Customer Story | Financial Services

The New Science of Threat Detection

Adversaries are already inside most organizations' networks, and security operations teams are often blind to these incursions. The security operations team at this leading financial services company relies on Vectra AI to gain visibility and can stop an attack in progress before damage is done.

Industry
Financial services

The Challenge
Protect prominent financial services against opportunistic and targeted attacks

The Solution
Security solution that delivers credible threat intelligence

The Results
- Detect hybrid attacks in real time
- Gain clarity about the most important threats
- Augment the cyber kill chain

Vectra AI is the cornerstone of security operations at leading securities exchange

The financial markets are a favorite target of cyberattackers, whether they are trying to disrupt the global economy, make a political statement or commit an act of war.

From the banks to dealers, clearing houses to exchanges, the industry strives to maintain the availability and integrity of the financial infrastructure. It's a massive challenge, where one worker's misstep or moment of inattention can lead to compromised systems, financial loss and damage to corporate reputation.

The Challenge

Enhancing the cyber kill chain

"We wanted to augment our cyber kill chain and controls because of the sophisticated nature of malware and its rapid transformation," says the deputy CISO at a premier financial services company in the U.S..

This financial services company is well prepared to defend against the everyday cybercrimes of monetary gain and reputational damage as well as black swan events. To stay ahead of bad actors and criminals, it continually improves its information security controls and systems — including relying on the Vectra AI Platform for threat detection and response.

Vectra AI provides hybrid attack surface coverage, real-time Attack Signal Intelligence and integrated, automated and co-managed response — detecting and prioritizing attacks so the team is still able to stop them post compromise.

The Solution

Advanced surveillance

"Vectra AI is like an advanced surveillance system in your house," says the deputy CISO. The reality is that adversaries are already inside most organizations' networks, and security operations teams are often blind to these incursions. With Vectra AI, the exchange's security operations team gains visibility and can stop an attack in progress before damage is done.

"Vectra AI gives us actionable intelligence so we can focus our resources to find the threat," he says.

Take the example of a targeted attack. If an email with an infected attachment, such as a zero-day vulnerability, that bypasses the service's perimeter defenses, enters an exclusive part of the network and the intended recipient opens it, it can infect the user's computer. From there, it may begin click fraud or virtual currency mining, or worse, it may perform reconnaissance of the internal network, infiltrate deeper into the network, or acquire data and eventually move it offsite. "In such a scenario, malware could be in the environment that may take days or weeks to be caught," he says.

Vectra AI listens to users' traffic to and from the Internet and the data center to identify anomalous behavior. It learns the typical behaviors on the network and correlates anomalous behaviors that it has seen hours, days or even weeks before. "There will always be some activity that leaves a footprint, if only for a moment," he says. "Vectra AI shows me the footprint and shows me how to navigate the threats."

Shift the focus to investigations

Vectra AI detections matter. Analysts can't afford to sift through many thousands of alerts to define the real threats. Vectra AI automatically displays the more significant threats in real time based on contextual scoring. Because Vectra AI listens, learns and remembers traffic and behaviors, it can distill and report the most important of these behaviors and analyze them over days, weeks or even months.

"The Vectra AI Platform can help analyze the patterns and drive through the gaps. With Vectra AI, the analyst can see high amounts of integrity in the detections and can focus on where he should drive next," he says.

"Vectra AI shows me the footprint and shows me how to navigate the threats."

Deputy CISO
Financial Services

The Results

Immediate and long-term value

Vectra AI has quickly become an essential part of the service's operations. "We got value out of Vectra AI on Day 1," says the deputy CISO. "Vectra AI helped me see things that we couldn't see before."

For example, Vectra AI helped identify a misconfiguration with its Kerberos authentication systems. It turned out that a weak encryption algorithm was being used and the situation was promptly remedied. "We would never have known about the root of the misconfiguration without Vectra AI," he says.

The value is growing. "We are operationalizing Vectra AI as the brains of our cybersecurity," he says. "Vectra AI will make our analysts' jobs much easier." With Vectra AI deployed, security analysts can investigate more deeply, rather than vetting whether the threat is real.

Vectra AI is also playing a role in helping meet the service's regulatory and audit requirements. "Regulatory oversight is greater and greater, and we have to prove that a control is working," he says. "Vectra AI gives us transparency so we can find control weaknesses and remediate them quickly."

The deputy CISO has more plans for the Vectra AI Platform, including integration with its Splunk security information and events management (SIEM) for even more insight and protection. "Vectra AI is part of the new science of threat detection," he says.

"Vectra AI is part of the new science of threat detection"

Deputy CISO
Financial Services

Read more customer stories

About Vectra AI

Vectra AI is the leader in AI-native security and observability. Vectra AI delivers organizations real-time visibility into their network, clear insight into which behaviors matter, and the ability to act before risk becomes impact. By connecting on-premises, multi-cloud, identity, SaaS, edge, and IoT/OT infrastructure, Vectra AI helps organizations reduce exposure, accelerate detection and response, and automate security operations with AI. With over a decade of AI and ML innovation, 39 patents and a Leader in the 2025 and 2026 Gartner Magic Quadrant for Network Detection and Response, Vectra AI empowers security teams to stay ahead of emerging AI powered attacks, increase operational efficiency, and prove resilient in an increasingly complex, AI-driven world. For more information, visit www.vectra.ai.

For more information please contact us: Email: info@vectra.ai | vectra.ai