Introduction to Splunk

Module 5: App Basics

Natasha Staples

CYBRARY

Apps vs. Add-ons

- Apps: user interface
- Add-ons: retrieve/work with data behind-the-scenes
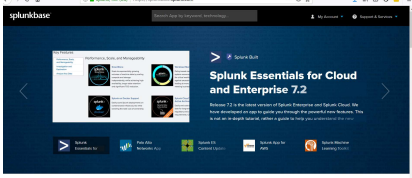
CYBRARY

Apps:

- Splunk built, vendor built, user built

- Install in test environment first

CYBRARY

Splunkbase:

- https://splunkbase.splunk.com/

CYBRARY

Popular apps to look for:

- Splunk Security Essentials
- DBConnect
- Lookup File Editor
- Vendor-specific apps

CYBRARY

Developer Life:

- You can make an app!
- Splunk Certified Developer

CYBRARY

Q. TRUE OR FALSE: YOU SHOULD FIRST INSTALL AN APP IN A PRODUCTION ENVIRONMENT BEFORE TESTING IT

_____
_____
_____
_____
_____
_____
_____

Next up: The last module!

CYBRARY

_____
_____
_____
_____
_____
_____
_____
_____