VECTRA
SECURITY THAT THINKS.®

CASE STUDY

GMMH NHS Foundation Trust stops attacks with Cognito for Office 365

Credential abuse, also known as an account takeover, is the leading cyberattack method used against software-as-a-service (SaaS) platforms. This is especially true for Microsoft Office 365, which has more than 200 million monthly users.

The sheer quantity of individuals using the service increases the chance that cyber hygiene will fall by the wayside, and knowledgeable attackers will exploit human behavior to gain high-privilege access to critical business-data.

This was a wakeup call for Greater Manchester Mental Health, an NHS foundation trust in North West England. The trust has about 5,400 employees, more than 140 locations, and provides mental health services for 53,00 patients a year.

"Before we deployed Vectra, we had limited visibility into malicious behaviors inside network traffic or Office 365," says Kevin Orritt, ICT security manager at Greater Manchester Mental Health. "We're impressed by what we can now see."

Running on the Cognito® platform from Vectra®, Cognito for Office 365 ingests activity logs from multiple services like Office 365, Azure Active Directory, SharePoint, OneDrive and Exchange.

NHS
Greater Manchester Mental Health
NHS Foundation Trust

Organization

Greater Manchester Mental Health NHS Foundation Trust

Industry

Healthcare

Challenge

Limited visibility into malicious behaviors inside network traffic or Office 365

Selection criteria

Automated threat detection to reveal hidden attacks and full network visibility

Results

- Visibility into threat behaviors across entire network
- Confidence to detect and stop credential abuse that is common in Office 365
- Ability to be proactive rather than reactive, providing more time to work with their end-user community

With a deep understanding of Office 365 application semantics, Vectra applies AI-derived machine learning algorithms to proactively detect and respond to hidden cyberattackers before damage or theft occurs.

Vectra analyzes events like logins, file creation and manipulation, data leakage protection configuration, and mailbox routing configuration and automation changes. It exposes attacker behavior patterns.

Detections are correlated to accounts and prioritized based on risk, giving security professionals a complete attack narrative to respond and mitigate threats quickly.

"Vectra gives us much better visibility into threat behaviors across our entire deployment," says Orritt. "We now have a greater degree of confidence that we can detect and stop credential abuse that has become common in Office 365."

"The onboarding and training was straightforward compared to other systems we've deployed that require a lot of time and effort to implement and configure."

Kevin Orritt,
ICT security manager at Greater Manchester Mental Health

Radar love

Greater Manchester Mental Health had its challenges on the network side, too. Despite antivirus software, a LogPoint SIEM and next-generation firewalls, network detection and response (NDR) had been on the radar for quite some time.

Greater Manchester Mental Health considered other NDR solutions but found it was cost-prohibitive and difficult to navigate. "Vectra was far more intuitive, easy to use and simple to understand," Orritt says.

After consulting with other NHS foundation trusts who deployed and recommended Vectra and knowing that it worked well in other NHS environments, Greater Manchester Mental Health secured funding to purchase and deploy Vectra.

"The deployment was quick and easy," Orritt notes. "The onboarding and training was straightforward compared to other systems we've deployed that require a lot of time and effort to implement and configure."

With 5,400 employees, one of the biggest network challenges at Greater Manchester Mental Health was handling security oversight for all devices, locations, and knowing how each device was communicating.

"Vectra enables me to be proactive rather that reactive, which is a big deal for us," he says. "Instead of chasing down alerts from irrelevant logs, I spend more time working with our end-user community to create awareness about important security practices."

"We have several tools that enable us to do some of this, but they are very time-consuming to use," says Orritt. "We had no way to see what types of traffic flowed from our devices or how they were behaving. It was a good time to put Vectra to the test."

The acid test

Shortly after the Cognito platform from Vectra was up and running, it identified a device that should not have been connected to the corporate network.

"Vectra showed us that it was a Windows 7 device, which we don't allow on our network, and it was communicating with an AWS cloud, which our organization does not use," says Orritt.

The device belonged to a company that was contracted to clean the Greater Manchester Mental Health offices.

"A contract worker plugged into our network," says Orritt. "It was a simple mistake that should not have happened. But we don't believe there was any malicious intent behind it. We have also detected legitimate users with approved devices trying to communicate with and access services that were off limits."

Have a nice day

Today, Vectra has become a daily part of Orritt's cybersecurity routine.

Vectra fits quite nicely into my day," he says. "The first thing I do in the morning is check if there are any new triaged alerts at a high or critical level. I also have it integrated with Microsoft Teams so I can check alerts when I'm away."

"If we detect anything unusual or suspect, we're able to respond that same day, which is a lot faster than we were doing it before," he adds.

While Vectra handles network detection and response, Orritt has more time to focus on creating end-user security awareness and hygiene.

"Vectra enables me to be proactive rather that reactive, which is a big deal for us," he says. "Instead of chasing down alerts from irrelevant logs, I spend more time working with our end-user community to create awareness about important security practices."

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

Email info@vectra.ai vectra.ai