splunk> a CISCO company

CUSTOMER STORY

Splunk Drives New Student Opportunities and SOC Efficiencies for Auburn University

Key Challenges

Auburn University's lean SOC team struggled to scale and maintain visibility in a complex, distributed environment, as well as manage on-premises infrastructure that limited their ability to focus on proactive defense and innovation.

Key Results

Migrating to Splunk Cloud and adopting Enterprise Security Premier provided a unified "central nervous system" that improved visibility, streamlined incident response, and offloaded infrastructure maintenance, as well as created a successful environment for a student-led SOC.

AUBURN UNIVERSITY

Industry: Higher Education

Solutions: Splunk Cloud, Splunk Enterprise Security Premier

Auburn University in Alabama, a major land grant research institution, is continually eyeing ways to open doors for its students. Guided by that principle, the university's security operations center (SOC) team regularly goes the extra mile; protecting data and systems from threats while offering hands-on career development.

"As a research-intensive institution, we're making heavy investments in cyber security. But as a land grant institution, we also give back to the community and the state," said Jay James, Cybersecurity Operations Manager at Auburn University.

When the SOC team turned to Splunk, they found that they could do it all.

Moving from legacy, on-premises infrastructure to Splunk Cloud was the critical shift the team needed to navigate a complex, distributed environment and contend with limited resources. Not only did it help the team modernize its operations and mature its security posture, the Splunk partnership also allowed the security team to put students in charge of the SOC, offering them real-world experience while filling talent gaps at the university and in their communities.

Outcomes

- **50%+ Improvement in MTTR**
- **Transformed SOC into a unified central nervous system**
- **100% job placement rate for graduates**

"We have found success with the current size of our team; however, we had to find something scalable for the growth of emerging threats," said James, "Having a partner like Splunk helped us make sure that we could keep our daily workflows going. Splunk really filled that gap for us."

Splunk Cloud brings data, and mission, into focus

For years, Auburn University operated with a traditional, on-premises security model. However, as their environment grew more distributed with faculty, staff, and research groups operating across the country and globally, system maintenance consumed more and more of their day. Upgrades, patches, and hardware refreshes took up valuable time that could have been spent on high-value threat investigations. And as the threat landscape evolved, the SOC team found it increasingly difficult to make informed business decisions and remain agile.

"Moving to the cloud felt like a necessity," said James. "We needed to scale. Universities don't necessarily have the largest cybersecurity teams with the most resources. So we were really thinking about the best way to scale quickly and make quicker decisions. It was just a little tougher to do with the resources we currently had to run those tools."

Splunk Cloud was the answer.

"As our technology environment continued to expand, maintaining our workflows with a lean cybersecurity team required a scalable approach.," said James. " Splunk Cloud enabled us to strengthen operational visibility, respond more efficiently, and support sustainable growth."

The team embarked on the cloud migration process, driven by a need for agility, visibility, and transparency. To maintain business operations and prevent disruptions, Auburn adopted a disciplined, phased approach. The team moved slowly at first, testing internally to ensure data fidelity. They treated the migration as an opportunity to clean up their environment, including doing inventory on dashboards and refining data sources. This methodical approach enabled them to integrate diverse log sources from a complex vendor ecosystem. Auburn realized compounding returns when they integrated their Cisco footprint, including Cisco XDR and Cisco Meraki.

> **We have found success with the current size of our team; however, we had to find something scalable for the growth of emerging threats. Having a partner like Splunk helped us make sure that we could keep our daily workflows going. Splunk really filled that gap for us."**
>
> Jay James, Cybersecurity Operations Manager, Auburn University

The result? "We were able to integrate more effortlessly across all our different tools. A lot of the infrastructural issues that we once worried about, we didn't have to worry about anymore," James said. "That was the immediate win."

Splunk Enterprise Security is SOC's "central nervous system"

For the Auburn University SOC team, migrating data to the cloud was just the beginning. The move to Splunk Cloud, coupled with adoption of Splunk Enterprise Security Premier (ES Premier), transformed the SOC's approach to incident response. approach to incident response.

In the past, the team triaged alerts across separate, siloed tools. "Before, everything was in its own domain. We would triage in separate tools, then try to bring it all together," said James. "Now, with Enterprise Security Premier, we have it all in one place. We can tell a full, comprehensive story around an incident with greater efficiency and confidence ." We also Reduced Mean Time to Respond (MTTR) by over 50%, enabling the security team to mitigate threats faster and significantly improve operational resilience.

