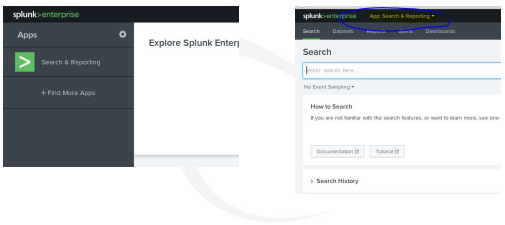
Introduction to Splunk

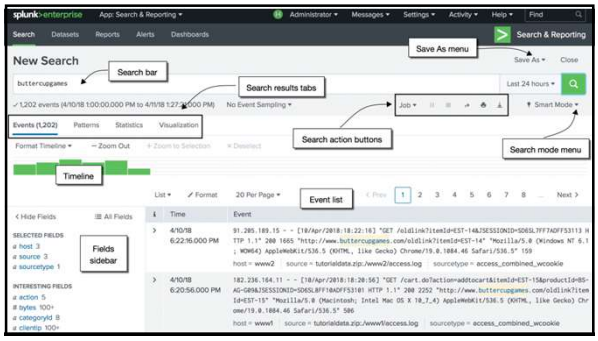
Module 5: Searches

Natasha Staples

CYBRARY



CYBRARY



SPL: Search Processing Language

Six categories of search commands:

- distributable streaming
- centralized streaming
- transforming
- generating
- orchestrating
- dataset processing

CYBRARY

Searching tips:

- The more specific, the better
- Limit searches by time, index, and other fields

CYBRARY

Fields:

Searchable name/value pairings

- Field names are case sensitive
- Field values are not case sensitive
- You can use wildcards
- Use quotation marks if there are spaces

Username=Sarah is not the same as username=Sarah
Username=sarah is the same as Username=SaRaH

* ←wildcard

Name=sa*

Results: Samantha, Sarah

Name="Sarah Smith" NOT
Name=Sarah Smith

CYBRARY

Boolean operators:

- AND
- OR
- NOT

Username=sarah AND Machine=host3

Username=sarah OR Machine=host3

Username=sarah NOT Machine=host3 Username=sarah Machine!=host3

CYBRARY

Next up: Splunk Searches

CYBRARY