splunk> a CISCO company

CUSTOMER STORY

The University of Alaska Prevents Over 2,000 Fraud Attempts with Splunk

Key Challenges

Facing sophisticated financial aid fraud ("ghost students") and incident response bottlenecks, the University of Alaska needed a unified solution to protect funds across its complex, distributed environment.

Key Results

With Splunk Platform and Splunk SOAR, the university gained automated threat response and unified visibility across tens of thousands of assets, averting more than 2,000 fraud attempts in just two years.

UNIVERSITY of ALASKA
Many Traditions One Alaska

Industry: Higher Education

Solutions: Platform, Security

Products: Splunk Platform, Splunk SOAR

Securing "The Last Frontier" requires unified visibility.

From its arctic research hubs in Fairbanks to its bustling urban campus in Anchorage, the University of Alaska (UA) system is more than an academic institution — it's a critical engine for the state's future. By tailoring its studies to vital sectors like mining, engineering, and healthcare, UA ensures a skilled workforce for Alaska's long-term success.

The university's Office of Information Technology (OIT) faces the unique challenge of protecting up to 45,000 staff and students across three independent institutions — UA Fairbanks, UA Southeast, and UA Anchorage — alongside a vast network of remote learning centers, under one centralized, comprehensive security framework.

Outcomes

- **2,000+ fraud attempts prevented**
- **Minutes to detect and respond**
- **Unified visibility across three universities**

That's why the UA security team turned to Splunk Platform and Splunk SOAR to unify and accelerate their operations. Despite its small team and massive geographic and digital footprint, they transformed fragmented data into actionable insights, building a security posture that is as rugged and adaptable as the state itself.

Protecting student funds in "The Land of the Midnight Sun"

Prior to Splunk Platform, the university had no central logging system for data visualization and retention. "Every department operated in their own data silo," admits Logan MacDonald, security operations manager at the University of Alaska. "So, there was no single pane of glass or correlation of data." This lack of visibility meant that, oftentimes, they were unaware of critical incidents until it was too late.

With Splunk Platform, the security team now aggregates logs from every campus and remote learning outpost, providing a comprehensive view of the entire computing estate. Rather than relying on out-of-the-box tools, MacDonald and Information Security Engineer Aiden Watson created custom dashboards and alerts tailored to the university's specific

needs. Every team across the university system now has access to critical data related to on-prem servers, firewalls, active directory (AD) logs, and more.

"We use Splunk Platform to bring together data from every system," MacDonald explains. "It's a powerful tool that lets us visualize activity, detect threats, and respond quickly." In fact, the university's Mean Time to Detect (MTTD) has reduced dramatically — from hours to minutes — enabling MacDonald and his team to stay on top of security events like ransomware attempts, phishing attacks, and external IP scanners.

This unified visibility was put to the test against a recent surge in sophisticated financial aid fraud. By using Splunk Platform to correlate data across systems, Watson built out 90 security detections, many of which help identify anomalous, suspicious patterns like shared IP addresses, improbable travel, and new accounts that use proxies or VPNs.

With these detections in place, UA thwarted over 2,000 fraud attempts in just two years, saving the university system tens of thousands of dollars. This proactive stance doesn't just protect funds. It ensures that the state's resources are directed to where they matter most: students.

> **When people ask how we achieve so much with a small team, the answer is Splunk. Its power and flexibility let us maximize every dollar and every insight."**
> Logan MacDonald, Security Operations Manager, University of Alaska

UA's security posture SOARS with automation

Small crew, massive geographic and digital footprint. That was the problem for UA's security team of six with no 24/7 SOC. Incident response was manual and time-consuming, requiring constant coordination across various teams. For a small security shop, this was a true vulnerability.

To bridge this gap, UA implemented Splunk SOAR to speed up workflows and maintain robust security operations around the clock. For example, Watson built out an automated ransomware playbook that can identify and quarantine an affected device within five minutes, requiring no manual intervention. Meanwhile, his canary playbook proactively gathers threat intelligence on IP addresses and blocks them if they don't meet specific security requirements.

Now that automation handles many routine tasks, their Mean Time to Respond (MTTR) has accelerated from hours to minutes. Plus, they've scaled their impact without increasing their headcount. MacDonald and his team now have time to focus on high-value work like threat hunting, strategic analytics, and collaborating with other departments.

"Automation is critical to our success," says MacDonald. "My goal is to empower my team to focus more on strategic work that strengthens the university's ability to serve the state and its people. Splunk enables us to do just that."

"North to the Future" — Alaska state motto

Looking ahead, MacDonald envisions every department at the university leveraging Splunk: "We want to empower others to use Splunk — to onboard their own data and build their own dashboards." With even deeper integration and AI-driven insights on the horizon, UA's security team plans to explore new incident management features to continue bolstering their security posture. "The work never stops," MacDonald admits. "But we're building a solid foundation for success."

26_CMP_cust_University-of-Alaska_v2