Top Five Hunt Hypothesis

Assignment

1h30m - 2h

✓ Status | Incomplete

Introduction

In this assignment, you will develop a hypothesis for identifying the top five cyber threats that require proactive threat hunting. The hypothesis should provide the understanding of the most significant cyber threats, their potential impact, and how to detect and prevent them.

Instructions for Creating Hypothesis

Follow the instructions given here to create your hypothesis:

1. Research and identify the top five cyber threats that require active hunting. These could be specific types of threats or vulnerabilities that are frequently exploited.
2. Develop a hypothesis that explains why these five cyber threats are significant and require threat hunting. Your hypothesis should address the following elements:
   - The potential impact of cyber threats on the organization's assets and operations.
   - The key indicators or signals that suggest the presence of the cyber threats.
   - The strategies or techniques that can be used to detect and prevent cyber threats.
3. Present your hypothesis in a brief report (about 3 pages long) that includes the following sections:
   - **Introduction**: Provide an overview of the importance of cyber threat hunting
   - **Hypothesis**: Present your hypothesis, including the potential impact of the cyber threats, key indicators, and detection/prevention strategies.
   - **Conclusion**: Summarize your findings and discuss the potential implications for cybersecurity practices.

> 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 on Discord for any peer feedback. You may also save the report to your PKM or professional portfolio for future references.

✓ Mark Completed

Previous

Next

← Reactive vs Proactive Threat Detection

Introduction to SIEM Systems →

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

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W08D2

Tue Aug 13

› Lectures (1)

⌄ Work (3)

4 hrs

- </> Top Five Hunt Hypothesis
- Introduction to SIEM Systems
- SIEM Architecture & Implementation

W08D2 Schedule »