz edilmesi ve engellenmesi konusundaki rolünü açıklamaktadır.



2. Cyber Kill Chain Nedir ?

➤Siber güvenlik dünyasında “Cyber Kill Chain” terimi, bir saldırının aşamalarını ve her aşamada ne yapılabileceğini anlamak için kullanılan bir modeldir. Lockheed Martin tarafından geliştirilmiş olan bu model, saldırganların bir siber saldırı gerçekleştirmek için takip ettiği adımları sistematik bir şekilde tanımlar. Cyber Kill Chain, savunma stratejilerinin geliştirilmesi ve saldırıların önlenmesi için kritik bir çerçeve sağlar.

➤Cyber Kill Chain’in mantığı, saldırganların her aşamada belirli adımları izleyerek bir saldırıyı gerçekleştirdiklerini varsayar. Bu model, savunucuların saldırının hangi aşamasında olduklarını anlamalarına ve saldırıyı durdurmak için gerekli önlemleri almalarına yardımcı olur. Cyber Kill Chain modeli, siber saldırılara karşı bütüncül bir savunma stratejisi geliştirilmesini sağlar.

➤Her aşama, saldırının durdurulabileceği bir fırsat penceresi sunar. Bu, savunucuların saldırıyı erken aşamalarda tespit edip durdurmasına olanak tanır. Cyber Kill Chain, saldırganların belirli bir düzende hareket ettiğini varsayar. Bu düzen, keşif aşamasından hedeflere ulaşma aşamasına kadar sistematik bir şekilde ilerler. Her aşamanın belirli zayıflıkları ve savunma stratejileri vardır.

3. Cyber Kill Chain Nasıl Çalışır?

➤Cyber Kill Chain, siber saldırının çeşitli aşamalarını belirleyerek çalışır. Her aşama, saldırganın belirli bir hedefe ulaşmak için gerçekleştirdiği adımları temsil eder. Saldırı aşamalarını anlamak, savunma ekiplerinin saldırganı erken tespit ederek saldırıyı engellemesine olanak tanır. Cyber Kill Chain'in temel çalışma prensibi, saldırganın faaliyetlerini erken aşamalarda durdurarak saldırının tamamlanmasını önlemektir.

4. Cyber Kill Chain Aşamaları Nelerdir?

➤Siber saldırıları analiz edebilmek amacıyla çeşitli modellerden birisi olan ve

Locheed Martin firması tarafından geliştirilen cyber kill chain keşif aşamasından

saldırı aşamasına kadar tanımlayan yedi temel aşamadan oluşmaktadır:

4.1. Keşif (Reconnaissance) ve Bilgi Toplama Süreci

➤Siber saldırılar gerçekleşmeden önce, saldırganlar hedef sistem hakkında mümkün olduğunca fazla bilgi edinmek için keşif ve bilgi toplama sürecine başlarlar. Bu aşama, saldırganın hedefin zafiyetlerini anlamasına ve saldırıyı şekillendirmesine yardımcı olur.

Keşif süreci, pasif bilgi toplama ve aktif bilgi toplama olmak üzere ikiye ayrılır.

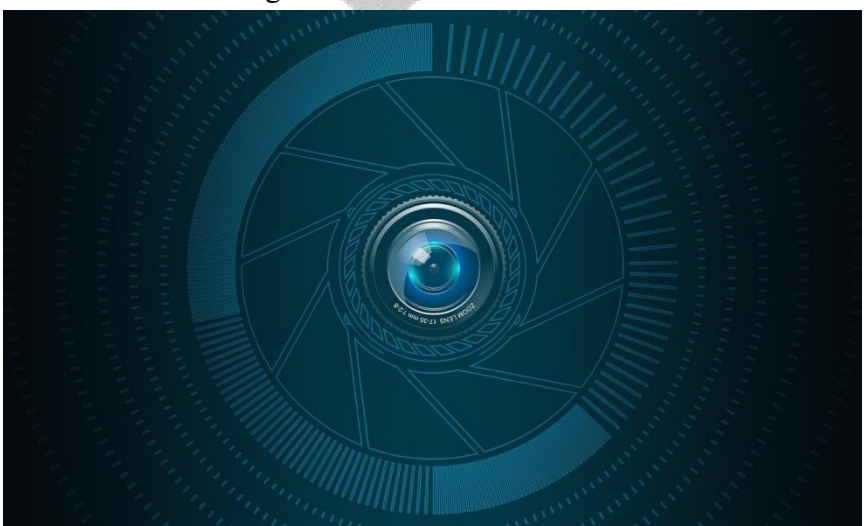
4.1.1. Pasif Bilgi Toplama

Pasif bilgi toplama, saldırganın hedef sistemle doğrudan etkileşime girmeden bilgi elde ettiği süreçtir. Bu yöntem, iz bırakmamak ve hedefin farkında olmamasını sağlamak için tercih edilir. Pasif bilgi toplama genellikle açık kaynak istihbaratı (OSINT - Open Source Intelligence) yöntemleri kullanılarak yapılır.

