PYRAMID OF PAİN

Hazırlayan: Şevval Kömeç

16.02.2024

İçindekiler

GİRİŞ

Günümüzde siber tehditler, kuruluşlar için giderek artan bir risk haline gelmiştir. Şirketler, hem kitlesel saldırı yüzeyleriyle başa çıkmak hem de sürekli gelişen tehditlere karşı savunma mekanizmalarını güçlendirmek zorundadır. Bu bağlamda, siber güvenlik stratejilerinin etkinliğini artırmak için kullanılan önemli bir kavram olan Pyramid of Pain (Acı Piramidi), tehdit aktörlerini alt etmek ve savunma mekanizmalarını geliştirmek için kritik bir çerçeve sunar. Bu rapor, Pyramid of Pain kavramını tanıtmak, piramidin altı seviyesini açıklamak ve bu çerçevenin siber güvenlik stratejilerine nasıl entegre edilebileceğini incelemek amacıyla hazırlanmıştır. Ayrıca, raporun sonunda, bu kavramın pratikte nasıl uygulanabileceğine dair öneriler sunulacaktır.

Tehdit Aktörlerini Nasıl Alt Edeceğinizi Öğrenmek

Günümüzde kuruluşlar, her zamankinden daha fazla siber tehditle karşı karşıya kalıyor. Kitlesel saldırı yüzeylerine sahip olmanın yanı sıra, şirketler güvende kalmak, tetikte olmak ve önde kalmanın yollarını bulmalıdır. Bu zorluğun üstesinden gelmenin etkili yollarından biri, Pyramid of Pain 'ni anlamaktır. Güvenlik uzmanı David Bianco, 2013 yılında bu kavramı geliştirerek, farklı türdeki tehlike göstergelerinin (IoC'ler) bir kuruluşun tehdit algılama ve azaltma stratejilerini nasıl etkileyebileceğini ortaya koydu.

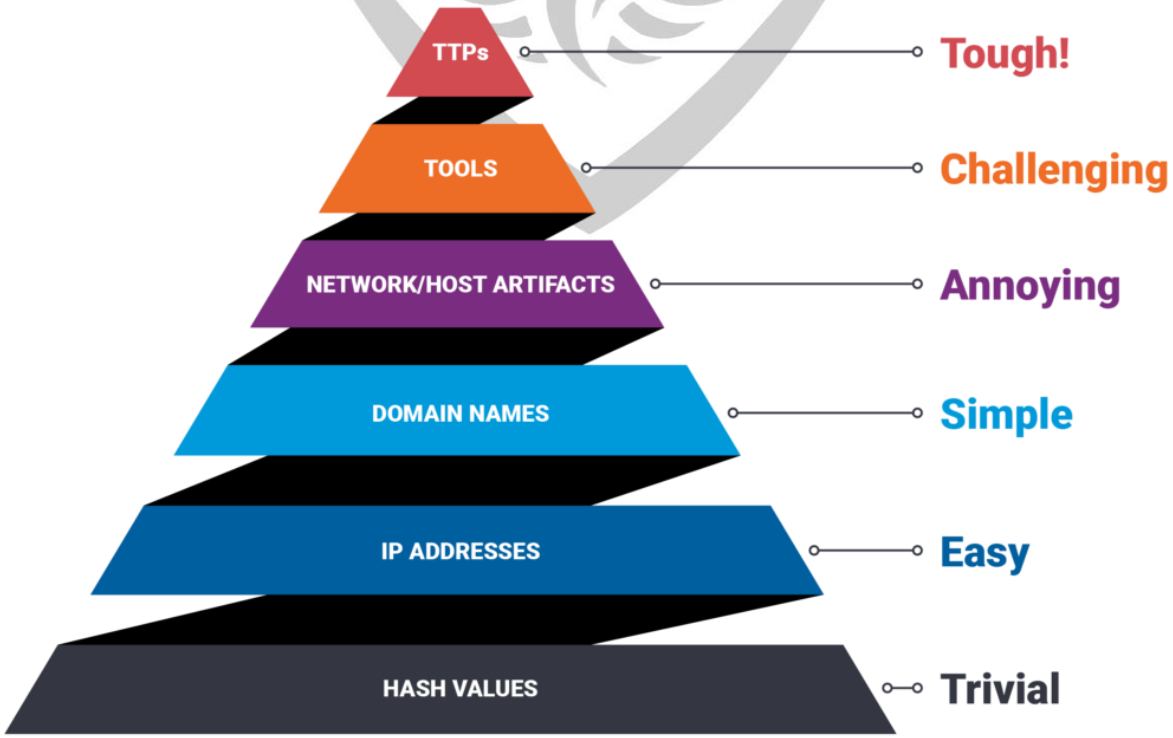
Pyramid of Pain deki 6 Seviye

Pyramid of Pain , en alttan en üste doğru, en az acı verenden en acı verene kadar altı IoC seviyesini tanımlar. Burada "acı verici" terimi, bir saldırganın bu seviyeleri üstlenmesinin ne kadar zor veya zahmetli olacağını ifade eder.

