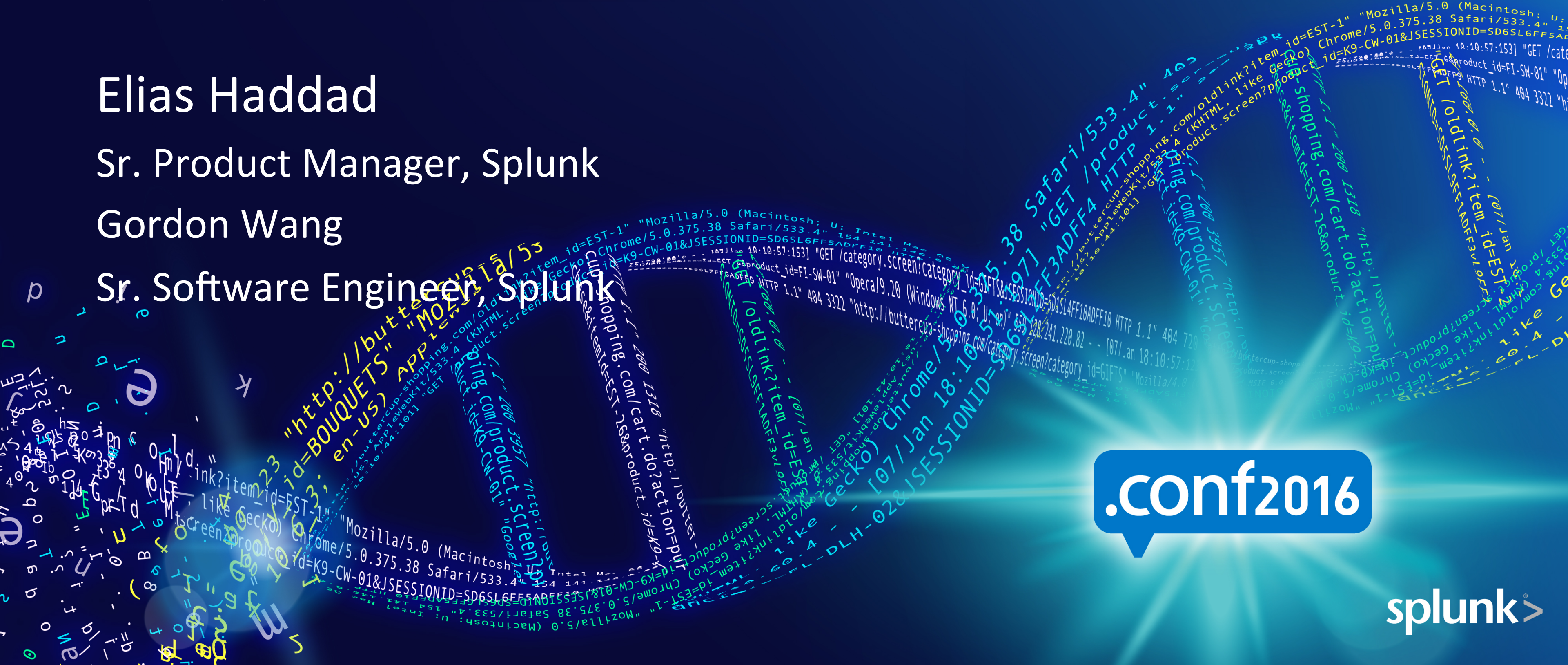
Onboard your data faster with Add-on Builder

Elias Haddad

Sr. Product Manager, Splunk

Gordon Wang

Sr. Software Engineer, Splunk



.conf2016

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.

