Threat Intelligence Integration

1. Objective

This report contains the details of the task includes Threat Feed Import, Alert Enrichment, and Threat Hunting. The goal of this task is to:

- Build proficiency in leveraging threat intelligence to enhance detection and response.

2. Introduction

Threat Intelligence Integration is a continuous process of feeding the information about threats to enhance and automate the organization's security defense .It feeds analyzed threat Data such as IOCs, and threat actors tactics to various defense tools to improve the detection, response , and overall risk management.

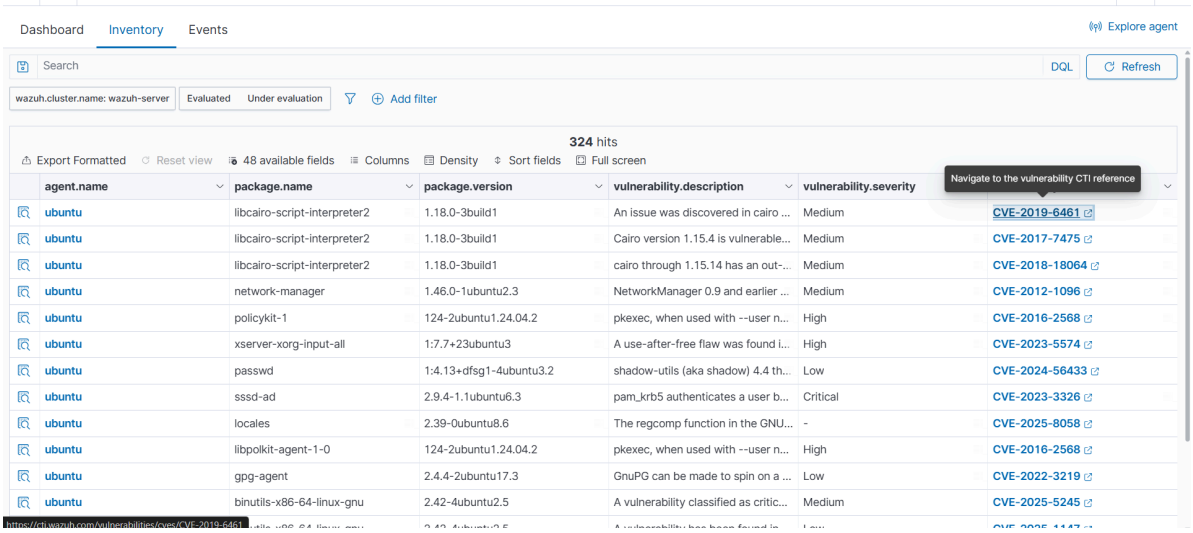
3. Tools

- Wazuh setup using Wazuh official documentation
  https://documentation.wazuh.com/current/quickstart.html
- AlienVault OTX
  https://otx.alienvault.com/
- TheHive is a Security Incident Response Platform (SIRP) tool. Setup using TheHive documentation.
  https://docs.strangebee.com/thehive/installation/installation-guide-linux-standalone-server/

4. Threat Feed Import

Importing an Alienvault OTX feed into Wazuh to match Indicators of Compromise (IOCs). Threat Feed Import this process includes creation of a python script used to import the feeds of Alienvault OTX. In the Wazuh manager configuration file add the integration code to make Wazuh to accept the feeds from the OTX. For this entire process it is necessary to have an API Key of Alienvault OTX.

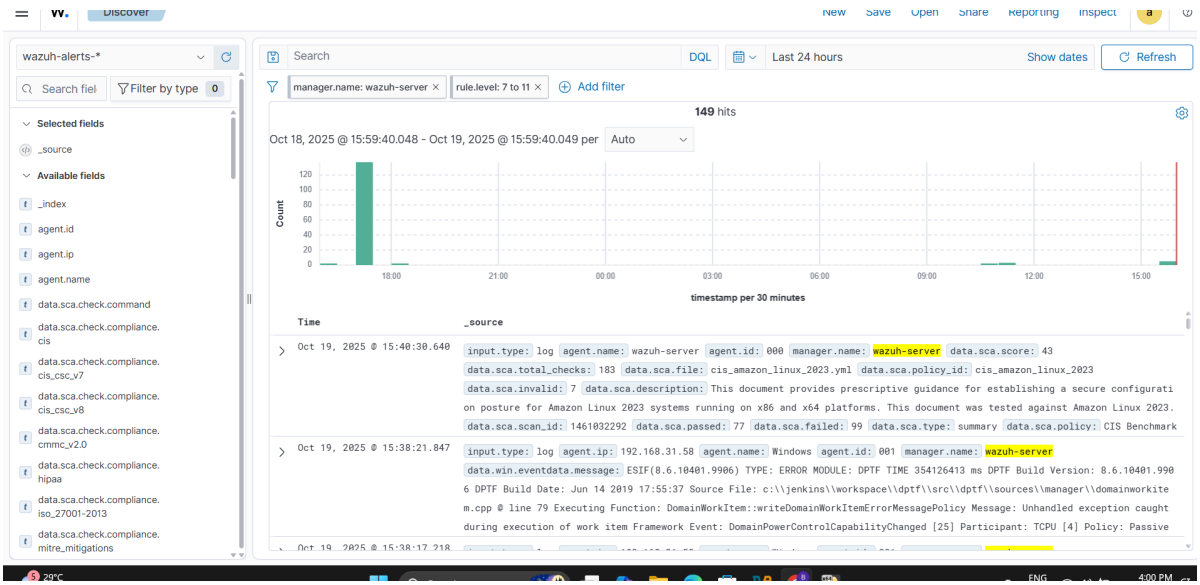
It is a continuous process of sending feeds to the SIEM tool to enhance the security defense, and to know the attackers tactics. It feeds already analyzed data that includes IOCs (IPs, domains, URLs, hashfiles). This data is very important to know the techniques used by attackers.



4.1 Alert Enrichment

Alert Enrichment is a process of adding contextual information into the raw alerts to make them more understandable. It involves automatically sending a basic alert with additional information, such as threat intelligence, asset details, or operational details to help SOCs and IT teams quickly investigate, and resolve issues.

Alert enrichment is important because it helps to understand the alerts and its reason for generating alerts. With the structured information the Organization's respond to the alerts immediately.



4.2 Metadata of the Alert

The table below shows the metadata that includes the Alert ID, IP, Reputation, and Notes. This metadata is important because it provides context for data, making it easier to find, and understand.

Alert ID	IP	Reputation	Notes
003	192.168.31.58	Malicious(OTX)	C2 Server

4.3 Threat Hunting

Threat Hunting is a proactive practice where analysts actively search an organization's network for any hidden or unknown threats that have bypassed automated tools. It is done by using both Manually and automatically. The goal is to find the advanced adversaries and stop them before they create any damage to the organization.