



App Sorcery 2.0

Building Better Apps with Best Practice

Matt Eglin

Senior Professional Services Consultant | Splunk

Forward-Looking Statements

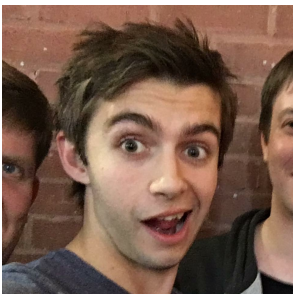


During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

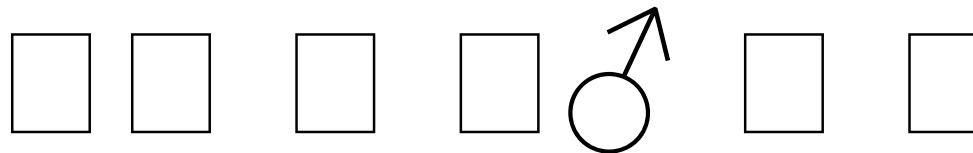
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the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

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Who is this human?



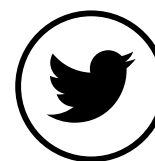
E U G B



splunk> 3.5 years



untappd.com/user/matteglin



@matteglin

In ~40 minutes...

What

Why

Where

How

What do we mean by “App”

Pre-packaged Content

- Dashboards & Searches
- Inputs
- Knowledge Objects

Bundles of Associated Configuration

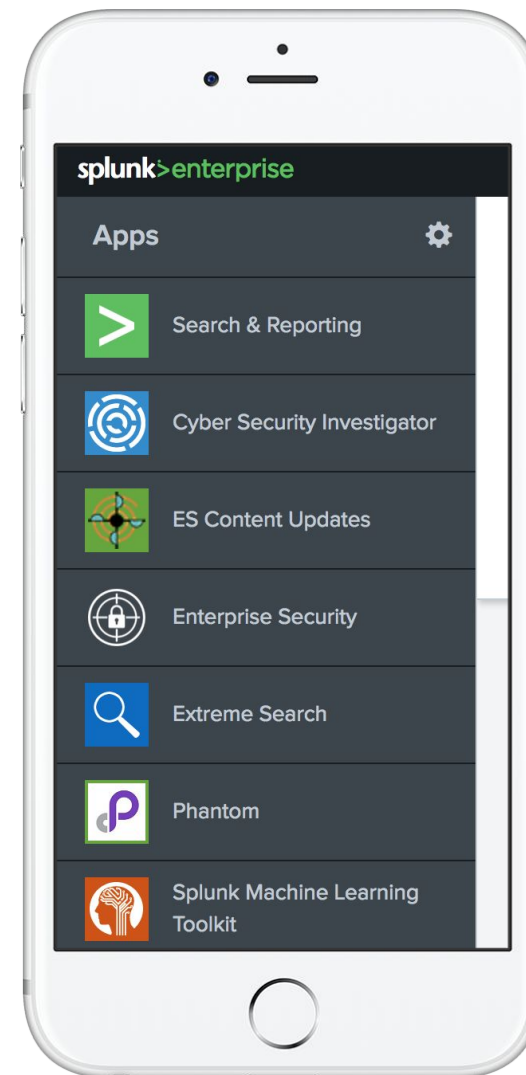
- Think Configuration Management

Integrations with third party, and associated Products

Transformative Experiences

- Splunk Premium Application

Extensions of Splunk Enterprise Functionality





What the App?

Where to begin?

What do we mean by “App”

MLTK

**Splunk Enterprise
Security**



MLTK



Splunk Add-on for



Why do we do this?

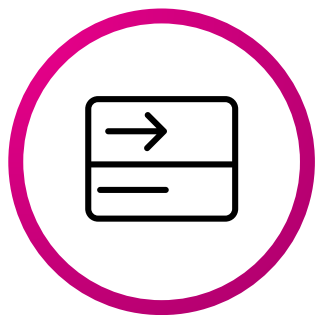
The point of using Apps

- Simplify Splunk Configuration Management and Deployment
- Package up complex content for easy deployment
- Leverage Splunk deployment methods like Deployment Server, Cluster Master and Deployer
- Easily reuse custom created configuration elsewhere
- One-Click Implementation of Data Use Cases
- Distributing your cool content to other Splunk Users

Deploying Apps

You have options!

**Deployment
Server**



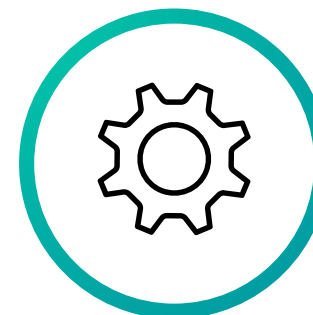
**Cluster
Master**



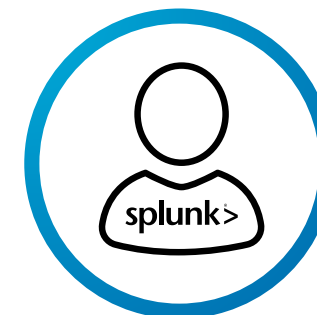
Deployer



**Puppet /
Chef / SCCM**







Manually...



Apps and TA's

More than just an acrony

	
Splunk Add-on for Unix and Linux	Splunk App for Unix and Linux
54474 Installs 	3725 Installs 

Aren't these the same thing?

