A Modern Elasticsearch Logging Workflow

This is a hands-on workshop showcasing the latest Elasticsearch log analytics employed in a practical workflow to debug a problem.

Background

Over the last few years, Elastic has rebuilt its logging toolset to match the scale of the very systems it is observing. Elastic's logging tools let SREs and Developers quickly and easily employ parsing, aggregations, and visualizations (ES|QL, Streams) as part of their daily-driver RCA workflows. Elastic has carefully woven ML (log rate analysis, log pattern analysis) and AI (generating GROK patterns and ES|QL queries) into those tools in ways which remove tedious and complex tasks, allowing the SRE and Developer to focus their attention on quickly and accurately determining a Root Cause. This in turn helps keeps MTTR constant, regardless of growth in the scale and complexity of the system being observing.

Time Required

90 minutes

Target Audience

- SREs
- Developers

Learnings

Participants will walk away from the workshop with an introduction to:

- Using ES|QL to search logs
- Using ES|QL to parse logs at query-time
- Using ES|QL to do advanced aggregations, analytics, and visualizations
- Using ES|QL with JOINs and COMPLETION to enrich records
- Creating a useful dashboard
- Using ES|QL to create Alerts
- Using AI Assistant to help write ES|QL queries
- Using Streams to setup ingest-time log processing (GROK parsing, geo-location, User Agent parsing)
- Setting up a SLO and corresponding Alert
- Using Maps to visualize geographic information
- Scheduling dashboard reports
- Organizing dashboards with collapsible sections
- Setting up a Pivot Transform and corresponding alert
- Setting up RBAC
- Setting up data retention with Streams