Threat Hunting Practice

1. Objective

This report contains the details of the task includes Hypothesis Development, Threat Intelligence Hunt, and Hunting Report. The goal of this task is to:

- Develop skills to proactively identify threats using structured methodologies and data analysis.

2. Introduction

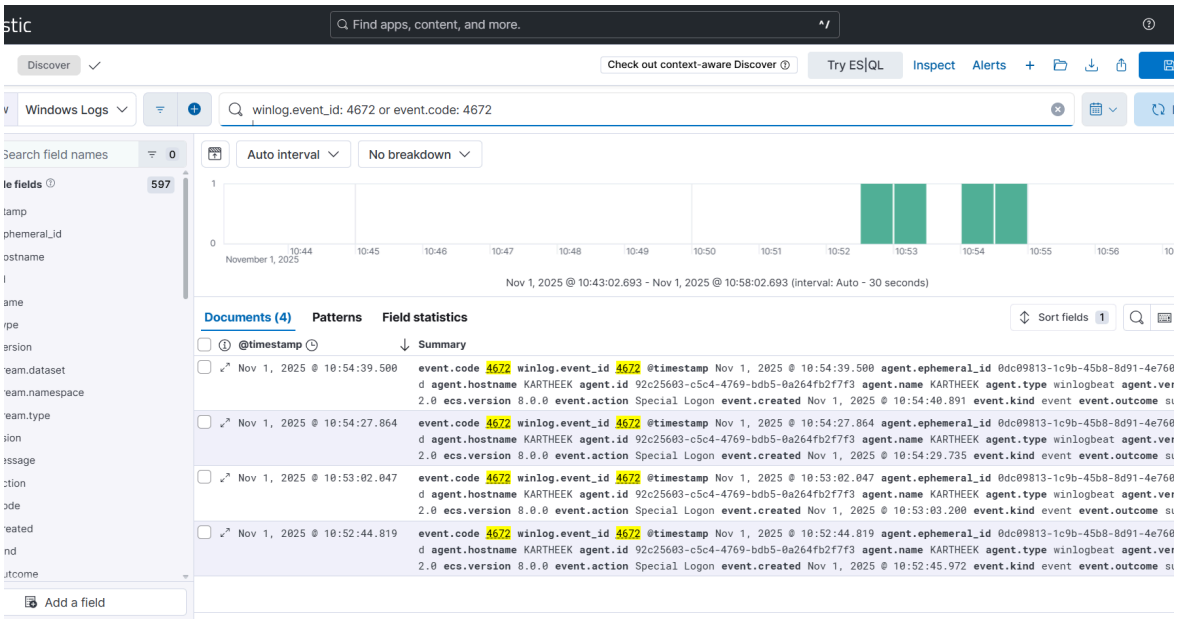
Threat hunting is a proactive security discipline focused on identifying malicious behavior that is better than traditional detection mechanisms. Instead of waiting for alerts, analysts apply hypotheses, threat intelligence, and deep log analysis to uncover suspicious activity across the environment. By combining investigative tools like Elastic Security, Velociraptor, and AlienVault OTX, hunters validate evidence, correlate telemetry, and document findings that directly strengthen detection capabilities. This practice enhances SOC readiness and aligns defensive improvements with real attacker techniques such as MITRE ATT&CK T1078 (Valid Accounts).

3. Tools

- Elastic Search setup using its official documentation.
  https://www.elastic.co/downloads/elasticsearch
- Velociraptor set it using its download documentation.
  https://docs.velociraptor.app/downloads/
- AlienVault OTX used it from a web browser.
  https://otx.alienvault.com/

