VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Vectra keeps Private Research Institution well ahead of cyberattackers

Charles Davidson started work as an information security analyst at a Private Research Institution, during a wave of uncertainty.

"I remember hearing the security engineers talk about a ransomware attack that was pretty intense," says Davidson. "They'd re-image machines in the morning and then do it again in the afternoon. They were really busy back then."

That was then. This is now.

Established in 1865, this Research Institution has more than 6,500 students and an academic staff of nearly 500 at its sprawling 95-acre campus in the United States.

"Things have changed so much since I joined years ago," he says. "There's far less stress and I feel like we have most everything covered."

Davidson equates the positive changes to having a better understanding of the network environment and threat landscape. And he credits the Cognito® network detection and response (NDR) platform and Sidekick Services™ from Vectra® for that transformation.

"It was like getting a new pair of binoculars. You don't realize what you're missing until you can see with absolute clarity."

Charles Davidson
IT Security Analyst
Private Research Institution

Organization

Private Research Institution

Industry

Higher Education

Challenge

Manual workload and risk of a second ransomware attack

Selection criteria

An AI-based Network Detection and Response (NDR) solution to automate SOC inefficiencies and prevent ransomware attacks

Results

- Ability to prioritize security alerts and visibility into when a compromised host is part of a larger attack campaign
- Sidekick services that help enable the security team identify and focus on what they need to fix
- Speedy response workflows to stop in-progress attacks faster

"Cognito with Sidekick support services enabled us to identify and focus on what we needed to fix," Davidson says. "It was like getting a new pair of binoculars. You don't realize what you're missing until you can see with absolute clarity."

Light years beyond the security industry's definition of NDR, the Cognito NDR platform uses AI-derived machine learning algorithms and deep learning to automatically detect, prioritize and respond to in-progress attack behaviors that pose the highest business risk – across cloud, data center, IoT, and enterprise networks.

"Vectra automation reduces the manual part of our workload," says Davidson. "We like Cognito because of its ability to detect and prioritize security alerts. We can even see when a compromised host is part of a larger attack campaign."

Sidekick Services enable the Research Institution's information security team to work with Vectra security experts who meticulously analyze the results from Cognito NDR deployments, identify critical security events, and provide remediation and investigative recommendations.

"Sidekick Services are an extra set of eyes for us," says Davidson. "It's great knowing that Vectra has my back to verify events and offer corrective measures. In one of our weekly meetings, a Sidekick engineer told me he saw botnet monetization behaviors that we traced to a student who was mining cryptocurrency."

> "As our primary security weapon, we're constantly squeezing as much intelligence out of Vectra as we possibly can,"
>
> **Charles Davidson**
> *IT Security Analyst*
> *Private Research Institution*

Defense in depth

For faster response time, the Cognito NDR platform integrates and shares attack context and insights with third-party security solutions – including EDR, SIEMs, SOAR tools, NAC, and next-generation firewalls – for end-to-end visibility and coordinated response workflows.

"We apply the knowledge we get from Vectra to our next-generation firewall and other security devices as part of a multilayered defense-in-depth approach," says Davidson. "This speeds-up response workflows to stop in-progress attacks faster."

The Research Institution takes response actions to the next level by integrating the Cognito NDR platform with deep process-level host context from their endpoint protection solution.

Vectra also sends Cognito platform detections to their SIEM for immediate analysis. These detections include direct links to the Cognito platform for even deeper analysis of individual threats. Forensic analysis about incidents are identifiable by devices, accounts and the type of attack.

Additionally, the Vectra threat intelligence feed proactively identifies and stops known attacks. When these known malicious behaviors are detected, Vectra instantly blocks and isolates attackers instead of cutting off resources to all users.

This combined effort results in improved security efficiency and reduces attacker dwell times that can increase business risk for the Research Institution. Vectra eliminates network blind spots by combining a 360-degree aerial view of all network interactions with an in-depth ground-level view.

"As our primary security weapon, we're constantly squeezing as much intelligence out of Vectra as we possibly can," notes Davidson. "We also use our SIEM as an investigative tool and I'm always pivoting back and forth between the two."

Dealing with constant change

Unlike most office environments, network devices at the Research Institution are constantly on the move. Students and staff connect in one class, then in another class in a different building, in residence halls, in the library, in labs and offices, and even outdoors. And every year, legions of new students arrive on campus with multiple personal devices.

"Vectra works well for us because it understands attackers, user roles, devices, locations, and credential misuse," says Davidson. "It links every threat behavior to specific phases of the attack lifecycle – command and control, internal reconnaissance, lateral movement, and data exfiltration."

One particular command-and-control incident detected by Vectra led the Research Institution information security team to a student who was using a Microsoft Surface Pro tablet. Vectra detected malicious traffic between the Surface Pro and a command-and-control server in Russia.

"The student didn't know that traffic was going to a malicious site," recalls Davidson. "We immediately reconfigured our firewalls to block the malicious IP address and contacted the student to remediate the threat. Although the Surface Pro was running anti-virus and anti-malware products, the software didn't flag the command-and-control behavior."

"This shows that we wouldn't know what's happening inside our network without Vectra," he adds. "The insights we get all day, every day, are critical. It makes me a better analyst and a better engineer."

> "The insights we get all day, every day, are critical. It makes me a better analyst and a better engineer."
>
> **Charles Davidson**
> *IT Security Analyst*
> *Private Research Institution*

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai