Bitkub Exchange frees up 20% of staff time by selecting Devo to modernize their SOC

CASE STUDY

Devo's cloud-native platform and advanced security analytics enable Bitkub Exchange to make faster decisions and proactively defend their data.

SUMMARY

Bitkub Exchange is a Thailand-based new generation digital asset and cryptocurrency exchange company. Bitkub Exchange offers advanced cryptocurrency exchange services to individuals who intend to buy, sell, and store cryptocurrencies. After three years of massive growth and achieving a unicorn valuation in 2021, the Bitkub Exchange security operations team started looking for a SIEM solution that could scale with their massive growth and keep their organization secure in an increasingly vulnerable cryptocurrency industry. Following the evaluation of several solutions on the market, Bitkub Exchange chose Devo because of its unique ability to optimize the analyst workflow and free up their analyst's time to work on other tasks such as threat hunting, investigation and proactive defense.

THE CHALLENGE

Bitkub Exchange did not previously have a SIEM solution in place. The cryptocurrency company was growing very quickly, but still operating using manual processes as a security team. This was not only extremely time consuming, but also left them in a less secure state, unable to gain full visibility into their data landscape.

INDUSTRY

- Technology

ENVIRONMENT

- Thailand-based company founded in 2018
- Thailand's second unicorn
- 500+ employees

SECURITY CHALLENGES

- Upward trend of cyber criminals targeting digital exchange platforms
- Lacked predefined use cases to automate and advance their threat detection
- Needed a cloud based solution that was able to expand with their increasing company growth

SOLUTION

- The Devo Platform with Devo Security Operations application

KEY BENEFITS

- Enhances threat detection with real-time monitoring
- Seamless alert integration with Bitkub Exchange environment
- Pre-built use cases and alert management with Devo Security Operations

20%
of staff time freed up

50%
reduction in staff time spent implementing manual use case

<2
months to see ROI

5X
faster implementation than anticipated

<2
weeks to master the Devo Platform

At the same time, the cryptocurrency landscape was changing and becoming increasingly targeted by cybercriminals. The industry was seeing increased levels of targeted hacks on digital exchange platforms. This new reality, paired with their reliance on manual work created a compound effect that heightened the need for a SIEM solution.

They wanted a modern SIEM application that included pre-built use cases and out-of-the-box content to decrease the need for manual use case creation and manual threat detection. Specifically, they needed a platform that was capable of successful IOC matching, with built-in threat intelligence, that could easily help them detect and remediate threats. Bitkub Exchange's team also expressed interest in SOAR capabilities in order to automate incident response.

> *"Devo's cloud-native model saved us a lot of time. We had originally projected that getting up and running with the platform would take us 5 times longer than it actually did. Being in an environment where scammers were becoming an increasing issue, we needed this fast implementation in order to respond to the threat before it grew. I don't think we would have been able to do this without Devo's cloud based model."*
>
> ***- Attaphon Phayak***
> ***CSO, Bitkub Exchange***

THE SOLUTION

To search for a SIEM, the Bitkub Exchange team began assessing Devo, Splunk, QRadar and Sumo Logic. Ultimately, Bitkub Exchange chose Devo as its SIEM platform because it provided them with a scalable cloud-native solution that could provide them with advanced analytics and detections to optimize the analyst workflow, save the team time, and keep Bitkub Exchange secure as they continued to grow.

Selecting a cloud-native solution aligned best with Bitkub Exchange's business model. As a cloud-first organization, implementing a cloud- based SIEM enabled the team to get ramped up quickly and see value within weeks. Bitkub Exchange also selected Devo for its ease of use, which helped their team easily master the platform without having to do any additional hiring.

Since manual use case implementation was a large time consuming issue for the client, they were drawn in by Devo Security Operations, which gave them access to predefined use cases and out-of-the-box alerts and visualizations in the Exchange. With access to immediately installable content, Bitkub Exchange's team is now able to free up significant time, increasing overall security productivity and improving time to value. Bitkub Exchange's security analysts are now able to spend less time on repetitive tasks such as manually configuring use cases, and instead focus their time on hunting, investigating and responding to the most pressing threats.

Devo provided pre-made use cases to directly address their needs, covering CASB, cloud security, and IDM technology. They also realized a boost in efficiency in using their log data during security investigations. The Devo Platform provided intuitive alert management and the Devo Exchange, the included application and content marketplace.

THE RESULT

Bitkub Exchange's team was able to get up and running with the Devo Platform within just **2 weeks**. Bitkub Exchange was also able to complete their onboarding process and begin seeing ROI in **under 2 months**. Their team explained that they were able to complete implementation **5 times faster** than their internal project scope projected.

Additionally, with the Devo Platform, Bitkub Exchange has been able to **free up 20% of their staff's time**, and focus on identifying and remediating threats sooner and faster. Bitkub Exchange's CSO, explained:

> *We have been able to drastically improve our threat detection and real-time monitoring by working with Devo. The platform helps us reduce staff time that was being used to manually build each use case. Now our team has much more time to allocate towards other tasks, such as alert triage and investigation. This is huge for us given the increased levels of cyber attacks that we are seeing in the industry.*
>
> ***- Attaphon Phayak***
> ***CSO, Bitkub Exchange***

The Bitkub Exchange team has been able to drastically reduce the amount of time they were spending on manual use case implementation. They now spend **50% less time** implementing manual case cases.

Using Devo has made Bitkub Exchange's SOC more efficient, specifically based on the search tools, alert management, Devo Exchange content, and predefined use cases that the platform offers. As a result of migrating to Devo, Bitkub Exchange was able to quickly adopt a new solution and see value immediately upon implementation.

WHAT'S NEXT

Bitkub Exchange plans to expand their use of the Devo Platform going forward, increasing their levels of data ingestion for improved visibility and working to automate more routine work, aligning with Devo's vision of the autonomous SOC. Their team is also excited about Devo SOAR to implement impactful automation and response capabilities.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.