VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Vectra gives beauty industry retailer a cybersecurity makeover

Every year, this global retail giant in the beauty industry hires consultants to conduct red team exercises to test the mettle of cybersecurity operations. And every year it failed.

"The red team would come in, leave and send us the results," says an information security architect at the company. "It was always the same – fail. We were getting fed up with it."

Unfortunately, the seven-member security operations center (SOC) team was saddled with a lean security budget despite having to maintain network security for hundreds of stores and a busy online retail business.

"We own the security of our stores – including all point-of-sale devices – and hundreds of other devices that are connected to the network," says the information security architect.

"A few years back I told my boss that if cyberattackers were in our network right now, we wouldn't know it," he says. "This was the problem we needed to solve and network detection and response was the solution we considered."

The retailer had a SIEM for log collection and forensics and endpoint detection and response (EDR).

Network detection and response (NDR) would identify attackers that bypass firewalls and IPS at the network perimeter and provide visibility into threats inside the network.

Showdown: Vectra vs. ExtraHop

The SOC team narrowed NDR down to two finalists – Vectra® and ExtraHop – which were operational in a proof-of-concept test. And by coincidence, at the same time the company was engaged in another red-team penetration test.

"Vectra clearly outperformed ExtraHop. Vectra detected red team activity during the proof-of-concept. That was the first time we ever detected a threat."

Information security architect
Beauty industry retailer

Organization

Global beauty retailer

Industry

Retail

Challenge

Needed visibility inside the network to detect and respond to hidden cyberattackers.

Selection criteria

A network detection and response platform that would identify attackers that bypass firewalls and IPS at the network perimeter and provide visibility into threats inside the network.

Results

- The SOC team passed red team testing for the first time with the Cognito® NDR platform from Vectra.
- A reduced SOC workload gives the security team more time to investigate incidents and proactively hunt for threats.
- Delivery of security insights and context about every attack, enabling the retailer's SOC team to perform faster more conclusive incident investigations.

"Vectra detected red team activity during the proof-of-concept," says the information security architect. "That was the first time we ever detected a threat."

ExtraHop eventually showed some detections, he says. "It appeared to be rule based instead of AI-based machine learning, and it didn't triage any detections for us. Vectra clearly outperformed ExtraHop."

Cognito Detect™, which runs on the Cognito® NDR platform from Vectra, uses AI-derived machine learning algorithms to automatically detect, triage, prioritize and respond to in-progress attack behaviors that pose the highest business risk – across cloud, data center, IoT, and enterprise networks.

By combining advanced machine learning techniques with always-learning behavioral models, Cognito Detect quickly and efficiently finds hidden and unknown attackers before they do damage.

"Vectra consolidates hundreds of events and historical context about attacks and correlates this data with compromised host devices," says, the information security architect. "This lets us respond faster to stop attackers and prevent data breaches."

By automating manual Tier-1 and Tier-2 security tasks, Vectra significantly reduced the SOC workload and gave the security operations team more time to investigate incidents and proactively hunt for threats.

"With Vectra, what used to take months now takes minutes," he says. "There's no need to sort through massive volumes of logs and chase down every single alert."

Vectra also delivers security insights and context about every attack by extracting metadata from all network traffic, as well as relevant logs from workloads and SaaS applications like Office 365.

This enables the retailer's SOC team to perform faster, more conclusive incident investigations and AI-assisted threat hunting.

"It's so simple and intuitive to use and I didn't need a five-day course to learn how to use it," he says. "I can easily see where attackers are hiding and what they're doing. The important details are always at my fingertips."

In addition to empowering quick, decisive action in response to cyberattacks, Cognito Detect provides a vital starting point for professional threat hunters that use Cognito Recall™ for deeper investigations.

As a comprehensive source of security network metadata, "Cognito Recall allows us to proactively hunt for threats and conduct more conclusive incident investigations," says the information security architect.

The ultimate pen test

Two red-team penetration tests were held since the Cognito NDR platform from Vectra was deployed. This time the results were completely different.

“I was able to see the red-team attack in progress and isolated the threat by turning off a switch port,” he says. “Later they did another, more elaborate pen test in one of our stores.”

Red-team consultants showed up at one of the retail stores dressed as company technicians with official-looking paperwork to get inside and access a rack of networking equipment.

“They connected to the store’s network rack and started the attack exercise,” he recalls. “Vectra detected the threat in minutes and we shut them down. Our executives wanted to know how we detected the attack so quickly and we told them – the answer is always the same, it was Vectra. That was pretty impressive.”

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

Email info@vectra.ai vectra.ai