

Implementing Threat Intelligence Principles

Project Overview

This report documents the practical implementation of threat intelligence principles. The project is divided into three main sections:

1. **Analysis of Indicators of Compromise (IoCs):** Identification, analysis, and detection methods for two specific IoCs.
 2. **OpenCTI Threat Intelligence Platform Implementation:** Setup and configuration of the platform using Docker or system installation, including the integration of two connectors.
 3. **Demonstration of Platform Usage:** A walkthrough of basic platform functionality with supporting evidence.
-

Section 1: Indicators of Compromise (IoCs)

Analysis

IoC 1: "LOWBALL" Malware

- **Description:** LOWBALL is a malware used by the "admin@338" China-based cyber threat group. It delivers malicious payloads by exploiting newsworthy events as lures.
- **Detection Methods:**
 - **File Hash Analysis:** Identifying unique file hashes related to LOWBALL samples.

- **Network Traffic Monitoring:** Observing abnormal traffic patterns linked to known LOWBALL command-and-control (C2) servers.
- **Threat Indication:**
 - Connections to LOWBALL C2 servers indicate potential compromise.

IoC 2: "Pink Sandstorm"

- **Description:** Pink Sandstorm is a ransomware and wiper malware associated with the "Agius" Iranian threat actor group. This malware has been active in Middle Eastern regions.
 - **Detection Methods:**
 - **Endpoint Detection:** Monitoring endpoints for encrypted files and wiper activity.
 - **Log Analysis:** Reviewing system logs for traces of unauthorized encryption tools or scripts.
 - **Threat Indication:**
 - Sudden appearance of encrypted files and the deletion of system recovery tools suggest ransomware activity.
-

Section 2: OpenCTI Threat Intelligence Platform Implementation

Installation Process

The OpenCTI platform was implemented using **Docker** for containerized deployment. Below are the steps:

1. **System Preparation:**
 - Installed Docker and Docker Compose on the host system.
 - Allocated required resources (CPU, RAM, and storage).

2. OpenCTI Setup:

- Pulled the official OpenCTI Docker images.
- Configured the `docker-compose.yml` file with environment variables.
- Started the services using `docker-compose up`.

Configuration of Connectors

Three connectors were integrated to enrich threat intelligence data:

1. VirusTotal Connector:

- Configured with an API key for retrieving IoC data from VirusTotal.
- Enabled automated ingestion of malware hashes and associated metadata.

2. MISP Connector:

- Linked to a MISP instance to sync threat reports and enrich OpenCTI datasets.

3. MITRE ATT&CK Connector:

- Integrated to map threat actor tactics, techniques, and procedures (TTPs).
- Automatically ingests and updates ATT&CK framework data within OpenCTI, providing detailed insights into adversarial behaviors.

Documentation of Setup and Integration

- Screenshots demonstrate the platform interface, showing active connectors and ingested data.
 - Logs confirm successful integration of connectors and data flow between systems.
-

Section 3: Demonstration of Basic Platform Usage

Evidence of Functionality

1. **IoC Search:**

- LOWBALL and Pink Sandstorm IoCs were queried within the platform.
- Detailed metadata, including associated threat actors and related malware, were retrieved.

2. **Visualization:**

- Generated a graph to visualize relationships between intrusion sets, malware, and targeted sectors.

3. **Analytics Dashboard:**

- Monitored the dashboard for statistics on the most active threats and malware over the last three months (refer to screenshots).

4. **MITRE ATT&CK Integration:**

- Explored ATT&CK mappings for associated TTPs of identified threat actors.
- Visualized the alignment of tactics and techniques with known intrusion sets, enhancing defensive strategy formulation.

Supporting Evidence

Screenshots provided illustrate:

- The "Intrusion Sets" section showcasing profiles such as "admin@338" and "Agrius."
 - The "Malware" section with entries like "LOWBALL" and "Pink Sandstorm."
 - The dashboard displaying metrics on active threats and malware.
 - MITRE ATT&CK connector demonstrating successful ingestion and mapping of TTPs.
-

Conclusion

This project successfully demonstrates an understanding of threat intelligence principles through:

1. Detailed analysis of two IoCs with detection methodologies.
2. Implementation and configuration of the OpenCTI platform with three operational connectors.
3. Demonstration of platform usage, supported by screenshots and functional evidence.

The insights gained through this implementation highlight the critical role of threat intelligence in proactive cybersecurity efforts.