Apps and TA's

More than just an acronym

App

- Visible in Web UI
- Contains Dashboards and Visual Content
- Contains Search Time Knowledge Objects
- Designed for End User interaction
- Search Head Deployment

Technical Addon

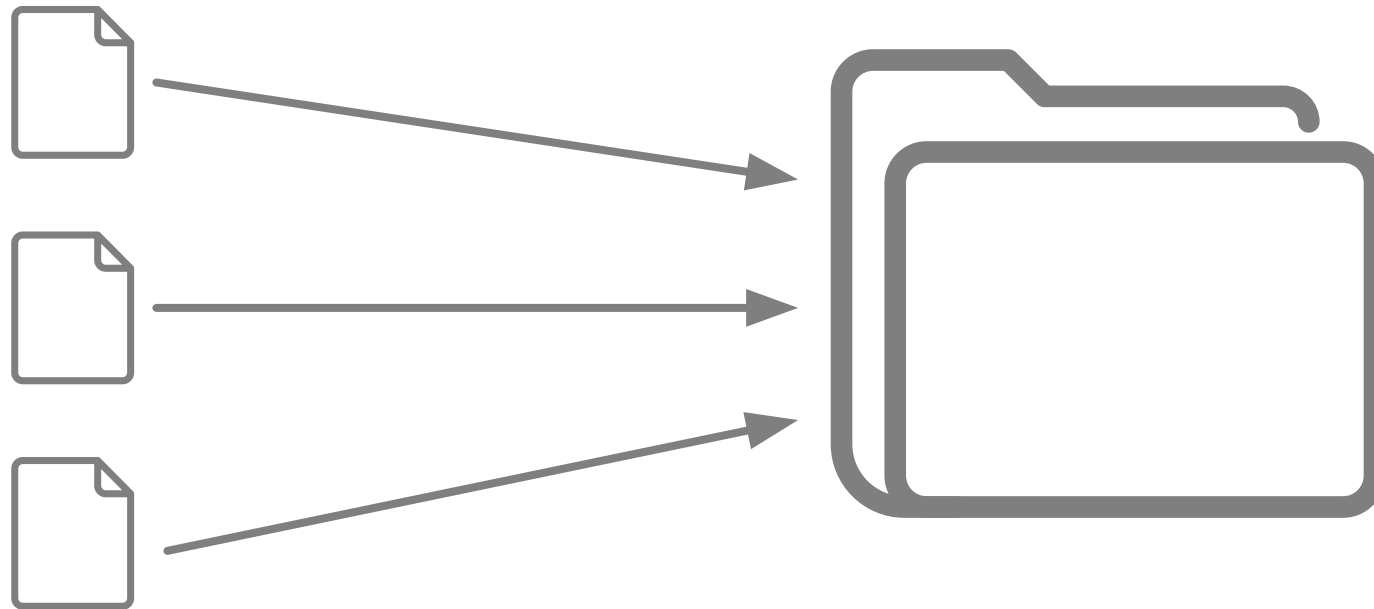
- Not visible in Web UI
- Contains Search Time Knowledge objects
- Contains Index Time Knowledge Objects
- Indexer / Search Head & Forwarder Deployment



Building an App

Putting it all together

The Basics



A structured directory of related files

The Basics

```
└─ default.meta
└─ windows_inputs
    └─ default
        ├── app.conf
        └─ inputs.conf
    └─ metadata
        └─ default.meta
```

A structured directory of related files

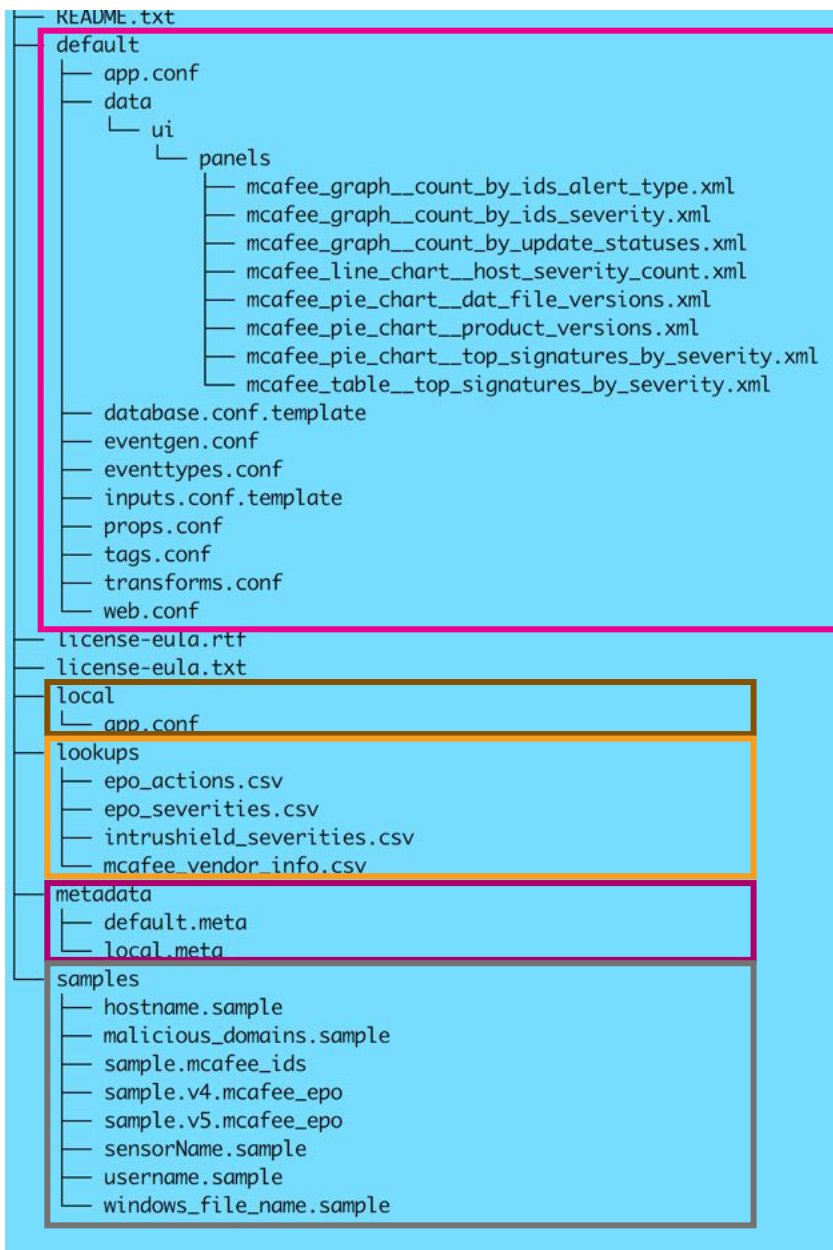
More Complex

What you normally find :

