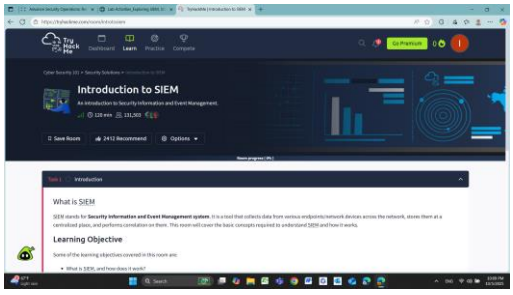
Cybersecurity Portfolio Project: TryHackMe – Introduction to SIEM

ITECH1502 Cybersecurity Fundamentals

Student: Intekub Hossen Khalid
Student ID: 30481057
GitHub Protfolio: ikhalid1057/Cybersecurity-Portfolio: Hands-on labs and projects for ITECH1502 Cybersecurity Fundamentals.

Summary-

The following is my Cybersecurity Portfolio Project from a hands-on lab entitled "Introduction to SIEM" on TryHackMe, an online platform for cybersecurity training. The aim was to gain hands-on experience in Security Information and Event Management (SIEM) through the handling of simulated network traffic, detection of suspicious activity, and alert management. I conducted step-by-step exercises including log correlation, alert investigation, and host analysis. In this exercise, I identified a malicious process (cudominer.exe) on host HR_02 being executed by the user Chris.fort, which was confirmed by SIEM dashboards. The project applied NIST Cybersecurity Framework (CSF) concepts to real-life incident response. This exercise improved my technical, analytical, and ethical decision-making capabilities in cybersecurity operations to be placed at entry-level SOC or analyst positions.

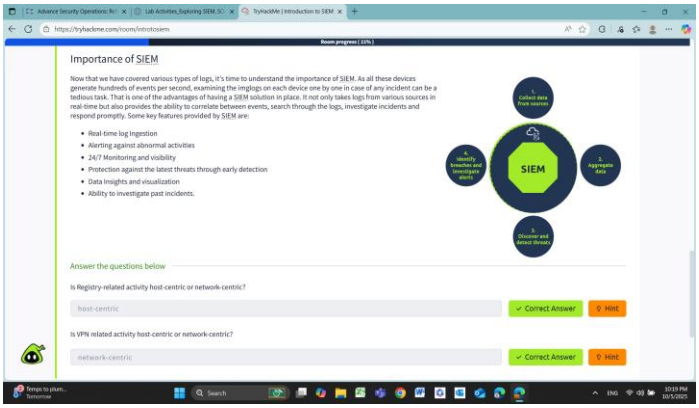


Introduction-

TryHackMe (https://tryhackme.com) is a browser-based learning platform with guided cybersecurity labs. I chose the Introduction to SIEM lab for this project, which instructs log monitoring, event correlation, and alert analysis. SIEM systems are invaluable to today's organizations as they

centralize security data from various hosts and identify irregularities using pattern detection. This room maps to ITECH1502 learning outcomes (S1, S2, A1, A2), i.e., fundamental security routines, tool use, and applying cybersecurity concepts to real situations. It also covers NIST CSF's "Detect" and "Respond" capabilities—two foundational columns of cybersecurity defense.

Problem / Challenge-



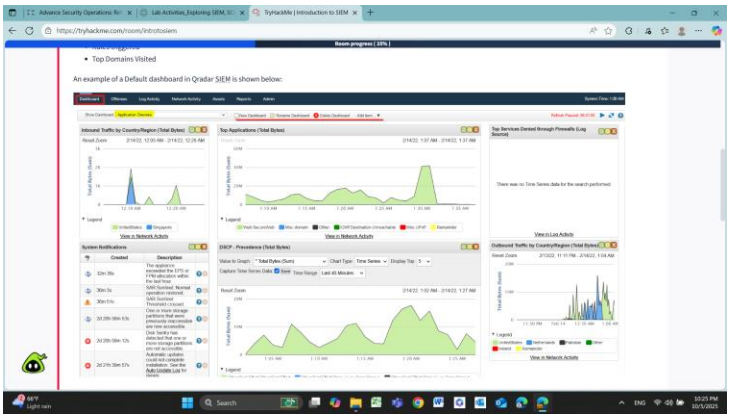
The test enterprise network had a few hosts and a SIEM dashboard with alerts based on logs. The goal was to find the particular event that caused an alert, verify if it was real or malicious, and take appropriate action. While researching, an unfamiliar process, cudominer.exe, was found running on host HR_02. By investigating correlated Windows Event Logs (AUDIT_SUCCESS) and system behavior, I verified that the process was crypto-mining malware. This exercise challenged my skills in differentiating between host-centric and network-centric incidents, verification of incidents through evidence, and adherence to ethical standards for reporting.

