splunk>

CASE STUDY

University of Adelaide Gains Operational Visibility, Enhances Incident Detection and Resolution

THE UNIVERSITY OF ADELAIDE AUSTRALIA

Executive summary

Established in 1874, the University of Adelaide is Australia's third oldest university, with a strong reputation for research and teaching excellence and producing graduates that make an impact on the world. As the university's large and disparate IT network expands, security remains a significant priority. Since deploying Splunk Enterprise, the university has seen benefits including:

- Hundreds of hours saved in security analyst time annually
- Improvements in uptime and service continuity
- Faster threat mitigation

Why Splunk

The University of Adelaide constitutes a vibrant and diverse community with over 3,500 staff members and more than 25,000 students across four main campuses. The Information Technology Services (ITS) Group oversees and maintains the university's IT operations security. Dealing with a steady stream of security attacks had become an increasingly cumbersome exercise for the ITS Group. "Phishing attacks in particular were a growing problem for the technology team and our user base," says Mathew Benwell, information security specialist at the university. "Being able to more quickly recognize and respond to attacks became an overriding imperative for us."

The ITS Group set out to find a flexible solution to tie large data sets together and enable them to understand and respond to potential security issues quickly and efficiently. Assisted by SecureWare, a leading-edge information security solutions consulting firm, the team deployed Splunk Enterprise via a centralized high specification server to collect, analyze and secure the university's growing machine data volume and provide better overall visibility into security log data.

Mitigating security threats more effectively

The University of Adelaide's data continues to grow unabated, with around 140GB pulled into its Splunk deployment daily. An immediate goal of the deployment was to reduce the number of security-related events, in addition to efficiently identifying the initial problem,

Industry

- Higher education

Splunk Use Cases

- Security
- IT operations
- Business analytics
- Internet of Things (IoT)

Challenges

- Phishing attacks were a regular occurrence
- Needed to more quickly recognize and respond to attacks became
- Dealing with a steady stream of security attacks was increasingly resource- and time-intensive

Business Impact

- Saves hundreds of hours per year in security analyst time by automating log search and providing faster insight into potential anomalies and security threats
- Ensures uptime and service continuity by mitigating security threats
- Monthly reporting provides management with user overview of resource usage and planning
- Anticipated future technology investment savings

Data Sources

- UDP input from central syslog server and Universal forwarder on Microsoft Windows and Unix hosts
- Email (Cisco IronPort, Microsoft Exchange)
- Windows—Active Directory
- Citrix XenApp and XenDesktop
- Radius and proxy servers
- VPN device logs
- Palo Alto Perimeter Firewall logs and policy

Splunk Products

- Splunk Enterprise
- Splunk DB Connect
- Splunk App for Citrix XenDesktop
- Splunk App for Palo Alto Networks

correlating the associated data and remediating the issue before it became a significant threat.

Splunk software now provides enhanced incident detection at the university through numerous security-related searches across all data log sets. A single Splunk search dashboard displays any number of current security events including phishing attacks, high volume email traffic, account-related events such as password attacks and anomalous log-on events. "We are now better placed to respond to security threats than ever before," says Benwell.

Monitoring Internet usage

The university had removed its Internet quota model, but this presented the challenge of how to control Internet costs without using a quota-based system. "With a tweak to the Splunk App for Palo Alto Networks, we are able to monitor chargeable Internet usage at a level of visibility never before seen," says Benwell. "We have the ability to pinpoint, at an application level, where our Internet charges are being incurred." With such a granular level of visibility, the university can take action to control charging costs before these costs become an issue.

The university also deployed a Citrix-based solution to provide anywhere, anytime access to licensed applications. Using the Splunk App for Citrix XenDesktop, it can monitor near real-time and trending usage across its Citrix systems. Citrix data is then enriched with external lookups that provide additional context, in turn increasing the value of the information being reported. As Benwell notes, "Reporting on our Citrix environment is being used to identify uptake of the new system so we can best tailor the system to our users' needs."

Planning for the future and getting creative

Although it was initially deployed at the University of Adelaide as a security solution to help identify vulnerabilities across the university's network and continues to provide invaluable insights, the Splunk platform's wider potential for real-time Operational Intelligence has been proven. The information security specialist's advice to other organizations considering the software is to "get as creative as you can."

"Previously it could take hours to extract and analyze logs to identify security issues—now it can be measured in minutes. Splunk has given us the highest degree of certainty in meeting our immediate and future security needs."

Mathew Benwell, Information Security Specialist
Information Technology Services
University of Adelaide

For example, in light of physical space being a finite resource, the university wanted to more accurately plan for future infrastructure investment. Working with the Space Planning team, the university created "UniSpace," its own Splunk app for facilities data. The UniSpace app contains a series of multilevel, tabbed dashboards designed to provide 24/7 detailed insight into physical facilities used by the university. UniSpace utilizes Splunk DB Connect to index data from the university facilities management software, Archibus and compare space usage over time, at will.

Benwell concludes, "As the university starts to draw more on the intelligence that can be provided through our data, I am confident that the functionality available within Splunk software will continue to deliver the results we need."