splunk> listen to your data™

CASE STUDY

Splunk at University of Texas, Austin

Ensuring Network Security for a Distributed Campus

"We use Splunk software daily and it's critical to our operations. It makes us better equipped to detect new anomalies and respond to them quickly. Without it, we would be far less effective—I'm sure of that."

Cam Beasley
CISO, Information Security Office, University of Texas at Austin

OVERVIEW

INDUSTRY
- Higher Education

SPLUNK USE CASES
- Threat identification and control
- Outbreak management
- Campus-wide innovation
- Value-add Splunkbase apps

BUSINESS IMPACT
- Saves hundreds of hours per year in security analyst time by automating workflows and providing faster insight into events and anomalies
- Reduces organizational risk by preventing costly network breaches and negative publicity
- Reduces incident investigation time by providing fast access and analysis of log data from any source
- Improves security posture by filtering out false positives and providing data visualization
- Avoids loss of intellectual property
- Ensures uptime and service continuity by catching unknown threats and new zero-day attacks

DATA SOURCES
- Network flow
- Departmental servers
- System logs: Linux/UNIX, Windows, OS X, Solaris
- Security data: IDS/IPS, firewalls, access controls

The Business

The University of Texas at Austin is a top-ranked state research university and the flagship of the University of Texas System, which includes nine academic universities and six health science centers. The *Princeton Review* named the university one of the nation's Best Value Colleges for 2012.

Challenges

Founded in 1883, UT Austin has grown from a single building with eight teachers and 221 students to more than 50,000 students and 24,000 faculty and staff, giving it the fifth largest single-campus enrollment in the country as of the fall of 2011.

Like many colleges and universities, UT Austin depends heavily on its wired and wireless networks to enhance the educational experience and quality of life for students, faculty and staff. The 350-acre campus includes nearly 200 buildings linked by a 10 gigabit fiber optic backbone.

Up to 120,000 individual devices may be connected to the network at any time, including servers, switches, wireless access points, desktops, laptops, tablets, smart phones, security cameras and other systems. UT Austin's Information Security Office (ISO) and Information Technology Services (ITS) are responsible for ensuring network security.

Before Splunk, the ISO analysts relied primarily on intrusion detection/prevention system (IDS/IPS) appliances and custom-developed software tools to monitor network activity. "We wanted to plug into the many different servers and devices downstream that were coming under attack to correlate our network information with actual system log data," explains Cam Beasley, UT Austin's chief information security officer. "We didn't want a big heavy SIEM product because we hadn't had much luck with them in the past. We needed a more flexible system that we could adapt to our unique needs."

Enter Splunk

Beasley and his eight-member ISO staff began using Splunk software as a free trial, but quickly discovered that its value warranted an Enterprise license. The ISO team saw that Splunk represented an important analytical tool that met most of the needs of network and information security analysts by helping them investigate security threats and incidents faster and more accurately across the distributed UT Austin network.

More importantly, Splunk Enterprise™ enabled the ISO group to move to a more proactive posture by helping to identify unknown threats and network anomalies and allowing the ISO to alert the impacted departments and schools faster than ever before.

Breakthroughs

Faster, more accurate threat identification

Striking a balance between a highly distributed campus and effective network security is fine a line that the ISO team is adept at walking thanks to the help it gets from Splunk software.

"Splunk allowed us to distribute Splunk forwarders to many units to access log data where we were not able to before," Beasley notes. "In our main data center, where all departments are represented, we have an extensive distributed search infrastructure based on Splunk, including numerous forwarders, indexes and search engines."

Splunk Enterprise has helped automate the identification and response to malware threats, helping to control outbreaks and reduce or eliminate escalations. "Searches that used to take ten minutes can now be done in seconds with Splunk," Beasley emphasizes. "When an analyst has to do that several times per day, the savings add up. More importantly, Splunk software helps us identify and create signatures for new threats and deploy those signatures much faster."

Outbreak management

One recent malware outbreak provides an example of how the ISO team uses Splunk to identify and control suspicious events before they escalate into outages or breaches. In April 2012 the so-called Flashback Trojan began infecting Apple's OS X operating system.

The ISO team used its own custom Splunk application for event correlation and anomaly detection in combating Flashback. "Splunk helped us do a lot of the initial detection and identification of anomalies," Beasley recalls. "We used Splunk to trigger on certain types of events and alert us. By reducing our response time, we were able to contain the event."

Campus-wide growth spurs innovation

Today, dozens of instances of Splunk Enterprise are in use across the university. The ISO team has helped evangelize the use of Splunk software and provides assistance to other departments or groups.

The J.J. Pickle Research Campus, located about nine miles north of the main UT Austin campus, has used Splunk since 2009 and currently uses the Splunk for Unix and Linux app from Splunkbase to run ausearch for audit.logs on 125 systems. In this way, Pickle helps verify for itself and users of its high-performance computing facilities that it is in compliance with auditing guidelines.

Splunkbase apps add value

The ISO group also uses four Splunkbase apps to enhance its Splunk use and save time. These Splunkbase apps include Splunk for Use With MaxMind, Splunk on Splunk, Field Extractor, and Sanity Check My Splunk!

For instance, the Splunk for Use With MaxMind app helps identify anomalies based on geographical location. A user may login at one location at a certain time and then login again moments later at a different location, perhaps miles away. In the case of geographically impossible logins, the ISO group is alerted and can shut down a suspicious logon that may indicate a compromised user account.

"Splunk provides a simple visual view into our data that enables us to see emerging patterns, compare results, isolate commonalities and take action that prevents escalations and outages," Beasley says. "We use Splunk software daily and it's critical to our operations. It makes us better equipped to detect new anomalies and respond to them quickly. Without it, we would be far less effective—I'm sure of that."

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

250 Brannan St, San Francisco, CA, 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.splunkbase.com