- Default Directory
- Local Directory
- Lookups
- Metadata
- Samples

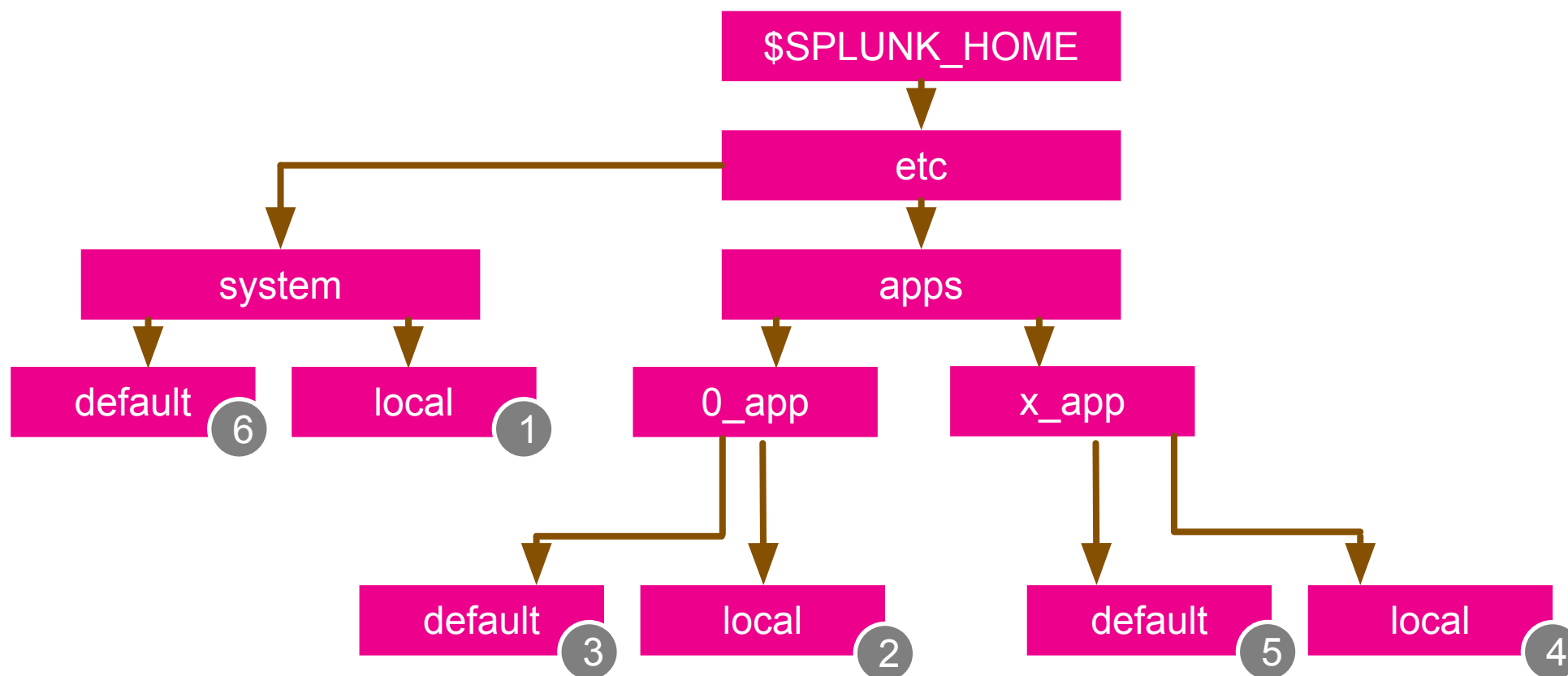
What you *might* also find :

- Bin directory with scripts
- Web Static content (js / images etc.)
- template .conf files
- More conf files!
- License Agreements



