CASE STUDY

SQUARESHIFT

SOC2 Compliant SIEM powered by Elastic Security for Asia's leading bill payments and collection platform to proactively secure IT infrastructure.

SOC2
Compliance

3
Regions

24x7
Monitoring

CLIENT

The client is a leading bill payments & cashflow management platform based out of Singapore.

The client also offers no-code platform for businesses to automate bill collection & bill payment processes.

TECHNOLOGY STACK

elasticsearch
Kibana
HashiCorp Terraform
Amazon RDS
Amazon CloudWatch
Amazon CloudTrail

PROJECT CONTEXT

The client needed a solution to monitor multi-cloud infrastructure and Security Information and Event Management (SIEM) solution. The solution should meet SOC2 compliance and guidelines.

The client needed a expert technology partner to discover and implement the solution that meets the requirements.

PROJECT REQUIREMENTS

- An unified platform for 24x7 monitoring of the system for High Availability, Performance and Infrastructure monitoring.
- A solution to debug production issues on multiple applications & databases
- A solution to proactively monitor and secure infrastructure.
- Economically viable solution to securely manage cloud native services & endpoints.
- The platform should meet SOC2 compliance standards.

SOLUTION DELIVERY

- Implemented Elastic Security to meet SIEM requirements.
- Developed Terraform script to provision AWS infra and automate creation of golden Images with embedded elastic agents.
- Configured threat detection and end point security with Elastic.
- Setup threat detection alerts and configured ML based anomaly detection.
- Built customised IT Ops/ performance dashboards for clients' GSOC, GNOC and Production support teams.