VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Commodities trader finds sweet spot with AI-powered threat detection

Security integration and automation enable ED&F Man to detect and stop attacks faster

ED&F Man Holdings has been trading sugar, coffee, molasses, and animal feed since the late 1700s. The company sources, stores, ships and distributes agricultural products around the world. It also helps customers and suppliers manage pricing risk through hedging and acts as a broker for hedge funds and professional traders.

Several years ago, a security incident served as a wake-up call to the increasing success of cyberattacks. An independent assessment indicated that the company needed to significantly step up its cybersecurity processes, tools and people.

ED&F undertook a complete security transformation.

Crystalizing a cybersecurity strategy

Carmelo Gallo took over as the cybersecurity manager to protect the operations of the $10 billion company that has a presence in 60 countries.

A focus on next-generation security technology, integration and automation has rapidly accelerated the company's security maturity.

Insight into hidden threats

Cognito®, the AI-driven threat detection and response platform from Vectra®, was a foundation of the ED&F security transformation.

"Cognito was key in our journey," says Gallo. "We started with the network because Cognito is easy to install and we get immediate visibility into attacker behaviors that hide in traffic."

ED&F MAN
EST. 1783

Organization

ED&F Man Holdings Ltd.

Industry

Commodities

Challenge

Transform security operations to mitigate cybersecurity risk

Selection criteria

Network threat detection and response that integrates with its endpoint detection and response and SIEM solutions

Results

- Integrated network detection and response, endpoint detection and response, and security analytics to streamline SOC operations
- Quickly identify and prioritize the highest-risk threats to stop attacks faster
- Cut investigation time from hours to minutes
- Reduced priority alerts from 800 to five per month

We used to get 200 alerts a week. Now with Cognito, we have four or five a month."

Carmelo Gallo
Cybersecurity Manager
ED&F Man Holdings Ltd.

The Cognito platform collects and stores the right network metadata and enriches it with unique security insights. Cognito Detect uses security-enriched metadata and sophisticated machine learning techniques to detect and prioritize attacks in real time.

Cognito's high fidelity means the ED&F security team has greater confidence in alerts and a lower number of high priority incidents to investigate. "We used to get 200 alerts a week," says Gallo. "Now with Cognito, we have four or five a month."

ED&F soon added Cognito Recall for AI-assisted threat hunting. "When we get an alert in Cognito Detect, we go straight to Cognito Recall and look at the metadata to see what the host is doing," says Gallo.

Integration streamlines operations

Security automation and integration delivered operational efficiency and improved the user experience.

ED&F also deployed next-generation endpoint detection and response and easily integrated its insights via the Cognito REST API. "The integration was seamless," says Gallo. "Before, it would take more than an hour to correlate the IP address to a host name and user name. Now it's done in minutes."

High and critical alerts from Cognito Detect are fed directly to its managed SOC provider, ensuring that security teams on three continents are working from a single source of truth.

Employing the SOC visibility triad of network detection and response, endpoint detection and response, and SIEM provides broad visibility into threat history and significantly reduces the chance that attackers can operate on the network long enough to accomplish their goals.

Automation and integration enable the security team to scale without adding more staff. "Automation is the way forward," says Gallo. "Automating repetitive, menial tasks also helps employee retention because people are freed up to do more interesting work."

Identify known and unknown threats

With Cognito, ED&F can quickly detect threats across its global environment, including 140 offices and multiple data centers.

Cognito has detected and defeated multiple man-in-the-middle attacks intent on invoice fraud. It stopped a sneaky cryptomining scheme in Asia. It found command-and-control malware that had been hiding for several years.

"We found the command-and-control malware with Cognito," says Gallo. "Signature-based security never saw it."

Cognito has been key to identifying risky employee actions, such as using unapproved remote-control software or storing files in public cloud services.

"Cognito gives us meaningful information about data exfiltration behaviors," says Gallo. "It would take a day to find it using firewall logs, and that's an impossible amount of time."

Real-world data makes cybersecurity awareness training more relevant. "If we see more ransomware or man-in-the-middle attacks in a particular month, we can do more training on that topic," says Gallo.

Earned the trust of the business

The ED&F security team is a trusted partner to the business units.

With a fresh attitude and a different approach, Gallo has turned around the perception of IT security as an obstacle.

"I can't remember the last time we said 'no' to the business," says Gallo. "We say here's the risk, and here's the solution you can use to alleviate the risk. We want to stop malicious activity but we don't want to stop the business."

That philosophy has paid off. "The business has faith that we're delivering against our objectives," says Gallo. "Our business relationships are second to none."

Get control of privileged accounts

Transformation is a journey, and ED&F continues to mature its security operations.

With privileged accounts a common entry point for cyberattackers, the team is exploring Cognito's new suite of Privileged Access Analytics (PAA) detection models, which monitors the interactions between user accounts, services and hosts.

"Privileged Access Analytics gives me continuous visibility into the accounts, services and hosts that are most valuable to me," says Gallo. "We can easily scrutinize the behaviors on each to see if they represent a significant risk to our organization."

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

Email info@vectra.ai vectra.ai

A true partnership

Working with Vectra has been different. "My experience working with vendors is that it's driven by the sales cycle," says Gallo.

"Vectra conducts a quarterly business review and gives us access to the right people to make sure our journey is a success," he continues. "Vectra is passionate about putting the customer first."

"Vectra is passionate about putting the customer first." **Carmelo Gallo**
Cybersecurity Manager
ED&F Man Holdings Ltd.