USE CASE

Intelligence-driven SOC

Filigran

OpenCTI empowers SOC teams to conduct security operations driven by intelligence from internal and external sources, enabling them to save valuable time. Thanks to automation and AI assistance, OpenCTI enhances cyber threat detection efficiency and timeliness.

Filigran Capabilities

Through OpenCTI's intelligence-driven operations, SOC teams save time and enhance their agility and effectiveness in tackling advanced cyber threats.

COMPREHENSIVE ALERT COLLECTION

Focus on relevant alerts rather than the entirety of your activity logs. By pushing cyber threat alerts from your SIEM or XDR to OpenCTI, your SOC team enhances its ability to analyze internal and external threats comprehensively.

Adopting an intelligence-driven approach enables SOC teams to implement proactive threat detection and prevention strategies. OpenCTI ensures that your security tools are automatically updated and optimized in real time.

ADVANCED THREAT IDENTIFICATION

Leverage **STIX 2.1 framework** and graph-based visualizations to classify threat intelligence and visualize entities and their relationships in a dynamic knowledge graph. This help SOC teams to easily pivot from entity to entity, for example from an IP address to a malware to a threat actor.

RECURRING PAIN POINTS

UNABLE TO TRACK THREATS

Hard to track threats from outside of the network with legacy tools.

LACK OF UP-TO-DATE INFORMATION

Outdated threat information leads to delayed responses.

DIFFICULT TO IDENTIFY THREATS

Difficulties in identifying threats behind indicators.

SKILL BARRIER

Coding automation tasks is time consuming.

INEFFICIENT THREAT DETECTION

False positives and false negatives hinder efficient threat detection.

Configure inference rules to automatically create logical STIX relationships, save the analyst's time and reinforce the graph's quality.

NO-CODE AUTOMATION PLAYBOOK

Program step-by-step playbooks with a few clicks to automate a series of manual tasks including but not limited to threat intelligence enrichment, data manipulation, data filtering and notification delivery.

Our no-code automation playbook allows cybersecurity teams to quickly schedule repetitive but necessary tasks without the need for in-depth coding skills.

FASTER THREAT DETECTION WITH GENERATIVE AI

Utilize **our generative AI tool, "Ask AI"**, in OpenCTI to effortlessly convert structured information to unstructured data and vice versa.

Trivialize time-consuming tasks such as reading reports and deciphering threat data into actionable intelligence. This enables SOC teams to focus their efforts on implementing customized threat detection strategies and analyzing their results.

Use case outcomes

By streamlining automation and offering AI assistance, OpenCTI enhances cyber threat detection efficiency and timeliness. SOC teams can benefit in three ways:

SINGLE SOURCE OF TRUTH

Streamline internal and external intelligence to identify the threats behind suspicious and malicious activities.

REDUCED MTTD AND MTTR

OpenCTI enables SOC teams to prioritize their response, establish the links amongst various threats and promptly implement effective detection strategies.

USER-FRIENDLY AUTOMATION

Save time on daily operations thanks to automation playbooks built with simply a few clicks.