Document 3: Alert Enrichment Table (Task 2.3)

A. Purpose

The purpose of this task is to demonstrate how a Threat Intelligence (CTI) tool such as **AlienVault OTX** can be used to enrich a raw security alert with additional context. This simulates how an analyst would use Cortex or similar platforms to validate and understand alerts in real-world scenarios.

A simulated event was generated containing the mock IP.
Wazuh parsed it through the OTX integration, adding reputation fields to the alert.

B. Alert Enrichment Table

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

Explanation:

- Wazuh received the alert (ID: 003).
- The OTX plugin enriched it with reputation data.
- The mock IP was labeled **Malicious** because it matched an OTX pulse entry.
- The alert was escalated for investigation due to possible C2 (Command-and-Control) activity.