Threat Intelligence Integration Report

1. Executive Summary

This report documents the integration of external threat intelligence into Wazuh using AlienVault OTX feeds. A malicious IP address (192.168.1.100) was detected and enriched with threat intelligence data. Threat hunting identified activity aligned with MITRE ATT&CK technique T1078 (Valid Accounts), indicating potential credential misuse or account compromise.

2. Environment and Tools

- SIEM: Wazuh
- Threat Intel: AlienVault OTX
- Data Sources: Authentication logs, network traffic logs
- Framework: MITRE ATT&CK

3. Threat Feed Integration

AlienVault OTX threat feeds were imported into Wazuh. The integration enabled real-time matching of IOCs such as malicious IP addresses against incoming logs.

Test IOC:

- **IP Address:** 192.168.1.100

Result:

- Wazuh successfully matched the IP against AlienVault OTX pulses.
- The IP was flagged as malicious.
- An alert was generated for further investigation.

Alert ID	IP	Reputation	Notes
003	192.168.1.100	Malicious (OTX)	Linked to C2 server

Table 1: Alert

4. Threat Hunting

MITRE ATT&CK Technique

- **Technique ID:** T1078
- **Name:** Valid Accounts
- **Tactic:** Defense Evasion / Persistence / Privilege Escalation

Observations

- Authentication events were observed from non-system user accounts
- Repeated login activity patterns were identified
- Behavior was inconsistent with normal baseline user activity

5. Recommended Actions

- Reset credentials for affected user accounts.
- Enable Multi-Factor Authentication (MFA).
- Block malicious IP (192.168.1.100) at firewall and endpoint level or using CrowdSec.
- Increase monitoring for authentication anomalies.

6. Conclusion

Threat hunting revealed activity consistent with MITRE ATT&CK T1078 (Valid Accounts), where non-system user accounts performed repeated authentication actions. Combined with malicious IP intelligence from AlienVault OTX, this suggests possible credential compromise or unauthorized access, warranting deeper investigation and credential review.