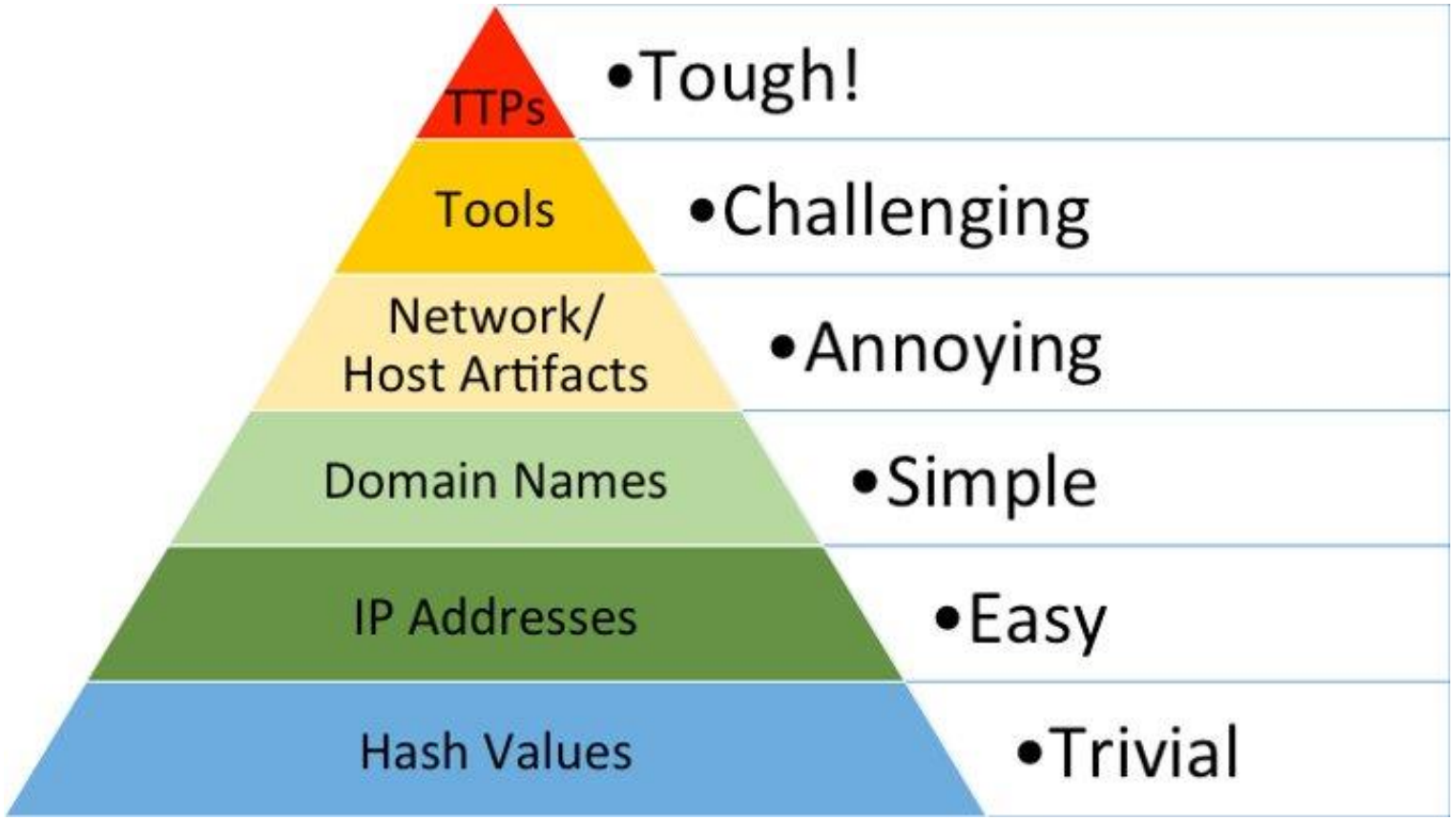
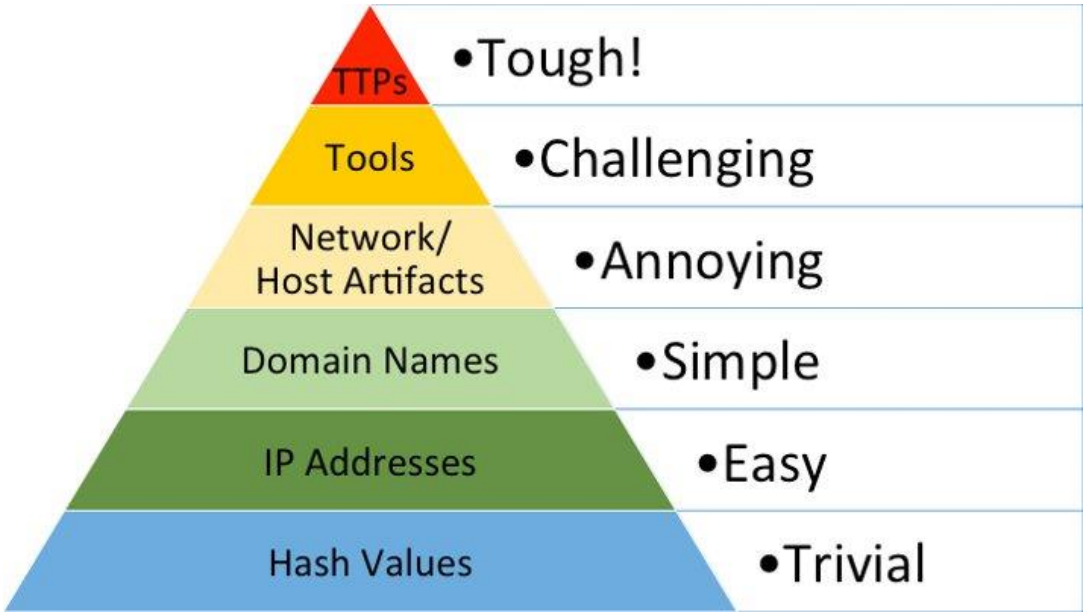
Cybersecurity Student Association

Pyramid of Pain



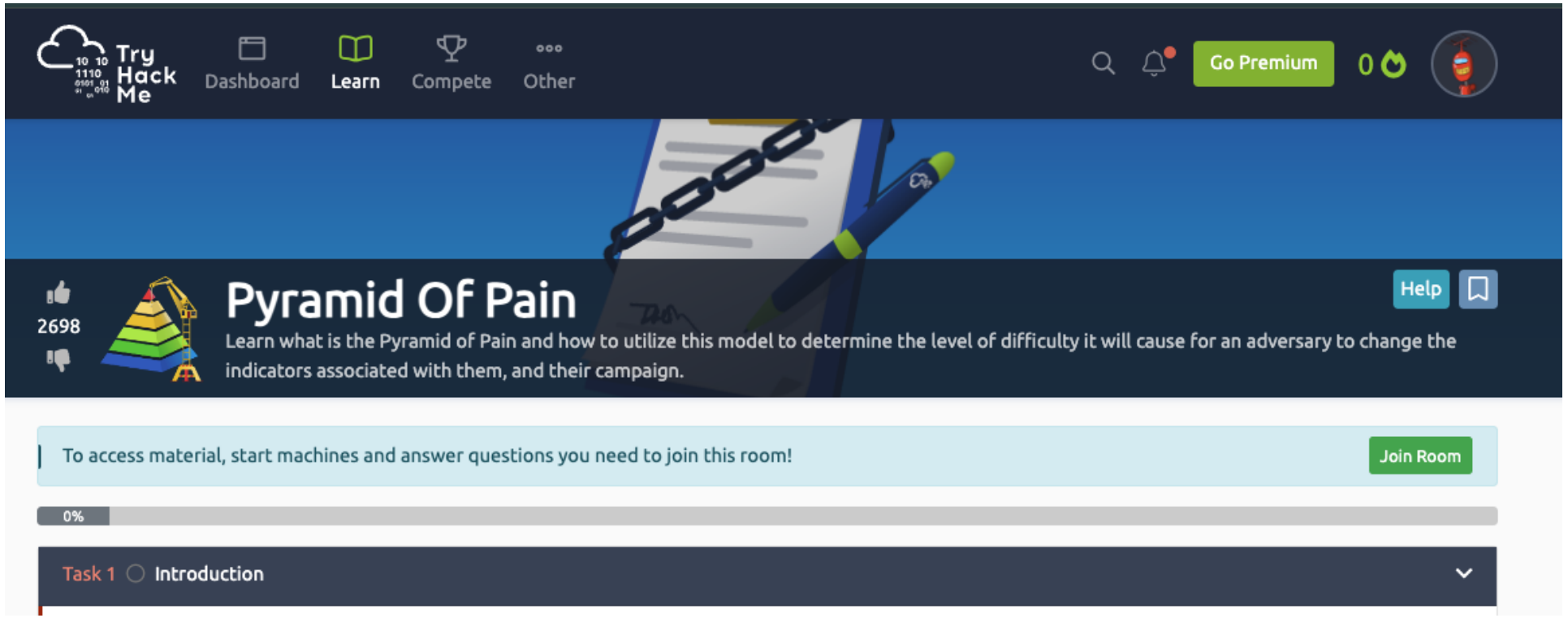
What is the Pyramid of Pain?

- The Pyramid of Pain is a conceptual framework that illustrates the varying levels of difficulty and cost an adversary would encounter to evade detection and continue their attack, in the context of cybersecurity defenses.
- It categorizes different indicators and attributes related to cyber threats, ranging from the trivial at the bottom to the most costly and complex to at the top.



TryHackMe

https://tryhackme.com/room/pyramidofpainax



Hash Values

A change as subtle as the addition or removal of a single space or a single line of code—provided it doesn't interfere with the program's operation—can entirely alter the hash value of the malware. This characteristic makes hash values highly susceptible to modifications, even those that are inconspicuous and don't disrupt the functionality of the underlying program or tool.

SHA3-256(1111111111111111111111111111111111111111) =
bf8d60cfc6654a2cd4dbf63e5a85cf8c34674c3f41f1bf38312ce88012536d69

SHA3-256(1111111111111111111111111111111111111110) =
b45d95d47b00d9fcdb9af0437bbaa5101a51f55ebcc2163bb731cee7761d6d80

IP Addresses

- IP addresses are easily changeable for adversaries using tools like proxy servers, VPNs, and dynamic IP assignments.
- The Tor network further anonymizes users by routing traffic through multiple servers.
- Adversaries can also hide their IP addresses by routing actions through compromised machines.
- IP addresses are fundamental indicators due to their ubiquity, but their ease of change places them at the widest part of the Pyramid of Pain.
- Denying adversaries the use of an IP address is often ineffective as they can easily switch to another.

Domain Names

- **Example 1:** sezname[.]cz
  - A malicious domain used by Snatch Ransomware Gang, illustrating how threat actors often create domains specifically for nefarious activities.
- **Example 2:** protonmail[.]com / proton[.]me
  - Legitimate and encrypted email services misused by threat actors, showcasing *how legal platforms can be exploited* for malicious communications.
- **Example 3:** sn.tchnews.top@protonmail[.]me
  - Specific email address reported by victims, *exemplifying the combination of legitimate email services* with uniquely crafted addresses for malicious interactions.

- They require registration, payment, and hosting but can still be changed relatively easily.
- Numerous DNS providers with lenient registration standards facilitate this ease of change.
- New domains may take up to a day or two to propagate throughout the Internet.
- However, malicious actors can swiftly switch to new domains once existing ones are blacklisted or taken down, minimizing disruption to their activities.
- Relying solely on domain names for defensive measures is insufficient due to the fluidity and variety of domains used by threat actors.

Network/Host Artifacts

- Categorized as "Annoying" to alter, are distinctive elements of malicious activity within a network or host.
- They serve as evidence of malicious activity and can disrupt an attacker's workflow if modified.
- Modifying these artifacts can make it more challenging for attackers to maintain stealth and evade detection.
- Detecting and responding to indicators at this level forces attackers to reconfigure or recompile their tools, causing inconvenience and hindrance to their malicious endeavors.
- For example, blocking requests with distinctive User-Agent strings in HTTP recon tools forces attackers to identify and overcome detection obstacles, albeit with potentially trivial fixes.

- URL Patterns
- Log Messages
  - ***Example:*** A Windows Defender Firewall setting was changed in private, public, and domain profile with type “Enable Windows Defender Firewall” and value of “no”.
- Command and Control (C2) Information,
- Registry Objects
  - ***Example:*** HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SuperBackupMan:Default:Service
- Files
- Folders
  - ***Example:*** C:$SysReset folder.

Tools

Creating or modifying malicious tools demands sophisticated skills and a deep understanding of the target system and the tool itself.

Attackers must invest substantial time and energy to develop, test, and deploy new malicious tools that can evade existing security measures, making it a burdensome task.

At this level, adversaries lose the ability to use specific tools, compelling them to find or create new ones.

Examples of tool indicators include antivirus or Yara signatures, distinctive communication protocols, and fuzzy hashes.

Detecting and responding to tool indicators require adversaries to invest time in research, development, and training, costing them valuable resources.

Tactics, Techniques, & Procedures

- Tactics, Techniques, and Procedures (TTPs) in the Pyramid of Pain represent a high level of difficulty and sophistication for adversaries to modify.
- TTPs detail the comprehensive methodologies used by attackers at every stage of the attack lifecycle, making them integral components of an adversary's toolkit.
- Altering TTPs requires profound understanding, inventive strategy, and adept execution, obstructing adversaries' ability to orchestrate malicious endeavors seamlessly.
- Detecting and responding to TTPs directly addresses adversary behaviors rather than their tools, making it the most effective level of response.
- Responding to TTPs quickly forces adversaries to either give up or reinvent themselves from scratch

