splunk>

CASE STUDY

Splunk® at the University of Adelaide, South Australia

Efficient Incident Detection and Resolution
Thanks to Increased Operational Visibility

THE UNIVERSITY OF ADELAIDE
AUSTRALIA

> "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."
>
> **Information Security Specialist**
> *Information Technology Services*
> *University of Adelaide*

OVERVIEW

INDUSTRY

- Higher education

SPLUNK USE CASES

- Security
- Monitoring and troubleshooting
- Capacity planning
- Business intelligence

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 providing management with user overview of resource usage and planning
- Future technology investment savings

DATA SOURCES

- UDP input from central syslog server and Universal forwarder on Windows and Unix hosts
- Email – Ironport
- Email – Exchange
- Windows – Active directory
- Citrix XenApp and XenDesktop
- Radius server
- Proxy server
- VPN Device logs
- Palo Alto Perimeter Firewall logs and policy

The Business

The University of Adelaide is one of Australia's leading research-intensive universities and is consistently ranked among the top one percent of universities in the world. Established in 1874, it 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. The University has produced over 100 Rhodes Scholars, including Australia's first Indigenous winner, with five Nobel Laureates among its alumni community. There are more than 25,000 students, with 30 percent of them international students from more than 90 countries.

Challenges

The University constitutes a vibrant and diverse community with over 3,500 members of staff across four main campuses. Like any world-class institution of higher education, the University of Adelaide has an extensive wired and wireless network that already meets a diverse set of staff and student learning and information requirements. As the higher education sector continues to be reshaped by globalization and the digital revolution, the University's technology assets will be important components of the University's 2013-2023 "Beacon of Enlightenment" strategic plan.

As its large and disparate network expands, security remains a significant priority for the University of Adelaide. Phishing attacks had become a regular occurrence for the Information Technology Services (ITS) Group, which oversees and maintains the security of the University's IT operations. "Phishing attacks in particular were a growing problem for the technology team and our user base," explains an information security specialist within the IT Risk and Security team. "Being able to more quickly recognize and respond to attacks became an overriding imperative for us."

Enter Splunk

In 2012 the ITS Group set out to find a flexible solution that would help tie large data sets together and enable the team to understand and respond to potential security issues quickly and efficiently. Assisted by SecureWare, a leading-edge information security solutions consulting firm, the Risk and Security team deployed Splunk Enterprise via a centralized high specification server to collect, analyze and secure the University's growing volumes of machine data and provide better overall visibility into the department's security log data. According to the information security specialist, the team had Splunk up and running in a matter of hours, with a minimum amount of training.

Breakthroughs

Mitigating security threats in minutes

The University of Adelaide's data volumes continue to grow unabated, with around 140GB of data being pulled into its Splunk deployment on a daily basis. As a result, dealing with a steady stream of security attacks had become an increasingly resource- and time-intensive exercise for the ITS Group. An immediate goal of the deployment was to reduce the number of security related events, in addition to efficiently identifying the initial problem, correlating the associated data and remediating the issue before it became a significant threat.

Splunk software is now providing unparalleled incident detection at the University of Adelaide through numerous security-related searches across all data log sets. A single Splunk search dashboard displays any number of current security events including

OVERVIEW

DATA SOURCES (CONT.)

- Juniper SRX Internal Firewall logs
- Network device logs
- Unix Server SSH authentication events
- Nexpose/Nessus Vulnerability scan data
- Archibus (Oracle Database)

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. The key to efficient incident detection and resolution is thanks to increased visibility,” says the information security specialist.

Adaptability

Although Splunk was initially used by the Risk and Security group, the software’s ease of use and flexibility has meant that other teams have benefited from having access. “Traditionally the University’s technology service group has never had this depth of reporting capability, the scale of which is limited only by what you ask of it,” says the information security specialist.

At the start of the 2014 calendar year, the University removed its Internet quota model. The change in Internet accounting set an interesting challenge: how to control Internet costs without using a quota-based system. According to the information security specialist, “With a tweak to the Splunk for Palo Alto Networks App, we are able to monitor chargeable Internet usage at a level of visibility never before seen. 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 is able to take action to control charging costs before these costs become an issue.

The University has also recently deployed a Citrix-based solution to provide anywhere, anytime access to University licensed applications. Using the Splunk for XenApp and XenDesktop applications, the University now has the capability to monitor near real-time and trending usage across the two 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 the information security specialist noted, “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—Space Utilization

As the University itself grows, physical space becomes a more valuable and finite resource. “Physical facilities require careful management and the University can’t simply commission new buildings on a whim,” says the information security specialist. “If we can better understand how the current space is being used, then we can also more accurately plan for future infrastructure investment.”

Introducing “UniSpace”! Working with the Space Planning team, the University created its own Splunk App for facilities data maintained by the Space Planning team. UniSpace contains a series of multilevel, tabbed dashboards designed to provide school and faculty managers with 24/7 detailed insight into physical facilities used by the University. UniSpace utilizes Splunk DB Connect to access University facilities management software, Archibus. Regular indexing of Archibus data allows the University to compare space usage over time, at will.

No Limits—Get 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’.

Splunk allows for creativity because it does not require pre-defined schemas and keeps the data unstructured. This enables users to gain insights from their data even if they didn’t know what they would need to see at the time the data was collected. Once a problem is raised, Splunk software allows users to start identifying and correlating the data to generate the answer.

The information security specialist 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.”