ALTAY

PYRAMID OF PAIN

ACI PİRAMİDİ

16.02.2025

MEHMET MERMER

SİBERVATAN

İÇİNDEKİLER

GİRİŞ

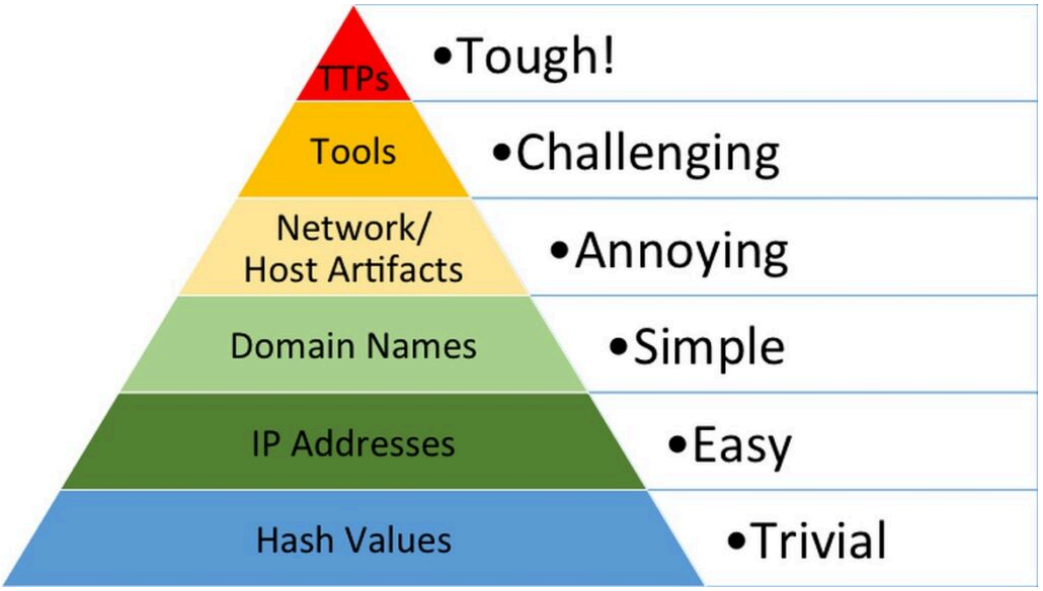
Siber güvenlik tehditleri, günümüzde giderek daha sofistike hale gelmekte ve güvenlik ekipleri için büyük bir zorluk oluşturmaktadır. Kötü amaçlı aktörler, saldırılarını daha etkili hale getirmek için sürekli yeni teknikler geliştirirken, savunma ekipleri de bu tehditlere karşı etkili yanıtlar vermek zorundadır. Tehdit istihbaratı, saldırganların kullandığı teknikleri, taktikleri ve prosedürleri (TTP'ler) analiz ederek savunma mekanizmalarının daha proaktif bir şekilde geliştirilmesini sağlar. Ancak, tehdit göstergelerini tespit etmek tek başına yeterli değildir; aynı zamanda saldırganları gerçekten zor duruma düşürecek önlemler almak da kritik öneme sahiptir.

Bu bağlamda, 2013 yılında David J. Bianco tarafından geliştirilen Pyramid of Pain modeli, güvenlik ekiplerinin tehdit göstergelerini nasıl değerlendirmesi ve hangi seviyede müdahale etmesi gerektiğini anlamalarına yardımcı olan önemli bir çerçevedir. Model, saldırganların faaliyetlerini sürdürmek için kullandıkları çeşitli göstergeleri (Indicators of Compromise - IoC) altı farklı seviyede sınıflandırarak, her seviyedeki müdahalenin saldırganlar üzerindeki etkisini açıklamaktadır. Pyramid of Pain'in temel amacı, yalnızca saldırıları engellemek değil, aynı zamanda saldırganların taktiklerini değiştirmeye zorlayarak onları gerçekten "acıya" sokmaktır.

Bu raporda, Pyramid of Pain modelinin temel bileşenleri ayrıntılı bir şekilde ele alınacak, her seviyenin siber güvenlik süreçlerindeki yeri incelenecek ve bu modelin pratikte nasıl uygulandığına dair örnekler sunulacaktır. Bu rapor, özellikle güvenlik operasyon merkezi (SOC) ekiplerine, hangi IoC'lerin tespit edilmesi ve engellenmesinin saldırganlar üzerinde en büyük etkiyi yaratacağı konusunda stratejik bir yol haritası sunmaktadır.

Pyramid of Pain Nedir?

David J. Bianco tarafından geliştirilen Acı Piramidi, tehdit istihbaratını optimize etmek ve siber güvenlik operasyonlarını güçlendirmek amacıyla oluşturulmuş stratejik bir modeldir. Bu model, tehdit göstergelerini hiyerarşik bir yapıda sınıflandırarak, siber güvenlik uzmanlarına saldırganları en üst seviyede engelleyebilecekleri noktaları vurgular. IoC'ler altı seviyeye ayrılır: Hash Değerleri, IP Adresleri, Alan Adları, Ağ/Sunucu Artifaktları, Araçlar ve Taktikler, Teknikler ve Prosedürler (TTP).



Temelde savunma ekiplerinin farklı tipteki IoC'leri ayırt etmesini kolaylaştırmayı amaçlamaktadır. Piramidin alt noktasından üst noktasına doğru ilerledikçe savunan taraf için IoC'lerin tanımlanması, saldırgan taraf için ise değiştirilmesi zorlaşmaktadır.

Saldırgan için örneklersek; saldırı içerisinde kullanılan hash değerleri manuel veya otomatik olarak kolaylıkla değiştirilebilirken, hedef organizasyon tarafından tespit edilmiş ve engellenmiş araçların yerine yenilerinin geliştirilmesi daha fazla efor gerektirecektir.

Savunan taraf içinse; saldırganın kullanmış olduğu zararlıya ait hash değerinin tespiti ve engellenmesi kolaylıkla yapılabilirken, bir tekniğin tamamen tespiti ve engellenmesi çok daha zor olacaktır.

Tehdit Göstergelerinin Hiyerarşisi

Acı Piramidi, IoC'leri saldırganlar üzerinde yarattığı etki ve tespit edilme zorluğuna göre altı seviyede sınıflandırır. Bu seviyeler; hash değerleri, IP adresleri, alan adları, ağ/sunucu artifaktları, araçlar ve taktikler, teknikler ve prosedürler (TTP) olarak sıralanmıştır. Her bir seviye, güvenlik ekiplerinin tehdit tespit ve önleme stratejilerini nasıl yapılandırmaları gerektiğine dair kritik bilgiler sunar. Piramit, en alt seviyedeki IoC'lerin tespit edilmesinin kolay, ancak saldırganlar üzerinde düşük etkiye sahip olduğunu; en üst seviyedeki IoC'lerin ise tespit edilmesinin zor, ancak saldırganlar için operasyonel maliyetlerinin yüksek olduğunu vurgular.

1. ***Hash Değerleri***

   Hash değerleri, belirli bir dosyanın veya verinin benzersiz dijital imzasını temsil eder. Bu değerler, genellikle zararlı yazılımları tespit etmek için kullanılır ve antivirüs yazılımları gibi araçlar tarafından sıkça başvurulan bir yöntemdir. Ancak, hash değerlerinin değiştirilmesi, saldırganlar için oldukça basittir. Bir dosyanın küçük bir kısmını bile değiştirmek, hash değerinin tamamen değişmesine neden olur. Dolayısıyla, hash tabanlı tespit mekanizmaları, genellikle statik ve değiştirilemeyen tehditlerle sınırlı kalır. Saldırganlar, basitçe zararlı dosyalarını yeniden derleyerek veya ufak değişiklikler yaparak, hash tespiti sistemlerini rahatlıkla atlatabilirler. Bununla birlikte, hash değerlerinin tespiti, düşük maliyetli ve hızlı bir çözüm sunması açısından avantajlıdır. Özellikle bilinen tehditlerin hızlıca belirlenmesi için bu yöntem etkin bir şekilde kullanılabilir. Ancak, gelişmiş ve sürekli değişen tehditlere karşı etkisiz kalabileceği göz önünde bulundurulmalıdır.

