**SOC Level 1 Learning Path Report**

**CyberDefence Frameworks: Pyramid of Pain**

**Introduction**

The journey through the CyberDefence Frameworks module continued with the "Pyramid of Pain" path on TryHackMe. This path focuses on understanding different indicators of compromise (IOCs) and their impact on adversaries. The Pyramid of Pain is a model that helps cybersecurity professionals understand the difficulty of detecting and responding to various types of IOCs. This report covers the first four tasks completed in this path.

Learning Objectives

The primary objectives of the Pyramid of Pain path included:

- Understanding the Pyramid of Pain model and its significance in cybersecurity.

- Learning about different types of IOCs and their level of difficulty for adversaries to change.

- Gaining practical knowledge on how to detect and respond to various IOCs.

Paths Completed

Pyramid of Pain (Tasks 1-4)

Detailed Analysis of Each Task

Task 1: Introduction.

Description:

The introduction provided an overview of the Pyramid of Pain model, developed by David J. Bianco. The model categorizes different types of IOCs based on the level of difficulty they pose to adversaries when detected and mitigated by defenders.

Key Learnings:

- The Pyramid of Pain consists of six levels, from easiest to hardest for adversaries to change: Hash Values, IP Addresses, Domain Names, Network/Host Artifacts, Tools, and Tactics, Techniques, and Procedures (TTPs).

- Understanding the Pyramid of Pain helps defenders prioritize their detection and mitigation efforts to cause maximum disruption to adversaries.

Tools and Techniques:

- Familiarity with the Pyramid of Pain model.

- Basic understanding of different types of IOCs and their implications.

Challenges and Solutions:

- Challenge: Grasping the concept and practical application of the Pyramid of Pain.

- Solution: Reviewed case studies and practical examples to better understand the model's application in real-world scenarios.

Practical Applications:

- Using the Pyramid of Pain to prioritize detection and response efforts.

- Identifying which IOCs to focus on to maximize impact on adversaries.

Task 2: Hash Values (Trivial)

Description:

This task focused on hash values as an IOC. Hash values are cryptographic representations of data, often used to identify malicious files.

Key Learnings:

- Hash values are unique identifiers for files, making them a useful IOC for detecting malware.

- Hash values are easy for adversaries to change, hence categorized as "trivial" on the Pyramid of Pain.

Tools and Techniques:

- Tools like MD5, SHA-1, and SHA-256 for generating and verifying hash values.

- Techniques for comparing hash values against known malware databases.

Challenges and Solutions:

- Challenge: Understanding how hash values can be effectively used in malware detection.

- Solution: Conducted practical exercises on generating and comparing hash values of different files.

Practical Applications:

- Scanning files in an environment to detect known malware using hash values.

- Cross-referencing hash values with threat intelligence databases.

Task 3: IP Addresses (Easy)

Description:

This task covered IP addresses as an IOC. IP addresses can be used to identify the source or destination of network traffic, including malicious activity.

Key Learnings:

- IP addresses can be blocked or monitored to detect and prevent malicious activities.

- While IP addresses are relatively easy for adversaries to change, they still provide valuable information for initial detection.

Tools and Techniques:

- Tools like WHOIS, traceroute, and IP reputation services.

- Techniques for monitoring and blocking suspicious IP addresses.

Challenges and Solutions:

- Challenge: Managing and correlating large volumes of IP address data.

- Solution: Utilized SIEM tools to automate the monitoring and correlation of IP addresses.

Practical Applications:

- Monitoring network traffic for connections to known malicious IP addresses.

- Blocking IP addresses associated with malicious activities to prevent further attacks.

Task 4: Domain Names (Simple)

Description:

This task focused on domain names as an IOC. Domain names can be used to identify malicious websites and command-and-control (C2) servers.

Key Learnings:

- Domain names are often used in phishing attacks and C2 communications.

- Detecting and blocking malicious domain names can disrupt adversaries' operations.

Tools and Techniques:

- Tools like DNS query logs, passive DNS databases, and domain reputation services.

- Techniques for monitoring and blocking suspicious domain names.

Challenges and Solutions:

- Challenge: Keeping up with the rapid creation and usage of new malicious domains.

- Solution: Implemented threat intelligence feeds to stay updated with the latest malicious domains.

Practical Applications:

- Monitoring DNS traffic for requests to known malicious domains.

- Using threat intelligence to block access to domains associated with phishing and malware.

Overall Reflections

The completion of the first four tasks in the Pyramid of Pain path provided a deeper understanding of different types of IOCs and their impact on adversaries. This knowledge is crucial for effective threat detection and response. The practical exercises reinforced the theoretical concepts, making it easier to apply them in real-world scenarios.

Areas for Further Improvement and Next Steps

- Continue Learning:

- Complete the remaining tasks in the Pyramid of Pain path to gain a comprehensive understanding of all IOC types.

- Hands-on Practice:

- Engage in more practical labs and simulations to enhance skills in detecting and responding to IOCs.

- Advanced Topics:

- Explore advanced threat detection techniques and tools to improve detection capabilities.

- Resources:

- TryHackMe Labs and Exercises

- Cybersecurity Blogs and Threat Intelligence Reports

This report outlines the completion of the first four tasks in the Pyramid of Pain path within the CyberDefence Frameworks module. It highlights the key learnings, challenges, and practical applications of each task, providing a valuable resource for further learning and professional development in cybersecurity.