splunk>

CUSTOMER SNAPSHOT

Splunk® at Mitsui Bussan Secure Directions, Inc.

Faster threat detection and analysis

MBSD

"Prior to the introduction of Splunk, 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
MBSD

OVERVIEW

INDUSTRY
- IT Risk Management Services / Security

SPLUNK USE CASES
- Security
- Monitoring

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

DATA SOURCES
- Email log data
- Proxies
- Anti-virus applications
- IDS/IPS
- File server inspection
- Firewalls
- Log data from numerous third-party systems

WHY SPLUNK
- Agile Reporting, Analytics & Visualization
- Fast Time to Value
- Open, Extensible Platform
- Powerful Search / Reporting Language

The Business

Founded in March, 2001, Mitsui Bussan Secure Directions, Inc. (MBSD), sets out an ambitious corporate policy of "providing customer security as a leading IT risk management company and contributing to building tomorrow's network company." The company provides many different kinds of security consulting, including information security diagnosis and 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, and many other comprehensive security services.

Challenges

In order to get an overview of its security posture, MBSD needed to collect, search and analyze log data from all of its 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.

Enter Splunk

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 center provides rapid response and counter-measures. To provide the appropriate response to targeted cyber attacks, MBSD created a log monitoring system with Splunk software. According to Mr. Saito, "Typically, in order to gauge the severity of a targeted cyber attack, 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," Mr. Saito says. "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."

According to Hisahi Gotoh, Manager of the IT Security Group, Consulting Division, "Prior to the introduction of Splunk, 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. Our plan is to further expand the use of Splunk to include SOX compliance and IT auditing, and create heuristic control."

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.apps.splunk.com

Item # SS-Splunk-Mitsui-101