2. ***IP Adresleri***

   IP adresleri, ağ altyapısı üzerinden yapılan saldırılarda saldırganların izlerini sürmek için sıkça kullanılan bir IoC türüdür. Özellikle dağıtılmış hizmet reddi (DDoS) saldırıları, kötü amaçlı yazılım komuta ve kontrol sunucuları veya oltalama saldırıları gibi tehditlerin izlenmesi için IP adreslerinin engellenmesi yaygın bir yöntemdir. Ancak, IP adresleri saldırganlar tarafından kolayca değiştirilip gizlenebilir.VPN'ler ve Tor ağı gibi araçlar kullanılarak, saldırganların gerçek IP adreslerini gizlemeleri mümkündür. Ayrıca, saldırganlar dinamik IP adresleri kullanarak, tespit edilme olasılıklarını daha da düşürmektedirler. Bu sebeple, IP adreslerine dayalı tespit yöntemleri, düşük etkililiğe sahip olabilir. IP adreslerini engellemek, saldırganın bir noktada faaliyetlerini kesintiye uğratabilir; ancak, bu engeller kolayca aşılabilir.

3. ***Alan Adları***

Alan adları, özellikle oltalama ve zararlı yazılım saldırılarında sıkça kullanılan IoC'ler arasındadır. Saldırganlar, kötü amaçlı aktivitelerini yürütmek için belirli alan adlarını kullanır ve bu alan adlarının tespiti, saldırıların önlenmesi açısından kritik olabilir. Ancak, IP adreslerinde olduğu gibi, alan adlarının değiştirilmesi de saldırganlar için görece kolaydır. Yeni bir alan adı kaydetmek hızlı ve düşük maliyetlidir. Ayrıca, saldırganlar alan adı üretim algoritmaları kullanarak sürekli olarak yeni alan adları oluşturabilirler. Alan adlarına dayalı tespit stratejileri, genellikle zararlı yazılım veya oltalama saldırıları ile ilişkilendirilen bilinen alan adlarının engellenmesine odaklanır. Ancak, saldırganlar genellikle DNS yönlendirme, CDN hizmetleri veya anonimleştirme teknikleri kullanarak bu tür engellemeleri aşabilirler. Bu nedenle, alan adlarının engellenmesi, saldırganları tamamen durdurmayabilir, ancak operasyonel maliyetlerini artırabilir.

4. ***Ağ ve Sunucu Artifikaları***

Ağ veya sunucu artifaktları, belirli bir ağda veya sistemde saldırganın bıraktığı izlerdir. Bu izler, genellikle ağ trafiğindeki anormallikler, sistem yapılandırmalarındaki değişiklikler veya saldırgan tarafından kullanılan belirli dosya yolları gibi unsurları içerir. Artifaktlar, saldırganın kullandığı araçlara ve tekniklere özgü olabilir ve saldırganın operasyonlarını etkili bir şekilde takip etmeyi sağlar. Bu tür IoC'lerin tespiti, genellikle daha gelişmiş güvenlik çözümleri gerektirir. Intrusion Detection Systems (IDS) veya Intrusion Prevention Systems (IPS) gibi araçlar, ağ ve sistemlerdeki anormallikleri tespit edebilir ve saldırıları önleyebilir. Ancak, ağ veya sunucu artifaktlarının değiştirilmesi saldırganlar için daha zordur, çünkü operasyonel süreçlerini önemli ölçüde değiştirmeleri gerekebilir. Bu nedenle, bu tür göstergelerin tespiti saldırgan üzerinde daha yüksek bir operasyonel maliyet yaratır.