Mitre ATT&CK

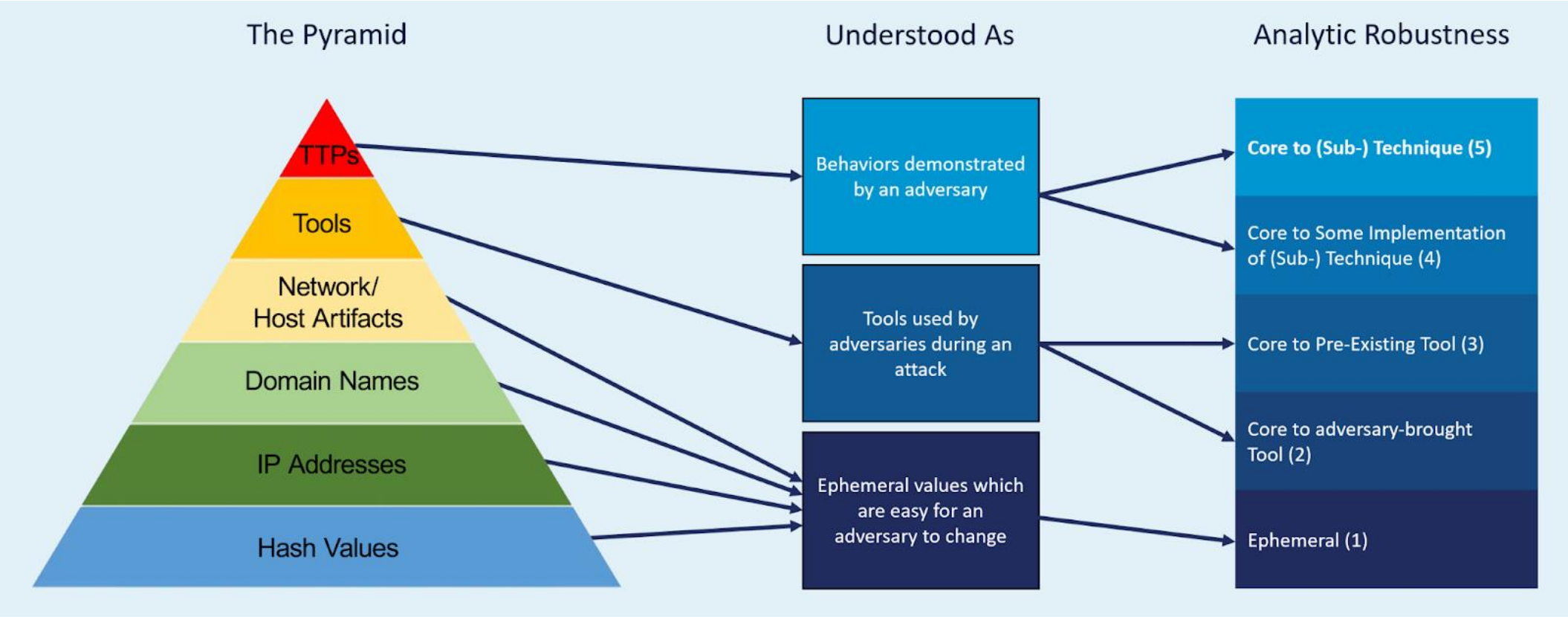
Benefits of the Pyramid

- **Prioritization:** Helps prioritize cybersecurity defenses by categorizing indicators based on their difficulty to change for adversaries. This allows organizations to focus resources on addressing high-impact threats first.
- **Understanding Adversaries:** Provides insights into the tactics, techniques, and procedures (TTPs) of adversaries by categorizing indicators based on their visibility and persistence. This understanding enables organizations to better anticipate and defend against future attacks.
- **Simplicity:** The Pyramid of Pain is relatively simple to understand, making it accessible to a wide range of users, from beginners to experts.
- **Structured Approach:** It offers a structured framework for organizing threat intelligence, facilitating more effective communication and collaboration within cybersecurity teams and across organizations.
- **Awareness:** Raises awareness about the importance of collecting and analyzing different types of indicators, encouraging organizations to invest in threat intelligence capabilities.

Limitations of the Pyramid

- **Limited Robustness Focus:** The original model lacked emphasis on the robustness and resilience of indicators, leading to operational challenges for security teams.
- **Operational Issues:** Security teams often struggled with transient and brittle indicators, resulting in a constant pursuit of adversaries and a high volume of false positives.
- **Predictive Limitations:** While the Pyramid of Pain helps understand past and current threats, its predictive value in anticipating future attacks may be limited due to evolving adversary tactics.
- **Complexity of Implementation:** Integrating the Pyramid of Pain into existing cybersecurity processes and tools can be challenging for some organizations.
- **Not Comprehensive:** While valuable, the Pyramid of Pain is just one framework among many in the cybersecurity field and may not address all aspects of cybersecurity, such as vulnerabilities and misconfigurations.

MITRE Engenuity's Summiting the Pyramid



https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/summiting-the-pyramid/

References

- Enterprise Detection & Response
- What Is Pyramid of Pain?
- Mitre ATT&CK
- SUMMITING THE PYRAMID
- CHATGPT