ThreatConnect.

Customer Spotlight

Enterprise Software Brand Slashed False Positives and Boosted Efficiency with Targeted Threat Intelligence

Customer Profile

Org. Size	*Industry/Sector*	*Headquarters*
7,000+ EMPLOYEES	INTERNET SOFTWARE & SERVICES	SAN JOSE, CA

Products Used: TI OPS | POLARITY

Background

As a global leader in automation software, this enterprise operates a complex, distributed environment spanning multiple regions and time zones. With 24/7 "follow-the-sun" operations and a vast digital footprint, the company faces an increasingly diverse and dynamic threat landscape. Recognizing that basic OSINT and bulk threat ingestion were no longer sufficient to inform their defense, the organization sought a more advanced and scalable approach to threat intelligence. By implementing ThreatConnect TI Ops with Polarity, the team was able to strengthen collaboration across geographies, accelerate investigations, and improve accuracy through automation and contextualized intelligence.

Challenges Faced

Despite its own deep expertise in automation, this software provider's cybersecurity program faced growing challenges in managing and contextualizing vast amounts of threat data. Traditional intelligence feeds delivered excessive information and limited actionable insight, overwhelming analysts and slowing investigations. The team's distributed nature made it difficult to align intelligence requirements and maintain shared visibility into threats across global operations.

Key challenges included:

- Inefficient threat intelligence workflows that slowed down investigations
- Excessive signal noise that hampered visibility into threats
- Difficulty maintaining global alignment across time zones and teams
- Reduced investigation speed and accuracy due to repetitive context switching
- Fragmented visibility into threats across a distributed attack surface

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

sales@threatconnect.com
+1.703.229.4240

How ThreatConnect Helped

This robust, forward-looking tech company needed a flexible, scalable system that would enable their cybersecurity team to surface relevant information quickly during time-sensitive investigations. The enterprise chose ThreatConnect for its versatile customization, powerful search, and automation capabilities — enabling more intelligent contextualization, faster response times, and more informed security decisions.

The enterprise leveraged ThreatConnect TI Ops Platform to automate remediation actions, intel enrichment, and malware analysis, and Polarity to speed up intelligence collection and repetitive research and lookups — all from a single pane of glass. Other key use cases included:

- Intelligence requirements that align security priorities, precisely track intel, and maximize CTI program planning and direction.
- Integrations that minimize tool-switching and allow intel and security controls to work together to fully protect their business.
- Dashboards to automatically monitor security operations and intelligence to easily visualize data and provide actionable insights into cybersecurity threats.

By leveraging ThreatConnect's automation and advanced CTI capabilities, the company's global security team now operates with greater efficiency, alignment, and confidence — enabling faster detection, reduced analyst fatigue, and improved decision-making across all time zones.

Results Include:

- 50–75% reduction in false positives
- Faster, more consistent global investigations
- Enhanced visibility and prioritization across a distributed attack surface
- Increased efficiency through automation and tool integration
- Stronger collaboration across global "follow-the-sun" operations

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.

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

sales@threatconnect.com
+1.703.229.4240