securonix | coinhako

CASE STUDY

Coinhako Improves its Security Posture by Moving SIEM In-House

securonix

coinhako

CASE STUDY

Coinhako Improves its Security Posture by Moving SIEM In-House

Key Challenges

- Build a modern security operations organization and implement a proper SIEM that provides optimal visibility, analytics, and response to meet the demand of a dynamic threat landscape.
- Improve the business's overall security posture using signature and anomaly-based threat detection; advance analytics with incident association for more accurate risk scoring; and streamline and automate threat remediation.
- Partner with a SIEM vendor specializing in correlating data from multiple cloud-based data sources and creating custom policies leveraging existing applications to shepherd the transition from MDR to in-house operations while meeting strict deadlines.

Challenge: Moving from a MDR for More Visibility and Control

Coinhako, an Asia-based provider of an easy-to-use cryptocurrency buying platform, needed more direct visibility and control to keep up with an ever-changing and dynamic threat landscape. Previously, Coinhako relied on a managed detection and response (MDR) solution to support its threat detection, investigation, and remediation (TDIR) needs. As Coinhako grew to serve more customers and handle more transactions, they strategically decided to support their TDIR activities in-house with a dedicated security operations team and solutions to address business-impacting threats. The cornerstone of this new security operation would be a modern SIEM. They needed a SIEM solution that could quickly identify anomalies, provide the proper analysis to understand the problem, and define a targeted remediation plan to quickly mitigate any potential threat.

Coinhako quickly realized that a cloud-native SIEM would be optimal to provide the scalability and speed needed to meet their needs. Coinhako's acceptance criteria extended beyond the solution being cloud-based. They did not want to toggle between multiple disparate user interfaces, so the solution needed to provide a unified experience throughout the entire TDIR workflow. It was also critical that the solution supplements the security team's activities through streamlined workflows and automation. Because the team was newly formed, they were focused on learning the environment and building processes, and it didn't make sense to add cumbersome, manual solutions into the mix. Coinhako did not only focus on the solution's capabilities but also on the type of partner the vendor would be in ensuring that the move from the MDR to in-house was smooth and met stringent timelines. At the end of the evaluation, they chose Securonix.

Not Just Deploying a SIEM Solution, Building a Partnership.

When Coinhako decided to move from the managed service to bringing a SIEM solution in-house, they extensively evaluated six highly regarded SIEM vendors. Securonix rose to the top of the list for several reasons:

1. Securonix collects data from on-premises and cloud-based sources, correlating and consolidating them into a single data set. Now, Coinhako has extensive visibility into the cloud assets within its environment.
2. Securonix delivers out-of-the-box behavioral analytics, detection threat models, and content. Securonix also provides the ability to develop custom detection rules that incorporates Coinhako's applications and data sources. Securonix continuously develops and makes available new threat content based on research done by the Threat Labs team that can be implemented in a few clicks. Coinhako can keep its solution up to date easily without overburdening its security analysts or system administrators for its top use cases and newly circulating threats.
3. Securonix automates the process of associating seemingly unrelated events into combined alerts. Coinhako security operation's team can understand the relationships between seemingly inconsequential alerts that were in fact significant issues.
4. Securonix delivers a streamlined workflow that can help Coinhako's security analysts go from detecting an incident, gathering the details about the incident and entities involved to understand the incident, to developing a precise and targeted remediation plan to mitigate the threat.

Not only did Securonix demonstrate the technical capabilities needed to meet the ever-changing threat landscape, Coinhako realized that Securonix's support and service set them apart from the pack. From the onset, Securonix worked with Coinhako to provide expertise and guidance to propose a solution that would meet their needs and deliver the support to implement the system effectively.

Coinhako's partnership with Securonix helped streamline the transition from relying on a service-based SIEM capability to now having the ability to detect threats, investigate them, and respond within their own security operations environment.

> "[Securonix] took the time to understand our needs and requirements and worked closely with us to ensure that the system was configured to meet our unique security challenges."
>
> – Pasi Koistinen, Chief Information and Security Officer (CISO) of Coinhako

Establishing the Foundation that Improves Security Posture Today and Tomorrow.

As Coinhako's business continues to grow to support more customers and transactions, having a dedicated team of security professionals at the helm is mission-critical to protect those customers and transactions. For security professionals to be effective, they need the right tools and partnerships to support them. Being able to consolidate a multitude of data sources together established the foundation within the Securonix SIEM these security experts depend on. With Securonix as the foundation, Coinhako's security operation team can quickly draw meaningful correlations between events and get highly dependable alerts based on risk scores to properly prioritize their activities and be as efficient as possible. More important than efficiency is that this automated ranking of threats allows Coinhako's security analysts to focus on threats with the highest potential of data exfiltration, ransomware, and impact on their reputation. And lastly, Securonix has been a partner every step of the way working with Coinhako to ensure timelines are met and that the solution is customized for their needs and environment.

Even as a new implementation, the security team and leadership already feel better positioned to protect Coinhako's data and reputation with improved threat detection and response capabilities. Koistinen shares, "Although it is still early to ascertain the exact business value of implementing the Securonix solution, we believe that over time we will be able to see returns on our engagement with Securonix."

About Coinhako

Founded in 2014 by Singapore entrepreneurs, Coinhako was created with a simple value proposition – to create a simple and hassle-free way to access Bitcoin. Over the years, they have expanded to provide access to a wide variety of digital assets, as they work towards their vision of enabling access to the crypto-economy across Asia and beyond.

For more information visit coinhako.com

About Securonix

Securonix is leading the evolution of SIEM for today's hybrid cloud, data-driven enterprises. Securonix Unified Defense SIEM provides organizations with the first and only content-driven threat detection, investigation, and response (TDIR) solution built with a highly scalable data cloud and a unified experience from the analyst to the CISO. The innovative cloud-native solution enables organizations to scale up their security operations and keep up with evolving threats.

For more information visit securonix.com