4.1.2 Aktif Bilgi Toplama

➤Aktif bilgi toplama sürecinde, saldırgan hedefle doğrudan etkileşime girerek bilgi toplar. Bu durum genellikle hedef sistemde iz bırakabilir, ancak saldırganlara daha fazla detay sunar.

➤➤Keşif aşaması, bir saldırının en kritik aşamalarından biridir. Saldırganlar, hedef sistem hakkında ne kadar fazla bilgiye sahip olursa, saldırıyı başarıyla gerçekleştirme olasılıkları o kadar artar. Bu nedenle, kuruluşların güçlü siber güvenlik politikaları uygulaması, sistemlerini güncel tutması ve saldırganların kullanabileceği pasif bilgi kaynaklarını minimize etmesi gerekmektedir.



4.2 Weaponization (Silahlandırma)

Siber saldırganlar, keşif aşamasında topladıkları bilgileri kullanarak hedef sisteme sızmak için silahlandırma (weaponization) aşamasına geçerler. Bu aşamada, hedef sistemde tespit edilen zafiyetler detaylı bir şekilde analiz edilerek uygun süzerlenebilir siber sılahlar geliştirilir. Saldrıganlar, bu aşamada kullanacakları teknikleri ve aracıları optimize ederek hedeflerine maksimum zarar vermeyi amaçlar.

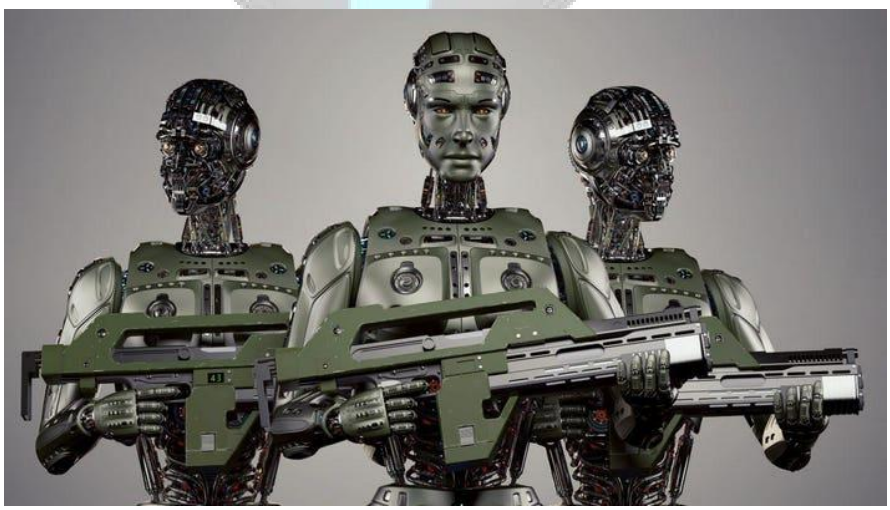
Silahlandırma aşamasında saldırganlar genellikle şu yöntemleri kullanır:

Exploit Geliştirme: Hedef sistemin zafiyetlerini istismar eden özel exploit kodları yazma veya mevcut exploitleri uyarlayarak etkili süzerlemeler yapma. Bu aşamada siber saldırganlar, exploit geliştirme için çeşitli tersine mühendislik tekniklerinden ve zafiyet analizlerinden faydalanır. Amaç, sistemdeki güvenlik açıklarını kullanarak sistemin kontrolünü ele geçirebilecek kodlar oluşturmaktır.

Zararlı Yazılım Oluşturma: Hedef sisteme bulaşacak özel virüsler, trojanlar, rootkitler veya ransomware hazırlama. Bu yazılımlar genellikle anti-virüs ve güvenlik yazılımları tarafından tespit edilmemesi için şifreleme ve gizleme teknikleri kullanılarak geliştirilir. Aynı zamanda, zararlı yazılımların özelleştirilerek belirli bir sisteme veya ağa yönelik çalışması sağlanabilir.

