splunk>

CASE STUDY

TransAlta Teams With Splunk for Security and Operational Intelligence

Executive summary

Power generation and wholesale marketing company TransAlta operates in Canada, the U.S. and Australia. Its information security team is dedicated to protecting the company's computing infrastructure while enabling a safe landscape for employees to conduct business. Previously, TransAlta used another market leading tool for security information and event management (SIEM), but it was difficult to use and lacked the advanced technical capabilities required. Since deploying Splunk Enterprise and Splunk Enterprise Security (ES), the company has seen benefits including:

- User investigation time reduced from days to minutes
- On-time delivery of new energy trading platform
- Cost savings of up to $1 million
- Fast time to value with no training required

Why Splunk

Since 2009, TransAlta had been using a competing SIEM tool, but the company's talented team of certified SIEM professionals struggled to build actionable dashboards, reports and alerts, and found it wasn't technically feasible to do advanced correlations. In addition, the tool's security investigation process was slow, and the company had trouble staffing its security team because a limited number of people were familiar with the legacy SIEM.

After the DevOps and IT security teams were introduced to Splunk software, TransAlta proceeded with a two-month proof of concept (POC). During the POC, the company was able to bring more data sources into Splunk ES than was possible during the previous three years with its legacy SIEM. According to Ikenna Nwafor, senior IT security specialist at TransAlta, when the company implemented the Splunk platform it gained immediate value for IT security, IT operations and DevOps — all without any training. TransAlta was productive with advanced security use cases such as event correlation across multiple sources with data enrichment in only three-to-four months, something it was never able to accomplish with its legacy SIEM.

Industry

- Energy

Splunk Use Cases

- Security
- IT Operations
  - DevOps

Challenges

- Struggled with slow security investigations
- Challenged to staff team due to small pool of people familiar with legacy SIEM
- Needed to scale energy trading risk management platform to accommodate high trading volume
- Required reliable energy trading risk management platform performance

Business Impact

- User investigation time reduced from days to minutes
- Helped ensure on-time delivery of new energy trading risk management platform
- Cost savings of up to $1 million
- Fast time to value with no training required
- Improved energy trading platform visibility and performance

Data Sources

- Windows logs
- Microsoft Active Directory
- Anti-malware solution
- Vulnerability detection solution
- Next-generation firewalls
- Threat lists
- Unstructured data
- Advanced threat protection solution
- Cloud services
- End-point logs and forensics
- Honeywell card access data

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security
- Palo Alto Networks App for Splunk

"With Splunk ES, we experienced quick time to value," Nwafor says. "It was very easy to get up to speed on it. What I dreamed of in the past that was never possible, Splunk makes possible. Now, if somebody has a question, I say, 'just give me a minute.'"

Security investigations in minutes

TransAlta's strategic information security team provides direction to staff in the company's outsourced security operations center (SOC). Nwafor and his team monitor security events, and they have embraced a continuous improvement process in partnership with the SOC. "We use the Splunk platform daily to analyze the data, and then make the appropriate changes to our technology foundation," Nwafor says.

Today, TransAlta translates approximately 200 to 300 security use case line items into high-level Splunk ES dashboards. The SOC team focuses on 10 to 12 key security categories including incident investigation and forensics, security and compliance reporting, real-time monitoring of known threats, detecting unknown threats and insider threats. "Previously, confidential user investigation took us days or longer, and now it takes us minutes," Nwafor says.

TransAlta staff appreciate the ability to combine security and operational information with relative ease and to maintain relevant information in one place. The Splunk platform answers questions team members have and questions they had not thought to ask. Nwafor also notes that the company has achieved cost savings by displacing existing technologies and eliminating the need for some future purchases. For instance, by bringing storage logs into Splunk Enterprise and using prediction algorithms to forecast storage growth across all data domains, the company has saved up to $1 million.

"With Splunk ES, we experienced quick time to value. It was very easy to get up to speed on it. What I dreamed of in the past that was never possible, Splunk makes possible. Now, if somebody has a question, I say, 'just give me a minute."

Ikenna Nwafor, Senior IT Security Specialist
TransAlta

Improving operations

Beyond security, TransAlta has identified additional opportunities for Splunk software to contribute to the business. Given that team members are collecting logs from security end-points, they also benefit from having operational logs. TransAlta also builds its own apps for the Desktop and Server teams, among many others. With Splunk Enterprise and custom apps, these teams have access to the actionable information that they need more quickly than is possible with their other monitoring tools. For example, the Desktop teams have a variety of dashboards where they can check the health of thousands of desktop, laptop and tablet end-points to see where problems exist. In the Microsoft Windows landscape, when things like BSOD (operating system crashes) occur, TransAlta has the details needed to troubleshoot problem systems, drivers or software updates that are causing the issue.