ThreatConnect.
now a part of Dataminr

Customer Spotlight

Large Diversified Financial Services Enterprise Scaled Threat Intelligence with ThreatConnect

Customer Profile

Org. Size	*Industry/Sector*	*Headquarters*
>200,000 EMPLOYEES	DIVERSIFIED FINANCIAL SERVICES	U.S. BASED

Products Used: TI OPS

Background

As a major global financial services enterprise, this organization operates in one of the most highly targeted sectors for cyber attacks. Sophisticated adversaries, regulatory scrutiny, and complex business operations require a mature, centralized approach to threat intelligence. While the company had strong security capabilities, it lacked a unified framework for aggregating, analyzing, and actioning threat intelligence across its many business units.

Security leaders saw that their teams were spending too much time stitching together intelligence sources rather than using that intelligence to drive decisions. To modernize their intelligence program and improve cross-team coordination, the organization turned to ThreatConnect.

Challenges Faced

As a long-time ThreatConnect customer, this diversified financial services enterprise has spent years maturing its threat intelligence program in partnership with ThreatConnect. Early in the relationship the security team needed to streamline how threat intelligence was collected, analyzed, and actioned across a broad and complex financial ecosystem.

Prior to adopting a unified approach, intelligence lived in pockets across the organization, limiting visibility and slowing collaboration between teams. Over the course of the partnership, ThreatConnect has played a central role in co-creating and refining the organization's intelligence workflows, helping them transition from fragmented, team-specific processes to a more cohesive, enterprise-wide threat intelligence function.

Key challenges included:

- Establishing a unified, centralized threat intelligence library
- Reducing reliance on manual enrichment and analysis
- Improving cross-team sharing of threat insights
- Increasing visibility into attacker behaviors across business units
- Creating consistent, repeatable intelligence workflows
- Laying the groundwork for automation across SIEM, EDR, XDR, and SOAR systems

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

sales@threatconnect.com
+1.703.229.4240

How ThreatConnect Helped

The enterprise selected ThreatConnect TI Ops to centralize its threat intelligence lifecycle and provide a single, authoritative platform for analysis, correlation, and enrichment. With TI Ops, the security team can now:

- Perform advanced ATT&CK-aligned threat analysis
- Detect and prevent threats earlier with high-fidelity intelligence
- Work from a unified threat library accessible across teams
- Generate strategic and operational intelligence for leadership
- Push intelligence into operational tools for faster response
- Automate enrichment and repetitive research tasks
- Prioritize vulnerabilities based on attacker behavior and likelihood
- Accelerate threat hunting with rich contextual data
- Build and maintain threat models across business units

For example, when new phishing infrastructure or malware campaigns are detected, ThreatConnect allows analysts to quickly correlate domains, IPs, and malware to known actors and campaigns, determine exposure across business units, and push validated intelligence into SIEM and EDR for immediate blocking and detection.

Features That Drive the Most Impact

- Integrations with SIEM, EDR, XDR, and SOAR tools to operationalize intelligence
- Automation (Playbooks) to reduce manual workloads and improve response times
- CAL Automated Threat Library, aggregating enriched intel from numerous sources
- Threat Scoring that helps analysts cut through noise and focus on what matters

> "Imagine if you had 1 interface to watch all of your favorite streaming shows, regardless of what streaming service you subscribe to? That is what ThreatConnect does for disparate intelligence feeds. It consolidates all into one platform, allowing for additional analysis and correlation."
>
> **— Principal Engineer**

Unifying Threat, Risk, and Action Across Teams

TI Ops has transformed the organization's security posture, strengthening intelligence maturity and reducing business risk. By automating workflows and correlating enterprise-wide data, the platform empowers teams to make faster decisions and prioritize action with confidence. This strategic foundation now supports both regulatory compliance and proactive defense against fast-moving threats.

Results Achieved:

- Reduced overall business risks
- Enabled team to make faster, more informed security decisions
- Better contextualize and prioritize threats and risks

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