Cybersecurity Portfolio Project: TryHackMe Hands-On Experience

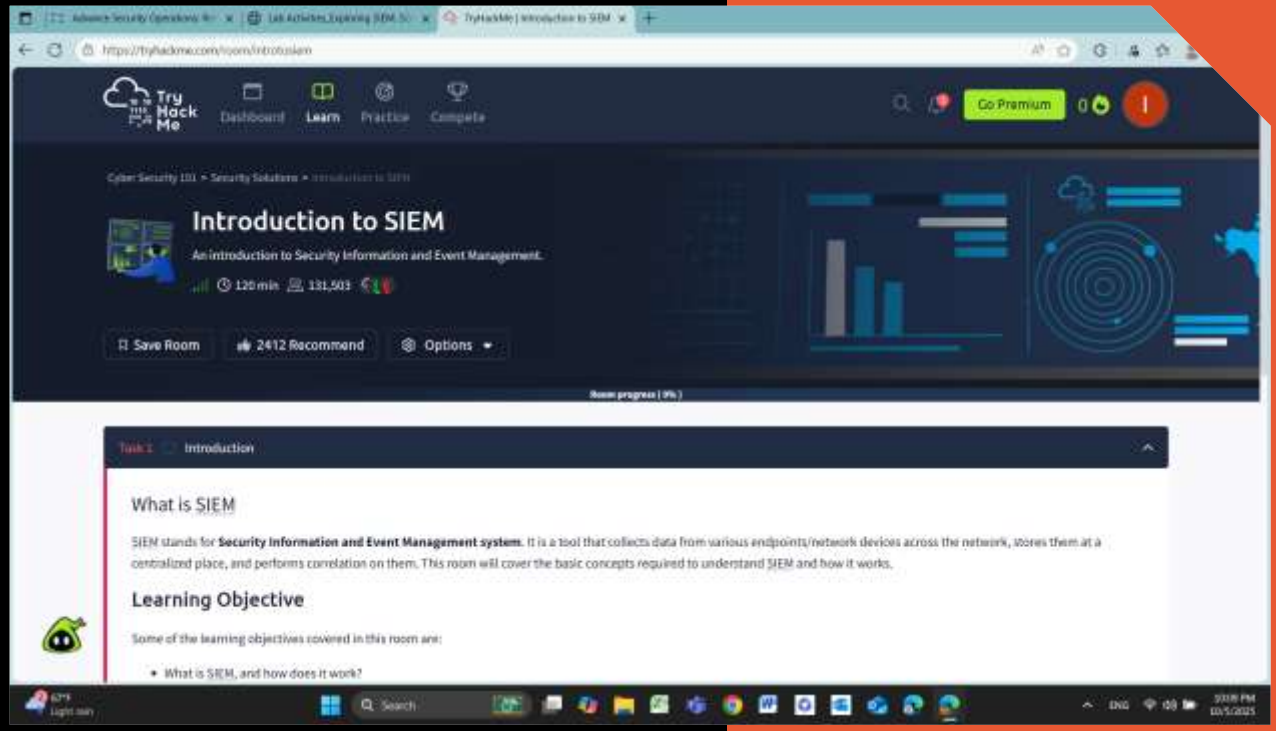
ITECH1502 – Cybersecurity Fundamentals

Name: Intekub Hossen Khalid
Student ID: 30481057

Date: 17 October 2025

Project Overview

- This project demonstrates my practical understanding of cybersecurity concepts through a hands-on TryHackMe challenge.
- It showcases my ability to identify vulnerabilities, use scanning tools, and apply cybersecurity frameworks.
- The project helped me connect theory (like NIST CSF and incident response) to real-world practice.

