Threat Hunting Summary (Task 2.4)

A. Document Name

Task 2: Threat Hunting Summary

B. Purpose

This document highlights the findings of threat hunting performed for MITRE ATT&CK technique **T1078 – Valid Accounts**, which focuses on detecting misuse or brute-force attempts against valid user credentials.

C. Summary

AlienVault OTX threat feeds were integrated into Wazuh to provide IOC-based enrichment. A malicious IP was successfully matched and flagged. Threat hunting for T1078 revealed non-system account activity but no malicious authentication behavior. No OTX-referenced threats were detected, though continuous monitoring is recommended.