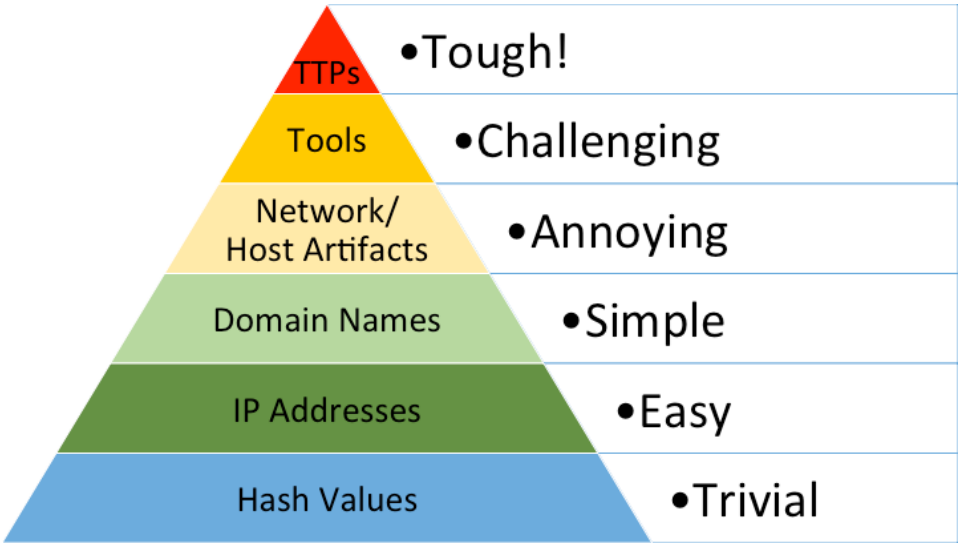
Pyramid Of Pain

Hazırlayan: Berra Söyler
Tarih: 17.02.2025

İçindekiler

1.Giriş

Siber tehdit aktörleri, sürekli değişen saldırı teknikleriyle güvenlik önlemlerini aşmaya çalışırken, savunma stratejilerinin de aynı hızla gelişmesi gerekmektedir. David Bianco tarafından geliştirilen Pyramid of Pain modeli, saldırganların operasyonlarını boşa çıkarmayı amaçlayan bir yaklaşımdır. Bu model, siber tehdit göstergelerini (IoC), saldırganlar açısından değiştirmenin ne kadar zor olduğuna göre farklı seviyelere ayırarak savunma mekanizmalarının etkisini artırmayı hedefler. Geleneksel imza tabanlı tehdit tespit yöntemlerinin sınırlamalarını göz önünde bulunduran Pyramid of Pain, TTP (Tactics, Techniques, and Procedures) odaklı bir savunma stratejisinin daha kalıcı ve etkili olduğunu ortaya koymaktadır. Bu rapor, Pyramid of Pain modelinin siber güvenlikteki önemini, MITRE ATT&CK çerçevesiyle entegrasyonunu ve proaktif savunma mekanizmalarının saldırganları nasıl zor durumda bırakabileceğini kapsamlı bir şekilde ele almaktadır.



2. Indicators of Compromise (IoC) Nedir?

Indicators of Compromise (IoC), bir sistemin siber saldırıya uğradığını veya kötü amaçlı etkinliklerin gerçekleştiğini gösteren belirtiler ve izlerdir. IoC'ler, güvenlik analistleri tarafından tehditleri tespit etmek, saldırıları analiz etmek ve olay müdahale süreçlerini yürütmek için kullanılır.

IoC'ler genellikle şu tür göstergeleri içerir:

- Hash Değerleri
- IP Adresleri
- Domain/URL
- Dosya ve Kayıt Defteri Değişiklikleri
- Ağ Trafiği Anormallikleri
- IoC'lerin Zayıf Yönleri

IoC’ler kolayca değiştirilebildiği için saldırganlar tarafından atlatılabilir. Örneğin, bir kötü amaçlı yazılımın hash değeri değiştirilerek tespit edilmesi engellenebilir veya IP adresleri dinamik olarak değiştirilebilir. Bu yüzden, Pyramid of Pain modeli bize IoC yerine TTP (Tactics, Techniques, and Procedures) bazlı tehdit tespitinin daha etkili olduğunu göstermektedir.

3. Pyramid of Pain Seviyeleri ve IoC ile Karşılaştırması

Pyramid of Pain modeli en alt seviyeden en üst seviyeye doğru saldırganların karşılaştıkları zorluk derecesine göre farklı göstergeleri sınıflandırır:

1. **Hash Değerleri** (En Kolay Değiştirilebilir)
    - Hash değerleri, bir dosyanın benzersiz kimliğini belirlemek için kullanılan kriptografik özetlerdir (örn. SHA-256).
    - Ancak saldırganlar, dosya içinde küçük değişiklikler yaparak hash değerlerini kolayca değiştirebilirler.
    - **IoC bazlı savunma**: Hash değerlerini tespit ederek engellemek kısa vadede işe yarasa da, saldırganlar kolayca yeni hash'ler üretebilir.

2. **IP Adresleri**
    - Saldırganlar, kötü amaçlı yazılımlarını veya saldırılarını belirli IP adreslerinden yönlendirirler.
    - Ancak VPN, proxy ve **IP değiştirme hizmetleri** kullanarak IP adreslerini değiştirebilirler.
    - **IoC bazlı savunma**: Kötü amaçlı IP adreslerini kara listeye almak faydalı olabilir ancak uzun vadede sürdürülebilir değildir.

3. **Domain/URL**
    - Saldırganlar, kötü amaçlı yazılımlarını dağıtmak veya **kimlik avı saldırıları (Phishing - T1566.001)** gerçekleştirmek için sahte web siteleri oluşturabilirler.
    - Yeni bir domain kaydetmek birkaç dakika sürebilir ve DNS yayılım süresi sonrası aktif hale gelir.
    - **IoC bazlı savunma**: Zararlı domainleri engellemek bir savunma katmanı oluştursa da, saldırganlar hızla yeni alan adları üretebilirler.

4. **Ağ ve Host Artefaktları**
    - Ağ trafiğinde belirli şüpheli paternler veya kötü amaçlı yazılımların bıraktığı sistem içi izler (örneğin, dosya isimleri, kayıt defteri anahtarları).
    - Bu seviyede savunma yapmak saldırganların daha fazla çaba harcamasına neden olur.
    - **TTP bazlı savunma**: Saldırganın genel davranışına odaklanarak, tekniklerini anlamak ve engellemek daha etkili bir yöntemdir.

5. **Araçlar (Tools)**
    - Saldırganlar genellikle belirli saldırı araçlarını (örneğin, Mimikatz, Cobalt Strike) kullanırlar.
    - Bu araçları değiştirmek veya tamamen yeni bir araç geliştirmek, saldırganlar için büyük bir zaman ve kaynak gerektirir.
    - **TTP bazlı savunma**: Araçların kullanımına dayalı tespitler yaparak, saldırganları daha fazla zorlamak mümkündür.
6. **TTP'ler (Tactics, Techniques, and Procedures) (En Zor Değiştirilebilir)**
    - TTP'ler, saldırganların saldırılarını nasıl gerçekleştirdiğine dair genel stratejiler ve tekniklerdir.
    - Yeni bir TTP oluşturmak, saldırganlar için **yoğun araştırma ve geliştirme gerektirir**, bu yüzden değiştirilmesi oldukça zordur.
    - **TTP bazlı savunma**: Saldırganların yöntemlerini anlamak ve MITRE ATT&CK çerçevesini kullanarak tespit etmek en uzun vadeli ve etkili savunma yöntemidir.

4. Siber Güvenlikte Kullanımı

Pyramid of Pain modeli, özellikle SOC (Security Operations Center), Threat Hunting ve Incident Response ekipleri tarafından aktif bir şekilde kullanılarak saldırganların, faaliyetlerini nasıl zorlaştırabilecekleri konusunda rehberlik eder. Özellikle üst seviyelerdeki göstergelere odaklanmak, saldırganların operasyonlarını daha maliyetli ve karmaşık hale getirir.

