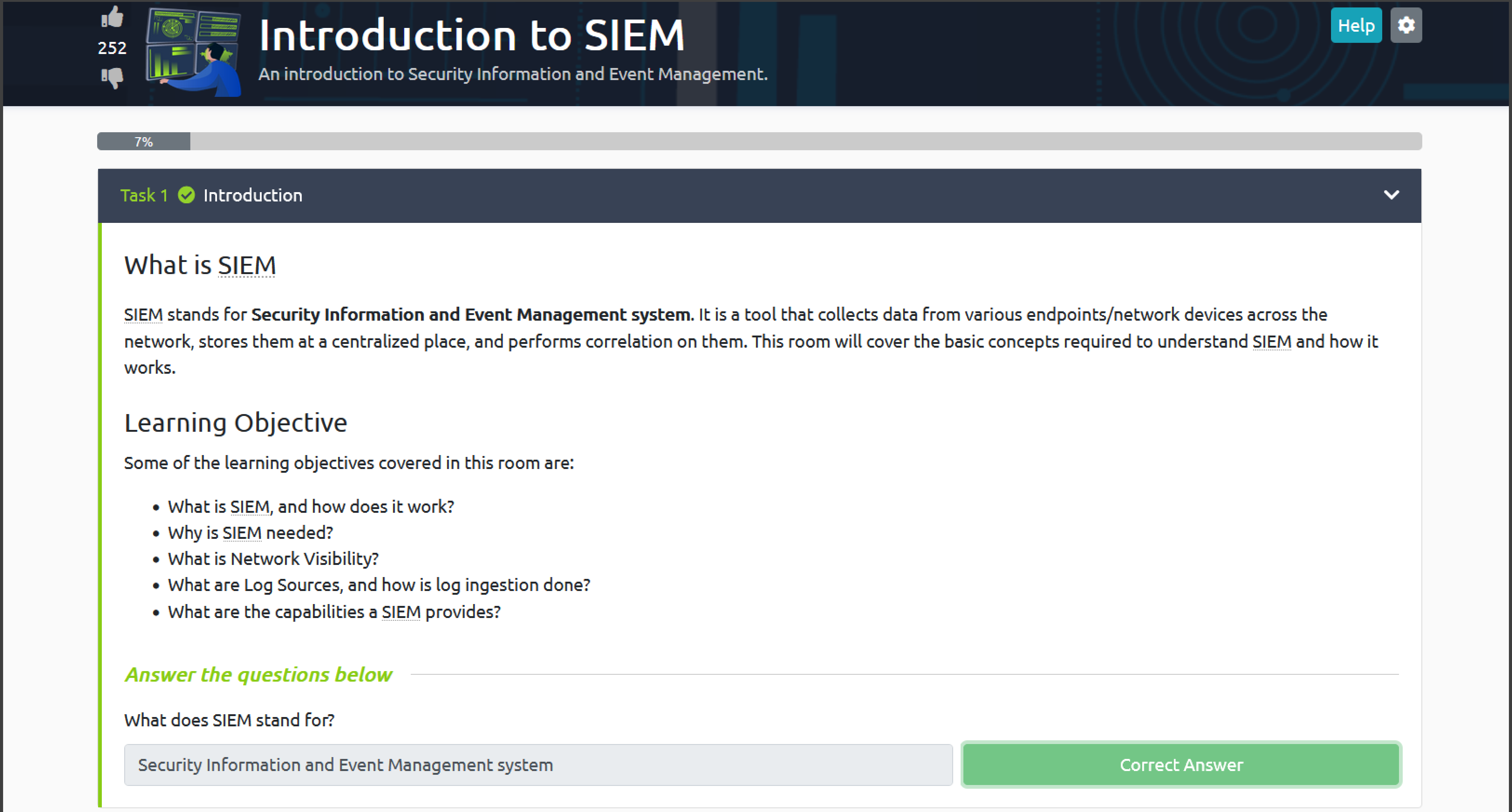
Assignment 6 –John Parr

Try hack me siem



Introduction to SIEM

An introduction to Security Information and Event Management.

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

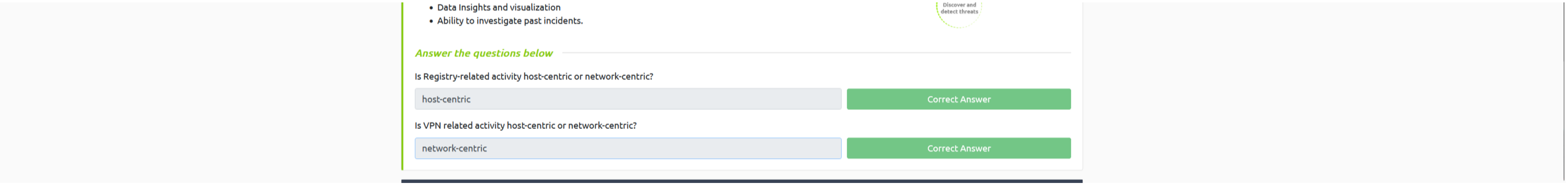
Some of the learning objectives covered in this room are:

- 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



- Data Insights and visualization
- Ability to investigate past incidents.

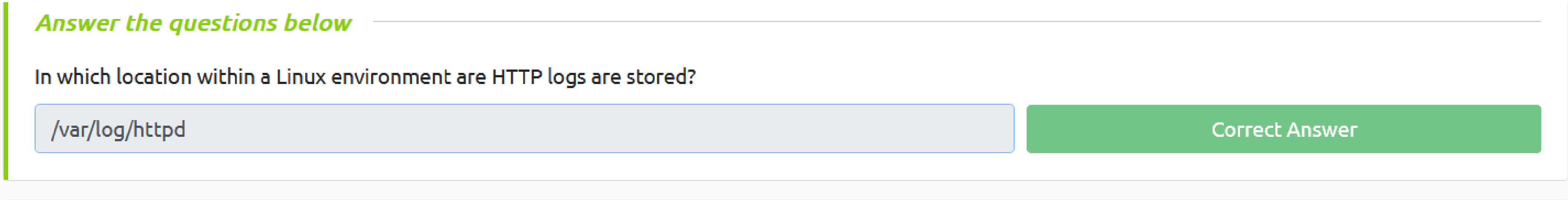
Answer the questions below

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

host-centric

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

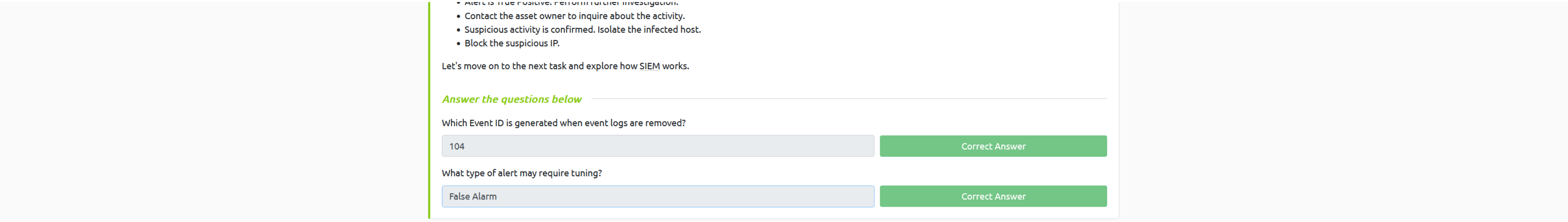
network-centric



Answer the questions below

In which location within a Linux environment are HTTP logs are stored?

/var/log/httpd



- 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.

