Case Study

An academic and research powerhouse

Texas A&M University System saves $7 million in one year with the Cognito® network detection and response platform from Vectra®

The Aggies may be known for football, but the Texas A&M University System is also an academic and research powerhouse.

The A&M System encompasses 11 university campuses, seven state agencies and numerous research institutes. Its research is as varied as tackling global hunger, advanced manufacturing, animal diseases that crossover to humans, and nuclear science. For a cyber thief, stealing that research is the ultimate touchdown.

A drought of cybersecurity talent

"One of the biggest challenges we faced was the lack of cybersecurity talent, which is a huge global issue right now," says Dan Basile, executive director of the Security Operations Center at the A&M System. "It's difficult to hire and retain skilled cybersecurity professionals."

"The other challenge is that we spend $4.2 billion in total expenditures," Basile added. "Vital research is performed with many important organizations like the U.S. Department of Energy, NASA and the U.S. Department of Defense. This makes us a target for nation-state cyberattackers."

Cut costs by detecting attackers fast and early

For the A&M System, whose network supports about 250,000 people at any given time, Cognito has proven to be the fastest, most efficient way to stop cyberattackers that evade perimeter security and spread inside the network in search of key assets to steal or damage.

THE TEXAS A&M UNIVERSITY SYSTEM

Organization

The Texas A&M University System

Industry

Higher education

Challenge

Protect high-value academic and research data

Selection criteria

Increase speed and efficiency of threat detection and incident response

Results

- Faster detection of hidden cyberattackers inside the network
- Saved $7 million in one year by eliminating the need for postbreach forensic analysis
- Cuts threat investigations from several days to a few minutes
- Automates the manual, timeconsuming Tier-1 analysis of security events

VECTRA®
Security that thinks®

The A&M System's Security Operations Center successfully detected and mitigated seven network cyberattackers in one year using tools such as Cognito. And there was little need for expensive post-breach forensic analysis, which only provides a rear-view mirror of an attack, often months after cybercriminals have made off with your crown jewels.

"You're looking at about $1 million every time you call in consultants to perform post-breach forensic analysis," Basile explained. "By eliminating this, Vectra saved the A&M System $7 million in a year and we cut threat investigation times from several days to a few minutes."

Automation creates opportunities

By closing the cybersecurity gap between network perimeter security and post-breach forensics, the A&M System can detect attacks faster and eliminate the need to analyze and chase down hundreds of thousands of NetFlow threat logs.

"Since deploying Vectra, our team can monitor the entire A&M System network for cyberattackers and run the Security Operations Center with incredible efficiency, despite having an extremely lean staff," Basile says.

Cognito has also been instrumental in helping the university overcome the cybersecurity skills shortage. Student interns who are interested in studying and developing careers in cybersecurity are trained to use Cognito as Tier-1 analysts in the Security Operations Center.

"Vectra is so intuitive and easy to use that interns can decide in a few minutes whether to act on a threat detection themselves or escalate it to a Tier-2 security analyst for further investigation," says Basile. "So the highly-skilled employees who used to be Tier-1 analysts are now working as Tier-2 analysts. This is where Vectra really shines."

"We continue to shrink our threat detection times with Vectra and student interns are now viable members of the security operations team," Basile adds. "That is massive in higher education. It's a big win for both students and the university."

How Cognito finds the highest-risk threats with certainty

By monitoring all internal network traffic, Cognito provides visibility into the actions of all devices – including BYOD and IoT – and automatically puts the most relevant information in context into the hands of the security operations team.

When active cyberattackers are found inside the network, Cognito automatically scores, prioritizes and correlates each threat detection with the compromised hosts and key assets that are under attack.

The Vectra Threat Certainty Index™ consolidates thousands of events and historical context to pinpoint the hosts that pose the biggest threat. With Cognito, analysts see the data that matters in full context, which speeds-up incident response.

Security analysts can instantly see which devices infected hosts are communicating with and how. Access to metadata in captured packets further accelerates threat analysis so security teams can take fast, decisive action.

> *"Vectra saved the A&M System $7 million in a year and we cut threat investigation times from several days to a few minutes."*

Dan Basile
Executive Director of the Security Operations Center
The Texas A&M University System

VECTRA
Security that thinks®

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