splunk>

CASE STUDY

Mitsui Bussan Secure Directions, Inc. Enhances Security Posture With Faster Threat Detection and Analysis

MBSD

Executive summary

Mitsui Bussan Secure Directions, Inc. (MBSD) provides comprehensive security consulting services, including information security diagnosis, monitoring, and IT risk and information disclosure handling, construction support for Private Security Operation Center (P-SOC) and Computer Security Incident Response Team (CSIRT) application management. In order to enhance its security posture and gain full visibility into potential threats, MBSD needed to implement a mechanism for log collection and an overall view of events and threats. Since deploying Splunk Enterprise, MBSD has seen many benefits, including:

- Reduced incident response times
- Faster threat detection and analysis
- Enhanced security posture

Why Splunk

In order to get an overview of its security posture, MBSD needed to collect, search and analyze log data from all of the company's security devices, as well as all IT equipment and applications used throughout its infrastructure. Information gleaned from this data was critical in determining whether a penetration had been made, gauging the extent of the threat and deciding on appropriate response measures. Previously, every server or security device was outsourced to different vendors, with the logs also managed separately. "We needed a single-pane-of-glass solution that could efficiently collect as many logs as possible and then quickly search through them," says Hiroki Saito, deputy general manager of MBSD's managed service division. To provide the appropriate response to targeted cyberattacks, MBSD created a log monitoring system with Splunk software.

Hisahi Gotoh, manager of MBSD's IT security group and consulting division, says, "Our IT experts must deal with a very complicated situation as they sift through huge sets of log data to track the moment-to-moment changes within a customer's IT environment. The Splunk solution answers the highest-level demands of these experts, and makes it easy to visualize the threats found within a vast number of logs."

Industry

- Technology (IT risk management services)

Splunk Use Cases

- Security
- IT operations

Challenges

- Needed to implement a mechanism for log collection and an overall view of events and threats
- Wanted to quickly detect and analyze events and indicators of trouble
- Difficulty in quickly and efficiently identifying the cause and range of effects
- Required a solution that is compatible with SOX compliance and IT auditing

Business Impact

- Incident response time reduced from weeks to hours
- Faster threat detection and analysis
- Increased efficiency of data analysis and reporting
- Enhanced security posture for customer base

Data Sources

- Email log data
- Proxies, firewalls and IDS/IPS
- Anti-virus applications
- File server inspection
- Log data from numerous third-party systems

Splunk Products

- Splunk Enterprise

Protecting customer sites from targeted attacks

At MBSD's Security Operation Center (MBSD-SOC), customer sites are monitored 24 hours a day, 365 days a year; when there are invasions or threats against them, the SOC provides rapid response and counter-measures. According to Mr. Saito, "Typically, in order to gauge the severity of a targeted cyberattack, we conduct a risk assessment of the customer environment by collecting logs from the firewall and all other security devices installed on the Internet boundary, as well as from anti-virus applications and servers storing critical information. Those logs are then gathered, stored, managed and analyzed on an integrated basis and in real time."

This structure means that every day, MBSD collects some 50 gigabytes, or 15,000 separate logs. "The volume we collect in one day in Splunk software is about the same as 100 years of a morning daily newspaper," says Mr. Saito. "From this huge amount of data, we can now easily extract cases of improper access or behavior, all the facts about them and the areas influenced by them. Also, based on characteristics such as the results of risk assessment and the customer environment, we can identify where there have been acts such as spoofing, which can all be carried out automatically using the flexible detection logic rules provided by Splunk Enterprise."

"Prior to the introduction of Splunk Enterprise, coming to a thorough conclusion on virus detection, log collection and determination of causes could take up to four weeks. With Splunk, we can detect viruses and recover the system in just a few hours."

Hisahi Gotoh, Manager, IT Security Group, Consulting Division

Mitsui Bussan Secure Directions, Inc.

"With a conventional log monitoring system, the log formats had to be converted, and dedicated developers had to spend a great deal of time just on initialization. Splunk Enterprise automatically adapts to the log format of different equipment, so that data can be taken in and used as-is. Because the information is immediately available for analysis, the initialization process is much shorter. "

Hiroki Saito, Deputy General Manager, Managed Service Division

Mitsui Bussan Secure Directions, Inc.

Security analysis reduced from weeks to hours

Since deploying Splunk software, MBSD has greatly increased the efficiency of numerous operational processes, saving time and allowing employees to focus on other tasks. Mr. Saito says, "With a conventional log monitoring system, the log formats had to be converted, and dedicated developers had to spend a great deal of time just on initialization. Splunk Enterprise automatically adapts to the log format of different equipment, so that data can be taken in and used as-is. Because the information is immediately available for analysis, the initialization process is much shorter. "

According to Mr. Gotoh, "Prior to the introduction of the Splunk platform, coming to a thorough conclusion on virus detection, log collection and determination of causes could take up to four weeks. With Splunk Enterprise, we can detect viruses and recover the system in just a few hours. Our plan is to further expand the use of Splunk software to include SOX compliance and IT auditing, and create heuristic control."