5. ***Araçlar***

Saldırganlar, hedeflerine ulaşmak için çeşitli araçlar ve yazılımlar kullanır. Bu araçlar, uzaktan erişim araçları (RAT), exploit kitleri veya zararlı yazılım framework'leri gibi çeşitli unsurları içerebilir. Acı Piramidi'nin beşinci seviyesinde yer alan bu IoC'lerin tespiti, saldırganın operasyonel verimliliğini ciddi şekilde etkileyebilir. Araçların değiştirilmesi, saldırganlar için ciddi bir zaman ve maliyet gerektirebilir, çünkü bu araçlar genellikle özelleştirilmiş ve belirli bir saldırı amacı için geliştirilmiştir. Örneğin, bir saldırganın kullandığı belirli bir uzaktan erişim aracı tespit edilip etkisiz hale getirildiğinde, saldırganın yeni bir araç bulması veya mevcut aracı yeniden yapılandırması gerekebilir. Bu da saldırganın operasyonel sürecinde ciddi bir kesinti yaratır. Araçların tespiti ve nötralize edilmesi, saldırganların operasyonel yeteneklerini önemli ölçüde sınırlandırabilir.

6. ***Taktikler, Teknikler ve Prosedürler (TTP)***

   Piramidin en üst seviyesinde yer alan Taktikler, Teknikler ve Prosedürler (TTP), saldırganların operasyonlarını yürütmek için kullandıkları genel stratejilerdir. Bu seviyede tespit edilen göstergeler, saldırganın operasyonel davranışlarını ve hedeflerine ulaşma biçimini doğrudan etkiler. TTP'lerin değiştirilmesi, saldırganlar için büyük operasyonel maliyetler yaratır, çünkü bu değişiklikler genellikle saldırının temel stratejilerini yeniden yapılandırmayı gerektirir. TTP'lerin tespiti, saldırganların genel operasyonel süreçlerini bozma açısından en etkili yöntemlerden biridir. Saldırganlar, belirli bir teknik veya prosedürle ilişkilendirildiklerinde, operasyonlarını sürdürmek için tamamen farklı bir yaklaşıma geçmek zorunda kalırlar. Bu da saldırganlar için operasyonel kesintiler yaratır ve saldırının başarılı olma olasılığını büyük ölçüde azaltır.

Pyramid of Pain ve Cyber Kill Chain

Pyramid of Pain modelinin Cyber Kill Chain ile ortak noktası, tehditlerin tespit edilmesine ve saldırganların faaliyetlerinin engellenmesine yönelik sistematik bir yaklaşım sunmasıdır. Ancak temel fark, Cyber Kill Chain modelinin saldırganların adımlarını tanımlayan bir yapı olmasıdır; saldırının aşamalarını belirler ve her aşamada neler yapılabileceğini analiz eder. Pyramid of Pain ise özellikle savunma ekipleri (Blue Team) için bir rehber niteliğindedir. Cyber Kill Chain saldırganın sürecini anlamaya odaklanırken, Pyramid of Pain bu süreci nasıl kesintiye uğratabileceğimizi ve saldırganı nasıl daha fazla zorlayabileceğimizi ele alır.

Blue Team ekipleri, Pyramid of Pain modelini kullanarak tehditleri önceliklendirebilir ve saldırıları engellemek için en etkili noktaları belirleyebilir.

Bu nedenle, Pyramid of Pain modeli, Blue Team'in sadece tehditleri algılamakla kalmayıp, aynı zamanda saldırganları gerçekten zor durumda bırakabilecek aksiyonları belirlemesine yardımcı olur. Etkili bir güvenlik operasyon merkezi, yalnızca imza tabanlı tehdit algılama mekanizmalarına güvenmek yerine, saldırganın yöntemlerini anlayarak ve bunları bozarak uzun vadeli bir savunma stratejisi oluşturmalıdır.

