CUSTOMER STORY

Filigran

From 5 Days to a Few Seconds: ASRG Scaled Automotive Threat Management with OpenCTI

Discover how ASRG collaborated with Filigran and leveraged OpenCTI to build a trusted, community-driven threat intelligence platform for the automotive industry. It automates enrichment processes and enables secure, scalable information sharing for global stakeholders.

1.2 Million +

vulnerability-related data points are stored in the world's largest open threat intel base for automotive cybersecurity

90%

automation of enrichment workflows leading to significant time savings

20K+ community members

can be reached with curated intelligence

OVERVIEW

ASRG

INDUSTRY

Non-profit organization
Automotive

PRODUCT USED

OpenCTI

USE CASE

- Threat Intelligence Library and Data Sharing
- Vulnerability Monitoring
- Automation & Scalability

About ASRG

The Automotive Security Research Group (ASRG) is a non-profit organization, founded in 2016 to advance cybersecurity in the automotive industry. With nearly 20,000 members worldwide, ASRG connects researchers and industry professionals through education, networking, and collaborative initiatives. As a Certified Numbering Authority (CNA), ASRG also supports responsible vulnerability disclosure by assigning CVE identifiers and coordinating actions with relevant stakeholders. It promotes a bottom-up, contributor-led approach in building trusted cybersecurity knowledge and solutions across the industry.

> **"With OpenCTI, the enrichment process now takes seconds. Before, setting up the system and dashboards took over 40 hours."**

John Heldreth
Founder, ASRG

Context

As cybersecurity threats have grown more sophisticated in the automotive industry, the need for a reliable and collaborative intelligence ecosystem has become increasingly obvious. Traditional IT threat-sharing models didn't address the unique challenges posed by the complexity of automotive systems.

That is why John Heldreth, then working at Porsche, launched what would become the Automotive Security Research Group (ASRG) in 2016: *"We realized that the community would play a very important role in the success of cybersecurity for automotive. It doesn't matter which company you work for: you're either part of the solution or you're on the other side."* ASRG quickly evolved into a global initiative with over 20,000 members, supported by a lean core team and hundreds of active volunteers contributing to projects worldwide.

Challenges

LIMITED INTEROPERABILITY AND EXTERNAL SHARING

While ASRG was already using a CTI platform, it lacked the flexibility and openness needed to organize, contextualize, and share information efficiently. The system was designed for internal use only, which made it difficult to build meaningful relationships between objects or expose threat intelligence externally.

"We create our own threat intelligence based on industry input, but we lacked a place to structure it, channel it, and make it usable for others," recalls John Heldreth. To enable collaboration, the team had to manually extract data via custom APIs, reformat it, and rehost it in external tools. *"In general, companies want to keep threat information secret, but we needed the opposite,"* John adds. This workaround created friction, increased the risk of errors, and made real-time information exchange nearly impossible.

HIGH INFRASTRUCTURE & MAINTENANCE COSTS

Maintaining two parallel systems – one for internal CTI management and one for external dashboards – resulted in significant overheads. ASRG had to run large servers and shoulder the cost of maintaining redundant infrastructure. This model was not sustainable for a non-profit organization operating on limited resources.

TIME-CONSUMING WORKFLOWS

Data enrichment and dashboard generation were largely manual processes, that required extensive time and effort to set up and maintain. *"It used to take over 40 hours of work,"* explains John Heldreth. This slowed down ASRG's ability to effectively disseminate information, limiting the platform's responsiveness to evolving threats and community needs.

LACK OF TRACEABILITY IN ENRICHMENT PROCESSES

When ASRG began automating enrichment using AI models, it faced a new challenge: tracking the origin and logic behind each piece of generated data.

John says: *"We needed to ensure the quality of the data. Every step of the enrichment process had to be traceable (who created what, and why) so that we could trust the data."* To build transparency and for audit purposes, ASRG needed a platform that could preserve this end-to-end traceability at every stage of enrichment.

Why did ASRG Choose Filigran's OpenCTI

COST-EFFECTIVE & OPEN SOURCE BY DESIGN

As a non-profit organization with limited resources, ASRG needed a platform that could scale without licensing constraints or vendor lock-in. While their previous CTI solution was used at no cost, it lacked the flexibility and openness required for automation, enrichment, and community-driven sharing. OpenCTI's open-source nature made it possible to get started without financial barriers. *"It was mostly cost-driven at the beginning,"* John Heldreth explains. This made Filigran's OpenCTI a great option to scale securely and independently.