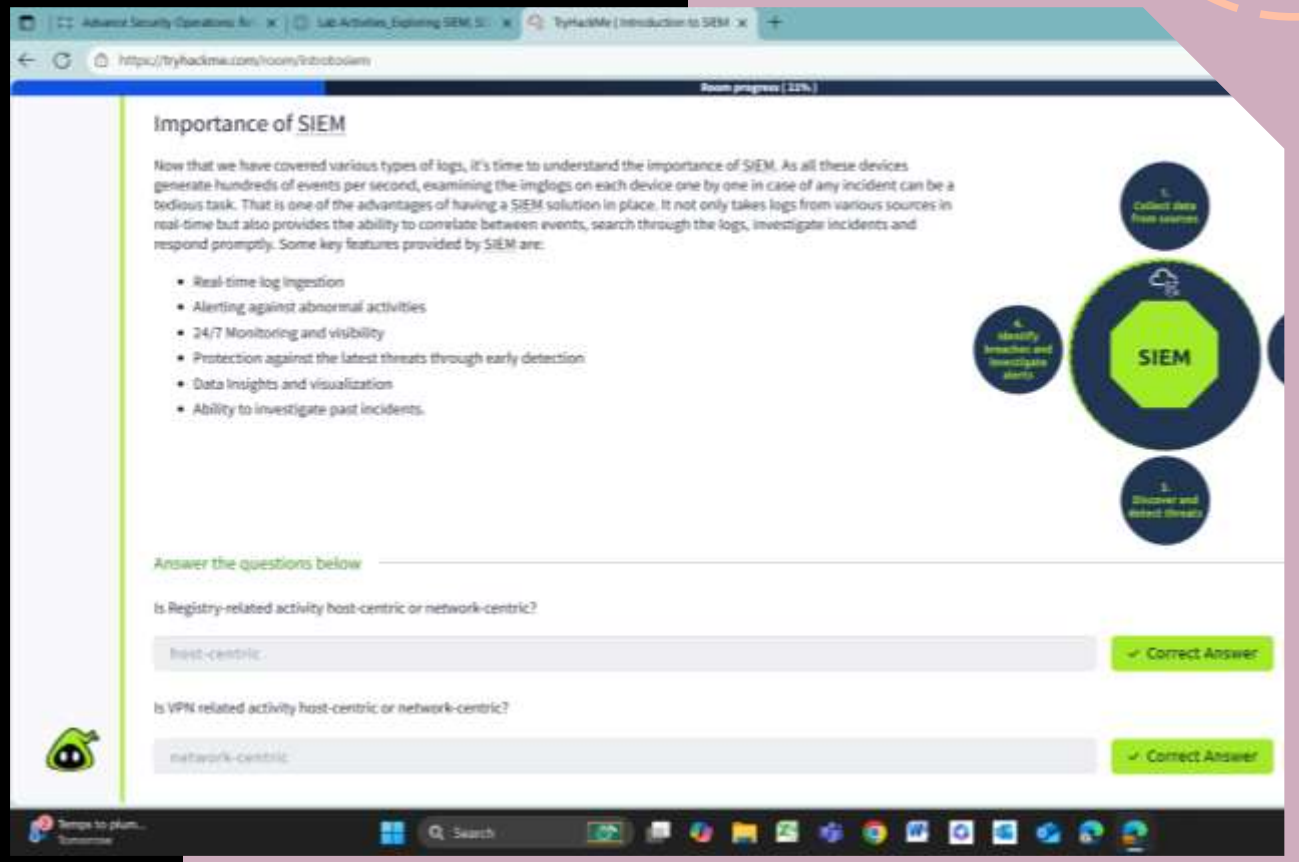


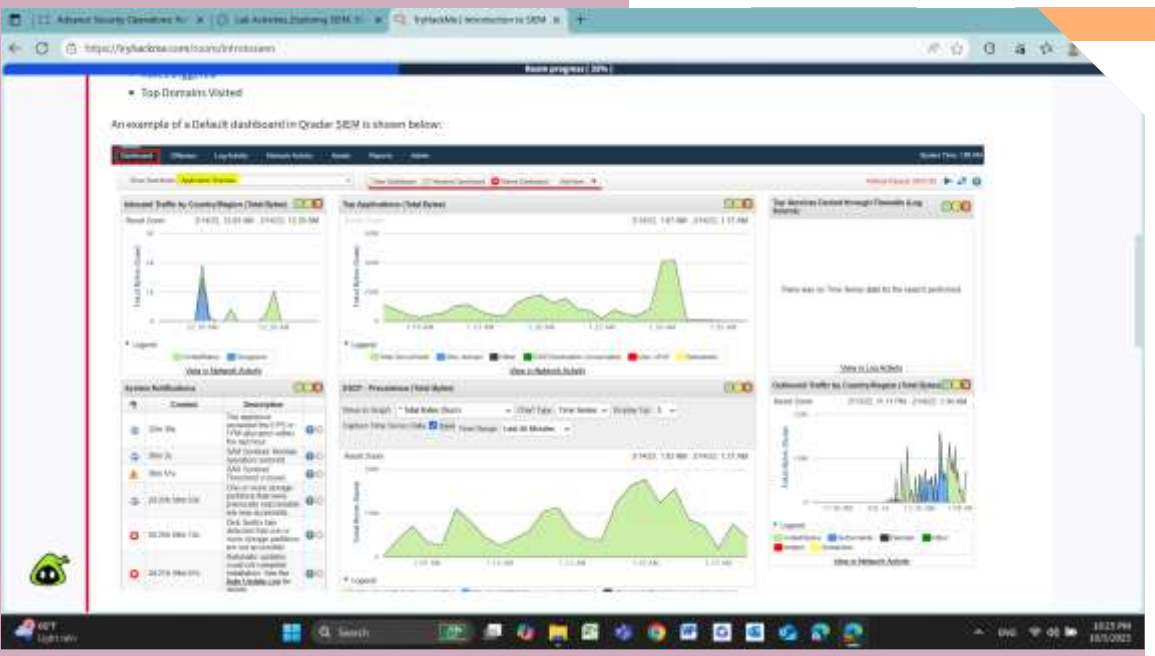
Platform Introduction & Setup

- Platform used: TryHackMe (https://tryhackme.com)
- Registered with FedUni email for verification.
- Room: *Introduction to SIEM* (Free room under Cyber Security 101).
- Estimated time: 120 minutes | Progress 100%.
- Tools: browser-based SIEM simulation + log analysis interface.

Challenge Description & Learning Objective

- Objective: Understand SIEM concepts and log correlation.
- Tasks included:
- Identifying network-centric vs host-centric events.
