CASE STUDY

SQUARESHIFT

A global cloud security leader streamlined log ingestion and automated Elasticsearch clusters, enhancing scalability and operational efficiency .

5x
Faster Log Ingestion

80%
Automation Efficiency

99%
Data Backup Reliability

CLIENT

A global leader in cloud security, specializing in network protection, secure access, and cloud-based solutions for enterprises.

GEO: San Jose, California

Networking & Security

TECHNOLOGY STACK

elasticsearch

Amazon S3

elastic apm

Kibana

Python

ANSIBLE

PROJECT CONTEXT

- The client required a scalable solution to ingest security logs into Elasticsearch with ECS compliance.
- Automation was essential to streamline multi-node cluster deployment and reduce manual effort.
- The project focused on secure log ingestion, optimized processing, and robust backup strategies.

PROJECT OBJECTIVES

- Integrate ZIA & Okta logs into Elasticsearch with ECS compliance.
- Automate multi-node Elasticsearch cluster deployment with Ansible.
- Implement a secure and efficient log ingestion pipeline with robust back strategies to ensure data retention and redundancy.

SOLUTION DELIVERY

- Fleet Setup with CA Certificates – Secured log ingestion and authentication using CA certificates in Fleet.
- ZIA Log Integration with ECS Mapping – Integrated ZIA logs with ECS mapping using NSS feed and custom S3-based ingestion.
- Amazon Security Lake Evaluation – Evaluated Security Lake for storage but retained Elasticsearch for log analysis.
- Okta Logs Integration – Created a guide for Okta log ingestion with ECS-compliant Elasticsearch pipelines.
- Elasticsearch Cluster Automation – Automated multi-node Elasticsearch setup with Ansible, including SSL certificates and authentication.