Pyramid of Pain

Hazırlayan: Esra Akteke

Tarih: 17.02.2025

İçindekiler

Giriş

Siber güvenlik dünyasında tehdit avcılarının ve SOC ekiplerinin en büyük amacı, siber saldırganların hareket alanını daraltmak ve onlara en fazla zarara neden olacak noktada baskı uygulamaktır. David Bianco tarafından geliştirilen Pyramid of Pain, saldırganların operasyonlarını devam ettirmek için hangi göstergeleri değiştirme yeteneğine sahip olduklarını ve hangi seviyelerde önlem alınırsa en çok zorlanacaklarını gösteren kritik bir modeldir.

Bu model bir saldırganın ne kadar zor durumda kalacaklarını belirlememize yardımcı olur. En alt seviyede kolayca değiştirilebilecek göstergeler varken, piramidin en üst seviyesinde saldırganların operasyon mantıklarını dahi değiştirmek zorunda kalacakları unsurlar bulunur. Bu raporda Pyramid of Pain'in katmanları detaylı olarak ele alınacaktır.

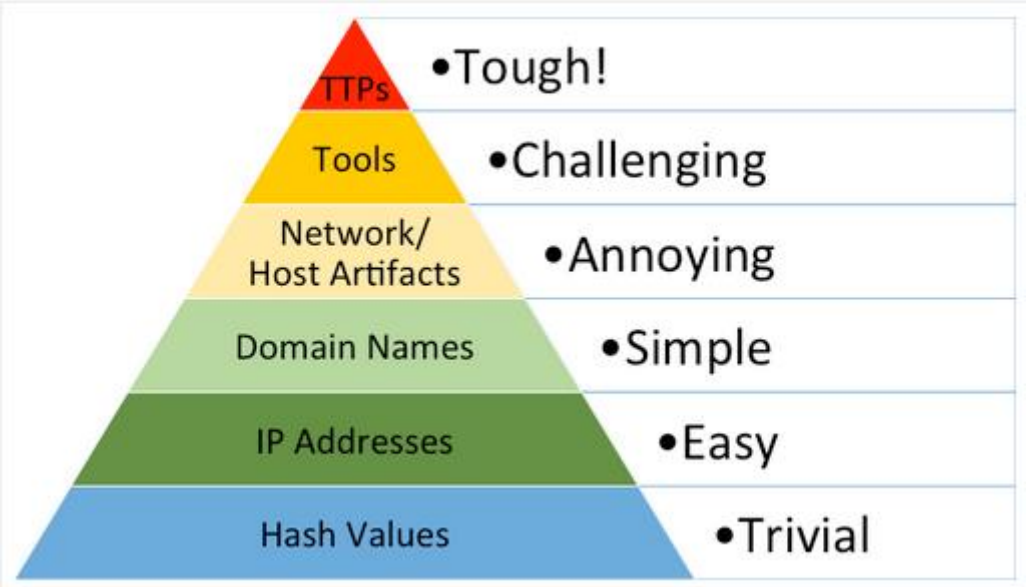
Pyramid of Pain Nedir?

Pyramid of Pain, Güvenlik uzmanı David J. Bianco tarafından, farklı türdeki saldırgan göstergelerinin tespit edilmesinin zorluğu ve bu göstergelere müdahale edilmesinin saldırganlar üzerinde yaratacağı zorluk seviyelerini açıklamak için geliştirilmiş bir kavramsal modeldir. Bu piramit tehdit aktörlerinin saldırılarını sürdürebilmesini zorlaştıran farklı türdeki göstergeleri hiyerarşik bir yapıda sunmaktadır.

Piramitin alt basamaklarında yer alan göstergeler saldırganlar tarafından hızla değiştirilebilirken, yukarıya doğru çıkıldıkça bu değişikliklerin yapılması daha zor hale geliyor. Üst seviyedeki unsurların tespiti, saldırganın taktik ve stratejilerini köklü şekilde değiştirmesini gerektirir ve operasyonel maliyetini artırarak ona ciddi zorluklar yaşatır.

Cyber Kill Chain modeline benzer bir yaklaşım olsa da Cyber Kill Chain modeli saldırganların izlediği adımları tanımlarken, Pyramid of Pain özellikle Blue Team için rehber niteliğindedir. Bu model güvenlik uzmanlarının saldırıları yalnızca tespit etmekle kalmayıp, tehdit aktörlerinin operasyonlarını sürdürebilmesini nasıl daha fazla zorlaştırabileceklerini anlamalarına yardımcı olur diyebiliriz.