Piramidin tabanında, saldırganların kolayca değiştirebileceği karma değerler ve IP adresleri gibi basit göstergeler yer alır. Yukarı doğru çıktıkça, etki alanı adları, ağ ve ana bilgisayar yapıtları, araçlar ve nihayetinde taktikler, teknikler ve prosedürler (TTP'ler) gibi daha karmaşık ve değiştirilmesi zor olan göstergeler bulunur.

Güvenlik ekipleri, Pyramid of Pain 'ni tehdit azaltma stratejilerine entegre ederek erken tespit, yanıt verme yetenekleri ve genel siber güvenlik dayanıklılığını artırabilir.

Siber Güvenlikte Pyramid of Pain



1. Hash Değerleri
Piramidin tabanında, bir tehdit aktörü için en kolay ve savunmasız hedeflerden biri olan karma değerler bulunur. Bu değerler, bir yazılım veya dosyanın dijital parmak izi olarak kabul edilen kriptografik karma işlevlerinin çıktısıdır. SHA-1 ve MD5 gibi algoritmalar, iki farklı dosyanın aynı karma değerine sahip olmayacağını neredeyse garanti eder.

2. IP Adresleri
Bir sonraki seviye, internete bağlı bir cihazı benzersiz şekilde tanımlayan İnternet Protokolü (IP) Adresleridir. IP adreslerini engellemek önleyici bir önlem olabilir, ancak saldırganlar bu adresleri kolayca değiştirebildiğinden, uzun vadede etkileri sınırlıdır.

3. Domain Adları
Piramidin ortasında, alan adları daha karmaşık bir yapı sunar. Kötü amaçlı alan adlarını engellemek, IP adreslerini engellemekten daha etkili olabilir. Ancak, saldırganlar yeni alan adları kaydedebilir veya alan adı oluşturma algoritmaları (DGA'lar) kullanarak bu engelleri aşabilir.

4. Ağ/Ana Bilgisayar Yapıtları
Piramidin üst kısmında, ağ ve ana bilgisayar yapıtları yer alır. Bu seviyede, saldırganların ağ trafiğinde veya ana bilgisayar sistemlerinde bıraktığı izler tespit edilebilir. Bu yapıtlar, kötü niyetli aktivitelerin erken tespitine yardımcı olur.

5. Tool lar
Tehdit aktörleri, hedeflerine ulaşmak için çeşitli yazılım araçları kullanır. Bu araçlar, arka kapılar, parola kırıcılar ve diğer kötü amaçlı yazılımları içerebilir. Ancak, bu araçları değiştirmek veya geliştirmek saldırganlar için maliyetli ve zaman alıcıdır.

6. Taktikler, Teknikler ve Prosedürler (TTP'ler)
Piramidin tepesinde, saldırganların en zor değiştirebileceği unsurlar olan TTP'ler bulunur. TTP'ler, saldırganların kullandığı yöntemler ve stratejilerdir. Bu seviyede, belirli araçlar veya göstergelerden ziyade, saldırıların temel yöntemleri ele alınır.

Piramidi Kullanarak Saldırganlarla Savaşma

Pyramid of Pain 'ni siber güvenlik stratejilerine uygulamak, tehdit algılama, olay müdahalesi ve genel savunma yeteneklerini geliştirmek için kritik öneme sahiptir. Bu yaklaşım, saldırganları önemli ölçüde zorlayan alanları hedeflemeye odaklanır ve karmaşık siber saldırılara karşı savunmaları güçlendirir. Göstergeler, siber güvenlikte tehdit algılamanın yalnızca bir parçasıdır.

Bir organizasyonun davranışsal tehdit analizi, imza tabanlı tespit, sezgisel tespit, makine öğrenimi ve yapay zeka tabanlı tespitlerle donanmış olması, itibar ve veri ihlali riski arasındaki farkı belirleyebilir.

Bu piramit çerçevesinde işlerin nereye düştüğünü takip etmek, siber güvenlik ekiplerinin çevrelerindeki potansiyel tehlikelere karşı çabalarını daha etkili bir şekilde odaklamalarını sağlar.

Güvenlik Kontrollerini Doğrulamak İçin Piramidi Kullanmanın Yolları

Pyramid of Pain , çeşitli tehditleri ne kadar iyi tespit edip yanıtladıklarını değerlendirerek güvenlik kontrollerinizi doğrulamak için etkili bir çerçeve sunar:

Dosya Karmaları (Alt Katman)

Doğrulama : Güvenlik sisteminizin bilinen kötü amaçlı dosya karmalarını algılayıp engelleyebildiğini test edin.

Zorluk : Saldırganlar dosyayı değiştirerek karmayı kolayca değiştirebilir. Sisteminizin en son tehdit istihbaratıyla güncellendiğinden emin olun.

IP Adresleri ve Domain Adları

Doğrulama : Sisteminizin bilinen kötü amaçlı sunucularla iletişimi engelleyip engelleyemediğini görmek için IP ve etki alanı kara listelerini uygulayın.