STRUCTURED, INTEROPERABLE, AND BASED ON OPEN STANDARDS

OpenCTI's compliance with the STIX 2.1 standard provided ASRG with a clear, interoperable framework for structuring threat intelligence. *"If someone understands the STIX schema, then they understand OpenCTI,"* explains John, *"That makes it easier for us to structure the data and build meaningful relationships between objects."* While STIX is not perfect, it provides a critical foundation for sharing knowledge across use cases.

API-FIRST ARCHITECTURE ENABLING AUTOMATION & ENRICHMENT

ASRG needed the freedom to extract, enrich, and reintegrate data according to its own workflows, especially to support its AI-driven enrichment pipeline. This process includes 32 sequential steps, where raw data is extracted from OpenCTI, analyzed, categorized, linked to relevant components, and continuously updated before being sent back to the platform. This end-to-end flow enables a continuous, bidirectional data loop.

"We have to do everything with minimal resources, so we use as much automation and artificial intelligence as possible," says John Heldreth. *"Being able to orchestrate that process end to end without being limited by the platform was essential."* OpenCTI's robust API and Python libraries gave the team full control over how data flows in and out of the system.

Adoption

Deploying Filigran's OpenCTI marked a turning point in ASRG's operations. The platform was integrated quickly thanks to its modular design and accessible tooling. Within a few weeks, ASRG had migrated its data and begun centralizing its threat intelligence into a unified and well-organized environment.

What made the difference was the close, responsive relationship with Filigran's team. Through a dedicated Slack channel, ASRG was able to raise questions, test ideas, and adapt the platform to fit the specific requirements of the automotive sector. *"We were always trying to find a way to best fit the automotive use case into the existing solution, and it was fantastic,"* says John. *"One of the best implementation experiences I've had with any software, especially for a non-profit where there's not a lot of money or revenue."*

How Filigran helps

OPERATIONAL EFFICIENCY THROUGH AUTOMATION

Thanks to Filigran's advanced tool, ASRG has achieved over 90% of automation across its enrichment workflows. Intelligence objects, such as vulnerabilities and reports, are now collected, contextualized, and redistributed with minimal human input. This has drastically accelerated internal processing times, as the founder of ASRG says: *"The time it takes to enrich something in OpenCTI is usually in seconds."* An essential level of efficiency for expanding capabilities without increasing cost.

CONFIDENCE IN DATA QUALITY AND PROVENANCE

OpenCTI's graph-based structure has allowed ASRG to enforce strict traceability on over 1.2 million vulnerability-related data points. Each object and relationship, whether produced by a human contributor or an automated process, is now fully documented and open to feedback from the community. Such traceability ensures that ASRG can uphold the level of trust expected by its global ecosystem when distributing actionable intelligence.

"If someone understands the STIX schema, then they understand OpenCTI. That makes it easier for us to structure the data and build meaningful relationships between objects"

John Heldreth
Founder, ASRG

STANDARDIZED SHARING WITH RELIABLE PARTNERS

Thanks to Filigran's OpenCTI, ASRG can now make curated intelligence available to selected peers in real time, via STIX/TAXII-compatible APIs and dashboards. This supports its long-term goal of fostering a transparent, community-driven model for automotive cybersecurity, where knowledge flows in both directions between contributors and consumers. *"We noticed that there was a need for a community where people can feel trusted, respected, and contribute to positive cybersecurity outcomes,"* says John.

The Road Ahead

ASRG aims to expand its use of OpenCTI to better reflect the complexity of modern automotive systems. One of the next priorities is the ability to map and track assets more precisely, especially hardware components, embedded software, and cryptographic elements. ASRG is closely following the evolution of emerging cybersecurity standards and vulnerability exchange formats and hopes to see stronger alignment with these in future versions of OpenCTI.

"We hope to work even more closely with the development team to make OpenCTI more relevant for the product world," John says.

Please feel free to reach out to John and ASRG if you are interested to work on a community intelligence project or would like to see the current OpenCTI implementation. They are one of the intelligence communities who is happy to show and share, and believe that the more we know about the situational environment of automotive products, the better we can secure them.