VECTRA

Customer Story | Retail

Vectra AI Gives Beauty Industry Retailer a Cybersecurity Makeover

As a major specialty retailer with a strong presence across North America and Europe, the beauty company supports millions of shoppers both in stores and online. With a small team managing a diverse retail and corporate environment, maintaining visibility and control across every corner of the business has become essential to keeping operations moving.

Organization
Global Beauty Retailer

Industry
Retail

The Challenge
A lean SOC struggled to detect attackers operating inside a large retail environment, repeatedly missing red-team activity despite having traditional security tools in place.

The Solution
With the Vectra AI Platform, the team gained real-time visibility across network and identity, achieved a 100% success rate in identifying red-team behaviors, and reduced noise through automated triage, enabling faster, more confident investigations.

Security Transformation

Platform value at a glance

Vectra AI's Impact	Outcome
Coverage	• Detected red-team behaviors in real time, giving the SOC visibility into attacker movement across network and identity. • Identified compromised accounts immediately during a large smishing attack, enabling rapid containment.
Clarity	• Highlighted meaningful behaviors while suppressing noise, eliminating blind spots that hid earlier red-team activity. • Delivered richer context with each detection, reducing investigation time from months to minutes.
Control	• Removed attackers within an hour of entry, giving the team tighter control over active threats. • Reduced manual workload through automated triage and event correlation, allowing analysts to focus on deeper investigations.

The Challenge

Where traditional defenses stop short

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 the CISO. "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 CISO.

Despite having a SIEM for log collection and endpoint detection and response (EDR) in place, the team still lacked visibility into attacker behavior inside the network. As the CISO explained:

"Although EDR is important, bad guys are finding their way around EDR. Before, cybersecurity was about protecting the perimeter, but that's changed. When the bad guys get in, the only thing that's going to save you is detecting them and getting them out of your network before they can cause damage."

They needed a way to detect attackers who bypassed perimeter defenses and to see suspicious behavior across both network and identity.

The Solution

Showdown: Vectra AI vs. ExtraHop

The SOC team narrowed its NDR evaluation to two finalists: Vectra AI and ExtraHop. Both platforms were deployed during a proof-of-concept test, which coincided with another red-team engagement.

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

ExtraHop surfaced some detections but appeared rule-based and lacked triage capability. "Vectra AI clearly outperformed ExtraHop," he said.

He went on to explain what he values in any security platform:

"There are three things I look for in a security platform. First, the ability to detect true positives — and Vectra AI has had a 100% success rate in detecting pen tests, red teams, and real incidents. Second, the noise level. If a critical alert is buried under a thousand false positives, it's almost the same as missing it. And third, the ability to tune the platform so the SOC can focus on the alerts that truly matter."

Streamlined triage and investigation

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

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

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

Vectra AI 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 Microsoft 365.

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

Clear signal the team can act on

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

"There are three things I look for in a security platform. First, the ability to detect true positives — and Vectra AI has had a 100% success rate in detecting pen tests, red teams, and real incidents. Second, the noise level. If a critical alert is buried under a thousand false positives, it's almost the same as missing it. And third, the ability to tune the platform so the SOC can focus on the alerts that truly matter."

CISO
Global Beauty Retailer

"With Vectra AI, we're able to eject them within an hour of getting into our network."

CISO
Global Beauty Retailer

The CISO noted how Vectra AI compares to their broader toolset:

"Not only is it Vectra AI that's alerting us — our other security tools most of the time don't alert us, or at best maybe we'll get an alert 24 hours later. The only one that's consistently alerted us is Vectra, and that's been the case for several years now."

Identity visibility also proved critical. As the CISO reflected:

"A few years ago, a large smishing attack targeted our users. Vectra AI was the only tool that alerted us when the first account was compromised. Without it, we wouldn't have known the attack was underway."

The Results

Real-time detection of red-team activity

Two red-team penetration tests were held after the Vectra AI Platform 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," says the CISO. "Later they did another, more elaborate pen test in one of our stores."

Red-team consultants later showed up dressed as company technicians with official-looking paperwork to access networking equipment in a retail store.

"They connected to the store's network rack and started the attack exercise," he recalls. "Vectra AI 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."

Reflecting on the team's current capability:

"With Vectra AI, we're able to eject them within an hour of getting into our network," he continued. "Before we had Vectra AI, we had no confidence. We weren't detecting red teams or pen tests, but since then, I have a very high confidence that if a bad guy is in our network, we will detect them."

Turning signal into speed

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

The Vectra AI Platform continues to provide enriched context and investigative depth, helping the SOC stay ahead of attacker behavior across the retailer's environment.

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

CISO
Global Beauty Retailer

Read more customer stories

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