MITIGA

Case Study

Cloud-native Financial Services Organization

The challenge: Cloud-native financial services and prioritizing security

A fully cloud-native financial organization, with solutions deployed via cloud services, has innovative technology and a strong commitment to customers. Ensuring that their services and customer data are secure is a priority for the organization.

At the same time, the security team is small and there are no internal incident response (IR) capabilities. The Chief Information Security Officer recognized that the team lacked both the ability to thoroughly investigate breaches and a good methodology to recover quickly and effectively from a critical incident.

While searching for an IR provider to bring on board via a retainer, after considerable research they did not feel that the vendors they spoke to were fit for purpose or understood the unique cloud and security requirements well enough.

" We needed an IR partner who understood our unique cloud and security requirements. "

-CISO, Financial Services Organization

The solution: Mitiga IR² subscription

Once this financial organization learned about Mitiga's readiness-first approach to IR, they quickly became an IR² subscriber and began the on-boarding process, which included understanding and mapping their environments. By identifying the assets that were most critical to the organization's ability to accomplish their mission, Mitiga ensured that the right forensic data was being collected and analyzed, available for rapid investigation in case of a critical incident.

The next phase was to connect Mitiga's adaptors to their environment and start ingesting their forensics data to make sure that the IR² platform contained a complete picture of all the required data, such as logs, configuration snap shots, and so on. After several days of digesting, analyzing, and storing the data, there was enough data to consider drills and exercises.

To ensure readiness for potential incident requires a more holistic approach than forensic data collection alone, however. The dedicated Mitiga IR squad, incident commander, and consulting team also worked closely with their security team to build a relationship ahead of any potential breach. To increase internal understanding of the potential impacts of a breach and the roles different members of the internal team would play during an attack, Mitiga consultants completed a tabletop exercise with the management team.

The squad also coordinated a drill with the customer, to increase trust and improve the ability to partner effectively with the internal security team on performing breach response end to end. Mitiga also conducted a blue team exercise to help the customer get detailed security recommendations and gain a detailed understanding of their potential cloud security gaps, tailored to their toolset and environment.

The results: Increased readiness, customer peace of mind

Today, Mitiga collects, structures, and analyses the customer‘s logs in the IR^2 platform at 24-hour intervals and security configuration snap shots are collected on a 7-day interval. The internal security team feels secure in their partnership with the Mitiga team and ability to work closely together if a critical incident occurs.

The combination of drills and exercises to increase readiness, a skilled and experienced team squad of incident responders and researchers, and platform designed to ingest, normalize, and analyze forensic cloud data helped this financial service provider rest more easily, knowing that they have the information, resources, and technology to respond rapidly if a breach occurs.

Mitiga’s technology and services provide continuous, proactive breach investigation, lower the impact of cyber breaches, and optimize readiness for cloud and hybrid incidents. This readiness-first approach accelerates response and recovery time, increasing resilience when incidents occur. Mitiga’s shared-responsibility model is unique. Unlike others, who charge additional fees for incident response and recovery, Mitiga subscribers face no add-on fees.

For more information, visit www.mitiga.io or email us at info@mitiga.io

MITIGA