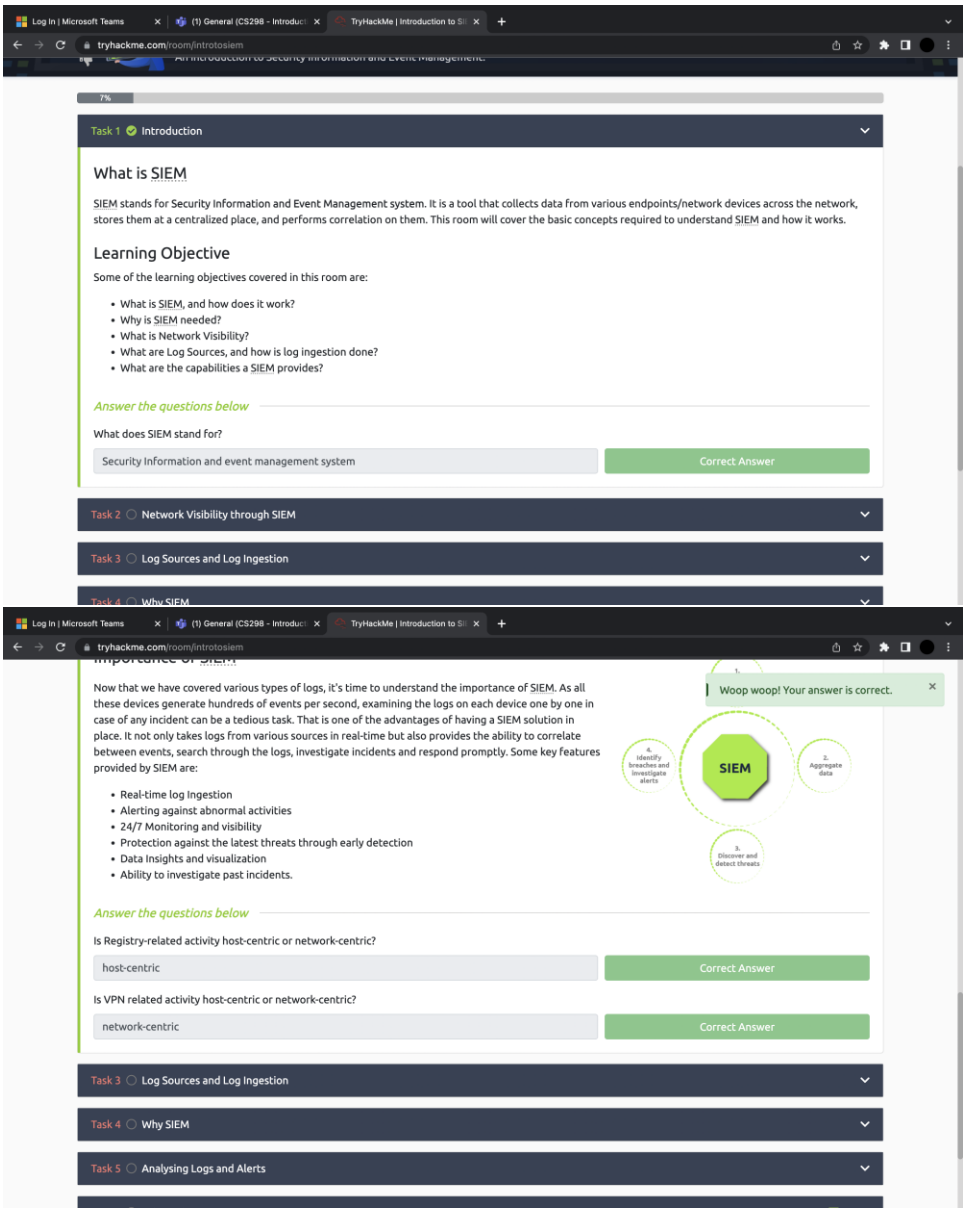
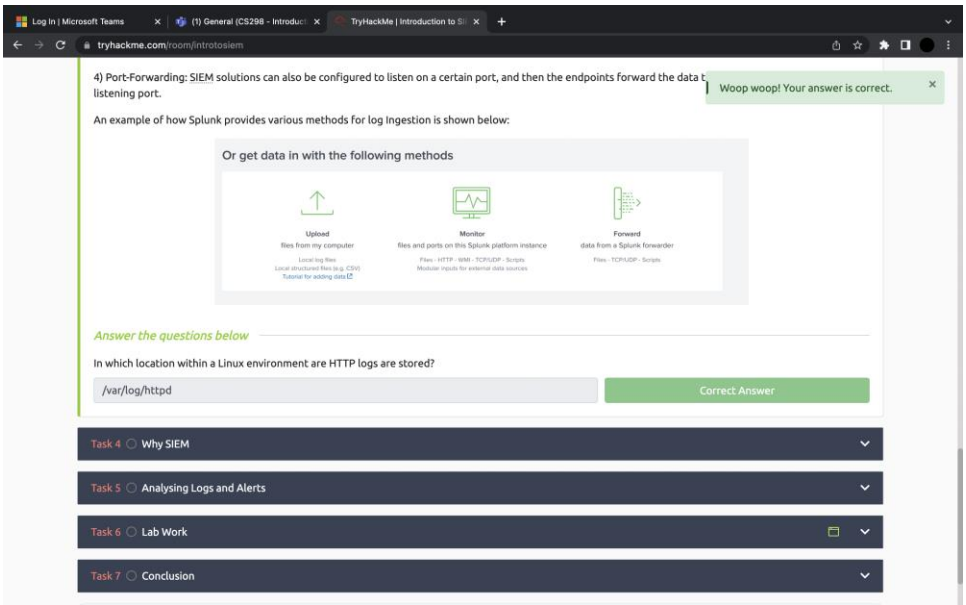
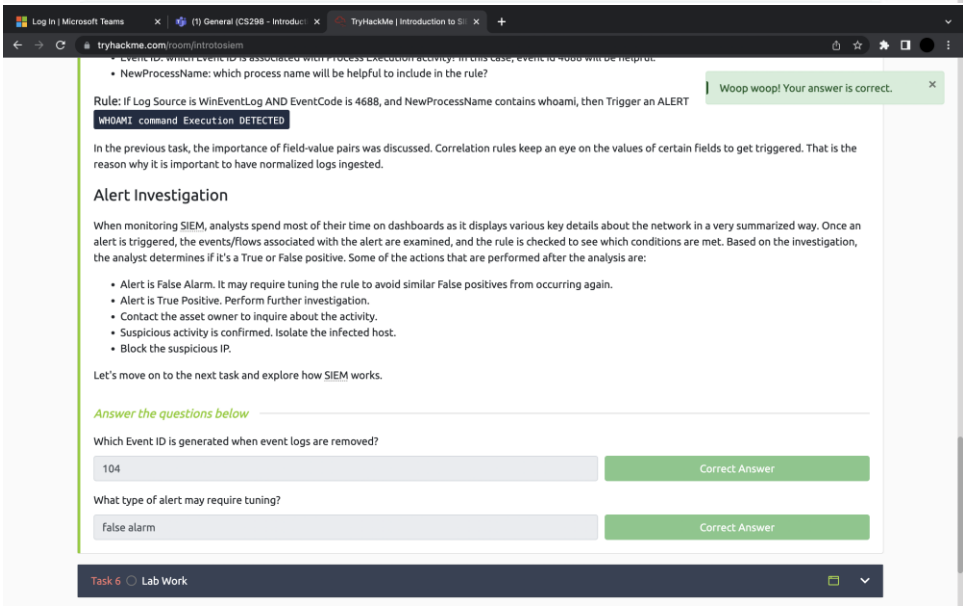
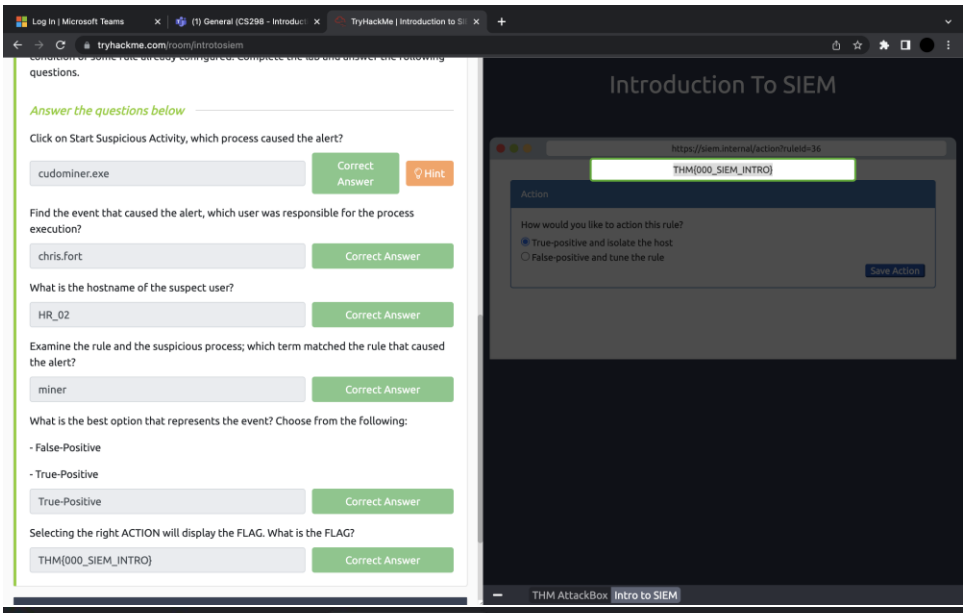
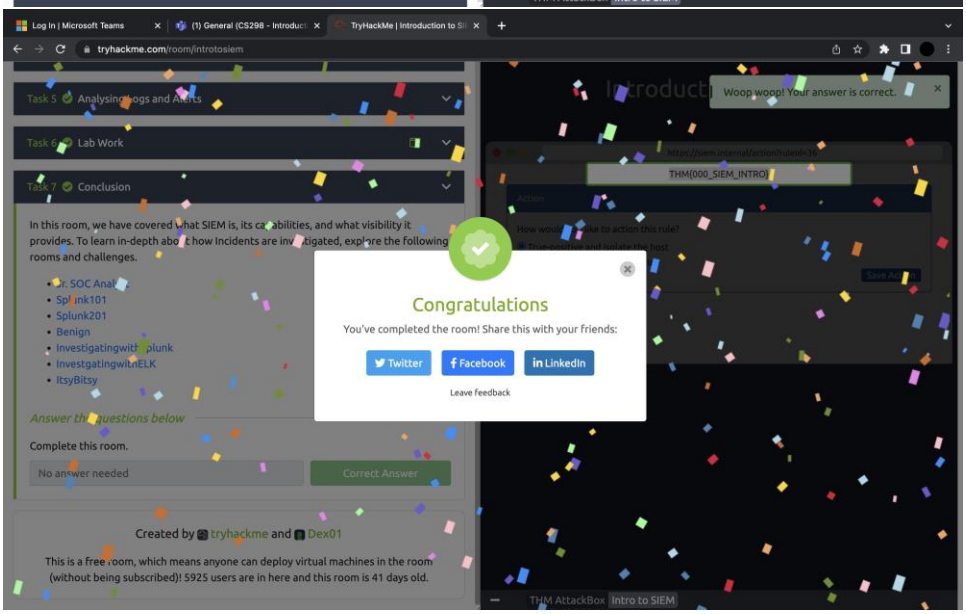

Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Introduction to SI
tryhackme.com/room/introtosiem
7%
Task 1 Introduction
What is SIEM
SIEM stands for Security Information and Event Management system. It is a tool that collects data from various endpoints/network devices across the network, stores them at a centralized place, and performs correlation on them. This room will cover the basic concepts required to understand SIEM and how it works.
Learning Objective
Some of the learning objectives covered in this room are:
What is SIEM, and how does it work?
Why is SIEM needed?
What is Network Visibility?
What are Log Sources, and how is log ingestion done?
What are the capabilities a SIEM provides?
Answer the questions below
What does SIEM stand for?
Security Information and event management system
Correct Answer
Task 2 Network Visibility through SIEM
Task 3 Log Sources and Log Ingestion
Task 4 Why SIEM

Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Introduction to SI
tryhackme.com/room/introtosiem
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 logs 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.
