Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk> .conf22

The Developer's App Starter Kit

DEV1127C

Tom West

Senior PS Consultant | Splunk

Tom West

Senior Professional Services Consultant
Splunk

splunk> .conf22

Agenda

1. Splunk App Dev
   - What is Splunk App Dev
2. Add-ons (TA)
   - What they are and how to create them
3. Custom Search Commands
   - SPL™ Friends!!!
4. Packaging & Review
   - The Finish Line?!

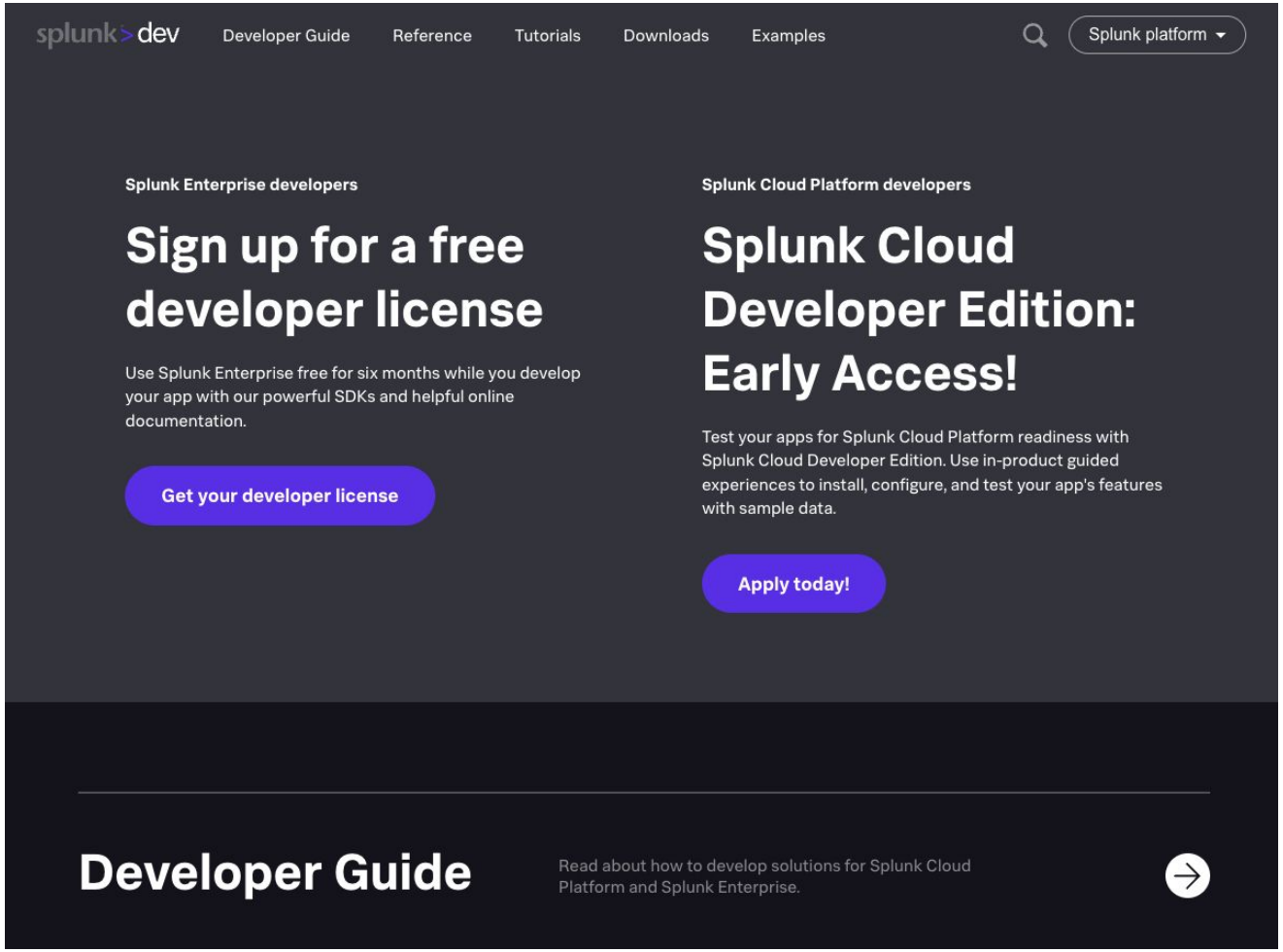
Splunk Dev

The area of Splunk that allows you to create and build solutions for / on the Splunk® Cloud Platform and Splunk® Enterprise.

