Deliver limitless learning and campus services with modern security operations

Institutional trust is essential in higher education. Students, staff, and faculty expect their personal and proprietary data to be protected at all costs — but an evolving threat landscape, growing compliance standards, and limited resources can make modern security a challenge.

The large volume of sensitive data that educational institutions collect makes them a prime target for various types of nation-state security attacks and increasingly sophisticated ransomware threats.

Global cyber risk scores for education and nonprofit organizations bumped up from "moderate" to "high" between 2022 and 2024.

There are also growing threats around Internet of Things (IoT) devices and enhanced connectivity from offerings like online classes. While these innovations can provide better student experiences, they also create more vulnerabilities and make it difficult to see, manage, and prevent cyberattacks.

These attacks can disrupt the processes universities use to deliver academic and student support services, which can frustrate some of the university's most important stakeholders.

When attacks succeed and personal data is leaked, students and staff lose trust in their university, leading to costly reputational damage that can harm enrollment and potential funding.

This is why higher education institutions must implement proactive cybersecurity and compliance practices campuswide, across many devices and departments.

Power the SOC of the Future

Although basic cyber hygiene can prevent the most obvious security threats, a modern security operations center (SOC) helps universities move into a stronger security position to detect, investigate, and respond to security threats.

The SOC of the future will have all the capabilities needed to build greater resilience, including detecting threats at scale, unifying security operations, and empowering security innovation.

The goal of the SOC of the future is unified threat detection, investigation, and response (TDIR). To achieve this, a modern SOC with scale, speed, and choice can improve your processes and empower your people.

56% of incidents are cybersecurity-related while 44% stem from app or infrastructure issues.

Detect threats at scale

The SOC of the future enables unified visibility and monitoring across all sources through AI and machine learning (ML) capabilities that analyze data in one place and proactively prioritize threats. From this vantage point, SOCs can unearth developing events and detect and respond to threats in real time.

Unify security operations

The modern SOC helps analysts get the information they need in a timely manner across siloed tools and systems. It also helps security teams, frequently burdened with reporting on scattered information, to comply with the evolving regulatory landscape.

Empower security innovation

As limited bandwidth and inflexible toolsets limit universities' innovation, partner and tool selections play a pivotal role in modernizing the SOC so teams can increase productivity and outwit adversaries.

Safeguard the student experience and university data with enhanced cybersecurity

Splunk provides the comprehensive visibility universities need to accurately detect threats and create more efficient processes in every aspect of academic life.

Protect institutions from sophisticated cyber attacks

With Splunk, universities can improve threat detection, investigation, and incident response to secure confidential information for students, researchers, and institutional partner organizations.

Sensitive information is safeguarded by securing access and mitigating exposure risk.

With thousands of students and staff accessing systems both from campus and remotely, having strong cybersecurity and identity management was key to Flinders University's small cybersecurity team. With Splunk's monitoring tools, the Australian university has expanded visibility into its networks, providing security monitoring, identity management, endpoint control, and more. Since a user only needs to press one button to see the data, teams can respond to alerts in minutes instead of hours.

Support compliance reporting and auditing

Security teams in higher education also face additional pressure to meet reporting and auditing requirements tied to funding. In the United States, for example, institutions need to meet compliance standards like those from the National Institute of Standards and Technology (NIST) to qualify for government research grants.

In addition to the general compliance requirements that all universities must follow, the University of Cincinnati, a Carnegie Mellon Research 1 institution, has to follow regulations protecting their highly sensitive U.S. Department of Defense research. Now with Splunk Cloud Platform, the university's security team has deep visibility into its entire environment so they can quickly investigate and address threats to its security posture, leading to better compliance.

Train the future cyber workforce

IT footprints have become increasingly complex, creating a greater need for cybersecurity employees — but there aren't enough skilled workers to fill the gap. An estimated 3.5 million cybersecurity jobs remain unfilled globally.

Some higher education institutions are addressing this shortage with student-powered SOCs. Involving students in cybersecurity can help to reduce the workload for IT and security teams, while providing career development for students.

Louisiana State University (LSU) is one of the state's leading cybersecurity education centers. Graduate students receive real-world, real-time experience with a cybersecurity workforce development and protection model that was made in partnership with TekStream and Splunk.

Students gain valuable skills like tier-one incident response, threat detection, and remediation, and provide much-needed cybersecurity services — up to 1,000 hours of frontline SOC experience each year. With the help of its student-powered SOC, LSU can offer 24/7 protection to 18 institutions, and that number is expected to grow to as many as 38 institutions in 2025.

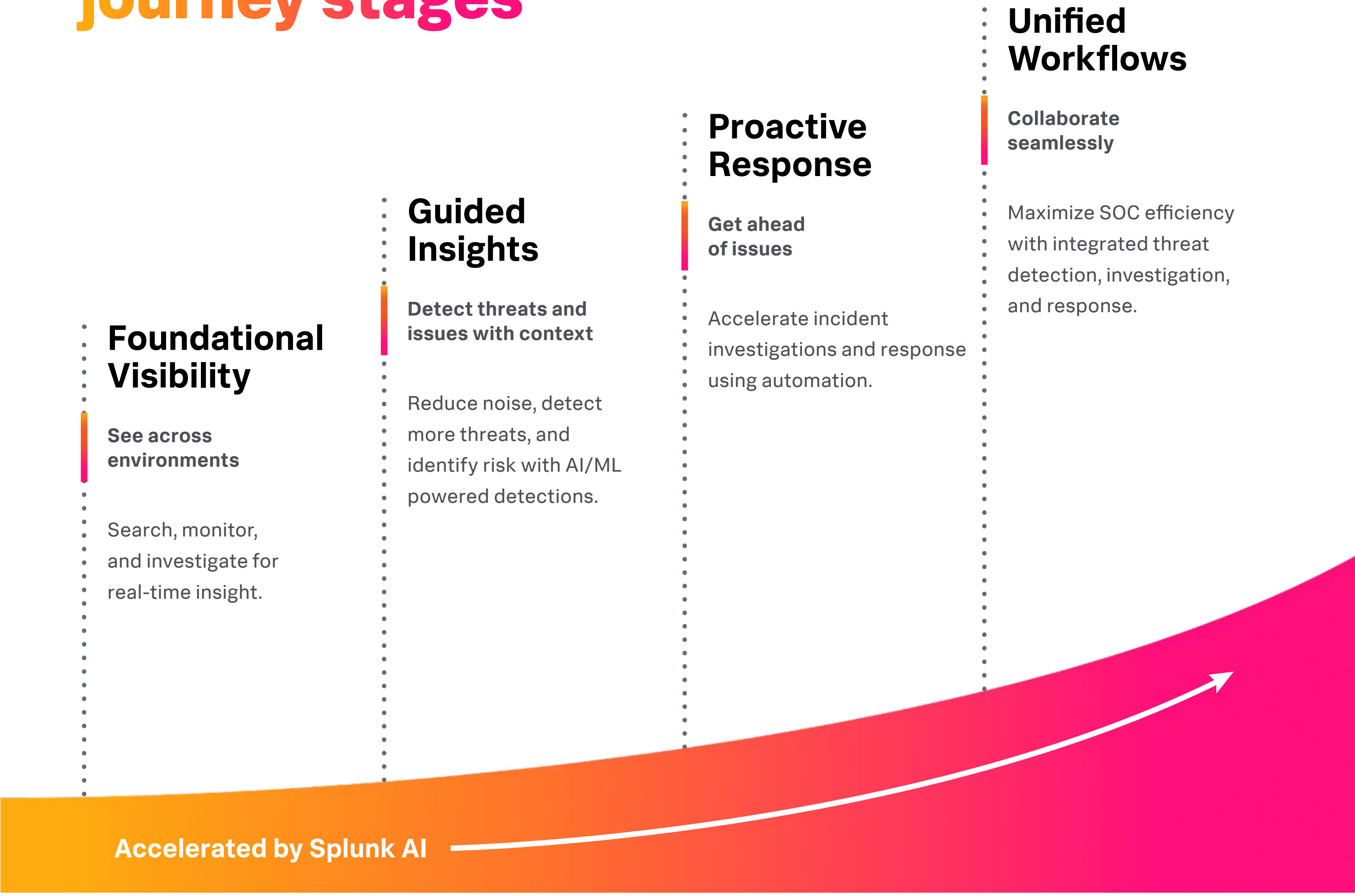
Splunk empowers the entire security journey

Digital resilience is a journey.

With that in mind, Splunk has created a model to help security teams in higher education expand into new and complementary use cases that advance security operations.

This approach shows universities how they can go beyond foundational visibility to be more proactive with unified workflows.

Powering the SOC of the future journey stages



Foundational Visibility

See across environments

Search, monitor, and investigate for real-time insight.

Guided Insights

Detect threats and issues with context

Reduce noise, detect more threats, and identify risk with AI/ML powered detections.

Proactive Response

Get ahead of issues

Accelerate incident investigations and response using automation.

Unified Workflows

Collaborate seamlessly

Maximize SOC efficiency with integrated threat detection, investigation, and response.

Accelerated by Splunk AI

Forging ahead on the security journey with Splunk

Student expectations for their university experience continue to evolve. To stay competitive, universities need to deliver reliable, high-quality academics and student support services, while safely handling sensitive data and maintaining compliance standards.

Modernize your SOC with greater visibility across the hybrid IT landscape and unified TDIR from Splunk Security Essentials. As the industry leader in security operations solutions, Splunk is the foundation of the SOC of the future — providing an unmatched breadth of technologies and expertise.

Splunk can help you power a digital foundation that delivers excellence and value while building a more resilient institution.

Discover how Splunk can transform your university's security operations >

Learn how the SOC of the future can strengthen digital resilience >

splunk> a CISCO company

Learn more: www.splunk.com/asksales

www.splunk.com