Splunk Cloud in CI/CD pipelines

Hello!

I am Atef KOUKI

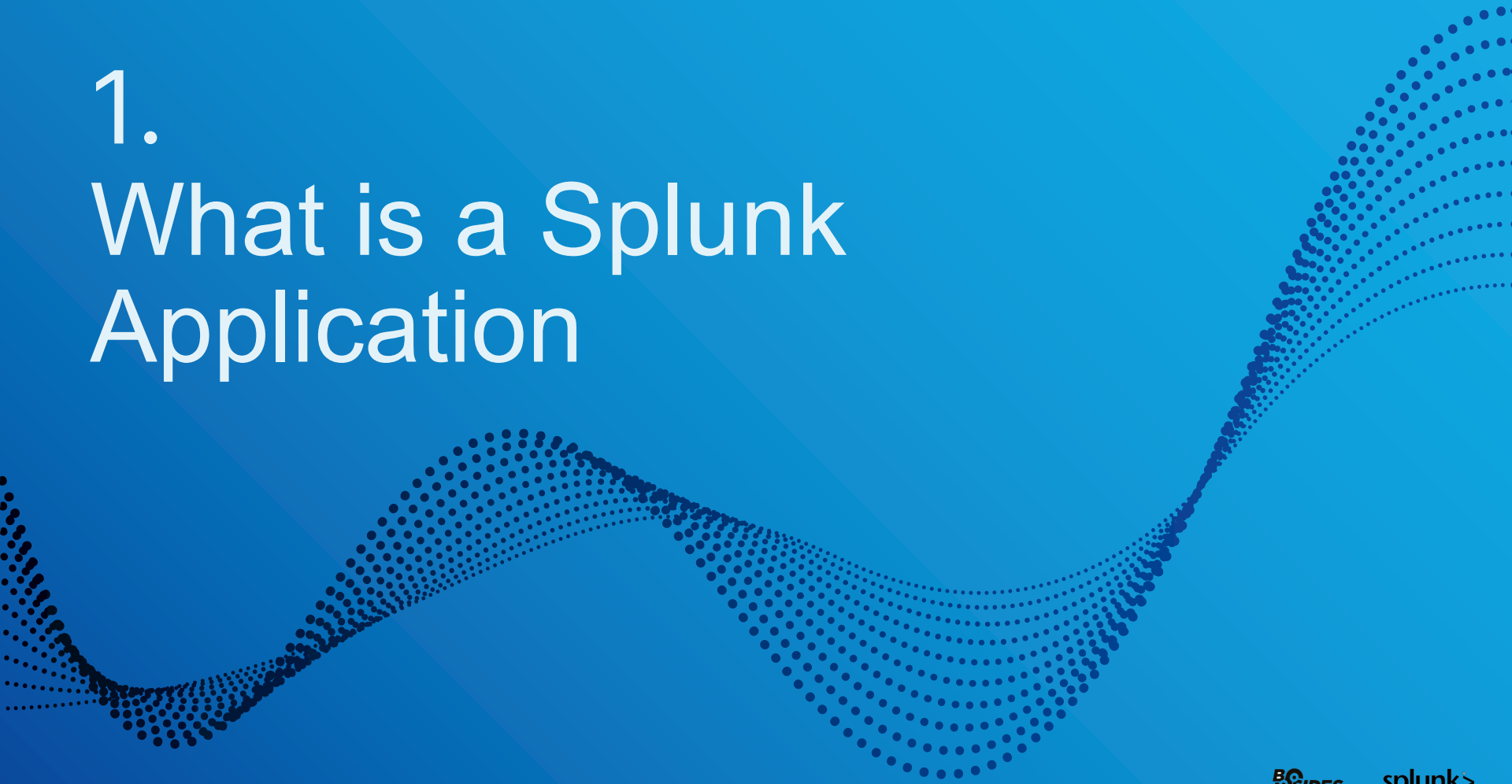
Consulting Sales Engineer

You can find me at @akouki_splunk

Plan

- What is a Splunk Application ?
- Available Splunk tools and helpers
- Splunk Cloud and App vetting
- CI/CD and Splunk Cloud : Architecture
- Demonstration