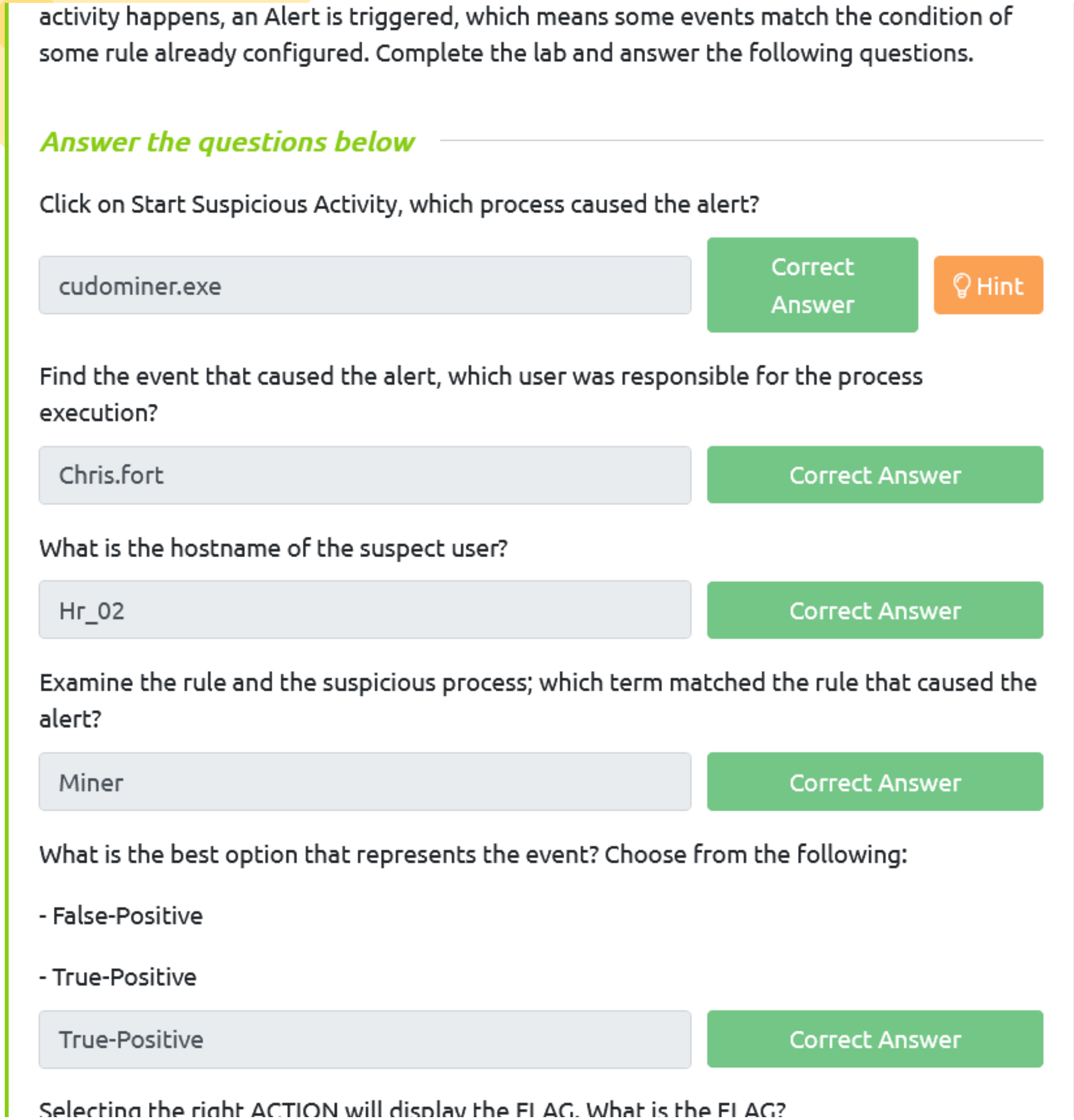
Answer the questions below

Which Event ID is generated when event logs are removed?

104

What type of alert may require tuning?

False Alarm



activity happens, an Alert is triggered, which means some events match the condition of some rule already configured. Complete the lab and answer the following questions.

Answer the questions below

Click on Start Suspicious Activity, which process caused the alert?

cudominer.exe

Find the event that caused the alert, which user was responsible for the process execution?

Chris.fort

What is the hostname of the suspect user?

Hr_02

Examine the rule and the suspicious process; which term matched the rule that caused the alert?

Miner

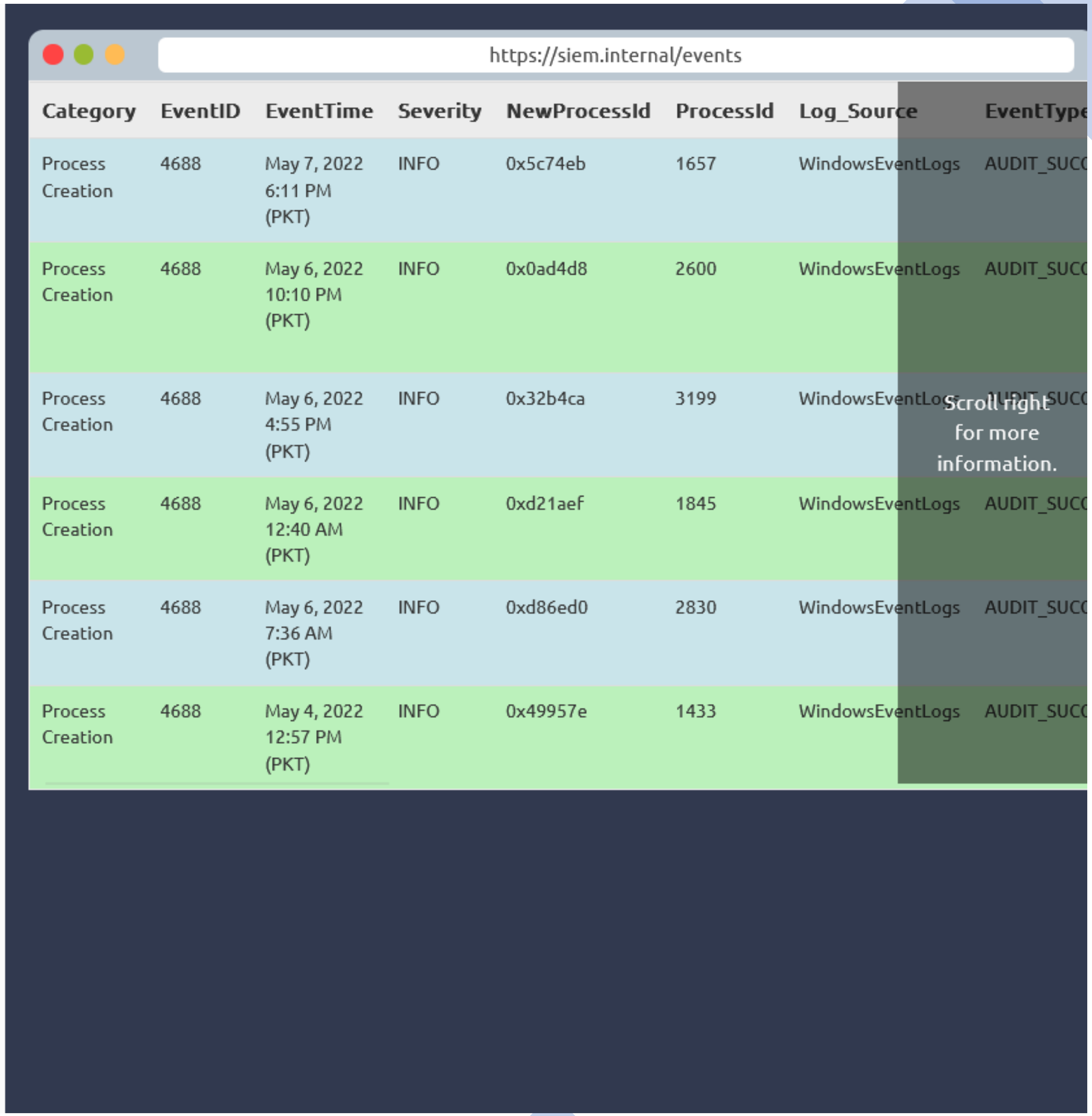
What is the best option that represents the event? Choose from the following:

- False-Positive

- True-Positive

True-Positive

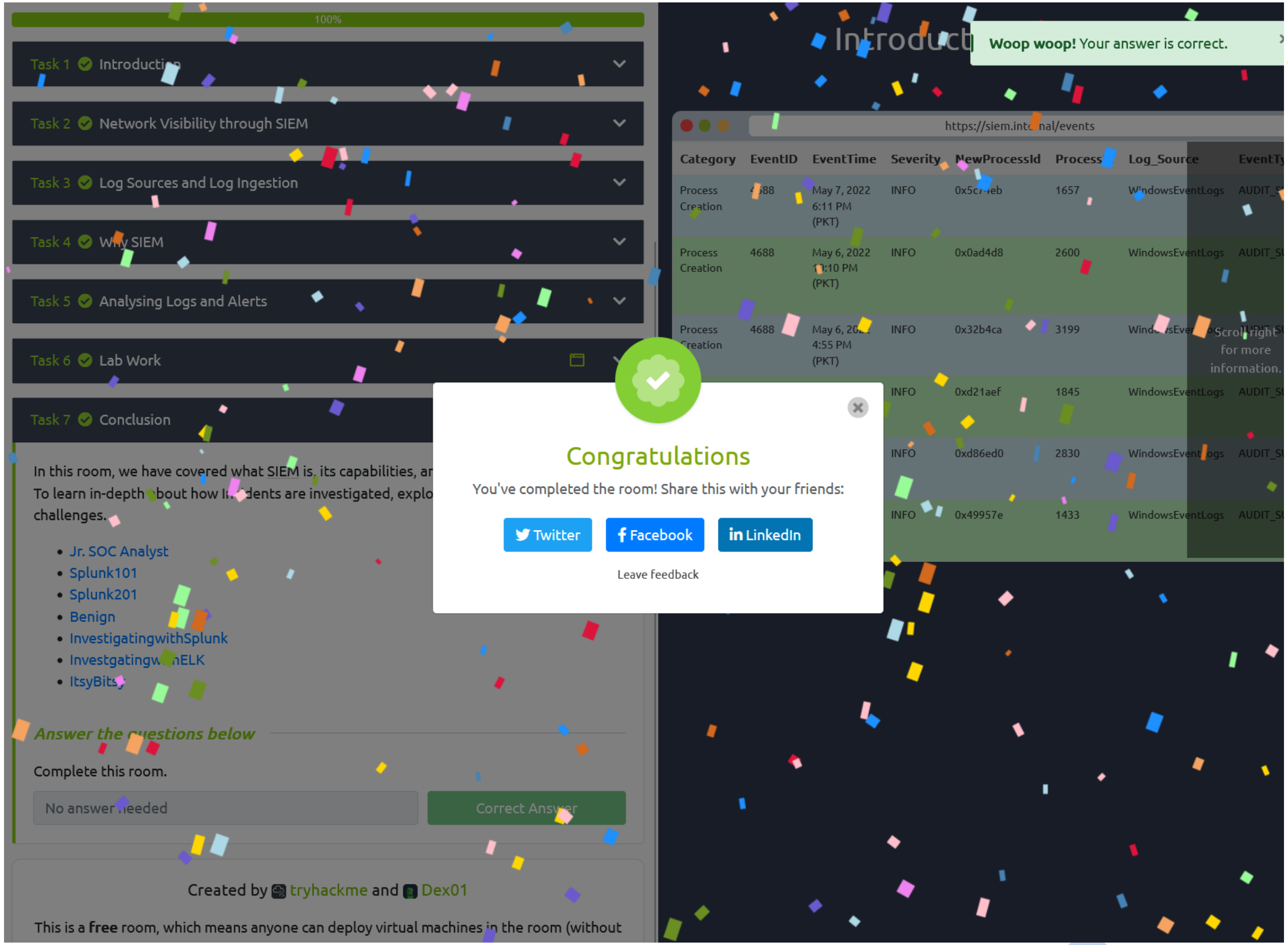
Selecting the right ACTION will display the FLAG. What is the FLAG?



https://siem.internal/events

Category	EventID	EventTime	Severity	NewProcessId	ProcessId	Log_Source	EventType
Process Creation	4688	May 7, 2022 6:11 PM (PKT)	INFO	0x5c74eb	1657	WindowsEventLogs	AUDIT_SUCC
Process Creation	4688	May 6, 2022 10:10 PM (PKT)	INFO	0x0ad4d8	2600	WindowsEventLogs	AUDIT_SUCC
Process Creation	4688	May 6, 2022 4:55 PM (PKT)	INFO	0x32b4ca	3199	WindowsEventLogs	AUDIT_SUCC
Process Creation	4688	May 6, 2022 12:40 AM (PKT)	INFO	0xd21aef	1845	WindowsEventLogs	AUDIT_SUCC
Process Creation	4688	May 6, 2022 7:36 AM (PKT)	INFO	0xd86ed0	2830	WindowsEventLogs	AUDIT_SUCC
Process Creation	4688	May 4, 2022 12:57 PM (PKT)	INFO	0x49957e	1433	WindowsEventLogs	AUDIT_SUCC

Scroll right for more information.



Task 1 ✓ Introduction

Task 2 ✓ Network Visibility through SIEM

Task 3 ✓ Log Sources and Log Ingestion

Task 4 ✓ Why SIEM

Task 5 ✓ Analysing Logs and Alerts

Task 6 ✓ Lab Work

Task 7 ✓ Conclusion

In this room, we have covered what SIEM is, its capabilities, ar
To learn in-depth about how Incidents are investigated, explo
challenges.

- Jr. SOC Analyst
- Splunk101
- Splunk201
- Benign
- InvestigatingwithSplunk
- InvestgatingwithELK
- 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

Introducti

Woop woop! Your answer is correct.

https://siem.internal/events

Category	EventID	EventTime	Severity	NewProcessId	Process	Log_Source	EventTy
Process Creation	4688	May 7, 2022 6:11 PM (PKT)	INFO	0x5c7[illegible]eb	1657	WindowsEventLogs	AUDIT_S
Process Creation	4688	May 6, 2022 10:10 PM (PKT)	INFO	0x0ad4d8	2600	WindowsEventLogs	AUDIT_SU
Process Creation	4688	May 6, 2022 4:55 PM (PKT)	INFO	0x32b4ca	3199	WindowsEventLogs	AUDIT_SU
			INFO	0xd21aef	1845	WindowsEventLogs	AUDIT_SU
			INFO	0xd86ed0	2830	WindowsEventLogs	AUDIT_SU
			INFO	0x49957e	1433	WindowsEventLogs	AUDIT_SU

Scroll right for more information.

Congratulations

You've completed the room! Share this with your friends: