

Cybersecurity Portfolio

Project: TryHackMe Hands-On Experience

ITECH1502 – Cybersecurity Fundamentals

Name: Intekub Hossen Khalid

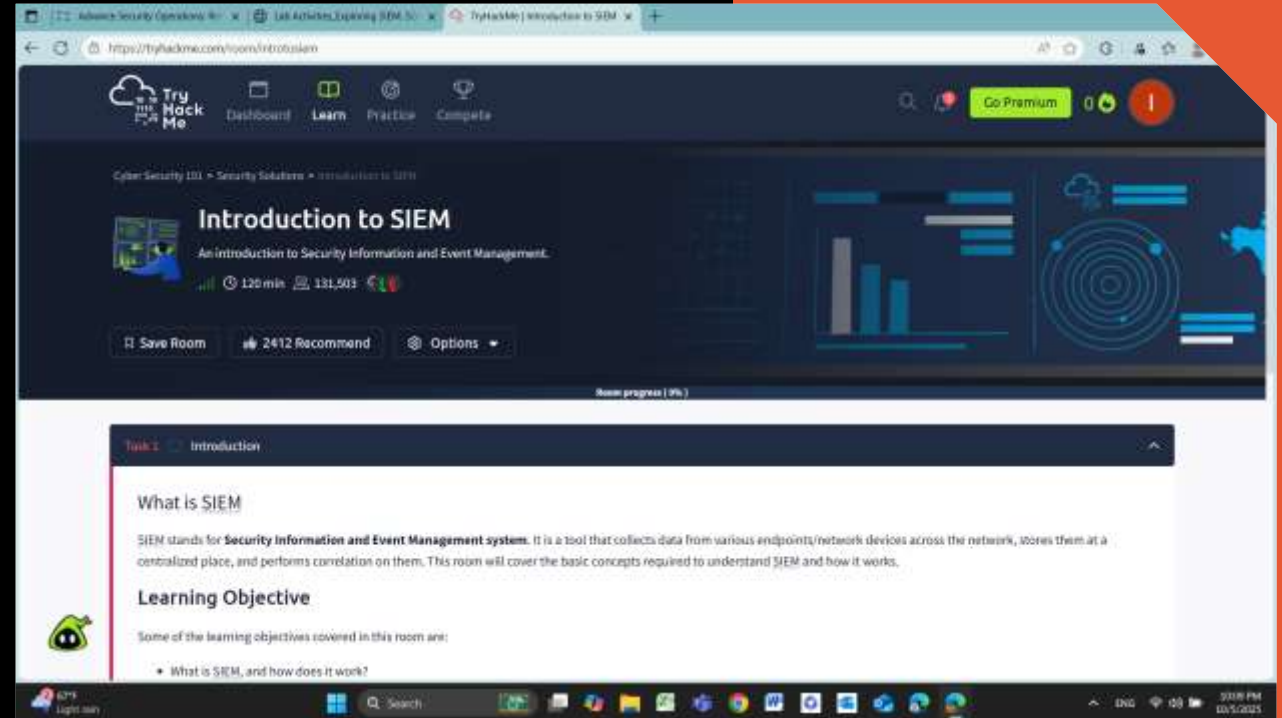
Student ID: 30481057

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.

The screenshot shows a web browser window displaying a TryHackMe room page. The browser's address bar shows the URL <https://tryhackme.com/room/6tztobolm>. The page title is "Importance of SIEM". The main content area contains a paragraph explaining the importance of SIEM, followed by a bulleted list of key features: Real-time log ingestion, Alerting against abnormal activities, 24/7 Monitoring and visibility, Protection against the latest threats through early detection, Data insights and visualization, and Ability to investigate past incidents. To the right of the text is a diagram with a central green circle labeled "SIEM" and four surrounding blue circles labeled 1. Discover and detect threats, 2. Collect data from sensors, 3. Identify breaches and investigate alerts, and 4. (partially visible). Below the text, there is a section titled "Answer the questions below" with two questions: "Is Registry-related activity host-centric or network-centric?" and "Is VPN related activity host-centric or network-centric?". Each question has a text input field and a green "Correct Answer" button. The first question's input field contains "host-centric" and the second's contains "network-centric". A small green robot icon is visible in the bottom left corner of the page. The Windows taskbar is visible at the bottom of the screen.

