splunk>

CASE STUDY

UCAS Secures Millions of University Applications With Splunk Enterprise Security Analytics

UCAS

Executive summary

UCAS, the Universities and Colleges Admissions Service, is a charity, and the U.K.'s shared admissions service for higher education. They manage almost three million applications from around 700,000 people, each year, for full-time undergraduate courses at over 380 universities and colleges across the U.K., hosting a highly complex flow of sensitive, personal data. Demand for its services peaks in August when exam results are published — a period of heightened scrutiny from the media, public and government. Since deploying Splunk Cloud with Splunk Enterprise Security (ES), the company has seen benefits including:

- Real-time operational insights across infrastructure and business applications
- Increased security assurance with vital asset protection
- More time and resources for strategic thinking and business-oriented planning

Why Splunk

Demand for UCAS's services spikes over a two week period every August when the majority of exam results are published. During this critical period, UCAS has to scale exponentially, with the website receiving thousands of hits per second as university users log on for the latest view of applicants and applicants check to see if they have a place at university. Year-round, but especially during these two weeks, it needs to deliver faultless security assurance to stakeholders, including the students and universities whose data it holds and shares. Faced with such data volume and velocity, this challenge is considerable.

Previously, UCAS wanted a single, top-down and "live" analytics view of its security. But this was impossible with its existing, disparate systems, which often required manual monitoring by the team.

UCAS adopted Splunk ES with Splunk Cloud to gain real-time, end-to-end security visibility and reporting across its on-premises and Amazon Web Services (AWS) environments. An automated analytics-driven approach with Splunk lets UCAS identify and respond to issues before they become real problems.

Industry

- Higher education

Splunk Use Cases

- Security
- Fraud Detection

Challenges

- Lacked automated, analytics-driven approach to identify security anomalies
- Needed to assure security for public, education and government stakeholders
- Wanted real-time, end-to-end visibility and reporting across on-premises and AWS environments

Business Impact

- More resources for strategic planning by eliminating the need for an army of traditional security analyst roles
- Easier to prove security posture internally and externally through live dashboards
- Real-time operational insights into security systems enable UCAS to make better decisions during critical periods

Data Sources

- Antivirus
- File system auditing
- Database auditing
- Web access
- Web application
- Endpoint protection
- Boundary firewalls
- IDS/IPS
- Network firewalls
- Amazon Web Services

Splunk Products

- Splunk Enterprise Security
- Splunk Cloud
- Splunk App for AWS

Centralized visibility removes the need to firefight

Previously, UCAS had a very traditional approach to security analytics, manually crawling across systems, scanning for things that might or might not be malware. In recent years, the team has set up Splunk ES across a set of screens in its security operations center (SOC), so it could track and identify threats, trends and anomalies live across multiple security domains simultaneously. If something looked like a potential danger, the security team could respond in real time and investigate to prevent damage or escalation.

In removing potential firefighting scenarios, UCAS was able to allocate more time and resources to looking strategically at the threat landscape. This is an approach the organization continues to use and benefit from today.

Protecting vital assets with automated alerts

Every year UCAS hosts results data. This information is highly sensitive, so it's imperative that only authorized people can access it. As a priority, UCAS monitors file auditing on its systems to detect any activity from unauthorized users.

Manual execution of this task was inefficient, so the team deployed Splunk ES. The software enabled file storage area auditing and data onboarding within a day, and now automated alerts are sent to UCAS every morning detailing new folders and accounts created in the last 24 hours. "Rather than looking for trouble, all we have to do is look for an email," says Neil Bell, Security Assurance Manager, UCAS.

"With Splunk, we don't get sucked into the here and now. Instead, we can focus on responding to new upcoming threats, analyzing what our overall maturity looks like, and planning on how we're going to improve. There's no firefighting; we don't need to do that."

Neil Bell, Security Assurance Manager
UCAS