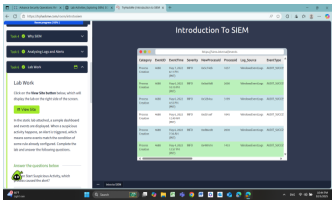
Project Goals and Objectives-

Objectives for the activity were to:

1. Deploy theoretical SIEM in a real-world scenario.
2. Analyze logs and correlate events to identify threats.
3. Classify false alarms from actual incidents.
4. Enhance incident response and reporting.
5. Put all evidence and reflection into a professional portfolio.

These learning objectives also align with the unit learning outcomes (S1–S2: application of security tools, A1–A2: case analysis and mitigation).

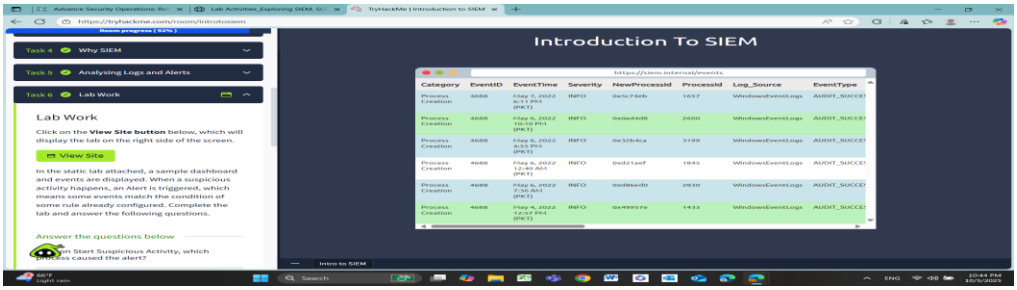




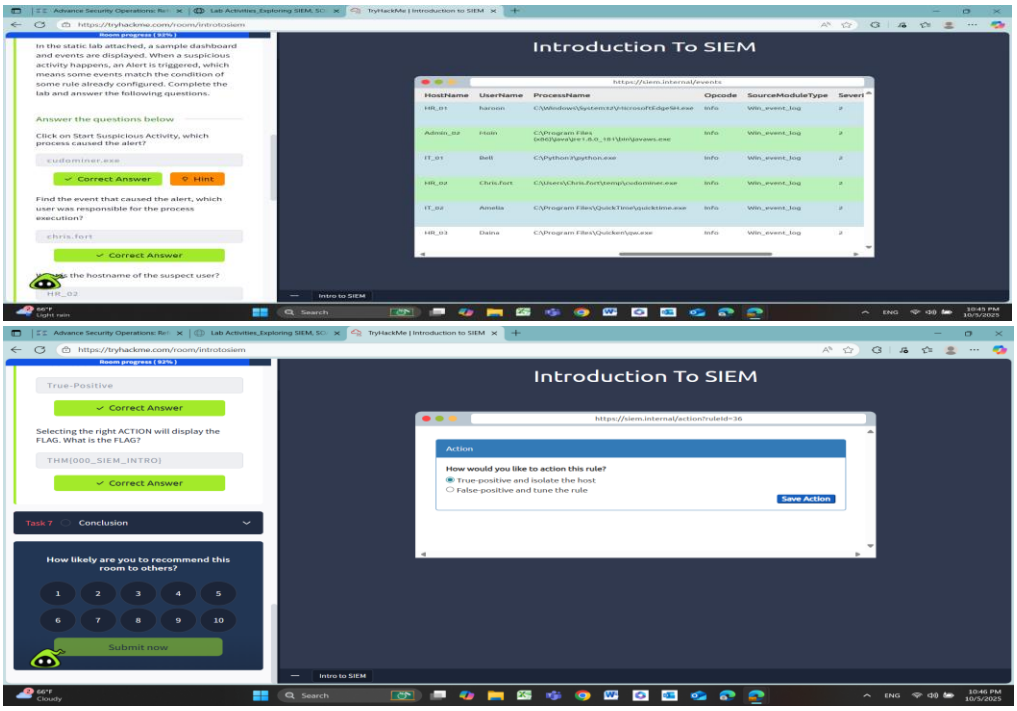
Methodology-

I adopted a rational workflow in the completion of the TryHackMe lab:

1. Accessed the *Introduction to SIEM* room via TryHackMe using my FedUni email.
2. Completed Tasks 1–3: Understanding SIEM concepts, visibility, and importance.
3. Navigated to the **Lab Work** section (Tasks 5–6) to explore real log data.
4. Monitored Windows Event Logs, filtering alerts based on process, host, and user.
5. Identified the malicious **cudominer.exe** process triggered on host HR_02.
6. Recorded findings and completed guided investigation questions within the platform.
7. Submitted responses and captured the final completion flag.



Results and Evidence-



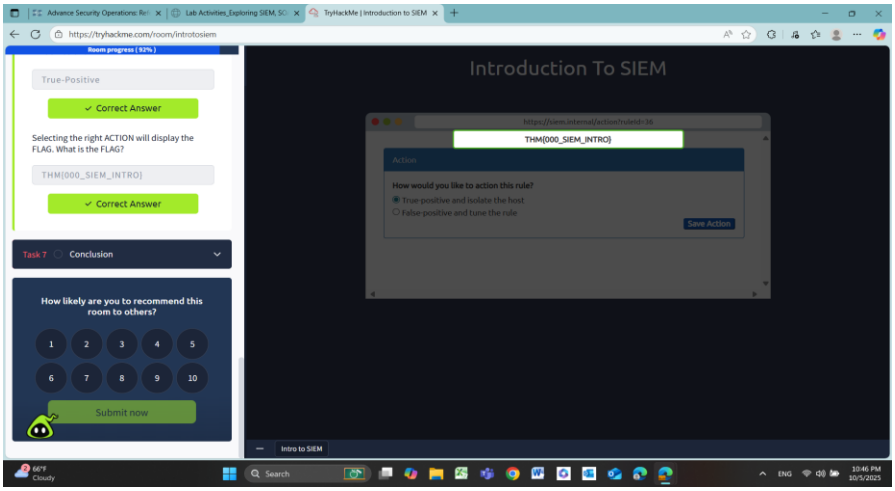
The lab successfully simulated an alert investigation process. Findings included:

Parameter	Observation
Process Name	cudominer.exe
User	Chris.fort
Host	HR_02
Event Type	Windows Event Log (AUDIT_SUCCESS)
Severity	2 – Information
Action	Isolate host, mark alert as true positive
Completion Flag	THM{000_SIEM_INTRO}

Reflection-

This practice better informed me about how SOC analysts detect and act upon threats. I learned how to use log data to discover information about suspicious behavior and distinguish between false positives and true positives. It also shed some light on the importance of adequate documentation and ethical behavior when handling system data. A few areas of challenge were understanding unknown fields within logs and correlating time stamps from multiple sources.

Overcoming these improved my analytical and technical self-assurance. If I repeated the exercise, I would pay closer attention to optimizing detection rules and investigating SIEM capabilities such as correlation searches and anomaly detection.



Conclusion-

This TryHackMe exercise gave a realistic flavor of cyber operations. It merged theoretical ideas from ITECH1502 with practical exercises in SIEM investigation, meeting the course outcomes. I developed technical skills and professional capabilities on how current SOC teams deal with alerts and incidents. This is a valuable part of my cybersecurity portfolio, now hosted on GitHub as evidence of my learning experience. I will continue to contribute to it with further labs that relate to incident response and digital forensics.

GitHub protfolio link: [ikhalid1057/Cybersecurity-Portfolio: Hands-on labs and projects for ITECH1502 Cybersecurity Fundamentals.]