Acı Piramidinin Önemi

Acı Piramidi modeli, siber tehdit istihbaratını optimize etmek için stratejik bir yaklaşım sunar. Bu model, güvenlik ekiplerinin kaynaklarını en etkili göstergelere yönlendirmelerini sağlar ve saldırganlar üzerinde en büyük operasyonel zorlukları yaratacak alanlara odaklanmalarına yardımcı olur. TTP'ler gibi üst düzey IoC'lere odaklanmak, saldırganların taktiklerini değiştirmelerini zorlaştırır ve operasyonel maliyetlerini artırır. Böylece, tehdit avcılığı ve tespit süreçleri daha etkili hale gelir. Bu nedenle, siber güvenlik operasyonlarında proaktif tehdit tespiti stratejileri geliştirirken Acı Piramidi'ni bir rehber olarak kullanmak, saldırılara karşı etkili bir savunma sağlar.

SONUÇ

Bu raporda, Pyramid of Pain modelinin siber güvenlikteki rolü ve önemi detaylı bir şekilde incelenmiştir. Model, tehdit istihbaratının seviyeleri ve bu seviyelere karşı savunma yeteneklerinin nasıl geliştirilebileceği üzerine bir çerçeve sunmaktadır. Pyramid of Pain, saldırganların savunma sistemlerini aşma çabaları sırasında maruz kaldıkları zorlukları analiz etmektedir.

Modeldeki her seviyede, ilgili tehdit istihbaratının değeri arttıkça savunma stratejileri daha etkili hale gelir. Özellikle Taktikler, Teknikler ve Prosedürler (TTP'ler) seviyesinde yapılan iyileştirmeler, organizasyonların saldırganları tespit etme ve engelleme yeteneğini güçlendirir. Bu model, en temel seviyedeki hash değerlerinden, daha karmaşık ve derinlemesine analiz gerektiren TTP seviyelerine kadar farklı savunma stratejilerini kapsar.

Savunma stratejilerinin her seviyede uygulanabilmesi, tehdit istihbaratının etkin kullanımıyla mümkündür. Bu rapor, organizasyonların yalnızca temel savunma önlemleriyle yetinmeyip, daha dinamik ve etkili bir yaklaşım benimsemeleri gerektiğini vurgulamaktadır. Saldırganların sistemleri aşma çabaları, savunma sistemlerinin derinlemesine olmasıyla zorlaşacaktır, ancak bu durum aynı zamanda kaynakların verimli kullanılması gerektiğini de ortaya koymaktadır.

Sonuç olarak, Pyramid of Pain modelinin etkili bir şekilde uygulanması, kurumların siber güvenlik savunmalarını güçlendirmekte önemli bir rol oynamaktadır. Bu model, tehditlere karşı stratejik bir yaklaşım geliştirilmesine katkı sağlayacak ve organizasyonların savunma kapasitesini artıracaktır. Modelin her seviyesinde yapılacak iyileştirmeler, uzun vadede daha etkili savunma stratejileri geliştirilmesine olanak tanıyacaktır.

KAYNAKÇA

1. https://cybershieldcommunity.com/pyramid-of-pain/
2. https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
3. https://kaganeglence.com/2021/10/29/red-team-siber-istihbarat-ve-red-team/
4. https://www.gaissecurity.com/blog/aci-piramidi-siber-tehdit-istihbaratinda-analitik-bir-model
5. https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain#what-is-pyramid-of-pain?
6. https://www.linkedin.com/pulse/olay-m%C3%BCdahalesi-s%C3%BCre%C3%A7lerinde-ioc-tespiti-pyramid-pain-fatih-%C3%A7i%CC%87ro%C4%9Flu/