

Mike Macancela
Intro To 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 network, stores them at a centralized place, and performs correlation on them. This room will cover the basic concepts required to understand 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

Task 5 Analysing Logs and Alerts

Type here to search

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:

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

Network-Centric Log Sources

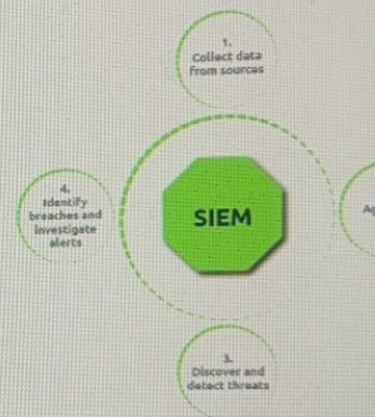
Network-related logs are generated when the hosts communicate with each other or access the internet to visit a website. Some network-based logs are SSH, VPN, HTTP/s, FTP, etc. Examples of such events are:

- 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 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.



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


```
May 28 15:04:20 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 for user root job sys-daily to /dev/nu
```

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 attempts. Locations to write all apache related logs are `/var/log/apache` or `/var/log/httpd`.

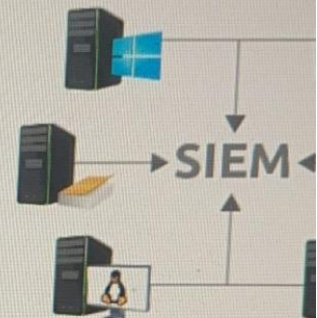
Here is an example of Apache Logs:

```
192.168.21.200 - - [21/March/2022:10:17:10 -0300] "GET /cgi-bin/try/ HTTP/1.0" 200 3395  
127.0.0.1 - - [21/March/2022:10:22:04 -0300] "GET / HTTP/1.0" 200 2216
```

Log Ingestion

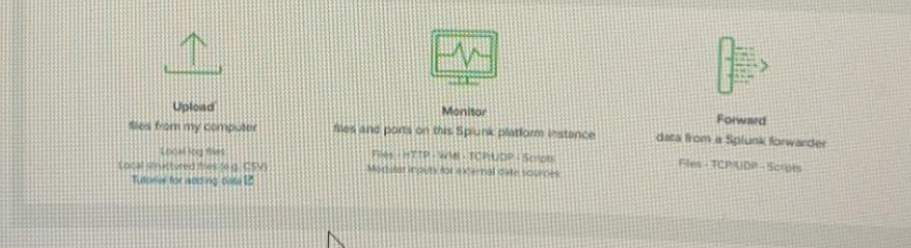
All these logs provide a wealth of information and can help in identifying security issues. Each SIEM solution has its own way of ingesting the logs. Some common methods used by these SIEM solutions are explained below:

- 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 listening port.



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

Or get data in with the following methods



Answer the questions below

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

`/var/log/httpd`

Correct Answer

This alert enables the analysts to take suitable actions based on the investigation. SIEM plays an important role in the Cyber detect and protect against the latest threats in a timely manner. It provides good visibility of what's happening within the network.

SIEM Capabilities

SIEM is one major component of a Security Operations Center (SOC) ecosystem, as illustrated below. SIEM starts by collecting 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 are:

- 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.

No answer needed

Correct



Type here to search



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 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 Al

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 ce 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. Once an alert is triggered, the events/flows associated with the alert are examined, and the rule is checked to see which investigation, the analyst determines if it's a True or False positive. Some of the actions that are performed after the anal

- 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

What type of alert may require tuning?

false alarm

Task 6 ☐ Lab Work

Task 7 ☐ Conclusion

Created by  tryhackme and  Dex01

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 6502 users are days old.



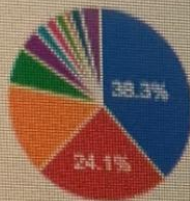
Type here to search



Introduction To SIEM

https://siem.internal/dashboard

Top 10 event codes

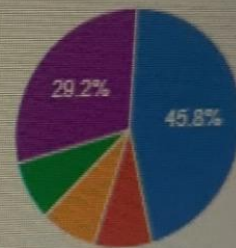


Alert
Potential CryptoMiner Activity Observed, find and click on the triggered event to show the details. [Find Event](#)

Number of events

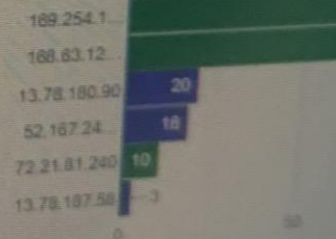


MITRE ATT&CK



Process Name	Count
chrome.exe	9,007
cmd.exe	3,187
svchost.exe	1,636
cmdminer.exe	1

IP+Port Destination



Introduction To SIEM

https://siem.internal/events

SourceModuleType	SeverityValue	index	SubjectDomainName	Channel
Win_event_log	2	winlogs	cyberteers.local	Windows
Win_event_log	2	winlogs	cyberteers.local	Windows
Win_event_log	2	winlogs	cyberteers.local	Windows
Win_event_log	2	winlogs	cyberteers.local	THM_SIAM
Win_event_log	2	winlogs	cyberteers.local	Windows
Win_event_log	2	winlogs	cyberteers.local	Windows

Introduction To SIEM

https://siem.internal/events

Event Type	Source Module Name	Host Name	User Name	Process Name	
AUDIT_SUCCESS	eventlog	HR_01	haroon	C:\Windows\System32\MicrosoftEdge5H.exe	In
AUDIT_SUCCESS	eventlog	Admin_02	Moin	C:\Program Files (x86)\java\jre1.8.0_181\bin\javaws.exe	In
AUDIT_SUCCESS	eventlog	IT_01	Bell	C:\Python3\python.exe	In
AUDIT_SUCCESS	eventlog	HR_02	Chris.fort	C:\Users\Chris.fort\temp\cudominer.exe	In
AUDIT_SUCCESS	eventlog	IT_02	Amelia	C:\Program Files\QuickTime\quicktime.exe	In
AUDIT_SUCCESS	eventlog	HR_03	Daina	C:\Program Files\QuickTime\qw.exe	In

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

Task 4 ✓ Why SIEM

Task 5 ✓ Analysing Logs and Alerts

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 if 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

Correct Answer

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

chris.fort

Correct

What is the hostname of the suspect user?

hr_02

Correct

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

miner

Correct

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

- False-Positive

- True-Positive

True-Positive

Correct

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

THM{000_SIEM_INTRO}

Correct

Task 7 ○ Conclusion

Created by tryhackme and Dex01

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 6502 users are days old.

Introduction to SIEM

An introduction to Security Information and Event Management.

100%

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, and what visibility it provides. To learn in-depth the following rooms and challenges.

- [Jr. SOC Analyst](#)
- [Splunk101](#)
- [Splunk201](#)
- [Benign](#)
- [InvestigatingwithSplunk](#)
- [InvestgatingwithELK](#)
- [ItsyBitsy](#)

Answer the questions below

Complete this room.

No answer needed

