elastic | THE TEXAS A&M UNIVERSITY SYSTEM

SUCCESS STORY

The Texas A&M University System protects students, emergency responders, and leading research institutions with Elastic Security

Region
United States

Industry
Government

Solution
Elastic Security

Saves 100 hours of analyst time every month

- The Texas A&M University System saves over 100 analyst hours per month by automating documentation and other security processes with Elastic Security.

Reduces incident resolution time by 99%

- With Elastic Security, The Texas A&M University System has reduced the time to resolve like-for-like incidents from months to just two hours a reduction of 99%.

Enables rapid integration of additional security features

- With Elastic Security, The Texas A&M University System has a single SIEM vendor with regular releases and frequent feature updates.

The Texas A&M University System deploys Elastic Security to protect students, emergency responders, and leading research institutions from state-sponsored hackers and cybercriminals.

Defending IT systems is hard enough when there are thousands of cyberattacks worldwide every day. It's even more challenging when you're a public organization with dozens of partners, tens of thousands of endpoints, and billions of telemetry events every month. That's the challenge facing the Cybersecurity Operations team at The Texas A&M University System, a public, land-grant research institution with the second-largest student body in the U.S.

As well as protecting 11 universities that comprise the A&M System, the cybersecurity team must defend eight state agencies. These include the Texas Division of Emergency Management and the Texas A&M Forest Service. The research sector also depends on the A&M System's cyber defenses as it covers some of the world's leading centers for engineering innovation.

Braxton Williams, Security Analyst, The Texas A&M University System Offices, says, "Our mission is to safeguard data across all our members, maintain high availability for emergency response services, and ensure that research for all our stakeholders and federal partners is delivered uncompromised."

> We selected Elastic Security for Endpoint because it doesn't just alert you to something bad, it empowers you to do something about it, fast.

Braxton Williams
Security Analyst, The Texas A&M University System

elastic

The A&M System must achieve all this on a tight budget, and its position at the heart of an international research network puts it in the firing line of state-sponsored actors and hackers. “We have thousands of students and users all with their own devices. It’s a massive threat surface for ransomware and phishing attacks that threaten to disrupt operations or extort money,” says Williams.

Security analysts play a critical role in defending the A&M System’s. In the past, their skills were hindered by the need to source data from multiple security products based on different query languages. Long hours added to the pressure on the team as they gathered and shared information with their colleagues.

In pursuing an endpoint detection and response (EDR) solution that addressed these issues, the A&M System selected Elastic Security for Endpoint. “Instead of several security products and portals, we now have one interface for all our security analysts. It gives them every tool that they need to investigate and remediate security incidents,” says Williams.

The cybersecurity team now deploys Elastic Security automatically on all devices in its universities, agencies, emergency response teams, and research organizations. “We have 30 days of data from 25,000 endpoints, including device telemetry, phishing data, and threat intelligence data. With Elastic, everything we need is just one query away in a common language with a single schema.”

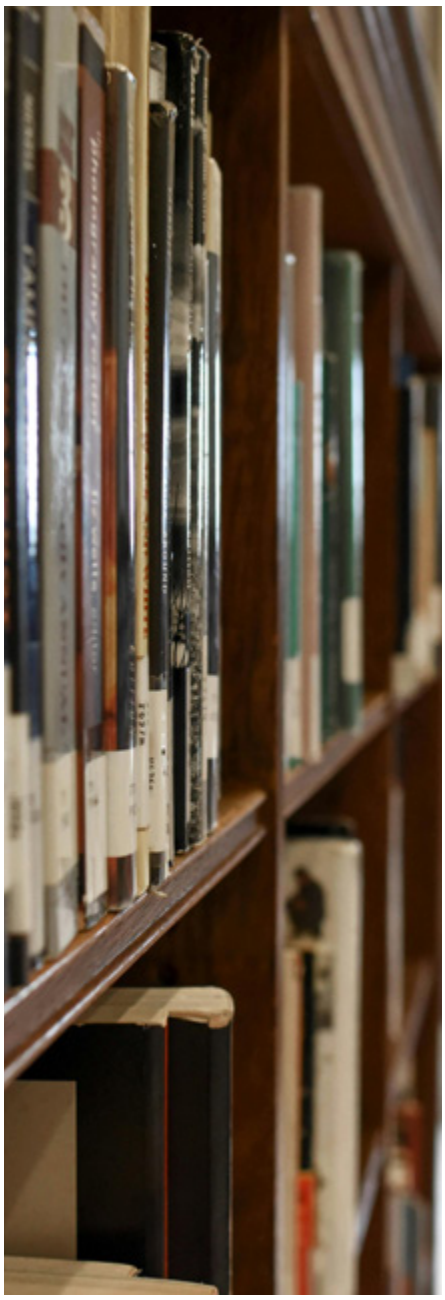
Saving time, avoiding burnout

Elastic Security massively curbs the volume of documentation created during security workflows and reduces duplicate detections and false positives. “By adding an automation layer to our documentation process, we’re saving about 100 hours of analyst time per month. We can focus on delivering results, which is a massive morale boost,” says Williams.

To illustrate the point, Williams compares two near identical attacks from the same adversary, which took place before and after the deployment of Elastic Security. The first attack succeeded in sending phishing emails using a university’s internal relays. When the breach was detected after several months, it took two more weeks to investigate compromised computers and mitigate the attack.

Following the deployment of Elastic Security, two years later, the same adversary attempted a similar campaign. “We shut it down completely and mitigated the issue in a couple of hours, representing an 11,000% acceleration compared with the previous response time,” says Williams. “With the combined endpoint and SIEM capabilities in the Elastic Security solution, it provides us with a single, intelligence-led solution, which further streamlines our security operations,” says Williams.

He also gives plenty of credit to the Elastic support team, whose expertise enabled the A&M System to expand its SIEM rapidly. “Whenever we talk to an Elastic engineer, it feels like we speak the same language, which means we can fix things during a short conversation rather than a prolonged escalation process.”



> The biggest advantage of Elastic is that it excels in so many areas. To achieve the same results, you’d need to deploy three or four separate products from other vendors. As an organization that’s responsible for public budgets, it’s great that we can demonstrate value in the procurement of critical security software.

Braxton Williams
Security Analyst, The Texas A&M University System

elastic

Pricing is also an advantage, especially in the government sector, where universities are expected to manage budgets wisely. Rather than per-endpoint charging, the A&M System pays for resource capacity. “We expect the number of our endpoints to increase to 85,000 in the next couple of years potentially,” says Williams. “Elastic’s consistent and transparent pricing framework helps us to plan with certainty.”

Now, Williams is turning his attention to the latest wave of Elastic’s AI and machine learning technology. This includes anomaly-based detection that can potentially uncover new or unknown attacks even if they don’t have a signature. Adding innovative features and releases also gives him confidence in the ongoing defense of the A&M System. “Elastic has always been at the forefront of research and deployment, whether it’s out-of-the-box detections or adding new capabilities that address emerging cybersecurity threats,” he says.

Above all, Elastic Security enables the A&M System Cybersecurity Operations team to defend assets against a multitude of threats. “The A&M System’s institutions and agencies have private and federal sponsors that award us a significant number of grants. Elastic delivers the necessary levels of security to enable partnerships with these high-profile organizations and support research.”

