USE CASE

Threat monitoring and hunting

Filigran

OpenCTI enables organizations to analyze threat intelligence in real time and across systems to detect and respond to potential threats promptly. This helps prevent security breaches and reduce the impact of cyberattacks.

Filigran Capabilities

OpenCTI enables organizations to analyze threat intelligence in real time and across systems to detect and respond to potential threats.

USER-DEFINED CUSTOM DASHBOARDS

Dashboards show a clear representation of your work that can be appreciated by security analysts, managers and executives.

With OpenCTI, users can create as many custom dashboards with as many widgets as they want and display any data type from the platform in their preferred manner. This flexibility enables users to effectively illustrate both **high-level assessments of the threat landscape** as well **specific Priority Intelligence Requirement-led (PIR) threat hunting dashboards**.

Beyond operational flexibility, users can easily make these dashboards publicly available or specific to a community and even control the whether sensitive information is included or not.

BI-DIRECTIONAL INTEGRATIONS

Establish a connection between OpenCTI and other existing detection solutions by transmitting data from OpenCTI to third-party solutions, as well as drawing alerts from third-party solutions into OpenCTI.

RECURRING PAIN POINTS

POOR COLLABORATION

Unable to streamline information exchange across teams during a cyber incident response

INTENSIFIED THREATS

Due to lack of correlation, identification and understanding across internal events and external threat intelligence

UNCLEAR PERFORMANCE

Unable to measure the performance of the cyber threat intelligence team

LEGACY SOLUTIONS

Unable to operationalise strategic information in legacy solutions (SIEM, EDR, XDR...)

SILOED TEAMS, CLIENTS AND KNOWLEDGE

Unable to share information with internal/external stakeholders, which leads to siloed teams, clients and knowledge bases

UNACCEPTABLE DELAY

Unacceptable delay between the internal production of threat intelligence and its use for threat hunting and remediation

This bi-directional integration is essential to enhance visibility on possible threats, synergize existing security solutions and maintain the integrity of strategic information during threat hunting and monitoring.

CASE MANAGEMENT WITH TEMPLATES

OpenCTI supports case management with templates that include pre-defined tasks and severity matrices based on the origin of the case. These templates save a significant amount of time for cybersecurity teams, streamlining the process of tracking and managing potential threats.

This consistency across various types of information and solutions enhances the overall efficiency and reliability of threat management efforts.

EASE OF SHARING INTELLIGENCE

Share threat intelligence, dashboards, and KPIs with subsidiaries and within the client group by publishing feeds on the internet, within the community, and sharing via email or a permanent link.

OpenCTI not only allows users to share information and intelligence with others but also to receive and consume information from partners, external sources, and customers via manual or automated mechanisms.

OpenCTI users can easily create and manage new accounts, users, and access, ensuring full control over the complexity of information sharing. This facilitates collaboration, enhances visibility in threat hunting and threat monitoring, ensures seamless knowledge sharing, and improves threat management efficiency.

Use case outcomes

OpenCTI helps internal and external security stakeholders prevent security breaches and reduce the impact of cyberattacks in three ways:

BI-DIRECTIONAL INTEGRATION

Integrate OpenCTI with 3rd party detection solutions to deliver threat data and ingest security alerts.

OPTIMAL CASE MANAGEMENT

Centralize use cases and support case templating with pre-defined tasks and workflows.

SHARED KNOWLEDGE

External stakeholders can both consume and contribute via public dashboards, TAXII/CSV feeds and many other mechanisms.