VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Global financial services firm banks on NDR to stop cyberattacks

When this global financial services company deployed the Vectra® network detection and response solution, "it was as if the fog suddenly lifted from our security operations," says the firm's head of cybersecurity.

He is of course referring to Cognito®, the NDR platform from Vectra that detects and responds instantly to elusive cyberattacks against cloud and data center workloads, services like Microsoft Office 365, and user and IoT devices.

With over $118 billion in assets, visibility into the hidden actions of cyberattackers is critically important to this independent financial services company, whose rich history in banking and asset management dates back 150 years.

From zero to 100

"We went from zero to 100 percent visibility into attacker behaviors with Vectra," says the company's head of cybersecurity. "We were amazed at what Vectra could see inside network traffic. We get context and details about every attack and know which ones are the most critical."

However, the road to success was not easy to navigate.

"When I first started, we already had a SIEM," he explains. "But nobody really took care of it, so it was outdated and required a lot of software patches. We rebooted it and leveraged the security tools we had but it was still quite a challenge."

In those early days, the company's the security operations center (SOC) was in constant reactive mode. According to the head of cybersecurity, it was like putting out fires. The SOC team would see smoke and rush over to investigate.

"We went from zero to 100 percent visibility into attack behaviors with Vectra."

Head of security
Global financial services firm

Organization

Financial company

Industry

Financial services

Challenge

Their security team was in constant reactive mode. They were working off of homegrown solutions that required a lot of software patches.

Selection criteria

A platform that would enable their security team to proactively detect and respond to hidden threats inside their networks.

Results

- Gained more value from Vectra in a week than from configuring their SIEM for an entire year
- No longer have to sift though DHCP logs or identify IP address changes during an investigation
- Cognito Detect tells his team every critical alert worth investigating and how to go about resolving it

The company started to evaluate potential NDR solutions, including Darktrace and Vectra. The SOC team hoped that the right NDR solution would enable them to proactively detect and respond to hidden threats inside the network.

"We weren't convinced by Darktrace," says the head of cybersecurity. "It had a dazzling interface but didn't operate very efficiently."

Conversely, the company's SOC team described its first experience with Vectra as "quite pleasant" and "empowering" to use. Vectra even detects attacker behaviors in encrypted traffic without requiring any decryption or deep packet inspection.

"Vectra was up and running quickly" said the head of cybersecurity. "It was easy to use and the graphical dashboard was very intuitive to navigate. You don't have to be a cybersecurity expert to use Vectra."

For its NDR solution the financial services company ultimately chose Vectra –Cognito Detect™ for Office 365, Cognito Detect and Cognito Recall™, all running on the Cognito platform.

A hunting we will go

Credential abuse is the leading cyberattack method used against Office 365, which has more than 200 million monthly users. Smart attackers will exploit human behavior to hijack passwords, takeover accounts and steal critical business-data.

To combat this, the company's SIEM had been receiving Office 365 logs, which required the SOC team to configure time-consuming setup rules. But that tedious, manual work has been eliminated since deploying Cognito Detect for Office 365.

"We gained more value from Vectra in a week than we gained from configuring our SIEM for an entire year," says the head of cybersecurity.

Cognito for Office 365 ingests activity logs from multiple services like Office 365, Azure Active Directory, SharePoint, OneDrive and Exchange. Vectra analyzes logins, file creation and manipulation, DLP configuration, and mailbox routing configuration and automation changes.

Vectra applies AI-derived machine learning algorithms to proactively detect and respond to attack behaviors in these services to avert damage and theft. Detections are correlated to accounts and prioritized based on risk, giving security professionals a complete attack narrative to quickly stop and mitigate threats.

"Vectra gives all the necessary threat information to our SOC analysts," says the head of cybersecurity. "Cognito for Office 365 is priceless."

The power to detect and recall

In the enterprise, the financial services company relies on Cognito Detect to identify and stop in-progress cyberattackers that can easily evade firewalls, IDPS and other perimeter security.

"Cognito Detect is absolutely essential," says the head of cybersecurity. "It extracts value out of the box in a short amount of time. Every critical alert that appears in the dashboard is worth investigating, and Cognito tells you exactly how to go about it."

He also likes the flexibility to deploy sensors anywhere they are needed in the network. “I can deploy as many sensors as I want to get rid of blind spots in traffic,” he notes. “The entire platform is easy to use, fast and well-integrated.”

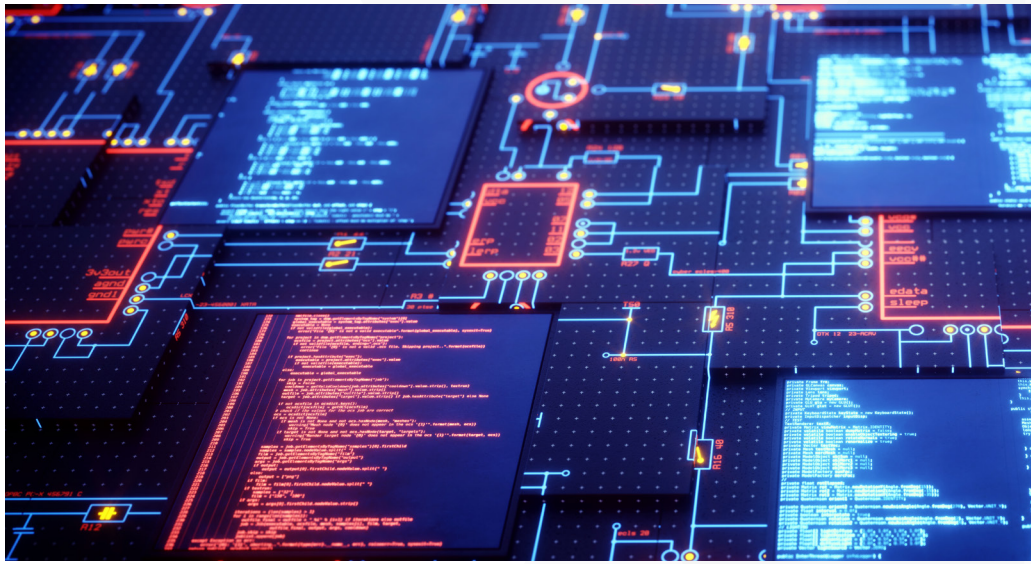
The company also deployed AI-driven Cognito Recall, a cloud-hosted investigative workbench that uses security-enriched metadata to dramatically improve threat hunting and incident investigations.

Vectra extracts, analyzes and stores relevant logs, cloud events and metadata at scale from all network traffic, including cloud/SaaS and data center workloads and user and IoT devices. Metadata contains no personal information, which protects data privacy and ensures compliance with strict financial services policy mandates.

This metadata is then enriched with deep security insights and context about every attack. This gives the financial services company unprecedented visibility to detect, respond, hunt and investigate cyberthreats with greater efficiency and precision.

“I can deploy as many sensors as I want to get rid of blind spots in traffic. The entire platform is easy to use, fast and well-integrated.”

Head of security
Global financial services firm



The enriched metadata contains no personal information, which protects data privacy and ensures compliance with financial services governance policies and regulatory mandates.

The metadata also includes host names, not just IP addresses. “We don’t have to sift through DHCP logs to find a device IP address or identify IP address changes during an investigation,” says the head of cybersecurity. “Searching for host names is much faster when you have little time.”

For this financial services company, the Cognito platform is an essential part of its SOC, enabling the organization to take a proactive approach to identifying and stopping potentially catastrophic cyberattackers.

Email info@vectra.ai vectra.ai

© 2020 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.Version: **100520**

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