Okay, let's break down how to approach this threat intelligence project based on your requirements.

1. Analysis of 2 Indicators of Compromise (IoCs)

Here's a structured way to analyze two IoCs:

- **IOC 1: A Malicious IP Address**
    - **Example:** 192.168.100.123
    - **Detection Methods:**
        - **Firewall Logs:** Examine firewall logs for connections to or from this IP address.
        - **Intrusion Detection Systems (IDS):** IDS like Snort or Suricata can be configured to alert on traffic involving this IP.
        - **Endpoint Detection and Response (EDR):** EDR tools can detect processes on endpoints communicating with this IP.
    - **How it Indicates a Threat:**
        - Communication with a known malicious IP could indicate:
            - Command and Control (C&C) activity (malware receiving instructions).
            - Data exfiltration (sensitive data being sent to the attacker).
            - Reconnaissance activity (attacker scanning the network).
- **IOC 2: A Malicious File Hash**
    - **Example:** SHA256 hash: a1b2c3d4e5f6...
    - **Detection Methods:**
        - **Antivirus Scanners:** Antivirus software compares file hashes to its database of known malware.
        - **Endpoint Detection and Response (EDR):** EDR can detect the presence of files with this hash on endpoints.
        - **File Integrity Monitoring (FIM):** FIM tools monitor critical files for changes, including changes to their hashes.
    - **How it Indicates a Threat:**
        - A file with a known malicious hash is a strong indicator of malware. This could be:
            - A virus or worm.
            - Ransomware.
            - A trojan horse.

Documentation for IoC Analysis:

For each IoC, create a document that includes:

- The specific IoC value.
- A detailed description of the detection methods used.
- An explanation of how the IoC indicates a threat, including potential attack scenarios.
- Evidence (screenshots, log excerpts, etc.) to support your analysis.

2. OpenCTI Platform Implementation

You have the choice of Docker or system installation. Docker is generally easier for setup.

- **OpenCTI with Docker**
    - **Installation:**
        - Follow the official OpenCTI documentation for Docker installation. This will involve using `docker-compose`.
        - Documentation should include:
            - Docker version used.
            - `docker-compose.yml` file (or relevant configuration).
            - Commands used for installation (e.g., `docker-compose up -d`).
            - Screenshots of successful container startup.
    - **Connector Configuration (2 Connectors):**
        - Choose two connectors (e.g., MISP, VirusTotal, or a threat feed connector).
        - Document the configuration process for each connector:
            - Connector name and version.
            - Any API keys or credentials required.
            - Configuration file snippets.
            - Screenshots of the connector configuration within OpenCTI.
    - **Basic Usage Demonstration:**
        - Demonstrate the following in OpenCTI:
            - Importing the IoCs you analyzed in Part 1.
            - Searching for information related to the IoCs.
            - Visualizing the IoCs in the OpenCTI graph.
            - Showing how the connectors enrich the IoC data (e.g., VirusTotal adding reputation information).
        - Include screenshots of each step.

Key Documentation Points for OpenCTI:

- **Platform Setup:** Detailed steps taken to install OpenCTI (Docker or system). Include any troubleshooting encountered and how it was resolved.
- **Connector Integration:** Configuration details for each connector, including any specific settings or API keys.
- **Usage Demonstration:** Screenshots and descriptions of how you imported, searched for, and visualized the IoCs, and how connectors added value.

Important Considerations:

- **Evidence:** Back up your work with evidence. Screenshots, log excerpts, configuration files, etc., are crucial.
- **Clarity:** Write clear and concise documentation. Assume the reader has some technical knowledge but needs to be guided through your specific implementation.
- **Security:** Be mindful of security best practices. Do not expose sensitive information (like API keys) in your documentation.
- **Official Documentation:** Always refer to the official documentation for OpenCTI and the connectors you use.

This comprehensive approach should provide you with a solid foundation for your threat intelligence project!