splunk> a CISCO company

CUSTOMER STORY

Top-Ranked University Powers Student SOC with Splunk

Key Challenges

A University's four-person SOC was overwhelmed by thousands of alerts from information technology (IT), operational technology (OT), and public-safety systems. Meanwhile, early-career students were facing challenges breaking into the security industry with no experience and completing their co-op requirements.

Key Results

A student-powered SOC grew from four to ten co-op analysts, providing a scalable talent pipeline and real-world training. Centralizing logs in Splunk Cloud and automating response with SOAR cut account-lock times from 30 minutes to seconds, enabled the university's quick, compassionate, and data-centric response to students who had threatened self-harm, and enhanced security of all university community members.

Industry: Higher Education

Products: Splunk Cloud, Splunk SOAR, Splunk Academic Alliance, Splunk ITSI, Splunk UBA

Solutions: Incident Response, Infrastructure Monitoring, Security, Compliance

Capabilities: SIEM / Security Analytics, Investigation and Forensics, Risk-Based Alerting, Compliance Monitoring and Reporting, Infrastructure Monitoring and Troubleshooting, Incident Response and Automation

From co-ops to campus defenders

The University faced two urgent challenges. Its lean SOC was "about a quarter of where we should be for an institution of our size," recalls the Associate Vice President Office of Information Security & Chief Information Security Officer. Alerts streamed in from identity platforms, research-lab logs, OT and IoT sensors, network devices, service-monitoring tools, and environmental systems, overwhelming the small team. At the same time, the university's first-in-the-nation century-old co-op program required every sophomore and junior to do a six-month job placement, yet few local employers could host them with limited experience.

To address both needs, the university launched a co-op program on Splunk Cloud and Splunk SOAR. Starting with just four student analysts, the program quickly grew to ten rotating co-ops, prompting the university to move into a larger, purpose-built facility. Each newcomer follows a documented standard on-boarding procedure, completing Splunk Academic Alliance modules in DDAS/DDIA and hands-on playbook exercises before earning full Splunk access and owning Tier-1 triage. The Splunk Academic Alliance program provides free training and certifications to university students, faculty, and IT staff, helping develop skilled talent for the future while supporting both business school students and the university SOC team.

Outcomes

- **Secured** 48,000 university community members
- **Reduced** account lock time from 30 minutes to under 10 seconds
- **Geolocated** and dispatched help to students in crisis

Under the CISO's leadership, the university pushed its vendors to go beyond off-the-shelf. "We ask our vendor partners, 'Can you help us work on university-specific solutions versus just being a vendor to us?' That's why we've been very successful with Splunk," says the CISO. She also challenged departments to squeeze 100% of the value from every tool. "We make sure our tools serve the whole institution, not just security."

> If we can't see it, we can't stop it.
>
> **Associate Vice President,** Office of Information Security & Chief Information Security Officer

Co-ops in command

The Incident Response Manager grew up in the co-op program, joining as a student worker, advancing through Analyst I–III, and now leading the program. She recalls, "Before Splunk, we had to check all the different platforms for specific alerting, going into each one to correlate data across Microsoft, our antivirus solution, and other tools just to get a broad overview." Analysts bounced between secure shell sessions, spreadsheets, and legacy consoles for every incident.

In short, the university's security demands were outpacing its workforce.

What started as four student analysts soon swelled to seven this summer, and the university is targeting a 10:5 student-to-staff ratio next term as it heads toward 24/7 coverage. Under the Incident Response Manager's guidance, the program spun up its first SOAR playbook to lock compromised accounts in seconds and is now building a phishing-analysis runbook to quarantine malicious emails automatically.

Partnering with Splunk Academic Alliance provided foundational training before co-ops received full Splunk access. Students dove into alert review, SOAR playbook execution, and customized dashboard creation. Several co-op alumni have since joined the university full time, carrying their co-op experience into broader security and IT roles.

Turning visibility into action

To eliminate dangerous blind spots, the university centralized all logs in Splunk Cloud, giving analysts a single pane of glass. Now identity logs (over a million accounts), network and service-monitoring events, and OT/environmental feeds — from turbine telemetry to freezer temperatures — are all searchable together. "If we can't see it, we can't stop it," the CISO says. Onboarding new data feeds now takes days instead of weeks.

> Our micro-action playbooks aren't just faster; they're defensible. We know exactly what happened, every time.
>
> **Executive Director,** Office of Information Security & Deputy Chief Information Security Officer

With that unified view in place, the co-op delivered immediate, measurable benefits. A Splunk-powered mental health crisis workflow, developed jointly with the university Public Safety, helps locate students in need of urgent support. Through visibility into access anomalies, dropped sessions, and odd application behavior, multiple students received the help they needed quickly from the university's dedicated campus police. "Our responsibility is to the campus community. If we have a tool that can help in a non-security situation, we embrace those opportunities," the CISO says. Mean time to lock compromised accounts plummeted from thirty minutes to seconds, freeing analysts and co-ops to focus on Tier-2 and Tier-3 investigations. The next phase of innovation will be focused on detection of IT and OT issues before outages; monitoring mobile blood-bank labs for tampering; feeding real-time data into the Emergency Operations Center; and generating CMMC compliance reports at the click of a button.

"Our micro-action playbooks aren't just faster; they're defensible. We know exactly what happened, every time," says the Executive Director Office of Information Security & Deputy Chief Information Security Officer.

Charting the next co-op program

"What we're building is essentially a SOC 3.0, where security operations cross disciplines (network, facilities, and public safety) to provide value to the entire university," the CISO explains. With Splunk ITSI in pilot for predictive analytics, and UBA under evaluation for insider-threat detection, the university is on its way toward true 24/7 operations. The team is also conducting a gap analysis on critical infrastructure logs and other missing streams, ensuring every high-value feed is onboarded for real-time alerting and faster incident resolution.

The Incident Response Manager's advice for any university standing up a student-led SOC is, "Invest early in role-based Splunk training before granting platform access, and hold weekly check-ins with your analysts to identify dashboard or playbook gaps."

"Each new dashboard or playbook is another spark of creativity," the CISO says. "With Splunk as our engine and a culture that prizes partnership, we're protecting today's campus and training tomorrow's cybersecurity leaders."

Our responsibility is to the campus community. If we have a tool that can help in a non-security situation, we embrace those opportunities.

Associate Vice President, Office of Information Security & Chief Information Security Officer