Out of the box detection rules allowed the team to deploy quickly and focus on high-risk uses and immediate threats, rather than building detections from scratch, which helped the team shift out of "survival mode." "It's getting the low-hanging fruit, where we can identify the riskiest behavior across users just by turning on these detection rules," said James. "That is the game changer."

The SOC team secured leadership buy-in by demonstrating how the platform benefitted the SOC as well as the entire organization, James said. The comprehensive visibility also improved the university's compliance posture and operational efficiency.

By using Enterprise Security Premier, the SOC team was able to consolidate tools, an effort that increased ROI and made the upgrade to Premier an easy sell to leadership.

"Making the investment in Enterprise Security Premier really helped us find that central nervous system we always wanted," said James. "We're now working to ingest any new logs into one area, which allows us to carve out new use cases that leadership hadn't considered before."

Student SOC builds a pipeline of opportunity

The partnership with Splunk does more than protect the university from threats; it also supports the mission of building a bright future for students by powering a student-led SOC.

Launched in 2019, the student-run SOC has grown from a small pilot into a cornerstone of the university's security strategy. "It started with me, two students, and a dream, just trying to figure out how we're going run it," recalled James. The program now supports six to eight students at a time, who handle 75% to 80% of the SOC team's Tier 1 triage, while dedicating the remainder of their time to independent cybersecurity projects.

But the program is more than just a staffing solution — it's become an engine for developing a qualified and sustainable workforce pipeline. The SOC gives students from the College of Engineering and College of Business opportunities to work on real-world security incidents, build dashboards, and contribute to automation efforts. "If there's anything that they want to lean into, we find ways to incorporate it, so they can get more skills on their resume," said James. "If they say, 'I wish I had a dashboard for this,' we give them the opportunity to build it."

As a testament to the program's success, 100% of participating students secured full-time cybersecurity roles within six months of graduation. They often return during recruiting season to share their experiences with incoming students.

> **Before, everything was in its own domain. We would triage in separate tools, then try to bring it all together. Now, with Enterprise Security Premier, we have it all in one place. We can tell a full, comprehensive story around an incident with greater efficiency and confidence."**
>
> Jay James, Cybersecurity Operations Manager, Auburn University

"Many students struggle to find jobs because they lack experience. The student SOC gives them an opportunity right where they are. One of our students from our inaugural 2019 class is now working in the SOC at a financial institution," said James. "We get the operational support we need, and the students get the hands-on experience that employers are looking for. It's a win-win."

AI, Auburn, and the future

As Auburn University matures its security operations, James notes that automation and orchestration are the team's "number one priority." Having Splunk's SOAR offering embedded directly into Splunk Enterprise Premier created a cost-effective way to expand the team's capabilities while providing a unified analyst experience. "Previously, our focus was on building a strong foundation for visibility and data integration.," he said. "Once that foundation was in place, we were ready to invest in SOAR and take the next step in our cybersecurity maturity journey."

But beyond that, AI also presents an immense opportunity for the students to get ahead of the curve. As the student program grows, the team plans to integrate AI technologies, so the students develop expertise in leveraging AI to defend the organization.

"We've been thoughtful about integrating AI technologies into our workforce development program so that when they interview, they can demonstrate AI skills along with the cybersecurity skills to stand out," he said. 'It's not going to be AI that replaces you, it will be those who understand how to use AI. We're ensuring that our students are the ones getting that experience."

Splunk success drives power of partnership

As Auburn University eyes the future, its partnership with Splunk will drive its continued success. By embracing

the cloud, the university has transformed its security operations from a fragmented, resource-heavy environment into a streamlined, student-focused engine. And their vision for AI and automation will continue to open new doors for students in the AI era.

"We have the opportunity to grow with Splunk and put more people into the cybersecurity world," said James. "It's something the world desperately needs."

> **Many students struggle to find jobs because they lack experience. The student SOC gives them an opportunity right where they are. One of our students from our inaugural 2019 class is now working in the SOC at Regions Bank. We get the operational support we need, and the students get the hands-on experience that employers are looking for. It's a win-win."**
>
> Jay James, Cybersecurity Operations Manager, Auburn University