TryHackMe | Introduction to SIEM

igor_sec · Follow

11 min read · Sep 25, 2023

Listen Share More

This my write-up for TryHackMe's Introduction to SIEM, which provides an overview of what SIEM is, its significance, and how it works. I will explore fundamental concepts such as network visibility, log sources, and the analysis of logs and alerts. The objective is to gain an understanding of how SIEM protects networks and data, offering improved visibility, faster threat detection, and enhanced security outcomes.

Room link: Introduction to SIEM

Task 1: Introduction

A SIEM, which stands for Security Information and Event Management system, is a powerful tool that gathers data from multiple devices on a network, centralizes and

stores it, and then performs analysis to identify correlations. This post will provide an overview of the fundamental concepts of SIEM and its functioning.

Learning Objective

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?

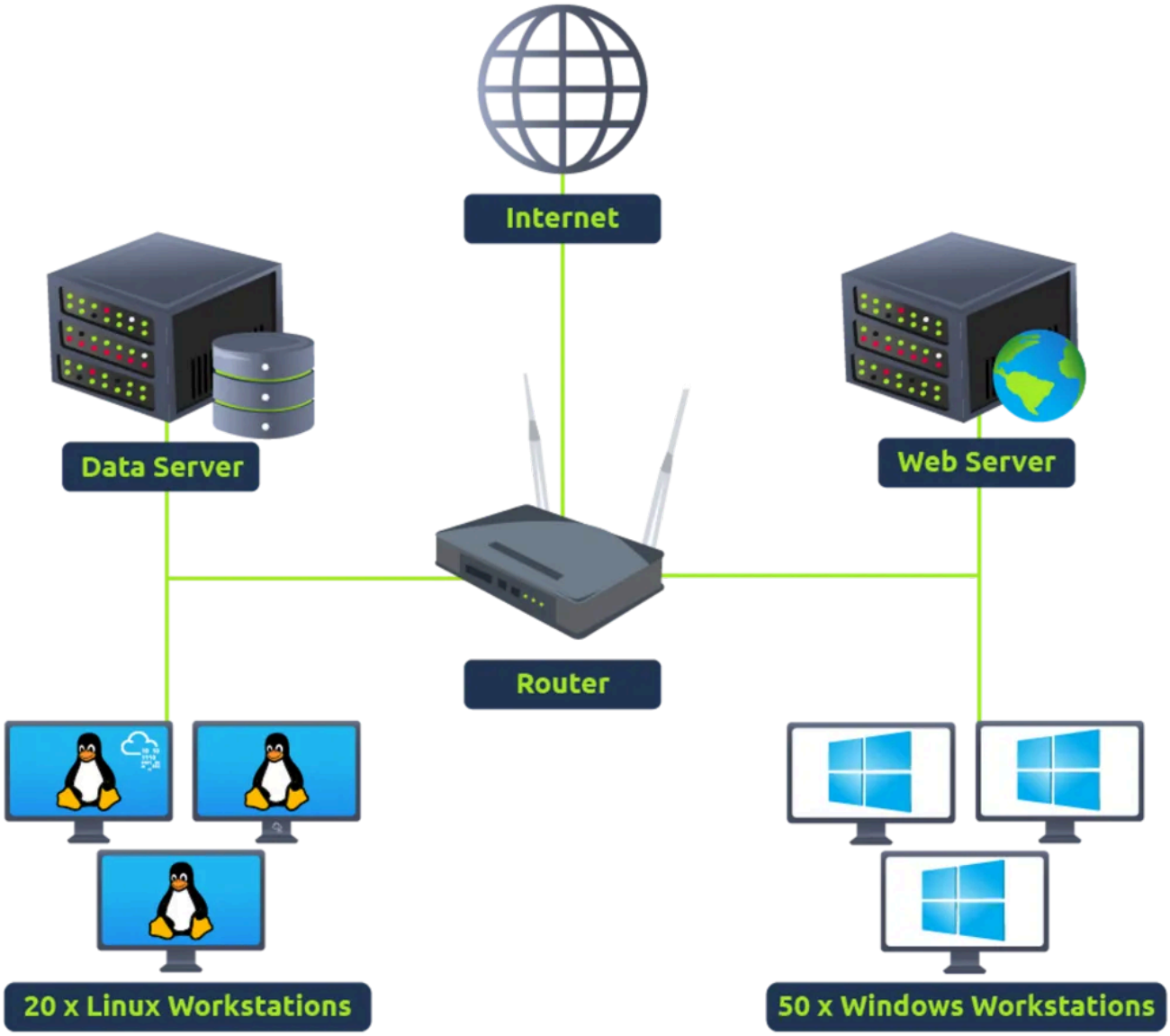
Answer the questions below

What does SIEM stand for?

Answer: Security Information and Event Management system.

Task 2: Network Visibility through SIEM

In order to understand the significance of SIEM, let us first grasp the rationale behind the need for enhanced visibility of network activities. The diagram provided illustrates a basic network structure consisting of various Linux/Windows endpoints, a data server, and a website. Each element interacts with others or connects to the internet via a router.



As we know, each network component can have one or more log sources generating different logs. One example could be setting up Sysmon along with Windows Event logs to have better visibility of Windows Endpoint. We can divide our network log sources into two logical parts:

1) Host-Centric Log Sources

These are log sources that capture events that occurred within or related to the host. Some log sources that generate host-centric logs are Windows Event logs, Sysmon, Osquery, etc. Some examples of host-centric logs are:

- A user accessing a file
- A user attempting to authenticate.
- A process Execution Activity
- A process adding/editing/deleting a registry key or value.

- Powershell execution

2) Network-Centric Log Sources

Network-related logs are generated when the hosts communicate with each other or access the internet to visit a website. Some network-based protocols are SSH, VPN, HTTP/s, FTP, etc. Examples of such events are:

- SSH connection
- A file being accessed via FTP
- Web traffic
- A user accessing company's resources through VPN.
- Network file sharing Activity

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 imglogs 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?

Answer: host-centric

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

Answer: network-centric

Task 3: Log Sources and Log Ingestion

Every device in the network generates some kind of log whenever an activity is performed on it, like a user visiting a website, connecting to SSH, logging into his workstation, etc. Some common devices that are found in a network environment are discussed below:

Windows Machine

Windows records every event that can be viewed through the Event Viewer utility. It assigns a unique ID to each type of log activity, making it easy for the analyst to examine and keep track of. To view events in a Windows environment, type `Event Viewer` in the search bar, and it takes you to the tool where different logs are stored and can be viewed, as shown below. These logs from all windows endpoints are forwarded to the SIEM solution for monitoring and better visibility.

Linux

Linux OS stores all the related logs, such as events, errors, warnings, etc. Which are then ingested into SIEM for continuous monitoring. Some of the common locations where Linux store logs are:

- /var/log/httpd : Contains HTTP Request / Response and error logs.
- /var/log/cron : Events related to cron jobs are stored in this location.
- /var/log/auth.log and /var/log/secure : Stores authentication related logs.

- /var/log/kern : This file stores kernel related events.

Here is a sample of a cron log:

```
May 28 13:04:20 ebr crond[2843]: /usr/sbin/crond 4.4 dillon's cron daemon, star
May 28 13:04:20 ebr crond[2843]: no timestamp found (user root job sys-hourly)
May 28 13:04:20 ebr crond[2843]: no timestamp found (user root job sys-daily)
May 28 13:04:20 ebr crond[2843]: no timestamp found (user root job sys-weekly)
May 28 13:04:20 ebr crond[2843]: no timestamp found (user root job sys-monthly)
Jun 13 07:46:22 ebr crond[3592]: unable to exec /usr/sbin/sendmail: cron output
```

