ThreatConnect.

Customer Spotlight

Global Automotive Enterprise Cuts False Positives

Customer Profile

Organization Size	Industry/Sector	Headquarters
14,500+ EMPLOYEES	AUTOMOTIVE	LISLE, ILLINOIS

Background

As a leader in the automotive industry, this enterprise is known for designing and manufacturing vehicles that power the future of transportation. While its products drive innovation, its threat intelligence operations were lagging behind. Faced with an increasingly complex threat landscape and mounting internal pressure to improve detection and response, the company turned to ThreatConnect for a more effective and efficient way to manage and disseminate threat intelligence. As a result, it cut false positives in half, reduced signal noise, and improved mean time to respond (MTTR).

Challenges Faced

Before partnering with ThreatConnect, this automotive enterprise was overwhelmed by excessive signal noise and siloed threat feeds. Without automation to enrich and prioritize threats, along with visibility and integrated tooling, the security team struggled to identify relevant threats or respond in a timely manner. Their existing solutions lacked the scale, speed, and sophistication needed to support proactive defense.

Key challenges included:

- Lack of context or prioritization on threats
- High mean time to detect (MTTD) and mean time to respond (MTTR)
- Difficulty integrating operational tools like SIEMs, SOARs, EDRs, and more
- Inefficient manual threat intelligence workflows and processes

While this company leads in automotive innovation, its threat intelligence function was stuck in the past— without the automation, scale, or clarity needed to protect its people and infrastructure.

How ThreatConnect Helped

The company needed to shift from reactive, manual threat intelligence to a more proactive, strategic, and automated approach. They chose to partner with ThreatConnect for its ability to unify threat, risk, and action across teams.

They also cited the platform's:

- Product functionality, performance, and features
- Customizable and flexible user interface
- Competitive pricing and overall value

With ThreatConnect's Threat Intelligence Platform (TI Ops), the company now harnesses AI and automation to aggregate, enrich, and analyze threat intelligence across its ecosystem — empowering teams to identify what matters and act confidently.

With ThreatConnect's single, unified platform, they can now:

- **Contextualize** — Perform threat hunting, detection, and prevention with high-fidelity, business-relevant context at the moment of need
- **Prioritize** — Cut through the noise to focus on the most critical threats and vulnerabilities
- **Automate and Operationalize** — Streamline workflows, enrich intel automatically, and act faster, without adding complexity to their tech stack

As a result, the company has **cut false positives by 50%**, allowing the InfoSec team to focus on high-priority, business-critical threats.

Unifying Threat, Risk, and Action Across Teams

ThreatConnect's TI Ops platform helped the automotive enterprise break down silos, streamline intelligence workflows, and improve response times. Key differentiators:

- Alignment with cyber threat intelligence (CTI) tradecraft and intelligence requirements
- Ability to operationalize and automate threat intelligence at scale
- Automating intel enrichment and escalation actions
- Scalability across millions of indicators of compromise (IOCs)

ThreatConnect's automation, dashboards, integrations, fast time to value, and API capabilities drove measurable impact — empowering the team to contextualize threats, prioritize faster, and act decisively.

> "ThreatConnect enables proactivity in IT Security."
>
> **— Senior InfoSec Engineer, Enterprise Automotive Company**

ThreatConnect continues to help the company's security team operate more efficiently, make faster decisions, and respond with precision — reducing noise, avoiding burnout, and staying ahead of evolving threats.

About ThreatConnect:

ThreatConnect powers smarter, faster, and more resilient cyber defense by uniting threat intelligence, security operations, and cyber risk management. Our Intel Hub platform brings threat and risk data together to help organizations prioritize what matters most, operationalize defenses more efficiently, and communicate cyber risk in business terms. Trusted by over 250 global enterprises, ThreatConnect enables security teams to adapt to evolving threats, make better decisions, and prove their impact — from the SOC to the C-suite.