Pyramid of Pain Raporu

Hazırlayan: Sema Nimet Ünal  
Tarih: 17.02.2025

İçindekiler

[1. Giriş 3](#_Toc190679157)

[2. Pyramid of Pain Modeli 3](#_Toc190679158)

[2.1 Modelin Katmanları ve Anlamları 3](#_Toc190679159)

[Hash Values (Özet Değerleri) 3](#_Toc190679160)

[IP Addresses (IP Adresleri) 3](#_Toc190679161)

[Domain Names (Alan Adları) 3](#_Toc190679162)

[Network/Host Artifacts (Ağ/Sistem Artifaktları) 4](#_Toc190679163)

[Tools (Araçlar) 4](#_Toc190679164)

[TTPs (Tactics, Techniques, and Procedures - Taktikler, Teknikler ve Prosedürler) 4](#_Toc190679165)

[2.2 Siber Güvenlikte Kullanımı 4](#_Toc190679166)

[2.3 Tehdit Avcılığı (Threat Hunting) İçin Önemi 4](#_Toc190679167)

[3. Sonuç 4](#_Toc190679168)

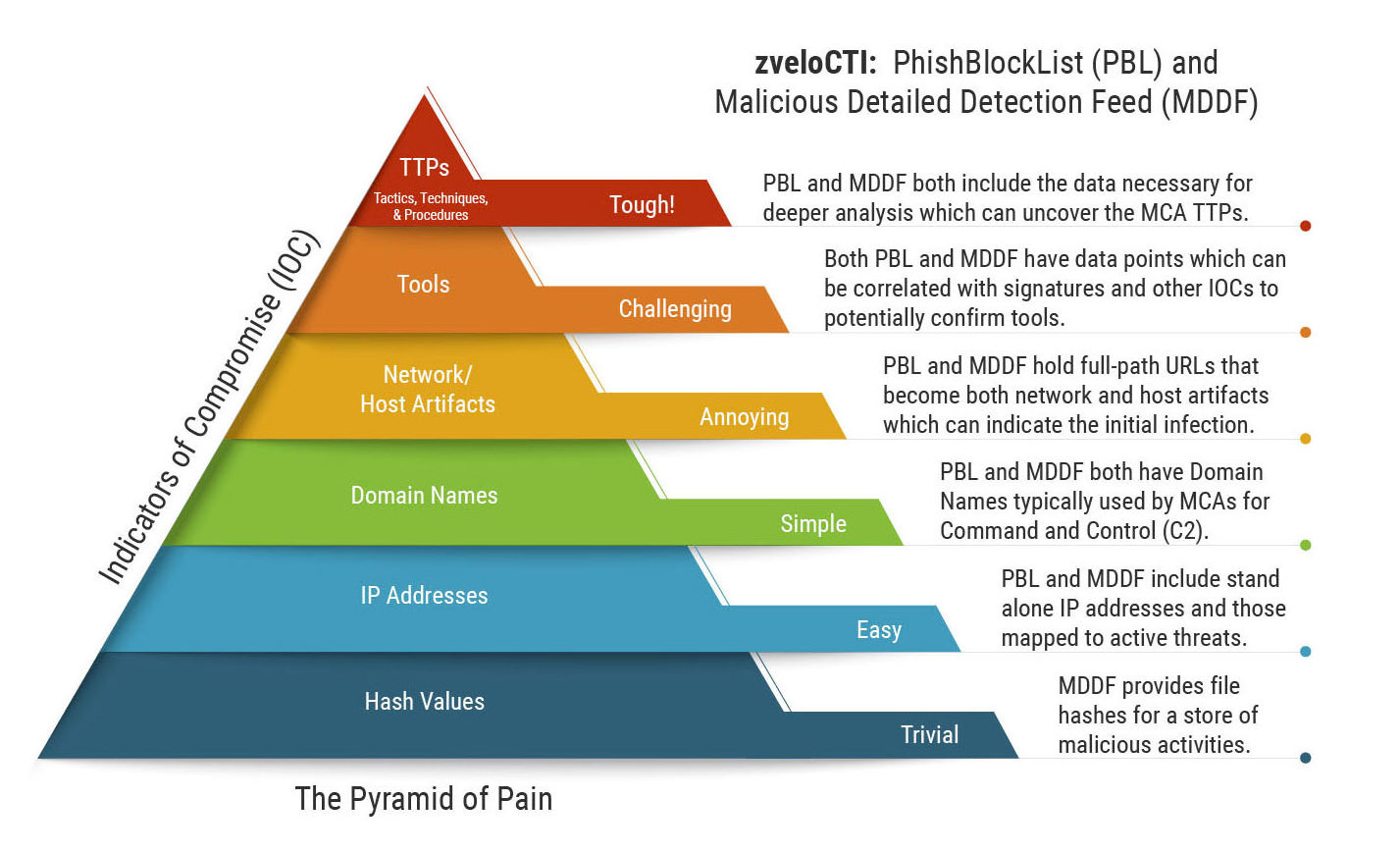
[4. Kaynakça 4](#_Toc190679169)