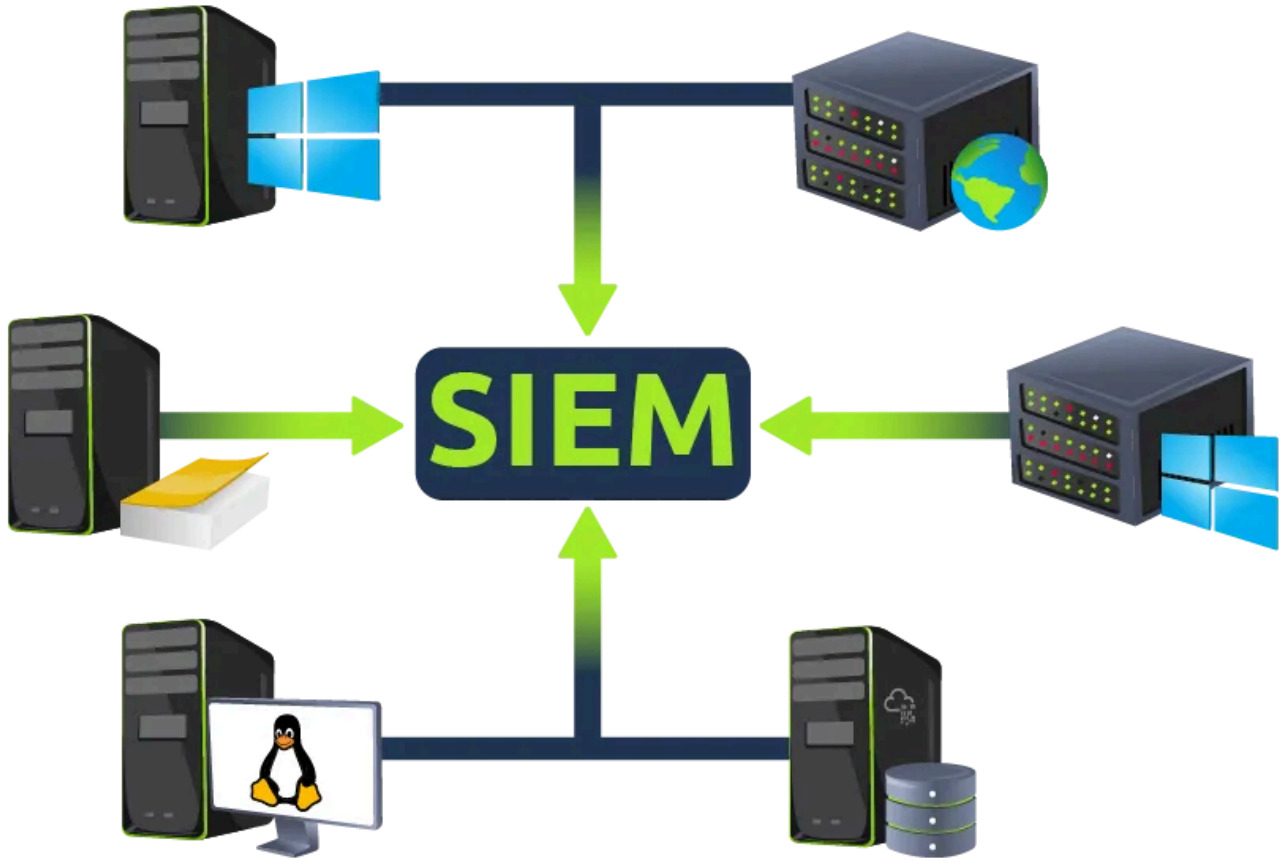
Web Server

It is important to keep an eye on all the requests/responses coming in and out of the webserver for any potential web attack attempt. In Linux, common locations to write all apache related logs are /var/log/apache or /var/log/httpd.

Here is an example of Apache Logs:

```
192.168.21.200 - - [21/March/2022:10:17:10 -0300] "GET /cgi-bin/try/ HTTP/1.0"
127.0.0.1 - - [21/March/2022:10:22:04 -0300] "GET / HTTP/1.0" 200 2216
```

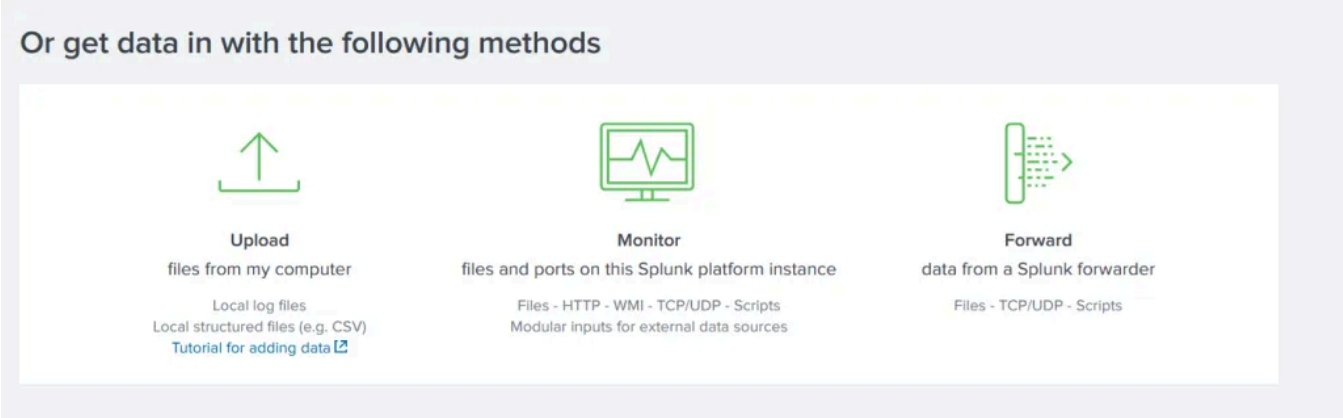
Log Ingestion



All these logs provide a wealth of information and can help in identifying security issues. Each SIEM solution has its own way of ingesting the logs. Some common methods used by these SIEM solutions are explained below:

1. Agent / Forwarder: These SIEM solutions provide a lightweight tool called an agent (forwarder by Splunk) that gets installed in the Endpoint. It is configured to capture all the important logs and send them to the SIEM server.
2. Syslog: Syslog is a widely used protocol to collect data from various systems like web servers, databases, etc., are sent real-time data to the centralized destination.
3. Manual Upload: Some SIEM solutions, like Splunk, ELK, etc., allow users to ingest offline data for quick analysis. Once the data is ingested, it is normalized and made available for analysis.
4. Port-Forwarding: SIEM solutions can also be configured to listen on a certain port, and then the endpoints forward the data to the SIEM instance on the listening port.

An example of how Splunk provides various methods for log Ingestion is shown below:



Answer the questions below

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

Answer: /var/log/httpd

Task 4: Why SIEM

SIEM is used to provide correlation on the collected data to detect threats. Once a threat is detected, or a certain threshold is crossed, an alert is raised. This alert enables the analysts to take suitable actions based on the investigation. SIEM plays an important role in the Cyber Security domain and helps detect and protect against the latest threats in a timely manner. It provides good visibility of what's happening within the network infrastructure.

SIEM

SIEM is one major component of a Security Operations Center (SOC) ecosystem, as illustrated below. SIEM starts by collecting logs and examining if any event/flow has matched the condition set in the rule or crossed a certain threshold

Some of the common capabilities of SIEM are:

- Correlation between events from different log sources.
- Provide visibility on both Host-centric and Network-centric activities.
- Allow analysts to investigate the latest threats and timely responses.
- Hunt for threats that are not detected by the rules in place.

SOC Analyst Responsibilities

SOC Analysts utilize SIEM solutions in order to have better visibility of what is happening within the network. Some of their responsibilities include:

- Monitoring and Investigating.
- Identifying False positives.
- Tuning Rules which are causing the noise or False positives.
- Reporting and Compliance.
- Identifying blind spots in the network visibility and covering them.

Answer the questions below

Read the task above.

Task 5: Analysing Logs and Alerts

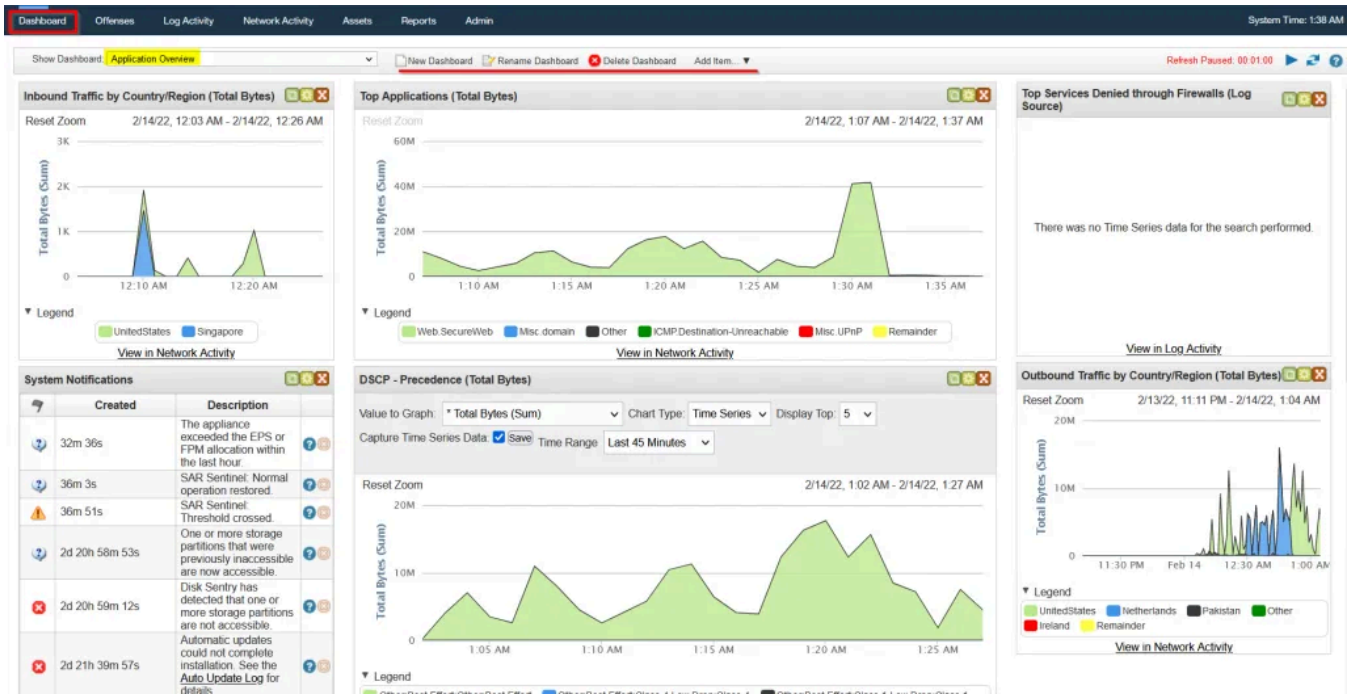
SIEM tool gets all the security-related logs ingested through agents, port forwarding, etc. Once the logs are ingested, SIEM looks for unwanted behavior or suspicious pattern within the logs with the help of the conditions set in the rules by the analysts. If the condition is met, a rule gets triggered, and the incident is investigated.