Pyramid of Pain Katmanları



Şekil 1. David Bianco'nun icat ettiği Acı Piramidi

Siber güvenlikte tehdit istihbaratı saldırganların izlerini takip etmek ve onları etkisiz hale getirmek için kritik bir bileşendir. Pyramid of Pain, bu süreçte kullanılan göstergelerin saldırganlar üzerindeki etkisini gösteren bir modeldir. Piramit, saldırganları engellemenin onları ne kadar zorlayacağını katmanlar halinde açıklıyor.

Piramit ne kadar yukarı çıkarsa, saldırgan için değişiklik yapmak o kadar zahmetli ve maliyetli oluyor. Alt seviyedeki unsurlar kolayca değiştirilebilirken üst seviyeye çıkıldıkça saldırganın operasyonlarını kökten değiştirmesi gerekir. Bu yüzden siber güvenlik ekipleri sadece basit göstergelere değil, saldırganın çalışma yöntemlerine odaklanarak daha kalıcı bir savunma inşa edebilir. Katmanlar sırasıyla aşağıdaki gibidir.

1)Hash Değerleri

Hash değerleri belirli bir dosyanın özgün parmak izi gibidir diyebiliriz. Genellikle MD5, SHA-1, SHA-256 gibi algoritmalarla oluşturulur. Ancak bu değerler saldırganlar tarafından değiştirilmesi en kolay olan unsurlar arasındadır.

Bir zararlı yazılım veya sahte bir belge tespit edildiğinde hash değeriyle kara listeye alınabilir ve sistemlerde bloklanabilir. Saldırgan için aslında bu katmanda bir engelleme yapıldığında, saldırganın tek yapması gereken zararlı dosyaların çok ufak bir özelliğini değıştirerek yeni bir hash oluşturmaktır.

Bu nedenle, hash değerlerine dayalı tespit yöntemleri yalnızca kısa vadeli bir çözüm sunar ve saldırgan üzerinde kayda değer bir caydırıcı etki yaratmaz. Çünkü en küçük bir değişiklik bile tamamen farklı bir hash değeri üreterek bu yöntemin sürdürülebilirliğini ve etkinliğini ortadan kaldırabilir.

Örnek olarak, SHA3-256 hash fonksiyonuyla hesaplanan iki benzer girişin tamamen farklı çıktılar ürettiği görülebilir.

SHA3-256(1111111111111111111111111111111111111111111111) =
bf8d60cfc6654a2cd4dbf63e5a85cf8c34674c3f41f1bf38312ce88012536d69

SHA3-256(1111111111111111111111111111111111111111111110) =
b45d95d47b00d9fcdb9af0437bbaa5101a51f55ebcc2163bb731cee7761d6d80

Görüldüğü gibi yalnızca tek bir bitin değişmesi bile tamamen farklı bir hash değeri üretmektedir. Bu durum hash tabanlı tehdit avcılığının tek başına yeterli olmadığını gösteriyor. Saldırganlar kötü amaçlı yazılımlarında küçük ve işlevsiz değişiklikler yaparak yeni hash değerleri üretebilir ve böylece hash tabanlı tespit mekanizmalarını geçebilir. Bu nedenle daha gelişmiş analiz yöntemleri ve davranışsal tespit mekanizmaları kullanılmalıdır.

2)IP Adresleri

Günümüzde IP adreslerini değiştirmek oldukça basit bir işlemdir. VPN'ler, proxy servisleri ve Tor ağı gibi araçlar sayesinde saldırganlar farklı IP adreslerinden bağlantı kurarak kimliklerini gizleyebiliyorlar. Dinamik IP adresleri de siber suçlular için ek bir avantajdır diyebiliriz çünkü internet servis sağlayıcıları, kullanıcılarına periyodik olarak yeni IP adresleri atayarak sürekli değişen bir yapı oluşturur.

Örneğin fidye yazılım grupları genellikle anonimliklerini artırmak için Tor ağı üzerindeki geçici kimlikleri kullanır. Bu durum, saldırganların tespit edilmesini zorlaştırırken IP adreslerini izleyerek tehditleri engellemeye çalışan güvenlik ekipleri için büyük bir dezavantaj yaratır.

