splunk>

CASE STUDY

Financial Services Provider Delivers Analytics and Security Intelligence for Regulatory Compliance

Financial Services

Executive summary

This financial services provider offers industry-leading credit, debit and prepaid card servicing to millions of cardholders, as well as bill payment solutions to a significant volume of online bill payment subscribers. In order to conduct in-depth investigations into incidents, the company needed consolidated views into its siloed security systems. Since deploying Splunk Enterprise, the company has seen benefits including:

- Greater levels of security
- Highly-flexible SIEM functionality
- Accelerated remediation of issues

Why Splunk

The financial services provider processes billions of credit card numbers at any point in time. As a result, it must comply with the Payment Card Industry Data Security Standard (PCI DSS), which calls for securing credit, debit and cash card transactions, as well as cardholders' personal information. However, without a centralized repository for the security data generated by each of its safeguards, the provider's small security staff was forced to resort to laborious and time consuming manual processes.

To enhance its security posture while reducing the burden on its staff, the financial services provider initially deployed Splunk Enterprise to collect and index logs and other data from any networked source, enabling staff to query and correlate this information and display the results in dashboards. The provider subsequently deployed Splunk Enterprise Security (Splunk ES), a premium security solution that enhances the Splunk platform to help security teams quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk and safeguarding the business. Splunk ES provides a clear visual picture of the organization's security posture, delivering a comprehensive set of pre-built dashboards, reports, analytics and correlations to rapidly respond to threats.

Industry

- Financial services

Splunk Use Cases

- Security

Challenges

- Lack of operational visibility into systems and network
- Siloed infrastructure without centralized repository for security data
- Time-consuming manual processes straining employee resources for incident investigation and mitigation

Business Impact

- PCI DSS compliance
- Greater levels of security
- Highly-flexible SIEM functionality
- Accelerated remediation of issues
- Greater efficiencies for reduced headcount

Data Sources

- Perimeter firewalls and VPN servers
- IDS/IPS systems
- Microsoft Active Directory
- Virtual private networks (VPNs)
- Threat intelligence feeds and malware lists
- Workstations, endpoints and databases

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security

Splunk eliminates silos for enterprise-wide security intelligence

By using Splunk software to aggregate and visualize data from its infrastructure and many security tools to the Splunk platform, the financial services provider now has unified views of all security information and events. Thanks to Splunk dashboards, administrators discovered that the firm's disparate security systems were blocking 400,000 attempted port intrusions every four hours and had deterred 16,000 pieces of malware from entering the network over a month.

The flexibility of the Splunk platform has enabled the information security principal to further customize the views of the organization's security data by developing several enhancement apps. One provides additional real-time views of security systems and the other facilitates investigations into security incidents.

Deeper, faster correlations and investigations

Splunk Enterprise and Splunk ES allow the security team to correlate data faster and more flexibly than a traditional SIEM solution. With analytics-driven security, the team can assess security events holistically rather than from discrete silos, adding context to security investigations. Additionally, Splunk ES dashboards have given the company situational awareness of its security posture at a glance.

"Splunk ES offers far more versatility than the rigid frameworks of legacy SIEM products," says the information security principal. "I have a dashboard showing the number of users entering our network from each of our VPN locations. Achieving such visibility with legacy SIEMs would be time consuming and expensive. Instead, our Splunk platform gives us any views of our PCI controls that we require, enabling a small security team like ours to easily access and evaluate the data."

"No off-the-shelf SIEM solution can anticipate every environment and that's where the magic of the Splunk platform comes in. Splunk software lets us collate logs and data according to our precise needs because it imposes no limitations like rules-based correlations, predefined schemas or syntax normalization. Splunk ES so streamlines correlations with its built-in security intelligence that we don't require a full-time employee to collect data from our security islands and build searches for every incident."

Information Security Principal

Financial services provider

Full operational visibility across the organization

With Splunk, the security team has visibility into all data across the organization, enabling them to rapidly detect and respond to attacks. A perimeter threat dashboard, for example, collects data from RSA security solutions, IPS and IDS technologies and other systems, and allows staff to collate additional data from endpoints, database access logs or web traffic to analyze exploits and incidents. The mapping function in Splunk Enterprise permits them to geo-locate the origins of exploits and malware from abroad and to identify improper communications with foreign sites.

Analysts have enterprise-wide visibility to detect sophisticated hazards like advanced persistent threats (APTs) and conduct forensic investigations. At any time, they can drill deeper into the data for more granularity. Moreover, Splunk ES enables them to assign risk to any event, asset, behavior, or user, allowing them to prioritize security events by their potential impact on the provider's financial services and credit card processing.