- SOC Ekipleri: SIEM (Security Information and Event Management) sistemleri kullanılarak belirlenen göstergelere dayalı olarak anlık tehdit tespiti yapılır.
- Threat Hunting: Siber tehdit avcıları, TTP'leri hedef alarak saldırganların genel yöntemlerini analiz eder ve uzun vadeli koruma stratejileri geliştirir.
- Incident Response: Güvenlik ihlalleri durumunda, saldırının hangi seviyede olduğu tespit edilerek gerekli müdahale adımları belirlenir.

5. Pyramid of Pain ve MITRE ATT&CK Entegrasyonu

MITRE ATT&CK, siber saldırganların kullandığı teknikleri, taktikleri ve prosedürleri sistematik bir şekilde tanımlayan açık bir bilgi tabanıdır. Pyramid of Pain modeliyle birleştiğinde, saldırganların yöntemlerine karşı daha derinlemesine bir savunma geliştirmek mümkündür.

Örneğin, Kimlik Avı Saldırılarında(Phishing - T1566.001):

Hash seviyesi: Zararlı e-posta eklerini engellemek.

IP/DNS seviyesi: Saldırganın kullandığı IP veya domainleri kara listeye almak.

Ağ Artefaktları seviyesi: E-postalardaki şüpheli bağlantıları analiz etmek.

Araçlar seviyesi: Saldırganların kullandığı araçları belirlemek.

TTP seviyesi: Saldırganın kimlik avı metodolojisini inceleyerek yeni savunma mekanizmaları geliştirmek.

Bu seviyelerden en uzun vadeli ve etkili çözüm, TTP'lere odaklanmaktır. Çünkü Pyramid of Pain modeline göre, TTP'ler **saldırganlar için değiştirilmesi en zor olan unsurlar** olduğu için, güvenlik çözümlerini bu seviyeye odaklamak **uzun vadede daha etkili ve sürdürülebilir** bir savunma sağlar.

Bu bağlamda, TTP (Tactics, Techniques, and Procedures) bazlı tespitler, saldırganların yöntemlerine derinlemesine bir anlayış kazandırarak, savunma stratejilerini daha dirençli hale getirir. Geleneksel tespit yöntemleri, yalnızca yüzeysel seviyelerde koruma sağlarken TTP'ler üzerine kurulu tespitler saldırganların saldırı yöntemlerini temelden değiştirmeye zorlar ve uzun vadeli bir savunma stratejisi sunar. MITRE ATT&CK çerçevesiyle entegrasyon, bu savunma süreçlerini daha etkin ve sürdürülebilir kılar. Çünkü bu yöntemler saldırganın tekniklerine yönelik sürekli bir adaptasyon gerektirir.

Geleneksel tespit yöntemleri (imza tabanlı, anomali tabanlı tespitler), genellikle Pyramid of Pain'in alt seviyelerine odaklanır. Ancak bu göstergeler kolayca değiştirilebilir ve saldırganlar için büyük bir zorluk oluşturmaz.

Buna karşılık:

- **TTP bazlı tespitler**, saldırganların operasyonlarını tamamen değiştirmeye zorlar.
- **Uzun vadeli koruma sağlar**, çünkü TTP'ler sık sık değiştirilemez.
- **MITRE ATT&CK gibi çerçevelerle birlikte kullanıldığında**, tehdit avcılığı ve saldırı tespit mekanizmaları daha etkili hale gelir.

6. Örnek Saldırı Senaryosu: MITRE ATT&CK ve Pyramid of Pain

Siber saldırılara karşı etkili bir savunma geliştirmek için **MITRE ATT&CK çerçevesi** ve **Pyramid of Pain modeli** birlikte kullanılabilir. Bu model, saldırganların tekniklerini anlamayı ve onlara karşı etkili savunma stratejileri geliştirmeyi sağlar.

Örnek bir saldırı senaryosu ele alındığında, kimlik avı (Phishing - T1566.001) yöntemiyle bir sisteme sızmaya çalışan bir saldırgana karşı, Pyramid of Pain modeli kullanılarak farklı savunma katmanları oluşturulabilir:

- **Hash Değerleri (Kolay Değiştirilebilir):** Zararlı dosyanın hash değeri tespit edilerek güvenlik sistemlerinde engellenir.
- **IP Adresi:** Kimlik avı saldırısının kaynağı belirlenerek güvenlik duvarı kurallarına eklenir.
- **Domain/URL:** Zararlı web sitesi güvenlik sistemlerine tanıtılarak erişimi engellenir.