3)Domain Adları

Domain adları, tehdit aktörlerinin kötü niyetli faaliyetlerini sürdürmek için sıklıkla değiştirdiği unsurlar arasındadır. Bir domain adı güvenlik ekipleri tarafından tespit edilip engellendiğinde, saldırganlar hızla yeni bir domain adı kaydederek operasyonlarını sürdürebiliyor. Alan adlarının ucuz ve erişilebilir olması bu süreci daha da kolaylaştırmaktadır.

Saldırganlar genellikle meşru platformları da kötüye kullanabilir. Örnek vermem gerekirse **protonmail[.]com** veya **proton[.]me** gibi güvenli e-posta servisleri, kötü niyetli iletişimler için bir aracı olarak kullanılabilir. Bu tür domain adlarını takip etmek önemlidir ancak saldırganlar hızla yeni kimlikler oluşturabildiğinden, yalnızca domain adlarına dayanarak savunma stratejisi geliştirmek yetersiz kalabilir. Etkili bir güvenlik stratejisi için daha kapsamlı analiz ve çok katmanlı tehdit tespit yöntemleri gereklidir.

4) Network ve Host Artifactları

Siber saldırganların faaliyetleri sırasında bıraktıkları meşru sistem etkinliklerinden farklı ve ayırt edici izlerdir. Bu izler, bir saldırının izlerini takip etme ve tehditleri tespit etme açısından son derece önemli olabilir. Bu tür artifactslar saldırganın hareketlerini daha iyi anlamak ve onun faaliyetlerini engellemek için kritik bilgiler sunar.

Aşağıda listelenen başlıca artifacts türleri şunlardır:

*****URL artifactsları

*****Log mesajları

*****Komuta ve Kontrol (C2) bilgileri

*****Kayıt defteri anahtarları

*****Dosya ve klasör değişiklikleri

Bu artifactsların değiştirilmesi veya engellenmesi, saldırganın operasyonlarını bozarak gizliliğini sürdürmesini zorlaştırır ve tespit edilme riskini artırır. Etkili tehdit istihbaratı kullanımı saldırganların hareket alanını kısıtlayarak kötü amaçlı faaliyetleri etkili şekilde engelleyebilir.

5) Araçlar

Bir saldırganın kullandığı araçları değiştirmek, büyük çaba ve zaman gerektirir. Özel kötü amaçlı yazılımlar veya saldırı araçları geliştirmek ciddi teknik bilgi ve kaynak gerektirir. Bu nedenle saldırganları durdurmanın en etkili yollarından biri, onların kullandıkları araçları etkisiz hale getirmektir.

Bir güvenlik ekibi, belirli bir kötü amaçlı yazılımı veya saldırı aracını analiz edip tespit ettiğinde saldırganın yeni bir araç geliştirmesi veya mevcut aracı değiştirmesi gerekir. Bu süreç oldukça zaman alıcıdır ve maliyetli olabilir çünkü yeni bir araç tasarlamak, saldırgan için hem teknik zorluklar yaratır hem de saldırıyı başlatma sürecini uzatır. Bu nedenle piramidin üst sıralarında yerini almaktadır.

6) Taktikler, Teknikler ve Prosedürler

Piramidin en üst seviyesinde saldırganların temel saldırı metodolojileri yer almaktadır. Bir saldırganın kullandığı Taktikler, Teknikler ve Prosedürler, onların saldırı süreçlerini şekillendirir. Bu seviyede değişiklik yapmak, saldırganlar için en büyük zorluklardan biridir çünkü bir saldırganın başarılı olması için belirli bir iş akışına sahip olması gerekir ve bu iş akışını değiştirmek, ciddi bilgi ve adaptasyon gerektirmektedir.

Aşamayla ilgili küçük bir örnek vermek gerekirse, örneğin fidye yazılım grupları genellikle belirli bir saldırı akışını takip etmektedir.

Öncelikle saldırganlar hedef sistemleri keşfederek zayıf noktalarını analiz eder. Ardından kimlik bilgilerini çalarak veya kötü amaçlı e-posta göndererek sisteme ilk erişimi sağlarlar. Bir sonraki adımda sistemde yönetici hakları elde ederek kontrolü artırırlar. Son olarak, verileri şifreleyip erişilemez hale getirir ve fidye talep ederler. Bu aşamalar saldırganın başarılı olabilmesi için dikkatlice uyguladığı kritik adımlardır.