Sosyal Mühendislik Saldırıları: Kullanıcıları kandırarak zararlı dosyaları açmalarını sağlama (oltalama e-postaları, sahte web siteleri vb.). Bu aşamada siber saldırganlar, hedef kişi veya kurum hakkında toplanan bilgiler ışığında gerçekçi görünümde sahte mesajlar oluşturur. Örneğin, hedefin çalıştığı kurumun resmi bir biriminden geliyormuş gibi görünerek parola veya diğer hassas bilgilerin ele geçirilmesi amaçlanabilir.

➤➤Silahlandırma aşaması, bir siber saldırının başarıya ulaşması için kritik bir noktadır. Bu nedenle, savunma mekanizmalarının bu aşamaya yönelik olarak da güçlendirilmesi önem arz etmektedir. Kurumların, sık sık güncellenen exploit veritabanlarını ve zararlı yazılım analizlerini takip etmeleri, çalışanlarını sosyal mühendislik saldırılarına karşı bilinçlendirmeleri ve sıkı güvenlik politikaları uygulamaları gerekmektedir.



4.3 Delivery (Teslimat)

Delivery (Teslimat) aşaması, saldırganın silahlandırdığı (weaponized) saldırı aracını hedef sisteme ulaştırdığı kritik aşamadır. Bu aşamada saldırgan, exploit içeren kötü amaçlı dosyaları, oltalama e-postalarını veya ağ saldırılarını kullanarak zararlı yazılımı hedefe bulaştırmaya çalışır.Saldırganlar, teslimat aşamasında hedefin güvenlik mekanizmalarını atlatmak için çeşitli teknikler kullanır.

E-posta Yoluyla Teslimat: Oltalama (phishing) saldırıları kapsamında sahte e-postalar hazırlanarak, hedefin kötü amaçlı ekleri açması veya zararlı bağlantılara tıklaması sağlanır. Saldırganlar, kurumsal kimlikleri taklit eden e-postalar kullanarak saldırının meşru görünmesini amaçlar.

USB veya Taşınabilir Cihaz Kullanımı: Fiziksel erişim gerektiren bir yöntem olup, saldırganlar zararlı yazılım içeren USB bellekleri veya taşınabilir diskleri hedef kişilere ulaştırarak sisteme bulaşmasını sağlarlar. Bu teknik, özellikle iç ağlara erişim sağlamak için kullanılır.

Ağ Üzerinden Bulaştırma: Güvenlik açıkları bulunan sistemlere uzaktan erişim sağlayarak zararlı yazılımın yüklenmesi. Bu yöntem, özellikle açık portlar veya güvenlik yamaları eksik olan sistemleri hedef alır. Saldırganlar, kötü amaçlı ağ paketleri göndererek hedef sistemde kod çalıştırmayı amaçlarlar.

➤➤Teslimat aşaması, saldırının başarıya ulaşması için kritik bir adımdır ve bu nedenle kuruluşların güçlü güvenlik politikaları geliştirmesi gerekmektedir. Kullanıcı farkındalık eğitimleri, e-posta filtreleme çözümleri, ağ izleme sistemleri ve fiziksel güvenlik önlemleri ile bu aşamada gerçekleşebilecek saldırılar minimize edilebilir. Aynı zamanda, sistemlerin düzenli olarak güncellenmesi ve güvenlik açıklarının kapatılması saldırıların etkisini azaltmada önemli bir rol oynar.

4.4 Exploitation (İstismar)

Exploitation (İstismar) aşaması, saldırganın hedef sisteme gönderdiği zararlı yükü çalıştırarak zafiyeti istismar ettiği aşamadır. Bu aşamada saldırgan, keşif ve silahlandırma süreçlerinde belirlediği güvenlik açıklarını sömürerek hedef sistem üzerinde kontrol sağlamaya çalışır.

Saldırganlar, istismar aşamasında genellikle şu teknikleri kullanır:

Uzaktan Kod Çalıştırma: Hedef sistemde bulunan bir güvenlik açığından yararlanarak saldırganın kötü amaçlı kod çalıştırmasını sağlama. Bu yöntem, özellikle işletim sistemi veya uygulamalardaki kritik açıklar üzerinden gerçekleştirilir.

Yetki Yükseltme: Sistem içerisinde sınırlı haklarla erişim sağladıktan sonra, mevcut güvenlik açıklarını kullanarak yönetici yetkilerini ele geçirme. Bu sayede saldırgan, hedef sistem üzerinde tam kontrol sahibi olabilir.

