Sierra-Cedar

Client Snapshot

About

Financial Services Company Client is one of the largest providers of mutual funds and exchange-traded funds (ETFs) in the world. The company also offers brokerage services, variable and fixed annuities, educational account services, financial planning, asset management, and trust services.

The Splunk Enterprise Security premium application was a robust replacement for the client's aging security system. The state-of-the-art Splunk cloud-based platform also supported traditional IT operations and IT Service Intelligence use cases.

Eric Newman
Director, Splunk Services
Sierra-Cedar, Inc.

Location:

Mid-Atlantic region of the United States

Industry:

Financial Services

Technology:

Splunk Cloud, Splunk Enterprise Security (ES), Splunk IT Service Intelligence (ITSI), Amazon Web Services (AWS)

About Sierra-Cedar

Sierra-Cedar delivers industry-focused client success by providing consulting, technical, and managed services for the deployment, management, and optimization of next-generation applications and technology.
www.Sierra-Cedar.com

Background

The operations of a global financial services company with over $5 trillion in assets under management were being hindered by an antiquated, limited-capacity Security Information Event Management (SIEM) system. This system, built with numerous Windows-based servers that were difficult to manage and maintain, was ineffective at managing security alerts and was prone to frequent outages. Additionally, the company's on-premise log management system was frozen to new data, creating a large backlog of additional use cases that were not being served.

Challenges

The company needed a partner who could help it overcome these challenges:

- An outdated SIEM and log management system that limited the ability to effectively monitor security
- The inability to provide suitable access and availability to more than 1,000 users and several business units spread across the globe
- Lack of capacity to efficiently handle a high volume of events from multiple data centers (more than 7TB/day)

Solution

With Sierra-Cedar's assistance, the company implemented the Splunk Cloud platform, including the Enterprise Security (ES) and Information Technology Service Intelligence (ITSI) premium applications. The solution included multiple intermediate forwarder tiers to manage the parsing of events from thousands of devices across multiple time zones and data centers.

The solution also implemented a series of high-capacity syslog clusters designed to capture traffic for network and security devices:

- Multiple Firewall Vendors
- Wireless Access Points
- Web Application Firewalls
- Intrusion Prevention Systems
- Data Loss Prevention Hardware
- Router and Switches
- Load Balancers
- Mainframe systems

To gather information from cloud-based systems, Sierra-Cedar assisted with the creation of data collection nodes based on Amazon Web Services (AWS) that leveraged an Infrastructure-as-Code process and the customer's existing continuous delivery pipeline.

With a single, highly available system, the company was positioned for success.