CASE STUDY

SQUARESHIFT

Custom integrations to ingest from all the sources for end-to-end monitoring with Elastic for a 120 year old leading department store chain

CLIENT

The client is a 120 year old leading department store chain in the USA.

The clients website is one of the top visited e-commerce websites with close to 50 million visits every month.

TECHNOLOGY STACK

PROJECT CONTEXT

The client had deployed Elasticsearch for centralised log management and monitoring. It collected logs and metrics from several heterogeneous sources.

However the existing setup was limited to out of the box integrations from Elastic. Thus leading to lack of end to end monitoring of the infrastructure in Elastic cloud due to no ingestion of logs from legacy solutions.

The client required expert support for custom integrations to ingest from all the sources for end-to-end monitoring.

PROJECT REQUIREMENTS

- Integration with legacy SNMP protocol based Traps (Alerts)
- SNMP Traps had to be normalised to Elastic common schema and parsed to identify impacted components.
- Integration needed to be customised for Pure Storage and VMWare Center
- Create a centralised Logstash pipeline setup to manage a fleet of Logstash instances

SOLUTION DELIVERY

- Offered expertise on the legacy SNMP protocol to configure with Elasticsearch.
- Normalised SNMP Traps to Elastic common schema and parsed to identify impacted components.
- Leveraged a broader professional network to gain vCenter expertise and resolved the issues.
- Setup centralised Logstash pipeline setup.
- As a result, successfully delivered on the project objective of end-to-end monitoring of the IT infrastructure.