splunk> .conf22

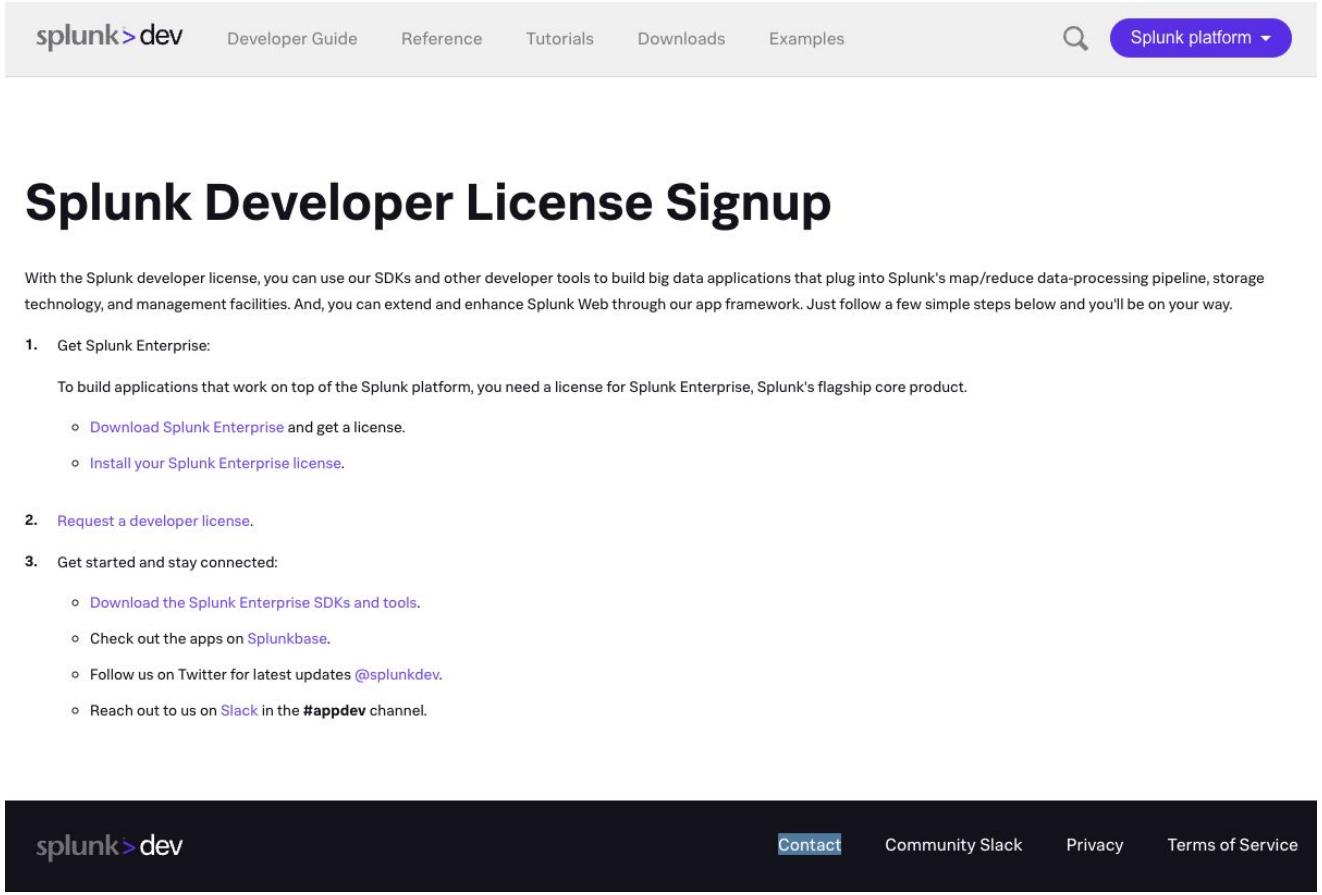
Resources

- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



Resources

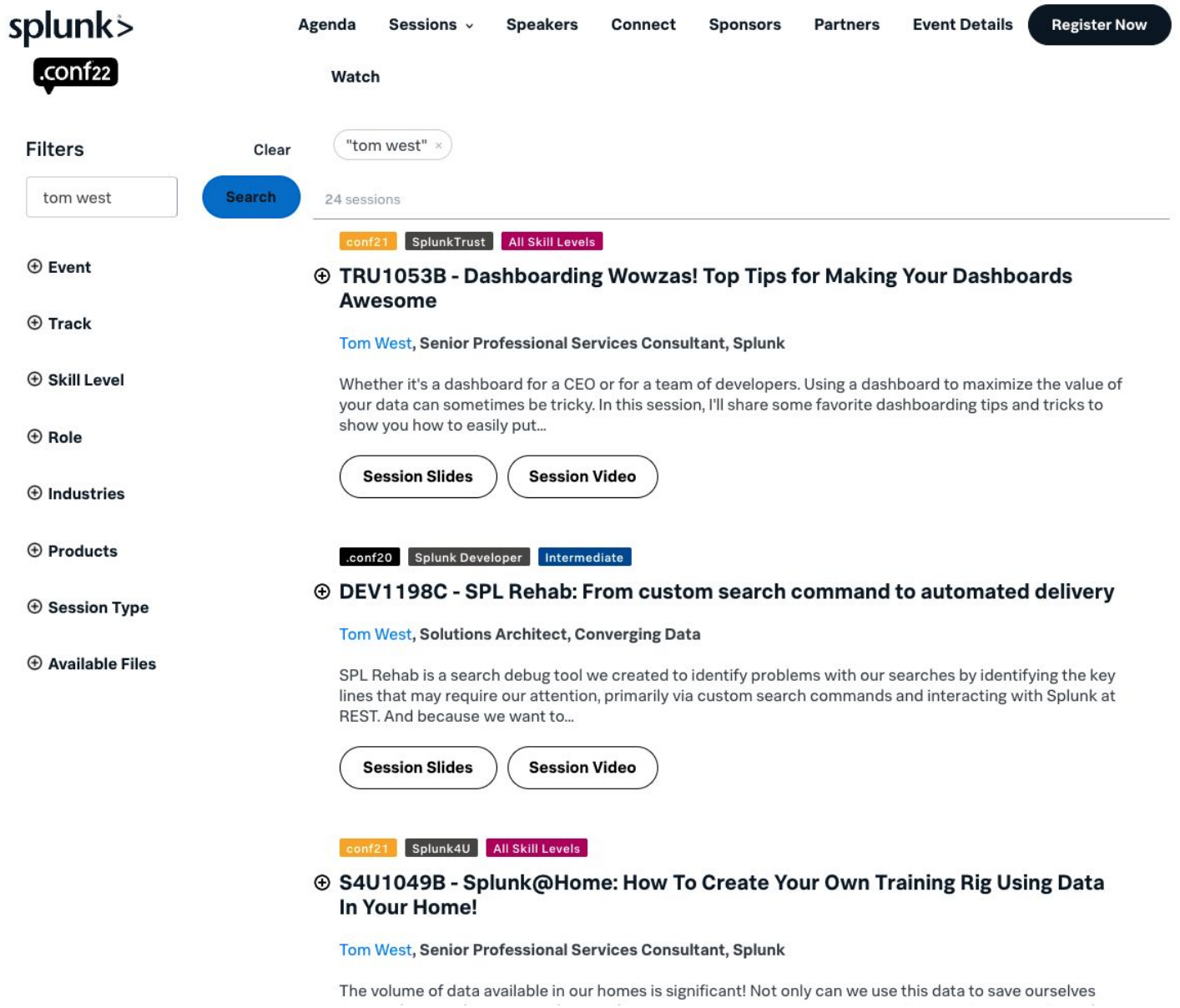
- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



splunk> .conf22

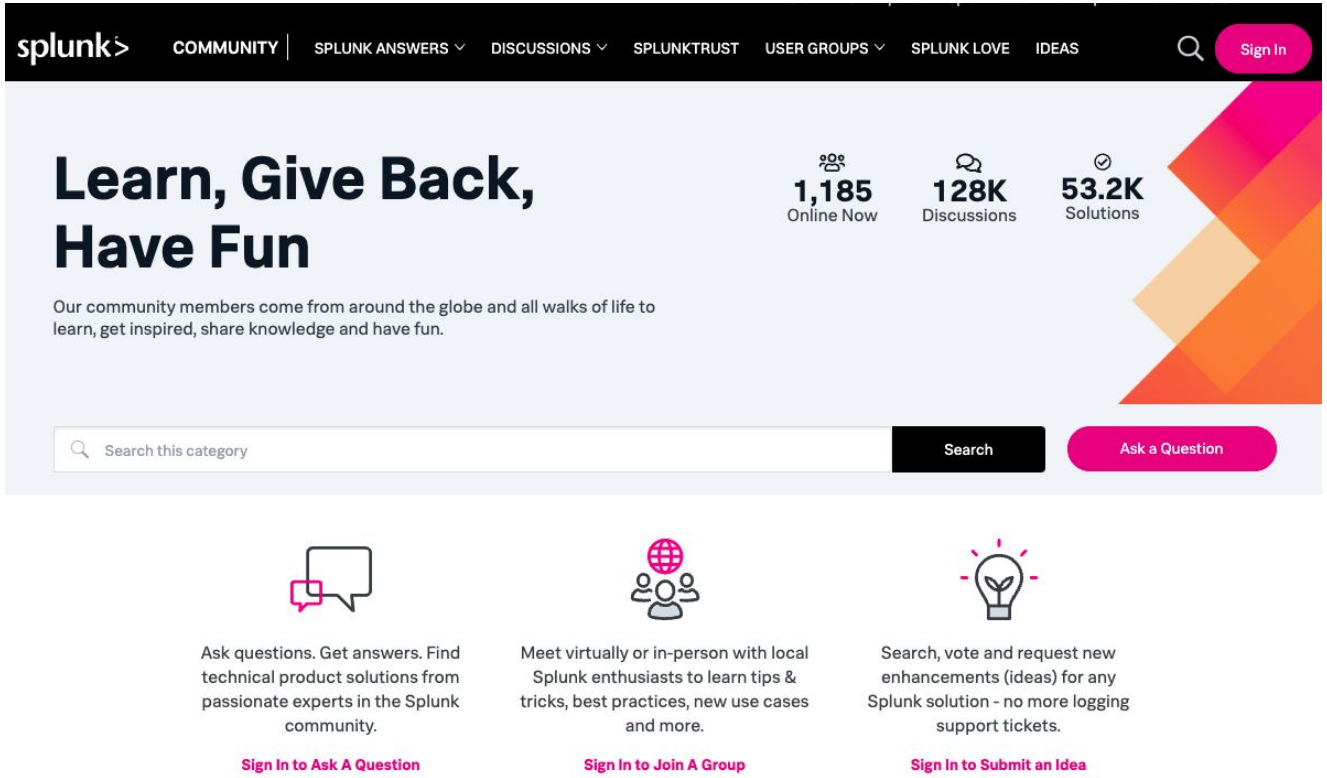
Resources

- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



Resources

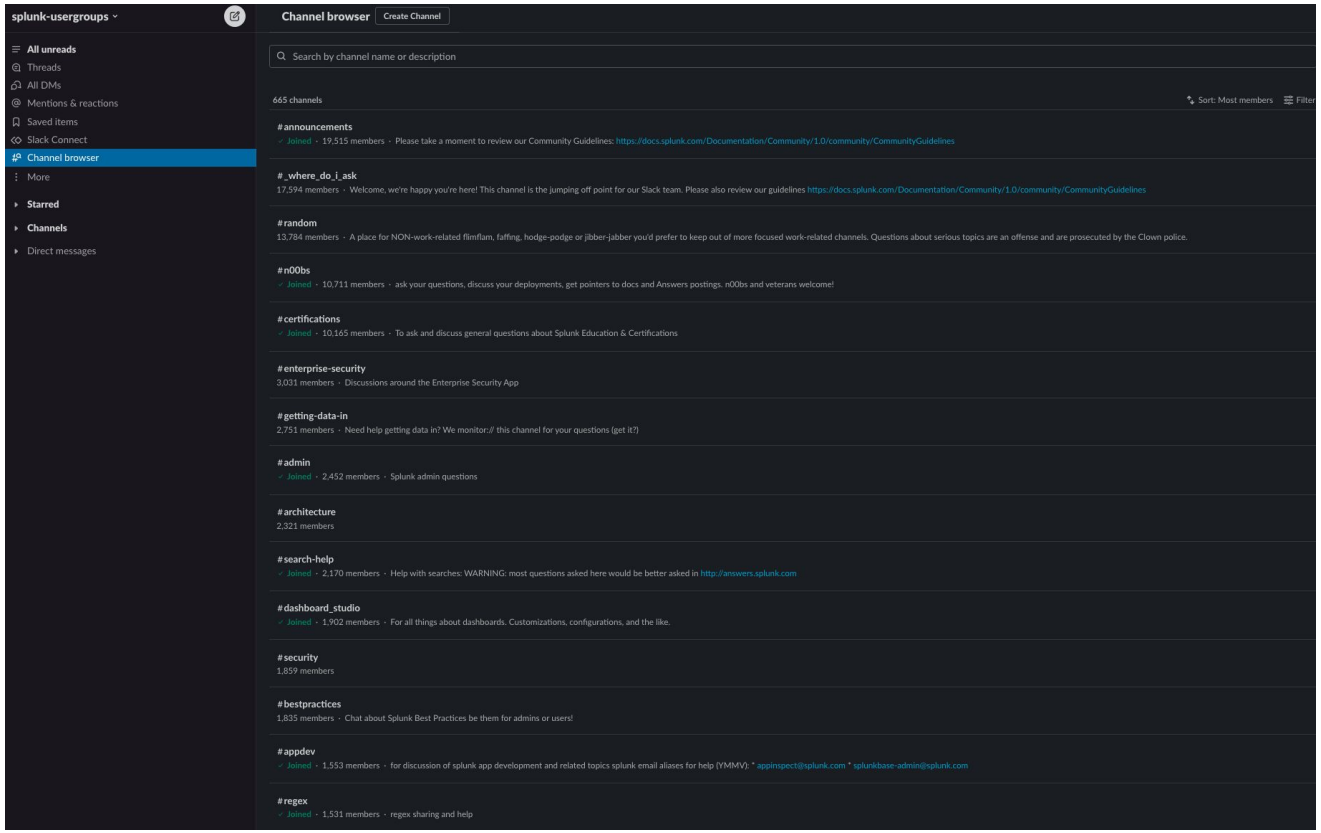
- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



