Using ELK/Kibana for Log Analysis

Let by Travis Haagen, with Jason Lemay

Highlights:

- As of latest product releases (January 2016), there is a **C**ommon **Aud**it Framework (CAUD):
  - Provides a single common auditing service across the platform.
  - Enables you to trace the entire lifecycle of users, devices, things, and service events.
  - Audit Handler can log data into different formats (csv, syslog, db for example), and can send it to third-party SIEM and analytics tools like Splunk or the ELK stack.
- Travis showed how to configure an ELK stack handler in IDM.
- Travis started elaticsearch on his laptop (very easy to install with home-brew on MacOS).
- Kibana is also very easy to install.
- Travis showed how Kibana can be configured.
- Travis showcased a recon failure, captured its transactionId, and then found the underlying cause by searching for activity events of this Id.
- Different handlers can be created to handle different audit events (for indexing purposes).
  - For example by "topic": one handler for access events, one handler for activity events, etc.