ThreatConnect.
now a part of Dataminr

Customer Spotlight

Utilities & Energy Enterprise Reduces False Positives by More Than 75%, Strengthening Critical Infrastructure Defense

Customer Profile

Organization Size
24,000+ EMPLOYEES

Industry/Sector
UTILITIES AND ENERGY

Headquarters
U.S. BASED

Background

As a critical infrastructure leader in the U.S. utilities and energy sector, this enterprise requires mission-critical threat intelligence to ensure operational continuity, public safety, and regulatory compliance. To defend against threats that directly impact service reliability, the organization sought a robust, scalable solution to enhance visibility and enable proactive defense without overwhelming its security team.

Challenges Faced

Before partnering with ThreatConnect, the company's threat intelligence operations were hampered by excessive noise and fragmented tooling. A lack of context made it difficult to identify relevant threats or collaborate across teams effectively.

Furthermore, manual, non-scalable workflows struggled to support organizational growth. The team faced significant hurdles integrating intelligence with existing SIEM, SOAR, and EDR platforms, which limited their ability to operationalize data and respond to threats in real time.

Key challenges included:

- Limited visibility into threats due to excessive signal noise and poor-quality intelligence
- Difficulty identifying relevant intel and prioritizing threats
- Inefficient, time-intensive threat intelligence workflows
- Challenges integrating SIEMs, SOARs, EDRs, and other operational tools
- Difficulty taking action on threats
- Lack of threat context
- Threat intelligence operations that lacked scalability and flexibility
- Limited or poor collaboration between teams

Without a unified approach, valuable analyst time was consumed chasing false positives and manually stitching together intelligence — leaving the organization exposed to emerging risks.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240

How ThreatConnect Helped

The company transitioned from fragmented, manual processes to a proactive, AI-driven strategy by leveraging ThreatConnect's TI Ops Platform. Chosen for its superior integration capabilities and intuitive interface, ThreatConnect allowed the organization to unify intelligence across teams and automate complex workflows. By harnessing AI-powered enrichment and automation, the team now operationalizes high-fidelity intelligence across critical use cases, including:

- **Streamlined Operations:** Automating intelligence enrichment and ATT&CK analysis.
- **Strategic Defense:** Prioritizing vulnerabilities and supporting risk mitigation.
- **Proactive Response:** Leveraging high-fidelity data to detect and prevent threats in real-time.

> "We have built out a significant amount of information in ThreatConnect over the last eight or so years, allowing us to quickly link threats."
>
> **— Senior Intelligence Analyst**

Centralized intelligence and automated enrichment now allow the team to pivot quickly and uncover related indicators with real-time context.

Unifying Threat, Risk, and Action Across Teams

ThreatConnect's TI Ops platform helped the utilities enterprise break down silos, improve collaboration, and significantly enhance the effectiveness of its security tools and teams.

Key differentiators included:

- Deep integration capabilities across the security ecosystem
- User-friendly interface and ease of use
- Robust functionality, performance, and feature set
- Ability to unify threat, risk, and action across teams

> "ThreatConnect allows us to identify, contextualize, and enrich potential threats quickly, while also allowing us to pivot on those threats to identify additional items of concern." **— Senior Intelligence Analyst**

As a result, the organization achieved measurable impact:

- Reduced false positives **by over 75%**
- **Reduced MTTR** for standard incidents
- Significantly **reduced analyst workload**
- Markedly **improved effectiveness** of SIEM, EDR, XDR, and SOAR tools
- ThreatConnect is now considered **"critical to operations"**

With clearer intelligence, faster workflows, and better collaboration, the security team now operates with greater confidence — reducing noise, avoiding burnout, and strengthening defenses across critical infrastructure.

About ThreatConnect:

ThreatConnect, now a part of Dataminr, enables threat intelligence, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense. With ThreatConnect, organizations can infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to contextualize an evolving threat landscape, prioritize the most significant risks to their business, and operationalize defenses. More than 250 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

ThreatConnect.
now a part of Dataminr.

ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
+1.703.229.4240