

Threat Hunting Procedure Template

Threat hunting is a proactive and iterative approach of searching networks, devices, endpoints, and datasets to identify and isolate the cyber threats that have entered a network by evading the current security systems.

Details of the Organization	
Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Details of the Incident Responder			
Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

Hypothesis	
Attackers TTP:	
Network and System Logs: (Describe in detail)	
Tools Used:	

Type of Threat Identified:				
Severity of the Threat:	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High	<input type="checkbox"/> Critical

Threat Data Collection and Processing

Tasks Performed:	
Considerations:	
Tools Used:	

Threat Analysis

Tasks Performed:	
Considerations:	
Tools Used:	
Identified Malicious Activity:	

Questions that needs to be answered

Considering the threat-hunting procedure, the organization affected by the incident should answer the following questions:

Who is responsible for the threat?	
What is the type of the threat?	
What are the actions taken to resolve?	
Who will be affected by the threat?	
What is the effect and impact of the threat?	
What procedure will be used to record log data?	
What can be identified by analyzing the logs?	

Details of the Investigation

Threat Code:		
Threat Name:		
Tools Used:		
Performed By	Threats Eliminated	Actions Taken

--	--	--

Recommended Resolution Actions		
Performed By	Date	Action Taken

Conclusion

[Conclusion of the assessment process.]

--

Incident Handler's Signature

Date