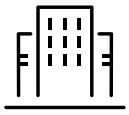
splunk>

CASE STUDY

US Government Cabinet-Level Department Reduces Costs, Improves Security Posture With Splunk Platform



Public Sector

Executive summary

Citizens expect government agencies to not only spend taxpayer dollars wisely but also make every effort to ensure resilient operations to deliver services effectively. One large U.S. cabinet-level department previously had HP ArcSight, a slow and expensive security information and event management (SIEM) tool that did not stand up to the needs of the agency. Since replacing it with Splunk Enterprise for security and compliance the department has seen benefits including:

- Saving $900,000 annually on software maintenance
- Improving security detection, response and remediation
- Reducing security investigation time from hours to minutes

Why Splunk

Originally a consultant with Qmulos, a Premier Splunk Partner, Jonathan Margulies and his team of Splunk architects and developers manage a large Splunk deployment serving a federal department made up of approximately 40 agencies, upward of 200,000 hosts and 130,000 users. Before Margulies joined the organization, the department's security operations center (SOC) was using HP ArcSight as its primary SIEM. "ArcSight was slow, difficult to develop on, and it was hard to find good experts who could use it," says Margulies, a Splunk architect and department consultant from Qmulos. "It was also very expensive and running typical investigations was an hours-long nightmare."

What's more, security compliance was lacking when it came to auditing logs. According to Margulies, some system owners weren't looking at logs at all, while others spent hours per week looking at logs that were mostly noise, all part of an effort to prove to an auditor that the department was following proper protocol. The department initially made a small Splunk Enterprise investment to augment its capabilities and improve compliance.

"Eventually the SOC just landed on Splunk," Margulies says. "They started using it, and with no training they jumped in and started searching for things. It was faster and it returned results better than ArcSight."

Industry

- Public Sector

Splunk Use Cases

- Security
- Compliance

Challenges

- Slow searches and investigations
- Costly software maintenance
- Limited talent available to run legacy software

Business Impact

- Savings of $900,000 annually on legacy software maintenance
- Proactive security stance and faster incident response
- Cutting security investigation time from hours to minutes
- Reducing waste, fraud and abuse
- Increasing security analysts' productivity

Data Sources

- Firewalls
- Web proxy
- VPN
- Email
- Intrusion detection systems
- Host data from workstations and servers
- Malware scanners
- Configuration management database (CMDB)
- Domain name system (DNS)

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security

Proactive security approach

Margulies and his team support the department's SOC, including 40 analysts who use Splunk Enterprise to investigate security incidents, as well as a large enterprise IT team that depends on the software for troubleshooting and reporting. Additional customers include staff who must ensure the department complies with security regulations.

Margulies explains that Splunk Enterprise has helped the department adopt a more proactive security approach. Previously, team members focused on responding to and remediating security incidents after receiving an alert from one of its tools. Now, staff have more time to hunt, and intuitive searches are rewarding because they complete quickly and reveal important insights. For instance, Splunk Enterprise has helped identify and reduce waste, fraud and abuse incidents, such as users visiting websites they shouldn't, wasting bandwidth, and so forth.

In addition, one major benefit the department has realized from using Splunk Enterprise is rapid detection, response and remediation of email phishing campaigns. As an example, a custom Splunk Enterprise email dashboard that helps track which emails reach their targets is saving the department hours of investigation time. Previously, those investigations sometimes ran overnight, and the department now has information it needs in minutes.

Meeting security compliance

Margulies notes that logging compliance has improved since the department implemented Splunk Enterprise. With Splunk Enterprise maintaining the raw logs, including web proxy, VPN and host data from workstations and servers, malware scanners, email, domain name system (DNS), firewalls and intrusion detection systems, auditors are satisfied and requirements are met. Another tangible result is that staff productivity has significantly improved. Instead of spending four-to-six hours per week poring through logs, they now load a dashboard once a week and take a quick look for anomalies.

"Splunk has helped my department save $900,000 in maintenance this year, which paid for my whole team."

Jonathan Margulies
Splunk Architect and Consultant, Qmulos

Scalable, easy-to-use, cost-effective platform

With Splunk Enterprise, the department easily built a single pane-of-glass for the SOC to monitor and alert on user log data, enabling department-wide visibility and security. And, because the security platform was built to store and work on raw log data, it makes compliance, legal and security a cinch. The department also appreciates having a complete programming platform with great documentation and offering additional flexibility.

Margulies and his colleagues value Splunk Enterprise for many additional reasons, including its scalability, the ability to customize it, its easy-to-use visualizations and the cost savings it offers. "Splunk has helped my department save $900,000 in maintenance this year, which paid for my whole team," Margulies concludes.

"Eventually the SOC just landed on Splunk. They started using it, and with no training they jumped in and started searching for things. It was faster and it returned results better than ArcSight."

Jonathan Margulies
Splunk Architect and Consultant, Qmulos