VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Mega-producer of consumer goods relies on Vectra in the SOC

Fenaco is one of those big companies you haven't heard of. And there's good reason for that. Named by Deloitte as a large producer of consumer goods, Fenaco operates and sells its products almost exclusively in Switzerland.

The 7 billion CHF ($7.7 billion U.S.) company, founded in 1993 as a merger of six agricultural cooperatives, employs 10,000 people and is indirectly owned by about 43,000 cooperative members, 22,000 of them active farmers.

Fenaco ensures that Swiss foods reach consumers – from fruit, vegetables, potatoes and grain to meat and beverages. Its business units cover the agriculture, energy, retail, food industry, transport, chemicals, and veterinary medicine sectors.

Keeping this complex ecosystem of 50 business units safe and operational is Fenaco Informatik, the cooperative's IT, telecommunications and security organization.

"Our security operations had been decentralized, meaning each team had its own set of security tools. Most were relying on firewalls and logs to secure the perimeter of the network."

Gustavo Ricco
Security Operations Manager
Fenaco Informatik

fenaco

Organization

Fenaco

Industry

Consumer goods

Challenge

Decentralized security operations and limited visibility provided by perimeter security tools.

Selection criteria

An AI-based network detection and response (NDR) solution to automate SOC inefficiencies.

Results

- Threat coverage with visibility into attack behaviors inside their network and in traffic going to and from the internet
- Automation of manual tasks giving more time to focus on critical requirements like threat hunting and incident investigations
- Prioritized detections that make critical alerts easy to address

"Vectra offered excellent visibility about what attackers do inside the network"

Gustavo Ricco
Security Operations Manager
Fenaco Informatik

The challenge: Building a SOC

"Our security operations had been decentralized, meaning each team had its own set of security tools," recalls Gustavo Ricco, security operations manager at Fenaco Informatik. "Most were relying on firewalls and logs to secure the perimeter of the network."

However, perimeter security is difficult and costly to scale and is easily bypassed by cyberattackers. It also offers zero visibility into cyberattackers who evade perimeter defenses to spy, spread and steal inside networks.

But change was coming. The company knew it had to modernize its organization into a single security operations center (SOC) to prevent unnecessary redundancies and overlap that can drive up costs.

Ricco, who today is head of the security operations center, knew that a fully operational SOC was the only way to deal with cyberthreats in its network and data center. He clearly understood the role of AI-based network detection and response (NDR) in automating many SOC inefficiencies.

For example, many security operations teams are overburdened by manually investigating thousands of threat alerts per day that might or might not represent attacks. Chasing-down every indicator causes significant alert fatigue and gives real attacks more time to spread.

The solution: AI-driven NDR

Fenaco Informatik considered several NDR solutions.

"Vectra offered excellent visibility about what attackers do inside the network," says Ricco. "So, we went with Vectra, specifically Cognito Detect and Cognito Stream software, which both run on the Cognito platform."

With help from Vectra®, Fenaco underwent a very rapid time-to-value on its investment in the Cognito® platform. The company's modernized SOC became fully operational in just two to three months.

The Cognito platform from Vectra is light years beyond the security industry's definition of NDR. It takes a huge leap forward in solving the formidable challenges faced by SOC teams who are entrusted to protect critical business data.

Running on the Cognito platform, Cognito Detect™ applies AI-derived machine learning algorithms to automatically detect and respond to in-progress cyberattack behaviors in cloud/SaaS, data center, IoT, and enterprise networks.

Attack behaviors that pose the greatest risk with the highest degree of certainty are automatically prioritized, enabling SOC analysts at Fenaco to immediately determine where to start remediation, hunting and investigating.

To further reduce time and resources, Cognito Detect rolls-up multiple alerts into a single incident or attack campaign for investigation. AI-based machine learning automatically ties related threat detections into a chain of events.

"Vectra automated many manual tasks in our SOC," says Ricco. "This gives us much more time to focus on critical requirements like threat hunting and incident investigations."

The gold standard in data

The secret to the effectiveness of the Cognito platform is the data. It extracts, analyzes and stores relevant logs, cloud events and metadata at scale from all network traffic – from cloud/SaaS and data center workloads to user and IoT devices.

This metadata is then enriched with deep security insights and context, which provides unprecedented visibility to detect, respond, hunt and investigate cyberthreats with extraordinary efficiency and precision.

"We have excellent threat coverage with visibility into attack behaviors inside our network and in traffic going to and from the internet," explains Ricco. "The detections are always prioritized so we know which ones are critical to address first."

Faster threat hunting and investigations

The Fenaco SOC team uses Cognito Stream™ on the Cognito platform to speed-up threat investigations that are launched in response to critical attack detections.

Cognito Stream delivers security-enriched metadata at scale from native cloud, hybrid cloud and enterprise traffic, which empowers Fenaco SOC analysts to perform more conclusive incident investigations.

With Cognito Stream, the Fenaco SOC team can leverage the deep security insights and unique context from Vectra to build custom tooling and feed models to detect, investigate and hunt for attacks.

Delivered in open-source Zeek format, Cognito Stream seamlessly integrates security insights and context about attacks into data lakes – and in the case of Fenaco, its Splunk SIEM – without the overhead and scale limitations that accompany open-source Zeek.

For faster response, the Cognito platform integrates and shares the same context and insights with third-party security solutions – including EDR, SIEMs and SOAR tools – for end-to-end threat management and visibility.

"The integration between Vectra and Splunk was so simple and easy that we were able to get up and running in the SOC very quickly," says Ricco. "Now we look at Vectra for the most critical alerts and we send syslogs and metadata to Splunk for investigations."

"Along with Splunk, Vectra has been instrumental in reducing threat investigations from several days to just a few hours," Ricco adds.

"The integration between Vectra and Splunk was so simple and easy that we were able to get up and running in the SOC very quickly. Now we look at Vectra for the most critical alerts and we send syslogs and metadata to Splunk for investigations."

Gustavo Ricco
Security Operations Manager
Fenaco Informatik

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai