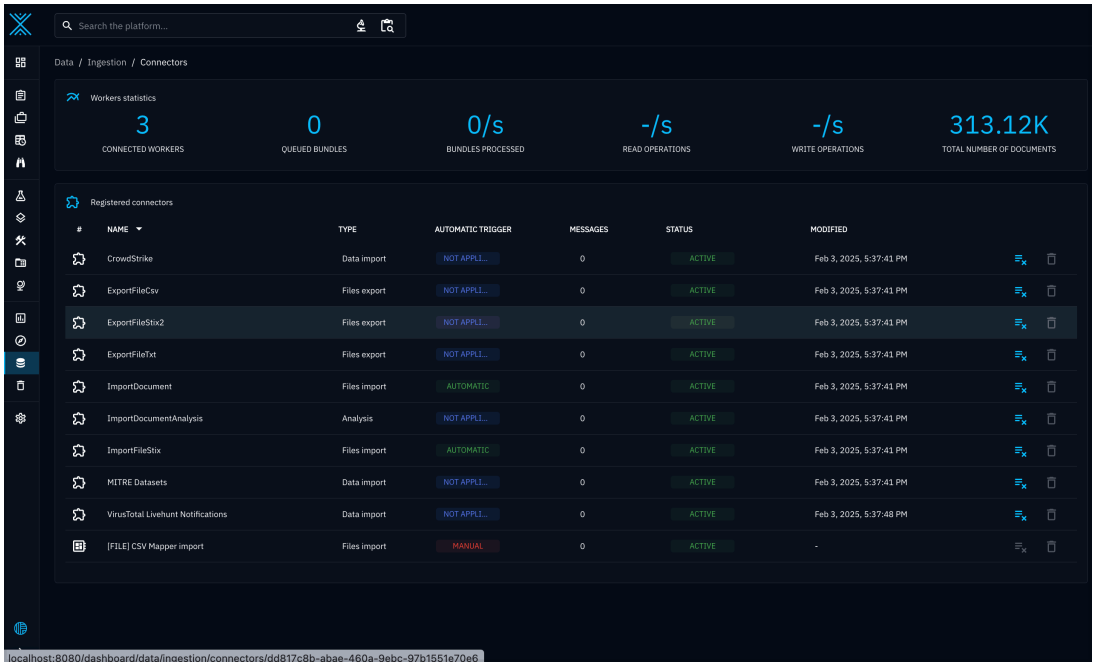
Implement Threat Intelligence Principles

1. Introduction

Threat intelligence helps organizations detect, analyze, and prevent cyber threats. This report covers the analysis of two Indicators of Compromise (IoCs), detection methods, and the implementation of OpenCTI for managing threat intelligence data.

Dashboard where you see all the different connectors and its processes.



Shows the specific Connectors that are used in the dashboard

2. Indicators of Compromise (IoCs) and Detection Methods

IoCs are pieces of forensic data that indicate a system breach. Two IoCs analyzed in this project are:

2.1 IoC 1: Malicious IP Address

- **IP:** 192.168.100.50 (Example IP for analysis)
- **Detection Method:**
  - Used **VirusTotal** to check reputation.
  - **CrowdStrike** provided contextual threat intelligence.
  - The IP was flagged for hosting phishing content.
- **Threat Indication:** If detected in network logs, it suggests an attempted attack or unauthorized access.

2.2 IoC 2: Malicious File Hash

- **SHA-256 Hash:** 3a5f...b3d9 (Example hash for analysis)
- **Detection Method:**
  - Uploaded to **VirusTotal** for multi-engine scanning.
  - Correlated with **MITRE ATT&CK** framework for attack patterns.
  - Results showed it was associated with a known malware variant.
- **Threat Indication:** If detected on a system, it indicates a malware infection.

3. OpenCTI Threat Intelligence Platform Implementation

OpenCTI is an open-source platform for managing cyber threat intelligence. We implemented OpenCTI using **Docker** for easy deployment and configured two connectors.

3.1 Installation Using Docker

- Installed Docker and Docker Compose.
- Cloned OpenCTI repository:
  git clone https://github.com/OpenCTI-Platform/docker.git
- cd docker
- Started OpenCTI with:
  docker-compose up -d

3.2 Configured Connectors

Two connectors were integrated to automate intelligence gathering:

Connector 1: MITRE ATT&CK

- Pulls adversary tactics and techniques into OpenCTI.
- Provides threat context based on the MITRE ATT&CK framework.

Connector 2: VirusTotal

- Allows automated scanning of file hashes and URLs.
- Enables quick IoC validation from OpenCTI's interface.

Configuration for VirusTotal connector:

```
{
  "connector_id": "virustotal",
  "api_key": "your_api_key_here",
  "base_url": "https://www.virustotal.com/api/v3"
```

}

3.3 Basic Usage Demonstration

- Uploaded IoCs into OpenCTI.
- Used VirusTotal connector to check file hash reputation.
- Cross-referenced threat data with MITRE ATT&CK.
- Created threat reports summarizing intelligence findings.

4. Conclusion

By using **MITRE ATT&CK**, **CrowdStrike**, and **VirusTotal**, we successfully analyzed IoCs and detected threats. Implementing **OpenCTI** with **Docker** enabled efficient threat intelligence management, allowing real-time IoC correlation and threat analysis. This setup enhances cybersecurity defenses by automating threat detection and response.