Dashboard

Dashboards are the most important components of any SIEM. SIEM presents the data for analysis after being normalized and ingested. The summary of these analyses is presented in the form of actionable insights with the help of multiple dashboards. Each SIEM solution comes with some default dashboards and provides an option for custom Dashboard creation. Some of the information that can be found in a dashboard are:

- Alert Highlights
- System Notification
- Health Alert
- List of Failed Login Attempts
- Events Ingested Count
- Rules triggered
- Top Domains Visited

An example of a Default dashboard in Qradar SIEM is shown below:



Correlation Rules

Correlation rules play an important role in the timely detection of threats allowing analysts to take action on time. Correlation rules are pretty much logical expressions set to be triggered. A few examples of correlation rules are:

- If a User gets 5 failed Login Attempts in 10 seconds — Raise an alert for `Multiple Failed Login Attempts`
- If login is successful after multiple failed login attempts — Raise an alert for `Successful Login After multiple Login Attempts`
- A rule is set to alert every time a user plugs in a USB (Useful if USB is restricted as per the company policy)
- If outbound traffic is > 25 MB — Raise an alert to potential Data exfiltration Attempt (Usually, it depends on the company policy)

How a correlation rule is created

To explain how the rule works, consider the following Eventlog use cases:

Use-Case 1:

Adversaries tend to remove the logs during the post-exploitation phase to remove their tracks. A unique Event ID **104** is logged every time a user tries to remove or clear event logs. To create a rule based on this activity, we can set the condition as follows:

Rule: If the Log source is WinEventLog **AND** EventID is **104** — Trigger an alert `Event Log Cleared`

Use-Case 2: Adversaries use commands like **whoami** after the exploitation/privilege escalation phase. The following Fields will be helpful to include in the rule.

- Log source: Identify the log source capturing the event logs
- Event ID: which Event ID is associated with Process Execution activity? In this case, event id 4688 will be helpful.
- NewProcessName: which process name will be helpful to include in the rule?

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?

Answer: 104

What type of alert may require tuning?

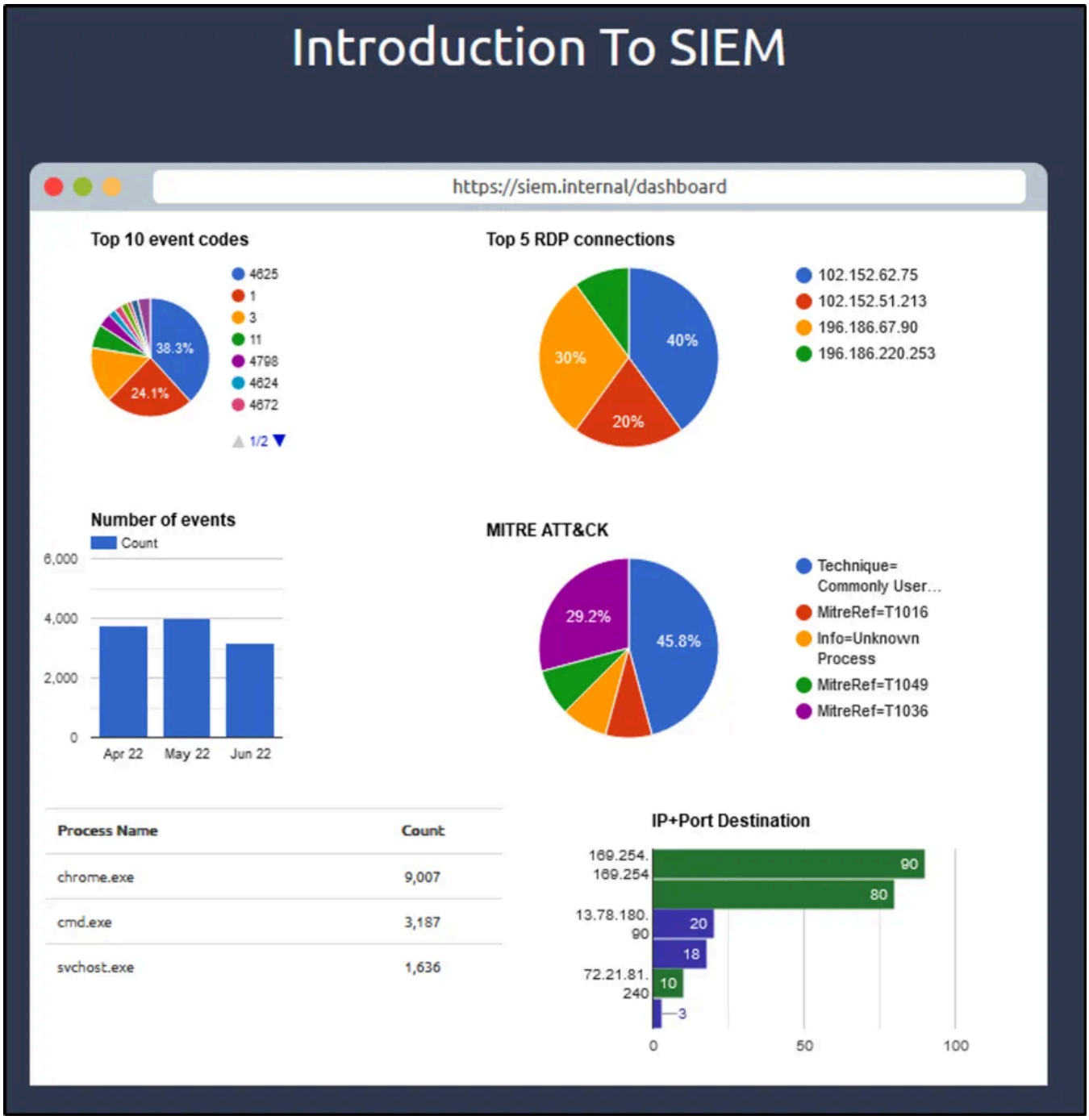
Answer: false alarms

Task 6: Lab Work

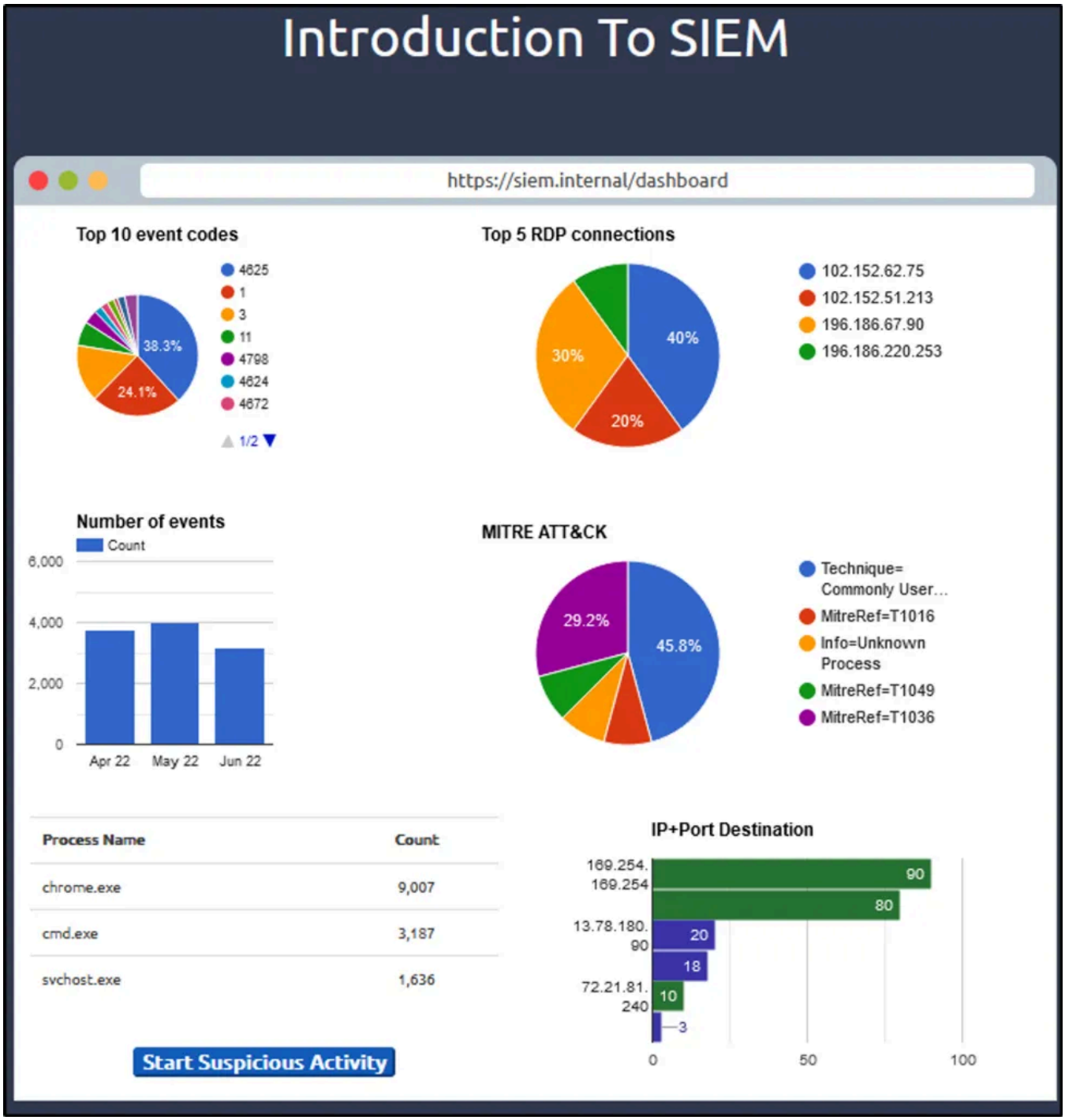
Lab Work

Click on the **View Site button**, which will display the lab on the right side of the screen.

In the static lab attached, a sample dashboard and events are displayed. When a suspicious 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.



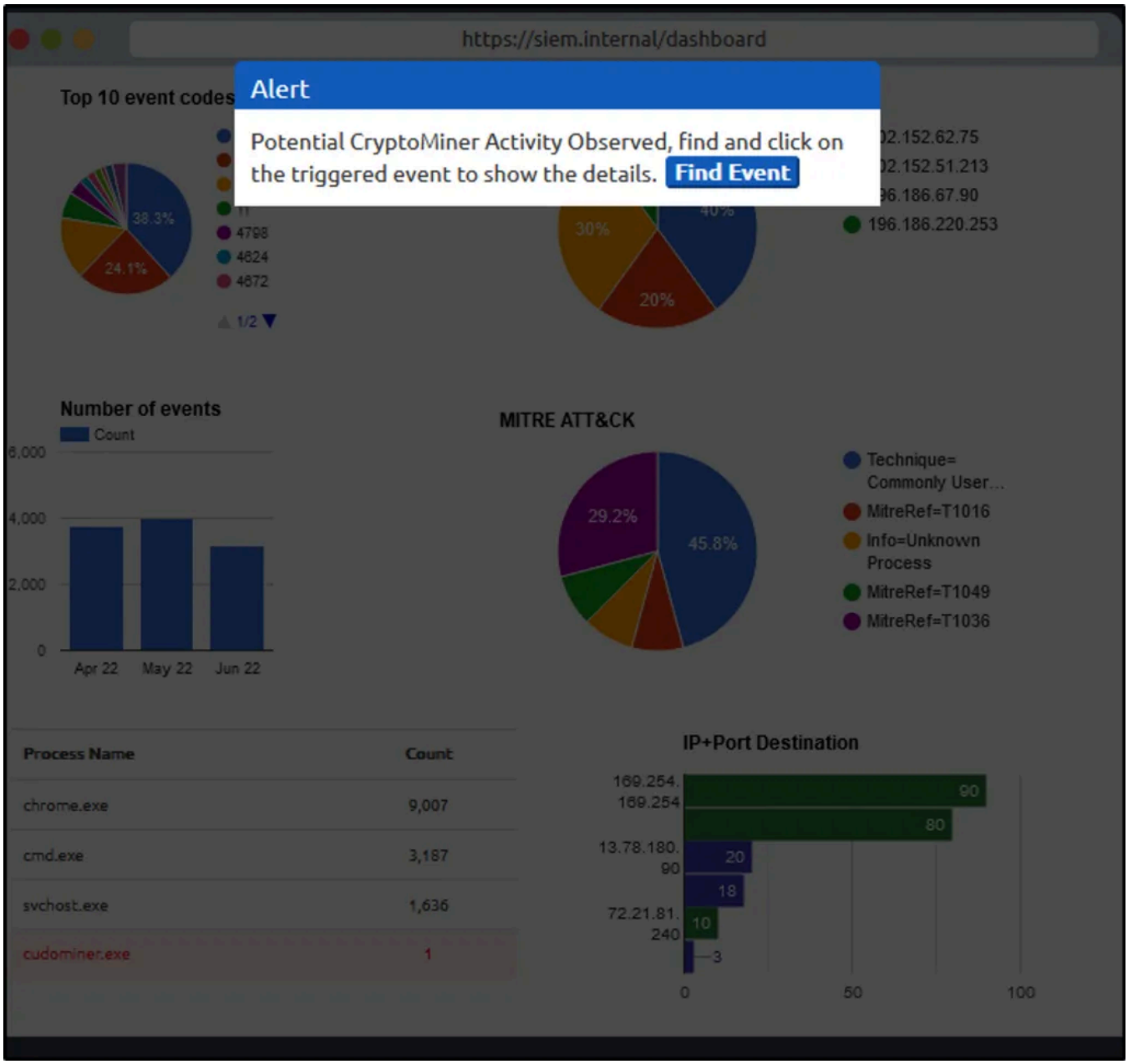
Click on “Start Suspicious Activity”



