CUSTOMER STORY

Filigran

How OpenCTI Saved 15 Workdays Monthly by Replacing 3 Platforms for a Global Defense Leader

Before OpenCTI, this global defense leader struggled with 3 disjointed systems and siloed data, wasting critical time and resources. Now, OpenCTI turns fragmented data into faster, sharper decisions and proactive threat response.

From 3 to 1 platform

From 3 knowledge platforms to 1 centralized intelligence hub

15 workdays saved monthly

in report processing, from 30 to 10 minutes per report

90% faster report generation

from several days to ~1 hour

OVERVIEW

INDUSTRY

Aerospace and Defense

HEADQUARTERS

USA

PRODUCT USED

OpenCTI

USE CASE

- IoC Management & Detection
- Threat Landscape Monitoring
- Threat Intelligence Library
- Vulnerability Monitoring
- Incident & Case Management

About the customer

This global organization operates at the intersection of aerospace and defense. The sensitivity of its activities and the extent of its international footprint make it a prime target for advanced cybercriminals.

At the heart of its response sits the Cyber Threat Intelligence team, the nerve center of the cybersecurity organization. Its mission is to translate the noise of the threat landscape into signals that detection, vulnerability, and response teams can act on.

When every alert competes for attention, it helps the organization prioritize the most significant risks.

Context

Operating in a high-risk environment, the organization faces sustained activity from highly skilled malicious actors. “We're dealing with some of the most advanced nation-state threat actors out there, so we need equally advanced techniques to defend against them,” explains the Cyber Threat Intelligence Analyst. “Our job is to figure out what defenses are needed and build the plan to implement them.”

Previously, the CTI team relied on a traditional indicator-focused platform, supported by several adjacent tools for reporting, ticket management, and metrics. But as the volume of intelligence grew, this ecosystem became increasingly difficult to manage.

> “We’ve always prioritized intelligence quality over quantity, but OpenCTI - especially with connectors - made it much easier to execute that principle. We can now focus on what we care about and avoid filling the platform with noise.”
>
> **Cyber Threat Intelligence Analyst**
> *Aerospace and Defense*

Challenges

A MANUAL, UNSCALABLE INTELLIGENCE ENVIRONMENT

The team relied on an aging, indicator-centric repository. It had gradually become slow, difficult to maintain, and unable to support the growing volume and diversity of threat intelligence data. Processing a single intelligence report used to involve logging in to multiple sites, manually downloading, reuploading, and enriching the data just for workbench validation. “On average, we used to spend around 30 minutes per report,” says the Cyber Threat Intelligence Analyst. “We’re a very large organization, which means we deal with a constant flow of intelligence, from phishing emails to reports coming from both public and private sources. We needed a platform that could handle that volume, and fast.”

FRAGMENTED TOOLING LIMITING CONTEXT, ANALYSIS, AND EFFICIENCY

Reports and indicators were scattered across separate platforms serving different purposes: indicator storage, narrative reporting, ticketing, and metrics. In addition to limiting the team’s ability to develop a consistent analytical framework over time, this fragmentation has created significant operational overhead. Analysts spent valuable time navigating tools and reconstructing context: “It was time-consuming and costly to maintain a custom intelligence metrics dashboard and host it ourselves,” explains the CTI Analyst.

LIMITED ABILITY TO PRIORITIZE THREATS AND VULNERABILITIES

Operating in a highly targeted environment, the team had to constantly decide which vulnerabilities required immediate action and which could be monitored over time. Without structured tracking and grouping capabilities, vulnerability information lacked a centralized analytical view, making prioritization less data-driven than desired. Additionally, the team struggled to ensure data reliability and was unable to implement custom filtering of indicators for various platforms. “Our old environment only allowed a single point-in-time measure of fidelity, not real-time changes,” remarks the CTI Analyst.

DATA SENSITIVITY AND ACCESS CONTROL CONSTRAINTS

The cyber threat team handles highly sensitive information, subject to strict access restrictions. They needed a solution to manage differentiated visibility permissions within a single platform, ensuring that all analysts could perform comprehensive analyses while respecting role-based data access constraints.

Why OpenCTI?

SCALABLE THREAT INTELLIGENCE PLATFORM

OpenCTI provides a scalable threat intelligence platform designed to meet the growing demands of modern security operations. It automatically ingests, normalizes, and enriches millions of heterogeneous data points (from commercial feeds, open-source repositories, and internal systems), consolidating them into a single, unified workflow. With over 30 automated and custom connectors, the platform continuously pulls and processes intelligence from key sources, eliminating manual bottlenecks and ensuring real-time updates.

UNIFIED THREAT INTELLIGENCE INTO A SINGLE PLATFORM

Intelligence processing no longer requires switching between systems. Now, all threat intelligence is centralized, enriched, and structured within a single platform, using the standardized STIX language. “We used to have three different tools, now we only use one. That’s less work for our support and development team to maintain, and less context-switching for analysts,” notes the Cyber Threat Intelligence Analyst. “We are now able to track threat hunt reports and metrics directly in OpenCTI and upload Jupyter notebooks and other code directly in the platform for reuse, while previously we had to store them in separate platforms and link them together.”

STRUCTURED, CONTEXTUAL, AND DATA-DRIVEN ANALYSIS

Thanks to OpenCTI’s relational intelligence model, the CTI team can leverage new critical contextual entities such as victimology, targeted regions, source regions, sectors, etc.

By correlating CVEs with malicious actors and campaigns, OpenCTI concentrates vulnerability information into a clear analytical view. This empowers analysts to structure intelligence in a way that facilitates attribution, long-term tracking, and data-driven vulnerability prioritization.

“Saving entities was a new concept for us. We had only ever focused on indicators of compromise,” the customer says. “The CVE connector is very useful. It automatically retrieves information and scores for each CVE that we can enhance with our reporting before sending to vulnerability management. Plus, the “Sightings” feature of OpenCTI has opened up a new path for us to conduct continuous evaluation on the health of our intelligence data set.”

GRANULAR ACCESS CONTROL FOR SENSITIVE INTELLIGENCE

OpenCTI enabled the team to bring together information while applying differentiated visibility permissions. This security measure ensures compliance with strict government requirements for data processing without fragmenting analysis across systems.

> "Being able to tie reports and indicators back to a threat actor, and to track those threat actors over time, was something we simply couldn't do effectively before."
>
> **Cyber Threat Intelligence Analyst**
> *Aerospace and Defense*

Adoption

The team adopted OpenCTI, step by step, starting with report ingestion, workbench usage, then expanding to entity extraction and automation. After validating the platform with the Community Edition, the company upgraded to Enterprise features, which enabled it to manage new functionalities. These include information requests from teams across the organization who have questions about campaigns, geopolitical developments, specific vulnerabilities, etc. Previously handled without a formal structure, these requests could now be integrated directly into OpenCTI via a dedicated information request workflow.

Throughout the deployment, the relationship with the Filigran team proved to be just as important as the technology itself. "The support portal and dedicated Slack channel made a real difference. We always feel heard and our priorities are taken seriously," recalls the CTI Analyst. "New features are constantly being developed, and the enhancements we request often get implemented. This is very helpful for us."

> "We used to have three different tools; now we only use one. That's less work for our support and development team to maintain and less context-switching for analysts."
>
> **Cyber Threat Intelligence Analyst**
> *Aerospace and Defense*

How Filigran helps

FASTER INTELLIGENCE WORKFLOWS SAVE 15 WORKDAYS MONTHLY

OpenCTI enabled the seamless migration of a large-scale indicator dataset from the legacy TIP, ensuring no loss of coverage during the transition. Then, by unifying all this intelligence into a real-time workflow, OpenCTI reduced report processing time from 30 minutes to just 10 minutes - saving 15 workdays per month. This efficiency gain enables the team to process more reports than ever before each month. “OpenCTI has fundamentally changed the way we run intelligence,” shares the Cyber Threat Intelligence Analyst. "We're now operating much more efficiently. That's a huge shift for our team."

FROM 3 KNOWLEDGE BASES TO 1 INTELLIGENCE HUB

By consolidating intelligence into a single source of truth, the company eliminates silos, ensures uniform, high-quality analyses, and preserves institutional knowledge. “Besides, a single system is cheaper to maintain than three!" the CTI Analyst adds. The practical impact is tangible. When management requested a consolidated view of intelligence products, what would previously have taken several days of manual filtering was accomplished in about an hour using entity-based queries and the PyCTI library. The transformation doesn’t stop there: “Automatically collecting metrics and building queries into a unified dashboard has been incredibly useful to both our team to check on our targets and our leadership to ensure we are prioritizing effectively and our impact is felt,” says the CTI Analyst.

FASTER AND DEFENSIBLE RISK DECISIONS

Discussions about vulnerability management are no longer driven solely by technical severity levels. The CTI team can now support remediation decisions with real-time contextual intelligence, eliminating ambiguity and internal debate. Risk assessments are documented, traceable, and easier to justify, both operationally and at the executive level, strengthening alignment across different intelligence departments. “We can now track the fidelity of our intelligence in close to real-time.”

HIGH-INTEGRITY INTELLIGENCE UNDER STRICT ACCESS CONTROLS

Fine-grained access controls now guarantee that restricted government-sourced data remains protected, while preserving the analytical relationships between entities. As the CTI Analyst says, “Being able to control who sees what is a major capability for us.”

The Road Ahead

Now that a solid intelligence foundation has been established, the cyber threat intelligence team is focusing on the next stage of maturity: smart automation. OpenCTI has already streamlined ingestion and analysis, so artificial intelligence represents the next frontier.

"AI is the hot topic right now. We want to leverage AI to improve our processes and reduce the time analysts spend on repetitive tasks," explains the Cyber Threat Intelligence Analyst.

By continuing to work hand in hand with Filigran, the international company will further consolidate data quality and save time in its processes to develop higher value-added strategic intelligence.