Learning Report

Name: Aisha Apanpa

Platforms: TryHackMe & LetsDefend

Introduction

This report documents the successful completion of TryHackMe and LetsDefend labs focused on Security Operations Center (SOC) fundamentals.

Labs Completed

1. Junior Security Analyst – TryHackMe

• Security Analyst Journey

• SOC team and their daily duties

• The role of a Security Analyst

2. SOC Fundamentals

A Security Operations Center (SOC) is operated by a specialized security team that monitors an organization's network, identifies suspicious activities, and prevents potential damage. The main focus of a SOC is to maintain effective detection and response.

The three pillars of SOC include:

• People: SOC team

• Process: The 5Ws (What, When, Where, Who, and Why)

• Technology: Security solutions

3. SOC Role in the Blue Team

Understanding the security hierarchy in cybersecurity is important. Examples of security teams include:

• Red Team: Offensive security experts, penetration testers, or ethical hackers who identify security weaknesses

• GRC Team: Specialists responsible for policies, risk management, and regulatory compliance

• Blue Team: Defensive security professionals such as SOC analysts, security engineers, and incident responders

The Blue Team continuously monitors for attacks and responds to incidents promptly. Departments within the Blue Team include:

- SOC Team: The central hub of an organization’s cybersecurity and first line of defense

- Cyber Incident Response Team: Often referred to as firefighters, handling urgent security incidents and breaches

- Specialized Defensive Roles

4. SOC Analyst Level 1 – LetsDefend

This lab simulates a real SOC environment where alerts are generated, analyzed, escalated, and documented. It closely reflects real-world SOC operations.

Conclusion

Completing the TryHackMe Junior Security Analyst, SOC Fundamentals, SOC Role in Blue Team, and LetsDefend SOC Level 1 labs has significantly strengthened my foundation in cybersecurity and SOC operations. These experiences have prepared me for further learning and advanced SOC training.