splunk>

CASE STUDY

SAIC Builds New World-Class Security Operations Center

SAIC®

Executive summary

Science Applications International Corp. (SAIC) is a leading technology integrator that specializes in technical, engineering and enterprise information markets. With expertise in domains such as scientific research, program management and IT services, SAIC derives most of its income from the U.S. government. The company needed to build out a robust security operations center (SOC) and computer incident response team (CIRT) to defend against cyberattacks. Since deploying the Splunk platform, the company has seen benefits including:

- Improved security posture and operational maturity
- 80+ percent decrease in incident detection and remediation times
- Comprehensive visibility throughout the enterprise environment

Why Splunk

After the original SAIC split into two companies in 2013 to avoid organizational conflicts of interest, SAIC needed to build a SOC as part of its new security program. Although it had most of the security tools it needed, SAIC lacked a security information and event management (SIEM) solution to anchor its defenses. The traditional SIEM used by the original company as its core tool for security investigations had limitations. SAIC supplemented the SIEM with Splunk Enterprise, using the platform for incident detection via correlation searches, as well as for incident investigations. SAIC's IT operations staff is now also using the Splunk solution for network monitoring, performance management, application analytics and reporting.

Once SAIC began building its new SOC, the company decided to rely on Splunk as the single security intelligence platform for all of its SIEM-like needs, including incident detection, investigations and reporting for continuous monitoring, alerting and analytics. SAIC also purchased Splunk Enterprise Security (Splunk ES) for its pre-built correlation searches, incident review workflow, reports, dashboards and threat intelligence feeds. SAIC began indexing hundreds of GB a day of data into the Splunk solution from various data sources, including firewalls, intrusion detection, anti-virus and vulnerability scanner systems.

Industry

- Technology

Splunk Use Cases

- Application delivery
- IT operations
- Security

Challenges

- Needed to create a world-class SOC with superior response and maturity levels
- Lacked SIEM solution
- Wanted full visibility across silos to rapidly search and analyze security-related events
- Seeking agile solution to decrease MTTR

Business Impact

- Increased security posture and operational maturity
- Measurable decrease (80 percent) in incident detection and remediation times
- A more efficient relationship between the SOC and CIRT teams
- Comprehensive visibility throughout the enterprise environment
- Efficiencies from leveraging a common tool between security and IT operations

Data Sources

- Palo Alto Networks and Juniper firewalls
- Sourcefire and Snort intrusion detection systems
- Anti-virus systems
- McAfee vulnerability scans
- Windows and Linux server OS logs
- Apache and IIS web server application logs
- Active Directory domain controllers
- IronPort email security appliance and email/SMTP servers

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security

Full visibility and threat detection across the environment

SAIC now uses Splunk software to monitor its environment for any threats. In the SOC, analysts monitor custom Splunk dashboards for alerts and signs of anomalous or unauthorized behavior. They're now immediately aware of known, signature-based threats (such as those logged by the IDS or malware solution), and unknown threats (such as a privileged account with atypical activity).

Traditional SIEMs generally search using pre-built, rigid searches, which fail to catch advanced threats and generate substantial false positives. With the Splunk platform, SAIC analysts have built new, highly accurate correlation searches to detect threats and indicators of compromise specific to SAIC, allowing the team to measure and manage risk at a high level. Executives, including the CISO, can now see key metrics around threat activity, including trends, the aggregated source location and newly seen indicators of compromise.

Faster and deeper investigations, reduced costs

When an incident is detected, Splunk dashboards accelerate analysis by allowing incident responders to quickly drill down into the underlying event data for details that reveal evidence of malicious activity. The dashboards let analysts simply enter an IP, user name or machine name to see all relevant information and context from many data sources. With historical data at their fingertips, analysts have full visibility into security events. As a result, SAIC has slashed the time needed to conduct investigations by more than 80 percent. According to Jonathan Jowers, chief information security officer, SAIC, "When the Splunk solution became our primary security tool, our resolution times dropped dramatically."

"The template for effective security is visibility, analysis and action. Our Splunk system gives us comprehensive optics and deep, data-driven analytics, enabling us to take highly informed action to protect our assets."

Jonathan Jowers, Chief Information Security Officer
SAIC

One example of an accelerated incident investigation occurred when an employee brought an infected personal laptop to work. Splunk software issued an alert in near real time that malicious traffic had been detected by the firewall as a result of the malware. Within minutes, analysts found the laptop's location and removed it from the network.

A SOC with world-class agility

With Splunk software, SAIC has been able to realize significant operational efficiencies and reduced labor costs across the 50-plus security personnel in the SOC and on the CIRT. Some of these efficiencies have come from accelerated incident investigations, less time researching false positives and a faster handoff between the SOC and CIRT teams, which can now share the same data.

Furthermore, data sharing in Splunk by various teams has led to greater ROI and improved overall IT efficiency. As an example of the data-driven approach enabled by Splunk software, analysts identified, isolated and remediated the Heartbleed bug within just 30 days of launching the SOC. Thanks to the Splunk platform, SAIC's SOC and CIRT teams are responding to threats with world-class agility.