splunk> .conf22

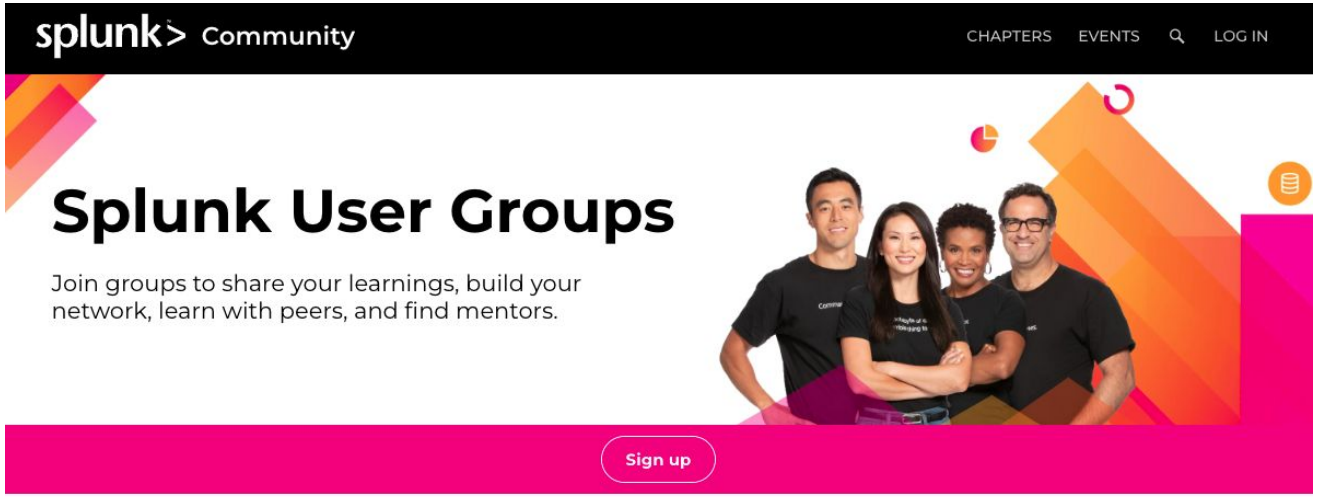
Resources

- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



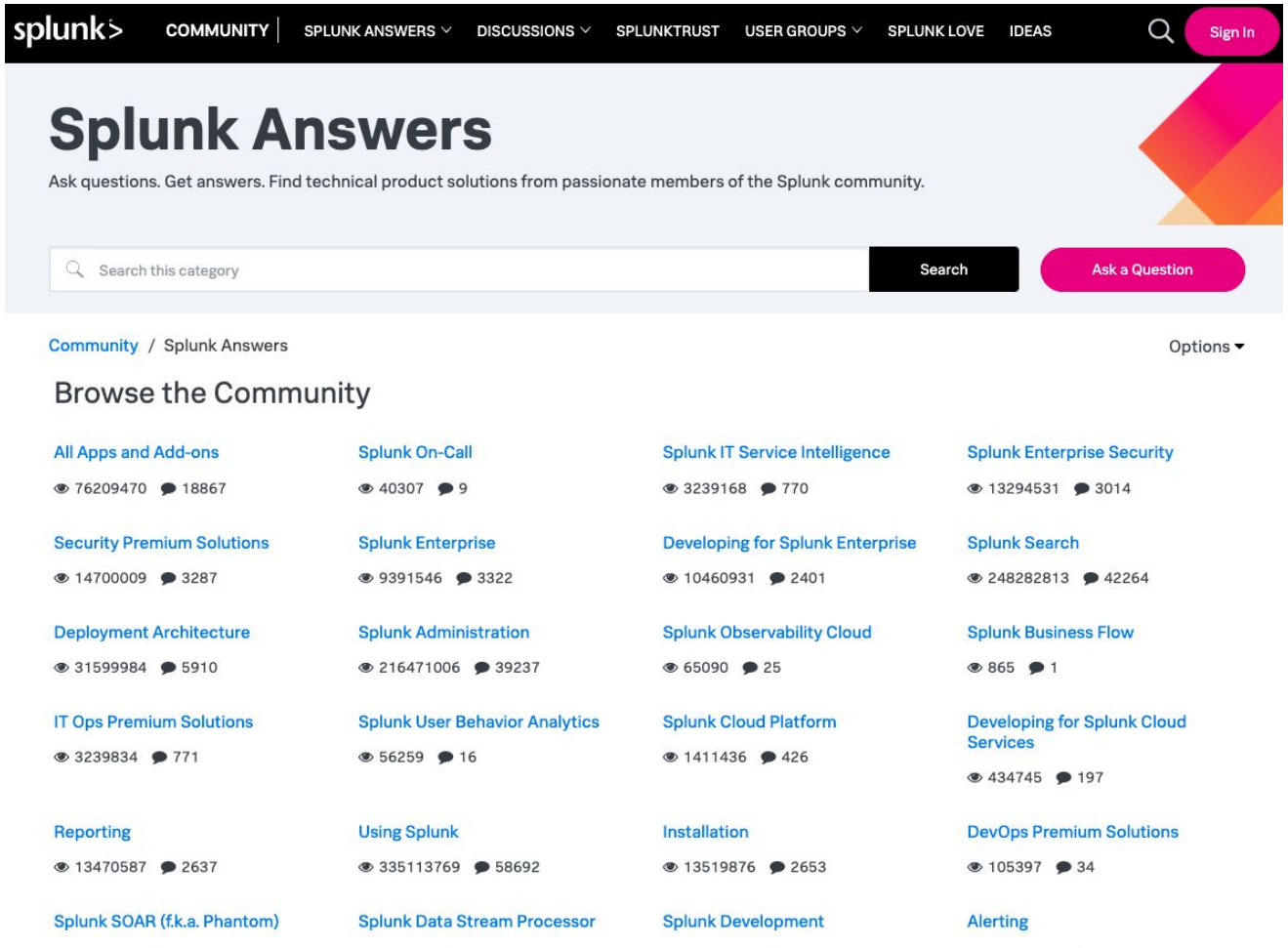
Resources

- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



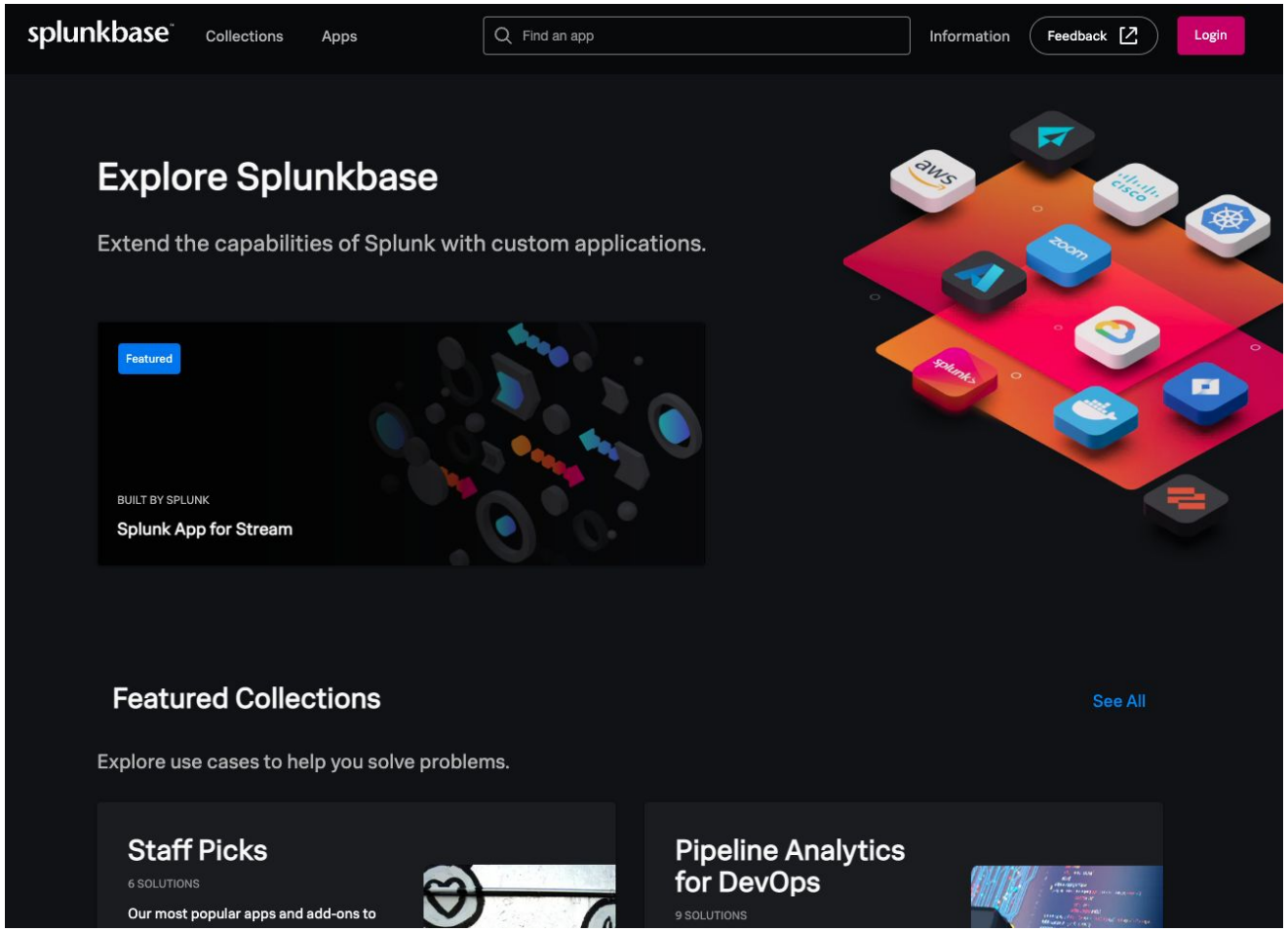
Resources

- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



Resources

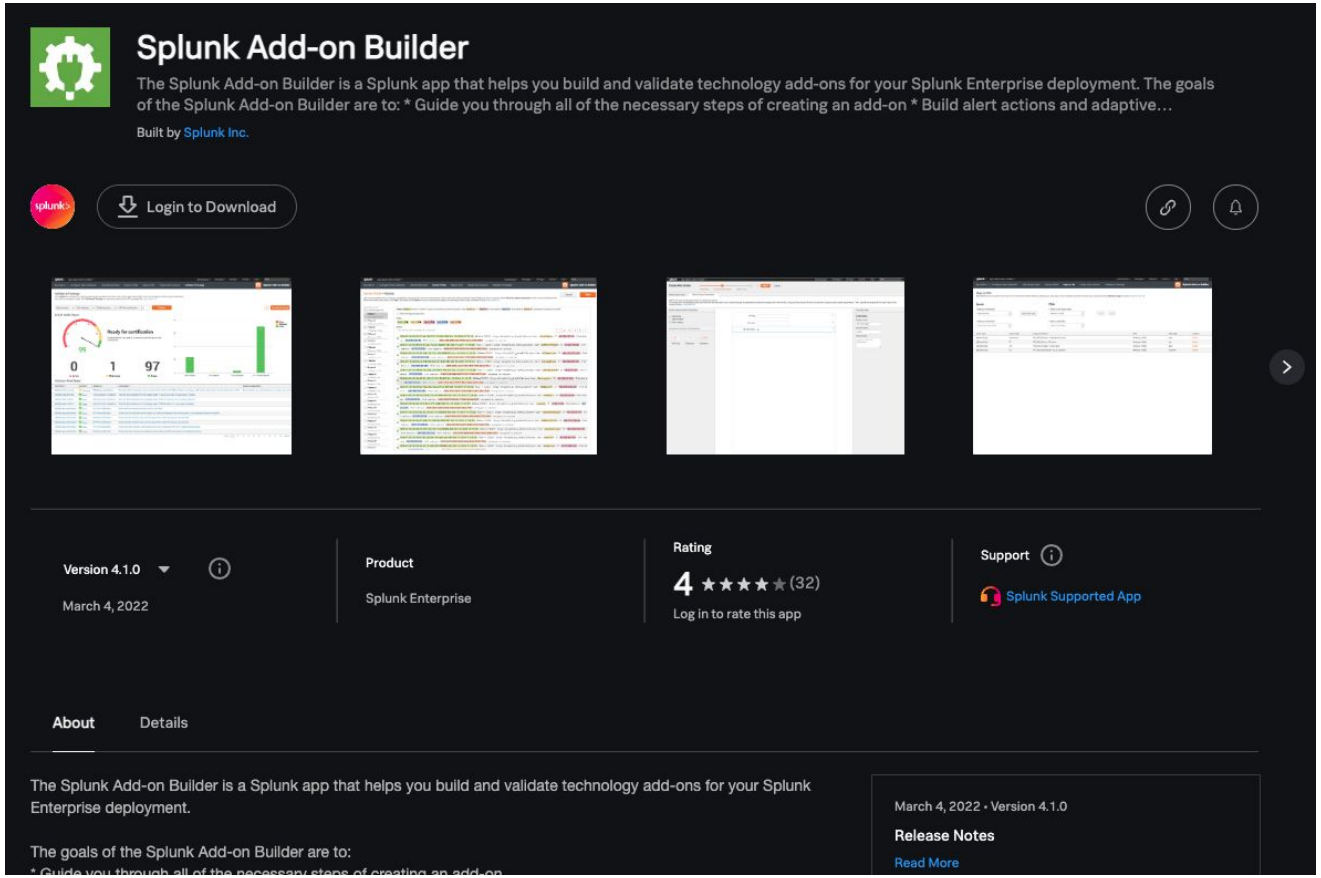
- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



splunk> .conf22

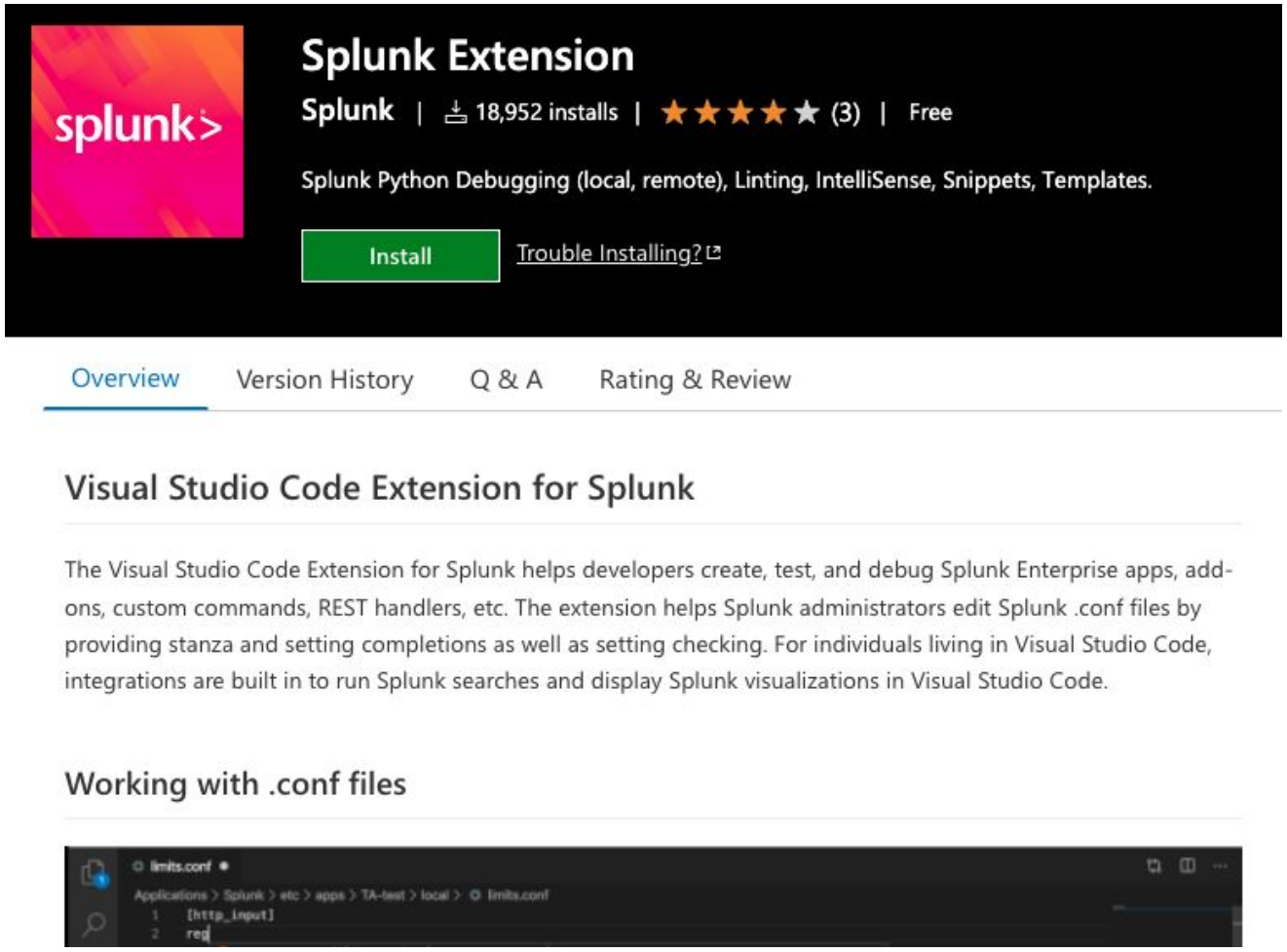
Resources

- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



Resources

- Documentation: DEV.SPLUNK.COM
- Dev License
- .conf Playback
- Community:
  - Slack - splk.it/slack (#AppDev)
  - User Groups
  - Answers
- Splunkbase™
- Add-on Builder
- VS Code Splunk Extension



Note: Screenshot is from Microsoft Marketplace.

Add-ons (TA)

splunk> .conf22

Apps v Add-ons

Add-ons (TA)

Apps

Contains objects which are directly used and interacted with by the user.

- Views
- Saved Searches
- Lookups

Add-ons

To aid with onboarding data and/or enhance the capabilities of other apps within your Splunk system.

Both found in ***/%SPLUNK_HOME%/etc/apps***

splunk> App: Splunk App for AWS | Power User | 1 Messages | Settings | Activity | Help

Overview | Topology | Usage | Security | Billing | Search | Configure | Splunk App for AWS

Estimated Billing - Current Month

Edit | More Info

Account ID: All

Currency: USD

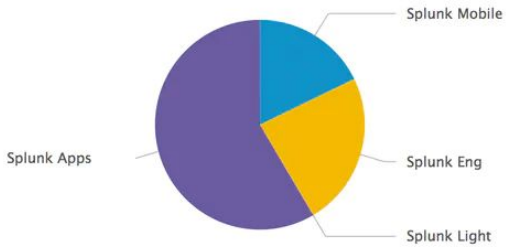
Estimated Cost - Month to Date

$33,419

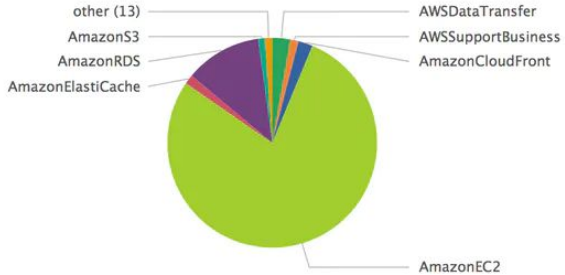
Total Projected Cost - This Month

$41,373

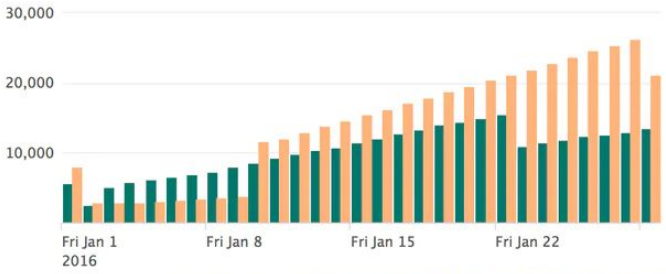
Estimated Cost by Account



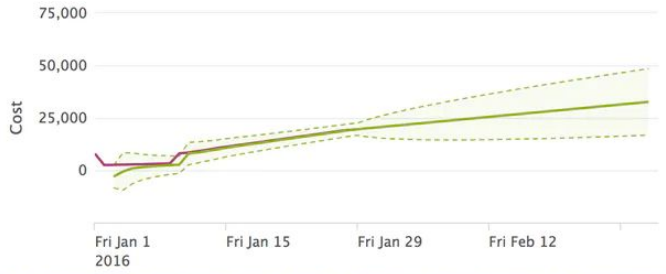
Estimated Cost by Service



Month over Month Comparison - Daily Cost



Cost Projection Over Time



Estimated Cost by Account and Service - Month to Date

Account ID	Account Name	Service	Cost	Percentage
737126726831	Splunk Cloud OPS	AmazonEC2	$13928	41.68%
063605715280	Splunk Mobile	AmazonEC2	$5565	16.65%
111353726070			$3940	11.79%
111353726070		AmazonEC2	$3571	10.69%
737126726831	Splunk	AmazonRDS	$3445	10.31%

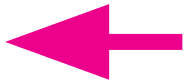
splunk> .conf22

Add-on Builder

Add-ons (TA)

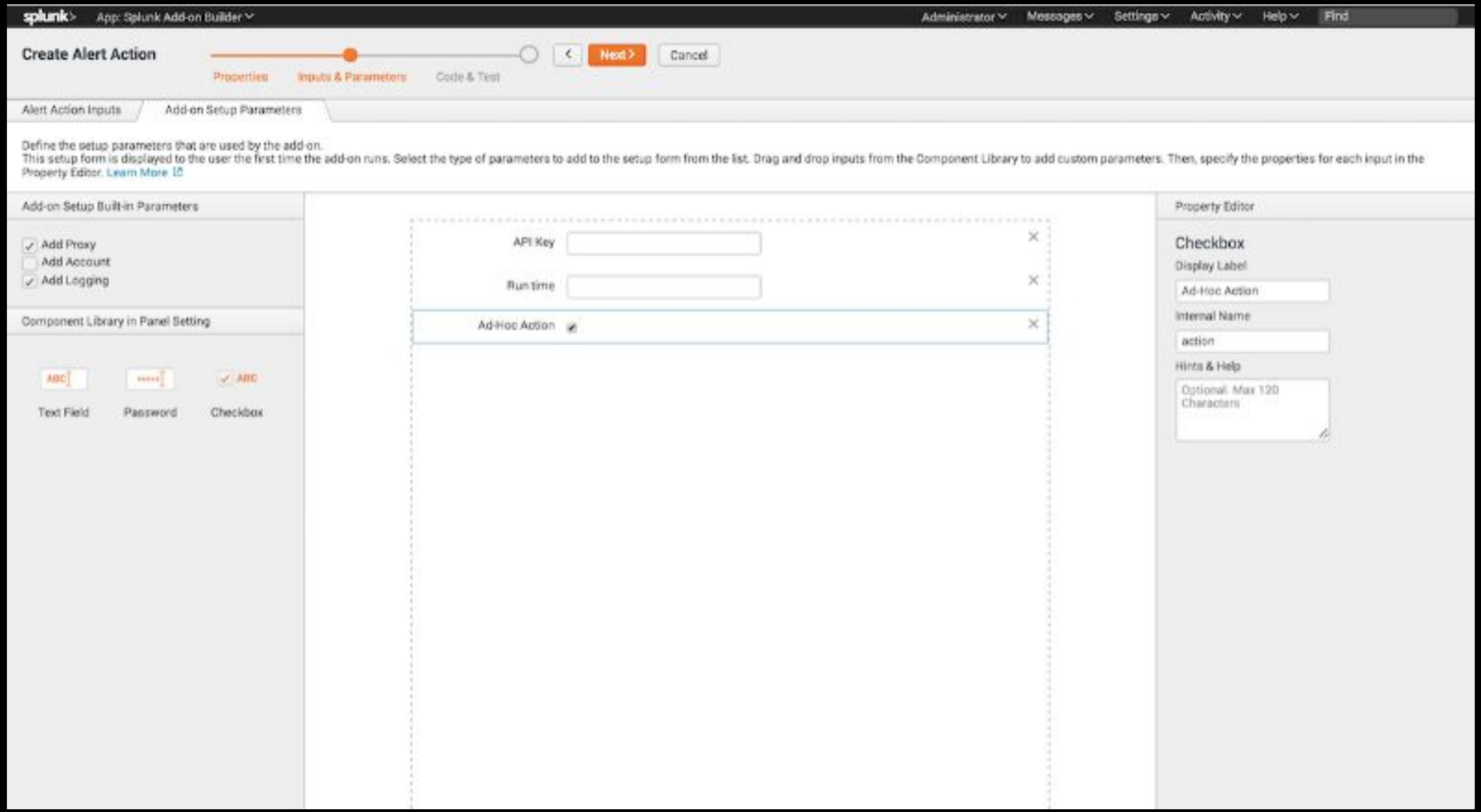
Methods:

- UI

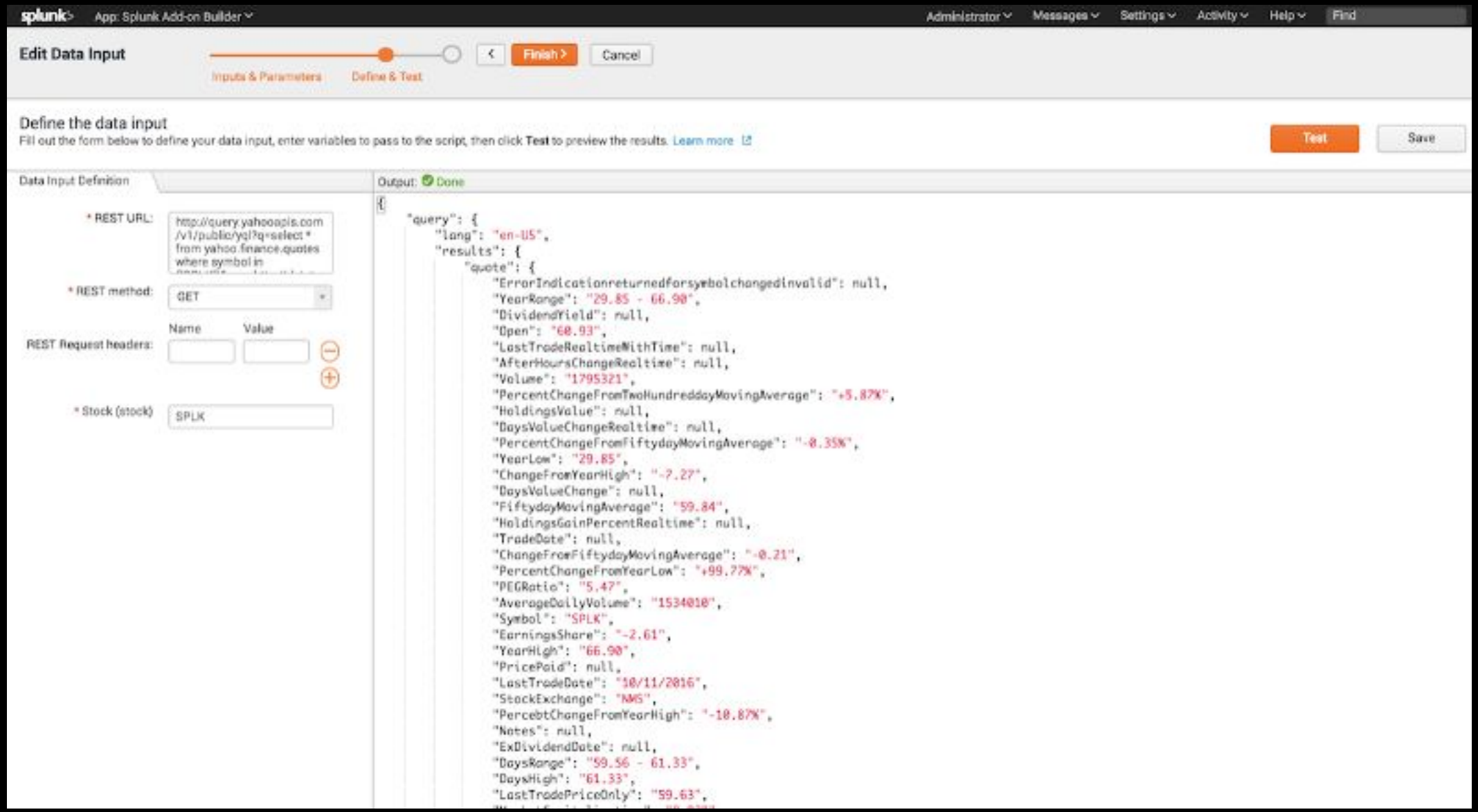


- Script

- Python
  - Allowing for far more advanced data collection (Multiple Endpoints, OAuth, etc)



