splunk>

CASE STUDY

Splunk® at OhioHealth

Delivering Enhanced Real-Time Risk Assessment
and Cross-Platform Security Correlation and Analysis

> "I want data from every source available for aggregation and correlation in Splunk Enterprise to help us find the problems that we're not seeing today. The business wants to know—what's our risk posture today? What are the scariest things on the horizon? How can we deal with it? That's what Splunk is helping us achieve."
>
> **Brandon Allen**
> **Manager, Infrastructure Technologies**
> *OhioHealth*

OVERVIEW

INDUSTRY

- Healthcare

SPLUNK USE CASES

- Internet of Things
- IT operations
- Security

BUSINESS IMPACT

- Enables cross-platform security correlation and analysis
- Accelerates incident investigations
- Provides automated real-time metrics and data analytics
- Saves approximately $5k per phishing session with Splunk-powered solution
- Avoids up to $30k in annual maintenance for Active Directory audit software
- Anticipated savings by eliminating legacy SIEM licensing fees

DATA SOURCES

- Firewall and domain controller logs
- Switches, routers and other network devices
- Endpoint antivirus systems
- Vulnerability scanners
- Apache web server access logs
- Data Loss Prevention logs

SPLUNK SOLUTIONS

- Splunk Enterprise
- Splunk App for Enterprise Security

The Business

OhioHealth is a not-for-profit healthcare organization with Methodist roots, based in Columbus, Ohio. Founded in 1891, OhioHealth is comprised of 28,000 associates, physicians and volunteers, and a network of 11 hospitals, more than 50 ambulatory sites, hospice, home-health, medical equipment and other health services spanning a 40-county area. OhioHealth is recognized as one of the top five largest health systems in America by Truven Health Analytics. It has also been recognized by FORTUNE Magazine as one of the "100 Best Companies to Work For" for eight consecutive years.

Challenges

OhioHealth relies on a networked environment to provide seamless and secure access to patient medical records, telemedicine and other healthcare services. The health network has many software and hardware tools to help secure its IT environment, including firewalls, data loss prevention (DLP) software, vulnerability scanning, Active Directory domain controllers, antivirus and anti-malware protection, as well as a security information and event management (SIEM) solution.

While the security tools used by OhioHealth are individually effective, there is little integration among them, making ad hoc analysis a challenge and providing little opportunity for the aggregation and correlation of disparate security data. The health network wanted a solution that would work across data silos to consolidate its security tools, build an industry-leading security program, and provide an easy means of communicating potential risks to the organization.

Enter Splunk

OhioHealth's security operations team deployed Splunk Enterprise on a server dubbed "The Beast" and installed Splunk forwarders on all firewalls, domain controllers, switches and other devices. Splunk forwarders provide reliable and secure collection and delivery of data to the Splunk platform for indexing, storage and analysis.

Once logs and other data began to flow into Splunk Enterprise, the team used the solution to better support its missions: "guard the gates," ensure compliance to HIPAA and other regulatory requirements, and act as advisors to other IT groups and the business. Splunk enables the group to pull in data from all machine data sources, including firewalls and domain controllers. It also enables integration with an IT service management solution. Splunk software has helped accelerate incident investigations, enhance event correlation, and provide automated, real-time data analytics.

Breakthroughs

Phishing for the greater good

According to the Anti-Phishing Working Group, there were nearly 124,000 unique phishing attacks worldwide in the first half of 2014 alone. Every organization is susceptible to phishing attacks since they attempt to gain trusted access to critical data and personal information by exploiting human weaknesses, fooling someone to click on a malicious executable or link that is embedded in email. Healthcare providers are common phishing targets.

OhioHealth was evaluating services to conduct phishing audits of its health network. The security group was close to hiring a service that would have cost $5,000 per phishing test session. Instead, the team tied an internal phishing web server to Splunk Enterprise and wrote a basic script to send phishing emails to 700 randomly selected recipients throughout the OhioHealth network. After months of tests, the team conducted a live demo for upper management, using Splunk dashboards to display the results in real time. They were able to see exactly who clicked on the email—and if the phishing emails had been real, this would have resulted in potential infection or stolen credentials.

"The live Splunk demo raised awareness among our business leaders of the importance of risk analysis and mitigation," notes Brandon Allen, manager, infrastructure technologies, for OhioHealth. "Not only did Splunk help us create our own phishing test system, but we're saving the money we budgeted for an outside service." These phishing audits and demos have resulted in both soft (increased awareness, reduced susceptibility of being phished) and hard (conducted phishing tests using existing resources/tools) benefits.

Active Directory audits

During the implementation of a new biometric access system for OhioHealth physicians and other clinicians, critical blocks of users were inadvertently deleted from Active Directory. While the implementation team was eventually able to restore the users, the cause of the deletions remained unknown.

"We considered a leading security and compliance solution, but we realized it wasn't exactly what we needed and it would have cost us about $30k annually," says Allen. "We needed a way to audit our Active Directory services and determine what and when things were happening. We discovered we could create the system using Splunk Enterprise, basically for free."

By deploying Splunk forwarders on every domain controller to collect information from these devices and securely and reliably send them to the central Splunk instance for analysis, the security operations group was able to monitor the entire Active Directory Forest in real time, including any changes made to directories and user accounts. According to Allen, "We experienced the same access problem associated with the biometric solution about a week after we finished the auditing system in Splunk. This time, we found the source of the problem in matter of minutes. Problem solved."

IT troubleshooting

The OhioHealth networking group sends log data from all routers and switches to be indexed in Splunk Enterprise. The group was immediately rewarded with far deeper insight into network operations. Heretofore undiscovered operational details—such as disabled fans—were now easy to see and correct. The network group plans to feature Splunk as part of its next-generation network operations center (NOC).

SIEM replacement

OhioHealth is replacing its current SIEM with the Splunk App for Enterprise Security, which provides out-of-the-box incident review and classification, reports and security metrics, risk-based analyses, threat intelligence framework, unified search editor, statistical analysis and flexible dashboards.

Allen notes, "Our SIEM was just a SIEM, whereas Splunk is a data analytics platform with SIEM capability. Particularly when we have to dig through logs or look at Internet usage reports, it's just much faster to do it with Splunk Enterprise. If one of our business managers wants to know what his employees have been doing, we'll run that report in Splunk. We can ask any question and, with the right data, we can provide an answer with Splunk software. When it comes to anomaly detection, that's what we'll get with the Enterprise Security app."

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.