ThreatConnect

CUSTOMER CASE STUDY

Large Enterprise Energy & Utilities Company

Background

This large Energy and Utilities enterprise operates in a highly complex environment, especially in regards to maintaining their critical infrastructure. They struggled with an enormous amount of manual processes that slowed down their ability to aggregate and act on critical threat intelligence, resulting in missed alerts and an inability to respond effectively to emerging threats. Siloed teams compounded the problem with inconsistent data sharing and limited visibility across teams. This organization's critical use cases are phishing analysis and response, automated malware analysis, and generating strategic intel.

Business Challenges

Prior to implementing the ThreatConnect TI Ops Platform, their threat intelligence processes were outdated, relying heavily on manual aggregation and ad-hoc collaboration. They struggled with prioritizing threats, keeping cybersecurity spend within budget, responding effectively and efficiently, and generating actionable intelligence.

CTI Team Needs

To support their mission of ensuring the resilience of the company's critical systems, the CTI team needed to integrate, aggregate, and correlate threat intelligence from multiple sources in a single repository for analysis and action. They also needed a means to continuously monitor intelligence and alerts and automate workflows to enhance their threat response capabilities. This would enable them to identify threat actor behaviors, understand emerging trends, and make informed decisions to proactively improve infrastructure security. This organization was struggling to keep efficiency up, spending costs down, and save time across its entire security team.

> "Having all the relevant intelligence feeds in one place makes our detection and response process very efficient."
>
> – SOC team lead, Energy & Utilities Company

Solution

The organization implemented the ThreatConnect TI Ops platform to bridge the gap between their existing technologies and processes, providing a comprehensive platform to centralize threat intelligence data, automate workflows, integrate with other security tools, and measure performance. With automated workflow capabilities in place and centralized data at their fingertips, they were able to accurately prioritize threats, better understand their environment, and respond more effectively. The platform delivered a powerful solution that allowed the team to continuously monitor threats while reducing manual workloads with faster response time. This led to significant cost and time savings and enabled the analysts to focus on higher-value tasks.
In addition, by leveraging the platform's integrated analytics and reporting capabilities, the organization was able to generate actionable intelligence, enabling them to make more informed decisions. With improved visibility into their environment, they could identify patterns previously hidden from view and take steps toward improving their defense posture while detecting threats faster and mitigating risks more effectively.

Why They Chose ThreatConnect

Unlike a traditional threat intelligence platform (TIP), ThreatConnect goes beyond simply collecting threat intelligence to enable its customers to truly operationalize intel to improve response times, enhance collaboration, and improve efficiency. The platform's flexibility and scalability were particularly attractive to this customer, making ThreatConnect the natural choice to meet their needs.

Implementing the ThreatConnect TI Ops Platform revolutionized how this organization leveraged threat intelligence to improve its cyber defenses. It bridged the gap between their existing technologies and processes, providing a comprehensive solution that enabled their team to centralize threat intelligence data, automate workflows, integrate with other security tools, and measure performance.

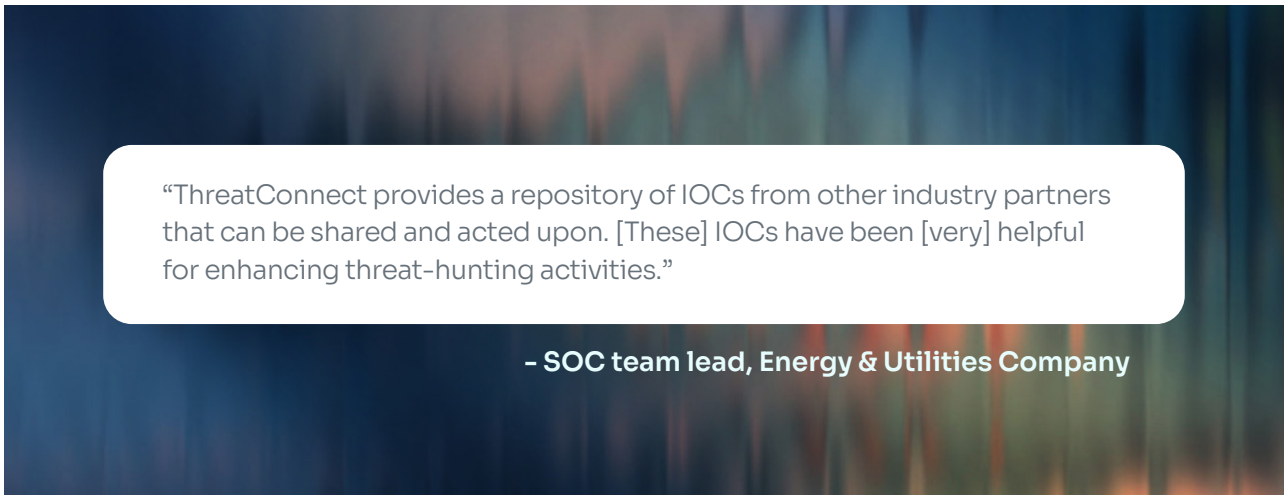
With automated workflow capabilities in place and centralized data at their fingertips, they were able to accurately prioritize threats, better understand their environment, and respond more effectively. Manual processes were replaced with automated ones, ensuring threat intelligence was aggregated swiftly and efficiently. The organization's teams became better aligned and their processes integrated, breaking down silos and enabling effective collaboration.

This organization witnessed a few other remarkable savings and improvements. With annual cost savings of $500K, they significantly reduced expenses across the board.
They also optimized their workflows and increased efficiencies by 90%, allowing for smoother operations and enhanced productivity. Additionally, they experienced 74% more time saved per week, resulting in significant time freed up for other critical tasks. Our platform truly revolutionized their operations, offering unparalleled value and efficiency.

With ThreatConnect, this organization gained real-time visibility into potential threats and the ability to take proactive action to bolster defenses and respond to threats rapidly, reducing the potential for attacks or disruptions to their critical processes and overall infrastructure.

Benefits of ThreatConnect's Threat Intelligence Platform

With ThreatConnect's Threat Intelligence Operations Platform, security teams are empowered to achieve breakthrough effectiveness. Putting Threat intelligence at the core of their security operations enables teams to gather, analyze, and prioritize crucial information from a single platform. The ThreatConnect Platform provides the tools and capabilities to transform raw data into actionable insights, enhancing proactive threat mitigation and operationalization of threat intelligence. It's highly scalable and flexible, and organizations can adapt and grow their security operations seamlessly. The platform integrates AI and ML capabilities, low-code automation, and robust interoperability, allowing teams to focus on what matters to improve cyber defenses.



Cost Savings	Increased Efficiencies	Time Savings
$500K	**90%**	**74%**
COSTS SAVED PER YEAR	INCREASED EFFICIENCY PER MONTH	TIME SAVED PER WEEK

Reach out to learn how the ThreatConnect Platform can make you and your team more effective, decisive, and collaborative.

+1 (800) 965.2708 - or - https://threatconnect.com/request-a-demo

ThreatConnect.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets. **Learn more at www.threatconnect.com.**

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708