Room progress (12%)

Importance of SIEM

Now that we have covered various types of logs, it's time to understand the importance of SIEM. As all these devices generate hundreds of events per second, examining the imlogs on each device one by one in case of any incident can be a tedious task. That is one of the advantages of having a SIEM solution in place. It not only takes logs from various sources in real-time but also provides the ability to correlate between events, search through the logs, investigate incidents and respond promptly. Some key features provided by SIEM are:

- Real-time log ingestion
- Alerting against abnormal activities
- 24/7 Monitoring and visibility
- Protection against the latest threats through early detection
- Data insights and visualization
- Ability to investigate past incidents.

Answer the questions below

Is Registry-related activity host-centric or network-centric?

host-centric

Correct Answer

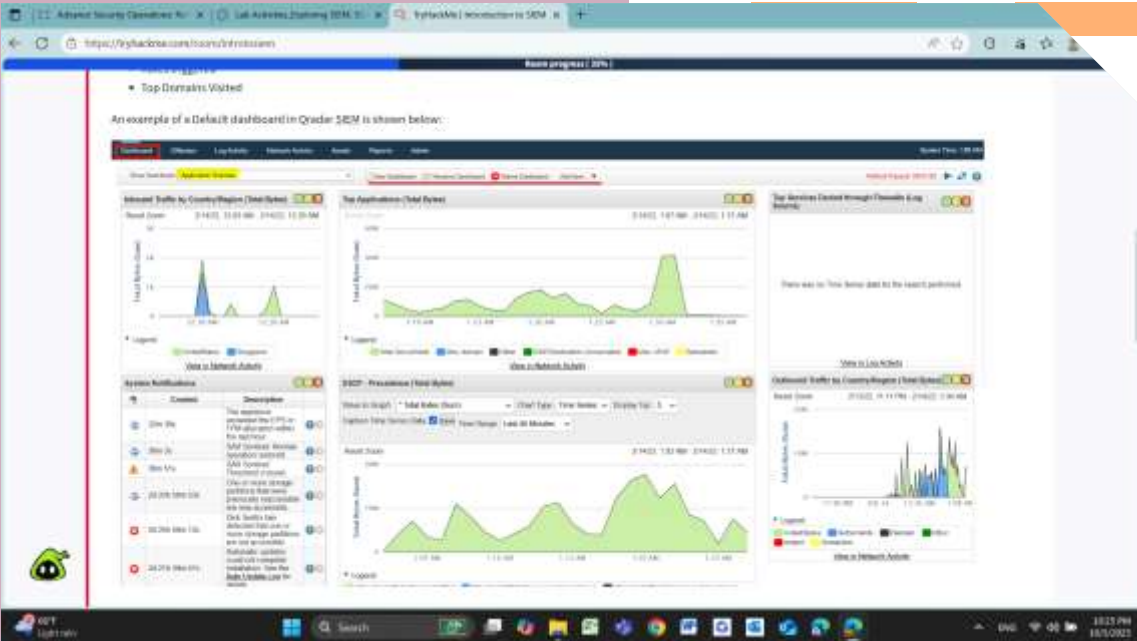
Is VPN related activity host-centric or network-centric?

network-centric

Correct Answer

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.



The screenshot shows the 'Introduction To SIEM' lab interface. On the left, there's a sidebar with 'Task 5: Analysing Logs and Alerts' and 'Task 6: Lab Work'. The main area displays a table of log events. Below the table, there's a section for 'Answer the questions below' with a 'Submit' button and a 'Hint' button. The table has columns: 'HostName', 'UserName', 'ProcessName', 'Opcode', and 'SourceModuleType'.

HostName	UserName	ProcessName	Opcode	SourceModuleType
HT_01	Admin	C:\Windows\System32\cmd.exe	info	Win_event_log
HT_02	Admin	C:\Program Files\Internet Explorer\iexplore.exe	info	Win_event_log
HT_01	Admin	C:\Program Files\Internet Explorer\iexplore.exe	info	Win_event_log
HT_02	Admin	C:\Windows\System32\cmd.exe	info	Win_event_log
HT_01	Admin	C:\Program Files\Internet Explorer\iexplore.exe	info	Win_event_log
HT_02	Admin	C:\Program Files\Internet Explorer\iexplore.exe	info	Win_event_log