1.
What is a Splunk Application

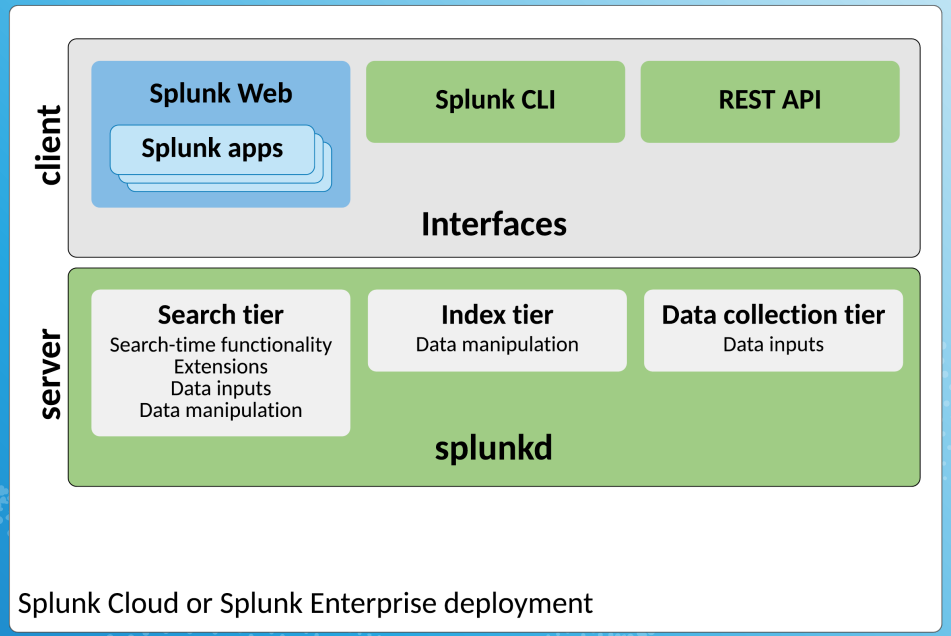


“Definition”

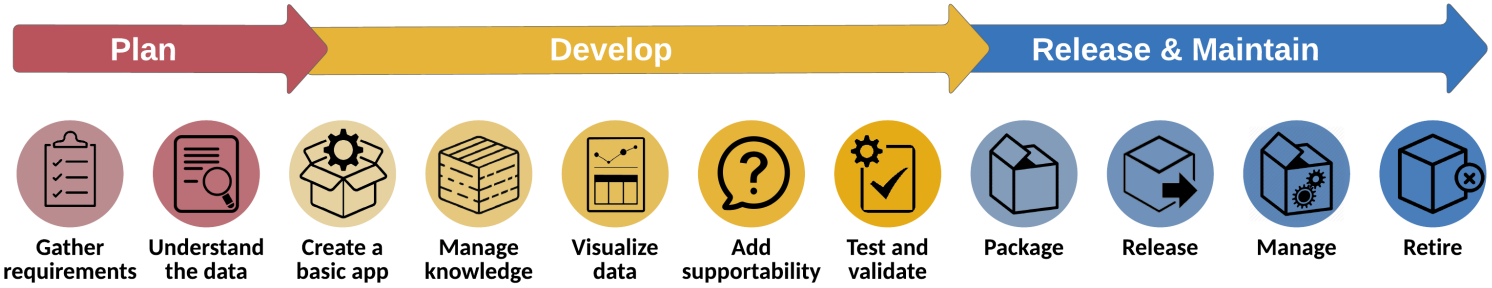
- Packaged solution that runs in a Splunk Cloud or Splunk Enterprise deployment.
- Typically provides a customized experience that targets a specific set of data for a specific purpose.
- Contains a collection of knowledge objects and extensions for a specific technology or use case.
- Can be extended, customized, modified.

Different functions

Contains the configuration files and knowledge objects that perform different functions and runs on different Splunk servers/roles (search head, indexers, forwarders)



Lifecycle of a Splunk app



Lifecycle of a Splunk app

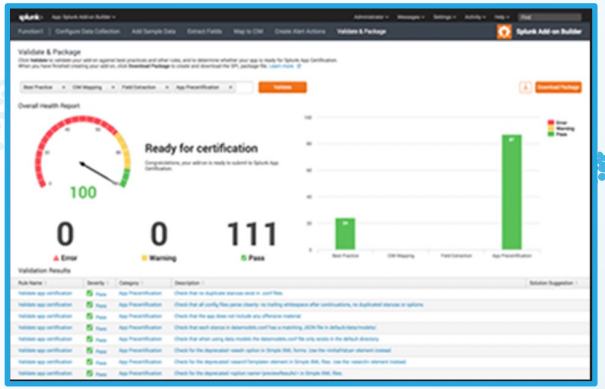
2. Available Splunk tools and helpers

Automation friendly

Addon Builder

https://splunkbase.splunk.com/app/2962/

- Use the Addon builder to accelerate dev:
  - Create easily source types
  - Help to extract fields (schema on the fly)
  - Help to create alias
  - Common information model friendly
  - Quickly inspect and test current dev

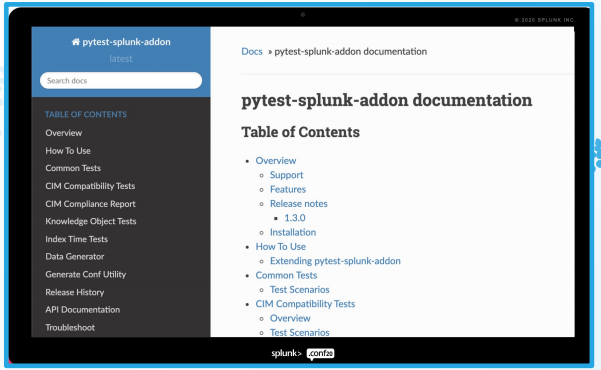


SimData

- A tool that generates event data from a simulation of a user-defined scenario :
  - Easy to automate data generation (CLI)
  - Instead of using a sample set of data that is repetitive and unrealistic, SimData allows you to generate a rich and robust set of events
  - change variables at runtime to demonstrate how an app responds to different behaviors.
  - Need JAVA env

