CASE STUDY

International Financial Services Group

Changing the way Africa uses eCommerce

Business Objective

A financial services group in South Africa wants to embrace digital transformation in a continent where the use of credit is much less common than in the U.S. Leveraging their digital wallet functionality, their goal is to facilitate eCommerce across Africa. Their vision is to provide a 'do-everything' eCommerce platform that covers anything from buying and selling goods, to service payments, delivery fees, and everything in between.

Problem

In order to accomplish their business imperative, the bank needs to scale the application in an enterprise-ready environment, with world-class security, and competitive performance. As step one, the bank needed a comprehensive DevSecOps assessment to identify existing security issues, and assess software development and IT operations for functionality, performance, and usability. The bank partnered with 2nd Watch to see how the app performed compared to our other global partners in the finance industry.

Solution

2nd Watch security experts completed a full assessment of the bank's mobile app to identify gaps and potential risks, as well as suggest remediations. Our DevOps team also completed an assessment, interviewing a variety of the bank's development employees, assessing knowledge management, the actual code, architecture, and capabilities. The app was measured against DevSecOps best practices, and the bank was presented with the findings. 2nd Watch continues to serve as a cloud security advisor, helping the bank safely move toward their business goals.

2nd Watch security experts completed a full assessment of the bank's mobile app to identify gaps and potential risks, as well as suggest remediations.

About the Business

This financial services group is located in South Africa and offers wholesale and retail banking services, insurance, and asset and wealth management.

The Business Challenges

Without internal resources and experience, the financial services group sought advanced and experienced cloud advisors to help in three specific areas – scaling the application, deploying a reliable application, and ensuring security. Unfortunately, the bank had exhausted the capabilities of South African technology consultants, but hadn't yet met their goals around functionality, security, and performance. They contacted 2nd Watch based on our cloud services experience with worldwide, recognized brands. We started our partnership with an initial DevSecOps assessment to understand their current structure and create a plan for moving toward optimization.

During the security side of the assessment, 2nd Watch pinpointed cybersecurity issues putting application data at risk. Data loss via accidental and malicious deletion, ransomware, and other malware attacks threatened user data, application reliability, and the bank's reputation. Issues included, unrestricted administrative privileges, lack of security incident detection and controls, incident response, and a largely handcrafted, bespoke environment.

The DevOps side of the assessment revealed an attempt at agile implementation, although the bank's practices were not living up to the approach. Development was outsourced between two different companies, and many of the processes, tools, and architectural foundation needed to be modernized. Onboarding was cited by the bank as another insufficient process, and they sought advisement on endpoint protection, multi-factor authentication, and unified access to systems.

The financial services group sought advanced and experienced cloud advisors to help in three specific areas:

1. Scaling the application
2. Deploying a reliable application
3. Ensuring security

The 2nd Watch Solution

2nd Watch DevOps and security teams converged for a DevSecOps evaluation of the application. After identifying challenges within the bank, 2nd Watch recommended a variety of solutions to improve the application. We provided our findings in a detailed document and presented them to two different audiences at the bank. Remediations include:

- Modernize development processing and tools
- Implement peer review
- Utilize automated tests
- Update architecture and distributed system designs

The Business Benefits

Since the DevSecOps assessment was completed and findings were presented to group leaders, 2nd Watch has helped the bank take next steps. Starting with tightening access to their public IP server, Bastion. We saw that the bank's process was to allow anyone in the organization to logon to Bastion – which is not advised, but not uncommon. An instance profile was then attached to Bastion so anybody logged in was automatically an administrator and had an unprotected public IP. Based on 2nd Watch suggestions, the bank removed the instance profiles from Bastion, thereby limiting administrative privileges and securing access.

Equipped with a list of necessities, remediations, best practices, and cloud experts, the financial services group knows what their foundation needs to look like in order to achieve scale and security.

We also delivered security remediation steps to implement incident protection. Rather than relying on unusually high billing statements to sound the alarm, 2nd Watch suggested creating an incident response plan. Should a cybersecurity event occur, we want the financial services group to be able to detect, alert, communicate, recover, and restore quickly and with minimal downtime and data loss. Environment automation, identity management, and established tools were also recommended to the financial services group to expand application safely.

Currently, 2nd Watch continues to serve in a cloud advisory role on a weekly basis. Most recently, we're working with the bank to turn on RDS, or Aurora authentication, using role-based authentication. This way, when employees sign on, they can assume a role and the database access assigned to that role – instead of everybody having a second set of permissions.

Equipped with a list of necessities, remediations, best practices, and cloud experts, the financial services group knows what their foundation needs to look like in order to achieve scale and security.