Junior Security Analyst Intro - TryHackMe Lab Report

Name: Ashish Sawant

Email: aaashi0301@gmail.com

GitHub: https://github.com/aaashi03

TryHackMe Profile: https://tryhackme.com/p/ashish0301

Date: April 13, 2025

# 🧠 Lab Overview

The 'Junior Security Analyst Intro' room on TryHackMe introduces core responsibilities, tools, and workflows relevant to a Level 1 SOC Analyst. It is designed to help newcomers understand how to navigate a SOC environment, recognize threat indicators, and use basic tools for monitoring and triage.

# 🎯 Objective

To gain a practical understanding of the roles, responsibilities, and key skills required as a Junior Security Analyst working in a Security Operations Center (SOC).

# 📚 Key Topics Covered

- SOC roles and responsibilities

- Cyber Kill Chain overview

- Common tools used in SOCs (SIEM, ticketing systems, threat intelligence)

- Log sources: Endpoint, Network, and Server

- Incident response basics

- How to triage alerts

# 🔐 Relevance to SOC Analyst Role

- Builds a strong foundation for handling real alerts in a SOC.

- Teaches how to think critically and use available tools to validate and escalate threats.

- Encourages familiarity with alert workflows and documentation.

# 🛠️ Hands-On Tasks Completed

- Learned how SOC teams operate in shifts and handle ticketing queues.

- Practiced reviewing alerts and identifying indicators of compromise (IOCs).

- Understood escalation paths and the importance of documentation.

- Reviewed logs to differentiate between false positives and actionable incidents.

# ✅ Conclusion

This lab offered a real-world perspective into the SOC environment, preparing me to handle Level 1 SOC tasks such as log review, incident triage, and alert escalation.