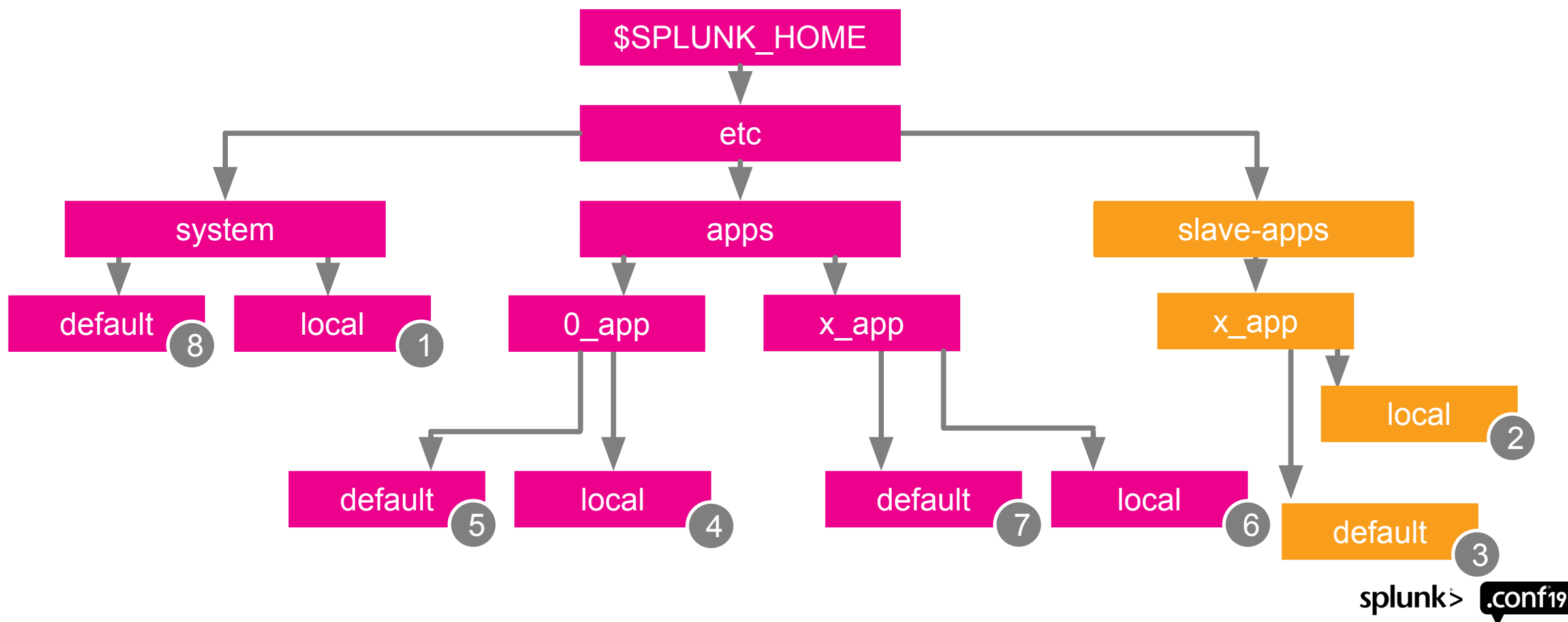
A Note on Configuration Precedence

Index time *and* System level precedence - *standalone*



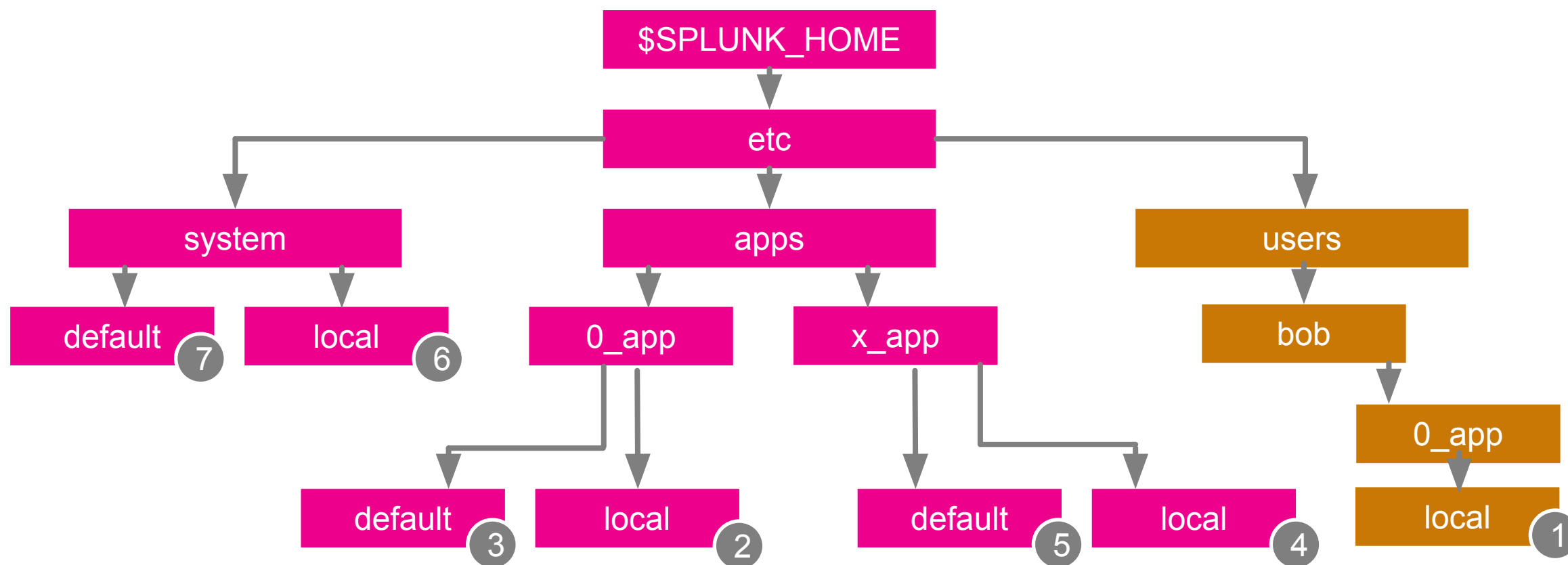
A Note on Configuration Precedence

When using Indexer Clustering



A Note on Configuration Precedence

At Search Time – users/local comes in to play!



A Note on Configuration Precedence

Key Points

- local configuration will always override default
- Apps with a “higher” ASCII order name will take precedence over “lower” ASCII order named Apps
- Config in system/local can override any app setting that tries to be global
- Search time configuration precedence is user centric
- When in doubt – use splunk **bttool** to debug active config

Metadata

It's always in control

- Metadata controls access and visibility to App contents
- default.meta / local.meta files
- Role based access
- Can be global or granular

Application-level permissions

□

```
access = read : [ * ], write : [ admin ]
export = system
```

TAGS

```
[tags]
export = system
```

SAVED SEARCHES

```
[savedsearches/Errors%20in%20the%20last%2024%20hours]
access = read : [ * ], write : [ admin ]
```

```
[savedsearches/Errors%20in%20the%20last%20hour]
access = read : [ * ], write : [ admin ]
```

```
[savedsearches/Messages%20by%20minute%20last%203%20hours]
access = read : [ admin ], write : [ admin ]
```

```
[savedsearches/Splunk%20errors%20last%2024%20hours]
access = read : [ admin ], write : [ admin ]
```

Alert Actions

Watch out for Configuration Spread

It's not butter

- Be very aware of the export level of your configuration
- Configuration can spread to, and impact other Apps
- Can be especially problematic with Splunk Enterprise Security
- If you don't need to export to 'system', then export to 'app' instead

```
□  
access = read : [ * ], write : [ admin ]  
export = system
```



```
□  
access = read : [ * ], write : [ admin ]  
export = app
```

Top Tips

Do

- Include app.conf
- Include default.meta
- Include Documentation
- Include Example Data
- Utilise a setup.xml screen
- Check file ownership / permissions
- Test your work

