ThreatConnect.
now a part of Dataminr

Customer Spotlight

Scaling Threat Intelligence for a Global Professional Services Leader

Customer Profile

Organization Size
470,000+ EMPLOYEES

Industry/Sector
ENTERPRISE PRO SERVICES

Headquarters
LONDON, ENGLAND

Background

As one of the world's largest professional services organizations and a member of the Big Four, this enterprise operates at an extraordinary scale — supporting clients across highly regulated, high-risk industries including financial services, healthcare, government, and technology.

That scale makes the organization a significant and persistent target for cyber threats. With a vast global footprint, complex infrastructure, and diverse risk exposure, the company requires a threat intelligence program that is not only sophisticated, but deeply integrated across its broader security ecosystem. To stay ahead of adversaries, the organization needed a platform capable of unifying threat intelligence, improving collaboration between teams, and enabling faster, more confident action across security operations.

Challenges Faced

Before ThreatConnect, the organization's threat intelligence was hindered by **siloed tools** and **manual workflows**. Fragmented integrations with SIEM, SOAR, and EDR platforms slowed response times and limited cross-team collaboration.

Simultaneously, analysts were overwhelmed by high-volume, low-context alerts. This excessive noise forced teams to spend their time manually triaging data rather than focusing on proactive threat hunting and strategic analysis.

Key challenges included:

- **Operational Inefficiency:** Heavy reliance on manual, time-intensive processes and fragmented tools (SIEM/SOAR/EDR) hindered scalability.
- **Intelligence Fatigue:** Excessive noise and low-quality data lacked the context necessary to assess threat relevance or impact.
- **Organizational Silos:** Limited visibility and poor collaboration between CTI and security operations teams stalled proactive defense.

What they needed: a centralized, scalable threat intelligence platform that could unify tools, reduce noise, provide actionable context, and support collaboration across teams — without adding complexity.

How ThreatConnect Helped

The enterprise partnered with ThreatConnect to modernize its program, moving from fragmented workflows to a unified TI Ops Platform. By integrating AI and automation, the team now aggregates and acts on high-fidelity intelligence at scale, mapping data directly to their specific organizational needs..

Operationalizing Intelligence Through Automation

Using TI Ops, the organization automates core CTI processes to:

- **Enrich & Contextualize:** Link adversaries and malware for a complete threat picture.
- **Accelerate Response:** Automate remediation and threat-hunting workflows.
- **Inform Strategy:** Generate high-level intelligence for leadership risk initiatives.

> "ThreatConnect is a critical part of our operations... a high-quality platform for managing threat data and operationalizing intelligence." **— Threat Manager**

Measurable Results

The platform transformed isolated tasks into a cohesive system, breaking down silos between CTI and SOC teams to enable faster, more consistent decision-making. By feeding high-fidelity context directly into SIEM, EDR, and SOAR workflows, the organization achieved:

- 75% Reduction in MTTD and MTTR
- 75% Increase in CTI analyst efficiency
- 50% Reduction in false positives

ThreatConnect also enhanced the effectiveness of the organization's broader security tooling — including SIEM, EDR, XDR, and SOAR — by feeding high-fidelity, contextual intelligence directly into operational workflows.

Just as importantly, the platform enabled stronger collaboration between the CTI team and other security stakeholders, reinforcing a more proactive, unified security posture across the enterprise.

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