Pyramid of Pain

Bilgehan Bayrak

17.02.2025

2025

İçindekiler Tablosu

GİRİŞ2

PYRAMİD OF PAİN MODELİNİN TANITIMI 2

MODELİN KATMANLARI 3

SİBER GÜVENLİK UYGULAMALARI VE KULLANIMI4

PYRAMİD OF PAİN’İN GÜÇLÜ YÖNLERİ 4

SONUÇ4

KAYNAKÇA5

**GİRİŞ**

Siber güvenlik dünyasında tehdit aktörlerinin tespit edilmesi ve analiz edilmesi, her geçen gün daha önemli hale gelmektedir. Tehdit istihbaratı, bu tehditlerin anlaşılmasında ve onlara karşı etkili bir mücadele verilmesinde kritik bir rol oynar. Ancak, tehditlerin tespiti ve izlenmesi çok çeşitli zorluklarla karşılaşabilir. Bu noktada, Pyramid of Pain modeli devreye girer. Bu model, tehdit verilerini analiz ederken karşılaşılan zorlukları ve bu zorlukların seviyesini görsel olarak temsil eden bir çerçeve sunar.

Ron Gula tarafından ortaya konan Pyramid of Pain, tehdit aktörlerinin izlerini sürerken karşılaşılan güçlüklerin derecesini ortaya koyar. Modelin temel amacı, siber güvenlik profesyonellerinin tehditleri anlamalarına ve ne tür tehditlerin daha kolay veya zor tespit edilebileceğini öğrenmelerine yardımcı olmaktır.

Bu rapor, **Pyramid of Pain** modelini derinlemesine incelemeyi amaçlamaktadır. Modelin yapısını, her bir katmanın ne ifade ettiğini ve siber güvenlik stratejilerine nasıl entegre edilebileceğini açıklayacağız. Ayrıca, modelin organizasyonlara sunduğu avantajları ve tehdit tespitindeki zorlukların nasıl aşılabileceğini tartışacağız.

**PYRAMİD OF PAİN MODELİNİN TANITIMI**

**Pyramid of Pain**, siber güvenlikteki tehdit analizlerinde kullanılan bir modeldir. Model, tehdit aktörlerinin tespiti ve izlenmesi sırasında karşılaşılan güçlüklerin seviyesini belirler. Her bir katman, tehdit verisinin ne kadar zor tespit edilebileceğini ve tehdit aktörlerinin izlerinin ne kadar belirgin olduğunu gösterir. Bu piramit, bir tehdit analistinin karşılaştığı zorlukları anlamalarına yardımcı olur ve bu zorlukların tehdit verisinin seviyelerine göre nasıl değiştiğini görselleştirir.

Pyramid of Pain modeli, beş ana seviyeden oluşur:

1. **Hash Değerleri (En Alt Seviye)**
2. **IP Adresleri**
3. **Domain Adları**
4. **Yöntemler ve Araçlar (Taktikler, Teknikler ve Prosedürler - TTP’ler)**
5. **Saldırı Stratejileri ve Davranışları (En Üst Seviye)**

Her seviyedeki zorluk, verilerin tespit edilmesinin ne kadar zor olduğunu gösterir. En alt seviyedeki veriler (örneğin: hash değerleri), tehdit aktörlerinin izlerinin en belirgin olduğu ve kolayca tespit edilebilen verilerdir. Buna karşın, en üst seviyedeki saldırı stratejileri ve davranışlar, analiz edilmesi en zor ve karmaşık verilerdir.

**MODELİN KATMANLARI**

**1. Hash Değerleri (En Alt Seviye)**

Hash değerleri, bireysel dosyaların dijital parmak izleridir. Bu değerler, bir dosyanın içeriğini temsil eden sabit uzunluktaki sayı dizileridir. Hash değerleri genellikle MD5, SHA-1 veya SHA-256 algoritmalarından biriyle hesaplanır. Bu seviyede tehdit tespiti, dosyaların belirli bir hash değeriyle eşleşmesi ile yapılır ve bu veriler kolayca toplanabilir ve analiz edilebilir. Kötü amaçlı yazılımlar ve zararlı dosyalar hash değerleriyle hızlı bir şekilde tanımlanabilir.

**2. IP Adresleri**

IP adresleri, bir cihazın internet üzerindeki kimliğidir. Siber güvenlikte, kötü amaçlı aktiviteler genellikle belirli IP adreslerinden gelir. Bu katman, belirli IP adreslerinin kötü amaçlı yazılımlar tarafından kullanılıp kullanılmadığını tespit etmeye yöneliktir. IP adreslerinin takibi, genellikle hızlı bir şekilde yapılabilir. Ancak, IP adresleri kolayca değiştirilebilir veya gizlenebilir, bu nedenle bu veriler belirli bir süre sonra daha az güvenilir olabilir.

**3. Domain Adları**

Domain adları, internet üzerindeki belirli web sitelerine veya hizmetlere işaret eder. Kötü amaçlı yazılımlar, zararlı web sitelerine yönlendirebilir veya komuta ve kontrol (C2) sunucularıyla iletişim kurmak için domain adlarını kullanabilir. Domain adlarının tespiti, IP adreslerinden daha karmaşık olabilir, çünkü domainler değiştirilebilir, yeni domainler oluşturulabilir veya domainler gizlenebilir.

**4. Yöntemler ve Araçlar (Taktikler, Teknikler ve Prosedürler - TTP’ler)**

Bu seviyede, tehdit aktörlerinin kullandığı araçlar ve yöntemler analiz edilir. Tehdit aktörlerinin kullandığı yöntemler, belirli bir saldırının nasıl gerçekleştirildiğine dair bilgi verir. Bu katman, analistlerin tehdit aktörlerinin kullandığı araçları ve taktikleri anlamalarına yardımcı olur. Ancak, bu tür veriler daha karmaşık ve daha az belirgindir, bu nedenle bu seviyedeki tehditlerin tespiti daha zordur.

**5.Saldırı Stratejileri ve Davranışları (En Üst Seviye)**

En üst seviyede yer alan saldırı stratejileri ve davranışlar, tehdit aktörlerinin uzun vadeli hedeflerine ve saldırı yöntemlerine dair bilgi verir. Bu seviyedeki tehdit tespitleri, genellikle en zor olanlardır, çünkü bu veriler, tehdit aktörlerinin davranışsal kalıplarını anlamayı gerektirir. Bu stratejiler, bir saldırının hangi yollarla genişleyeceğini ve nasıl daha derinlemesine yayılabileceğini anlamaya yönelik olan analizleri içerir.

**SİBER GÜVENLİK UYGULAMALARI VE KULLANIMI**

Pyramid of Pain, siber güvenlik profesyonellerinin tehdit aktörlerini anlamalarına yardımcı olur. Tehdit istihbaratı, organizasyonların hangi seviyelerdeki tehditlere odaklanmaları gerektiğini belirlemek için bu modelden faydalanır. Modelin her bir seviyesi, tehdit verisinin ne kadar kolay tespit edilebileceğine dair bilgiler sunar ve analistlerin hangi tehdit verilerine odaklanmaları gerektiğini gösterir.

Örneğin, hash değerleri gibi düşük seviyeli veriler hızlıca toplanabilir ve analiz edilebilir. Bu veriler, genellikle kötü amaçlı yazılım tespiti için kullanılır. Ancak, daha yüksek seviyeli tehditler (örneğin: TTP’ler veya saldırı stratejileri) daha zor tespit edilir ve daha derinlemesine analiz gerektirir.

**PYRAMİD OF PAİN’İN GÜÇLÜ YÖNLERİ**

* **Hızlı Tehdit Tespiti:** Düşük seviyeli tehdit verileri (hash, IP adresleri) hızlıca tespit edilebilir ve daha hızlı bir yanıt süresi sağlar.
* **Kaynakların Verimli Kullanımı:** Model, tehdit verisinin tespit edilme zorluğuna göre analizleri önceliklendirmeyi sağlar. Bu, siber güvenlik ekiplerinin sınırlı kaynaklarını daha verimli kullanmalarına olanak tanır.
* **Derinlemesine Analiz:** Yüksek seviyedeki tehdit verileri (TTP’ler ve saldırı stratejileri), uzun vadeli tehditleri analiz etmek için önemlidir. Bu veriler, saldırıların daha kapsamlı ve karmaşık doğasını anlamaya yardımcı olur.
* **Proaktif Savunma Stratejileri:** Model, tehditlerin belirli seviyelerdeki zorluklarını anlamaya yardımcı olduğu için, organizasyonlar bu tehditlere karşı daha proaktif savunmalar geliştirebilir.

**SONUÇ**

Pyramid of Pain modeli, siber güvenlik dünyasında tehdit aktörlerini izlemek ve tespit etmek için son derece önemli bir araçtır. Bu model, tehdit verilerinin ne kadar zor tespit edilebileceğini anlamayı sağlar ve organizasyonların siber güvenlik stratejilerini daha verimli bir şekilde oluşturmalarına yardımcı olur. Düşük seviyedeki tehdit verileri, hızlı tespit ve yanıt sağlarken, yüksek seviyedeki tehditler daha derinlemesine analiz gerektirir. Sonuç olarak, Pyramid of Pain modeli, tehdit istihbaratını daha etkili hale getirir ve organizasyonları daha güçlü savunmalar geliştirmeye yönlendirir.

**KAYNAKÇA**

* 1. <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>
  2. <https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain>
  3. <https://cybershieldcommunity.com/pyramid-of-pain/>
  4. <https://chatgpt.com>