Threat Hunting

Task:

Establish a threat hunting program to proactively search for signs of compromise within the network.

What is Threat Hunting?

Threat hunting is a cybersecurity approach where analysts actively search for hidden threats within an organization's network. Instead of waiting for security alerts, threat hunters proactively look for indicators of compromise (IOCs) and suspicious activities to detect and mitigate cyber threats early.

Steps to Establish a Threat Hunting Program

1. Define Objectives and Scope

Determine what threats to hunt for and which systems to monitor.

2. Collect and Analyze Data

Use SIEM tools to gather logs, network traffic, and endpoint activity.

3. Identify Indicators of Compromise (IOCs)

Search for suspicious behaviors, anomalies, and known attack patterns.

4. Investigate and Respond

Analyze findings, validate threats, and take necessary mitigation actions.

5. Improve and Automate

Refine hunting techniques and integrate automation for continuous improvement.

Threat Hunting Resources:

- MITRE ATT&CK Framework: https://attack.mitre.org/
- Threat Hunting Framework: https://www.sans.org/cyber-security-courses/threat-hunting/
- Elastic Security for Threat Hunting: https://www.elastic.co/security
- Zeek (formerly Bro) Network Security Monitor: https://zeek.org/