# 1. Giriş

Bu rapor, siber güvenlik alanında tehdit istihbaratını daha iyi anlamak için kullanılan Pyramid of Pain modelini açıklamaktadır. Model, saldırganların kullandığı izlerin tespit edilmesi ve bunlara karşı koyma stratejileri hakkında bilgi sağlar.

# 2. Pyramid of Pain Modeli

Pyramid of Pain, David J. Bianco tarafından geliştirilen ve saldırganların kullandığı tehdit göstergelerinin (IoC - Indicators of Compromise) güvenlik analistleri tarafından ne kadar zor tespit edilebileceğini ve saldırganlar için ne kadar yıkıcı olacağını gösteren bir modeldir.



## 2.1 Modelin Katmanları ve Anlamları

Pyramid of Pain modeli, altı farklı tehdit göstergesi seviyesinden oluşur:

### Hash Values (Özet Değerleri)

* + MD5, SHA-1, SHA-256 gibi dosya bütünlüğü hash’leri.
  + Kolayca değiştirilebilir ve tespit edildiğinde saldırganlar için düşük seviyede bir engel oluşturur.

### IP Addresses (IP Adresleri)

* + Kötü amaçlı IP adresleri engellenebilir, ancak saldırganlar farklı IP'ler kullanarak bunu aşabilir.

### Domain Names (Alan Adları)

* + Saldırganlar tarafından kullanılan kötü amaçlı alan adları, DNS filtreleme ile engellenebilir.
  + Ancak, yeni alan adları oluşturmak nispeten kolaydır.

### Network/Host Artifacts (Ağ/Sistem Artifaktları)

* + Özel protokoller, belirli dosya yolları veya sistem yapılandırmaları gibi kalıntılar.
  + Saldırganlar için daha büyük bir zorluk oluşturur çünkü değiştirilmesi zaman alır.

### Tools (Araçlar)

* + Saldırganların kullandığı özel yazılımlar, exploit kitleri ve otomasyon araçları.
  + Engellenmesi saldırganları yavaşlatabilir ve yeni araçlar geliştirmeye zorlayabilir.

### TTPs (Tactics, Techniques, and Procedures - Taktikler, Teknikler ve Prosedürler)

* + Saldırganların kullandığı yöntemlerin tespit edilmesi en etkili savunma yöntemidir.
  + TTP'lerin değiştirilmesi saldırganlar için en büyük zorluktur, çünkü operasyonel süreçlerini yeniden tasarlamaları gerekir.

## 2.2 Siber Güvenlikte Kullanımı

Pyramid of Pain modeli, saldırganların davranışlarını analiz ederek daha etkili tehdit avcılığı yapılmasını sağlar. Yüzeysel tehdit göstergelerinin tespiti yerine davranışsal analiz ve TTP tabanlı tehdit avcılığı ön plana çıkar.

## 2.3 Tehdit Avcılığı (Threat Hunting) İçin Önemi

* Düşük seviyeli IoC'lerin (hash, IP, domain) hızlı değiştirilebileceği unutulmamalıdır.
* TTP’lere odaklanarak saldırganların hareketlerini analiz etmek daha güçlü bir savunma sağlar.
* Güvenlik sistemleri, Pyramid of Pain katmanlarını temel alarak tehdit istihbaratı geliştirebilir.

# 3. Sonuç

Pyramid of Pain modeli, saldırganların kullandığı izlerin ne kadar kolay değiştirilebileceğini ve savunma mekanizmalarının nasıl güçlendirilebileceğini göstermektedir. Tehdit avcılığı sürecinde, düşük seviyeli göstergeler yerine TTP'lerin tespit edilmesi en etkili savunma stratejilerinden biridir.

# 4. Kaynakça

1. David J. Bianco – The Pyramid of Pain
2. https://zvelo.com/pyramid-of-pain/