splunk>

CASE STUDY

Leidos Taps Splunk ITSI for Better Event Management

Executive summary

Leidos' 48-year history spans everything from supporting the U.S. space shuttle program to helping design an America's Cup yacht race winner. Today the Fortune 500 science and technology solutions leader is working to solve global challenges in defense, intelligence, health and other markets—and facing its own challenges to ensure its services are always available to customers. Since replacing its legacy event management solution with Splunk IT Service Intelligence (ITSI), the Leidos internal IT department has seen benefits including:

- Real-time enterprise-wide infrastructure monitoring
- Robust solution to tear down IT silos and correlate events
- Dashboards for different audiences, from problem-solving techs to big-picture managers

Why Splunk

Leidos director of performance management Don Mahler says, "We have a real passion for infrastructure monitoring. Operational staff don't focus only on what's working; they want to know what's broken. Many issues result in more 'brown-out' conditions, not 'service-down' conditions. It is important operationally to get ahead of those before they get worse."

It's a 24/7 job, which Mahler divides into four operational areas where he uses Splunk ITSI. The first is situational awareness—determining what's working and what needs to be fixed. The second is performance and capacity planning, looking at components' performance over time to see if space, CPU, link utilization or other metrics are over dynamic thresholds. The third is logging for forensic, security and availability reasons. Finally, there is service delivery reporting, providing Leidos with real-time visibility into its operational environment.

The acid test is finding and fixing glitches before customers encounter them. Leidos needed a solution that could bring together sub-departments, IT and functional silos and triage a flood of events—spanning more than 120 IT services.

Industry

- Technology

Splunk Use Cases

- IT operations management
- Log management
- Security

Challenges

- Monitoring and response required for 24/7 customer access
- Separate silos created Balkanized IT department
- Needed to pare down thousands of alerts and events

Business Impact

- Real-time correlation and rules engine to automate event handling
- Seamless integration with management systems, apps and add-ons
- Easy to share and customize dashboards and glass tables for IT and business process views

Data Sources

- Application
- Device
- Firewall
- Network
- Server

Splunk Products

- Splunk Enterprise
- Splunk IT Service Intelligence (ITSI)
- Splunk DB Connect
- Splunk App for Microsoft Exchange

Beyond log management — transforming datacenter operations

Leidos started with a small Splunk Enterprise license to collect logs from routers and switches. The implementation rapidly grew to centralize alerts, ticketing, network, change and performance information from thousands of devices—all unstructured data, visualized in Splunk Enterprise dashboards.

A big benefit, Mahler says, is that the Splunk platform breaks silos by enabling teams to see data across the service stack. Not only can users get the information they need, but server staff, for example, can access relevant firewall data. "I see it as the common information model for the environment, and as a tool that can be used by every IT person—and business people—to get answers about the IT services."

According to Mahler, "I've been in IT management for over 20 years and I've not seen a product that does this. This is the first time I've been truly able to do heterogeneous, up-and-down-the-stack monitoring of my IT environment because Splunk has all the data and allows me to search it all in the same way."

Managing events smartly

The next natural step was alert management. Leidos had been using another solution for more than 15 years, which was not only outdated but bare-bones, with a complicated back-end rules language. The company wanted a modern product with out-of-the-box correlation and a rules engine to differentiate critical from minor events. The answer was Splunk ITSI.

"There are days when you get a flood of events; Splunk ITSI prioritizes the events, gives you insight into not only that this is broken but what's been affected right as you look at the alert screen," Mahler says.

"We have so much information at our fingertips thanks to Splunk… we're constantly solving business problems in creative ways."

Don Mahler
Director of Performance Management, Leidos

In addition to basic requirements such as consolidating events from its heterogeneous IT environment, detecting and suppressing duplicate alerts, clearing solved alerts and distilling them down to actionable events, the company needed extra functionality such as automatically escalating an alert after a period of time or suppressing one when a device was taken offline on purpose. Leidos achieved all of this with Splunk ITSI.

Today, approximately 20 management systems, from Microsoft System Center Configuration Manager (SCCM) to SolarWinds network management tools, more than 4,500 configuration items (CIs) across 120 IT services and 240 locations worldwide, feed into Splunk ITSI at Leidos, helping the company boil 3,500 to 5,000 daily alerts down to roughly 50 tickets for network and datacenter operations to act on. Passing CMDB information into Splunk ITSI allows different alert displays for different staff.

The bottom line: easier access to more relevant data, with staff time devoted to the issues that matter most. "My most important contribution at the end of the day is that we make a difference, that we provide a service that people find accurate and insightful," Mahler concludes. "The fact that Splunk has all of the information means that people can get their answers quicker, and more accurately and efficiently."