CUSTOMER STORY

Filigran

How a leading luxury manufacturer strengthens its cyber defense with OpenCTI

Learn how a major French luxury goods manufacturer built a high-performance internal CERT and threat intelligence capability using OpenCTI, improving detection, awareness, and response time across its global operations.

+650 hours saved
through automated report ingestion each year

1 major incident detected/month
previously undetected by other layers

< 15 minutes
Detection alerts deployment time

OVERVIEW

INDUSTRY
Luxury goods

PRODUCT USED
OpenCTI

USE CASE
- IoC Management & Detection
- Threat Landscape Monitoring
- Threat Intelligence Library
- Threat Awareness

About the customer

This customer is a major French luxury group, listed on the CAC 40 and employing over 20,000 people worldwide. With deep roots in traditional craftsmanship, the company has broadened its activities across various sectors of the luxury industry.

Despite its artisanal image, its global operations rely heavily on IT and digital processes. Since 2020, the company has made cybersecurity a strategic priority and has rapidly scaled its internal Computer Emergency Response Team (CERT) to over 30 professionals.

> **"Even if every other protection fails, OpenCTI gives us a last line of defense."**
>
> *CERT Analyst*
> Leading French Luxury Group

Context

In 2020, amid growing concern over cyber risks, the company's CISO decided to bring cyber defense in-house. Relying solely on third-party MSSPs was no longer sufficient for a business where image and trust are critical. *"As a luxury brand, a single leaked customer file or IT disruption could have severe reputational and operational consequences,"* explained the company's CERT Analyst we interviewed.

The brand created the CERT from scratch, growing it from 4 to over 30 members in just three years. The need for proactive, context-rich threat intelligence quickly emerged, not just for incident response, but also for strategic awareness and business protection. With limited CTI resources, they needed a tool that could automate, centralize, and surface the most relevant intelligence reliably and fast.

Challenges

LIMITED CTI CAPACITY & COSTLY MANUAL PROCESSING

With only a fraction of a full-time position allocated to threat intelligence, manual handling of reports and indicators wasn't scalable. In addition, transforming threat intelligence into detection rules was both time-consuming and resource intensive.

"We're essentially half an FTE on threat intel. I couldn't manually link entities and write detections from scratch," says the CERT Analyst from the luxury group. *"In a standard configuration, we would have had to create a retroactive hunting rule for each report, which takes time, increases CPU load, and often ends up being too resource-intensive to scale."*

DEPENDENCE ON THIRD PARTIES FOR CORE DETECTION CAPABILITIES

Relying on external MSSPs had its limits: visibility was fragmented, responsiveness wasn't always optimal, control over infrastructure and detection logic remained out of the team's hands. *"We wanted dedicated people in-house rather than depending on a third party with partial oversight,"* says the CERT Analyst.

Once cybersecurity was declared a top priority at the executive level, a major **restructuring was launched to build a dedicated CERT**. This internal team would require the best-in-class detection capabilities with full ownership, precision, and visibility across all endpoints.

NO CENTRALIZED DETECTION WORKFLOW FOR IOCS

"We had no real tool for automated IOC detection," the company's CERT Analyst admits. ***"It was only manual effort, and a lot of blind spots."*** Back in 2020, the company lacked a system capable of automating IOC ingestion, enrichment, and alerting. Indicators were managed manually or not at all, with no centralized way to correlate them with internal telemetry.

GAPS BETWEEN TRADITIONAL SECURITY LAYERS

Despite having multiple layers of defense (email filters, SIEM, EDR), certain threat vectors could still bypass detection. The CERT team needed a way to catch those that slipped through, especially exploiting user behavior or blind spots in infrastructure monitoring, as the CERT Analyst explains: *"If someone opens their personal inbox on a corporate workstation and clicks on a phishing link, that traffic won't go through our secured email gateway. We caught one of those thanks to OpenCTI. Otherwise, we might have missed it entirely."*

Why did they choose OpenCTI?

DETECTION-FIRST DESIGN

By integrating indicators directly into the OpenCTI detection workflow, the Computer Emergency Response Team could trigger alerts in their SIEM whenever a known threat matched internal tools. *"The big difference is that with our current setup, detection happens directly via OpenCTI, not just in the SIEM,"* explains the CERT Analyst. This unique positioning turned OpenCTI into an active detection layer, reinforcing endpoint protection across the organization.

SEAMLESS IOC CORRELATION OUTSIDE SIEM

Beyond its integration with the SIEM, OpenCTI operates as an autonomous correlation engine. It matches known IoCs with live observables, independently of other tools. This ensures **an additional safety net**, as the company's CERT Analyst explains: *"Even if every other protection fails, when something hits an IoC known in OpenCTI, we still get the alert."*

OPEN-SOURCE FLEXIBILITY & CO-EVOLUTION WITH THE PRODUCT

As an open-source platform, OpenCTI gave the team full autonomy to deploy, test, and scale the solution independently. **The company was one of our early adopters, implementing OpenCTI before Filigran even existed formally!** Over time, they **expanded their use case step by step** according to their needs.

