ThreatConnect.
now a part of Dataminr

CUSTOMER CASE STUDY

Banking and Finance Organization Matures Threat Intelligence Operations with ThreatConnect

"Matching around 2 million indicators against internal data set every 30 minutes"

Background

A UK banking and finance organization knew it was time to mature its threat intelligence program. Being a little late to the game, they were able to observe the approaches their industry peers took to implement a TIP or to operationalize threat intelligence.They learned they needed a clearly defined strategy and approach to ensure the platform they implemented was effective.

Business Challenges

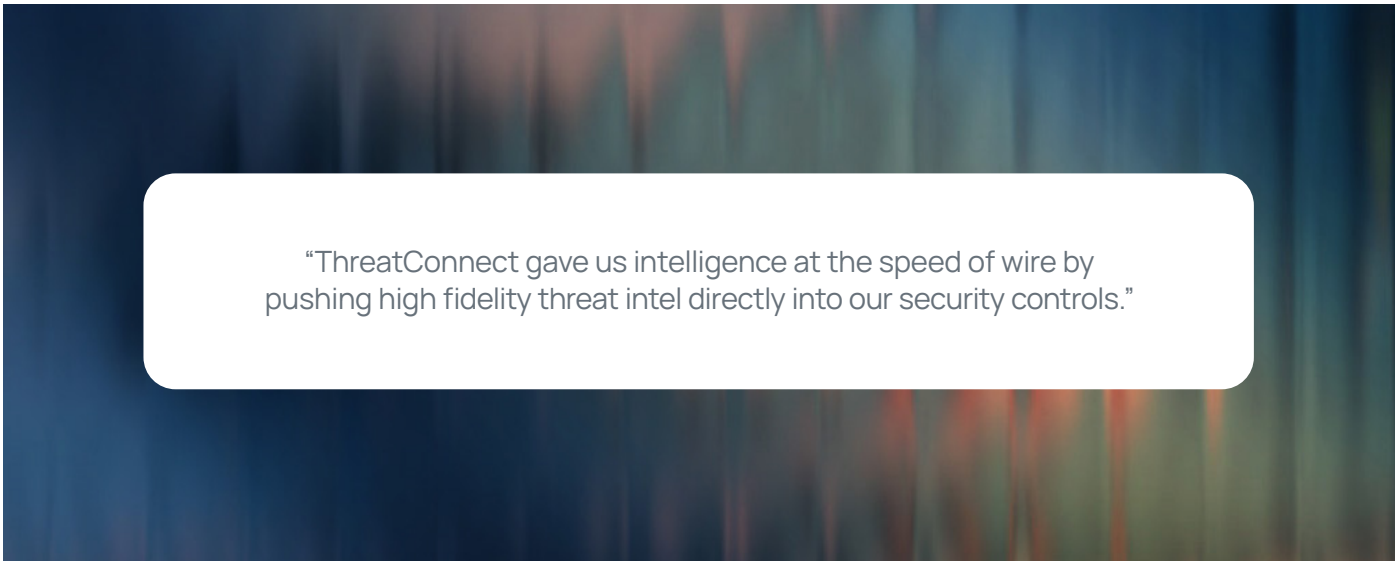
The organization's threat intelligence platform was mature but lacked automation and tooling. It had limited resources and lacked scalability but was still expected to analyze the same amount of data and produce intelligence as a mature organization. The Cyber Threat Intelligence Lead remembers having "significant challenges in the amount of intelligence we were receiving."

They needed a TIP to take their operations to the next level and help parse through tens of millions of indicators from multiple data sources. They needed a platform that was feature-rich that allowed analysts to dig into the data to understand what the intelligence was telling them and be able to leverage the data against their logs to surface high-fidelity threat intelligence to their other security teams, including their fraud team.

Why they Chose ThreatConnect

ThreatConnect rose to the top as a leader in the threat intelligence space due to its scalability, maturity, and functionality to help solve these problems and meet the organization's goals. What stood out about ThreatConnect was that it was more than just a management solution to push normalized data. It went beyond these capabilities with Case Management and workflow, Playbooks to automate processes, and indicator enrichment, like out-of-the-box geolocation information. Most importantly, ThreatConnect was able to meet all of this organization's needs within a single platform rather than other vendors that required them to purchase multiple products to meet the same needs.