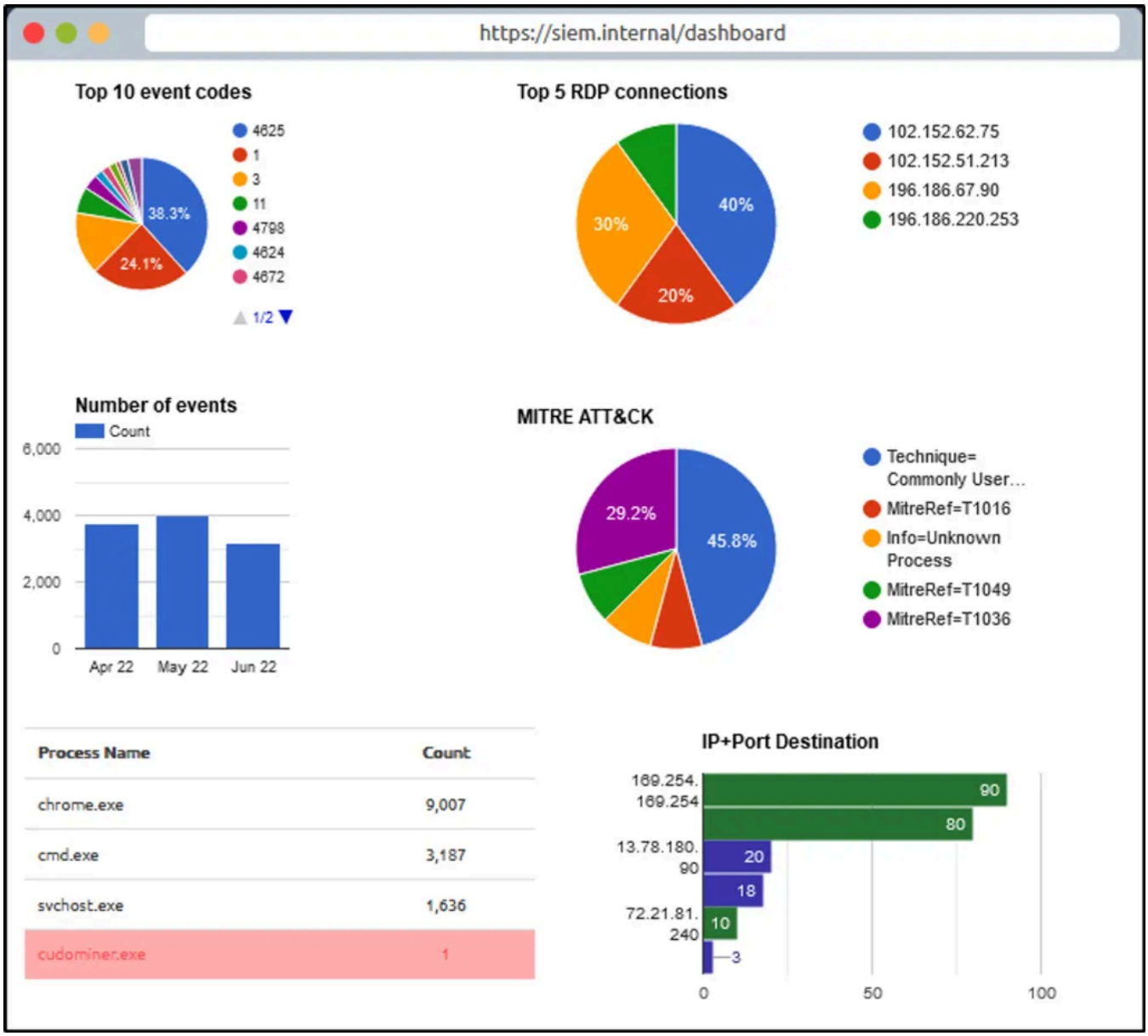
Answer the questions below

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

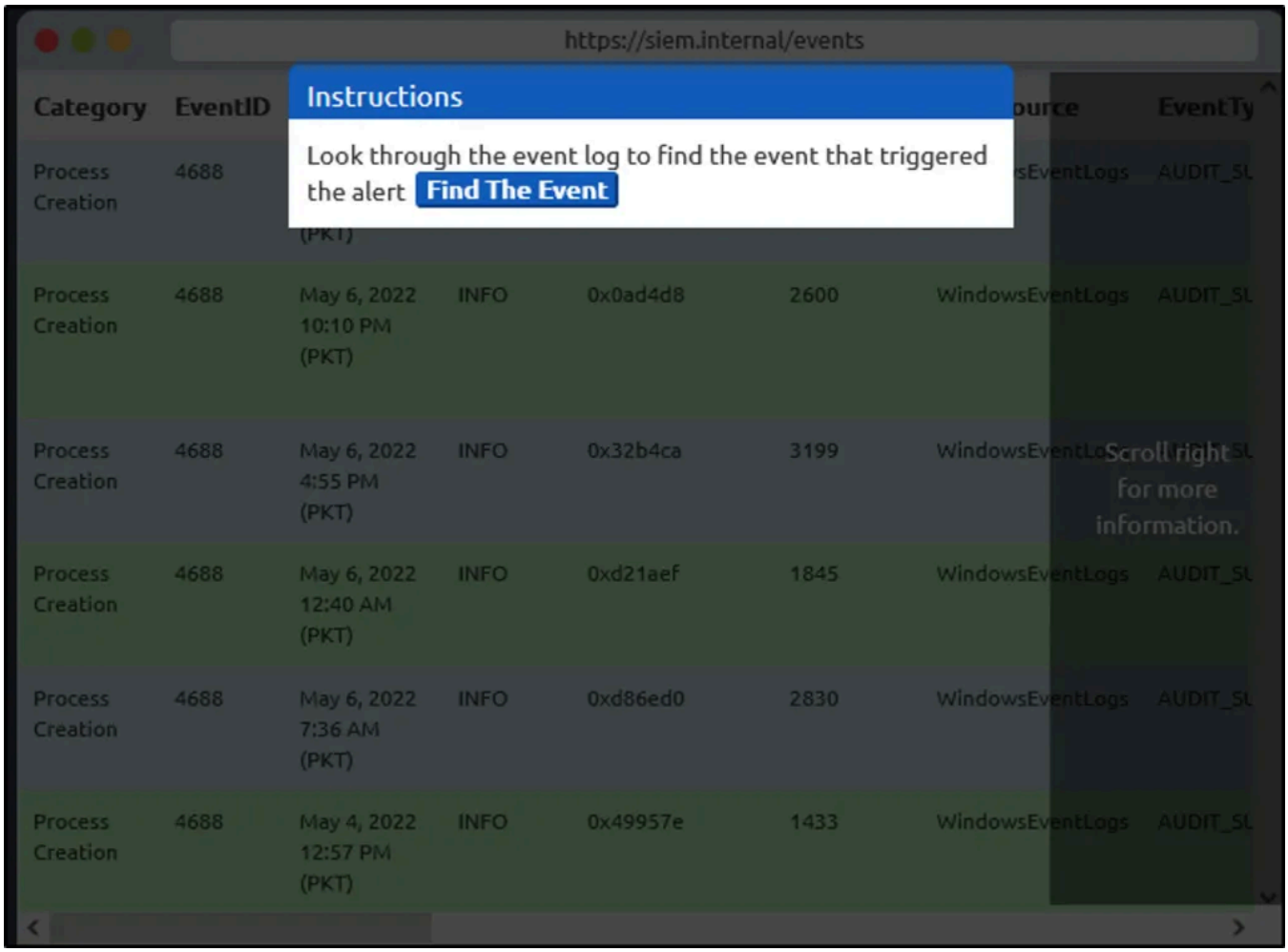
Answer: cudominer.exe



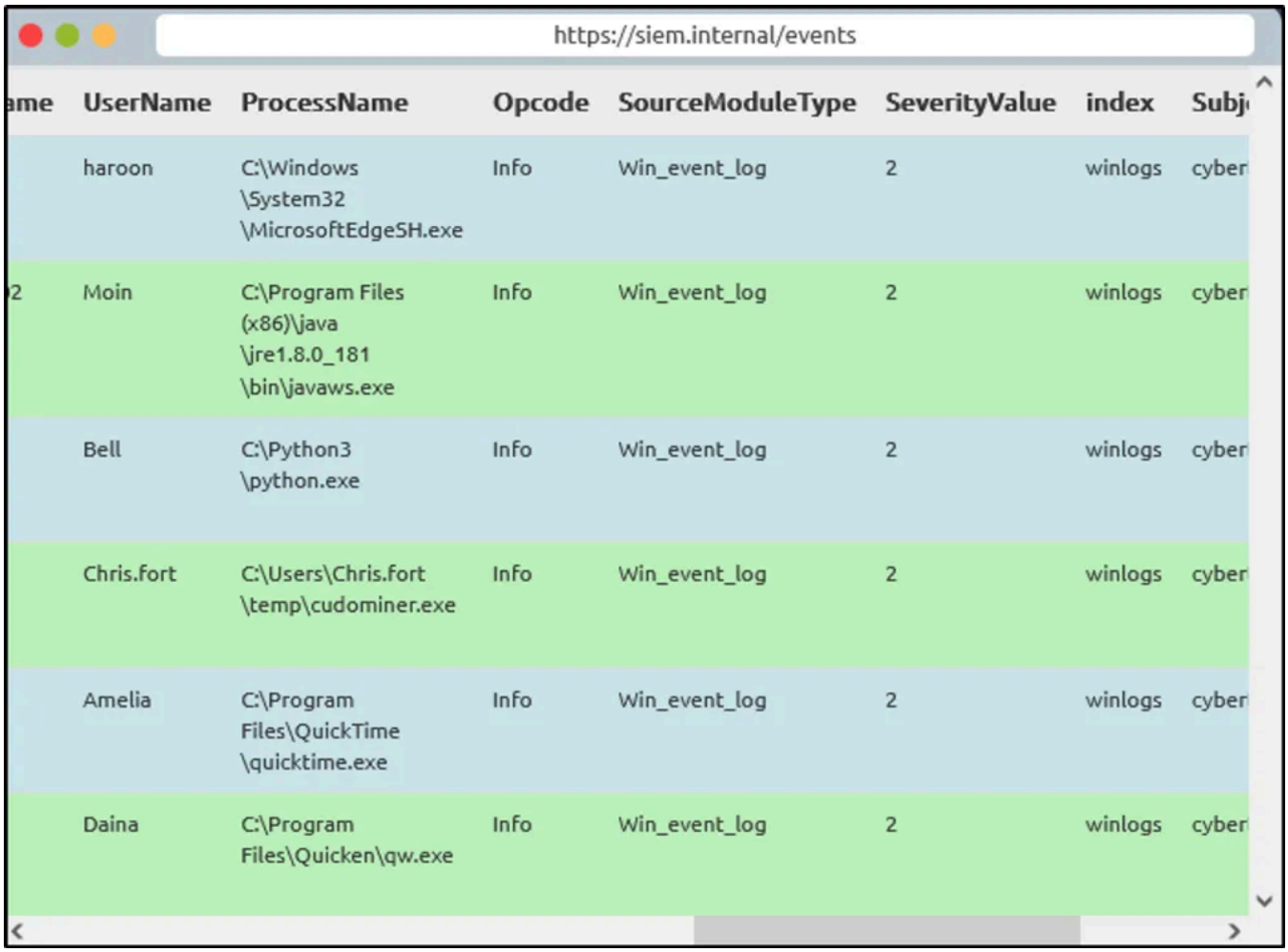
`cudominer.ex` e process is highlighted which is very suspicious.



