A Modern Elasticsearch Logging Workflow

Demo

- If you want to run this as a demo, you can use the Elasticsearch (breakout) tab in the first challenge with the full script. There are no hidden additional setup scripts that run in the subsequent challenges.

Timing

- If you need to shorten the course, drop:

1) RBAC (last challenge)
2) Transform+Alert (last part of second to last challenge)
3) All of the second to last challenge