Results & Evidence

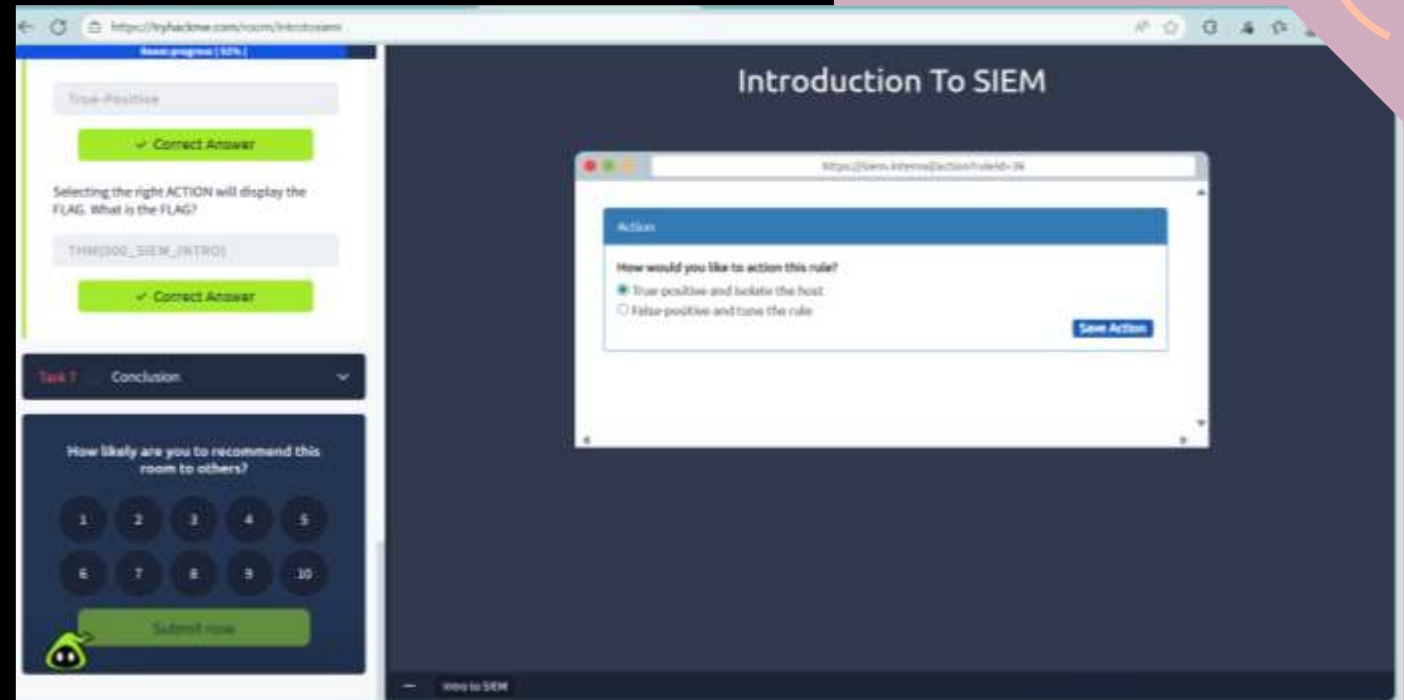
- Detected malicious process **cmdminer.exe** on host **HR_02**.
- Responsible user: **Chris.fort**.
- Event type: Windows Event Logs (**AUDIT_SUCCESS**).
- Severity: 2 – Info (alert generated).
- Final flag obtained: **THM{000_SIEM_INTRO}**.

Category	EventID	EventTime	Severity	NewProcessId	ProcessId	Log_Source	EventType
Process Creation	4688	May 7, 2022 6:11 PM (PCT)	INFO	0x00000000	1637	WindowsEventLog	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 10:10 PM (PCT)	INFO	0x00000000	2680	WindowsEventLog	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 4:55 PM (PCT)	INFO	0x00000000	3188	WindowsEventLog	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 12:40 AM (PCT)	INFO	0x00000000	1845	WindowsEventLog	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 7:36 AM (PCT)	INFO	0x00000000	2838	WindowsEventLog	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 12:37 PM (PCT)	INFO	0x00000000	1633	WindowsEventLog	AUDIT_SUCCESS

HostName	UserName	ProcessName	Opcode	SourceModuleType	Severity
HR_01	hazoom	C:\Windows\System32\MicrosoftEdgeS.exe	info	Win_event_log	2
Admin_00	hazoom	C:\Program Files\Win7\cmd.exe	info	Win_event_log	2
IT_01	hazoom	C:\Program Files\Win7\cmd.exe	info	Win_event_log	2
HR_02	Chris.fort	C:\Users\Chris.fort\AppData\Local\cmd.exe	info	Win_event_log	2
IT_02	hazoom	C:\Program Files\Win7\cmd.exe	info	Win_event_log	2
HR_03	hazoom	C:\Program Files\Win7\cmd.exe	info	Win_event_log	2

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.

