splunk>

CASE STUDY

# OhioHealth Accelerates Incident Investigations With Real-Time Data Analytics

OhioHealth

## Executive summary

Founded in 1891, OhioHealth is a not-for-profit healthcare organization 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 relies on a networked environment to provide seamless and secure access to patient medical records, telemedicine and other healthcare services. Since deploying Splunk Enterprise, the company has seen benefits including:

- Accelerated incident investigations
- Savings of about $5,000 per phishing session
- Avoidance of up to $30,000 in annual maintenance for Active Directory audit software

## Why Splunk

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, and a security information and event management (SIEM) solution. While these tools are individually effective, there's little integration among them, making ad hoc analysis a challenge and providing little opportunity to aggregate and correlate disparate security data. OhioHealth wanted a solution that would work across data silos to consolidate security tools, build an industry-leading security program and provide an easy means of communicating potential risks to the organization.

OhioHealth's security operations team deployed Splunk Enterprise 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 protect its infrastructure and ensure regulatory compliance to HIPAA and other requirements. Splunk software has helped accelerate incident investigations, enhance event correlation and provide automated, real-time data analytics.

### Industry

- Healthcare

### Splunk Use Cases

- IT operations
- Security

### Challenges

- Little integration among current security tools
- Ad hoc analysis was difficult
- Inability to aggregate and correlate disparate security data
- Wanted to build industry-leading security program

### Business Impact

- Enables cross-platform security correlation and analysis
- Accelerates incident investigations
- Provides automated real-time metrics and data analytics
- Savings of about $5,000 per phishing session
- Avoiding up to $30,000 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 Products

- Splunk Enterprise
- Splunk Enterprise Security

## Raising awareness about phishing and risk mitigation

OhioHealth was evaluating services to conduct phishing audits of its health network. The security group considered hiring a service that would have cost $5,000 per phishing test session. Instead, it 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," says the manager of infrastructure technologies at 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."

## Big savings on 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 eventually restored 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 $30,000 annually," says the manager. "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."

**"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. 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 Splunk Enterprise Security."**

Manager, Infrastructure Technologies
OhioHealth

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. When the same access problem occurred again, thanks to Splunk, the team was able to find the source of the problem in a matter of minutes.

## Deeper insight into network operations

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. Any undiscovered operational details—such as disabled fans—are now easy to see and correct. The network group plans to feature the Splunk solution as part of its next-generation network operations center (NOC). OhioHealth also plans to replace its SIEM solution with Splunk 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.