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.

B. Alert Enrichment Table

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

Explanation:

The CTI lookup (simulated using AlienVault OTX) identified the IP **192.168.1.100** as **malicious**, associated with a **Command and Control (C2)** server. This enrichment provides essential context to the alert, helping analysts prioritize incidents and take quick mitigation actions.