"We were very impressed by how simple and easy Sumo Logic's user interface was to understand compared to its competitors' solutions. This has meant that we can use it more intuitively and take advantage of its functionality more quickly."

Keita Kiyatake
Cyber Security Analyst

Coincheck

Coincheck banks on Sumo Logic to gather and scrutinize machine data to thwart security breaches.

Challenge

After being the victim of one of the worst cyberattacks in history, fast-growing Coincheck took the extraordinary step of halting much of its operations and then completely redesigning its entire customer-facing application portfolio. From the beginning of this remarkable transformation, the company also sought strategies to utilize its machine data collection to assist in its efforts to impede such an attack from ever occurring again.

Solution

Coincheck evaluated its options and quickly chose Sumo Logic's cloud native machine data management solution. The company soon began ingesting large volumes of log files from across its newly-revamped applications and infrastructure and with this raw data now assembled in one place, Coincheck was able to apply an extensive set of queries to start providing timely alerts.

Results

Sumo Logic promptly revolutionized Coincheck's relationship with its machine data. Continually examining this vital information has slashed the amount of time necessary to identify and stymie potential attacks. The upshot is that Coincheck now has vastly improved security capabilities and has set the stage for many other opportunities to derive meaning from this previously untapped information.

The History

Coincheck was established in August 2012 and launched its Crypto-Currency exchange in 2014. The company provides the Coincheck virtual currency wallet and exchange service, which supports nine virtual currencies, including NEM and Ripple as well as Bitcoin. Customers utilize iOS and Android apps to carry out their trading activities. Coincheck became a fully owned subsidiary of the Monex Group in April 2018 and was licensed as a virtual currency exchange provider in January 2019. Its other services include Coincheck Denki and the Coincheck lending virtual currency lending service. The company's entire application portfolio is developed and hosted on Amazon Web Services (AWS).

Industry

Financial services

Headquarters

Tokyo, Japan

Size

168 employees

Use cases

Security

"A major attraction was that using a SaaS solution made it quick to implement. At the time, it was vital for us to rebuild our monitoring system as soon as possible. The depth of Sumo Logic's support and the wealth of documentation really helped us to implement it quickly."

Hideaki Oura
Head of Cyber Security

In late 2017, Coincheck experienced tremendous growth in its virtual currency business, and accordingly upgraded its performance and monitoring capabilities. Unfortunately, the company didn't apply the same level of enhancements to its protective competencies quickly enough. This shortfall became painfully apparent in January 2018, when an unprecedented security breach resulted in the loss of $530 million in NEM virtual currency tokens. In response to this catastrophic event, Coincheck suspended part of its services and made improvements to its management and internal controls. It also took the extraordinary step of redesigning its entire customer-facing application portfolio, as well as its internal network and other assets. As part of this initiative, the company also created a dedicated security team to help prevent future incursions.

The Details

Coincheck's redesign team recognized that augmenting how it monitored its extensive log inventory could be a major ingredient in strengthening its overall security stance. The aim was to proactively avoid security abuses by centralizing machine data management for cloud servers, network security devices, and terminals. When unauthorized access episodes did occur, superior log monitoring would mean that the company would be in a much better position to detect them and apply the appropriate response. This not only ensured a high level of security, but also improved compliance and governance.

Having already suffered a devastating theft, time was of the essence for the company to inaugurate a Software as a Service (SaaS) security information and event management (SIEM) solution. Coincheck examined leading products such as Sumo Logic and Splunk. The evaluation team rapidly selected Sumo Logic for a variety of compelling reasons:

- Born-in-the-cloud product architecture
- Intuitive user interface
- Rich Web app collection
- Depth of support — both before and after the appraisal
- Comprehensive, high quality documentation
- Speed of implementation

Coincheck quickly launched its Sumo Logic instance by aggregating machine data from all corners of its freshly-overhauled technology collection, regardless of the source information's format (e.g. CSV, JSON, or XML). Concurrently, the security team devised a system to anticipate a range of scenarios and generate alerts whenever it detected incidents that could point to a security violation.

The company also employed sophisticated analytics by leveraging the greater than 150 monitoring templates included with Sumo Logic. These were powered by a substantial set of queries that were able to simultaneously interrogate multiple data sources rather than mandating more time-consuming sequential processing. Query performance was also boosted by Sumo Logic's field extraction functionality. Examples of these queries include:

- Identifying unauthorized secure shell (SSH) connections
- Applying integrated threat intelligence using geography and other flexible criteria
- Detecting malicious message transmission
- Matching network logs

Coincheck also configured an adaptable workflow based on the severity of the detected event: normal alerts are routed to Slack; high priority bulletins are automatically routed to on-call staff telephones via PagerDuty.

> **"We were able to start monitoring straight away, just by selecting the templates and logs to suit our requirements and our system. We also had no problem creating queries because Sumo Logic provided plenty of guidance, including how to write them."**
>
> **Yuki Nakai**
> Cyber Security Analyst

Going forward, as an organization that has suffered one of the largest attacks in history Coincheck aspires to become the most secure crypto currency and blockchain enterprises in the world by providing safe, yet easy-to-use applications. To help in these efforts, the company plans to expand its Sumo Logic utilization in a number of strategic ways:

- Enhancing dashboard adoption. Most of Coincheck's daily interactions with its machine data have not yet taken advantage of Sumo Logic's rich dashboard array.
- Expanding business intelligence and analytics. Coincheck is looking at Sumo Logic to become the default data analytics platform for multiple purposes, such as business management, marketing reviews, performance monitoring, and security.
- Trend analysis. Exploiting machine data can help uncover positive trends by evaluating internal activities — such as enabling more accurate code reviews.
- Machine learning and predictive analytics. As one example, Coincheck will leverage Sumo Logic's threat intelligence capabilities to help conduct its work in Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) activities.

"Sumo Logic provides a lot of functionality that we have not yet taken advantage of. By utilizing it as our platform for monitoring and analysis, we hope to make our security more robust, and also to help improve our services and systems." Hideaki Oura, Head of Cyber Security

Sumo Logic has become an indispensable tool for conducting cyber monitoring, thereby fulfilling Coincheck's original log aggregation mission. The company's user community continues to gain expertise in the product, which will help uncover even more opportunities to extract value.

About Coincheck

Coincheck operates virtual currency exchange Coincheck and Bitcoin payment service Coincheck payment. Based on the concept of "paying more conveniently and comfortably", we provide a service that allows anyone to easily trade and pay for virtual currency from a smartphone or PC. We aim to make people around the world more affluent and happier with new technology, and expand our business not only in Japan but also overseas, aiming to become an infrastructure that can be replaced by the Internet. For more information, visit www.coincheck.com.

About Sumo Logic

Sumo Logic is a leader in continuous intelligence, a new category of software, which enables organizations of all sizes 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 2,000 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.

Founded in 2010, Sumo Logic is a privately held company based in Redwood City, California, and is backed by Accel Partners, Battery Ventures, DFJ Growth, Franklin Templeton, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital, Sutter Hill Ventures, and Tiger Global Management. For more information, visit www.sumologic.com.

sumo logic

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com