CUSTOMER STORY

Filigran

How Rivian achieves a 95% reduction in response time with OpenCTI

Explore how Rivian leveraged OpenCTI to tackle data silos, improve threat detection and scale their cybersecurity operations effortlessly.

88%
Reduction in Mean Time to Detect (MTTD) over the past 12 months

95%
Improvement in response times

980M
IoCs blocked

OVERVIEW

RIVIAN

INDUSTRY

Automotive

PRODUCT USED

OpenCTI

OpenBAS

USE CASE

- IoC management and detection
- Incident and case management
- Data sharing
- Threat landscape and vulnerability monitoring

About Rivian

Rivian is a pioneering electric vehicle (EV) manufacturer headquartered in Irvine, California, with over 15,000 employees.

Known for its adventure electric trucks, SUVs, and delivery vans, Rivian's mission is to "**Keep the World Adventurous Forever**" by redefining mobility and manufacturing through innovation.

As both an EV manufacturer and a software company, Rivian is committed to creating a more sustainable future and preserving nature for future generations.

"OpenCTI has saved our CSOC several minutes per ticket, when the team goes through 100s of cases per day, this easily adds up to hours very quickly."

Chris Mandich, Director of Cybersecurity Operations at Rivian.

Context

As a software-defined vehicle company, Rivian's operations extend beyond building electric vehicles to managing a complex ecosystem of interconnected software and hardware.

"Protecting the many attack surfaces of our business—retail, manufacturing, enterprise, and applications—is critical. Because we design, manufacture, and sell electric adventure vehicles and own the technology stack end to end, we can implement robust cybersecurity across the complete ecosystem." as Chris Mandich, Director of Cybersecurity Operations mentioned.

This technological environment is therefore significantly exposed to diverse cybersecurity threats. It was critical for Rivian to implement a robust CTI solution to adopt a highly structured and proactive approach for protecting its operations.

Prior to implementing OpenCTI, Rivian leveraged separate platforms for CTI and case management which made it challenging to reach their objectives.

Challenges

To address their complex cybersecurity needs, Rivian identified several critical challenges requiring a unified and scalable platform:

SILOED DATA

The lack of integration between threat intelligence and case management platforms created inefficiencies. Nick Peterson explained, "Having separate case management and threat intelligence platforms required us to put engineering work into the integrations between the two of them." Analysts had to navigate multiple tools to gather context, slowing down incident resolution and adding complexity to operations.

These challenges highlighted the necessity for a unified, scalable, and efficient solution. Rivian's adoption of OpenCTI addressed these issues, streamlining their cybersecurity operations and enhancing overall efficiency.

INDICATOR EXPORT ISSUES

Rivian's previous cloud-based threat intelligence platform struggled to scale. According to Nick Peterson, Senior Staff Cybersecurity Engineer, "We had a block list that we spent time curating and populating with known bad elements, only to realize weeks later that it was failing open because the CTI solution we were using couldn't export these lists correctly." This issue provided a false sense of security, undermining their defenses.

Adoption

Rivian's transition to OpenCTI/OpenBAS was remarkably smooth. According to Nick Peterson, "We just spun up an OpenCTI instance and started using it," taking only 30 days from proof of concept to production.

The team tailored the deployment to their specific requirements, leveraging Infrastructure as Code using terraform and AWS infrastructure, Elastic Container Services, RabbitMQ, S3 for storage, and OpenSearch for backend integration. OpenCTI integrates seamlessly with Rivian's threat intelligence, incident response, and third-party risk teams, importing data from various sources to support alerting, risk scoring, and decision making.

This customization ensured the platform fit seamlessly into Rivian's ecosystem, providing a strong foundation for their cybersecurity operations.

How Filigran Helps Rivian

BOOSTED CSOC TEAM PRODUCTIVITY

Integrating case management with threat intelligence within OpenCTI was a game-changer for Rivian. According to Nick Peterson "One of the biggest benefits is a huge increase in efficiency." This co-location of functions allowed Rivian's CSOC to rapidly close cases, saving significant time and effort.

Chris Mandich highlighted, "OpenCTI has saved our CSOC several minutes per a ticket, when the team goes through 100s of cases per day, this easily adds up to hours very quickly." Analysts now focus on reviewing the data and making decisions to contain and remediate cybersecurity threats, streamlining operations.

This improved efficiency led to measurable outcomes: Rivian reduced response times by 95% and detection times by 88% over 12 months.

"One of the biggest benefits is a huge increase in efficiency."

Nick Peterson, Senior Staff Cybersecurity Engineer at Rivian.

ENHANCED THREAT DETECTION

The integration provided by OpenCTI significantly improved Rivian's threat detection and incident response capabilities. By consolidating data, the team could focus more on cybersecurity investigations rather than managing multiple tools.

Nick Peterson noted, "The STIX 2.1 standard provided uniformity across our cases and TIP, helping us standardize our indicator intake more effectively." This enhanced capability allowed Rivian to curate export lists that resulted in over 980 million blocks in a single 30-day period.

Chris Mandich added, "We have CTI, a detection and response team, and third-party risk management function all utilizing intelligence and cases centrally managed within the platform." This unified approach streamlined operations and reinforced Rivian's cybersecurity defenses.

SUBSTANTIAL COST SAVINGS

By consolidating tools and leveraging the open-source nature of OpenCTI, Rivian achieved significant cost reductions. Nick Peterson explained, "There was another huge benefit in terms of cost savings by moving from two platforms to one."

The open-source nature of OpenCTI provided additional savings while fostering a collaborative environment. "Having a robust open-source project actively contributed to by the community was a significant benefit," Nick Peterson shared. Maintaining their own instance enabled Rivian to customize their setup and contribute to the platform's evolution.

Chris Mandich emphasized, "We've gained scalability and the ability to address our needs by directly contributing to the project, with our connectors now benefiting the entire community."

CONTINUOUS IMPROVEMENT THROUGH COMMUNITY SUPPORT

The responsiveness and frequent updates from the OpenCTI team provided Rivian with a robust foundation for continuous improvement. Chris Mandich praised the team's efficiency: "The feedback and responsiveness—whether fixing bugs, enhancing features, or adding functionalities—was really impressive. Issues were addressed, and updates were pushed to the main branch swiftly."

This agility allowed Rivian to stay ahead of emerging threats, ensuring their cybersecurity infrastructure remained at the forefront of innovation.

Key results

NEARLY 88% REDUCTION IN MEAN TIME TO DETECT (MTTD) OVER THE PAST 12 MONTHS

Consolidating tools and adopting OpenCTI reduced operational expenses while providing scalability and fostering a collaborative environment.

RESPONSE TIMES IMPROVED BY 95%

Rivian's CSOC dramatically reduced response times, allowing analysts to process up to 100 cases daily with increased efficiency.

980 MILLION IOCS BLOCKED

Within a single 30-day period, Rivian's curated list of indicators generated 980 million indicator of compromise blocks by leveraging OpenCTI's indicator export capabilities.

Future outlook

Rivian is committed to continuing its journey with OpenCTI and OpenBAS, expanding its use of these tools to further enhance its cybersecurity posture. Nick Peterson envisions, “We’re working on getting additional context for risk scoring for organization entities within OpenCTI... We can manage the intake of information for all of them under one umbrella.”

Chris Mandich added, “OpenBAS is coming out. The strategic evolution of that platform is exciting, as it enables us to measure both our effectiveness from an incident response or tabletop perspective and continuously test and validate the tools and technologies we use. Having that vision and delivering it as a product is truly inspiring.”

This partnership underscores Rivian's dedication to **innovation, sustainability, and robust security practices**. With a dedicated team and advanced solutions, Rivian is poised to continue making a positive impact on the world.

ABOUT FILIGRAN

Filigran, a cybertech company founded in 2022, offers open-source cybersecurity solutions covering end-to-end threat intelligence management, attack simulations, and security posture validation for organizations.

© Filigran 2025 All rights reserved.