splunk>

CASE STUDY

Splunk® at Union Hospital of Cecil County

Comprehensive Visibility Into Security Landscape and Microsoft Infrastructure

UNION HOSPITAL

"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

OVERVIEW

INDUSTRY
- Healthcare

SPLUNK USE CASES
- Security
- Microsoft infrastructure monitoring
- Compliance

BUSINESS IMPACT
- A more robust security posture with reduced time needed to investigate and resolve security events
- 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

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

The Business

Union Hospital of Cecil County (UHCC) in Elkton, Maryland is a 122-bed, non-profit, full-service healthcare facility. It is nationally recognized for its clinical excellence, yet it remains a community hospital. Whenever a baby is born on its premises, for example, a lullaby plays over the intercom system. One thousand staff members and 260 physicians deliver outpatient, surgical and emergency services, including an average of 20 procedures a day in the hospital's six operating rooms.

Challenges

Like all healthcare providers, Union Hospital must safeguard its patients' records. For security, the hospital relies on firewalls, anti-malware software and Active Directory domain controllers to deter breaches and threats like Advanced Persistent Threats (APTs).

"Every week, it seems another enterprise is compromised by a sophisticated cyberattack," says the security analyst for Union Hospital. "Deterring them requires in-depth intelligence into what's happening in your environment. Logs offer this visibility by revealing who's accessing your network or trying to do so. Best practices call for analyzing the logs of key systems to correlate events and detect intrusions."

Union Hospital's many systems, however, generate gigabytes of logs daily, making scrutiny of these data very laborious. Its thirty-person IT staff, already tasked with around-the-clock monitoring of vital clinical systems, 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," adds the security specialist. "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."

Enter Splunk

Union Hospital's IT staff worked with Annapolis, MD–based BAI Commercial, a provider of network security solutions for enterprise organizations, to install Splunk Enterprise. By leveraging BAI Commercial's world-class engineering services, UHCC was able to link the software to the hospital's firewalls, anti-virus servers and domain controllers—and within an hour, the Splunk platform was ingesting logs.

"We were struck by how quickly the Splunk system was operational," says the security analyst. "Moreover, we were surprised by how much data our security solutions generate. We started with a license to ingest two gigabytes of data daily and almost immediately expanded to five gigabytes."

By the third day, the IT team was developing Splunk dashboards to visualize data from its security systems and its anti-virus server. The team also deployed a variety of Splunk Apps 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 IT team also began indexing logs for the hospital's Microsoft Exchange server. It installed the Splunk App for Microsoft Exchange to gather performance metrics, log files and PowerShell data from the application and related components. "We quickly derived value from our Splunk solution, and its ecosystem lets us meet our needs precisely and cost-effectively," says the security analyst. "We use many built-in dashboards, but we also created a few ourselves to capture the data we wanted. We soon increased our license to 20 gigabytes a day to ensure sufficient capacity."

Breakthroughs

Securing the hospital with advanced analytics

Using Splunk software, Union Hospital bolstered its security posture with comprehensive visibility and alerts. Splunk Enterprise now serves as a security intelligence platform that uses analytics to help detect both known and unknown threats. Whereas reading and correlating logs from multiple sources in multiple formats was previously challenging, analysts now access data and correlate events almost instantaneously.

Leveraging out-of-the-box dashboards from the Splunk App for Microsoft Exchange, UHCC analysts can track email traversing the hospital's network, who logs into the network, who has tried unsuccessfully to do so or if there are multiple failed log-ins, suggesting a brute force attack. They can correlate Outlook Web App (OWA) data with firewall and anti-malware logs to determine if any suspicious files enter the infrastructure. Because the Splunk platform can capture and index data over time, they 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.

"Correlating a firewall event with Exchange or Active Directory logs used to require so much time," says the security analyst. "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."

Seeing the network through Exchange

Using dashboards and reports from the Splunk App for Microsoft Exchange, the IT staff has optics, including performance metrics, into Exchange and its underlying infrastructure like 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.

Detecting APTs

To aid in detecting Advanced Persistent Threats (APTs), the Splunk platform alerts IT on attempts to remotely access the hospital's infrastructure from foreign countries such as Russia, in which the hospital does not do business. Additionally, with many attack vectors starting with phishing email to infiltrate malware, analysts can correlate Exchange, anti-malware servers and firewall logs for evidence of questionable downloads.

"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 allows us to cross-reference any data at any time, letting us identify attack patterns and unauthorized actions that would otherwise go undetected."

This awareness also extends to malware that circumvents firewalls and enters the network through employees' laptops. Splunk dashboards for the anti-virus 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

Union Hospital intends to expand its use of the Splunk platform. Because most applications and devices generate logs, the healthcare provider can use the solution to gain holistic views of its entire virtualized infrastructure. It is also 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."

Item # CS-Splunk-UH-105