Zorluk : Saldırganlar sıklıkla IP adreslerini ve etki alanlarını değiştirir. Sisteminizin bu değişikliklere hızlı bir şekilde uyum sağlayabildiğini doğrulayın.

Ağ/Ana Bilgisayar Yapıtları

Doğrulama : Güvenlik kontrollerinizin kötü amaçlı etkinliği gösteren ağ trafiğindeki veya ana bilgisayar yapılandırmalarındaki kalıpları belirleyebildiğini kontrol edin.

Zorluk : Bu tür tespitler daha sofistike mekanizmalar gerektirir. Düzenli penetrasyon testleri ve simülasyonlar yaparak kontrollerinizin bu yapıtları tanıyabildiğinden emin olun.

Tool lar

Doğrulama : Saldırganlar tarafından yaygın olarak kullanılan belirli kötü amaçlı araçların ve yardımcı programların kullanımını tespit edin ve engelleyin.

Zorluk : Saldırganlar araçları değiştirebilir veya mevcut olanları değiştirebilir. Kontrollerinizin yeni veya değiştirilmiş araçları tespit edebildiğinden emin olun.

Taktikler, Teknikler ve Prosedürler (TTP'ler)

Doğrulama : Güvenlik önlemlerinizin, saldırganların kullandığı belirli yöntemleri (örneğin, kimlik avı girişimleri veya ağ içinde yatay hareketler) tespit edip engelleyebildiğini değerlendirin.

Zorluk : Bu, davranışsal analiz gerektirir ve saldırgan metodolojilerinin derinlemesine anlaşılmasını gerektirir. Tespit kurallarınızı düzenli olarak güncelleyin ve tehdit avı egzersizleri yapın.

Pratik ve Çözüm Önerileri

Red Team Egzersizleri Gerçekleştirin : Pyramid of Pain nin tüm katmanlarında çeşitli IoC'leri kullanan saldırıları simüle edin. Güvenlik kontrollerinizin her gösterge türünü ne kadar iyi algıladığını ve yanıtladığını değerlendirin.

Düzenli Güncellemeler : Yeni ve gelişen tehditlere yanıt vermek için tehdit istihbaratı beslemelerinizin, tespit kurallarınızın ve yanıt stratejilerinizin düzenli olarak güncellendiğinden emin olun.

Sürekli İzleme : Anormallikleri ve potansiyel tehlike göstergelerini gerçek zamanlı olarak tespit etmek için sürekli izleme ve kayıt tutmayı uygulayın.

Güvenlik Araçlarının Entegrasyonu : Piramidin farklı katmanlarını kapsayan güvenlik araçlarının bir kombinasyonunu kullanın. Örneğin, dosya karmaları için antivirüs yazılımı, ağ eserleri için saldırı tespit sistemleri ve TTP'ler için davranışsal analizler.

Eğitim ve Farkındalık : Güvenlik ekibinizi piramidin tüm seviyelerinde göstergeleri tanımaları ve bunlara yanıt vermeleri için eğitin. Farkındalık ve eğitim, genel güvenlik duruşunuzu önemli ölçüde iyileştirebilir.

Raporun Değerlendirilmesi ve Kazanımlar

Bu rapor, siber güvenlikte Pyramid of Pain inceleyerek, tehdit aktörlerini alt etmek ve savunma mekanizmalarını güçlendirmek için kullanılabilecek bir çerçeve sundu. Piramidin altı seviyesi üzerinden, saldırganların savunma mekanizmalarını aşmak için kullandıkları yöntemler ve bu yöntemlere karşı alınabilecek önlemler ele alındı. Özellikle üst seviyelerdeki TTP'ler gibi unsurların değiştirilmesinin daha zor ve maliyetli olduğu vurgulandı.

Raporda ayrıca, Pyramid of Pain'in güvenlik stratejilerine entegre edilmesi ve güvenlik kontrollerinin bu çerçeve kullanılarak doğrulanması için pratik öneriler sunuldu. Kırmızı takım egzersizleri, düzenli güncellemeler ve sürekli izleme gibi adımlar, kuruluşların siber savunma yeteneklerini geliştirmelerine yardımcı olacak önemli uygulamalar olarak öne çıktı.

Sonuç olarak, Pyramid of Pain, siber güvenlik ekiplerinin tehditleri daha etkili bir şekilde tespit etmelerine ve savunma mekanizmalarını güçlendirmelerine yardımcı olan değerli bir araçtır. Bu çerçeve, kuruluşların siber güvenlik duruşlarını önemli ölçüde iyileştirebilir.

KAYNAKÇA

https://www.attackiq.com/glossary/pyramid-of-pain/

https://www.youtube.com/watch?v=S7AxXavRNQE

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

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

https://www.criticalstart.com/threat-detection-and-the-pyramid-of-pain/

https://chat.qwenlm.ai/

https://chatgpt.com/

https://chat.deepseek.com/