splunk>

CASE STUDY

University of San Francisco Promotes Efficiency, Increases Transparency With Splunk Cloud SIEM

UNIVERSITY OF SAN FRANCISCO

Executive summary

Founded in 1855, the University of San Francisco (USF) is a Jesuit university located in the heart of San Francisco. Like other universities, USF faces many challenges—from making payroll on time to maintaining accreditation and ensuring IT and security systems are in place to educate 10,000 students and support 2,500 faculty and staff. After evaluating several options, USF invested in Splunk Cloud as its new security information and event management (SIEM) solution. Since deploying Splunk Cloud, USF has seen benefits including:

- Improved security posture and ensured payment card industry (PCI) compliance
- Reduced phishing investigations from days to minutes
- Promoted transparency among university executives and staff

Why Splunk

Within USF's Information Technology Department, the Information Security and Compliance (ISC) group is tasked with the enormous challenge of providing security strategy, assessment and risk consultation as well as compliance monitoring and auditing across the university. Previously, ISC staff were concerned about the university's security posture and its ability to protect against and prevent phishing attempts and security breaches. USF recognizes the need to protect valuable personally identifiable information (PII), such as Social Security numbers and credit card data.

Nick Recchia, ISC director and information security officer, explains that as the university underwent a technology transformation, the group sought a SIEM solution that would enable the department to be more proactive in preventing security breaches. Additionally, USF required a solution that could ensure PCI requirements were met, and that would promote security operations transparency among university executives and staff.

"We evaluated a handful of SIEM solutions and created a matrix to compare them against one another. There were several similar features and opportunities among them, but there were also big differences," Recchia explains. "Splunk's turnkey cloud offering and hybrid option makes it magnitudes better than any of the others."

Industry

- Education

Splunk Use Cases

- Security
- Compliance
- IT operations

Challenges

- Needed to maintain high standards and keep the university's excellent reputation intact
- Wanted to enhance security posture and reduce vulnerabilities within systems
- Needed a baseline to establish health of information security
- Tasked with protecting PII data and ensuring PCI compliance
- Lacked security operations visibility among university staff and executives
- Recruitment and retention of talented InfoSec professional staff

Business Impact

- Implemented SIEM solution to create a more secure online environment and further safeguard university reputation
- Transformed data into valuable insights to enhance security posture
- Established baseline to monitor and improve health of information security
- Ensured PCI compliance by creating and sending automated alerts for faculty and staff to reset their passwords
- Protected PII data
- Provided a time-saving solution that promotes transparency across the university and among executives
- Provided a platform to increase engagement and meaning behind the work performed by InfoSec professional staff

Data Sources

- Server
- Application
- Network Device
- Firewall
- ServiceNow IT Service Management (ITSM)
- Banner Enterprise Resource Planning (ERP)
- Canvas Learning Management System (LMS)

Splunk Products

- Splunk Cloud
- Palo Alto Networks App for Splunk
- Qualys Technology Add-on for Splunk
- Cisco Cloudlock for Splunk
- Splunk App for ServiceNow

Automation brings meaningful alerts

Previously, USF had found difficulties in ensuring that all faculty and staff completed the mandatory information security training required by university officials. Recchia explains, "We have over 2,500 hard-working people throughout this university who are required to take basic training. And it's difficult for them to remember to take time out to complete this important task. So, how do you ensure they complete it and make it a simple process? We did it by creating a meaningful alerting system."

The ISC department uses the Splunk platform, integrated with ServiceNow, to send automated alerts to everyone required to take the course, to notify supervisors of their employees' status, and to enable staff to visualize the information gathered from the alerting system. As a result, the university has also significantly increased knowledge and transparency among executives, particularly through the widespread distribution of monthly reports that track university employees' progress in completing the training. Overall, the department has been able to produce measurable and substantial results, improving security awareness while gaining notice and visibility throughout the university.

"The way that we see the problem is that universities need to establish a baseline for IT security health," Recchia says. "And if they're ready to take that step toward it and make meaningful progress, coupled with executive leadership support and talented staff, such as USF Splunk expert Tim Ip to manage the product, then Splunk can be the most favorable tool you can get."

Phishing for a more transparent solution

Recchia explains that in the past the ISC department's systems and responses to security threats lacked transparency, both within the department and across the university. Since implementing Splunk Cloud as part of its technology transformation, the department is not only promoting efficiency but also providing full transparency into its processes.

> **"The top benefit of using Splunk Cloud is that it provides a system that promotes transparency and engagement. The platform has really opened the eyes of our peers and colleagues to the positive impact of a SIEM solution."**
>
> Nick Recchia,
> ISC Director and Information Security Officer,
> University of San Francisco

Prior to adopting Splunk Cloud, the manual process of investigating a phishing email would span from hours to days. Now, the Splunk platform enables the department to generate a list of all who need to be contacted, enabling investigations to take place within minutes. This new process has given all parties involved access to the steps taken within the investigation.

"The top benefit of using Splunk Cloud is that it provides a system that promotes transparency and engagement," Recchia says. "The platform has really opened the eyes of our peers and colleagues to the positive impact of a SIEM solution."

Additionally, with the use of Splunk Cloud to automate processes, the department has assured that USF remains PCI-compliant. For example, alerts have been helpful both in informing employees to change their passwords at a set pattern, and in providing reminders to update their antivirus software.

"The value Splunk adds is tremendous," concludes Recchia."And it's fun. When you can do something that's fun and you strive to make your career fun, and we can map out professional development and then demonstrate value to the organization, overall, it is an amazing and rewarding investment."

> **"The way that we see the problem is that universities need to establish a baseline for IT security health, and if they're ready to take that step toward it and make meaningful progress, coupled with executive leadership support and talented staff, such as USF Splunk expert Tim Ip to manage the product, then Splunk can be the most favorable tool you can get."**
>
> Nick Recchia,
> ISC Director and Information Security Officer,
> University of San Francisco

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>

Learn more: www.splunk.com/asksales

www.splunk.com