splunk> Partnerverse CDI LLC

Petroleum Logistics Provider Transitions to Splunk Cloud for Intelligent Security & Compliance Analytics

CUSTOMER SUCCESS STORY

Key Challenges

Increased focus on unwavering commitments to safety, customer service, the environment and compliance identified a lack of full visibility into IT and industrial asset security. Alert fatigue and inability to verify potential treats required a modern, data driven approach.

Key Results

Insights provided into sophisticated attacks during rapid technology change and modernization of industrial control systems. Compliance and SOC teams have transitioned to a proactive posture and are able to review detailed and correlated data points and knowledge in real time.

Build a strong value proposition and fully understand the data landscape.

To modernize security and compliance operations, the Customer first needed to assess what telemetry is already being generated, how much of it is being captured, and where are the current portfolio of analytics solutions not providing the insights needed as the attack landscape is evolving. Coupled with a longer-term roadmap and strategy for investment in cybersecurity initiatives, the assessment solidified the business case to adopt Splunk Enterprise Security as the nerve center for security operations and built up the Splunk Cloud Platform to produce compliance audit evidence.

Turning a log and event assessment into a robust SIEM utilizing Splunk Cloud and Splunk Enterprise Security.

A log and event assessment assisted in benchmarking progress and identifying a long-term roadmap and strategy for log and event management. Over the last few years, following our prescribed roadmap with Splunk and ES as the core solution, their data centers are now secure, their security posture is hardened, and they are following recommended best practices of a mature information security and loss prevention program. Customer has been steadily increasing their ingest and has renewed their commitment to Splunk solutions for next three years.

Industry: Energy (Oil & Gas)

Solutions: Splunk Cloud Platform, Splunk Cloud Enterprise Security

Turning Data Into Outcomes

- Mean time to respond for security events reduced to under 30 minutes
- Ramp up time for new SOC Analysts dramatically reduced
- Reduce/mitigate risk
- Saved time with centralized monitoring from 250+ accounts
- Reduced latency across complex multi-cloud environment
- Threat detection for over 14,000 EDR endpoints

Iterative data onboarding and continued use case development and optimization.

Customer continues to engage with CDI in onboarding new data and advancing more sophisticated security use cases. We have assisted and provided services around crafting alerts, fixing data parsing issues, creating server certs, refining windows event filters, app installation, and forwarding server failures.

splunk> Partnerverse

Learn more: www.splunk.com/asksales

www.splunk.com