USE CASE

Filigran

Incident response & investigation

OpenCTI's case management is designed to streamline threat investigations. By seamlessly centralizing incident-related information, organizations improve their overall incident response efficiency.

Filigran Capabilities

Using OpenCTI and cyber threat intelligence-driven approach allows CSIRTs, CIRTs, and CERTs to save time in responding to incidents.

INCIDENT CREATION AND TRACKING

Initiate a new case to document and oversee a specific incident or threat, while assigning team members. This case serves as a centralized repository for all relevant incident-related information.

Keeping new findings, developments, and actions taken up-to-date enables clear tracking of the incident's status and response efforts.

COLLABORATIVE WORKSPACE

Team members can collaborate in real-time, while sharing insights, observations, and analysis related to the incident fostering teamwork and knowledge sharing.

Tasks can be assigned to specific users directly from the case, ensuring every aspect of the incident is addressed.

GRAPH AND KNOWLEDGE

Bring together diverse sources of information into a single, centralized location. All the knowledge contained can be visualized in comprehensive graphs so users can see relationships between entities, get a global view of the incident, and better understand context and actions that should be taken.

RECURRING PAIN POINTS

CROSS-PLATFORM SHARING

Hard to create and share reports with security teams and across platforms.

DIFFICULT TO QUALIFY ALERTS

Difficulties in qualifying alerts raised by detection systems.

POOR ORGANIZATION

Poor organization between incident responders during incident management.

EXCESSIVE WORKLOAD

Significant workload to gather and format the findings of the investigation/incident response.

Timelines and correlations with other cases are also available to represent the chronological sequence of events related to the incident.

AUTOMATED WORKFLOW

Replace manual tasks with intelligent, real-time automation. Automated workflow streamlines operations, prioritizes critical threats, and reduces response times. Traditional methods often resulted in lengthy processes, leaving systems vulnerable for extended periods.

Using automation for malware detection, incident triage, playbook execution, and documentation, significantly improves response times, alert prioritization and reduces the burden on security teams.

Use case outcomes

OpenCTI enables cybersecurity teams to organize, store, and operationalize threat information across technical, operational, and strategic levels. Organizations can improve their incident response efficiency in three ways:

CENTRALIZED KNOWLEDGE

Consolidate all relevant incident information into a single organized repository.

REAL-TIME COLLABORATION

Share insights, observations and analysis within the platform.

CORRELATION OF ELEMENTS

Gain valuable context, connecting incidents to existing data.