VECTRA

Customer Story | Consumer Goods

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

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.

fenaco

**Organization**
Fenaco

**Industry**
Consumer goods

**The Challenge**
Decentralized security operations and limited visibility provided by perimeter security tools.

**The Solution**
An AI-driven network detection and response (NDR) solution to automate SOC inefficiencies.

**The 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

**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-driven 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.

**"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."**

**The Solution**

## AI-driven NDR

Fenaco Informatik considered several NDR solutions.

"Vectra AI offered excellent visibility about what attackers do inside the network," says Ricco. "So, we went with Vectra AI, specifically the Vectra AI threat detection and response platform with Attack Signal Intelligence™"

With help from Vectra AI, Fenaco underwent a very rapid time-to-value on its investment in the Vectra Threat Detection and Response (TDR) platform.

The Vectra AI Platform 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.

Vectra AI applies AI 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, Vectra AI rolls-up multiple alerts into a single incident or attack campaign for investigation and automatically ties related threat detections into a chain of events.

"Vectra AI 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 integration between Vectra AI 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 AI for the most critical alerts and we send syslogs and metadata to Splunk for investigations."**

**Gustavo Ricco**
Security Operations Manager
Fenaco Informatik

**The Results**

## The gold standard

Vectra AI is able to erase unknown threats with the best AI-driven threat detection and response platform for hybrid and multi-cloud enterprises delivering the Attack Coverage, Signal Clarity and Intelligent Control security teams need to get ahead and stay ahead of modern cyber-attacks.

"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 Vectra Stream to speed-up threat investigations that are launched in response to critical attack detections.

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

Delivered in open-source Zeek format, Vectra 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 Vectra AI 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 AI 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 AI for the most critical alerts and we send syslogs and metadata to Splunk for investigations."

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

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

**Gustavo Ricco**
Security Operations Manager
Fenaco Informatik

## About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

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