splunk> .conf22

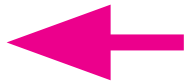


splunk> .conf22

Add-on Builder

Add-ons (TA)

Methods:

- UI
- Script 
- Python
  - Allowing for far more advanced data collection (Multiple Endpoints, OAuth, etc)

Add-on Builder

Add-ons (TA)

Methods:

- UI
- Script
- Python
  - Allowing for far more advanced data collection (Multiple Endpoints, OAuth, etc)

Add-on Builder

Add-ons (TA)

Other Benefits

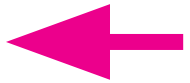
- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app

Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app

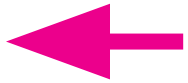


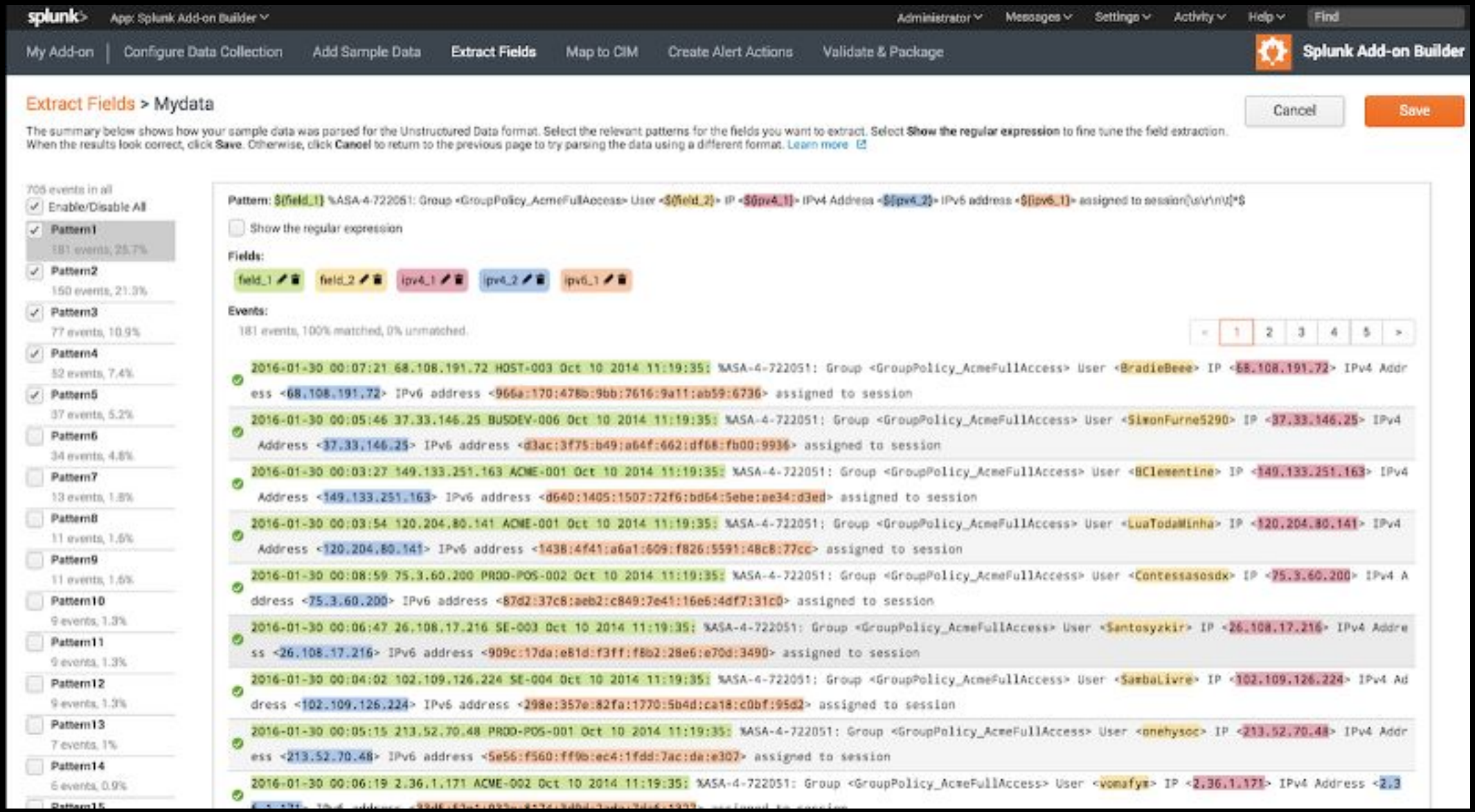
Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app





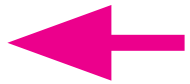
splunk> .conf22

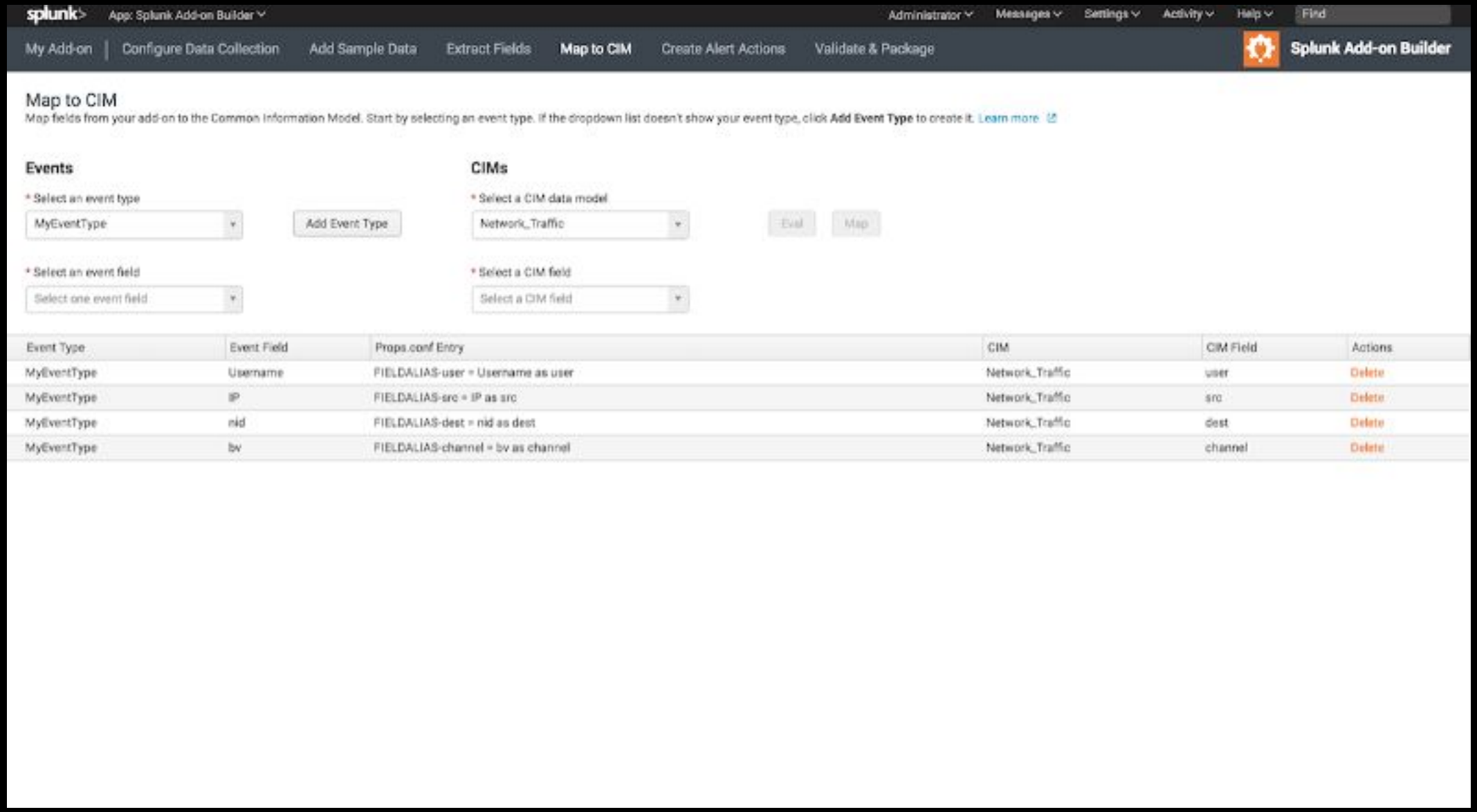
Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app