- Analysing real-time logs and alerts.
- Triggering alerts from suspicious processes (e.g., cudominer.exe).
- Outcome: Improved understanding of incident response and alert management.



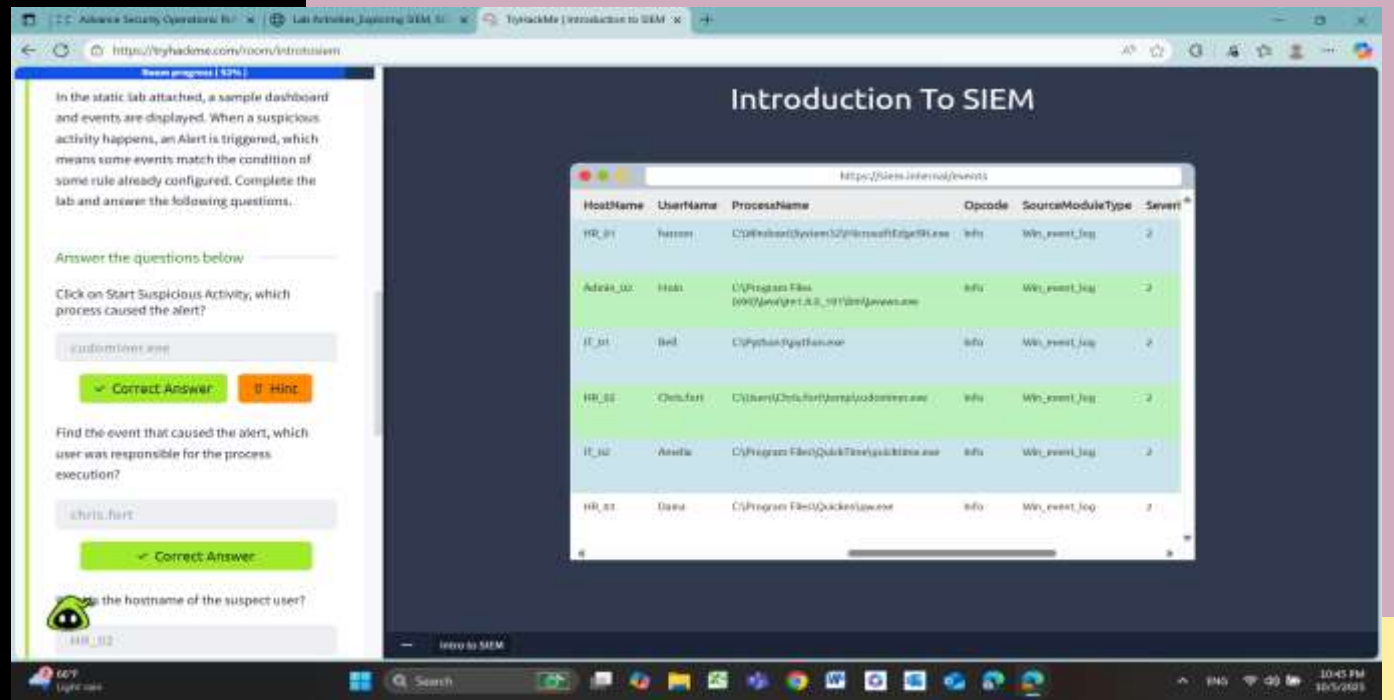


Methodology

- Opened Introduction to SIEM room on TryHackMe.
- Read overview and completed Task 1–3 (Intro, Visibility, Importance).
- Analysed default dashboard to understand log correlation.
- Accessed Lab Work (Tasks 5–6) to view real alerts and logs.
- Answered investigation questions (e.g., malicious process, user, host).
- Verified completion and captured flag.

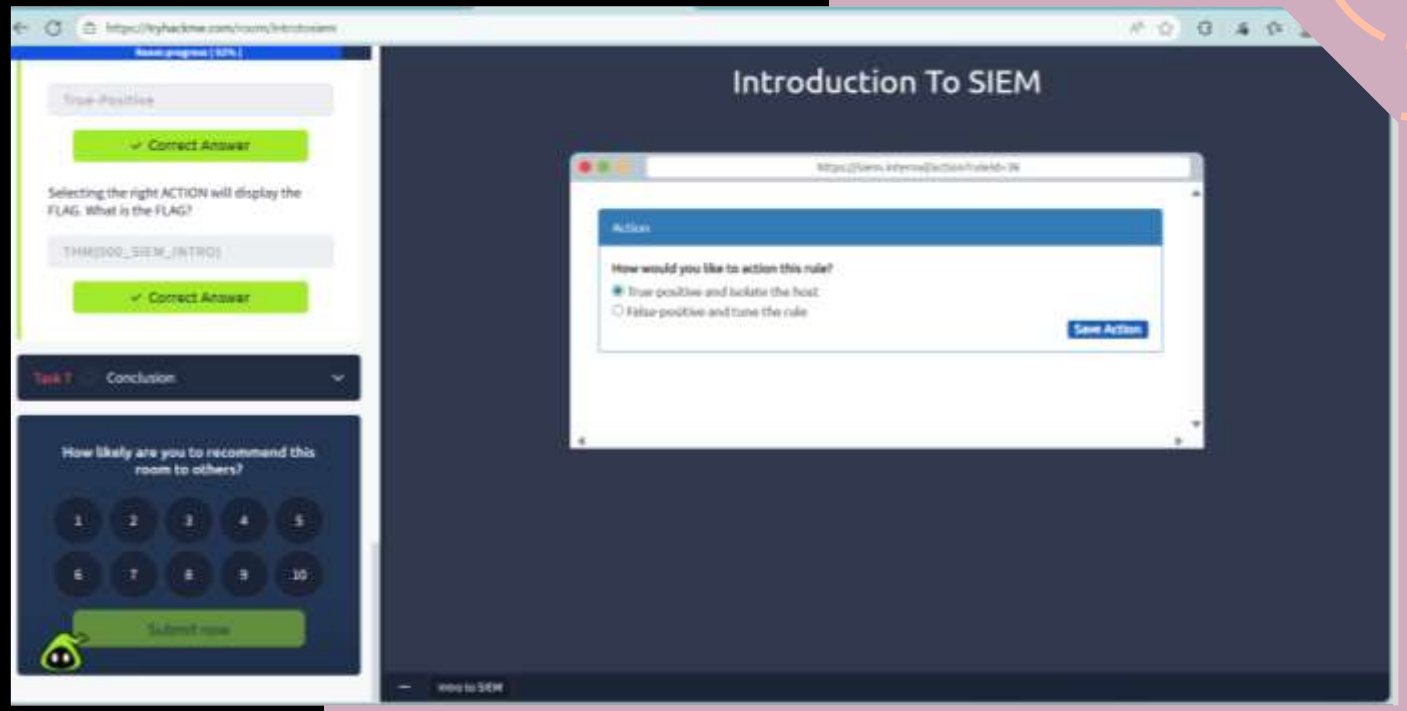
Results & Evidence

- Detected malicious process **cudominer.exe** on host HR_02.
- Responsible user: **Chris.fort**.
- Event type: Windows Event Logs (AUDIT_SUCCESS).
- Severity: 2 – Info (alert generated).
- Final flag obtained: **THM{000_SIEM_INTRO}**.



Reflection & Key Insights

- **Learnings:** Event logging, correlation, threat detection, alert classification.
- **Growth:** Improved problem-solving and analytical skills using realistic security data.
- **Challenges:** Understanding event relationships and decoding log fields.
- **Next time:** Would explore advanced rooms for incident response and forensics.



Conclusion & Next Steps

- Completing this lab enhanced my understanding of SIEM tools and alert response.
- Built hands-on experience identifying malicious activities and isolating hosts.
- Plan to continue learning incident response and threat hunting rooms on TryHackMe.