sumo logic

CASE STUDY

Creating a monitoring environment for cryptocurrency (virtual currency) exchanges and significantly strengthening the IT control for security and financial auditing

bitbank

Challenge

Bitbank operates its cryptocurrency (virtual currency) exchange system on AWS. They used the OSS distributed search and analytics engine for log monitoring, but the inability to perform tasks such as accurate error detection and analysis for the applications resulted in concerns about the IT control for maintaining security and financial auditing.

Solution

Sumo Logic was adopted because of its excellent compatibility with AWS and the flexible resource expansion. High-speed and accurate searches became possible even with large amounts of data. Sumo Logic was adopted not only because of the software's function to automatically structure unstructured data, but because the company has acquired ISMS, SOC2 and PCI DSS compliance certification, thus ensuring the safety of the important information being handled. Full operation was launched after approximately one month of verification in a trial environment.

Results

All the logs can be collected in Sumo Logic, without prior log collection and log transformation on the application side. Logs can be searched and extracted as necessary, security has been further strengthened and the IT control response to financial auditing has been implemented. Efforts are underway to utilize Sumo Logic's authority management function to allow the whole company, including the Development and Marketing departments, to make high-level use of logs.

Log monitoring became a problem due to a lack of security functions

bitbank, which operates the cryptocurrency (virtual currency) exchange "bitbank.cc" is at the top level in Japan for the volume of transactions for virtual currencies*1, including BitCoin, and is also at the top level of transaction volumes for the popular XRP and Monacoin currencies in the world. The company received top results for all of Japan for its security according to third-party research*2.

The company's systems are all configured and operated on AWS (Amazon Web Services), but log monitoring was always a problem.

Mr. Hashimoto, bitbank's security expert, said "In the past, monitoring was imperative work for the IT control to respond to financial audits, and while we used mostly the OSS distributed search/analytics engine for the minimum required level of monitoring, we knew that in order to greatly strengthen the security for our services, it was necessary to broaden the scope of the log monitoring and create a multi-person monitoring system. However, we were worried because we felt that the current OSS distributed search/analytics engine was lacking in both performance and security, and we knew that the monitoring environment needed to be reviewed."

Ms. Yatsu, bitbank's AWS expert, added "We weren't able to fully analyze and utilize the logs. Furthermore, the search/analytics engine system was complicated, and the AWS usage fees were piling up."

Industry

Financial

Headquarters

KDX Nishigotanda Building, 7th Floor, 7-20-9 Nishigotanda, Shinagawa Ward, Tokyo

Size

70

Use cases

Security Intelligence

bitbank, inc.
Risk Management Department
Kenji Hashimoto

bitbank, inc.
Systems Department, Data Team Leader
Yuuma Wakimoto

bitbank, inc.
Systems Infrastructure Team
Kaori Yatsu

There were also problems in the detection of errors in the application logs. “In terms of error detection for the applications, we were only able to detect simple errors with a predetermined pattern. Notifications would be sent to us, but a human would have to determine the details, which was not very efficient.” stated Mr. Wakimoto, bitbank's data analysis expert.

Adopting the highly AWS-compatible Sumo Logic

In June 2019, bitbank took its first step to creating its monitoring environment. They did this through the adoption of Sumo Logic’s SaaS-type SIEM (Security Information and Event Management) solution named “Sumo Logic”.

The fact that this solution was cloud-based, and could decrease the configuration and operation loads were major factors in its selection. Mr. Hashimoto commented, “Among all the advantages Sumo Logic offers, one of the big advantages is that it’s offered on AWS, the same as our own company’s systems, so linking logs is easy and we can increase or decrease resources quickly as needed.”

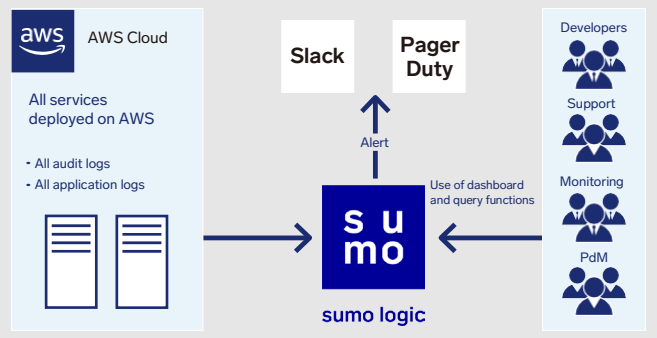
And regarding log data, Mr. Wakimoto noted “We really like the fact that searching is fast, even for large amounts of data. Unstructured data is automatically converted into structured data.” The usage charge system is determined only on the amount of stored data, and the confidence in the security of Sumo Logic as a thanks to the many international accreditations that they had acquired, such as ISMS, SOC2 and PCI DDS, also help boost its adoption.

A trial period of approximately 1 month was implemented after the decision to adopt the solution, and it went into full operation in October of 2019. The trial environment was verified using real data, and it was released as the production environment without major changes.

“We were issued multiple accounts for verification, which meant that we could try out a variety of different things, and it allowed us to carry out the verification very efficiently” (Ms. Yatsu)

Major improvement in log collection and search efficiency, now considering log use across the entire company

Thanks to the adoption of Sumo Logic, bitbank has been able to create a solid monitoring system. “Thanks to Sumo Logic, not only were we able to improve our financial audit and IT control system response, but we were also able to greatly improve our security measures. We're able to perform fast and accurate searches for detailed log audits, and thanks to the intuitive dashboard, we can quickly find the logs we need.” (Mr. Hashimoto)



Ms. Yatsu noted that for operations, “We’re now able to perform high-level log analysis as well. Because we’re no longer using the previous search and analytics engine, system complexity has been resolved, and we’ve been able to reduce the charges we were paying for that.”

Mr. Wakimoto continued, saying that for application error detection, “detection is now possible using complicated patterns, which has resulted in an improvement in our quality of service.” In addition to errors, the job execution time is measured using the logs, which has also allowed for optimization of AWS costs.

"Normally, if there’s a log that we want to collect, it is necessary to incorporate the method for collection during application development. With Sumo Logic, none of that is necessary. All the logs are stored, and it is possible to search the required ones later. The scope of log utilization has expanded, which has resulted in a significant decrease in the burden for development and operations.” Mr Wakimoto said.

In the future, bitbank wants to accelerate the utilization of the new monitoring environment, to implement proactive security measures such as detection of unnaturally frequent login activity or prevention of identity theft before it happens.

They are also considering making log viewing and analysis outside of systems operation managers available so that developers, customer support and marketing staff can also make use of the information in their work. “Because Sumo Logic can assign very detailed settings based on user or log type, it will be possible for the entire company to make use of the logs, while still maintaining security and compliance requirements.” (Mr. Hashimoto)

By actively pushing utilization of logs ahead, bitbank is working to improve service levels and competitiveness even further.

*1 February 20, 2020 CoinMarketCap research
*2 October 3, 2018 ICORating research

About bitbank

Established in 2014. Mainly operates the cryptocurrency (virtual currency) exchange “bitbank.cc”. They handle 6 different types of virtual currency, including BitCoin, offering the industry’s smallest spread (the difference between buying price and selling price), and an app that took the top spot in the Japanese app store. bitbank continues to receive support from a large number of users.

About Sumo Logic

Sumo Logic Inc., (NSDQ: SUMO) is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,100 customers around the world rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy. For more information, visit www.sumologic.com.

sumo logic

Sumo Logic Japan KK
Email: info-jp@sumologic.com

sumologic.jp