VECTRA
SECURITY THAT THINKS.®

CASE STUDY

INDEVCO relies on Vectra for complete visibility and proactive threat detection

A multinational manufacturing and industrial consultancy group founded in 1955, INDEVCO produces a wide portfolio of corrugated, paper, and plastic raw materials and packaging, jumbo tissue rolls, consumer and away-from-home disposables, renewable energy solutions, converting machinery, and CNC machined parts.

They serve a wide array of industries in nearly 90 countries worldwide, motivated by a grounding principle of sustainable development underscoring their dedication to integrating environmental sustainability and social responsibility in their operations.

With over 38 manufacturing plants and 38 commercial companies across the globe, INDEVCO needed a solution to help them better protect data and keep their operations running smoothly.

"Because of the rising threats, we decided to invest in a new security layer. We were looking for an NDR and Vectra was the most convincing."

Chadi Khadij
Head of Network and Security
INDEVCO

INDEVCO

Organization

INDEVCO

Industry

Manufacturing

Challenge

Traditional systems based on signatures or attack patterns only detect threats that are known to the system

Selection criteria

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

Results

- Swiftly identify and prioritize the highest-risk threats to stop attacks faster
- Integrate network detection and response, endpoint detection and response, and security information and event management to streamline SOC operations
- Threat coverage with visibility into attack behaviors inside their network

Choosing the right solution

Cognito®, the AI-driven threat detection and response platform from Vectra®, was key to developing a new security layer for INDEVCO's security operations center (SOC).

INDEVCO already had an open-source security information and event management (SIEM) solution and an endpoint detection and response (EDR) solution, but they still had trouble detecting internal threats, gaining visibility into their network, and maintaining network hygiene. This prompted them to seek a network detection and response (NDR) solution.

"We didn't have NDR before. Because of the rising threats, we decided to invest in a new security layer," said Chadi Khadij, Head of Network and Security at INDEVCO. "We were looking for an NDR and Vectra was the most convincing."

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 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.

Employing the SOC visibility triad of NDR, EDR, 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.

With help from Vectra, INDEVCO underwent a very rapid time-to-value on its investment in the Cognito platform. Once deploying Vectra, "it only took one week for Cognito to begin adding value to the company's SOC," said Khadij.

Better visibility, less noise

One of the key challenges INDEVCO faced when protecting their organization against cyberattacks was sifting through data. "We had thousands of logs coming and didn't know what was true or what was a false positive," Khadij disclosed.

> "Since deploying Vectra, we are now able to detect all types of threats across the enterprise in real time, and with a degree of precision that enables us to investigate and respond so quickly in a way that was not possible before."
>
> **Chadi Khadij**
> *Head of Network and Security*
> *INDEVCO*

"Most of the detections we received were produced by some of our legitimate applications that don't necessarily work in a concise way," Khadij explained. "Since deploying Vectra, we are now able to detect any types of threats across the enterprise in real time, and with a degree of precision that enable us to investigate and respond so quickly in a way that was not possible before."

The Vectra user interface provides fully customizable dashboards that allow users to prioritize alerts in quadrants, to pinpoint which alerts and detections require the most attention. The quadrant-based design intuitively displays the threats that are the biggest risk to an organization in the upper-right of the screen. This reduces the dwell time for analysts and enables them to tackle the most critical threats first.

In addition, the Vectra Threat Certainty Index™ plays a significant role in boosting efficiency. It automatically consolidates thousands of threat events and historical context to zero in on infected hosts that pose the greatest risk with the highest degree of certainty. Once located, these key hosts and other assets are explicitly tracked so security analysts can instantly see devices that infected hosts communicate with and how.

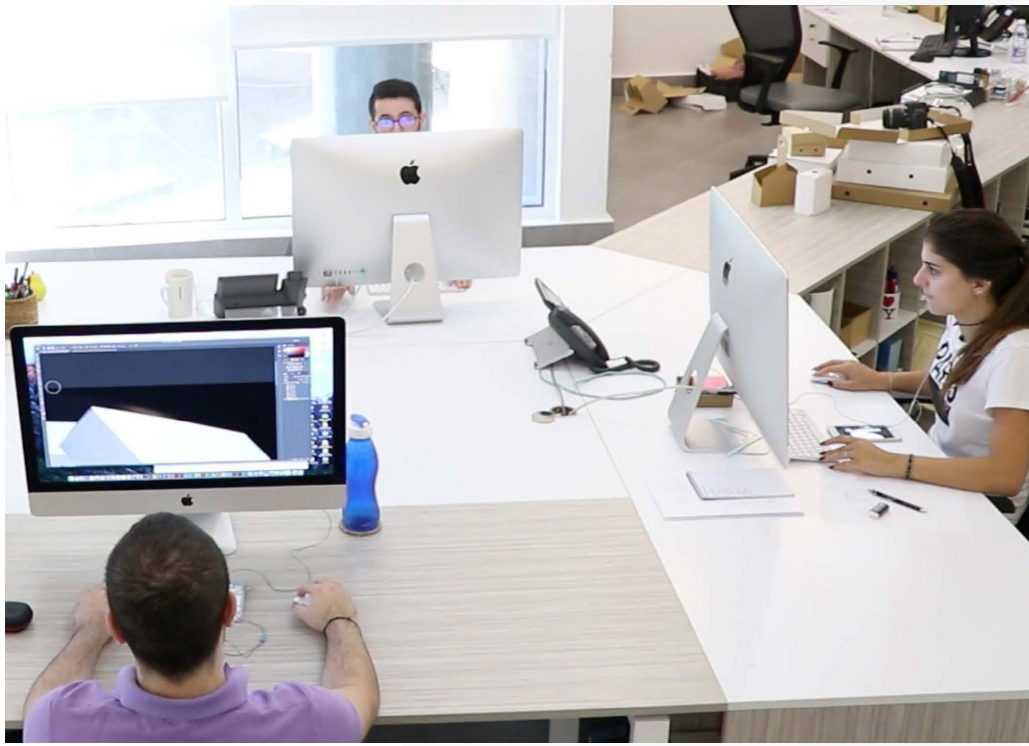
To further reduce time and resources for INDEVCO's security team, Cognito Detect rolls-up multiple alerts into a single incident or attack campaign for investigation. AI-based machine learning automatically ties related threat detections into a chain of events.

> "We are profiting the most from knowing what makes the most noise on the network and seeing why it was that way."
>
> **Chadi Khadij**
> *Head of Network and Security*
> *INDEVCO*

Swift threat hunting and resolution

"Since we deployed Vectra," Khadij shared, "we realized that we became able to prioritize threat detections based on their criticality, which helps us gain immense productivity time in our security operations as our analysts now focus their efforts on investigating the most critical detections and responding to them in almost real time. They avoid wasting time on less critical threats that are dealt with once the most critical alerts are resolved."

When it comes to Vectra, Chadi Khadij put it simply: "I think this is the best way for us to reduce the risk of breach."



By uniquely combining data science and security research, Vectra provides threat detection as a next layer of defense in today's security infrastructure – from cloud/SaaS and data center workloads to users and every type of connected device.

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

Email info@vectra.ai vectra.ai