splunk>

CASE STUDY

Union Hospital Gains Comprehensive Visibility Into Security Landscape and Microsoft Infrastructure

UNION HOSPITAL

Executive summary

Union Hospital of Cecil County (UHCC) in Maryland is a 122-bed, non-profit, full-service healthcare facility, nationally recognized for its clinical excellence. Staff members and physicians deliver outpatient, surgical and emergency services, including an average of 20 procedures a day in the hospital's six operating rooms. Like all healthcare providers, UHCC must safeguard its patients' records. Since deploying Splunk Enterprise, the hospital has seen benefits including:

- A more robust security posture
- Accelerated application development and testing
- Extensive operational visibility across infrastructure

Why Splunk

Union Hospital relies on firewalls, anti-malware software and Active Directory domain controllers to deter breaches and advanced persistent threats (APTs). But UHCC's many systems generate gigabytes of logs daily, making scrutiny of this data laborious. Its 30-person IT staff lacked the resources to monitor, correlate and analyze logs from security solutions. "For a robust security posture, we had to expedite the tracking and cross-referencing of logs," says the security analyst for Union Hospital. "We can't comb through gigabytes of data looking for needles in the haystack. For added protection, we also wanted visibility into our Microsoft Exchange server to monitor how email enters and moves across our infrastructure."

The IT staff worked with BAI Commercial, a provider of network security solutions, to install Splunk Enterprise and link the software to the hospital's firewalls, anti-virus servers and domain controllers. The team also deployed applications that integrate with Splunk Enterprise, including the Splunk App for Windows Infrastructure to monitor and manage UHCC's Windows infrastructure, the Splunk Support for Active Directory app, which offers such functionality as searches of Active Directory for information, and Google Maps for Splunk for delivering geo-visualizations. The team also installed the Splunk App for Microsoft Exchange to gather performance metrics, log files and PowerShell data from the application and related components.

Industry

- Healthcare

Splunk Use Cases

- Security
- IT operations
- Application delivery

Challenges

- Wanted to analyze logs from key systems to aid in detecting intrusions
- Cumbersome manual processes and limited employees resources to monitor security data
- Needed to correlate large amounts of data from numerous disparate systems
- Needed visibility into Microsoft Exchange server to monitor how email enters and moves across the infrastructure

Business Impact

- A more robust security posture with reduced time needed to investigate and resolve security events
- Accelerated application development and testing
- Full visibility into Microsoft Exchange environment
- Extensive operational visibility across entirety of infrastructure
- Compliance with healthcare regulations
- Greater IT efficiencies

Data Sources

- Active Directory domain controllers
- Firewalls
- Anti-virus servers
- Microsoft Exchange server
- PowerShell data

Splunk Products

- Splunk Enterprise
- Splunk App for Microsoft Exchange
- Splunk App for Windows Infrastructure
- Splunk Support for Active Directory
- Google Maps for Splunk

Full operational visibility into Exchange

Using dashboards and reports from the Splunk App for Microsoft Exchange, UHCC's IT staff now has full visibility, including performance metrics, into Exchange and its underlying infrastructure such as Active Directory, Windows and OWA. Available dashboards cover IT operations, security, capacity planning and even help desk functionalities. As an example of operational insight, the IT team built a dashboard in response to a request from the director for IT to enable him to track the size and usage of employees' email accounts, allowing the size of mailboxes to be expanded when quotas are exceeded. Analysts can track email traversing the entirety of the hospital's network and can correlate Outlook Web App (OWA) data with firewall and anti-malware logs to determine whether any suspicious files have entered the infrastructure.

Bolstering security posture with advanced analytics

Splunk Enterprise now serves as a security intelligence platform at UHCC, helping analysts detect both known and unknown threats. Reading and correlating logs from multiple sources in multiple formats was previously challenging, but analysts now access data and correlate events almost instantaneously. Because the Splunk platform can capture and index data over time, they can deploy Splunk dashboards to track historical trends for an array of security metrics and launch investigations when events or actions deviate from baselines or appear abnormal.

To help detect APTs, the Splunk platform alerts IT on attempts to remotely access the hospital's infrastructure from foreign countries in which the hospital does not do business. Rather than traditional robotic malware, APTs are directed by cunning cybercriminals, which is why we need Operational Intelligence to spot and prevent them," says the security analyst. "Splunk software allows us to cross-reference any data at any time, letting us identify attack patterns and unauthorized actions that would otherwise go undetected."

"Correlating a firewall event with Exchange or Active Directory logs used to require so much time. Thanks to our Splunk solution, when I now need to investigate an incident, I have the full story in front of me. Instead of spending days trying to piece together what happened, I do so in minutes."

Security Analyst
Union Hospital

This awareness also extends to malware that circumvents firewalls and enters the network through employees' laptops. Splunk dashboards for the antivirus server keep analysts apprised of detected infections. They can search for particular virus signatures to determine which devices are infected and take corrective measures promptly.

Covering the entire network

UHCC is planning to use the Splunk solution to gain holistic views of its entire virtualized infrastructure. The hospital is considering indexing logs from its clinical applications to track and audit transactions and patient access. "Now that we're achieving our core security objectives, we're envisioning using Splunk software for network monitoring, performance metrics and diagnostics," concludes the security analyst. "Our Splunk solution definitely makes our lives easier not only for compliance but for general troubleshooting. We're getting an excellent return on our investment and that will only improve as we expand into additional use cases."