VECTRA

CASE STUDY

American University jettisons signatures and open-source tools for network detection and response

University prepares for a bigger presence in the cloud

American University doesn't have a big cloud presence — but it will soon. That said, the private Washington D.C. university needed to step-up its cybersecurity efforts to protect the university's public cloud, data center and campus networks.

The university wanted to overcome two cybersecurity challenges, both of which involved a sizable chunk of time and resources: The use of open-source tools to monitor network traffic and the use of signatures to detect intrusions.

"Open-source monitoring tools are a lot of work to maintain and leverage," says Eric Weakland, director of information security at American University. "It creates a much higher operational burden for our team."

"Intrusion detection requires a security analyst to sift through volumes of signature hits," Weakland continues. "And it doesn't give you visibility into what's happening inside the network."

"We really needed a better, faster way to drink data from the security fire hose," he adds.

According to Weakland, the American University network supports about 60,000 users with more than 20,000 devices at any given time. It also supports 700 servers and hundreds of applications.

AMERICAN UNIVERSITY
WASHINGTON, DC

Organization

American University

Industry

Higher education

Challenge

Protect public cloud, data centers and campus networks

Selection criteria

A platform that allowed them to process and analyze data quickly.

Results

- Visibility across the full lifecycle of an attack
- Overall higher efficiency in processing data
- Greater protection for critical university assets

In its quest to shore-up security posture and spend time and resources more wisely, the information security team leaned toward non-open-source solutions that used artificial intelligence and complemented the goals they wished to achieve.

"We want to spend more time doing what's beneficial for the university, which is protecting it – not upgrading custom software and sifting through signatures," notes Weakland. "We looked at Corelight, ExtraHop and Vectra."

The value of AI

After considering the value of each vendor's cybersecurity solution, American University chose Vectra's Threat Detection and Response (TDR) platform.

The Vectra platform harnesses Security AI-driven Attack Signal Intelligence to automatically detect, triage and prioritize in-progress attack behaviors that pose the highest business risk – across cloud, SaaS, identity and network data centers.

Because east-west visibility includes dedicated connections to cloud instances, threat behaviors detected in the university's campus and data centers are instantly correlated with threat behaviors in its cloud. The university also deployed Vectra virtual sensors on every VMware server to monitor all traffic between servers.

> "We have visibility into malicious behaviors in internal east-west traffic and in north-south traffic to and from the internet," explains Weakland. "The detections are always prioritized so we know which ones are critical to address."

By automating manual and mundane Tier-1 and Tier-2 security tasks, the Vectra platform helped reduce the security analyst's workload, giving them more time to focus on incident investigations and threat hunting.

The Vectra platform has helped shift approximately 25 percent of Tier-2 analyst work to Tier-1 analysts. The information security team also reduced the time to respond to threats by about 20 percent.

"Vectra catches much more than an analyst who has to sift through signature alerts," says Weakland. "It also reduces false positives, especially from authorized PowerShell user traffic, which sometimes appears very suspicious."

To further reduce time and resources, Vectra rolls-up multiple alerts into a single incident or attack campaign for efficient investigation and response.

Vectra Attack Signal Intelligence delivers insights about attack behaviors that empower security teams to perform faster and more conclusive investigations and threat hunting.

"Vectra captures metadata at scale from all network traffic and enriches it with a lot of useful security information," says Weakland. "Getting context up-front tells us where and what to investigate."

To accelerate response time, the Vectra platform integrates and shares the same context and insights with third-party security solutions – including EDR, NDR and SOAR tools – for end-to-end threat management and visibility.

Open source creates an open door

"The Vectra platform is very stable and easy to maintain compared to the Linux open-source solution we used to have," says Weakland.

Although American University didn't encounter problems with its old Linux servers, advanced persistent threat (APT) groups often use them as an exfiltration gathering point, even after an operating system reinstalls.

A GRUB2 bootloader utilized by most Linux systems can be commandeered by ATP groups to gain arbitrary code execution during the boot process, even when secure boot is enabled.

Attackers who exploit this vulnerability can then install persistent and stealthy bootkits or malicious bootloaders, which give them near-total control over compromised devices.

After analyzing several remote access tools (RATs) used in this type of exploit, Vectra identified unique differences in communication patterns between attacker RATs versus legitimate sysadmin remote access tools.

“With Vectra, we can see if an exploit kit is being downloaded and if it was laterally distributed in the network,” notes Weakland. “We have visibility into behaviors across the full lifecycle of an attack beyond the internet gateway.”

Conclusion

“Our work is much more efficient with Vectra,” says Weakland. “We have greater protection for critical university assets. And we can detect, respond and investigate what’s important.”

“One thing that really excites us about partnering with Vectra are solutions for Azure and AWS clouds,” Weakland concludes. “This will give us the same visibility into cloud services that we’re getting in our campus and data center.”

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai