CUSTOMER STORY

From Siloed to Synergized: Cybersecurity Transformation at the University of Illinois Chicago

Key Challenges

Siloed security operations and limited infrastructure at UIC presented challenges in addressing cybersecurity threats across its 16 colleges and healthcare system. At the same time, the university needed to uphold its open-access mission, requiring a careful balance between security and academic freedom.

Key Results

Automated phishing response reduced support tickets from over 300 to near zero. Improved visibility and orchestration synergized UIC's security operations, significantly accelerating security maturity and enabling faster incident response across all departments.

The University of Illinois Chicago (UIC), a top-tier research institution nestled in the heart of Chicago, has long been recognized for its commitment to academic excellence and open-access education.

With 16 colleges and a sprawling healthcare system, UIC faces the dual challenge of maintaining robust cybersecurity while preserving the collaborative spirit essential to its mission. Under the leadership of Shefali Mookencherry, Chief Information Security Officer and Chief Privacy Officer, the university has embarked on a transformative journey to modernize its security maturity, infrastructure, and culture.

UIC's expansive and decentralized environment presented significant hurdles. Security operations varied widely across departments, leaving the institution vulnerable to threats. At the same time, the university's open-access mission demanded a delicate balance — ensuring protection without stifling innovation or collaboration.

With sensitive data flowing through research labs, clinical systems, and student services, UIC needed a solution that could unify its security posture while respecting the diverse needs of its academic community.

UIC UNIVERSITY OF ILLINOIS CHICAGO

Industry: Higher Education and Healthcare

Products: Splunk Cloud, Splunk Enterprise Security (ES), Splunk SOAR, Splunk ITSI, Splunk On-Call

Solutions: Security, Compliance, IT Operations

Capabilities: SIEM / Security Analytics, Security Orchestration, Automation and Response (SOAR), Investigation and Forensics, Risk-Based Alerting, Compliance Monitoring and Reporting (HIPAA), Infrastructure Monitoring and Troubleshooting, Incident Response and Automation, Cross-Departmental Visibility

Outcomes

- **300+/month** support tickets eliminated through automated phishing response
- **2x** scaling of the Splunk environment in just two years to support new security use cases
- Phased adoption across all **16 colleges** and edge units, fostering a unified security culture

The solution: Splunk-powered security orchestration

To address these challenges, UIC turned to Splunk's data analytics and automation capabilities. The adoption of Splunk marked a pivotal shift from reactive security practices to a proactive, intelligence-driven approach. By centralizing data visibility and automating threat response, UIC was able to streamline operations and enhance institutional alignment.

One of the most impactful changes was the implementation of automated phishing responses. Previously, phishing incidents generated over 300 support tickets, which was a drain on resources and a risk to data integrity. With automation in place, that number dropped to free up IT Security staff to focus on other security initiatives.

Cultivating a cybersecurity culture

Central to UIC's success has been the cultivation of a cybersecurity culture rooted in awareness, collaboration, and trust. Shefali Mookencherry emphasized the importance of engaging stakeholders across the university — from faculty and researchers to administrative staff and students. Through targeted training, transparent communication, and inclusive governance, UIC has built a resilient community capable of adapting to evolving threats.

> We're a public university, so finding the right security controls without hindering the university's core activities is challenging. We need solutions that provide balance and enable secure collaboration.
>
> **Shefali Mookencherry,** Chief Information Security Officer and Chief Privacy Officer

This cultural transformation has also extended to UIC's healthcare system, where data protection is paramount. Splunk's orchestration tools have enabled faster incident response and improved compliance with regulatory standards, reinforcing UIC's reputation as a leader in secure, patient-centered care.

> Splunk has been central to our transformation journey. Each year, we're leveraging Splunk more strategically, enhancing our security posture and supporting our broader institutional objectives.
>
> **Matt Riley,** Associate Vice Chancellor for Innovation and CIO

Looking ahead: a model for higher education

UIC's journey offers a compelling blueprint for other institutions navigating the complexities of cybersecurity in higher education. By aligning technology with mission-driven values, UIC has demonstrated that security and openness are not mutually exclusive — they are mutually reinforcing.

As threats continue to evolve, UIC remains committed to innovation, collaboration, and excellence. The university's experience underscores the power of strategic leadership, data-driven decision-making, and a community-first approach to cybersecurity.

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk> a CISCO company

Learn more: www.splunk.com/asksales

www.splunk.com