Case Study

State university tackles cyberthreats

Students are at the front line of cybersecurity at the University of Oklahoma

The University of Oklahoma is known as a Big 12 football powerhouse, but over in the security operations center (SOC), students are making a different type of touchdown. STEM students are on the front line of keeping the university safe from the onslaught of cyberattacks.

Aaron Baillio, deputy CISO at the university, has been on a quest to find and stop threats that could result in the damage or theft of financial or administrative data, disrupt university research programs ranging from microbiology to meteorology – or even keep students from playing Fortnite late into the early morning hours.

Over the last several years, Baillio tried three different AI-powered threat hunting products, but none could reduce the burden of finding threats in a university environment, which must delicately balance academic openness and tight security controls.

"At a university, it's hard to say we have standard behavior," says Baillio. The shortfalls varied: Threat findings weren't sufficiently meaningful, the products couldn't keep pace with traffic volumes or the cost was too high. Whatever the reason, gaps remained.

"Cognito was like a miracle"

At an Educause security conference, Baillio discovered Cognito®, the threat-detection and hunting platform from Vectra®. Hearing firsthand how students at the Texas A&M University System staffed front-line operations at its SOC was a lightbulb moment.

Baillio took his peer's recommendation and ran with Cognito Detect™ for AI-powered, real-time cyberattack detection and threat hunting.

The UNIVERSITY of OKLAHOMA

Organization

The University of Oklahoma

Industry

Higher education

Challenge

Accurately detect hidden cyberthreats across the network with less manual work

Selection criteria

Easy-to-use, accurate and affordable threat detection that could efficiently protect all university traffic

Results

- Detect hidden and unknown attackers targeting academic departments, research labs, university administration, and students
- Empower students at the front line of security operations with accurate detections and a clear starting point for investigations
- Easily integrate threat detection with endpoint security, analytics and other elements in the security ecosystem

VECTRA®
Security that thinks®

“Cognito was like a miracle dropped into our laps,” says Baillio. “It detects the threats that are most relevant to us.”

Cognito’s always-learning behavioral models detect hidden and unknown attackers in the network to enable a quick, decisive response and provide a logical starting point for threat investigations.

Finding hidden threats in a network with 30,000 people and 100,000 devices is no longer a daunting, time-consuming task.

“With Cognito, students are my boots on the ground,” says Baillio.

Student analysts need to only glance at the Cognito Threat Certainty Index™, which consolidates events and historical context to pinpoint the hosts that pose the greatest risk.

“We try to keep the Cognito UI’s upper quadrant, where the critical threats are shown, empty,” says Baillio. “Students know to look there first.”

Reveal hidden threats

Phishing is a big concern. Attacks spike when financial aid is disbursed by the federal government, with criminals hoping they’ll get lucky and redirect funds intended for needy students. Educating faculty and students on security awareness and hygiene is a difficult job.

Students, especially in engineering and computer science, are often adventurous in developing their skills. But now those threats aren’t hidden.

“With Cognito, we see computers get compromised and start mining cryptocurrency or become a Tor exit node,” says Baillio. “Cognito has helped us quickly identify unusual traffic patterns and investigate the cause.”

Threats are detected conclusively with Cognito, and student analysts have the full context of a threat at their fingertips, eliminating manual guesswork.

“With Cognito, the quality and priority of threat information is excellent,” he says. “We weren’t able to see a smash-and-grab scenario or a hidden tunnel before.”

Cognito also helped the SOC team identify misconfigured devices, enabling prompt, corrective action to be taken.

Easy integrations

The University of Oklahoma is creating even more value by integrating Cognito with its security ecosystem.

“Students helped build the integrations and automated detections,” says Baillio. “With the integrations, they can react quicker,” says Baillio.

For example, Cognito is integrated with the university’s Carbon Black Cb Response endpoint security to automatically add enriched context to investigations and to allow analysts to quickly isolate compromised devices.

The university is creating its own threat intelligence by feeding Cognito alerts into an Elasticsearch analytics engine, enabling threat data to be broadly correlated.

Real-world training

“Cognito is a great training tool,” says Baillio. “It helps students learn what’s involved in an investigation and how to do triage.”

Cognito has detailed descriptions of detections, which helps students – or any busy security analyst – understand the nature of a specific threat and where to start the initial investigation.

Using data to drive policy

Getting visibility into active threats also helps the university’s efforts around governance, risk management and compliance.

“If we detect a lot of unmanaged remote access but don’t have a policy governing its use, we can ask the university to address it,” says Baillio. “The insight from Cognito helps us inform the policy-making process.”

The University of Oklahoma has been operating its student-run SOC for about a year, and it keeps pushing ahead on its security roadmap. As university continues to mature its SOC, Baillio notes that “Vectra’s engineering support is really good and helps guide us in how to hunt for threats.”

> *“Cognito was like a miracle dropped into our laps. It finds the threats that are the most relevant to us.”*

Aaron Baillio
Deputy CISO
The University of Oklahoma

VECTRA
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020 www.vectra.ai