A Modern Elasticsearch Logging Workflow

Overview

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

Target Audience

- SREs
- Developers

Applicability

- Existing Customers (introduce them to ES|QL and Streams)
- New Customers (ES|QL and Streams are just part of the Elastic Logs experience)

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
- [new in 9.1] Using ES|QL to do advanced aggregations, analytics, and visualizations
- Creating a dashboard
- Using ES|QL to create Alerts
- Using AI Assistant to help write ES|QL queries
- [new in 9.1] Using Streams to setup ingest-time log processing pipeline (GROK parsing, geo-location, User Agent parsing)
- Setting up SLOs
- Using Maps to visualize geographic information
- [new in 9.1] Scheduling dashboard reports
- Setting up a Pivot Transform
- Setting up RBAC
- Setting up data retention