Threat Intelligence Integration Report

Threat Feed Import

Threat intelligence feeds from AlienVault OTX were integrated into the SIEM platform to enhance detection capabilities. The OTX feed provides indicators of compromise such as malicious IP addresses, domains, and hashes.

For testing purposes, a mock IP address (192.168.1.100) was used to simulate IOC matching within Wazuh alerts.

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

Alert Enrichment Analysis

The Wazuh alert was enriched using AlienVault OTX threat intelligence. The source IP was identified as malicious and associated with command-and-control infrastructure. Enrichment adds valuable context to alerts, allowing SOC analysts to prioritize incidents and accelerate response decisions.

Threat Hunting Activity – T1078 (Valid Accounts)

Threat hunting was conducted to identify potential misuse of valid accounts. Logs were queried for suspicious user activity using the condition:

```
user.name != "system"
```

Threat hunting revealed multiple non-system account login events outside normal usage patterns. Although no confirmed compromise was identified, the activity warranted further monitoring. Hunting using MITRE ATT&CK technique T1078 helps detect credential misuse that may bypass traditional signature-based detection.