How to Build a Technical Add-on In 5 Minutes

Gang Tao

Architect, Splunk

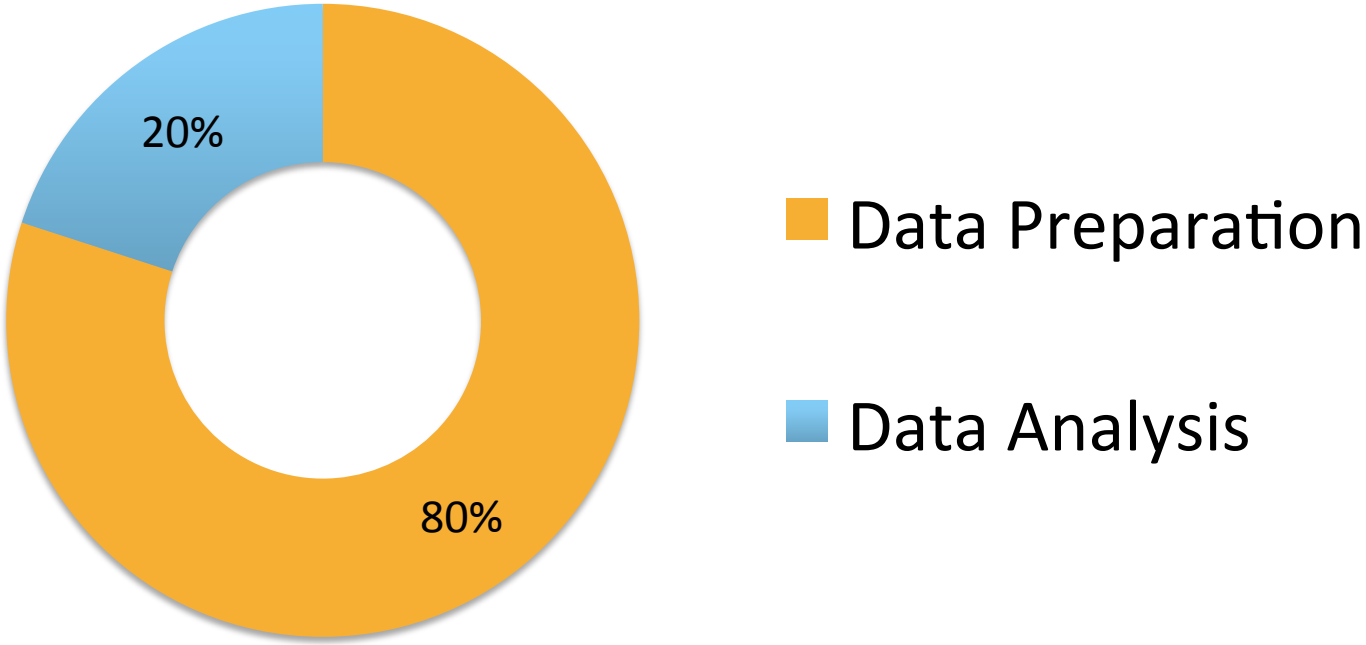
splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Time Spent on Data Input Projects



How to Get Data Into Splunk?

File monitors

TCP/UDP

Windows Event log

Scripted Input

Modular Input

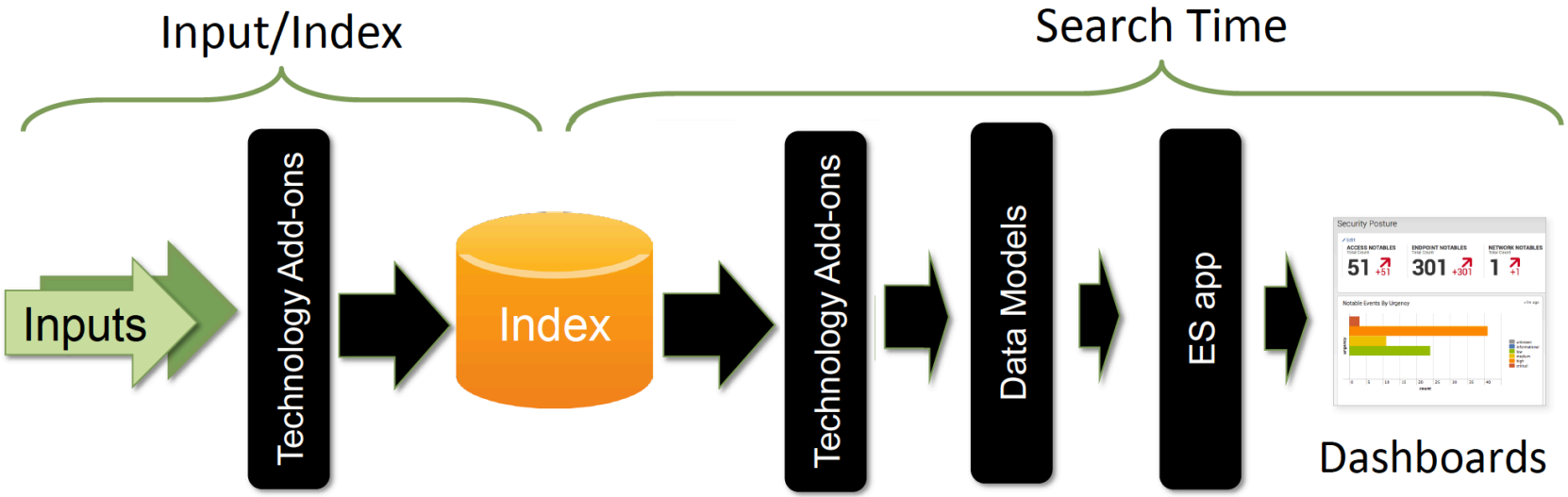
HTTP Event Collector

What Does A Technology Add-on Do?

- It is a Splunk App that does Data Preparation with followings:

Data Acquisition	Inputs (Files, Modular, TCP/UDP, etc)
Data Transformation	Line breaks, timestamps, field extraction
Data Normalization	CIM Mapping (Event types, Tags, aliases)
Data Enrichment	Prebuilt panels, saved searches, lookups

TA : From Inputs to Dashboards

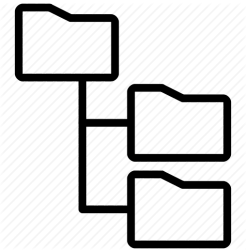


TA Challenges

Build a TA from Scratch is not easy, it requires some trivial steps and different knowledge about modular input, field extraction, CIM, etc.

TA Builder

App



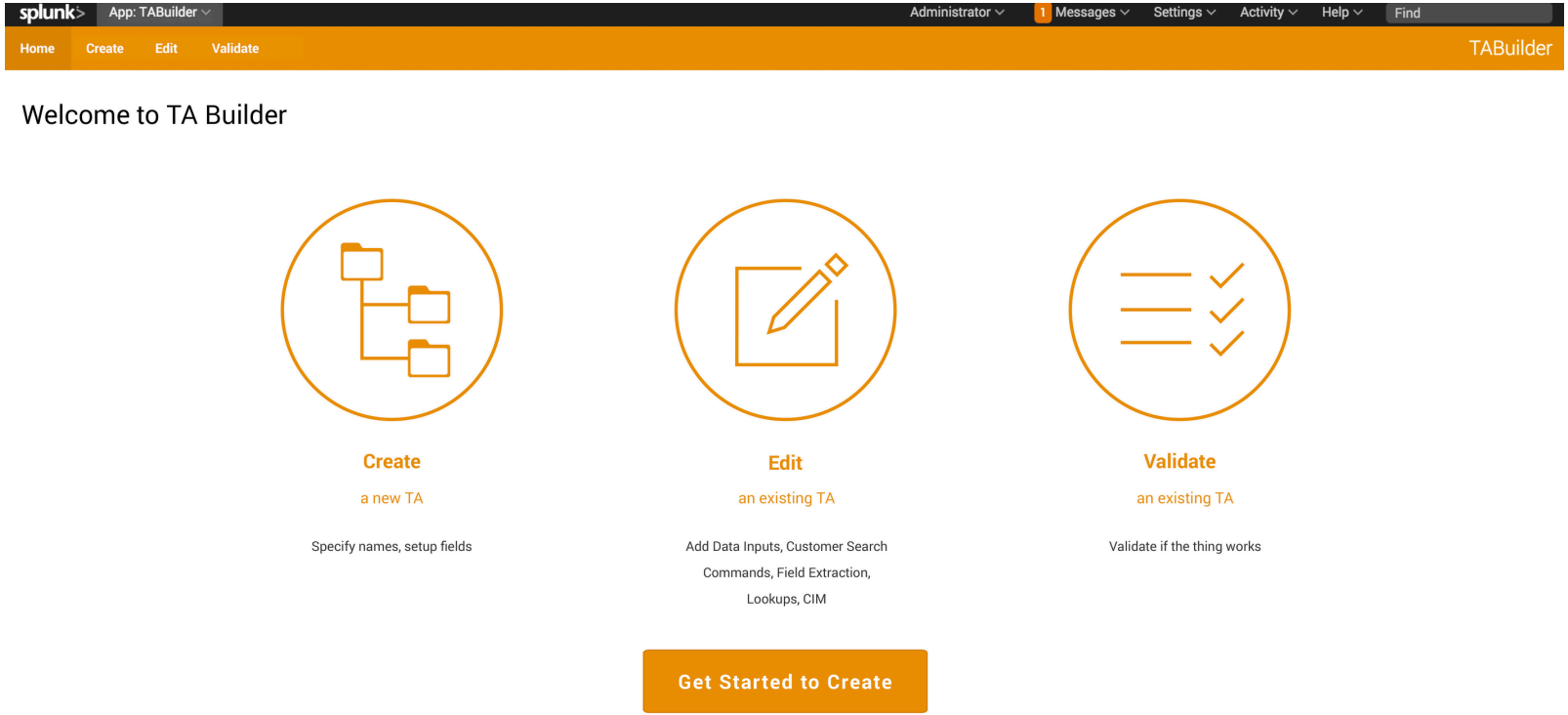
Skeleton Builder

Modular Input Builder

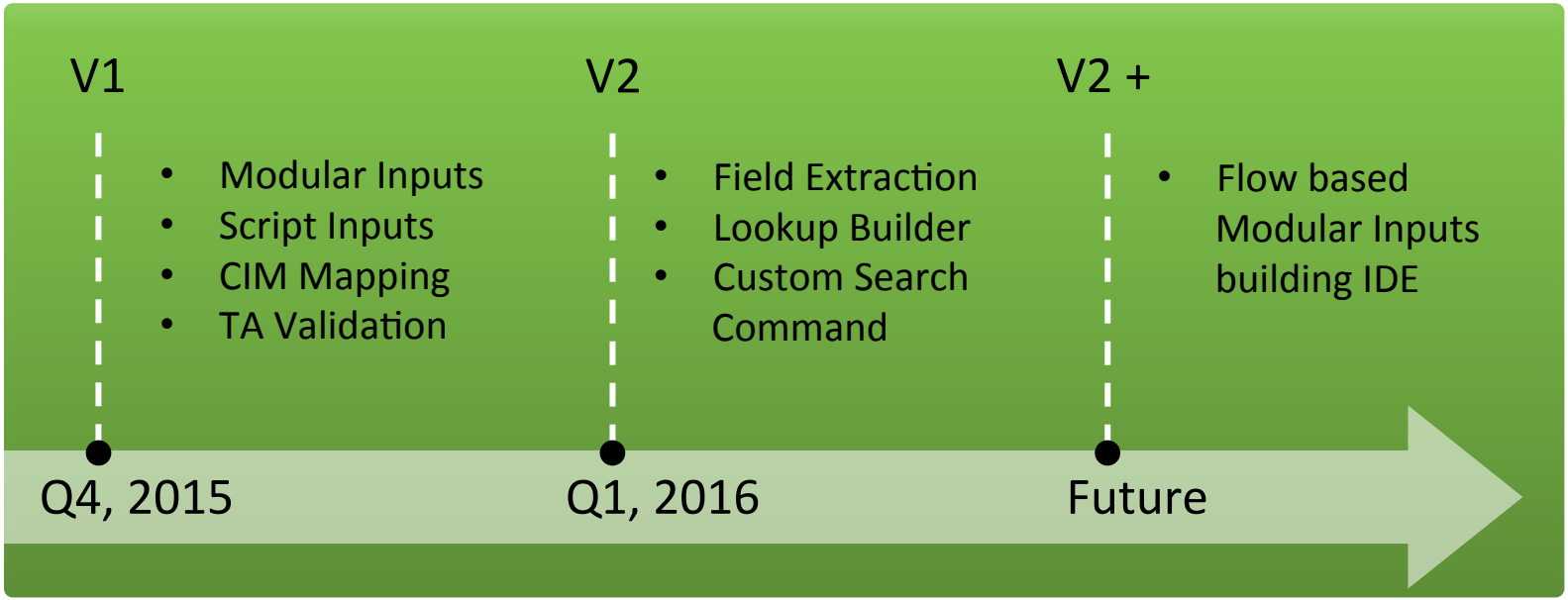
CIM Builder

Validator

Demo


splunk>
App: TABuilder
Administrator
1 Messages
Settings
Activity
Help
Find
Home
Create
Edit
Validate
TABuilder
Welcome to TA Builder
Create
a new TA
Specify names, setup fields
Edit
an existing TA
Add Data Inputs, Customer Search Commands, Field Extraction, Lookups, CIM
Validate
an existing TA
Validate if the thing works
Get Started to Create

Roadmap


V1
Modular Inputs
Script Inputs
CIM Mapping
TA Validation
Q4, 2015
V2
Field Extraction
Lookup Builder
Custom Search Command
Q1, 2016
V2 +
Flow based Modular Inputs building IDE
Future

Q&A

THANK YOU

splunk>