Threat Intelligence Lead, that enabled "intelligence at the speed of wire" by pushing high-fidelity intelligence directly to its security controls with fully automated processes for data ingestion and data analysis. Automating the analysis and dissemination of threat intelligence helps power investigations for its security operations center and helps focus analysis done by the threat hunting and analytics team. "ThreatConnect allows us to look at things from a start-to-finish perspective to understand the decisions made at every step."



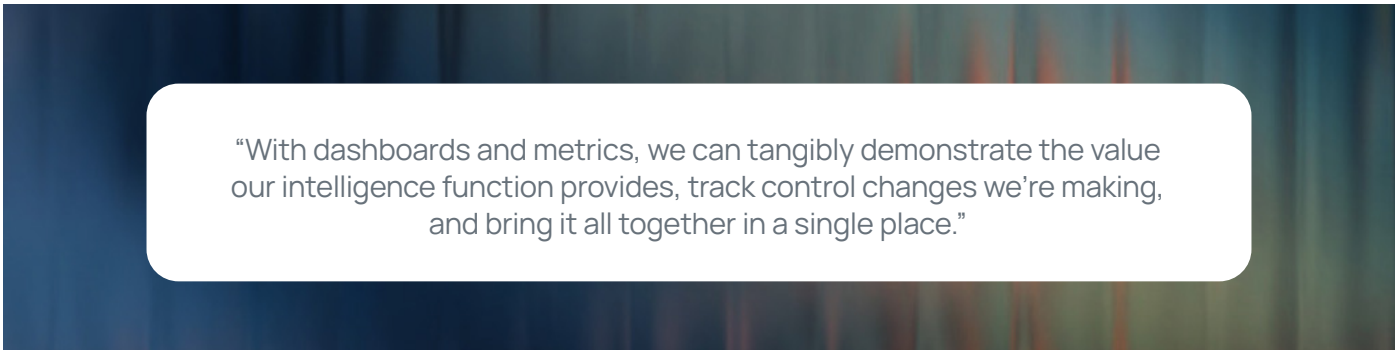
Ultimately, ThreatConnect helped the organization meet use cases across its 18 PIRs (Priority Intelligence Requirements), including defending against phishing attacks, Initial Access Brokers, Nation States, insider threats, and supply chain attacks while managing and prioritizing vulnerabilities and improving its perimeter defenses. The organization also leverages the in-Platform Diamond Model approach to understand the adversary, victim, infrastructure, and capabilities to draw links and associations.

"On day one with ThreatConnect, there was a trigger for an indicator related to a North Korean threat group. We immediately had a level of visibility we didn't have previously because we couldn't consume all the incoming data."

Benefits of ThreatConnect

By scaling threat intelligence operations and improving visibility across the threat environment, the organization could easily measure its ROI from the ThreatConnect Platform. Prior to ThreatConnect, they were manually reviewing around 40 indicators per day. Now, they're matching around 2 million indicators against their internal data set every 30 minutes.

ThreatConnect empowered this cyber threat intelligence team to easily prove the value they provided to other security teams and across the organization.



The organization now runs over 4,000 Playbooks per month, saving its team and organization about 675 hours and more than £55,000 pounds per month.

Overall, they view the ThreatConnect team as a true partner that goes above and beyond to support its organization and help reach its security goals.

Playbooks Run	Time Savings	Cost Savings
40,000	**675**	**£55,000**
Per Month	Hours Saved Per Month	Cost Savings Per Month

Find out what ThreatConnect can do for your organization. Schedule a demo today!

https://threatconnect.com/request-a-demo

ThreatConnect. now a part of Dataminr

By operationalizing threat and cyber risk intelligence, The ThreatConnect Platform changes the security operations battlefield, giving your team the advantage over the attackers. It enables you to maximize the efficacy and value of your threat intelligence and human knowledge, leveraging the native machine intelligence in the ThreatConnect Platform. Your team will maximize their impact, efficiency, and collaboration to become a proactive force in protecting the enterprise. **Learn more at www.threatconnect.com.**

ThreatConnect.com

3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708