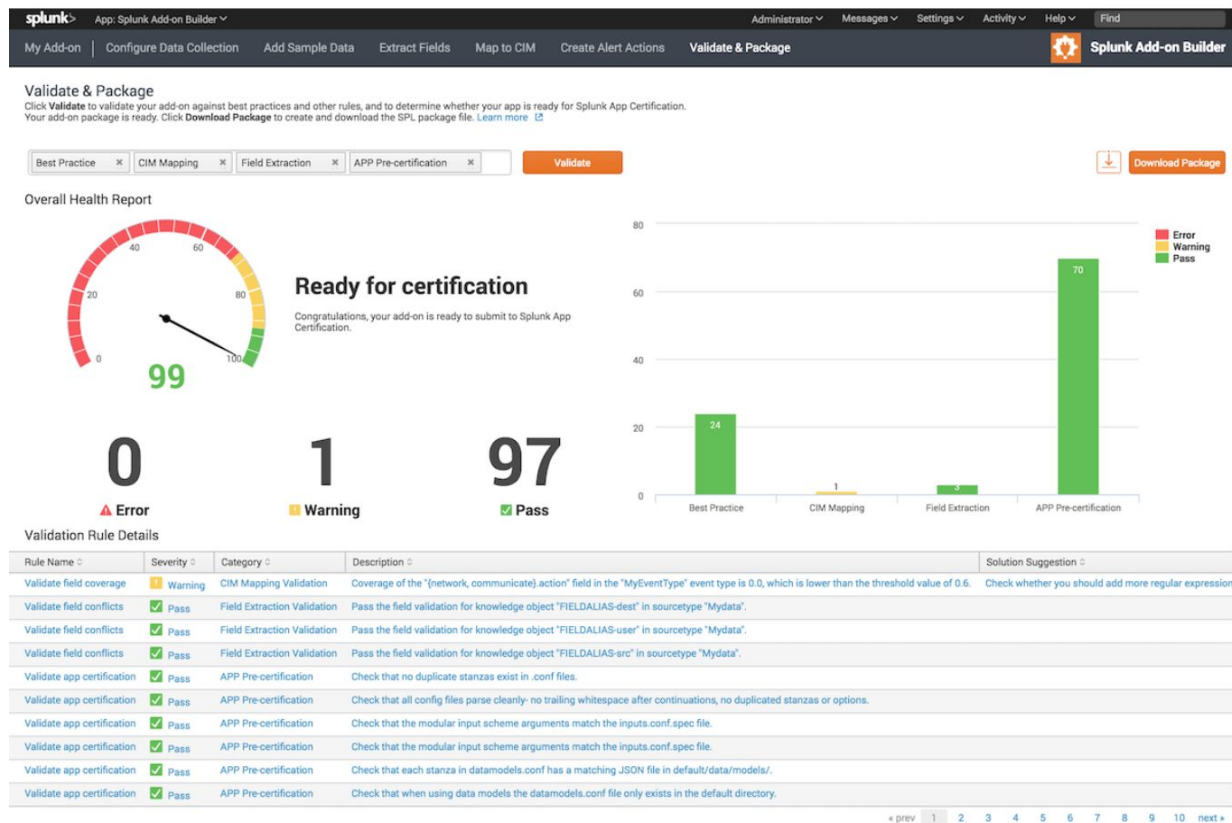
Do Not Do

- Data Model / Search Accelerations enabled by default
- local configuration
- Add excessive configuration
 - eventtypes / props / transforms etc.
- Assume index names in Searches and Dashboards
 - Consider using a macro instead

Splunk Add-on Builder

Add-ons Made Easy!

- Step by Step Process
- Save time and effort
- Easily package up Content
- Designed for making TA's
- Easy data source mapping to Splunk Common Information Model
- Prepare for Splunk Certification



Demo



Extending Splunk

Transforming the experience

REST API

An Overview

- REST endpoints to interact with splunkd without heavy browser interfaces
- Exposes configuration and settings
- Control Splunk Programmatically
- *Can* be extended to meet custom needs
- Custom features can be exposed to a wider audience

REST API

As implemented in Splunk Enterprise Security

The screenshot shows the 'Incident Review' page in the Splunk Enterprise Security interface. The top navigation bar includes 'splunk>enterprise', 'App: Enterprise Security', and user roles like 'Administrator'. The main navigation menu has options like 'Security Posture', 'Incident Review', 'Investigations', 'Glass Tables', 'Security Intelligence', 'Security Domains', 'Audit', 'Search', and 'Configure'. The 'Incident Review' section on the left includes filters for 'Urgency' (CRITICAL, HIGH, MEDIUM, LOW, INFO) and 'Status' (Select...). The main content area shows a timeline view with a search bar and a 'Submit' button. A message indicates '0 events (19/08/2019 11:00:00.000 to 20/08/2019 11:51:00.000)'.

