# Documenting Threat Intelligence through Practical Implementation

Date: June 23, 2025

## Indicator of Compromise (IoC) 1: Suspicious IP Addresses

Overview:

Suspicious or malicious IP addresses are critical indicators of threats such as Command-and-Control (C2) activity, malware distribution, and phishing campaigns.

Detection Methods:

1. Network Traffic Monitoring: Tools like Wireshark and Suricata detect traffic to/from known bad IPs.

2. Threat Feeds: Integrated feeds from VirusTotal, MISP, and others help flag IPs associated with malware or DDoS.

How It Indicates Threats:

- C2 communication signals device compromise.

- IPs involved in malware delivery or phishing increase threat likelihood.

## Indicator of Compromise (IoC) 2: Malicious File Hashes

Overview:

File hashes (MD5/SHA1/SHA256) uniquely identify files. Known malware hashes are essential for threat detection.

Detection Methods:

1. Antivirus and EDR: CrowdStrike, Windows Defender scan files and compare against known hash

databases.

2. Sandboxing: Tools like Cuckoo Sandbox analyze file behavior and hash matches.

3. Threat Intelligence: VirusTotal and MISP feeds list hashes linked to specific threats.

How It Indicates Threats:

- Presence of malware or backdoors.

- Detection of ransomware binaries or persistence mechanisms.

**OpenCTI Threat Intelligence Platform Implementation**

Setup Method: Docker-based installation.

Steps:

1. Cloned OpenCTI GitHub repository.

2. Used Docker Compose to deploy containers.

3. Verified access via browser on localhost:8080.

Connectors Implemented:

1. MITRE ATT&CK Connector - imports attack techniques.

2. CISA Known Exploited Vulnerabilities - feeds known threat data.

Verification:

- Connectors synced successfully (see attached screenshots).

- IOC data was ingested and visualized within the platform.

Usage Demo:

- Search for a known IP address or file hash.

- Visualize threat relations and history using OpenCTI's graph and dashboard views.

Documentation & Evidence:

- Screenshots of Docker Compose running.
- Evidence of data retrieved from both MITRE ATT&CK and CISA connectors.
- Queries on IPs and hashes with contextual threat enrichment.

Conclusion:

This project demonstrates the ability to analyze and respond to Indicators of Compromise using modern detection methods and tools. Implementation of OpenCTI with two threat intelligence connectors highlights operational understanding of threat ingestion, correlation, and visualization. With these capabilities, security teams can proactively defend against threats using validated intelligence workflows.