splunk>

CASE STUDY

Financial Services Company Gains Actionable Security Intelligence With Splunk Enterprise Security (ES)

Financial Services

Executive summary

In the highly regulated financial services industry, one leading global company encountered limitations with its legacy security investigation and event monitoring (SIEM) software. The financial services company needed a new solution that could ingest growing volumes of data, minimize risk, speed security investigations and integrate with its governance, risk and compliance (GRC) solution. Since deploying Splunk Enterprise and Splunk Enterprise Security (ES) as its data analytics security platform, the company has seen benefits including:

- Rapid implementation resulting in more than 100 use cases
- Ability to ingest growing volumes of data
- Quickly complete security searches and respond to actionable alerts in seconds

Why Splunk

Previously, the bank's global security operations center (SOC) was a multivendor environment that included HP ArcSight Logger and Enterprise Security Management (ESM) for security. The company's security team grew tired of continual challenges it faced in managing the volume of data coming in to the HP ArcSight environment and even more difficult issues around getting useful data out of it. The company's SIEM also was slow to search and lacked the scalability the company required. What's more, staff spent a lot of time keeping the software's custom data collectors up-to-date and had to bring in costly consultants to help manage the data collectors on an ongoing basis.

Even with all of the effort staff put forth with its previous SIEM, the company's security visibility was limited by the data sources it could ingest. Since it implemented Splunk Enterprise and Splunk ES, the company has been able to aggregate and correlate all of its multivendor data in one place. The amount of data volume that this company has and will have moving forward is exploding, which will require it to take a holistic view of its security posture. With Splunk ES, the company has a solution for handling terabytes of data regularly and responding to actionable alerts quickly. The ability to identify an issue and then plug the hole not only saves a lot of money and time but also diminishes the risk of future security problems occurring.

Industry

- Financial Services

Splunk Use Cases

- Security

Challenges

- Managing collectors was time-consuming and costly
- Security searches were slow
- Needed security data analytics platform that could scale
- Required security solution to integrate with GRC software

Business Impact

- Quickly generate searches to find the needle in the haystack, which was not possible with HP ArcSight or Logger
- Ability to ingest growing volumes of data — currently greater than 1TB of data per day
- Security searches and actionable alerts occur in seconds with Splunk ES versus multiple minutes with legacy SIEM
- Integration with GRC solution

Data Sources

- Proxy logs
- Endpoint logs
- Anti-malware logs
- Firewall logs
- Database logs
- Operating system logs
- IBM Resource Access Control Facility (RACF) and Guardium logs

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security

A staged approach

Typically, an HP ArcSight replacement may take up to 24 months – about the same amount of time to unwind it as to wind it up. In only six months, the company has replaced HP Logger and ESM with Splunk Enterprise and Splunk ES and is ingesting more than 1TB of data daily. The HP ArcSight replacement was completed in a staged approach. The first step was to set up the logging infrastructure, which was rebuilt to ingest all of the organization's security data and enabled the decommissioning of all of the HP loggers.

After that successful first step, the company accessed all Splunk ES security domains — including access, endpoint, network and identity — while it continued to use HP ArcSight for visibility into its security environment. From there, the company began replacement of the HP ESM functionality with a combination of Splunk ES and the integrated GRC solution. The implementation team maintained an aggressive pace of adding one to two data sources per week for many months, and now includes proxy, endpoint, anti-malware, firewall, database and operating system data. To date, the company has implemented 100 security use cases and plans are underway to add 40 more.

Rapid security investigations

Currently, up to 30 people use Splunk Enterprise and Splunk ES for security. The company is pleased with its Splunk implementation, as it is enabling the security team to handle and close security incidents faster than was possible in the past. For instance, typical Splunk ES searches occur in seconds versus multiple minutes previously, and what was a typical 30-minute search with HP ESM in the past can now be completed in just 10 seconds with Splunk ES.

Also notable is the fact that this company, like others in financial services industry, is highly compartmentalized, and while it moves somewhat slowly it still was able to begin using Splunk ES in a short period of time. With Splunk ES, the company has a solution that offers ease of use and at a cost that will enable it to scale. Moving forward, the company will begin conversations around using Splunk ES for additional use cases including fraud.