CASE STUDY

SQUARESHIFT

Deploying a production, air-gapped observability platform for critical compliance and visibility.

12TB
Dedicated Storage

1 Year
Compliance Retention

100%
Secured Infrastructure

CLIENT

The client is operating in the Critical Infrastructure industry needs deployment of a production, air-gapped observability platform for critical compliance and visibility of their systems.

GEO: A Premier South- East Asian Government

Logistics & Transportation Industry

TECHNOLOGY STACK

elasticsearch

APACHE HTTP SERVER PROJECT

logstash

podman

KIBANA

Red Hat

PROJECT CONTEXT

- The primary project goal was to deploy a production-grade, fully air-gapped Elastic Stack for comprehensive observability.
- Built on six powerful data nodes to handle high volume, meet the one-year minimum log data retention rule, and was supported by a dedicated monitoring cluster.
- Implemented the Elastic Stack version 9.0.1

PROJECT OBJECTIVES

- Deploy a highly available, multi-node production Elastic cluster.
- Establish a separate monitoring cluster for the main stack's health.
- Configure a complete air-gapped ecosystem with local registries (EAR/EPR).
- Ingest diverse data (OpenShift, VMs, Cisco, Fortinet).

SOLUTION DELIVERY

- Installed and configured all components (Elasticsearch, Kibana, Logstash, Fleet Server).
- Established local, air-gapped repositories (EPR/EAR) for internal distribution.
- Implemented client-issued CA-signed SSL/TLS certificates for all communication.
- Integrated the production cluster with LDAPs for centralized authentication and RBAC.
- Onboarded data sources via Elastic Agents (OpenShift, Linux, Windows) and Logstash pipelines (Cisco, Fortinet syslog).
- Enabled Centralized Pipeline Management for Logstash.