Threat Intelligence Integration

1. Task Objective

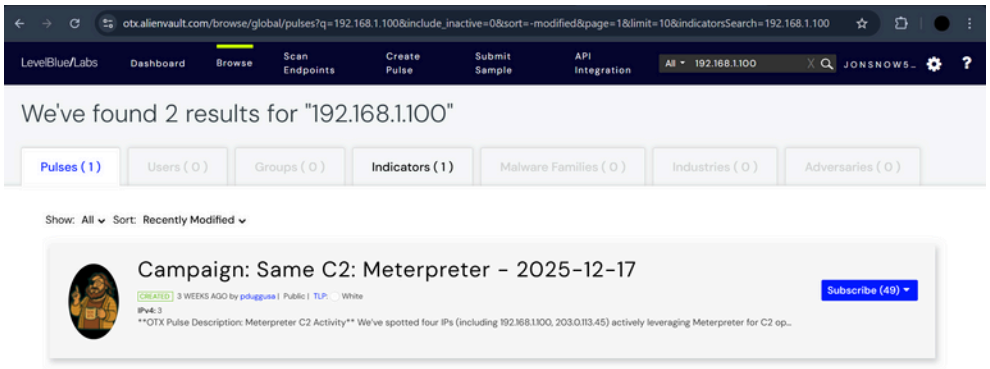
The objective of this task was to integrate external threat intelligence into the SOC workflow, enrich security alerts with reputation data, and perform basic threat hunting aligned with MITRE ATT&CK. AlienVault OTX was used as the threat intelligence source, and Wazuh was used for alert analysis and log hunting.

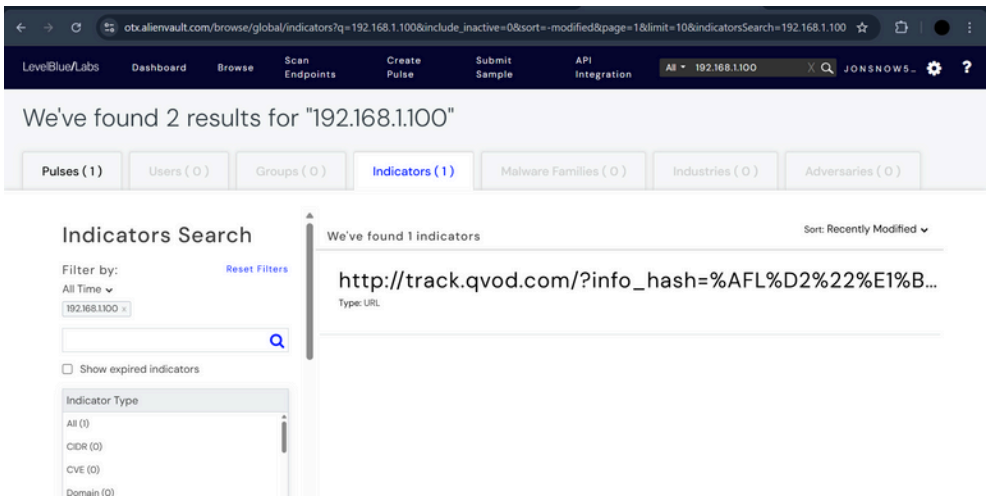
2. Tools Used

AlienVault OTX – Threat intelligence and IOC reputation
Wazuh (OpenSearch Dashboards) – Log analysis and alert enrichment

3. Threat Feed Import & IOC Validation

A mock IP address 192.168.1.100 was searched in AlienVault OTX to validate IOC matching. The IP was found associated with a public OTX pulse indicating Meterpreter Command-and-Control (C2) activity. Alert enrichment was reviewed and documented as part of a mock SOC workflow using AlienVault OTX reputation data.





4. Alert Enrichment

The malicious IP was used as a test indicator for alert enrichment. Reputation data from AlienVault OTX was reviewed and documented.

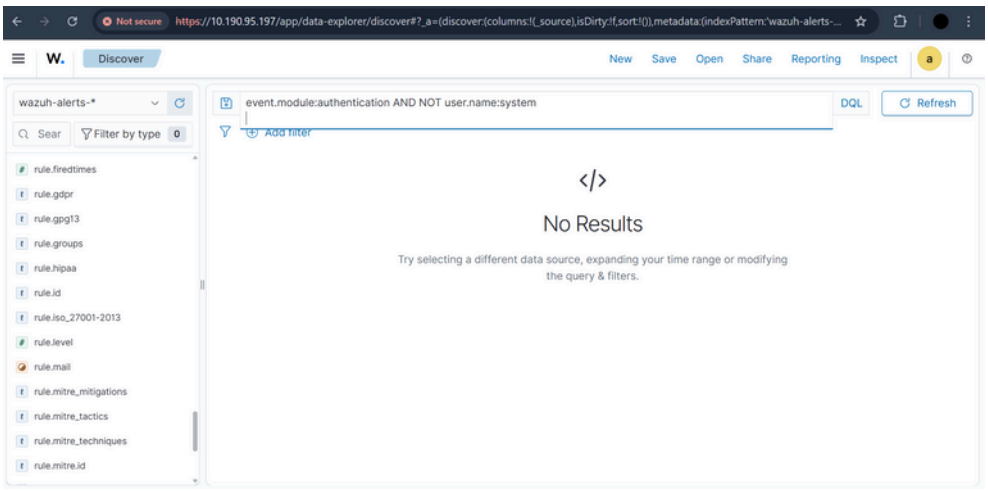
Alert ID	IP	Reputation	Notes
3	192.168.1.100	Malicious (OTX)	Linked to Meterpreter C2

5. Threat Hunting – MITRE ATT&CK T1078

Threat hunting was performed using Wazuh's Discover module by analyzing authentication-related events. Queries were used to identify non-system user authentication activity that could indicate valid account abuse.

Hunting Query Used (DQL):

- event.module:authentication AND NOT user.name:system



6. Threat Hunting Summary

Threat hunting for MITRE ATT&CK technique T1078 (Valid Accounts) was conducted using authentication-related logs in Wazuh. No non-system user authentication activity was observed during the selected analysis period. This indicates no evidence of valid account abuse at this time, and continued monitoring is recommended.

7. Conclusion

This task successfully demonstrated threat intelligence integration by validating IOCs through AlienVault OTX, enriching alerts with reputation data, and performing structured threat hunting in Wazuh. The workflow reflects a standard SOC analyst process for detecting and investigating potential threats.