Eğer bir güvenlik ekibi saldırganların bu sürecini bozabilirse saldırganların operasyonları büyük ölçüde sekteye uğrar. Yeni ve tespit edilmesi zor bir saldırı süreci geliştirmek, ciddi teknik beceri ve planlama gerektirir. Bu yüzden TTP'leri değiştirmek, saldırganlar için en zorlayıcı unsurdur ve dolayısıyla piramidin en üst seviyesinde yerini alır.

Pyramid of Pain neden önemlidir?

Pyramid of Pain, siber güvenlik dünyasında tehditleri analiz etme ve savunma stratejilerini belirleme konusunda önemli bir araçtır. Bu kavram basitçe saldırıların veya tehditlerin tespitiyle ilgili farklı zorluk seviyelerini tanımlar ve her seviyede karşılaşılan zorlukların artarak daha karmaşık hale geldiğini gösterir. Ancak bu piramidin anlamı ve önemi daha derindir çünkü her seviyedeki teknik ve taktikler, hem saldıran kişilerin hem de savunanların siber güvenlik süreçlerinde ne kadar derinleşebileceğini ve gelişebileceğini gösterir.

Pyramid of Pain'ın önemli olmasının temelinde sadece savunma stratejilerini geliştirmek değil, aynı zamanda tehdit aktörlerinin hareketlerini doğru tahmin etmek ve onlara yönelik etkili müdahalelerde bulunmak yatıyor. Alt seviyedeki göstergeler çoğu zaman hızla tespit edilebilir olsa da savunmanın bu göstergelerle yetinmesi, kalıcı ve etkili bir çözüm sunmaz. Ancak piramidin üst seviyelerine doğru çıkıldıkça tehdit aktörlerinin kullandığı araçlar ve davranış kalıplarının yalnızca teknik bir savunma değil, aynı zamanda stratejik bir bakış açısıyla anlaşılması gerekmektedir.

Bu yüzden siber tehditlere karşı yalnızca teknik bir çözüm değil, aynı zamanda sürekli öğrenme ve adapte olma gerekliliğini simgeler. Savunma ekibi her seviyede daha fazla bilgi ve beceri kazandıkça, savunmalarını daha karmaşık ve güçlü hale getirebilir. Böylece uzun vadede daha sağlam ve dayanıklı bir siber güvenlik altyapısı oluşturulabilir.

Sonuç

Pyramid of Pain, siber güvenlikte savunma stratejilerinin etkinliğini artırmak için güçlü bir model sunmaktadır. Bu model, saldırganların kullandığı göstergeleri ve taktikleri tespit etmenin zorluk seviyelerine göre sınıflandırarak güvenlik ekiplerinin hangi göstergelere odaklanarak daha fazla etki yaratabileceğini belirlemelerine yardımcı olur. Pyramid of Pain'in temel amacı, saldırganların operasyonlarını engellemek ve onları daha zor hale getirmektir. Bu yaklaşım savunma ekiplerinin yalnızca hızlı tepki vermekle kalmayıp aynı zamanda daha derinlemesine analizler ve stratejiler kullanarak saldırganları uzun vadeli olarak zora sokmalarını sağlar.

Pyramid of Pain'in uygulanması savunma stratejilerini daha hedeflenmiş, etkili ve uzun vadeli hale getirirken saldırganların da operasyonel maliyetlerini artırır. Bu süreçte SOC ekiplerinin sürekli olarak gelişen tehditlere uyum sağlamak ve kaynaklarını en verimli şekilde kullanmak adına Pyramid of Pain'i bir rehber olarak alması organizasyonlarının güvenliğini ciddi şekilde güçlendirmektedir diyebiliriz.

Kaynakça

https://cybershieldcommunity.com/pyramid-of-pain/#:~:text=%E2%80%9CPyramid%20of%20Pain%E2%80%9D%20(Ac%C4%B1,stratejik%20ad%C4%B1mlar%20atmak%20i%C3%A7in%20kullan%C4%B1l%C4%B1yor.

https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain

https://cybershieldcommunity.com/pyramid-of-pain/

https://www.vectra.ai/topics/pyramid-of-pain

https://www.csnp.org/post/tryhackme-pyramid-of-pain-room