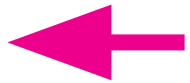


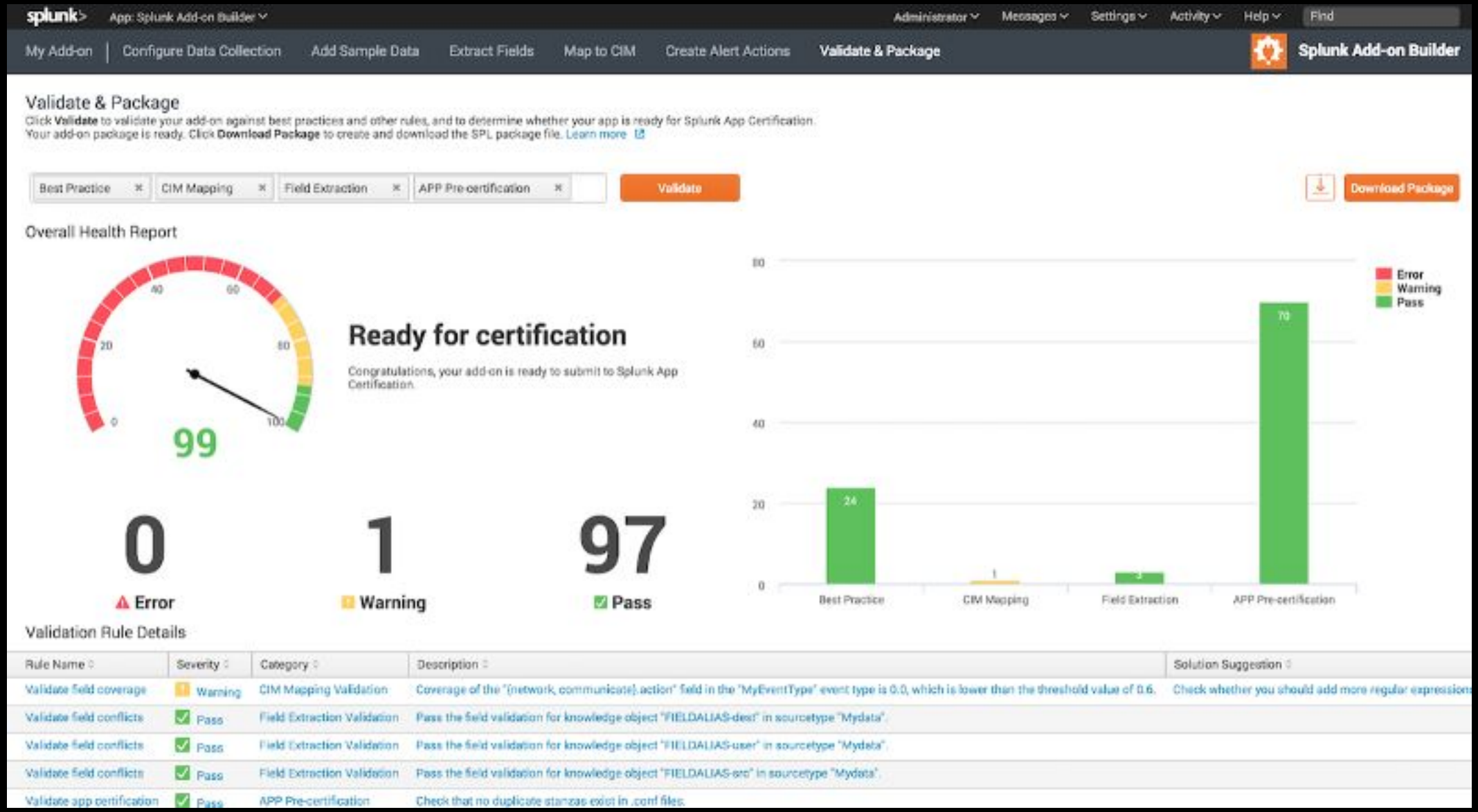
Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app



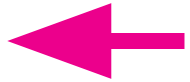


splunk> .conf22

Considerations

Add-ons (TA)

Points to be aware of:

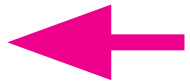
- Ensure tokens/secrets are securely stored 
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation

Considerations

Add-ons (TA)

Points to be aware of:

- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation

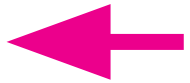


Considerations

Add-ons (TA)

Points to be aware of:

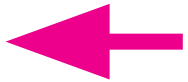
- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation



Considerations

Add-ons (TA)

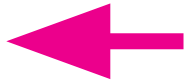
Points to be aware of:

- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up 
- User documentation

Considerations

Add-ons (TA)

Points to be aware of:

- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation 

HTTP Event Collector

Add-ons (TA)

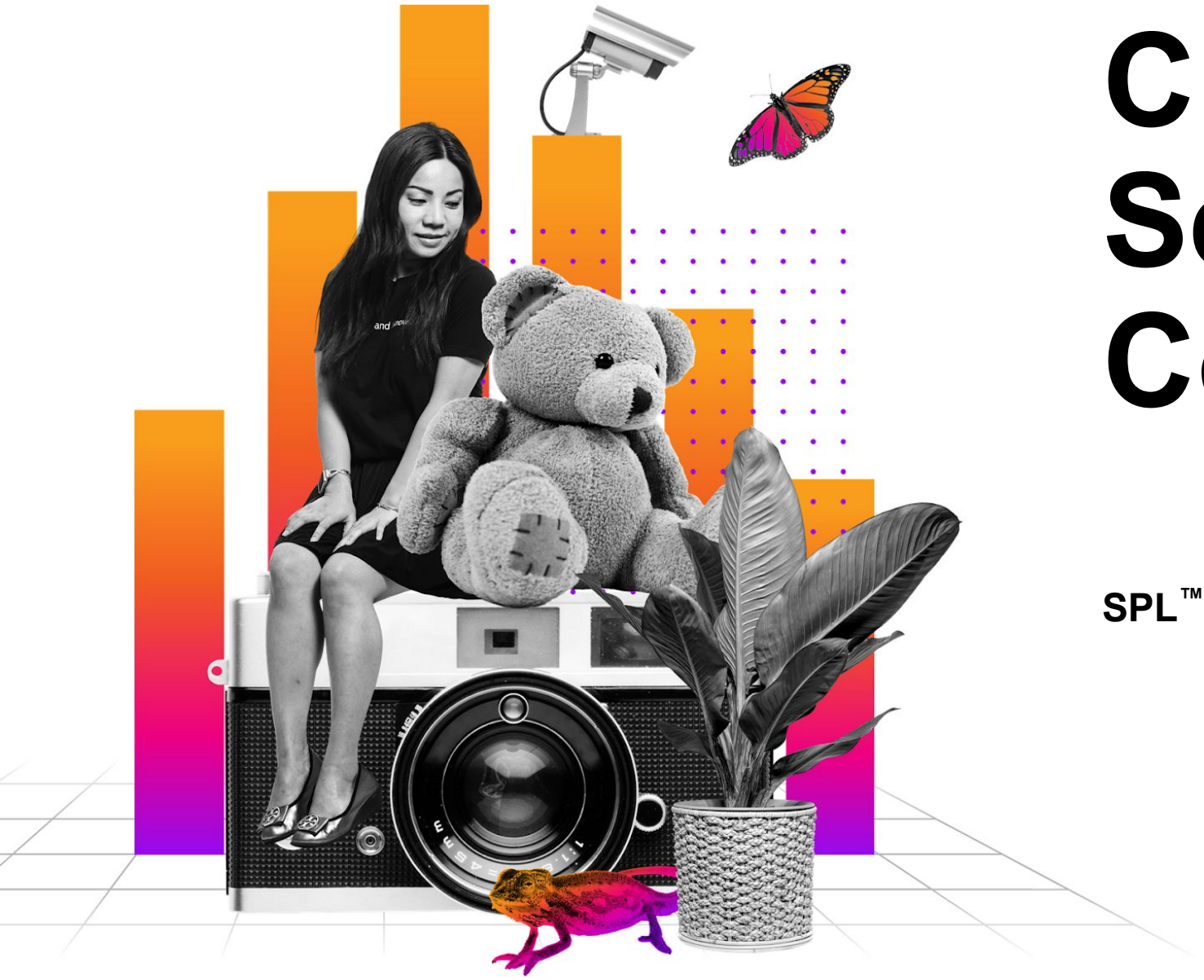
```
curl -k  https://hec.example.com:8088/services/collector/event
  – H "Authorization: Splunk B5A79AAD-D822-46CC-80D1-819F80D7BFB0"
  – d '{"event": "hello world"}'
```

Resources

Add-ons (TA)

Links:

- Modular Input Documentation
- Add-On Builder
  - User Guide
- HEC
  - Splunk Enterprise
  - Splunk Dev



Custom Search Commands

SPL™ Friends!!!!

splunk> .conf22

Custom Search Commands

Build your own search command for use within a splunk search

Types:

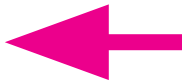
- Streaming
  - Distributable (Eval / Fields / Where)
  - Centralized (Head / Streamstats / Dedup)
- Transforming
  - Stats / Chart / Timechart
- Generating
  - search / inputlookup / tstats / makeresults
- Dataset Processing
  - sort / eventstats

