splunk>

CASE STUDY

Supporting SCADA Systems to Secure Pipeline

Energy

Executive summary

One leading energy company provides midstream energy services to producers and consumers of natural gas, NGLs, crude oil, refined products and petrochemicals. The company has approximately 50,000 miles of pipeline across the United States, controlled by complex supervisory control and data acquisition (SCADA) systems and embedded industrial devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs), which connect pipeline sensors, compressors, valves and actuators to control centers. Since deploying Splunk Enterprise, the company has seen benefits including:

- System data correlation and in-depth analytical reporting
- Improved system availability and increased pipeline visibility
- Reduced security investigation time

Why Splunk

The company manages and monitors tens of thousands of field devices responsible for endpoint messaging, timeouts, leak detection and other essential functions. These devices are anywhere from five to 20-years-old and communicate via 10 different protocols. To get visibility into these devices, the company relied on a hodgepodge of in-house solutions and vendor-built tools with limited capability. While the company could investigate and determine that something occurred on an endpoint, it was impossible to correlate it with other events, messages and sensor data being monitored and generated by the multiple SCADA systems.

Moreover, the Pipeline and Hazardous Materials Safety Administration (PHMSA) expects high pipeline system availability, with any downtime tracked and accounted for appropriately. In the past, the company had encountered some system stability issues that made it challenging to monitor and enforce compliance with other pipeline safety regulations.

According to the company's supervisor of SCADA infrastructure and cybersecurity, "While evaluating a number of possible solutions to help monitor our very complex environments, we found that in order to address our multiple needs, we would have to have three to four

Industry

- Energy

Splunk Use Cases

- Industrial Data and the Internet of Things
- Security

Challenges

- Needed to improve reliability and security of systems deployed within SCADA
- Needed to meet PHMSA regulatory requirements
- Long and tedious operations and security investigations lacked visibility

Business Impact

- Increased operational and security visibility
- Increased efficiency with proactive alerts
- Improved SCADA performance boosts the bottom line
- Gained ability to track downtime for PHMSA
- Reduced security investigations from up to 12 hours to about one hour

Data Sources

- Schneider Electric DNA application logs (SCADA OASyS DNA System)
- Proprietary SCADA application logs
- AutoSol AES Poller data logs
- Application logs
- Symantec antivirus logs
- Lumension whitelisting logs
- Windows event logs
- Windows registry and configuration files (for security monitoring)
- Configuration file change monitoring
- Nessus scanner logs

Splunk Products

- Splunk Enterprise
- Splunk DBConnect
- Splunk App for VMware
- Palo Alto Networks App for Splunk

different applications. Our need to correlate data effectively would not have been met and the overall cost of deploying multiple solutions was much larger than we wanted to invest in. We discovered that we could accomplish the same tasks as four different applications with a single instance of Splunk Enterprise. The TCO of Splunk is approximately 400 percent less. We are very pleased with our investment and the capabilities of Splunk software."

Central pipeline control center monitoring

Since implementing Splunk Enterprise, the company has gained real-time visibility into the data collected from tens of thousands of field devices consisting of hundreds of thousands of endpoints inside the SCADA systems. SCADA staff members are able to analyze endpoint messaging, timeouts, leak detection and other essential functions, and also correlate the sensor data with SCADA systems for true operational visibility.

Beyond application data, the company also collects infrastructure data. By bringing data from the Schneider Electric OASyS DNA and other internal SCADA systems into Splunk Enterprise, the team has been able to create alerts and now has better visibility into the platforms that pipeline control operations use. Other Splunk Enterprise alerts let staff know that there may be system stability problems, enabling rapid response and meeting availability requirements. The Splunk platform also has had a big impact on the bottom line; as long as the SCADA system is performing, it is generating revenue.

In terms of security, Windows security, IDS and vulnerability scan logs are helpful in providing important visibility into vulnerabilities so that staff can proactively remedy them. If there is a security issue affecting multiple endpoints, Splunk Enterprise helps accomplish the security investigation in about one hour, down significantly from as many as 12 hours required in the past.

"We discovered that we could accomplish the same tasks as four different applications with a single instance of Splunk Enterprise. The TCO of Splunk is approximately 400 percent less. We are very pleased with our investment and the capabilities of Splunk software."

Supervisor, SCADA infrastructure and cybersecurity

The SCADA team now has other groups inquiring about Splunk software capabilities. Within the SCADA group, plans are underway to roll out Splunk Enterprise to additional industrial endpoints on its legacy systems to increase visibility, improve reliability and also implement Splunk Enterprise Security (ES) and Splunk IT Service Intelligence (ITSI). Reports are also currently being generated for outside groups via Splunk software.

Rapid investigation, improved stability and security

With Splunk Enterprise, the company has dramatically reduced time to investigate incidents, increased SCADA system stability and overall pipeline visibility, and expanded its reporting and alerting capabilities to proactively warn users about control system stability. The company is now also able to identify issues and problems on the system, report issues with the system to upper management and help personnel increase their effectiveness.

"We found a great solution in Splunk Enterprise," concludes the company's SCADA cybersecurity coordinator. "It enables us to meet each of our goals, as well as perform customization that is necessary in a SCADA (operational technology) environment, which has some significant differences compared to traditional IT environments."