splunk>

CASE STUDY

American University of Sharjah Achieves Data Security and Fast ROI

Executive summary

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. Founded in 1997, AUS is based on American institutions of higher education, yet thoroughly grounded in Arab culture. The university needed the ability to run ad hoc investigations, create reports and proactively address data security concerns. Since deploying Splunk Enterprise, the university has seen benefits including:

- Improved security posture
- Savings of more than $25,000 per month in bandwidth costs
- Deep insight into complex campus operations

Why Splunk

The AUS Information Security Department (ISD) is charged with providing the AUS community with a secure computing environment. The department proactively monitors and protects the confidentiality and integrity of AUS data resources.

The ISD detected a security breach during a routine audit. When the department attempted to dig deeper, it found it did not have the ability to run ad hoc investigations nor generate reports. Until that point, the only person who had examined the data in question was the server owner, and he did so only to troubleshoot known issues. Event correlation was impossible because of the need to first consolidate various data sources and then perform the analysis. Faced with a serious breach, the university needed a way to automate investigations, isolate incidents and identify perpetrators.

AUS systems architect Will Froning was aware of Splunk and had been eager to use the product. Given the urgent security need, Froning's team compared Splunk software with competitive security information and event management (SIEM) products. The team discovered 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. The university deployed Splunk Enterprise across the organization in 2011.

Industry

- Higher education

Splunk Use Cases

- Security
- IT operations

Challenges

- Required to proactively monitor and protect confidential data resources
- Lacked ability to run ad hoc security investigations and reports
- Needed to provide centralized risk management and proactive mitigation
- Wanted to turn operational data into usable information

Business Impact

- Saving more than $25,000 (USD) per month in bandwidth costs through better monitoring and more cost-effective routing
- Improved security posture campus-wide, including proactive monitoring and faster threat resolution
- Providing deep insight into complex campus operations and distributed IT resources
- Improved user experience and quality of service

Data Sources

- Unix/Linux/Windows/AV server data
- UTM logs
- Syslog
- Web server logs
- Active Directory

Splunk Products

- Splunk Enterprise

Analytics-driven security

Splunk Enterprise continues to play a key security role at AUS, enabling the university to investigate suspicious activities in student and staff accounts, identify unusual behaviors, and provide incident reports on any anomalous events. For example, Froning has created a multi-login report to highlight any potential breach of a faculty member's account. The university is also using Splunk software to provide reports on computers infected with malware and for monitoring advanced persistent threats.

AUS is also using Splunk Enterprise for troubleshooting and resolving campus network issues. As Splunk software indexes all available data, it has made it easier for the AUS ISD team to correlate this 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.

Operational insights for informed decision-making

The university uses Splunk to turn operational data into usable information, generating daily reports that can then be used to create custom dashboards to aid in making business-critical decisions. These reports cover important metrics such as capacity, help desk inquiries, bandwidth usage, maintenance statistics, security and other issues relating to university infrastructure and operations.

"Splunk software 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

In addition to the daily reporting and investigative work, AUS is using Splunk Enterprise for ad hoc reporting. One such report on user email accounts was created by Froning on-the-fly and instantly provided information on the number of messages in the account, destination folders and the size of stored messages.

ROI is icing on the cake

The Splunk solution proved to have a speedy return on investment for AUS by enabling the university to monitor how much bandwidth was being consumed and to correlate usage with IP addresses. Bandwidth in the UAE is very expensive, and availability is limited. The university is now able to identify the highest trafficked Internet destinations such as YouTube and to create a routing rule to move traffic onto cheaper lines. As a result, instead of upgrading its main leased line, the university is able to buy a lower cost alternative, saving more than $25,000 (USD) per month.