Duke University Gains Powerful Security Insights and Fraud Protection

DUKE UNIVERSITY

Executive summary

Founded in 1838, Duke University (Duke) is a private research institution situated on an 8,500-acre campus in Durham, N.C. Duke is divided into 10 schools and colleges, serving nearly 15,000 undergraduate and graduate students. With faculty and staff added to the mix, Duke supports more than 68,000 active network users. The Duke IT Security Office was faced with data and usage challenges, including not having a security information and event management (SIEM) solution. Since deploying Splunk Enterprise, Duke has seen benefits including:

- Incident investigation and remediation reduced from hours to minutes
- Improved security posture
- Prevented phishing attacks and payroll fraud

Why Splunk

Duke's Information Security Office (ISO) became aware of Splunk software and its potential in 2013 during its search for a SIEM solution. The Duke Office of Information Technology (OIT) is a lean operation and typically creates its own tools or demands purchased solutions meet multiple needs—any SIEM solution had to be usable by those outside of security operations. "The SIEM products we reviewed seemed very powerful in demonstrations," explains Richard Biever, Duke's chief information security officer (CISO). "But when we tried to use them ourselves or when we tried to get other teams to use the tools, there was a frustrating learning curve. Splunk Enterprise was easy to deploy and use, and also flexible enough that we could adapt it to meet a wide range of needs across the university."

Today, Duke has a 1.25TB Splunk license shared among the ITO/ISO offices, the medical center and nine university departments. Nearly 3,000 devices run lightweight Splunk forwarders and capture data from more than 200 different source types, including syslogs, network/IPS/IDS/firewall devices, VPN, LDAP and operating systems.

"We wanted a solution that was not simply a security product,"

Industry

- Higher education

Splunk Use Cases

- Security

Challenges

- Lacked centralized log management system
- Difficulty detecting and investigating risks within IT environment
- Manual, laborious processes for incident investigation
- Wanted to improve reliability and security of email servers

Business Impact

- Reduces time to investigate and remediate security incidents from hours to minutes
- Provides quantifiable risk management information for use by academic business leadership
- Improves collaboration among formerly siloed departmental IT operations
- Extends security responsibility to entire organization through greater access and collaboration
- Meets need for customizable SIEM solution to accommodate the unique needs of a distributed IT environment
- Accelerates detection and correction of compromised user accounts, and helps detect and prevent phishing attacks and payroll fraud

Data Sources

- Web logs
- Sophos PureMessage anti-spam logs
- Postfix mail server logs
- Login event types: VPN, single sign on, SMTP
- Shibboleth single sign-on logs
- Operating systems, including Windows and *nix
- Network, IPS/IDS/Firewall logs
- LDAP

Splunk Products

- Splunk Enterprise
- Google Maps Add-on for Splunk Enterprise

Biever emphasizes. “We wanted something that could meet the unique needs of our systems team, our network team, application owners and identity management group. And that’s what we got with Splunk Enterprise. There’s no limit to what you can do with Splunk software. We have folks all over campus using it.”

Strengthening security posture with real-time alerting and reporting

Splunk Enterprise has enabled Duke to move from a reactive to a proactive approach to security, helped automate threat identification and remediation, centralized log management and analysis, streamlined performance monitoring, and made reporting more accessible and quantitative. The Splunk platform also plays a key role in real-time threat analysis and alerting. When indexed logs meet the parameters of an SSH brute force attack, for instance, the relevant IP addresses are flagged and sent to the school’s intrusion prevention system (IPS) for automated blocking.

Monitoring email traffic to increase security and identify DDoS attacks

In order to increase the security and reliability of the university’s email servers, Duke wanted to pinpoint the source of incoming junk email. While it seemed that most of this type of email was coming from outside the U.S., there was no hard evidence to support the theory. Jeremy Hopkins, a senior analyst for Duke’s enterprise internet services group, turned to Splunk Enterprise to make a case for geoIP-based filtering of email,

Hopkins and his team used advanced XML and the Google Maps Add-on for Splunk Enterprise to build a Splunk dashboard that could display recent junk email as geoIP hot spots on a global map view. This Splunk dashboard convinced management and Duke’s technology architecture group that email traffic needed to be filtered.

> “We wanted a solution that was not simply a security product. We wanted something that could meet the unique needs of our systems team, our network team, application owners and identity management group. And that’s what we got with Splunk Enterprise.”
>
> **Richard Biever**
> Chief Information Security Officer,
> Duke University

The university now also uses Splunk’s geoIP mapping capabilities to distinguish between Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Early identification of DDoS attacks is critical in combating the ongoing attack and preventing future events.

Waging war on fraud

In December 2013, a phishing email attack resulted in the theft of payroll deposits for several Duke employees. Immediately after receiving word of the phishing attacks, the Duke security team used Splunk Enterprise to set up a tracking dashboard to record suspected phishing messages in a Splunk lookup table. Another Splunk dashboard was created to aggregate phishing messages and recipient information, and provide information on recent changes to direct deposit accounts. These dashboards allow investigators to correlate information and contact employees to determine whether changes to direct deposit accounts are legitimate or are the result of phishing fraud.

“This type of visibility into logs and other sources did not exist for us before Splunk Enterprise,” concludes Hopkins. “In the past, the security office had to request access to logs. This is really a game changer for the security group. We have saved thousands of hours of work with Splunk software.”

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

© 2017 Splunk Inc. All rights reserved. Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.