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 (probably in this order):

1) RBAC: all of Challenge 6
2) New UA Alert using Transforms: last part of Challenge 5
3) Reporting and RBAC: all of Challenge 5