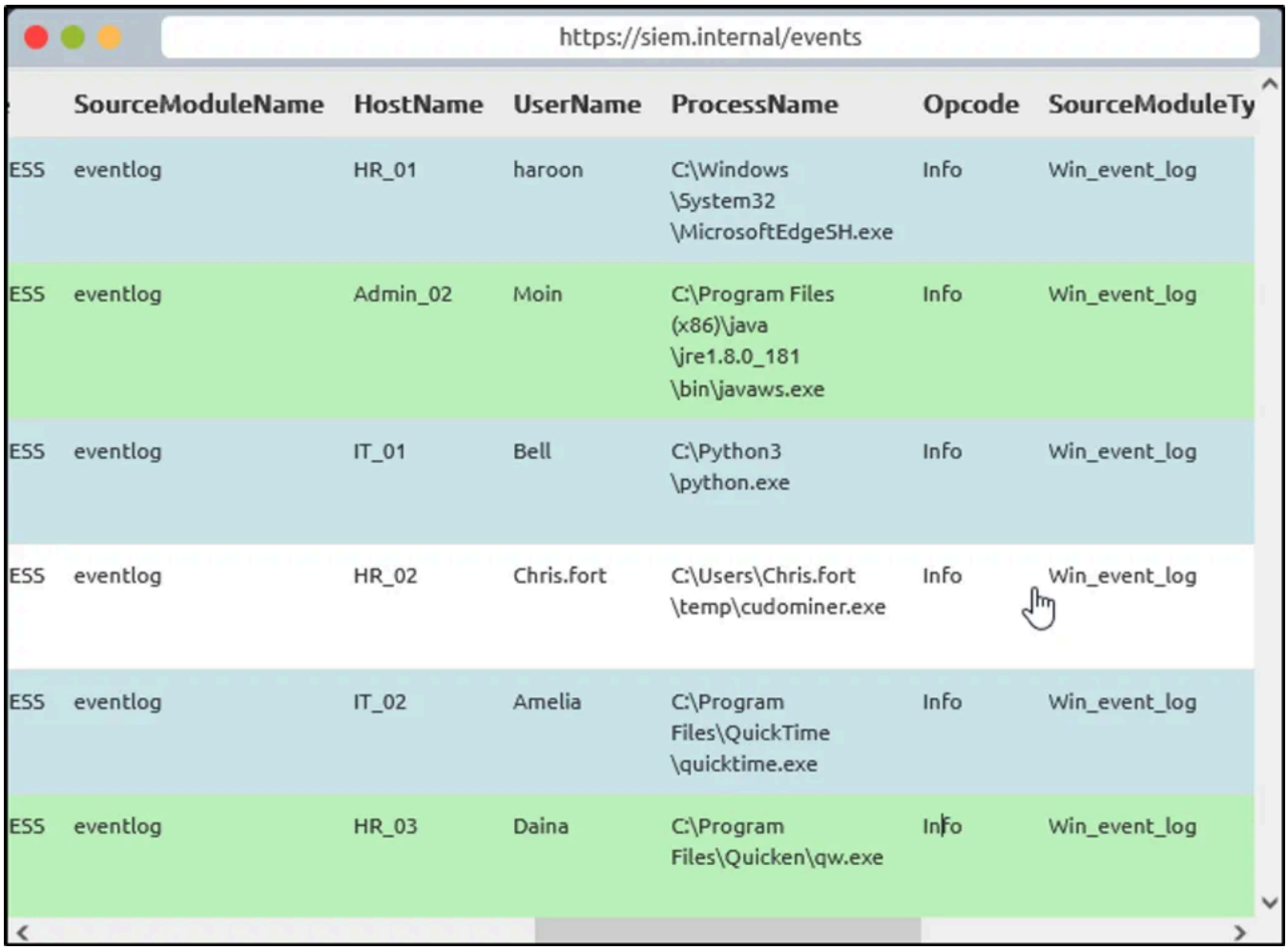
Navigate to the event logs and locate the event that triggered the alert.



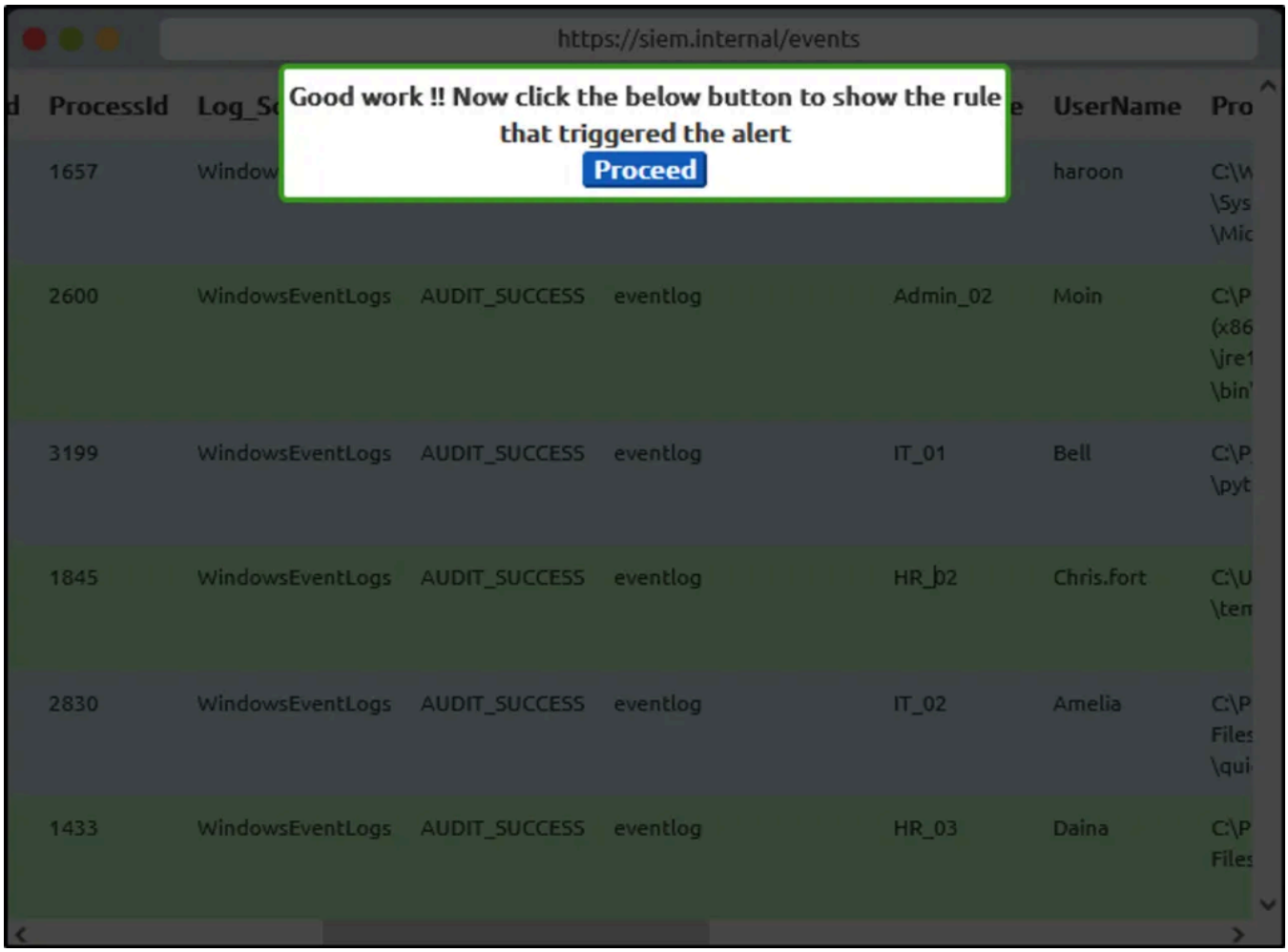
Below shows where the suspicious process is.



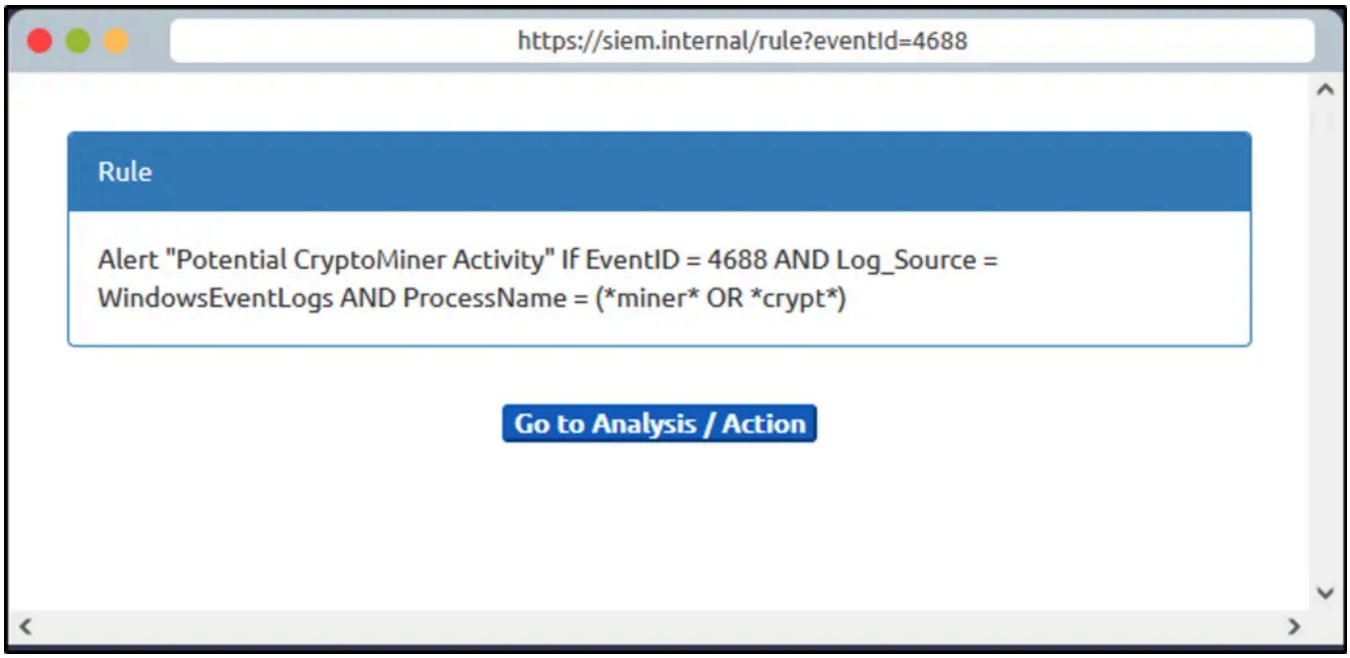
Click on the event to get more details.



Next is to click on the rule ID that triggered the alert.

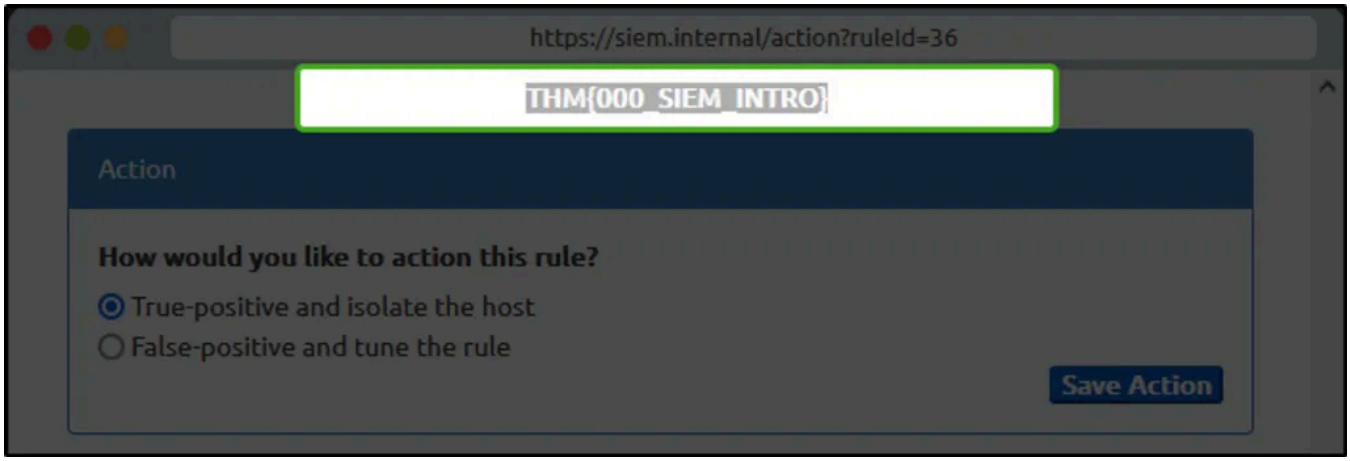


The following shows the rule.



Following the next task to be taken is to decide whether the alert was True-positive or False-positive and take corrective response.

Based from the information gathered, the alert is categorized as True-positive



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

Answer: Christ.fort

What is the hostname of the suspect user?

Answer: HR_02

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

Answer: miner

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

- False-Positive
- True-Positive

Answer: True-Positive

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

Answer: THM{000_SIEM_INTRO}

Task 7: Conclusion

This room provides comprehensive information on SIEM, including its capabilities and the visibility it offers. For a more thorough understanding of incident investigations, available resources include various rooms and challenges.

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

Answer the questions below

Complete this room.

SIEM platforms play a vital role in network security, aiding in the identification of potential incidents and constant monitoring of activities. This post explores essential principles and elements of SIEM solutions. It touches on processes such as log collection, data normalization, and the establishment of correlation rules to effectively identify threats. Dashboards provide valuable insights, while the ability to delve deeper into events aids in incident response.

Thank you for reading. Until next time :-)

Thm Tryhackme Siem Cybersecurity Blog

Follow

Written by igor_sec

368 Followers · 11 Following

No responses yet

What are your thoughts?

Respond

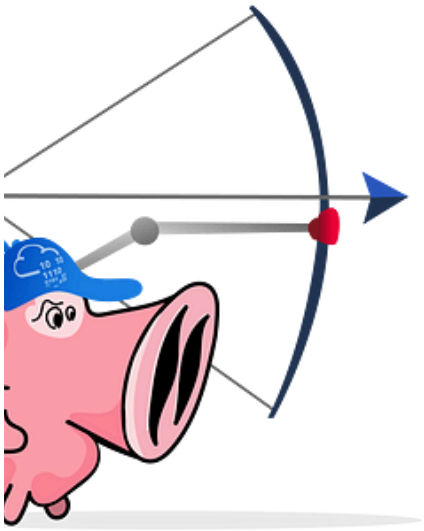
More from igor_sec

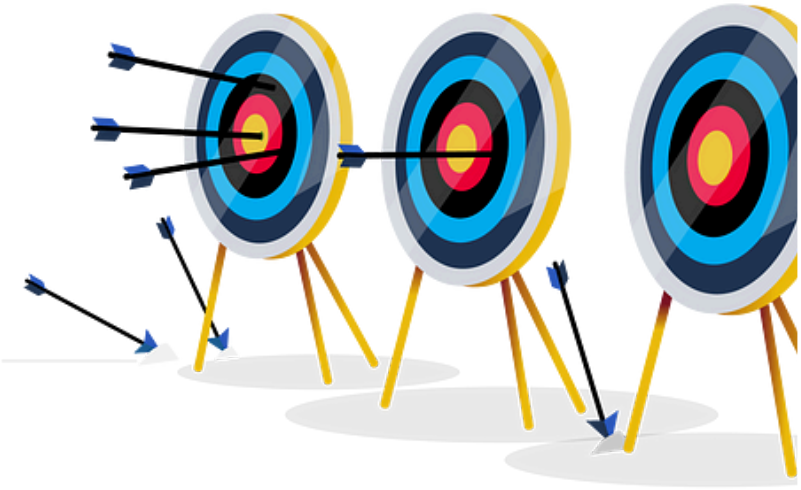
igor_sec

Snort | TryHackMe — Write-up

SNORT is an open-source, rule-based Network Intrusion Detection and Prevention System (NIDS/NIPS). It was developed and still maintained by...

Jul 20, 2023 114





igor_sec

Snort Challenge—The Basics : TryHackMe

Task 1: Introduction

Jul 20, 2023 67 2

igor_sec

TryHackMe | Zeek

Introduction to hands-on network monitoring and threat detection with Zeek (formerly Bro).

Jul 12, 2023 58 1

igor_sec

CyberDefenders | Boss Of The SOC v1

Jul 5, 2023 12

See all from igor_sec

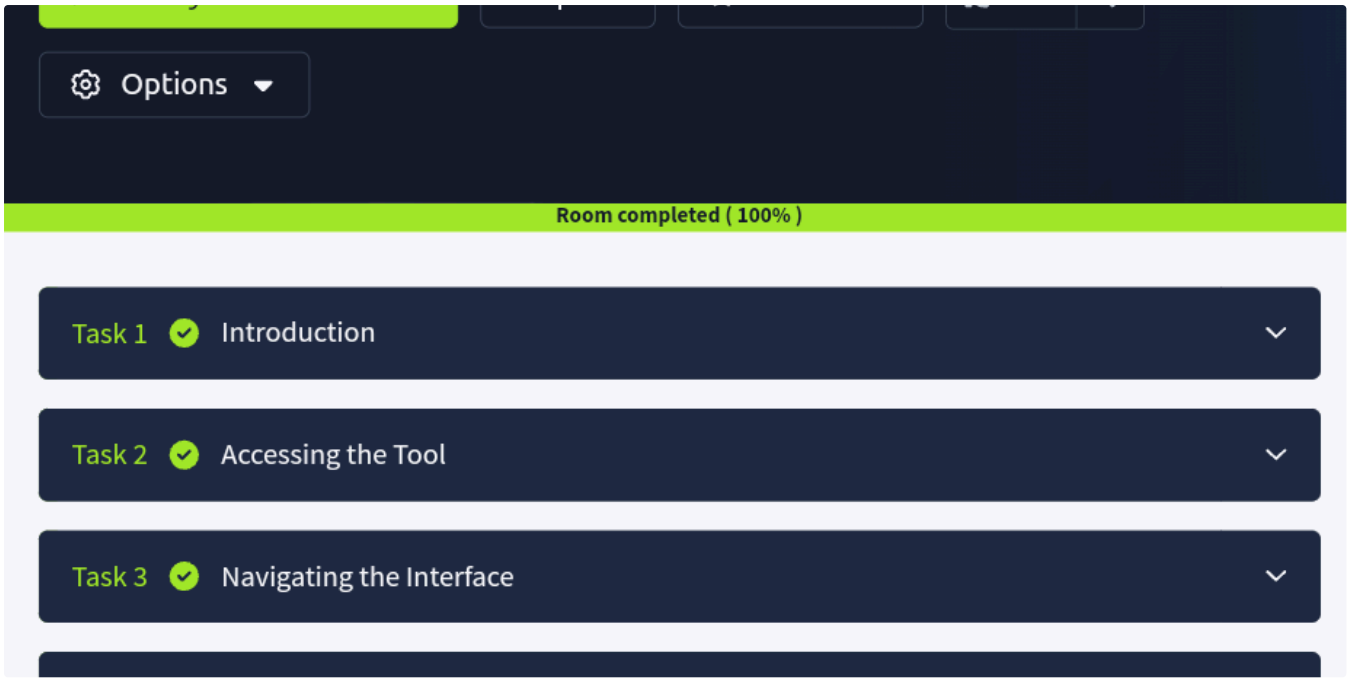
Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60



