GenAI Augmented Security Issues and Misconfiguration Monitoring and Advisory Platform

Executive Summary

As a worldwide-known global security provider, our client handles multiple services under one roof. This unique organization perceives cloud security solutions as the key to building the digital communities of the future. However, it is impossible to achieve this crucial goal without a stable technology foundation. Therefore, the Matoffo team developed a robust GenAI-powered security and misconfiguration monitoring platform that enables the client to automate manual business processes and achieve maximum efficiency while saving costs.

About the Customer

Specializing in identifying and eliminating security risks and misconfigurations across cloud infrastructures, our client serves as a globally recognized cloud security provider trusted by multiple companies from diversified industry verticals. While the holistic approach is one of their fundamental business values, their team aims to improve resilience by leveraging automation to manage security gaps efficiently, prioritizing remediation efforts based on business risks and operational impact. Summing up, the company delivers state-of-the-art security services with an emphasis on detecting and consolidating vulnerabilities in a quick and efficient manner.

Customer Challenge

When it comes to detecting misconfigurations, security policy gaps, and vulnerabilities across cloud infrastructures, it is nearly impossible to avoid challenges related to prioritization, automation, and scalability. Hence, our client is no exception. Managing and analyzing large amounts of logs and configuration files from various cloud services, their team required an efficient solution to handle high volumes of logs and data.

At the same time, ensuring compliance across multiple cloud environments (AWS, Azure, GCP) with differing policies was also pivotal. Struggling with a lack of automation, our client

experienced issues with the speed of critical misconfiguration identification. Besides, a wide array of manual processes caused the inability to scale manual remediation efforts in a growing infrastructure. Finally, it is essential to mention the challenges associated with assessing and prioritizing risks based on potential business impact.

Why AWS

There is no better choice than AWS, especially when it comes to Gen-AI and LLM solutions. Equipped with a vast selection of cloud-native tools that seamlessly integrate with the multi-cloud architecture, AWS is a perfect option for building secure and scalable solutions that bring maximum value from the long-term perspective. For instance, AWS services like CloudWatch can be a great match for log ingestion, while S3 is a great choice for centralized data storage and Bedrock for LLM integration.

Why Matoffo

It is always a pleasure to work with companies from a similar industry. Hence, Matoffo, a recognized leader in delivering cutting-edge cloud solutions and implementing innovative technology like AI and ML, is a perfect match for a company specializing in developing cloud security solutions. Backed by years of experience in identifying and eliminating security risks and misconfigurations across cloud infrastructures, our team came up with a promising project concept that met and exceeded the client's expectations.

Matoffo Solution

Since automated analysis of misconfigurations, logs, and cloud security policies was our key project objective, the solution architecture included several crucial phases:

- Data Ingestion:
  - AWS CloudWatch for log ingestion;
  - AWS Config for policy and configuration data.
- AI and Machine Learning:
  - EKS-hosted AI models for recommender systems and LLM orchestration;
  - AWS Bedrock for LLM integration and advanced natural language processing.
- Data Storage and Processing:
  - S3 for centralized data storage;

RDS for metadata storage;

DynamoDB for session history and feedback.

Security Scanning and Analysis:

Prowler on EKS for cloud security scanning (CloudScanner);

Custom Python-based analysis tools.

User Interface and Visualization:

React-based UI for the Control Center Portal;

Cloud-specific monitoring dashboards for each cloud provider.

Business Value

Finally, we have reached the point when it is time to reap the benefits. Read on to explore the business value we brought to a global security solutions provider:

Saving Time

Thanks to automated log analysis and prioritization, we reduced mean time to remediation (MTTR) by 82%. Now, the system can analyze over 10,000 logs per hour.

100% Compliance

Our solution enables early detection of non-compliance issues, significantly reducing the number of incidents by 35% within the first six months.

Next-Gen Security

Our skilled engineers identified and eliminated 12 severe security vulnerabilities within the first three days of implementation, improving overall security resilience.

Maximum Productivity

While we enhanced overall operational efficiency by 5x, security teams can now focus on critical tasks rather than manual log reviews.

Scaling without Risks

Our team scaled the solution to handle increasing log volumes and additional cloud environments without considerable infrastructure changes.

Cost Efficiency

There is no need to hire large security teams and manually review logs and configurations.

Client's Feedback

Overall, the client is completely satisfied with the outcome. The Matoffo team not only managed to deliver a solution that solved the client's challenges but also met their time and budget requirements. Over and above that, we ensure ongoing support and maintenance of GenAI-powered security and misconfiguration monitoring platform. Finally, we want to continue this fruitful cooperation and develop exciting projects for this incredible global security provider in the future.