**SOC Level 1 Learning Path Report**

**CyberDefence Frameworks: Junior Security Analyst Intro**

**Introduction**

The journey to becoming a Security Operations Centre (SOC) Level 1 analyst began with the CyberDefence Frameworks module on TryHackMe. This comprehensive learning path is designed to equip aspiring cybersecurity professionals with the foundational skills and knowledge required for a career as a Junior Security Analyst. The first path in this module, "Junior Security Analyst Intro," provided a detailed introduction to the role, the environment of a SOC, and the daily responsibilities of a Junior Security Analyst.

**Learning Objectives**

The primary objectives of the Junior Security Analyst Intro path included:

- Understanding the role and career prospects of a Junior Security Analyst.

- Familiarizing with the structure and functions of a Security Operations Center (SOC).

- Gaining insights into the daily activities and responsibilities of a Junior Security Analyst.

Paths Completed

Junior Security Analyst Intro

Detailed Analysis of Each Path

Path: Junior Security Analyst Intro

**Task 1: A Career as a Junior Security Analyst**

Description:

This task provided an overview of the career path of a Junior Security Analyst, outlining the skills required, potential career progression, and the importance of this role in cybersecurity.

Key Learnings:

- The role of a Junior Security Analyst is crucial for monitoring and responding to security incidents.

- Important skills include knowledge of cybersecurity principles, familiarity with security tools, and strong analytical abilities.

- Career progression can lead to roles such as Senior Security Analyst, SOC Manager, or specialized positions in threat intelligence or incident response.

Tools and Techniques:

- Basic understanding of SIEM (Security Information and Event Management) systems.

- Introduction to common cybersecurity frameworks and standards.

Challenges and Solutions:

- Challenge: Understanding the diverse skill set required.

- Solution: Supplemented learning with online resources and beginner-friendly courses in key areas like networking and security fundamentals.

Practical Applications:

- Monitoring security alerts and performing initial triage.

- Using SIEM tools to analyse logs and detect potential threats.

- Documenting and escalating incidents for further investigation.

**Task 2: Security Operations Centre (SOC)**

Description:

This task focused on the structure and function of a SOC, highlighting the roles within a SOC and how they collaborate to protect an organization’s assets.

Key Learnings:

- A SOC is a centralized unit that deals with security issues on an organizational and technical level.

- Key roles include Junior Security Analyst, Senior Security Analyst, SOC Manager, and Threat Hunter.

- SOCs operate 24/7 to ensure continuous monitoring and rapid response to security incidents.

Tools and Techniques:

- Introduction to SOC tools such as IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems).

- Understanding of ticketing systems used for tracking and managing incidents.

Challenges and Solutions:

- Challenge: Grasping the complexity of SOC operations and the interaction between different roles.

- Solution: Engaged in practical labs and simulations to gain hands-on experience.

Practical Applications:

- Coordinating with different roles within the SOC for effective incident management.

- Utilizing IDS/IPS to monitor and protect network traffic.

- Implementing and following incident response procedures.

Task 3: A Day in the Life of a Junior (Associate) Security Analyst

Description:

This task provided a realistic view of the daily activities and responsibilities of a Junior Security Analyst, including common challenges and workflows.

Key Learnings:

- Daily activities include monitoring security alerts, analysing suspicious activities, and responding to incidents.

- Importance of maintaining detailed documentation and incident reports.

- Continuous learning and staying updated with the latest threats and vulnerabilities.

Tools and Techniques:

- Regular use of SIEM for monitoring and analysis.

- Incident response playbooks and standard operating procedures (SOPs).

- Communication tools for coordinating with team members.

Challenges and Solutions:

- Challenge: Managing the volume of alerts and distinguishing between false positives and genuine threats.

- Solution: Developed a systematic approach to triage and prioritize alerts, and learned to use automation tools to streamline processes.

Practical Applications:

- Conducting thorough investigations of security alerts to identify potential breaches.

- Communicating findings and coordinating with senior analysts for deeper analysis.

- Keeping up-to-date with threat intelligence to anticipate and mitigate new threats.

**Overall Reflections**

Completing the Junior Security Analyst Intro path provided a solid foundation in understanding the role of a Junior Security Analyst within a SOC. The tasks highlighted the importance of continuous monitoring, effective incident management, and the need for collaboration within a SOC. The practical insights gained through this path have been invaluable in preparing for real-world applications and further learning in cybersecurity.

Areas for Further Improvement and Next Steps

- Deeper Technical Knowledge:

- Focus on advanced topics in threat hunting, malware analysis, and forensic investigations.

- Hands-on Practice:

- Engage in more practical labs and simulations to gain hands-on experience with SOC tools and incident response procedures.

- Certifications:

- Aim to achieve relevant certifications such as CompTIA Security+, CEH (Certified Ethical Hacker) and more specialized SOC certifications.

- Resources:

- TryHackMe Labs and Exercises

- Cybersecurity Blogs and Threat Intelligence Reports

This report outlines the completion of the Junior Security Analyst Intro path within the CyberDefence Frameworks module. It serves as both a reflection of the learning journey and a resource for others interested in pursuing a career as a Junior Security Analyst. The next steps involve deepening technical knowledge and gaining further hands-on experience to advance in this field.