splunk> a CISCO company

CASE STUDY

LSU's Student-Powered SOCs Provide 24/7 Security Coverage Across 18 Institutions

Key Challenges

As a leading cybersecurity institution, LSU wanted to offer students hands-on experience in security operations centers (SOCs) and increase the cyber posture of all higher education in Louisiana.

Key Results

Alongside Splunk and TekStream, LSU's student-powered SOCs protect 18 institutions across Louisiana from cyberattacks and give students up to 1,000 hours of frontline security experience each year.

Industry: Higher education, Public sector

Solutions: Security, Platform

Products: Splunk Platform, Splunk Enterprise Security, Splunk Academic Alliance, Splunk SOAR

LSU students have the eye of the tiger when it comes to cybersecurity.

For 164 years, Louisiana State University (LSU) has inspired students to achieve lifelong success and build a better future for the state. Under the banner of purple and gold, LSU had already earned its stripes for its best-in-class cybersecurity education, designated by the National Security Agency in 2023 as a Center of Academic Excellence in Cyber Operations. Following LSU President William Tate's cybersecurity directive, LSU CISO Sumit Jain approached CIO Craig Woolley with a bold idea to provide students with real-world SOC experience while increasing LSU's cybersecurity posture. And they didn't stop there. They partnered with the Louisiana Board of Regents to protect all of the state's higher education institutions.

LSU needed the right technology partners to make this bold idea a reality. Enter Splunk and managed security provider TekStream. Now, LSU's student-powered SOC program is live at 18 Louisiana institutions and counting. And adoption is accelerating fast, expected to reach as many as 38 institutions by 2025. It is improving the cybersecurity of academic institutions across the state, positively contributing to workforce development, and laying the groundwork for a nationally leading cybersecurity curriculum.

Outcomes

18
institutions protected

Up to 1,000 hours
of SOC experience for students each year

24/7
security coverage

Going for (purple and) gold

LSU's student-powered SOC program has grown to encompass 18 schools — with 20 more set to join. Efficiency increases in onboarding and student training allowed LSU to expand its program to even more institutions than initially thought possible. "The Splunk, TekStream, and LSU partnership is the perfect combination of the right people, processes, and technology," says Jain.

What truly sets this program apart is its inclusivity of the entire campus community. Student-powered SOCs typically gear toward IT, cybersecurity, and computer science majors. "Our leadership team and Board of Regents want this to be an opportunity for everyone," says Woolley. "Therefore, the program is open to students of all disciplines. The only criteria we look for is the ability to think critically. If they can do that, everything else can be taught."

Their strategy is working. "It's refreshing to see, since cybersecurity is highly technical," says Jain, who majored in human resources as an undergraduate. "But to build a robust cybersecurity workforce for the future and combat increasing threats, it's vitally important to work with students from different backgrounds."

> Splunk is the best product for us based on efficiency and ease of use. Splunk is best-in-breed."
>
> **Craig Woolley,** CIO, LSU

LSU students get Splunky

To support its student-powered SOC program, LSU explored different SIEM solutions. "At the end of the day, Splunk is the best product for us based on efficiency and ease of use," says Woolley. "Splunk is best-in-breed."

In just one year, each student participant can gain up to 1,000 hours of frontline SOC experience. Throughout their tenure, students work side-by-side with TekStream and train as actual employees: They take Splunk Academic Alliance courses and get schooled in TekStream playbooks built on Splunk SOAR, learning guides for different use cases, and what evidence they need to collect. Alongside TekStream, participants can investigate 22 different types of detections. And since the students started using Splunk SOAR in early 2024, they have worked on roughly 33% of all SOC cybersecurity incidents.

Each participating institution has its own instance of Splunk Cloud Platform and Splunk Enterprise Security (ES) in a shared Splunk SOAR environment with various dashboards, making analysis more efficient. "Before, we were doing things manually at LSU," says Jain. However, with automation in the Splunk SOAR platform, they now have a playbook designed to automatically remediate incidents for more efficient responses, especially after hours.

"At LSU, if an incident happened after six, seven, or eight o'clock at night, it would not get looked at until the next morning," continues Jain. "Now, with the SOC program, we have 24/7 coverage, 365 days a year, increasing the overall security posture of LSU and the state."

To Jain, the main benefit of leveraging Splunk in its student-powered SOC program is its ability to identify and report notable security events in a more consumable fashion. "Being able to bring all incidents into a single environment has had the biggest impact on the efficiency of our program and the safety of participating institutions," says Jain. Otherwise, each institution would have to check its own environments to see what notables came up. "Instead," continues Jain, "we work through a single pane of glass on top of an institution-level single pane of glass. Without Splunk, we wouldn't have a successful student-powered SOC program."

Come on, you Tigers!"

With its first class of student-powered SOC participants set to graduate in December 2024, LSU wants to create as many differentiators as it can for when participants enter the job market. In collaboration with TekStream, LSU will generate a transcript for each student, providing a holistic view of their SOC experience they can present at job interviews. "It would highlight all the critical incidents they worked on, how many they handled, and what kind of complexities they were exposed to," says Jain.

"Being able to prove this experience to future employers will set students up for success after graduation," says Woolley. "This truly sets the LSU program apart from the rest."

By June 2025, LSU hopes to have 38 institutions onboarded into the program, encompassing the vast majority of higher education institutions in the state. "We're still optimizing the onboarding process," says Woolley. "But we're on track to hit our goal."

But why stop there? "Because of our success, we're looking to create a second student-powered SOC that schools nationwide can use," concludes Woolley. "We don't see any reason to limit access to our program to just schools in Louisiana."

> Without Splunk, we wouldn't have a successful student-powered SOC program."
>
> **Sumit Jain,** CISO, LSU