

Setup Open Source SIEM

Assignment

1h30m - 2h



Status

Incomplete

Introduction

In this assignment, you will develop a list of networking and hardware requirements to install an open-source Security Information and Event Management (SIEM) system. The list should include the necessary components to support the installation and operation of the SIEM.

Developing a List of Networking & Hardware Requirements

Follow the instructions given here to create a list of requirements to install an open-source SIEM:

1. Research all the available open-source SIEM systems and identify the one that you think is most appropriate based on your understanding.
2. Determine the networking and hardware requirements necessary to support the installation and operation of the chosen open-source SIEM. Your list should include the following components:
 - Server requirements, including processor, RAM, and storage capacity.
 - Network requirements, including bandwidth and connectivity.
 - Additional hardware components, such as network adapters, hard drives, or specialized hardware.
3. Present your list of networking and hardware requirements in a written report. The report should include the following sections:
 - **Introduction:** Provide an overview of the importance of SIEM and the benefits of using open-source software.
 - **Networking and Hardware Requirements:** Present your list of networking and hardware requirements, including server, network, and additional hardware components.
 - **Conclusion:** Summarize your findings and discuss the potential implications for implementing SIEM in the organization.



The report must be developed in the Google Doc format.

Once the report is ready, you are encouraged to post the link to the Google Doc report on Discord for any peer feedback. You may also save the report to your PKM or professional portfolio.

✓ Mark Completed

How well did this activity help you to understand the content?

Let us know how we're doing



W08D3





Wed Aug 14

> Outline & Notes (1)

> Lectures (1)

✓ Work (4)

5 hrs

-  [Setup Open Source SIEM](#)
-  [Threat Defense Investigation & Research Report](#)
-  [Researching Cyber Security Attack](#)
-  [Sharing Research Findings](#)

W08D3 Schedule »