Hewlett Packard Enterprise

Case Study

招商銀行 CHINA MERCHANTS BANK

China Merchants Bank combats malicious threats

HPE ArcSight intelligent analysis helps bank with vital regulatory compliance

Objective
Make use of log event data to combat malicious IT threats and improve regulatory compliance

Approach
Researched and tested the Security Information and Event Management (SIEM) products of leading vendors

IT Matters
- Carries out correlation between security logs on different platforms
- Collates and filters event information that contains the biggest risks from millions of IT events

Business Matters
- Meets increasingly stringent regulatory requirements by implementing cross-platform log data collection, storage and backup
- Reduces unexpected security incidents by ensuring that warnings are handled appropriately
- Established a security management team to improve detection and response of security incidents

China Merchants Bank wanted to use its data center event logs to flag malicious IT threats and support regulatory compliance. With millions of logs a day, this was a challenging task. The solution was to collect the machine data with HPE ArcSight Logger and then correlate and analyze it with HPE ArcSight ESM security event manager software.

Challenge

Huge amounts of log data
Rapid expansion of financial markets and more stringent regulatory requirements have increased the amount of IT infrastructure and the level of system security that banks need - this was a challenge for China Merchants Bank.

The first joint-stock commercial bank in China to be wholly owned by corporate legal entities, China Merchants Bank is one of the most influential commercial banks in the country. From one branch with 30 employees and a capital of 100 million Yuan, it has grown into a nationwide organization with net capital exceeding 250 billion Yuan, assets of more than 3.4 trillion Yuan, and over 800 branches with 50,000 employees. Established 26 years ago, it now ranks among the world's top 100 banks.

"The main features of Hewlett Packard Enterprise security software are simplicity and effectiveness. All kinds of unusual situations that may be encountered during use are fully considered in the design process, making operation and maintenance much simpler."

– Head of security section, Information Technology Department Operations Centre, China Merchants Bank

The bank's two data centers in Shenzhen and Shanghai house several hundred physical servers, thousands of virtual machines, more than 800 databases and above thousands of security and network devices. They deliver core accounting, credit card production, backup, development and testing with the management getting more complex.

The data center equipment generates millions of log events every day and staff wanted to use this information to detect possible fraud and data leakage. Analyzing the data would also enable them to meet regulatory security requirements in a cost effective manner but tracking millions of log events in various data formats presented a formidable challenge.

To ensure security of critical business systems, analysts needed to quickly filter and identify unusual events. But to achieve this, the initial volume of events had to be reduced to manageable levels.

China Merchants Bank needed to deploy a Security Information and Event Management (SIEM) solution for efficient centralized storage and retention of log events, in addition to intelligent and scalable correlation analysis, and quick identification of security threats.

Solution

Ability to log and analyze

China Merchants Bank examined and tested the SIEM products of several of the industry's top manufacturers, and discovered that HPE ArcSight Enterprise Security Management (ESM) and HPE ArcSight Logger were the best fit for its needs, because the products were simple to operate, easy to maintain and provided a good user experience. The bank also realized that the powerful correlation analysis functions within HPE ArcSight ESM would help to identify genuine security threats from large amounts of data.

The bank's SIEM project was divided into several stages. HPE recommended a complete set of expansion and upgrades, and also actively participated in the implementation of the three stages completed so far.

Together with China Merchants Bank, HPE identified problems, established an internal Security Operations Center (SOC) and trained a rapid response group of security management staff. It also helped to build an IT Infrastructure Library (ITIL) management and automation platform.

HPE ArcSight ESM is a powerful and scalable security monitoring and regulatory compliance solution. It uses advanced algorithms and is capable of collecting and analyzing data from all of China Merchants Bank's hardware devices, systems, applications and databases. It can identify who is on the network, what data they are looking at and how they are using it, helping the real-time identification of network threats.

Through its real-time event management and dynamic forensics features, HPE ArcSight ESM can also trace some warnings back to their source and find the events that triggered them. Once a threat is identified, the program uses its built-in workflow engine to respond to threats and minimize damage caused by data leakage and malicious attacks.

Log management solution HPE ArcSight Logger provides a range of performance options covering equipment, software, virtual machines and cloud computing.

China Merchants Bank can use HPE ArcSight Logger to easily collect, transform and store all the log events and transaction data and integrate it into a common event format. It allows operators to use a text-based search tool to scour through millions of events with a simple interface, then store logs and events in an integrated format using a low cost method with a high compression ratio. Logger can also be used to automatically generate compliance reports, for example, on the validity of all access to display applications.

Case study
China Merchants Bank

Industry
Financial Services

Customer at a glance

Software

- HPE ArcSight Enterprise Security Management (ESM)
- HPE ArcSight Logger

Bi-directional integration can be set up between HPE ArcSight Logger and HPE ArcSight ESM. If an HPE ArcSight ESM user identifies a problem, they can use HPE ArcSight Logger to check how long the problem has existed and which people are specifically involved. It only takes a click of the mouse to search for this through long-term data on HPE ArcSight Logger so there is no need to keep switching the user interface.

Benefit

Efficient threat detection
Through the correlation and analysis of millions of events, HPE ArcSight identifies information that may contain the biggest risks. It alerts security managers to give these risks their immediate attention, significantly reducing unexpected security incidents.

China Merchants Bank has also established a lifecycle management process, ensuring quick response to malicious information. In addition, the bank has developed more than 30 kinds of parser and more than 600 abnormal behavior detection rules. A real-time risk display platform dynamically displays external attacks and internal security threats.

"In the course of implementing the project, we deepened our understanding of information security," says the head of security section, Information Technology Department Operations Centre, China Merchants Bank.

"The bank's internal security team was encouraged to make continuous improvements and master the skills of security operations management. This improved the capacity to detect and respond to security incidents such as abnormal behavior, making security maintenance more efficient."

Other benefits include the simplicity, effectiveness and design of the HPE solutions and their easy maintenance. The implementation process also deepened the bank's understanding of information security.

China Merchants Bank hopes to continue working with HPE to make its data centers more sophisticated and to implement an industry best practice and forward-looking IT infrastructure.

Learn more at
hpe.com/go/arcsight

Sign up for updates

4AA4-9945ENW, July 2016, Rev. 1

Hewlett Packard Enterprise