1. Indicators of Compromise (IoC) Analysis

IoC 1: 3PARA RAT

- **Description:** 3PARA RAT is a remote access tool (RAT) written in C++ used by Putter Panda.
- **Detection Method:**
    - Analyzed through OpenCTI for correlation with known intrusion sets.
    - Verified against threat intelligence feeds, including MITRE ATT&CK and CISA alerts.
    - Cross-referenced with VirusTotal for hash and signature detection.
- **Threat Indicators:**
    - Classified as a Remote Access Trojan (RAT).
    - Possible persistence mechanisms via system registry modifications or scheduled tasks.
- **Potential Impact:**
    - Allows unauthorized remote control over an infected machine.
    - Could be used for espionage or data exfiltration.

IoC 2: Agent Tesla

- **Description:** Agent Tesla is a spyware Trojan written for the .NET framework and has been active since 2014.
- **Detection Method:**
    - Analyzed using OpenCTI for correlation with previous attack patterns.
    - Examined behavioral indicators, including keylogging and credential theft.
    - Checked against CISA's known malware repository.
- **Threat Indicators:**
    - Uses email as a common delivery vector.
    - Captures keystrokes, clipboard data, and screenshots.
- **Potential Impact:**
    - Credential theft leading to unauthorized access.
    - Can be used in spear-phishing campaigns targeting organizations.

---

2. Implementation of OpenCTI Threat Intelligence Platform

Installation Method:

- **Platform:** OpenCTI deployed using Docker.
- **System Setup:** Installed on a dedicated threat intelligence workstation running Linux.

Configuration of Connectors:

MITRE ATT&CK Connector

- **Purpose:** Enrich OpenCTI with structured attack techniques, tactics, and procedures (TTPs).
- **Configuration Steps:**
    1. Installed MITRE ATT&CK connector via OpenCTI's Docker environment.
    2. Configured periodic data ingestion from MITRE's knowledge base.
    3. Verified that adversary techniques in OpenCTI match the MITRE ATT&CK framework.

CISA Connector

- **Purpose:** Ingest real-time threat intelligence and vulnerability alerts from CISA.
- **Configuration Steps:**
    1. Integrated CISA feed within OpenCTI to receive alerts on emerging threats.
    2. Mapped CISA-provided IoCs to observed malware in the dataset.
    3. Enabled correlation between CISA alerts and OpenCTI's internal threat database.

---

3. Basic Usage Demonstration

- **IoC Querying:**
    - Queried 3PARA RAT and Agent Tesla using OpenCTI's interface.
    - Mapped these malware families to their known adversaries and attack techniques.
- **Threat Intelligence Correlation:**
    - Used OpenCTI to visualize relationships between MITRE ATT&CK techniques and CISA advisories.
    - Generated reports linking 3PARA RAT with Putter Panda and Agent Tesla with multiple espionage campaigns.