Bellek İstismarı: Bellek taşması (buffer overflow) veya kod enjeksiyonu gibi tekniklerle sistemin normal işleyişini bozarak saldırganın kod yürütmesini sağlama. Bu yöntem, özellikle savunmasız uygulamalar ve işletim sistemlerinde etkili olabilir.

➤➤İstismar aşaması, saldırının doğrudan başarıya ulaştığı kritik bir süreçtir. Bu nedenle, organizasyonların güvenlik açıklarını sürekli olarak analiz etmesi, güncellemeleri zamanında yapması ve saldırı tespit sistemlerini aktif hale getirmesi büyük önem taşımaktadır. Ağ segmentasyonu, saldırı yüzeyini küçültmek için etkili bir yöntemdir ve siber güvenlik politikalarının güçlendirilmesi saldırganların başarı şansını azaltacaktır.

4.5 Installation (Kurulum)

Installation (Kurulum) aşaması, saldırganın hedef sisteme zararlı yazılımı kalıcı hale getirdiği ve sistem üzerinde tam kontrol sağlamaya çalıştığı kritik bir süreçtir. Bu aşamada, kötü amaçlı yazılım hedef sistemde çalıştırıldıktan sonra arka planda kendini sistem bileşenlerine entegre ederek tespit edilmesini zorlaştırır.

Saldırganlar, kurulum aşamasında genellikle şu teknikleri kullanır:

Kalıcı Arka Kapılar (Backdoors) Oluşturma: Sisteme gizli arka kapılar ekleyerek saldırganın gelecekte tekrar erişim sağlamasını mümkün hale getirme. Bu yöntem, özellikle hedef sistemin yeniden başlatılsa bile saldırganın erişimini sürdürebilmesi için kullanılır.

Rootkit Kullanımı: İşletim sisteminin çekirdek seviyesine sızarak saldırganın tespit edilmesini önleyen gelişmiş zararlı yazılımların yüklenmesi. Rootkitler, güvenlik yazılımlarını atlatmak ve sistemin savunmalarını etkisiz hale getirmek için yaygın olarak kullanılır.

Otomatik Çalıştırma Mekanizmaları: Zararlı yazılımın her sistem açılışında otomatik olarak çalışmasını sağlamak için görev zamanlayıcıları, başlangıç programları veya kayıt defteri değişiklikleri kullanma. Bu yöntem sayesinde saldırganın zararlı yazılımı sürekli aktif kalır.

➤➤Kurulum aşaması, saldırının uzun vadeli etkilerini artırmak için büyük önem taşır. Güvenlik ekipleri, sistem değişikliklerini izleyerek ve anormal aktiviteleri tespit ederek bu aşamayı engelleyebilir. Düzenli güvenlik taramaları, imza tabanlı ve davranışsal analiz yöntemleri ile saldırganların sistemde kalıcı hale gelmesini önlemek mümkündür.

4.6 Command and Control (C2) – Komuta ve Kontrol

Command and Control (C2) aşaması, saldırganın hedef sistem üzerinde tam kontrol sağladığı ve uzaktan komutlar gönderebildiği aşamadır. Bu süreçte, saldırganlar genellikle bir C2 altyapısı oluşturarak ele geçirilen sistemlerden bilgi toplar, kötü amaçlı komutlar çalıştırır ve sistem kaynaklarını yönetir.

Saldırganlar, C2 aşamasında şu teknikleri kullanır:

Gizli İletişim Kanalları: Zararlı yazılımlar, tespit edilmemek için HTTP/S, DNS tünelleme, şifreli bağlantılar veya sosyal medya gibi meşru hizmetler üzerinden saldırganla iletişim kurar.

Botnet Kullanımı: Ele geçirilen cihazları bir botnet ağına dahil ederek saldırıları yönetme ve dağıtık saldırılar gerçekleştirme. Bu yöntem, özellikle DDoS saldırılarında yaygın olarak kullanılır.

Komut Yürütme: Saldırgan, hedef sistem üzerinde uzaktan komutlar çalıştırarak dosya silme, veri çalma veya sistem yapılandırmalarını değiştirme gibi işlemleri gerçekleştirir.

Veri Sızdırma: Ele geçirilen sistemlerden kritik bilgileri saldırganın belirlediği sunuculara aktarma. Bu süreçte, saldırganlar genellikle şifreleme ve sıkıştırma yöntemleri kullanarak veri sızıntısını gizlemeye çalışır.

➤➤C2 aşaması, saldırının en tehlikeli bölümlerinden biridir çünkü saldırgan artık sistem üzerinde tam yetkiye sahip olabilir. Güvenlik önlemleri olarak, ağ trafiğinin düzenli olarak izlenmesi, anormal iletişim kalıplarının tespit edilmesi ve ağ segmentasyonu gibi yöntemler kullanılarak saldırganın kontrolünü kaybetmesi sağlanabilir.

4.7 Actions on Objectives (Hedeflere Yönelik İşlemler)

Actions on Objectives aşaması, saldırganın asıl hedefini gerçekleştirdiği ve sistemde kalıcı hasar veya veri hırsızlığı yaptığı aşamadır. Bu süreçte, saldırganın amacı bilgi sızdırmak, sistemleri devre dışı bırakmak, fidye talep etmek veya ağ içinde daha fazla yayılmak olabilir.

Saldırganlar bu aşamada genellikle şu yöntemleri kullanır:

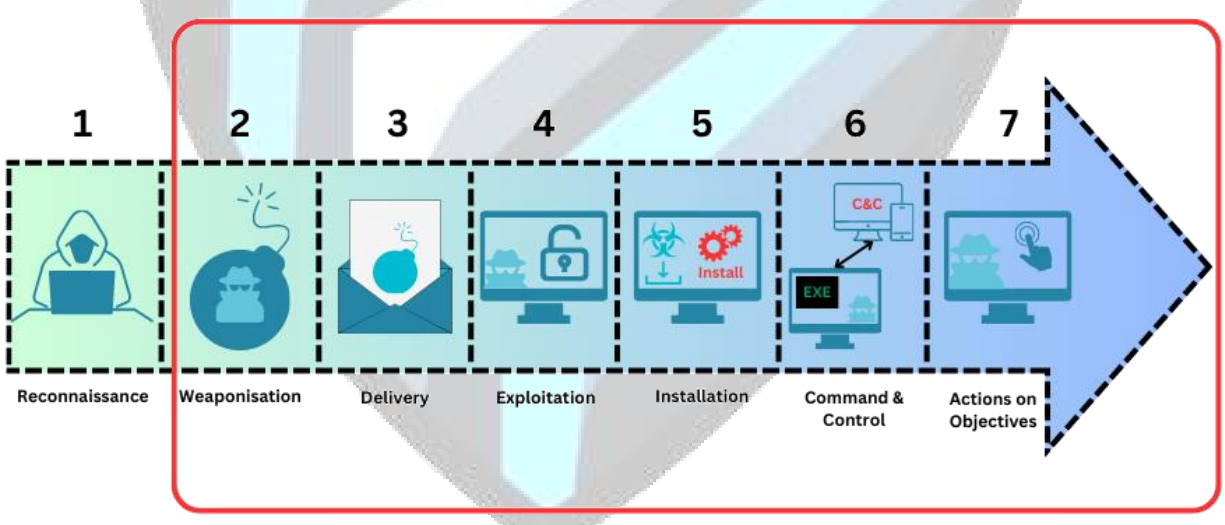
Veri Hırsızlığı: Hassas bilgilerin ele geçirilmesi ve üçüncü taraflara satılması veya kullanılması.

Fidye Yazılımları (Ransomware): Sistemleri şifreleyerek kurbanlardan fidye talep edilmesi.

Sistem Bozma (Sabotaj): Kritik altyapıların veya ağların devre dışı bırakılması.

Yanıltma ve İz Silme: Saldırının izlerini yok ederek tespit edilmekten kaçınma.

➤➤Bu aşamada etkili güvenlik önlemleri almak, izleme sistemlerini aktif tutmak ve olay müdahale planlarını güçlendirmek büyük önem taşır.



5. Cyber Kill Chain ile Siber Tehditleri Engelleme

➤Siber güvenlik tehditlerini en aza indirmek için Cyber Kill Chain modeli, saldırıların her aşamasında uygulanabilir savunma stratejileri geliştirilmesini sağlar. Erken tespit, ağ izleme, tehdit istihbaratı entegrasyonu ve zararlı yazılım analizleri, saldırganların sistemlere erişimini önlemek için kritik öneme sahiptir.

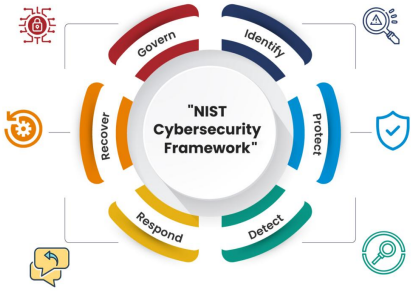
➤SOC ekipleri, SIEM (Security Information and Event Management) çözümleri, anormal trafik analizi ve Red Team/Blue Team çalışmaları ile saldırıları proaktif olarak tespit edip durdurabilir. Cyber Kill Chain'in diğer çerçevelerle entegre edilmesi, saldırı süreçlerinin daha iyi anlaşılmasını ve etkili bir savunma mekanizması oluşturulmasını sağlar.

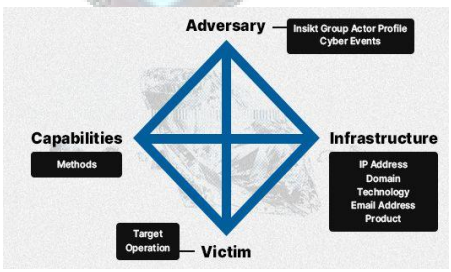
6. Cyber Kill Chain'in Diğer Güvenlik Framework'leriyle Karşılaştırılması

➤Siber güvenlik alanında tehditleri tespit etmek ve önlemek için birçok farklı çerçeve geliştirilmiştir. Cyber Kill Chain, saldırı süreçlerini aşamalara ayırarak analiz eden bir modeldir. Ancak, günümüzde MITRE ATT&CK, NIST Cybersecurity Framework (CSF) ve Diamond Model gibi diğer çerçevelerle birlikte kullanılması, güvenlik önlemlerinin daha kapsamlı hale gelmesini sağlar.

➤MITRE ATT&CK, saldırganların kullandığı teknikleri detaylı bir şekilde kategorize ederken, NIST CSF organizasyonların genel siber güvenlik stratejilerini belirlemelerine yardımcı olur. Diamond Model ise saldırgan ile hedef arasındaki bağlantıları analiz etmeye odaklanır. Cyber Kill Chain, bu çerçevelerle birlikte kullanıldığında, saldırıları daha erken tespit etme ve etkili müdahale sağlama imkanı sunar.

➤SOC ekipleri, Cyber Kill Chain'in saldırı sürecine odaklanan yapısını, MITRE ATT&CK'in detaylı taktiksel analizleriyle destekleyerek daha güçlü tehdit avcılığı yapabilir. Böylece, saldırganların sistemlere sızma sürecini en erken aşamalarda engellemek mümkün hale gelir.





MITRE ATT&CK™

7. Sonuç

➤Cyber Kill Chain modeli, siber saldırıların aşamalarını analiz ederek tehditleri daha iyi anlamamıza ve erken aşamada durdurmamıza yardımcı olan önemli bir güvenlik çerçevesidir. Keşif aşamasından hedefe yönelik saldırılara kadar süreci ayrıntılı bir şekilde ele alan bu model, savunma stratejilerinin geliştirilmesinde kritik bir rol oynar.

➤Bu raporda, Cyber Kill Chain modelinin her aşaması detaylandırılarak siber saldırganların izlediği yöntemler ve bu tehditlere karşı alınabilecek önlemler açıklanmıştır. Özellikle SOC ekiplerinin, SIEM çözümleri, anomali tespiti, tehdit istihbaratı ve saldırı simülasyonları gibi araçları kullanarak bu süreci daha etkin yönetebileceği vurgulanmıştır.

➤Günümüzde, siber tehditlerin giderek daha sofistike hale gelmesi, Cyber Kill Chain modelinin MITRE ATT&CK, NIST CSF ve Diamond Model gibi diğer güvenlik çerçeveleriyle birlikte kullanılmasını zorunlu kılmaktadır. Bu tür entegre yaklaşımlar, kurumların saldırıları erken tespit etmesini ve saldırganların ilerlemesini durdurmasını sağlayarak daha güçlü bir güvenlik altyapısı oluşturmasına yardımcı olacaktır.

➤Sonuç olarak, Cyber Kill Chain modeli, siber güvenlik dünyasında proaktif savunma mekanizmalarının oluşturulması için vazgeçilmez bir araçtır. Siber güvenlik ekiplerinin bu modeli etkin bir şekilde kullanması, saldırılara karşı daha dirençli ve hazırlıklı olmalarını sağlayacaktır.