Case Study

# 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 securities exchange relies on Vectra to gain visibility and can stop an attack in progress before damage is done.

## Cognito 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.

## 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 securities exchange in the U.S.

This exchange 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 and recently added the Cognito® network detection and response platform from Vectra® to its defenses.

### Organization

Securities Exchange

### Industry

Financial services

### Challenge

Protect prominent securities exchange against opportunistic and targeted attacks

### Selection criteria

Security solution that delivers credible threat intelligence

### Results

- Detect advanced persistent attacks in real time
- Gain real-time insight into the most important threats
- Augment the cyber kill chain

VECTRA®
Security that thinks®

Cognito provides malware detection and real-time insights into advanced persistent attacks on the network. Cognito detects any phase of an ongoing cyberattack as it happens and describes what the attacker is doing. Cognito machine learning adapts as attacks evolve and anticipates the attackers' next move in real time so it can be stopped.

## Advanced surveillance

"Vectra 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 Cognito, the exchange's security operations team gains visibility and can stop an attack in progress before damage is done.

"Cognito gives us actionable security 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 exchange'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.

Cognito listens to users' traffic to and from the Internet and the data center to identify anomalous behavior. Cognito 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 shows me the footprint and shows me how to navigate the threats."

## Shift the focus to investigations

Cognito detections matter. Analysts can't afford to sift through many thousands of alerts to define the real threats. Vectra's innovative Threat Certainty Index™ automatically displays the more significant threats in real time based on contextual scoring. Because Cognito 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.

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

## Immediate and long-term value

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

For example, Cognito helped the exchange 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 Cognito," he says.

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

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

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

> *"We are operationalizing Vectra as the brains of our cybersecurity."*
>
> Deputy CISO
> Securities Exchange

VECTRA®
Security that thinks®

**Email** info@vectra.ai **Phone** +1 408-326-2020 www.vectra.ai