

Okay, I can help you structure the report based on the provided `docker-compose.yml` file. Here's a suggested outline, incorporating the requirements from your prompt and mapping it to the content of the file.

Report: Implementation of Threat Intelligence Principles

1. Introduction

- Briefly define threat intelligence and its importance.
- State the purpose of the report: to document the implementation of threat intelligence principles, including IoC analysis and OpenCTI platform setup.
- Outline the key components of the project:
 - Analysis of 2 Indicators of Compromise (IoCs)
 - OpenCTI Platform Implementation
 - Connector Configuration
 - Documentation of Setup and Usage

2. Analysis of Indicators of Compromise (IoCs)

- *(This section will be filled in by you, based on your chosen IoCs)*
- **2.1 IoC #1: [Your IoC #1 - e.g., a specific IP address]**
 - Description of the IoC
 - Detection Methods (e.g., firewall logs, IDS signatures)
 - How it indicates a threat (e.g., communication with a known C2 server)
- **2.2 IoC #2: [Your IoC #2 - e.g., a file hash]**
 - Description of the IoC
 - Detection Methods (e.g., antivirus scans, EDR)
 - How it indicates a threat (e.g., associated with known malware)

3. OpenCTI Platform Implementation

- **3.1 Platform Setup**
 - Method Used: Docker Compose (as per the provided file)
 - Documentation of Setup:
 - Explain the purpose of the `docker-compose.yml` file.
 - Describe the services defined in the `docker-compose.yml` (Redis, Elasticsearch, Minio, RabbitMQ, OpenCTI, Worker)
 - Detail the configuration of each service (e.g., environment variables, volumes, ports, dependencies, health checks)

- Provide steps to deploy the platform using Docker Compose (e.g., `docker-compose up -d`)
 - Evidence of Functionality:
 - Screenshots of successful deployment (e.g., `docker-compose ps` output)
 - Screenshot of the OpenCTI dashboard (as in the provided file)
- **3.2 Connector Integration**
 - Configuration of 2 Connectors: *(This section will be filled in by you, based on your chosen connectors from the file)*
 - **3.2.1 Connector #1: [Your Connector #1 Name]**
 - Purpose of the connector (e.g., import STIX files)
 - Configuration details (referencing the `docker-compose.yml` file - e.g., environment variables like `OPENCTI_URL`, `OPENCTI_TOKEN`, `CONNECTOR_ID`, etc.)
 - Documentation of integration steps
 - Evidence of functionality (e.g., screenshots of data being imported/exported)
 - **3.2.2 Connector #2: [Your Connector #2 Name]**
 - Purpose of the connector (e.g., import documents)
 - Configuration details (referencing the `docker-compose.yml` file)
 - Documentation of integration steps
 - Evidence of functionality
- **3.3 Basic Usage Demonstration**
 - Describe basic operations within OpenCTI (e.g., creating objects, searching, relationships)
 - Provide screenshots to illustrate usage (some are already in the file)

4. Conclusion

- Summarize the project's achievements.
- Discuss any challenges encountered and how they were addressed.
- Reflect on the importance of threat intelligence platforms like OpenCTI.

Appendices

- `docker-compose.yml` file (as provided)

- Any other relevant configuration files or scripts.

Important Notes for Filling in the Blanks:

- **IoC Analysis:** You'll need to research and provide actual IoCs, their detection methods, and how they indicate threats. This is the core analytical part of your work.
- **Connector Selection:** Choose two connectors from the `docker-compose.yml`. Here are some options from the file:
 - `connector-export-file-stix`
 - `connector-export-file-csv`
 - `connector-import-file-stix`
 - `connector-import-document`
 - `connector-analysis`
 - `connector-cisa-known-exploited-vulnerabilities`
 - `connector-opencti`
- For each connector, explain its purpose and how it's configured using the environment variables defined in the `docker-compose.yml`.
- **Evidence:** Provide screenshots and logs to demonstrate the successful setup and operation of OpenCTI and the connectors.

I'm ready to help further as you provide the specifics of your IoCs and connector choices! Just let me know what you'd like to work on next.

Sources and related content

[png2pdf \(4\)](#)



[PDF](#)

write a document and a code

Analysis
Analysis

- Query successful

Okay, here's a draft of the report, including code from the `docker-compose.yml` file and placeholders for the information you'll provide.

Report: Implementation of Threat Intelligence Principles

Apr 23, 1:58 PM

Try again without Canvas

This report provides a structured framework for documenting your threat intelligence project. Fill in the bracketed sections with the specific details of your IoC analysis, connector selection, and OpenCTI usage. Let me know if you have any questions or need further assistance