4. Hypothesis Development

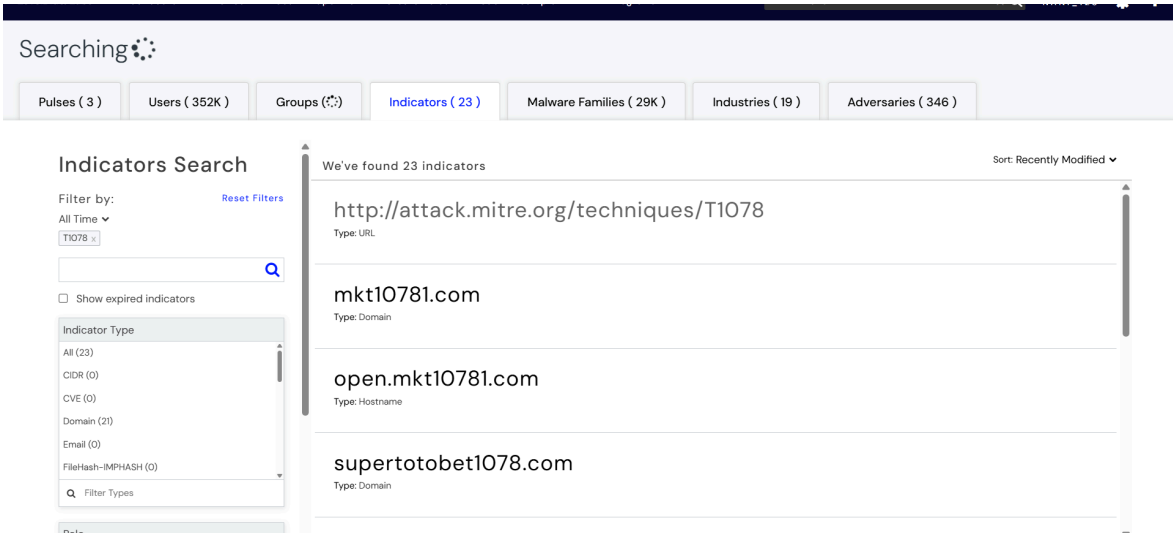
Hypothesis development is a proactive threat hunting that it is better than reactive threat hunting. Guessing about potential threats to guide threat hunting and security analysis. Hypothesis development is not works on random guesses; they are informed by threat intelligence, network observations, SIEM tools etc. Developing a hypothesis allows analysts to create a structured plan with specific evidence to search for, making hunting more efficient. Now the task includes formulating a hypothesis (e.g., “Unauthorized privilege escalation in domain accounts”). Querying elastic search for event ID 4672 (role assignment).

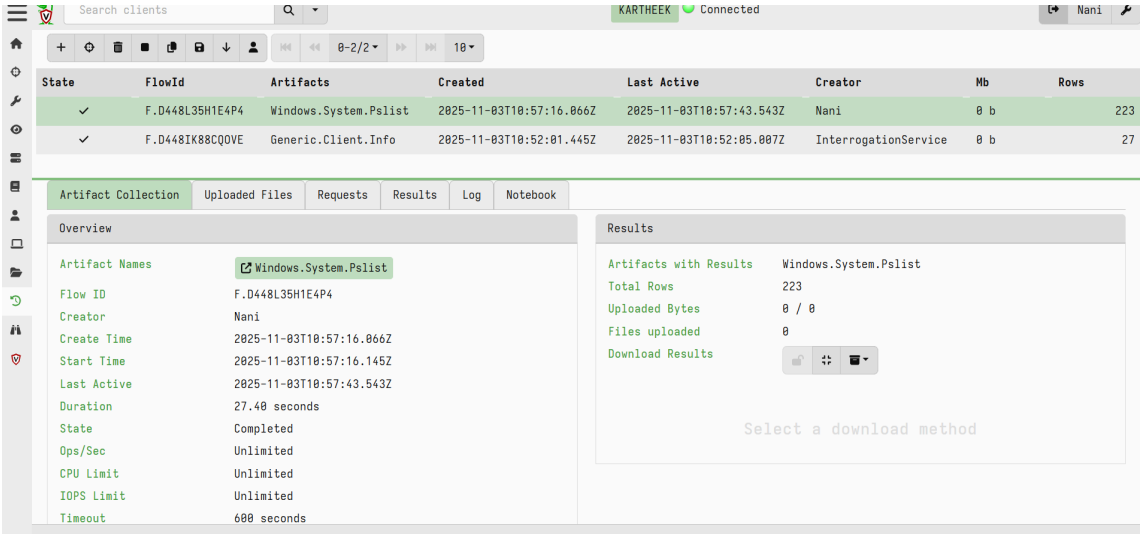


Timestamp	User	Event ID	Notes
2025-11-01	Kartheek	4672	Unexpected admin role

6. Threat Intelligence Hunt

Using AlienVault OTX which is a threat intelligence tool used for searching T1078 IOCs (e.g., Suspicious IPs). I performed cross reference with Velociraptor tool to check for the tactic ID using Velociraptor Query Language and the query I used is (SELECT * FROM processes).





7 Hunting Report

During a proactive threat hunting exercise focused on Valid Accounts (MITRE ATT&CK T1078), we identified suspicious privilege escalation activity within the domain environment. Log analysis in Elastic Security revealed Event ID 4672 assigned to the user testuser at an unusual time with no associated change request. This behavior suggested potential misuse of legitimate credentials for unauthorized access. Threat intelligence from AlienVault OTX indicated related IOCs tied to credential compromise. Velociraptor process queries showed no immediate persistence, though investigation continues. The account was temporarily restricted, and enhanced monitoring rules were deployed to detect further unauthorized privilege activities.