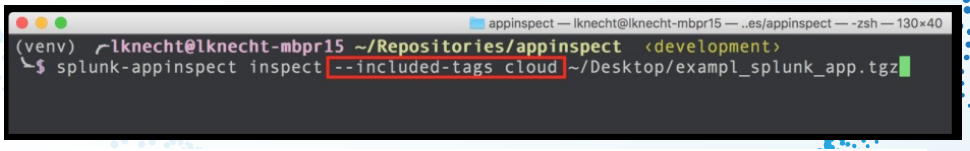
Pytest

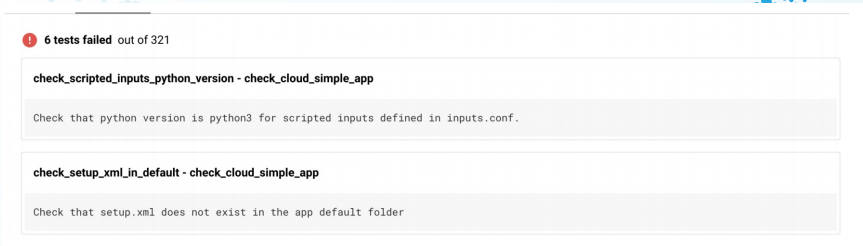
- Use Pytest to inspect fields extraction and data quality :
  - Easy to automate
  - Using data samples test every knowledge object to confirm use (no dead code) and correctness (produces a result)
  - confirm that CIM tagged events contain correct values
  - Test common index time operations



AppInspect

- Use AppInspect to verify best practices and configurations spec rules :
  - Easy to automate (CLI or API integration)
  - Static analysis of best practices and identification of worst behaviors
  - Gives your developers confidence via the AppInspect badge your add-on is safe to deploy
  - Gives your users confidence with Cloud Ready validation of best practices





BSIDES splunk>

Splunk Cloud REST API

- A splunk cloud user can call a limited subset of the Splunk Enterprise REST API endpoints.

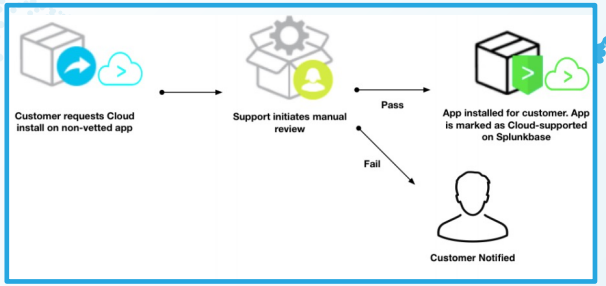
Category	Support level	Description
Access control	Partial	Authorize and authenticate users.
Applications	None	Install applications and application templates.
Clusters	None	Configure and manage indexer clusters and search head clusters.
Configuration	Partial	Manage configuration files and settings.
Deployment	None	Manage deployment servers and clients.
Inputs	None	Manage data input.
Introspection	None	Access system properties.
Knowledge	Full	Define indexed and searched data configurations.
KV store	None	Manage app key-value store (KV store).
Licensing	None	Manage licensing configurations.
Metrics	Partial	Enumerate metrics.
Outputs	None	Manage forwarder data configuration.
Search	Full	Manage searches and search-generated alerts and view objects.
System	Partial	Manage server configuration.
Workload management	Partial	Manage system resources for search workloads.

BSIDES splunk>

3.
Splunk Cloud and App Vetting

What is Cloud Vetting

- Checks for security vulnerabilities
- Checks for operational issues
- Is required before your app can be installed on Splunk Cloud!
- Automated process, but sometimes requires a manual review:
  - Splunk Inc. runs the Splunk AppInspect API to perform automated cloud vetting.
  - When necessary, a Splunk employee performs a manual cloud vetting process to further evaluate the app or add-on.



4.
Splunk Cloud in CICD pipelines

Splunk Cloud and CI/CD NOW

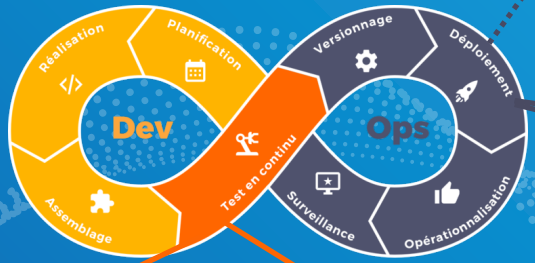
Manual App Vetting
for advanced devs

splunk> cloud

Deploy by
Endpoints

AppInspect

Test App structure , best practices, configurations



Parse Configurations and match compatible splunk cloud endpoints

Config parser
python

docker

Validate extractions against
data samples + simData

BSIDES splunk>

5.
Demonstration Time

Thanks!

Any questions?

You can find me at :

- @akouki_splunk
- akouki@splunk.com

Source code : bit.ly/bsides-cicd

BSIDES splunk>