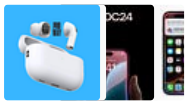
Jawstar

CyberChef: The Basics Tryhackme Write up

Tryhackme

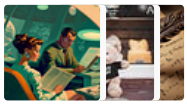
Nov 7, 2024 8

Lists



Tech & Tools
22 stories · 377 saves

MODERN MARKETING
204 stories · 974 saves



Medium's Huge List of Publications Accepting Submissions
377 stories · 4299 saves

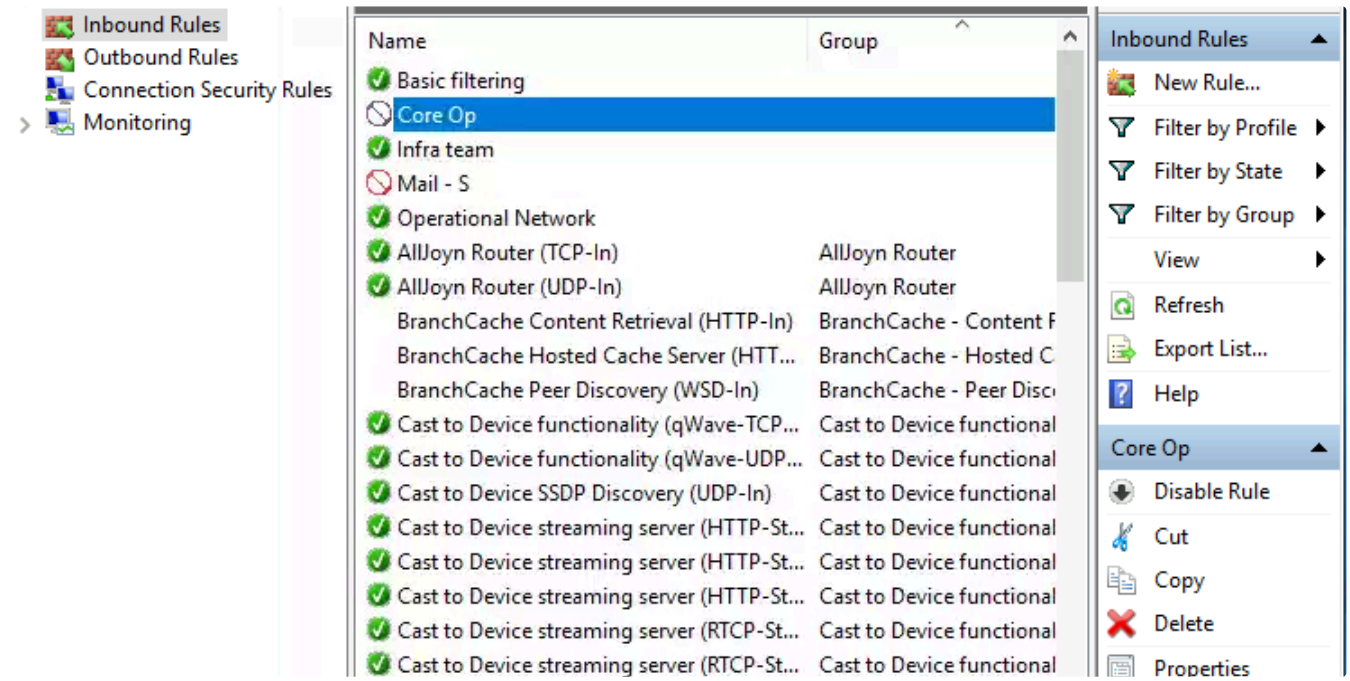
Staff picks
791 stories · 1544 saves

rutbar

TryHackMe—CAPA: The Basics | Cyber Security 101 (THM)

Tool Overview: How CAPA Works

Oct 23, 2024 13

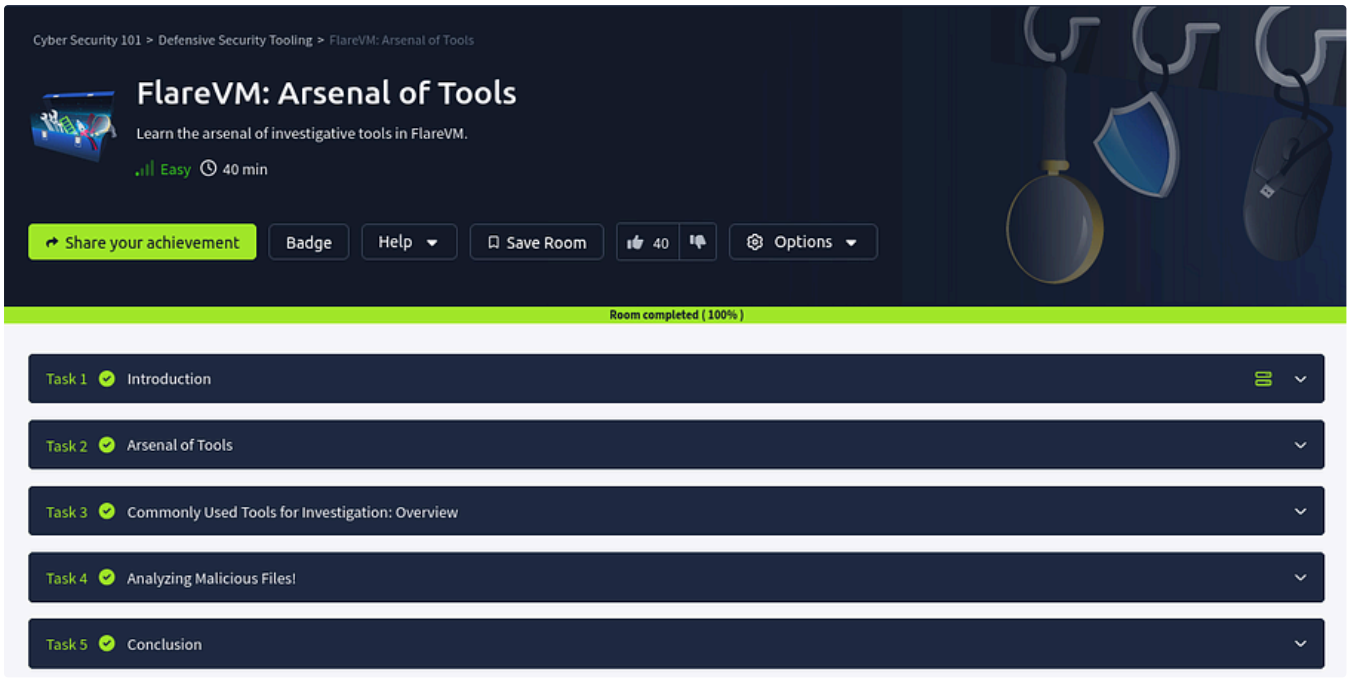


embossdotar

TryHackMe—Firewall Fundamentals—Writeup

Key points: Firewall | FW | Types | Windows built-in firewall | Linux built-in firewall | Rules. Firewall Fundamentals by awesome...

Oct 22, 2024 35 2



Jawstar

FlareVM: Arsenal of Tools

CYBER SECURITY 101 Tryhackme Write up

Oct 29, 2024 37 1

Procmon	Tracks system activity, especially for malware research, troubleshooting, and forensics.
Process Explorer	Provides insights into the parent-child relationship of processes, DLLs loaded, and paths.
HxD	Examines or alters malicious files via hex editing.
Wireshark	Investigates network traffic for unusual activity.
CFF Explorer	Generates file hashes for integrity verification and validates system file sources.
PEStudio	Static analysis tool for studying executable file properties without execution.
FLOSS	Extracts and de-obfuscates strings from malware programs using advanced

rutbar

TryHackMe—FlareVM: Arsenal of Tools | Cyber Security 101 (THM)

Arsenal of Tools In this task, we'll introduce you to tools inside FlareVM, which offers specialized tools for forensics, incident...

Oct 23, 2024 12

See more recommendations