MITTRE ATT&CK

13/02/2025

MURAT GÜRSOY

İçindekiler

Giriş

MITRE ATT&CK Framework, tehdit aktörlerinin kullandığı taktikleri, teknikleri ve prosedürleri (TTP) kategorize eden kapsamlı bir bilgi tabanıdır. Bu framework, güvenlik ekiplerinin saldırı yaşam döngüsünü anlamalarına, tehdit avı (Threat Hunting) ve saldırı tespit mühendisliği (Detection Engineering) süreçlerini geliştirmelerine yardımcı olur.

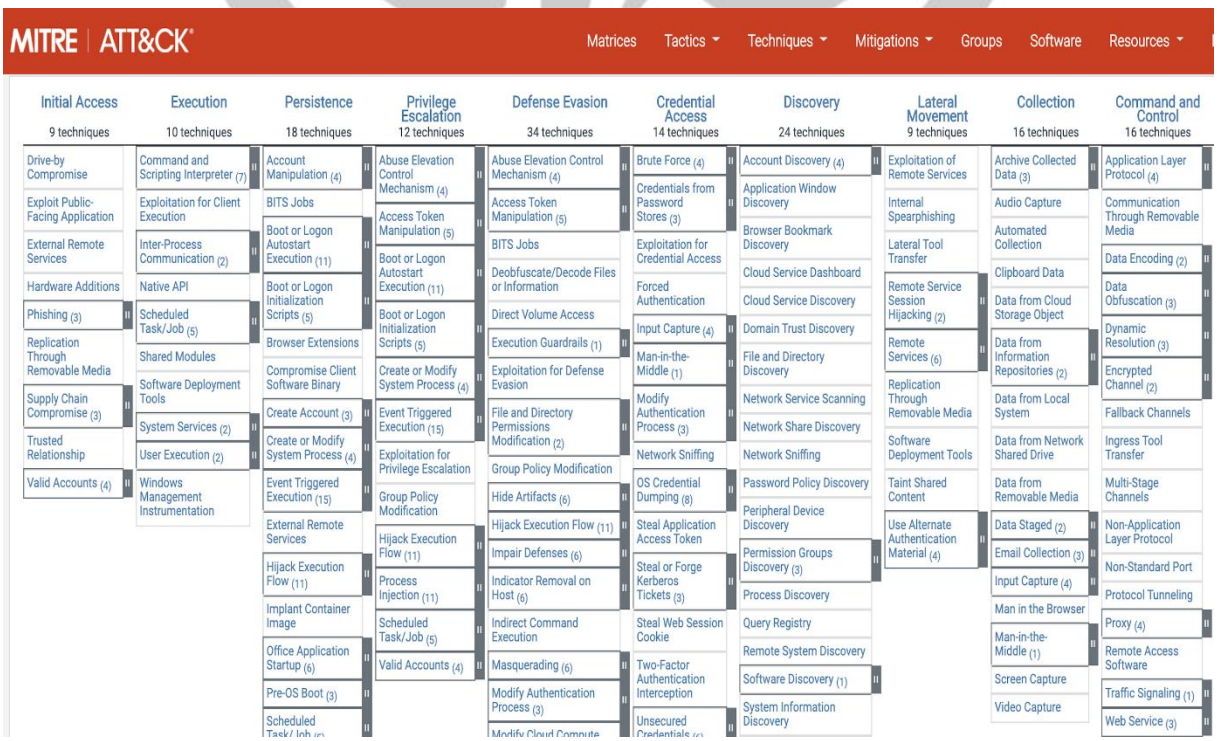
Bu raporda, MITRE ATT&CK tablosunun önemi, içeriği ve nasıl kullanıldığı detaylandırılacaktır. Ayrıca, tehdit aktörlerinin saldırı senaryoları çerçevesinde nasıl ilerlediği örneklenecek ve özellikle **2022 Ukraine Electric Power Attack (C0034)** incelenerek kullanılan teknikler analiz edilecektir. Son olarak, siber saldırıların nasıl gerçekleştiğini anlamak amacıyla bir şirketin siber saldırıya uğradığı bir senaryo oluşturulacak ve saldırının MITRE ATT&CK bağlamında taktikleri ve teknikleri açıklanacaktır.

Mitre Att&ck Framework

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), siber saldırganların kullandığı yöntemleri analiz etmek ve savunma stratejileri geliştirmek amacıyla oluşturulmuş açık kaynaklı bir bilgi sistemidir. MITRE Corporation tarafından geliştirilen bu framework, saldırganların kullandığı taktikler, teknikler ve prosedürleri (TTP) kategorize ederek siber güvenlik ekiplerinin tehditleri daha iyi anlamasına ve tespit etmesine yardımcı olur.

Mitre Att&ck Tablosu

Saldırganların siber sistemlere nasıl sızdığını, ağ içinde nasıl hareket ettiğini ve hedeflerine nasıl ulaştığını ayrıntılı bir şekilde gösterir. Ayrıca, farklı tehdit gruplarının ve kötü amaçlı yazılımların hangi teknikleri kullandığını belirleyerek siber güvenlik ekiplerine saldırıları tespit etme ve önleme konusunda önemli bir avantaj sağlar.



Mitre Att&ck Tablosu neden önemlidir?

- **Saldırı Tespiti ve Önleme:** Güvenlik ekipleri, saldırganların kullandığı teknikleri analiz ederek savunma mekanizmalarını güçlendirebilir.
- **Tehdit İstihbaratı:** Siber saldırı gruplarının geçmiş saldırılarında hangi teknikleri kullandığını anlamaya yardımcı olur.
- **Siber Savunma Stratejileri:** Şirketler, Mitre ATT&CK Framework'ü kullanarak güvenlik altyapılarını tehditlere karşı daha dayanıklı hale getirebilir.
- **Tehdit Avcılığı ve Anomali Tespiti:** Güvenlik analistleri, sistemlerinde şüpheli aktiviteleri belirlemek için ATT&CK tablosundaki teknikleri referans alabilir.
- **Siber Güvenlik Eğitimleri:** Güvenlik uzmanları ve tehdit avcıları, ATT&CK tablosunu kullanarak tehdit modelleme ve simülasyon yapabilir.

Mitre Att&ck Framework'de bulunan taktik ve tekniklerin önemi

- Taktikler, saldırganların hedeflerine ulaşmak için kullandıkları genel stratejik hedefleri tanımlar. Örnek olarak, "İlk Erişim (Initial Access)" veya "Savunmadan Kaçınma (Defense Evasion)" gibi kategoriler verilebilir.
- Teknikler, bu taktikleri gerçekleştirmek için kullanılan belli başlı yöntemlerdir. Örnek olarak, kimlik avı saldırıları (T1566) veya meşru hesapların kötüye kullanımı (T1078) gibi teknikler söylenebilir.

TTP Nedir?

TTP, "Taktik, Teknik ve Prosedür" (Tactics, Techniques, and Procedures) teriminin kısaltmasıdır ve siber saldırganların hedeflerine ulaşmak için kullandıkları yöntemleri tanımlar. MITRE ATT&CK framework, bu kavramları düzenli bir şekilde sınıflandırarak siber güvenlik profesyonellerinin saldırganların davranışlarını anlamalarına yardımcı olur. Şimdi bu 3 kavramı açıklayalım:

1. Taktik (Tactics)

Taktikler, saldırganların hedeflerine ulaşmak için izlediği genel hedefleri veya stratejik amaçları tanımlar. Taktikler, genellikle bir saldırının hangi aşamasında olduğuna göre değişir. MITRE ATT&CK çerçevesinde, her taktik, bir saldırının belirli bir aşamasına karşılık gelir.

Örnek:

- **Initial Access (Başlangıç Erişimi)**: Saldırganların hedef sisteme ilk erişimi sağlamak için kullandıkları yöntemler.
- **Privilege Escalation (Yetki Yükseltme)**: Saldırganların daha yüksek yetkiler elde etme amacıyla uyguladıkları yöntemler.

2. Teknik (Techniques)

Teknikler, saldırganların belirli bir taktiği uygulamak için kullandığı **spesifik yöntemler** veya **araçlardır**. Yani, bir taktiği gerçekleştirmek için kullanılan somut adımlardır. MITRE ATT&CK, her taktiği destekleyen çeşitli teknikleri listeler.

Örnek:

- **Spearphishing Attachment (T1071)**: "Initial Access" taktiğiyle ilişkili bir teknik. Hedefe kötü amaçlı eklentiler içeren e-postalar gönderilerek sisteme sızılır.
- **Exploitation for Privilege Escalation (T1068)**: "Privilege Escalation" taktiğiyle ilgili bir teknik. Sistemdeki güvenlik açıklarını kullanarak daha yüksek yetkiler elde edilir.

3. Prosedür (Procedures)

Prosedürler, saldırganların belirli bir teknikle gerçekleştirdiği **adım adım** işlemler veya **uygulama şekli** olarak tanımlanabilir. Prosedürler, tekniklerin nasıl ve hangi araçlarla kullanıldığını daha ayrıntılı bir şekilde açıklar.

Örnek:

- **Phishing E-mail (E-posta Phishing)**: "Spearphishing Attachment" tekniğini uygularken, saldırganlar genellikle e-postaya kötü amaçlı dosyalar ekler ve hedef kişiyi bu dosyayı açmaya ikna etmek için sosyal mühendislik kullanır.
- **Exploiting Vulnerabilities in RDP**: "Exploitation for Privilege Escalation" tekniğinde, saldırganlar genellikle uzak masaüstü protokolü (RDP) üzerinden bir güvenlik açığını keşfeder ve bu açığı kullanarak hedef makinede yüksek ayrıcalıklar elde eder.

Özetle:

- **Taktik**: Bir saldırının amacını veya genel stratejisini belirtir (örneğin, “Persistence(süreklilik)”
- **Teknik**: Bu amacı gerçekleştirmek için kullanılan yöntemler veya araçlar (örneğin, “Spearphishing Attachment”).
- **Prosedür**: Tekniklerin uygulanmasıyla ilgili ayrıntılı adımlar veya süreçler (örneğin, "Phishing e-posta göndermek ve kötü amaçlı dosyalar eklemek").

1. TTP-Based Threat Hunting (TTP Tabanlı Tehdit Avcılığı)

Tehdit avcılığı, güvenlik ekiplerinin **proaktif** bir şekilde, yani saldırganlar henüz saldırıya geçmeden önce, organizasyonların ağlarını veya sistemlerini tarayarak olası tehditleri bulmalarını sağlar. TTP tabanlı tehdit avcılığı ise, bu tehdit avcılığını daha hedefli ve verimli hale getirir.

Nasıl İşler?

TTP tabanlı tehdit avcılığı, saldırganların ne tür yollarla sisteme girmeyi ve sistemi kontrol etmeyi hedeflediğini bilerek çalışır. MITRE ATT&CK çerçevesi, siber saldırganların kullandığı **taktikler** (saldırının amacı), **teknikler** (saldırıyı gerçekleştirmek için kullandıkları yollar) ve **prosedürler** (saldırıyı uygularken izledikleri adımlar) hakkında ayrıntılı bilgiler sunar.

Bir tehdit avcısı, bu bilgileri kullanarak, hedef organizasyona gelen e-postalar veya ağ trafiği gibi verileri analiz eder. Örneğin, saldırganın kullandığı bir teknik **Spearphishing** (hedefli kimlik avı) ise, avcı bu tekniği kullanarak şüpheli e-postaları veya kötü amaçlı eklentileri araştırabilir. Burada amaç, saldırganların kullandığı belirli tekniklere karşı ağda olası ipuçlarını (örneğin, şüpheli dosyalar veya anormal bağlantılar) bulmaktır.

Örnek:

Bir saldırgan, **Spearphishing** (hedefli kimlik avı) tekniğiyle, kötü amaçlı bir dosya içeren e-postalar gönderebilir. Bir tehdit avcısı, bu tür e-postaların ağda izlerini arayarak, hedefli saldırıları tespit etmeye çalışır.

2. Detection Engineering (Tespit Mühendisliği)

Tespit mühendisliği, siber tehditlerin etkili bir şekilde tespit edilmesini sağlamak için kullanılan tekniklerin ve araçların geliştirilmesidir. Burada amaç, saldırganların davranışlarını **erken tespit edebilmek** için **algoritmalar**, **kurallar** ve **gözlemler** geliştirmektir. Tespit mühendisleri, MITRE ATT&CK'ı temel alarak, saldırganların kullandığı teknikleri anlamaya çalışır ve buna göre tespit kuralları oluştururlar.

Nasıl İşler?

Tespit mühendisliği, sistemleri ve ağları sürekli olarak izleyerek, saldırganların kullandığı **TTP'leri** algılayacak kurallar geliştirmeye dayanır. Örneğin, **PowerShell** komutları, sıklıkla kötü amaçlı yazılımların çalıştırılmasında kullanılır. Tespit mühendisleri, PowerShell kullanımını izleyen ve anormal bir komut algıladığında alarm veren kurallar oluşturabilir.

Örnek:

Bir tespit mühendisi, PowerShell komutlarının kötü amaçlı yazılımlar için nasıl kullanılabileceğini belirledikten sonra, bu tür aktiviteleri tespit etmek için bir kural yazabilir. Bu, ağdaki kötü amaçlı hareketliliği erken tespit etmek için önemli bir adımdır.

TTP-Based Threat Hunting ve Detection Engineering Arasındaki Farklar:

- **TTP-Based Threat Hunting** daha çok proaktif bir yaklaşımdır; saldırganın sistemdeki varlığını bulmak için daha fazla **araştırma** yapar. Buradaki amaç, sistemdeki gizli tehditleri keşfetmek ve henüz zarar vermeden tespit etmektir.
- **Detection Engineering** ise daha çok **reaktif** bir yaklaşımdır ve saldırganın aktivitelerini **gözlemleyip tespit etmeyi** hedefler. Burada, saldırı tespit edilene kadar beklenir, ardından gerekli önlemler alınır.

Her iki yaklaşım da birlikte çalışarak, **daha sağlam bir güvenlik savunması** sağlar. Tehdit avcıları, saldırganların potansiyel hareketlerini tespit ederken, tespit mühendisleri, bu hareketleri tespit etmek için gerekli kuralları ve algoritmaları geliştirir.

2022 Ukraine Electric Power Attack C0034

2022 Ukrayna Elektrik Gücü Saldırısı (Kampanya C0034), Sandworm Team tarafından gerçekleştirilen ve Ukrayna'daki bir elektrik hizmet sağlayıcısını hedef alan bir siber saldırıdır. Bu saldırıda, saldırganlar GOGETTER, Neo-REGEORG, CaddyWiper gibi araçlar ve "living off the land" (LotL) tekniklerini kullanarak SCADA sistemleri üzerinden yetkisiz komutlar göndermiştir.

Saldırıda kullanılan teknikler ve bunların MITRE ATT&CK TID (Teknik Kimlik) değerleri açıklamalarıyla birlikte aşağıdadır:

Komut ve Betik Yorumlayıcı: PowerShell (T1059.001)

Saldırganlar, TANKTRAP adlı bir PowerShell aracını kullanarak, Windows Grup İlkesi aracılığıyla bir wiper (silici) yazılımını yaymış ve çalıştırmıştır.

Sistem veya Hizmet Süreci Oluşturma/Değiştirme: Systemd Servisi (T1543.002)

GOGETTER adlı kötü amaçlı yazılımın kalıcılığını sağlamak için Systemd yapılandırması değiştirilmiş ve sistem kullanıcı girişlerini kabul etmeye başladığında çalışacak şekilde ayarlanmıştır.

Veri İmhası (T1485)

Saldırganlar, CaddyWiper adlı zararlı yazılımı kullanarak, OT (Operasyonel Teknoloji) ile ilgili dosyaları, eşlenmiş sürücüleri ve fiziksel disk bölümlerini silmiştir.

Etki Alanı veya Kiracı İlkesi Değiştirme: Grup İlkesi Değiştirme (T1484.001)

Grup İlkesi Nesneleri (GPO'lar) kullanılarak zararlı yazılım dağıtılmış ve çalıştırılmıştır.

Yanal Araç Transferi (T1570)

CaddyWiper'ın çalıştırılabilir dosyası olan msserver.exe, bir hazırlık sunucusundan yerel bir sabit diske kopyalanmıştır.

Gizleme: Görev veya Hizmet Taklidi (T1036.004)

Systemd servis birimleri kullanılarak, GOGETTER kötü amaçlı yazılımı meşru veya meşru görünen servisler olarak gizlenmiştir.

Uygulama Katmanı Dışı Protokol (T1095)

Komuta ve Kontrol (C2) iletişimleri, TLS tabanlı bir tünel içinde proxy'lenmiştir.

Protokol Tünelleme (T1572)

GOGETTER tünelleme yazılımı kullanılarak, harici bir sunucu ile "Yamux" TLS tabanlı bir C2 kanalı oluşturulmuştur.

Zamanlanmış Görev/İş: Zamanlanmış Görev (T1053.005)

Grup İlkesi Nesnesi (GPO) aracılığıyla zamanlanmış görevler kullanılarak, CaddyWiper belirli bir zamanda çalıştırılmıştır.

Sunucu Yazılım Bileşeni: Web Shell (T1505.003)

İnternete açık bir sunucuya Neo-REGEORG web shell'i yerleştirilmiştir.

Otomatik Çalışan Görüntü (T0895)

Mevcut hiper yönetici erişimi kullanılarak, a.iso adlı bir ISO görüntüsü, bir SCADA sunucusu çalıştıran sanal makineye bağlanmıştır. SCADA sunucusunun işletim sistemi, CD-ROM görüntülerini otomatik çalıştıracak şekilde yapılandırıldığından, ISO görüntüsündeki kötü amaçlı VBS betiği otomatik olarak çalıştırılmıştır.

Komut Satırı Arayüzü (T0807)

MicroSCADA platformunda scilc.exe ikili dosyası kullanılarak SCIL-API aracılığıyla komutlar yürütülmüştür.

Betikleme (T0853)

lun.vbs adlı bir Visual Basic betiği kullanılarak n.bat dosyası çalıştırılmış ve ardından MicroSCADA scilc.exe komutu yürütülmüştür.

Sistem İkili Proxy Yürütme (T0894)

MicroSCADA uygulama ikili dosyası scilc.exe kullanılarak, saldırgan tarafından tanımlanan s1.txt dosyasında belirtilen SCADA talimatları gönderilmiştir.

Yetkisiz Komut Mesajı (T0855)

MicroSCADA SCIL-API kullanılarak, trafo merkezi cihazlarına yetkisiz komutlar gönderilmiştir.

Auditore Şirketler Grubu'na Yapılan Siber Saldırı

Auditore Şirketler Grubu, finans ve teknoloji sektörlerinde faaliyet gösteren büyük ve köklü bir kuruluştur. Geniş müşteri portföyü ve kritik finansal verileri, siber tehdit aktörlerinin dikkatini çeker. Tehdit aktörleri, Auditore Şirketler Grubu'nu hedef alarak bir saldırı planlamaya başlar. Öncelikle, şirketin zayıf noktalarını keşfetmek ve saldırıyı başarılı bir şekilde gerçekleştirebilmek için çeşitli yöntemler kullanırlar.

1-Keşif Aşaması (Reconnaissance) Tactic ID: TA0043

Saldırganlar, Auditore Şirketler Grubu hakkında bilgi toplamak için çeşitli keşif yöntemlere başvururlar. İlk olarak, açık kaynak keşfi (T1593) yaparak şirketin web sitesi, sosyal medya hesapları ve iş ilanlarını incelerler. Bu sayede, şirketin kullandığı teknolojiler, sistem altyapısı ve çalışanlar hakkında kritik bilgiler edinirler. Ayrıca, şirketin ağ yapısını anlamak adına ağ tarama (T1046) tekniklerini kullanarak dış IP adreslerini belirler ve açık portları tespit ederler. Burada elde edilen bilgiler, saldırıya dair yol haritası oluşturulmasını sağlar.

2-İlk Erişim (Initial Access) Tactic ID: TA0001

Keşif aşamasında elde edilen bilgileri kullanarak Auditore Şirketler Grubu'na erişim sağlamaya çalışırlar. Bunun için öncelikle çalışanları hedef alan bir kimlik avı (T1566) saldırısı düzenlerler. Sahte bir e-posta ile çalışanlara zararlı bir bağlantı veya ek gönderilir. Şirket çalışanlarından biri, bu bağlantıyı açarak saldırganların sisteme sızmasına neden olur. Alternatif olarak, saldırganlar çalınan kimlik bilgilerini kullanarak geçerli hesaplarla erişim (T1078) sağlamaya çalışırlar. VPN veya uzaktan masaüstü protokolü (RDP) üzerinden şirket ağına giriş yaparak, sistemde gizlice ilerlemeye başlarlar.

3-Yanal Hareket (Lateral Movement) Tactic ID: TA0008

İlk erişimi başarıyla elde eden saldırganlar, ağ içinde daha fazla yetkiye sahip olmak ve kritik sistemlere erişmek için hareket etmeye başlarlar. İlk olarak, kimlik bilgisi toplama (T1555) teknikleriyle daha yüksek yetkilere sahip hesaplara ulaşmaya çalışırlar. Ele geçirilen kullanıcı hesapları üzerinden sistem yöneticisi hakları elde etmek için kimlik bilgileri bellekte taranır ve parola dosyaları incelenir. Daha sonra, uzaktan hizmet kullanımı (T1021) yöntemlerini devreye sokarak, SMB ve RDP gibi servisler üzerinden şirket ağı içinde farklı sistemlere erişim sağlarlar. Bu sayede, saldırganlar giderek daha kritik sistemlere erişim elde ederler.

4-Etki Yaratma (Impact) Tactic ID: TA0040

Saldırganlar, Auditore Şirketler Grubu'nun sistemlerine erişim sağladıktan sonra, saldırının asıl amacını gerçekleştirmeye başlarlar. İlk olarak, fidye yazılımı kullanarak dosya şifreleme (T1486) gerçekleştirirler. Şirketin kritik finansal verileri şifrelenerek sistemler kullanılamaz hale getirilir ve fidye talebinde bulunulur. Ayrıca, saldırganlar sistemdeki hassas verileri çalarak veri sızıntısı (T1567) gerçekleştirirler. Çalınan müşteri bilgileri ve finansal veriler Dark Web'de satışa sunulur veya kamuya sızdırılmakla tehdit edilir.

5-Kalıcılığı Sağlama (Persistence) Tactic ID: TA0003

Saldırganlar, sistem yöneticileri tarafından tespit edilip temizlenmemek için kalıcılık sağlamaya çalışırlar. Bunun için, zararlı yazılımları sistem başlangıcında çalışacak şekilde başlangıç kayıt anahtarı değiştirme (T1547) yöntemiyle yapılandırırlar. Ayrıca, şirket sistemlerinde kendilerine sürekli erişim sağlamak için yetkili kullanıcı hesapları oluşturma (T1136) taktiğini kullanarak yeni yönetici hesapları oluştururlar. Böylece, saldırganlar şirketin farkına varıp önlem almaya çalışsa bile, uzun süre boyunca sistemde kalmaya devam edebilirler.

MITRE ATT&CK Tablosu

Taktik	Teknik Adı	TID
Keşif (TA0043)	Açık Kaynak Keşfi	T1593
Keşif (TA0043)	Ağ Tarama	T1046
İlk Erişim (TA0001)	Kimlik Avı	T1566
İlk Erişim (TA0001)	Geçerli Hesapların Kullanımı	T1078
Yanal Hareket (TA0008)	Kimlik Bilgisi Toplama	T1555
Yanal Hareket (TA0008)	Uzaktan Hizmet Kullanımı	T1021
Etki (TA0040)	Dosya Şifreleme	T1486
Etki (TA0040)	Veri Sızıntısı	T1567
Kalıcılık (TA0003)	Başlangıç Kayıt Anahtarı Değiştirme	T1547
Kalıcılık (TA0003)	Yetkili Kullanıcı Hesapları Oluşturma	T1136

SONUÇ

MITRE ATT&CK Framework, tehdit aktörlerinin saldırı süreçlerini sistematik bir şekilde anlamamızı sağlayan kritik bir kaynaktır. Siber güvenlik uzmanları, bu framework sayesinde tehdit aktörlerinin **keşif (reconnaissance)** aşamasından **nihai hedeflerine** ulaşana kadar izledikleri yolları detaylı bir şekilde inceleyebilir ve buna uygun güvenlik önlemleri geliştirebilir.

Yapılan analizler, siber saldırıların genellikle çok aşamalı olduğunu ve farklı taktiklerin bir araya getirilerek gerçekleştirildiğini göstermektedir. **2022 Ukraine Electric Power Attack (C0034)** vakası, saldırganların enerji altyapısını hedef alarak operasyonel sistemleri etkisiz hale getirme stratejisini gözler önüne sermektedir. Bu tür saldırılara karşı önlem almak için tehdit istihbaratı, proaktif tehdit avcılığı ve gelişmiş tespit mühendisliği stratejileri kritik bir rol oynamaktadır.

Senaryo çalışması, saldırganların bir şirketi nasıl hackleyebileceğini göstererek, MITRE ATT&CK tablosunun siber güvenlik operasyonlarında nasıl kullanılabileceğini ortaya koymuştur. Siber güvenlik uzmanlarının, bu framework'ü aktif bir şekilde kullanarak saldırıları hızlı bir şekilde tespit etmesi ve önlem alması gerekmektedir.

Kaynakça

https://attack.mitre.org/campaigns/C0034/

https://attack.mitre.org/

https://www.nist.gov/