VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Electricity distribution to homes and businesses

Hydro Ottawa automates threat detection and response to dramatically reduce the time spent on threat investigations

More than 323,000 business and residential customers depend on Hydro Ottawa for power. Attacks on electrical grids and utility providers have been surging, and for Hydro Ottawa, the largest distributor in eastern Ontario, delivering electricity means protecting its corporate IT and critical infrastructure systems from cyberattacks.

Cyberattacks are a reality

"The reality is cyberattacks are going to happen," says Jojo Maalouf, IT security manager at Hydro Ottawa. "That means you have to be able to detect and remediate threats as quickly as possible. We were using a log aggregator that required a lot of manual threat hunting."

"That's why we turned to Vectra," Maalouf explains. "Vectra is a security analyst in software that handles tedious, labor-intensive threat hunting and automatically detects, scores and prioritizes the highest-risk threats. This dramatically reduces the time we spend on threat investigations."

The Cognito® network detection and response platform from Vectra® augments the work of security analysts at Hydro Ottawa using artificial intelligence and a combination of data science, machine learning and behavioral analysis. Although cybercriminals are adept at concealing their presence in your network, Cognito reliably detects and exposes their attack behaviors – even in encrypted traffic.

With Cognito, the Hydro Ottawa security team can rapidly detect cyberattackers that evade firewalls, intrusion prevention and endpoint security systems and spread inside the network in search of key assets to steal or destroy.

HydroOttawa

Organization

Hydro Ottawa

Industry

Public utilities

Challenge

Close the gap between infection and detection

Selection criteria

Automate threat management that is simple to use and integrates easily with other security tools

Results

- Faster threat detection and response
- Eliminates manual threat hunting and speeds-up threat investigations
- Highest-risk threats are automatically scored and prioritized so security teams can quickly stop attackers before damage is done
- Advanced cybersecurity protection based on the NIST framework

Vectra automates tedious, labor-intensive threat hunting and detects, scores and prioritizes the highest-risk threats.

Jojo Maalouf
IT Security Manager
Hydro Ottawa

Automating threat management

"Vectra does exactly what we need," says Maalouf. "Our team can act instantly to stop attackers before they have a chance to steal data or damage critical infrastructure. The actionable information we get from Vectra is incredibly useful."

By detecting threats in real time on the corporate network, Hydro Ottawa can prevent targeted attacks from spreading to the operational network and eliminate disruptions to the distribution of power throughout the region.

Hydro Ottawa also has visibility into all phases of a cyberattack. Cognito exposes fundamental attack behaviors like command-and-control communications, internal reconnaissance, lateral movement, and data exfiltration as well as the early signs of ransomware, remote access tools, hidden and encrypted tunnels, backdoor vulnerabilities and administrative credential abuse.

In addition, Cognito monitors physical and virtual hosts to detect signs of compromise or insider threats. And by using supervised and unsupervised machine learning, Cognito easily adapts to the changing network environment to detect unknown and known threats.

More effective security operations

"Vectra has made our entire security operation far more effective and we conduct threat investigations with much greater efficiency," says Maalouf.

The Vectra Threat Certainty Index™ plays a significant role in boosting efficiency. It automatically consolidates thousands of threat events and historical context to pinpoint infected hosts that pose the greatest risk with the highest degree of certainty.

"I love the quadrant-based design of the Vectra user interface," he says. "Quite intuitively, the threats that are the biggest risk to our organization appear in the upper-right of the screen."

Threat and certainty scores can trigger notifications to the Hydro Ottawa security team or a response from endpoint security, firewalls, SIEMs and other enforcement points. For example, Maalouf has alerts set up for data exfiltration.

Cognito also provides context so the security team can stop threats faster. Key hosts and other assets are explicitly tracked and security analysts can instantly see devices that infected hosts communicate with and how. And on-demand access to metadata from packet captures speeds-up incident response.

Maalouf appreciates that Cognito analyzes network traffic as its authoritative source, rather than looking in the rearview mirror with log data. "Network traffic is the single source of truth," he says.

This newfound efficiency has led Hydro Ottawa to improve threat remediation by creating plans to integrate Cognito with Carbon Black endpoint security, its IBM QRadar SIEM, and Palo Alto Networks firewalls.

Simplifying audits

Maalouf noted that the actionable threat information from Cognito is instrumental in helping Hydro Ottawa conduct internal audits and implementing the NIST cybersecurity framework. The NIST framework offers guidelines and recommendations for identifying cybersecurity risk as well as detecting, responding and recovering from threat events.

“With Vectra, I was able to close the gap between infection and detection,” says Maalouf.

Nevertheless, “compliance is just a baseline,” he says. Protecting the distribution of electricity means strong security practices as well as meeting compliance regulations.

Adding immediate value

The time-to-value with Cognito was swift at Hydro Ottawa. While proof-of-concept tests for security are legendarily time-intensive, Maalouf described the Cognito evaluation as “very easy.”

Cognito has continued to add value from that first day, and has become an essential part of the Hydro Ottawa security operations team.

“With Vectra’s early-detection capabilities, we have more confidence in stopping cyberattackers before critical infrastructure is damaged or valuable data is stolen,” says Maalouf. “Vectra has even helped us eliminate vulnerabilities by changing the configuration of specific network devices.”

Cognito has continued to add value from that first day, and has become an essential part of the Hydro Ottawa security operations team.

Email info@vectra.ai vectra.ai

For more information please contact a service representative at sales-inquiries@vectra.ai.