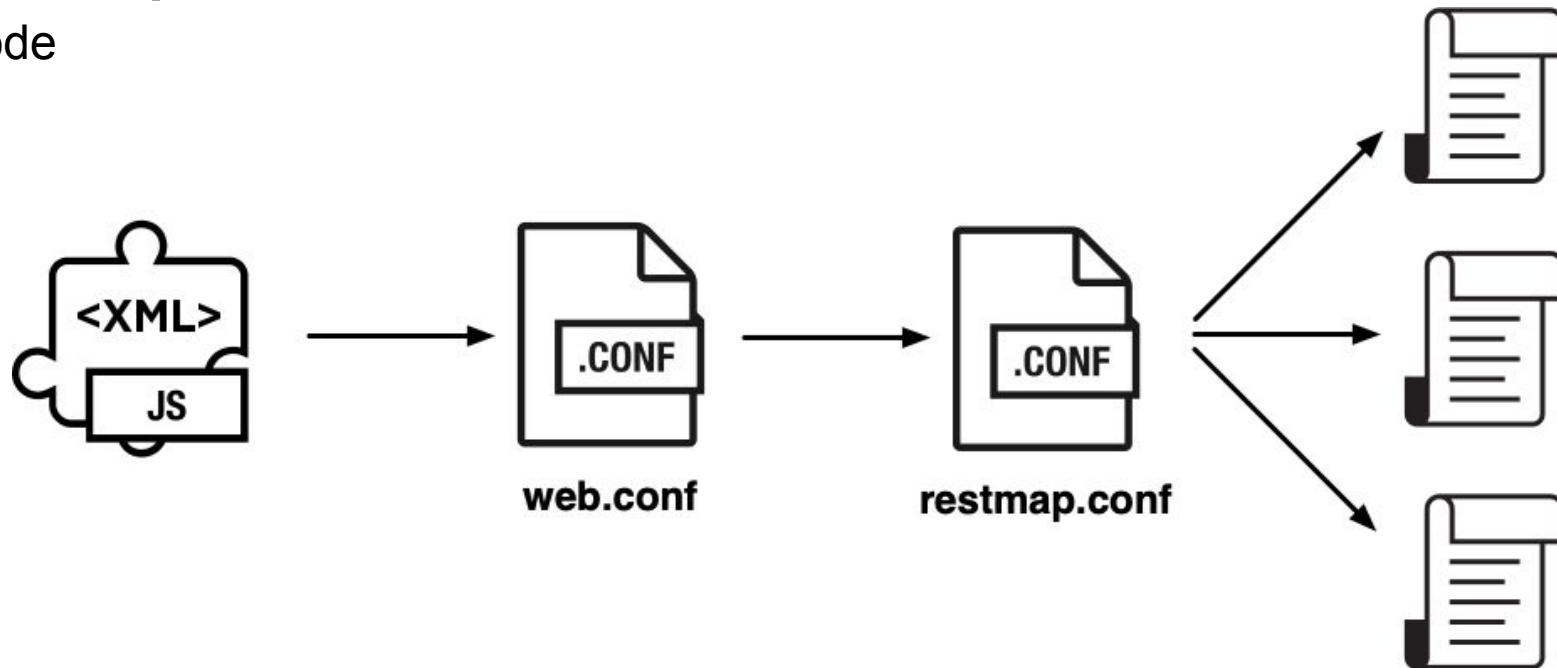
The screenshot shows the 'Investigations' page in the Splunk Enterprise Security interface. The top navigation bar is similar to the previous screenshot. The main navigation menu highlights 'Investigations'. The 'Investigations' section includes a 'Create new investigation' button and a table with columns: 'Name', 'Description', 'Status', 'Created', 'Last Modified', and 'Collaborators'. The table is currently empty, showing 'Showing 0 to 0 of 0 entries'.

REST API

Chaining it all together

web.conf / restmap.conf

- From call to code



REST API

Make the Call

Calling *back* into Splunk from a script

- Authentication is token based
- Scripts executed by Splunk are passed a token on the call
- Valid for calls back into *splunkd*
- Grab the token and authentication is yours

Custom Assets

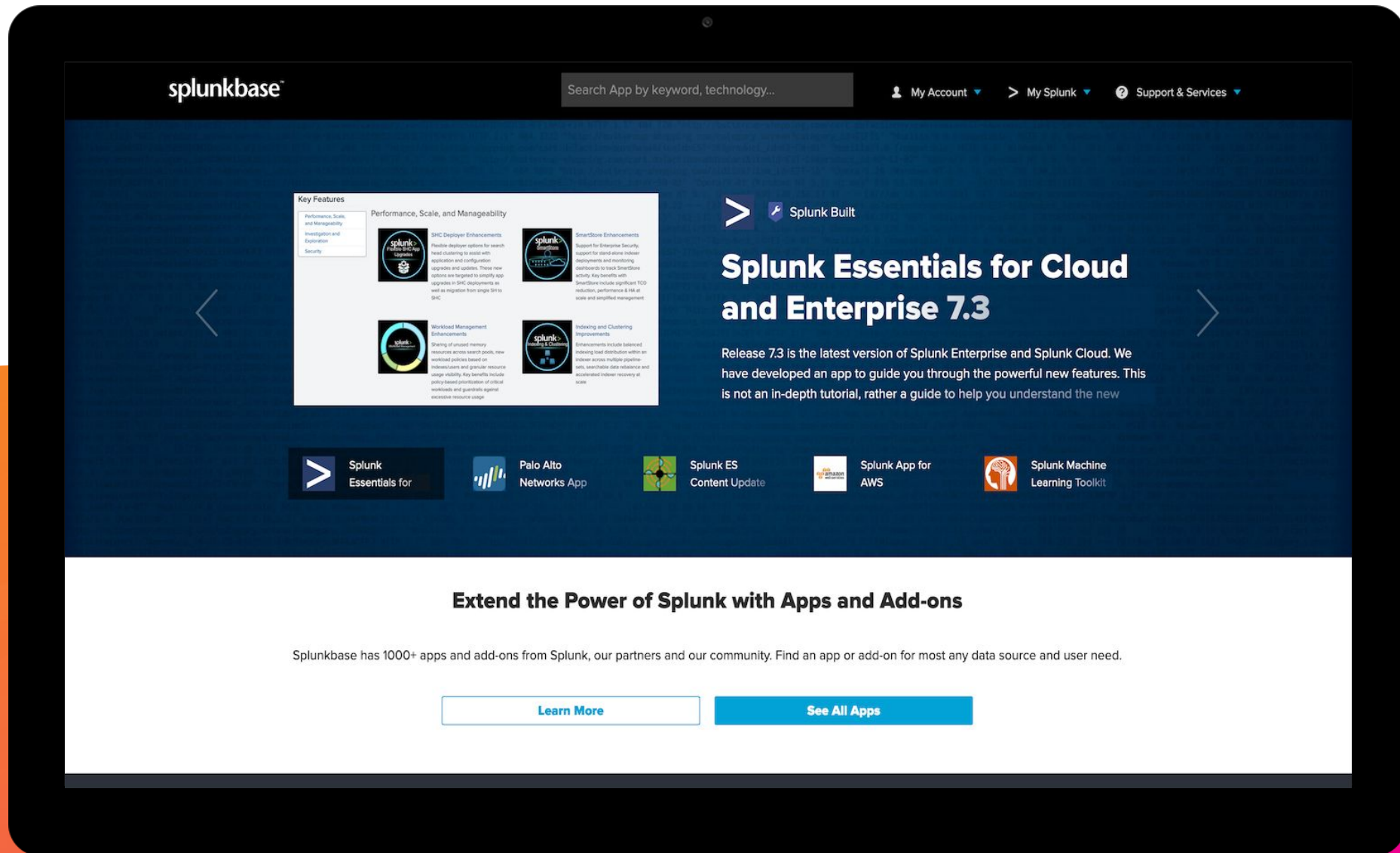
Serving Custom Assets from Splunk

- Store in your app /appserver/static/ and REST GET will deliver what you need
- `https://<splunk_url>:<port>/static/app/<app_dir>/<filename>`
- Images / CSS / JS for fancy dashboard experiences



Apps On Splunkbase

Getting it out there!

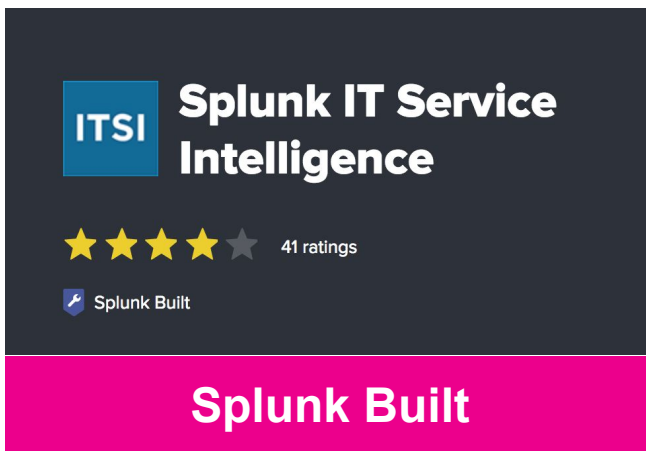


Apps on Splunkbase

Splunkbase?


Splunk Managed repository of Apps and TA's

One stop shop for all your Splunk needs

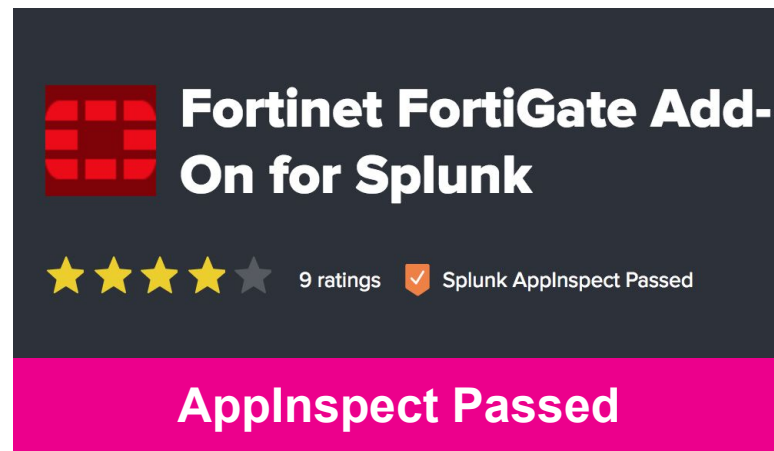



ITSi **Splunk IT Service Intelligence**


★★★★☆ 41 ratings

 Splunk Built

Splunk Built



 **Fortinet FortiGate Add-On for Splunk**

★★★★☆ 9 ratings  Splunk AppInspect Passed

AppInspect Passed

Apps on Splunkbase

Badging



Splunk Built

- Splunk Built First Party App
- Supported and Validated by Splunk



Splunk AppInspect Passed

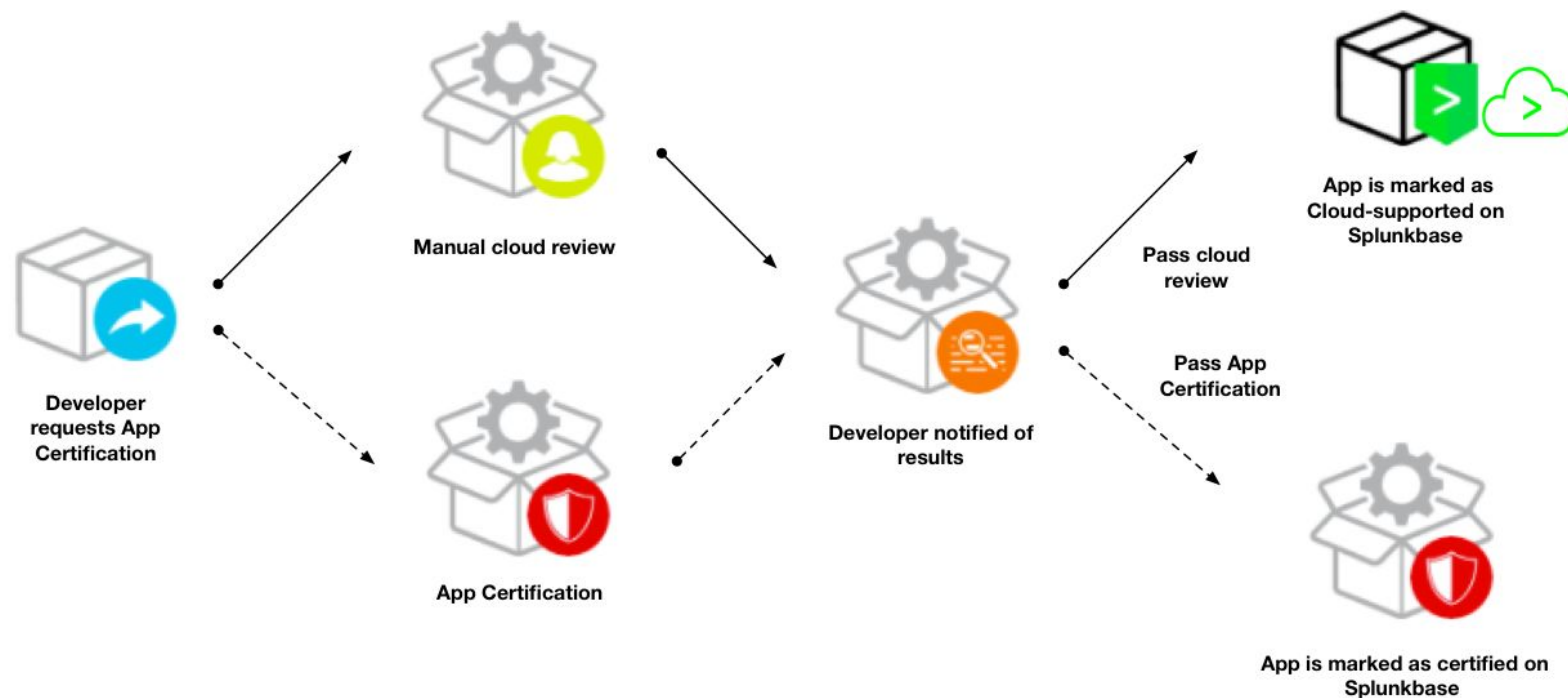
- Splunk Certified Third Party Apps
- Mark of Validation and Quality
- Supported by the Creator



Not always available for Splunk Cloud

Validation Process

- Strict set of criteria required for an App to be “Certified”
- Certification Process once Submitted to Splunkbase



Validating for Splunkbase

AppInspect

Download and install tool from Splunk Dev

- <http://dev.splunk.com/view/appinspect/SP-CAAEE9U>

Install pre-requisites

Run your App through AppInspect *before* submitting to Splunkbase

- `splunk-appinspect inspect app_path/app_filename.tgz --mode precert --included-tags splunk_appinspect`
- Review the output and correct any Failures




```
2. bash
Check iframe elements for compliance with Splunk Cloud security policy.
  SKIPPED: Skipping due to package validation issues.
Check that all XML files are well-formed.
  SKIPPED: Skipping due to package validation issues.
Check any XML files that embed JavaScript via CDATA for compliance with
Splunk Cloud security policy.
  SKIPPED: Skipping due to package validation issues.
Ensure that global event handlers are not used within XML files.
  SKIPPED: Skipping due to package validation issues.

repcap Report Summary:
  skipped: 240
  success: 7
  manual_check: 0
  failure: 3
  warning: 0
  error: 0
  not_applicable: 3
-----
  Total: 253

(venv) meglin-mbp:~ meglin$
```

Validating for Splunkbase

Apps will be reviewed








 **Report Capture**

DOWNLOAD



This app is pending approval and is not yet publicly visible.

⚙️ **ADMINISTRATOR TOOLS:** [Manage App](#) | [View App](#) | [View Analytics](#)

STATUS: PENDING

-  Hosting
-  [Description](#)
-  [Media](#)
-  [Details](#)
-  [Settings](#)
-  [Leads](#)
-  [Editors](#)

VERSIONS [+ New Version](#)

VERSION	DEFAULT	VISIBILITY	COMPATIBILITY	UPLOAD DATE
0.8.4			7.1, 7.0, 6.6	Aug 21, 2018


To schedule a Release Date, click [here](#).

REQUEST APP DELETION

🔔 Want to host externally or transfer ownership? [Contact Us](#)

Managing on Splunkbase

Once approved, versions can be managed

 **PDF Report Capture for Splunk**

DOWNLOAD

⚙️ **ADMINISTRATOR TOOLS:** Manage App | View App | View Analytics

STATUS: APPROVED

🔒 Hosting

Description

🖼️ Media







📄 Details

⚙️ Settings

🔍 Leads


👤 Editors

VERSIONS [+ New Version](#)

VERSION	DEFAULT	VISIBILITY	COMPATIBILITY	UPLOAD DATE	APPINSPECT STATUS
0.8.6	<input checked="" type="radio"/>		7.1, 7.0, 6.6	Jan 2, 2019	 Details
0.8.5	<input type="radio"/>		7.1, 7.0, 6.6	Nov 27, 2018	 Details
0.8.4	<input type="radio"/>		7.1, 7.0, 6.6	Aug 21, 2018	 Details

REQUEST APP ARCHIVING

[Learn more about app archiving.](#)

[? Want to host externally or transfer ownership?](#)  [Contact Us](#)

Validating for Splunk Cloud

AppInspect

Download and install tool from Splunk Dev

- <http://dev.splunk.com/view/appinspect/SP-CAAEE9U>

Install pre-requisites

Run your App through AppInspect *before* submitting to Splunkbase

- `splunk-appinspect inspect app_path/app_filename.tgz --mode precert --included-tags cloud`
- Review the output and correct any Failures



```
2: bash
Check iframe elements for compliance with Splunk Cloud security policy.
  SKIPPED: Skipping due to package validation issues.
Check that all XML files are well-formed.
  SKIPPED: Skipping due to package validation issues.
Check any XML files that embed JavaScript via CDATA for compliance with
Splunk Cloud security policy.
  SKIPPED: Skipping due to package validation issues.
Ensure that global event handlers are not used within XML files.
  SKIPPED: Skipping due to package validation issues.

recap Report Summary:

  skipped: 240
  success: 7
  manual_check: 0
  failure: 3
  warning: 0
  error: 0
  not_applicable: 3
-----
  Total: 253

(venv) meglin-mbp:~ meglin$
```


Validating for Splunk Cloud

Step by Step

1. Register for a Splunk Developer Account
2. Run your App through Splunk AppInspect
 - Exhaustive Criteria List - <http://dev.splunk.com/view/app-cert/SP-CAAEE3H>
3. Make some Documentation!
 - Release Notes
 - Description
 - Splunk Enterprise Version Compatibility
 - CIM Compatibility
4. Decide to host on Splunkbase or Externally
5. Submit @ <https://splunkbase.splunk.com/new/>

Managing Custom Apps in Splunk Cloud

Make Cloud your own

- Keep your Custom Enterprise Apps following migration
- Validation process is the same as for Splunkbase
- Upload and manage your Private Apps via your Search Head
- *Automatic* propagation of config to Indexers
- Premium Search Head install needs PS or a Support ticket
- Forwarders still need an on-premise Deployment Server

Key Takeaways

1. Configuration Precedence Rules
2. Don't overload Apps / TA's with config. Smaller, more atomic is best
3. Splunk is *mostly* limited by your imagination!
4. Always test your creations



splunk>

Thank

You



Go to the .conf19 mobile app to

RATE THIS SESSION

