splunk>

CASE STUDY

Digital Services Provider Improves Security Posture With Splunk Enterprise Security

Digital Services Provider

Executive summary

When an innovative digital services provider faced security and compliance challenges, it was concerned that failure to address issues quickly could have a negative impact on the bottom line. At the time, the company relied on a managed security services provider (MSSP) that was not providing the visibility and robust security coverage the company required. After evaluating its options, the digital services provider decided to augment its MSSP by bringing security monitoring in-house. Since deploying Splunk Enterprise Security (ES) as its security information and event management (SIEM) solution, the company has seen benefits including:

- Improved security posture through an increase in reporting frequency from daily to real time
- Compliance with SOC 2 Type II to keep customer data safe
- Freeing up engineering resources to focus on hunting and policy recommendations

Why Splunk

Prior to deploying Splunk ES, the digital services provider sent log data from its customer hosting environment to its MSSP. However, this method failed to provide enough value in sorting out false positives and negatives, which increased the workload for the company's geographically dispersed team of 12 security analysts and engineers tasked with protecting customer data. What's more, the company was concerned about delays in receiving important information. Rather than getting actionable alerts or access to visualizations in real time, the MSSP provided reports to its customer at the end of each day. This meant that the digital services provider's risk exposure was gated by the MSSP's delivery window. Any specific incident—from an attempted breach to a viable attack—could remain within the company's infrastructure for long periods of time.

The company realized it needed to own its security posture end-to-end, and it issued an RFP to vendors in the Gartner SIEM Magic Quadrant, including Splunk, HP, IBM and LogRhythm, before narrowing its selection to Splunk and LogRhythm. The ability to get to raw data fidelity with

Industry

- Technology (Digital Services)

Splunk Use Cases

- Security
- Compliance

Challenges

- Lack of real-time security information left the company vulnerable to breaches and attacks
- Many false positives and negatives increased the workload for security analysts and engineers
- The company needed to demonstrate SOC 2 Type II compliance

Business Impact

- Improved security posture through an increase in frequency of reporting from once daily to real time
- Freed up engineering resources to focus on higher-level hunting and policy recommendations
- Achieved SOC 2 Type II compliance, demonstrating the company's commitment to keeping customer data safe

Data Sources

- Windows Servers (security, system, application, IIS, SharePoint, SQL Server, CRM, DHCP, Hyper-V, SCEP)
- Linux Servers (Syslog, Apache, BIND)
- Endpoint antivirus and antimalware
- DNS
- Microsoft Azure Cloud Services, SharePoint
- Routers, switches, load balancers, web application firewalls, next-generation firewalls
- VMware vSphere
- Homegrown software

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security

Splunk ES, rather than having to go to another log aggregation location, intrigued the company's advanced analysts and engineers. The value and credibility of Splunk's implementation services delivery, its ability to address multiple use cases beyond security, its Splunkbase apps ecosystem, and the ability of Splunk ES to scale were deciding factors in the company's decision.

Through the excellent delivery services provided by Splunk partner rSolutions and by enabling the customer through Splunk education courses, the company was able to gain needed insights with Splunk ES quickly.

Comprehensive visibility with tiered MSSP and SOC responsibilities

With Splunk ES, today the digital services provider has the analytics it needs to monitor and respond to incidents in its security operations center (SOC). The company can now make decisions for the business regarding who, where, and how its security posture is manifested, with full visibility into the data that supports those metrics. Using Splunk ES, the security team is not only meeting its previous use cases but is expanding into additional use cases as well.

For now, the company has retained its MSSP to focus on low-level monitoring and other targeted Tier 1 responsibilities. If the MSSP identifies something of interest, it can then escalate it to the security engineers and analysts in the SOC. Meanwhile, the more advanced Tier 2 and Tier 3 security engineers and analysts in the SOC no longer have to sort through noise and can instead focus on hunting, investigating and monitoring actionable information.

Engineers and analysts can also focus on validation of policies, and recommend work flow or policy changes, if necessary. What's more, with SOC 2 Type II certification the company has proven that its system is designed to keep its clients' sensitive data secure.

Today, instead of relying too much on its MSSP, the company is able to make better use of its internal and external resources. With the Splunk ES platform, the digital services provider's SOC analysts and engineers now have end-to-end security visibility.

Threat intelligence framework adds value

The company also relies on the Threat Intelligence framework, a mechanism for consuming and managing threat feeds, detecting threats, and alerting—one of five frameworks that organizations can integrate into Splunk ES. This digital services provider sees value in having up-to-date intelligence regarding today's bad actors. Subscribing to both open-source and commercial feeds brings the best research together for the company's security posture.