Woop woop! Your answer is correct.
SIEM
4. Identify breaches and investigate alerts
2. Aggregate data
3. Discover and detect threats
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
Task 3 Log Sources and Log Ingestion
Task 4 Why SIEM
Task 5 Analysing Logs and Alerts


Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Introduction to SI
tryhackme.com/room/introtosiem
4) Port-Forwarding: SIEM solutions can also be configured to listen on a certain port, and then the endpoints forward the data t
listening port.
Woop woop! Your answer is correct.
An example of how Splunk provides various methods for log Ingestion is shown below:
Or get data in with the following methods
Upload
files from my computer
Monitor
files and ports on this Splunk platform instance
Forward
data from a Splunk forwarder
Answer the questions below
In which location within a Linux environment are HTTP logs are stored?
/var/log/httpd
Correct Answer
Task 4 Why SIEM
Task 5 Analysing Logs and Alerts
Task 6 Lab Work
Task 7 Conclusion


Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Introduction to SI
tryhackme.com/room/introtosiem
• NewProcessName: which process name will be helpful to include in the rule?
Woop woop! Your answer is correct.
Rule: If Log Source is WinEventLog AND EventCode is 4688, and NewProcessName contains whoami, then Trigger an ALERT
WHOAMI command Execution DETECTED
In the previous task, the importance of field-value pairs was discussed. Correlation rules keep an eye on the values of certain fields to get triggered. That is the reason why it is important to have normalized logs ingested.
Alert Investigation
When monitoring SIEM, analysts spend most of their time on dashboards as it displays various key details about the network in a very summarized way. Once an alert is triggered, the events/flows associated with the alert are examined, and the rule is checked to see which conditions are met. Based on the investigation, the analyst determines if it's a True or False positive. Some of the actions that are performed after the analysis are:
• Alert is False Alarm. It may require tuning the rule to avoid similar False positives from occurring again.
• Alert is True Positive. Perform further investigation.
• Contact the asset owner to inquire about the activity.
• Suspicious activity is confirmed. Isolate the infected host.
• Block the suspicious IP.
Let's move on to the next task and explore how SIEM works.
Answer the questions below
Which Event ID is generated when event logs are removed?
104
Correct Answer
What type of alert may require tuning?
false alarm
Correct Answer
Task 6 Lab Work


Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Introduction to SI
tryhackme.com/room/introtosiem
questions.
Answer the questions below
Click on Start Suspicious Activity, which process caused the alert?
cudominer.exe
Correct Answer
Hint
Find the event that caused the alert, which user was responsible for the process execution?
chris.fort
Correct Answer
What is the hostname of the suspect user?
HR_02
Correct Answer
Examine the rule and the suspicious process; which term matched the rule that caused the alert?
miner
Correct Answer
What is the best option that represents the event? Choose from the following:
- False-Positive
- True-Positive
True-Positive
Correct Answer
Selecting the right ACTION will display the FLAG. What is the FLAG?
THM{000_SIEM_INTRO}
Correct Answer
Introduction To SIEM
https://siem.internal/action?ruleId=36
THM{000_SIEM_INTRO}
Action
How would you like to action this rule?
True-positive and isolate the host
False-positive and tune the rule
Save Action
THM AttackBox
Intro to SIEM


Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Introduction to SI
tryhackme.com/room/introtosiem
Task 5 Analysing Logs and Alerts
Task 6 Lab Work
Task 7 Conclusion
In this room, we have covered what SIEM is, its capabilities, and what visibility it provides. To learn in-depth about how Incidents are investigated, explore the following rooms and challenges.
Splunk101
Splunk201
Benign
ItsyBitsy
Answer the questions below
Complete this room.
No answer needed
Correct Answer
Created by tryhackme and Dex01
This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 5925 users are in here and this room is 41 days old.
Woop woop! Your answer is correct.
THM{000_SIEM_INTRO}
Congratulations
You've completed the room! Share this with your friends:
Twitter
Facebook
LinkedIn
Leave feedback
THM AttackBox
Intro to SIEM