"We basically evolved alongside OpenCTI," recalls the CERT Analyst. *"We didn't just need a platform, we needed something that could grow with us, automate detection, and help us see what others miss."* This **agile, open architecture** proved essential as the CERT scaled its structure and matured its threat detection workflows.

NATIVE SUPPORT FOR STIX, MITRE, AND STRUCTURED INTELLIGENCE SHARING

OpenCTI provided **native alignment with STIX, MITRE ATT&CK, and CVE references**, enabling the team to structure and centralize their threat intelligence knowledge. This made it easier to contextualize indicators, track actor behaviors, and share internally or with an external database like MITRE. *"Thanks to those native supports, we're starting to build a really coherent knowledge base for high-quality threat intelligence,"* says the CERT Analyst.

Adoption

The company's Computer Emergency Response Team rolled out OpenCTI early on, even before cyber threat intelligence became an official function. The first deployment started directly from the open-source GitHub repository, with a real formal onboarding process.

However, the implementation was fast and largely self-driven. As the team added connectors, data sources, and enrichment logic, a few performance issues required support from the Filigran team. It took only a few infrastructure changes and adjustments to get the platform back to stable, optimized, and highly customized.

After a few years of successfully using the open-source version, the company briefly explored the SaaS model, but chose to keep an on-prem deployment that better meets its requirements in terms of performance, cost, and autonomy. Throughout the whole process, Filigran's support team was responsive and helpful: *"Even during our infrastructure rebuild, Filigran provided us with unwavering support. That collaboration helped us keep the platform running smoothly,"* enthuses the CERT Analyst.

The luxury brand operates OpenCTI daily with a strong focus on operational automation and strategic awareness, regularly contributing to the broader Filigran community.

How Filigran helps

CRITICAL THREAT DETECTION

The CERT has successfully identified and contained threats that slipped past traditional protections, such as phishing links opened through personal inboxes on corporate devices. *"OpenCTI helps catch the one case that falls through the cracks. That's when you realize it's more than a backup, it's a safety net,"* says the CERT Analyst. **The platform generates 1 to 2 high-confidence alerts per month** that might otherwise have gone unnoticed, directly contributing to incident prevention.

> **"We didn't just need a platform — we needed something that could grow with us, automate detection, and help us see what others miss."**
>
> *CERT Analyst*
> Leading French Luxury Group

SUBSTANTIAL TIME SAVINGS ON REPORT INGESTION

Before OpenCTI, transforming threat reports into detection rules could take up to an hour per report. With automated ingestion, MISP connectors, and direct integration into detection workflows, the first step now takes just seconds.

"In three clicks, I have my indicators in detection," says the CERT Analyst. This automation saves the team **up to 20 hours per week** (or more than 650 hours annually), time that can be reinvested in more strategic investigations. When indicators are flagged in OpenCTI, they are immediately sent to the detection layer. *"Once it's in detection, we usually get the alert within a quarter of an hour,"* he confirms.

OpenCTI also makes it possible to **monitor 10 to 15 reports from various intelligence sources on a daily basis**, thus ensuring broad coverage and timely detection, leaving no critical signal overlooked.

STRUCTURED INTEL FOR BETTER DECISION-MAKING

OpenCTI's dashboards and STIX-native architecture allow the CERT to track emerging threats and justify mitigation actions with reliable, internal data.

"I can generate a histogram showing that a given technique is increasingly mentioned; and it's our own data, not scraped from someone else's report," explains the analyst. This structured intelligence supports monthly reporting and feeds decision-making at both operational and strategic levels.

CONTINUOUS MONITORING WITHOUT MANUAL EFFORT

With OpenCTI acting as a centralized hub, the team can monitor global threat activity in real time without switching between tools or risking missed information. Reports and indicators from both free and commercial feeds are automatically aggregated and correlated. ***"We plug in as many sources as possible and centralize everything in OpenCTI. It helps us keep up with daily intel and avoid missing anything important,"*** says the CERT Analyst. This aggregation power improves situational awareness and reduces cognitive load on the CTI team.

Future Outlook

As the CERT continues to mature, OpenCTI will play an increasing role not only in detection and correlation, but also in raising cybersecurity awareness across the organization. Monthly incident reports and dashboards integrated into OpenCTI are already being used to communicate threat trends internally, and the team plans to go further. *"We use OpenCTI to highlight techniques, threat actors, and attack patterns; then share those insights with the right teams within the group,"* explains the CERT Analyst.

This dissemination approach helps ensure that detection, response, and prevention strategies are aligned, whether it is a matter of alerting the network team about a new technique, the Red Team to a new attack vector, or communicating about an emerging phishing campaign.

The CERT also plans to **expand its connector base, refine correlation logic, and enhance trend monitoring**, while maintaining a lightweight platform adapted to its operational reality.

Going forward, OpenCTI will continue to support the group's ambition to stay proactive, informed, and resilient.