Custom Search Commands

Build your own search command for use within a splunk search

Types:

- Streaming
  - Distributable (Eval / Fields / Where)
  - Centralized (Head / Streamstats / Dedup)
- Transforming
  - Stats / Chart / Timechart
- Generating
  - search / inputlookup / tstats / makeresults
- Dataset Processing
  - sort / eventstats



Custom Search Commands

Build your own search command for use within a splunk search

Types:

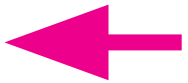
- Streaming
  - Distributable (Eval / Fields / Where)
  - Centralized (Head / Streamstats / Dedup)
- Transforming
  - Stats / Chart / Timechart
- Generating
  - search / inputlookup / tstats / makeresults
- Dataset Processing
  - sort / eventstats

Custom Search Commands

Build your own search command for use within a splunk search

Types:

- Streaming
  - Distributable (Eval / Fields / Where)
  - Centralized (Head / Streamstats / Dedup)
- Transforming
  - Stats / Chart / Timechart
- Generating
  - search / inputlookup / tstats / makeresults
- Dataset Processing
  - sort / eventstats



How To Create One

Custom Search Commands

commands.conf Your own code

Commands.conf

Custom Search Commands

```
[COMMAND_NAME]
filename = your_file_here.ext
```

Supported Executable Formats

Custom Search Commands

Extensions

- bat
- cmd
- exe
- js
- pl
- py
- sh

Available SDK

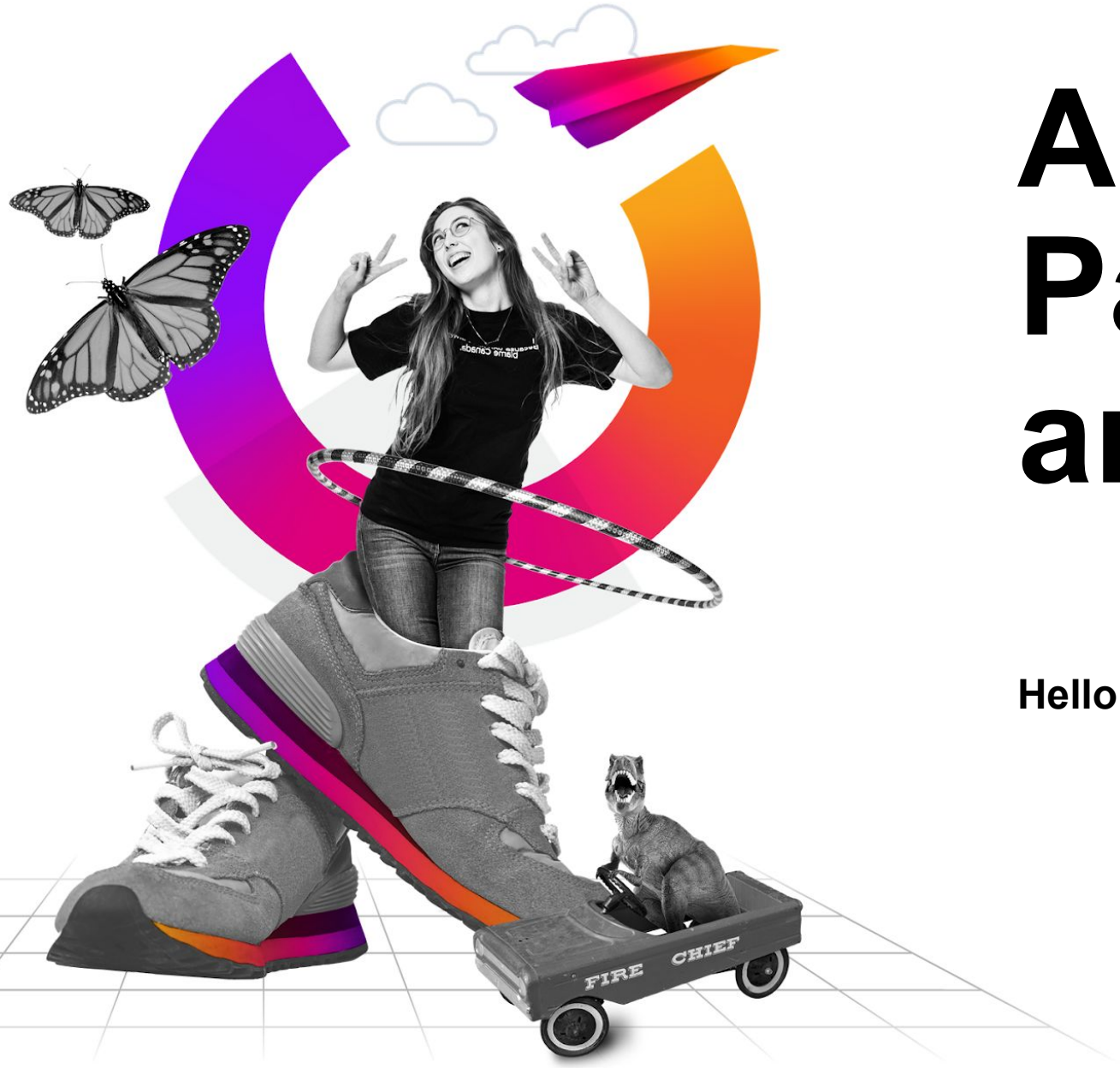
- Python

Resources

Custom Search Commands

Links

- Overview
- Non-Python
- Examples



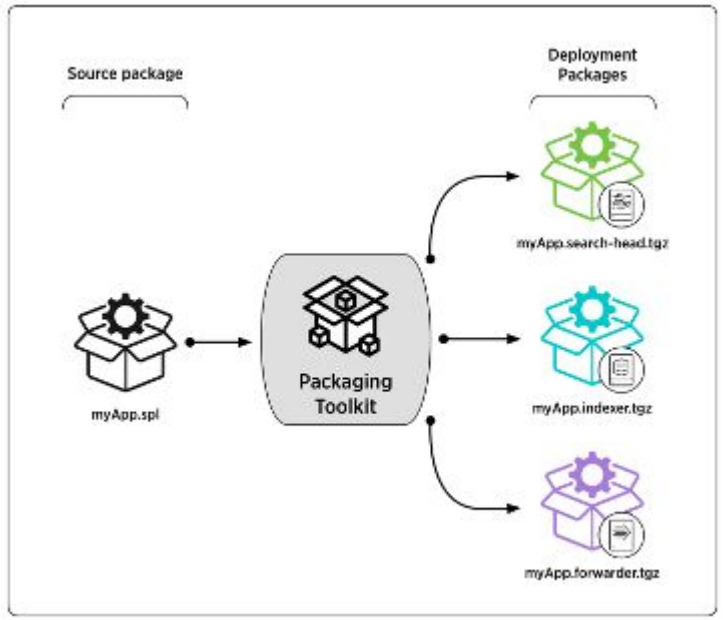
App Packaging and Review

Hello World!

splunk> .conf22

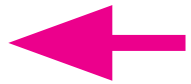
App Packaging

- Splunk® Packaging Toolkit
- Splunk® Enterprise CLI Command
- Manually



App Packaging

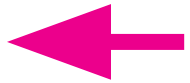
- Splunk® Packaging Toolkit
- Splunk® Enterprise CLI Command
- Manually



```
splunk package app <appname>
```

App Packaging

- Splunk® Packaging Toolkit
- Splunk® Enterprise CLI Command
- Manually



```
COPYFILE_DISABLE=1 tar -cvzf <appname>.tar.gz <appname_directory>
```

AppInspect

Automated App Review

Available In

- CLI
- API

```
pip install splunk-appinspect
```

```
splunk-appinspect inspect <APP-PACKAGE>
```

AppInspect

Automated App Review

Available In

- CLI
- API

```
curl -k -u <USERNAME> \
     --url "https://api.splunk.com/2.0/rest/login/splunk"
```

```
curl -X POST \
     -H "Authorization: bearer <TOKEN>" \
     -H "Cache-Control: no-cache" \
     -F "app_package=@\"/<PATH/APP-PACKAGE>\\"" \
     --url "https://appinspect.splunk.com/v1/app/validate"
```

Resources

Packaging

Links

- Deployment Architecture
- Packaging Apps
- AppInspect

Resources

More from me

.conf22

- PLA1128 - Dashboarding Wowzas! Getting to know Splunk Dashboard Studio
- PLA1455 - Splunk is in the Lobby! How the McLaren Shadow Team Use Splunk to Level Up F1 eSports Performance

.conf Online Catalog

- DEV1198 - SPL Rehab: From Custom Search Command to Automated Delivery
- TRU1053 - Dashboarding Wowzas! Top Tips for Making Your Dashboards Awesome
- S4U1049 - Splunk@Home: How to Create Your Own Training Rig Using Data In Your Home!

Resources

More @ .conf22

- Builder Bar
- Talks
  - DEV1168 - Best Practices and Better Practices for Splunk Development
  - DEV1385 - Debug Deep Dive: Using Visual Studio Code to Debug Splunk Code Wherever it Runs
  - DEV1160 - Forget Add-On Builder! Build Splunk Platform Apps with Config Explorer!
  - DEV1204 - Making Your Splunk App Look Sweet With SUIT
  - DEV1703 - How Expedia Manages and Deploys Over 2000 Apps Using CI/CD and AppInspect

Thank You

splunk> .conf22