29% COMPLETE 86/287 Steps

‹ Previous Topic

Mark Complete ✓

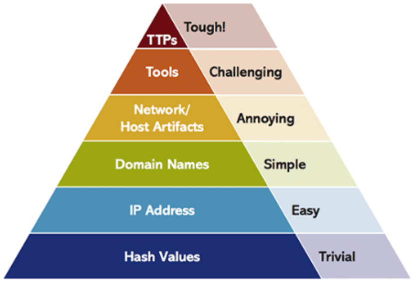
Pyramid of Pain

Blue Team Level 1 Certification (Standard) > TI3) Operational Threat Intelligence > Pyramid of P... IN PROGRESS

The rising difficulty is what we want to the layout before attackers. Our data is a resource that we work daily to digest and to put into useful intelligence. These resources are also what malicious actors want as well. They want your information and the ability to sit and farm. Luckily, how quickly we respond, and the level of protection given to that resource can help be defined by what is called "The Pyramid of Pain."

WHAT IS IT?

The pyramid of pain is a visual representation of the amount of pain we can cause a malicious actor in denying them certain indicators. By that, the base of the pyramid is the lowest amount, near trivial. Each trivial section is wider to indicate the breadth of the room given to those indicators is wide.



HASH VALUES

Trivial amounts of pain relate to **hash values.** They can provide the highest confidence indicators yet are vulnerable to modification by the attack or accidentally by the end-user. By the degree that these can change and how often, these would be the least useful indicators and provide a minimal amount of frustration to an attacker.

IP ADDRESS

Stepping up the pyramid, next is **IP addresses.** Though having a unique address is beneficial, it is not uncommon to change these with VPNs, TOR browsing, or open proxies to reassemble your attack from a different address.

DOMAIN NAMES

Blue Team Level 1 Certification (Standard)

Introduction to BTL1

~~Welcome to Blue Team Level 1!~~
4 Topics

~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

~~Introduction to Security Fundamentals~~
1 Topic

~~Soft Skills~~
7 Topics

~~Security Controls~~
5 Topics | 1 Quiz

~~Networking 101~~
6 Topics | 1 Quiz

~~Management Principles~~
4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

~~PA1) Introduction to Emails and Phishing~~
7 Topics | 1 Quiz

~~PA2) Types of Phishing Emails~~
10 Topics | 2 Quizzes

~~PA3) Tactics and Techniques Used~~
12 Topics | 2 Quizzes

~~PA4) Investigating a Phishing Email~~
8 Topics | 2 Quizzes

~~PA5) Analysing URLs, Attachments, and Artifacts~~
8 Topics | 1 Quiz

PA6) Taking Defensive Actions
12 Topics | 1 Quiz

PA7) Report Writing
7 Topics | 1 Quiz

PA8) Phishing Response Challenge
3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence
7 Topics

TI2) Threat Actors & APTs
6 Topics | 2 Quizzes

TI3) Operational Threat Intelligence
7 Topics | 1 Quiz

Section Introduction, Operational Intelligence

Precursors Explained

Indicators of Compromise Explained

MITRE ATT&CK Framework

Lockheed Martin Cyber Kill Chain

Attribution and its Limitations

Pyramid of Pain

Activity) End of Section Review, Operational Intelligence

TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz

○ TI5) Strategic Threat Intelligence
● 5 Topics | 1 Quiz

○ TI6) Malware and Global Campaigns
● 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics
● 5 Topics

○ DF2) Forensics Fundamentals
● 10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection
● 8 Topics | 1 Quiz

○ DF4) Windows Investigations
● 3 Topics | 3 Quizzes

○ DF5) Linux Investigations
● 4 Topics | 2 Quizzes

○ DF6) Volatility
● 3 Topics | 1 Quiz

○ DF7) Autopsy
● 4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ SI1) Introduction to SIEM
● 7 Topics | 1 Quiz

○ SI2) Logging
● 6 Topics | 2 Quizzes

○ SI3) Aggregation
● 2 Topics | 1 Quiz

○ SI4) Correlation
● 6 Topics | 1 Quiz

○ SI5) Using Splunk
● 5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

○ IR1) Introduction to Incident Response
● 8 Topics | 1 Quiz

○ IR2) Preparation Phase
● 10 Topics | 2 Quizzes

○ IR3) Detection and Analysis Phase
● 7 Topics | 4 Quizzes

○ IR4) Containment, Eradication, and Recovery Phase
● 5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting
● 7 Topics

○ IR6) MITRE ATT&CK
● 13 Topics | 2 Quizzes

BTL1 EXAM

○ Exam Preparation

○ Using RDP and SSH

○ How to Start Your Exam

DOMAIN NAMES

Rising higher we sit on **domain names**, which can be changed, but require registration and hosting. Many DNS providers do not all have the same standards across the board in terms of legality and restrictions, which can make it fairly easy for an attacker to change domains. Though not as easy as IP addresses, these can be modified with a longer wait time.

NETWORK/HOST ARTEFACTS

Network and host artifacts start to provide more difficulty to the attacker once you begin implementing defenses against these tools and methods they are using. This could be determined by finding where directories are commonly created, specific registry values, files, etc. As an example, the Locky spam waves showcased:

- different domain names
- different IP addresses
- different hashes

But, through a three-month campaign, the host artifacts performed the same. Changing the logic in the malware is much harder than changing IP addresses. By signaling out these indicators and stopping them, it creates greater frustration and hurdle for the attacker.

TOOLS

Tools are hard to change. Carpenters can use a reliable saw for years. The same goes for adversaries attacking your network. Identifying one or more of the tools they are using to distribute attacks and halting their use puts a severe bend in their hose. This requires re-tooling, researching, or building another method to attack. This could also simply force them to move on.

TTPs

Finally, we come to **tactics, techniques, and procedures (TTPs).** These are not just tools, but these are behavior patterns. You learn their methods by profiling the behavior and responding accordingly, such as spearphishing with PDFs. These attackers are human and act in similar, producible patterns. Forcing them to change their behavior and methods is the most time-consuming defense against them. This requires a reworking of their whole methodology in attacking.

WHY USE IT?

The purpose in recognizing these indicators is how to best identify weaknesses and mitigate them. Most importantly, it makes the lives of these adversaries harder. Each layer in front of the bad actor helps solidify your response and tune your organization to better prepare and detect and respond to indicators of compromise.

‹ Previous Topic   Mark Complete ✓

Back to Lesson