# **Threat Hunting Checklist Outline**

1. Preparation Phase:

* Identify and Document Objectives:
* Define the specific goals and objectives of the threat hunting exercise.
* Assemble Threat Hunting Team:
* List the individuals and roles involved in the threat hunting process.

1. Data Collection:

* Define Data Sources:
* Specify the sources of data to be monitored (logs, network traffic, etc.).
* Data Aggregation:
* Detail how data will be collected and aggregated for analysis.

1. Threat Intelligence Integration:

* Incorporate Threat Intelligence:
* Specify the threat intelligence feeds and sources to be used.
* Determine how threat intelligence will be applied to enhance hunting.

1. Tool and Technology Setup:

* Select Threat Hunting Tools:
* List the tools and technologies to be used for threat hunting.
* Ensure they are properly configured and updated.

1. Execution Phase:

* Continuous Monitoring:
* Outline the schedule and frequency of monitoring.
* Specify the time duration for threat hunting exercises.

1. Analysis Procedures:

* Behavioral Analysis:
* Describe methods for detecting abnormal behavior or deviations.
* Signature-based Analysis:
* Explain how known threat signatures will be used in the analysis.
* Anomaly Detection:
* Detail the approach for identifying anomalies in the data.

1. Incident Response Planning:

* Incident Triage:
* Define the process for prioritizing and categorizing incidents.
* Communication Plan:
* Outline how the team will communicate and escalate findings.

1. Documentation and Reporting:

* Record Findings:
* Specify how identified threats and incidents will be documented.
* Reporting Structure:
* Outline the structure and content of threat hunting reports.
* Include key metrics and observations.

1. Post-Threat Hunting Activities:

* Lessons Learned:
* Conduct a debriefing session to discuss lessons learned.
* Continuous Improvement:
* Detail how the threat hunting process will be refined based on findings.

1. Legal and Ethical Considerations:

* Ensure Compliance:
* Confirm that threat hunting activities comply with legal and ethical standards.
* Privacy Measures:
* Detail how privacy of individuals and sensitive data will be protected.