- **Ağ Artefaktları:** Zararlı e-postalar ve anormal trafik analiz edilerek tehditler belirlenir.
- **Araçlar ve Teknikler:** Şüpheli PowerShell komutları gibi saldırganın kullandığı araçlar tespit edilerek önleyici tedbirler alınır.
- **TTP'ler (En Zor Değiştirilebilir):** Saldırganın kimlik avı metodolojisi incelenerek, bu tür saldırıları önlemek için uzun vadeli güvenlik politikaları geliştirilir.

Bu yaklaşımla, saldırılar erken aşamada tespit edilerek tehdit aktörlerinin operasyonları engellenebilir.

Örnek Olay İncelemesi

Finans sektörüne yönelik gerçekleştirilen bir hedefli saldırıda, saldırganların belirli bir zararlı yazılım kullandıkları tespit edilmiştir. Güvenlik ekibi, yalnızca bu yazılımın hash değerlerini tespit etmekle yetinmemiş, aynı zamanda yazılımın davranışsal özelliklerini ve iletişim protokollerini analiz etmiştir. Bu sayede, saldırganlar yalnızca dosyanın hash değerini değiştirerek engelleme mekanizmasını aşamamış, daha kapsamlı savunma önlemleri ile karşı karşıya kalmıştır. Özellikle ağ artefaktları ve saldırı teknikleri gibi daha zor değiştirilebilen göstergeler üzerinden yapılan analizler, saldırganların hareket kabiliyetini ciddi şekilde kısıtlamıştır.

Bu tür saldırılara karşı etkili bir savunma stratejisi oluşturabilmek için güvenlik politikalarının sürekli güncellenmesive saldırganların kullandığı tekniklerin yakından izlenmesi gerekmektedir.

- **Proaktif Tehdit Avı:** Kimlik avı saldırıları tespit edildiğinde yalnızca zararlı e-postalar engellenmekle kalmaz, aynı zamanda saldırganın kullandığı Komuta ve Kontrol (C2) altyapıları analiz edilerek geniş çaplı bir engelleme mekanizması uygulanır.
- **SIEM ve EDR Kullanımı:** SIEM ve EDR gibi sistemler sayesinde, saldırganların sistem üzerindeki izleri sürekli izlenir ve yeni tehditler tespit edildiğinde anında müdahale edilir.
- **Taktiksel ve Stratejik Önlemler:** Güvenlik ekipleri, yalnızca belirli tehdit göstergelerine odaklanmak yerine saldırganların genel yöntemlerini analiz ederek **uzun vadeli ve stratejik savunma önlemleri** geliştirir.

Bu bütüncül yaklaşım, saldırıları erken aşamada tespit ederek tehdit aktörlerinin operasyonlarını etkisiz hale getirmeyi sağlar.

5.Sonuç

Siber tehdit aktörleri, sürekli değişen IoC'ler ile güvenlik önlemlerini aşmaya çalışırken, kalıcı ve uzun vadeli bir savunma stratejisi oluşturmak için TTP tabanlı tespit ve müdahale yöntemlerine odaklanmak gerekmektedir. Pyramid of Pain modeli, saldırganların operasyonlarını bozmak için hangi seviyedeki göstergelere müdahale edilmesinin daha etkili

olduğunu açık bir şekilde ortaya koymaktadır. MITRE ATT&CK çerçevesiyle entegre edilen bu model, saldırganların tekniklerine yönelik derinlemesine analiz yaparak onların saldırı yöntemlerini değiştirmeye zorlar. Geleneksel imza tabanlı tespit yöntemleri saldırganlar için kolayca aşılabilirken, TTP odaklı bir yaklaşım onları daha büyük maliyetlere ve zorluklara sürükleyerek etkin bir savunma sağlar. Bu bağlamda, güvenlik ekiplerinin olay müdahale süreçlerini ve tehdit avcılığı yaklaşımlarını Pyramid of Pain modeline göre şekillendirmesi, siber tehditlerle mücadelede kritik bir rol oynayacaktır.

6. Kaynakça

https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain
http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
https://cymulate.com/cybersecurity-glossary/pyramid-of-pain/
https://www.youtube.com/watch?v=emzUhkiXM0g&t=67s