splunk> listen to your data™

CASE STUDY

Splunk® at American University of Sharjah

Enhanced investigation capabilities leading to fast ROI and improved academic integrity

"Splunk can index any data and help you to create meaningful reports for any situation. I have learned to throw as much data as possible at Splunk. The more you use it, the more value you get from it."

Will Froning
Systems Architect, American University of Sharjah

OVERVIEW

INDUSTRY
- Education

SPLUNK USE CASES
- Security incident investigation and resolution
- Infrastructure and Operations Management
- Troubleshooting

BUSINESS IMPACT
- ROI through bandwidth management saving 92,000 AED (over $25,000) per month
- Improved security awareness and clean computing environment

DATA SOURCES
- Unix/Linux/Windows/AV server data
- UTM logs/syslog/web server logs/ active directory

The Business

American University of Sharjah (AUS) is an internationally accredited, independent, co-educational institution in the United Arab Emirates (UAE), serving a diverse student body from the Middle East and around the world. The university was founded in 1997 by His Highness Sheikh Dr. Sultan Bin Mohammad Al Qassimi, Member of the Supreme Council of the UAE and Ruler of Sharjah, who envisioned it as a leading educational institution in the Gulf region. Consciously based upon American institutions of higher education, AUS is thoroughly grounded in Arab culture and is part of a larger process of the revitalization of intellectual life in the Middle East.

Challenges

The Information Security Department at AUS coordinates with the AUS community to provide a safe computing environment. As such, it proactively monitors and protects the confidentiality and integrity of AUS data resources.

During a routine audit, the Information Security Department detected a security breach by some community members. When the IS department attempted to dig deeper, it found it did not have the ability to run ad hoc investigations nor generate reports. Previously, the only person that examined the data was the server owner and he only looked to troubleshoot if there was a known issue. Event correlation was impossible because of the need to first consolidate the various data sources and then perform the analysis. Faced with a serious security breach, the university needed a way to automate investigations, to isolate the incidents and identify the perpetrators.

Enter Splunk

The AUS's Systems Architect, Will Froning, was aware of Splunk® and had been eager to use the product for some time, but had never found a business case to put the technology forward. His team looked into competitive SIEM products but found that Splunk was the only solution that could provide a complete view of all the data sources across all business units to help identify anomalies and correlate information. While Splunk's free version was great for selective investigation, the university was going through 20 gigs of data a day and needed a full license to monitor on an on-going basis. The university therefore deployed the full Splunk Enterprise™ software across the organization in July 2011.

Troubleshooting

The key use case for Splunk at AUS is troubleshooting and resolving problems in the network area. As Splunk software indexes all the data available, it has made it easy for the AUS IS team to correlate data to identify the cause of problems and provide a speedier resolution to downtime or disruption. AUS has developed alerts for instances of equipment going offline, maintenance windows and any other issues

that could impact efficiency. This proactive monitoring enables the university to redirect activities and pre-empt any help desk calls, greatly improving the user experience and quality of service.

Investigations

Splunk Enterprise is playing a key security role at AUS, enabling the university to investigate suspicious activities in student and staff accounts. It is helping to identify unusual behaviors and provides incident reports should anything out of the ordinary occur. For example, Froning has created a multi-login report to highlight any potential breach of a faculty member's account. The AUS is also using Splunk software to provide reports on computers infected with malware and for monitoring advanced persistent threats. Splunk software is key to protecting the university's academic integrity.

Operational Management

Splunk is used by AUS to turn operational data into usable information, generating daily reports which can then be used to create custom dashboards to aid in making business-critical decisions. These reports include issues such as capacity, help desk inquiries, bandwidth usage, maintenance, security and other issues relating to the university's infrastructure that could impact on service.

Breakthroughs

ROI

Splunk has enabled AUS to demonstrate a speedy Return on Investment. Bandwidth in the UAE is very expensive, as availability is limited. Using Splunk, Froning's team is able to monitor how much bandwidth is being consumed and to correlate usage with IP addresses. Using this data, the university has been able to identify the highest trafficked internet destinations such as YouTube and to create a routing rule to move traffic onto a cheaper line. As a result, instead of upgrading its main leased line, the university is able to buy a lower cost alternative, creating a monthly saving of over $25k.

Ad hoc Enquiries

In addition to the daily reporting and investigative work, AUS has discovered that it can run just about any report it wants through Splunk. Froning was asked to create a report on user email accounts that provided information on the number of messages in the account, destination folders and the size of the stored messages. At first he thought this would not be possible, until he ran it through Splunk and was able to create a report in a very short space of time.

Community

AUS has attended a number of user training days and conferences to learn more about how Splunk can be utilized. AUS is a regular user of Splunkbase and sees it as a great source of information and app downloads. As a result, the dashboards created by AUS are getting more sophisticated and the searches more customized.