Agenda

- Why Add-on Builder
- What is Add-on Builder
- Features Highlights
- What’s new in Add-on Builder 2.0
- Demo
- Q&A

All Data is Relevant

Databases

Email

Web

Desktops

Servers

DHCP/ DNS

Network Flows

Hypervisor

Badges

Firewall

Authentication

Vulnerability Scans

Custom Apps

Service Desk

Storage

Mobile

Intrusion Detection

Data Loss Prevention

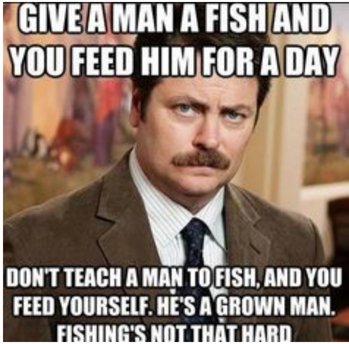
Anti-Malware

Industrial Control

Call Records

Why Add-on Builder

- **Expand the ecosystem** of Partners, Vendors, and Customers building Add-ons
- **Reduce the time** spent by engineers building one-off Add-ons
- Improve **consistency** and adherence to **best practices**
- Enable Development Partners with the **right tools** to be **successful**
- **Accelerate development beyond what we can do alone**


GIVE A MAN A FISH AND YOU FEED HIM FOR A DAY
DON'T TEACH A MAN TO FISH, AND YOU FEED YOURSELF. HE'S A GROWN MAN. FISHING'S NOT THAT HARD

Refresher: What is an Add-on?

- Data Collection – Modular Input
- Abstraction layer:
  - Field Extraction
  - CIM, Domain Add-on Mapping
  - Indexed-time extraction
- Data Enrichment using lookups
- Modular Alerts
- Saved Searches
- Pre-Built Panels

What is Add-on Builder

- Splunk Add-on Builder is an App on Splunkbase:
  - https://splunkbase.splunk.com/app/2962/
- The goals of the Splunk Add-on Builder are to:
  - Guide you through all of the necessary steps of creating an add-on
  - Reduce development and testing time
  - Follow best practices and naming conventions
  - Maintain CIM compliance
  - Maintain quality of add-ons
  - Validate and test the add-on, helping you to identify any limitations such as compatibilities and dependencies
  - Maintain a consistent look and feel while still making it easy for you to add branding

What does Splunk Add-on Builder do?

Automate code generation

- Intuitive and process driven UI
- Supports multiple input types, including shell, REST, and Splunk Python SDK

Extract and Map fields

- Extract fields using automated event analysis
- Map fields to CIM with click of button

Score Health of Add-on

- Validate for CIM compliance and naming conventions (best practices?)
- Detect problems with field extraction

Create Add-on using step by step process

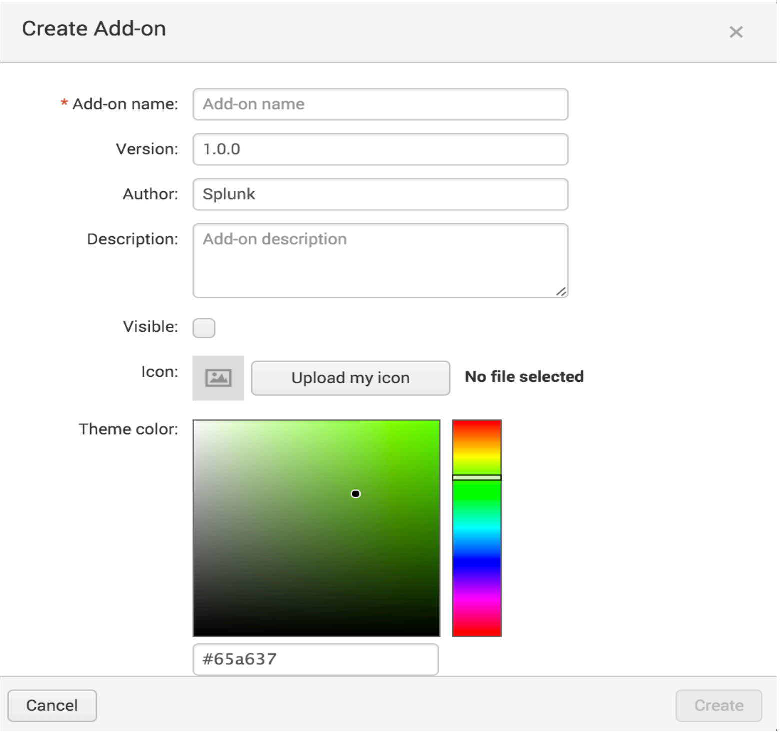
Add-on Builder Feature Highlights

- Version 2.0.0 Features Highlight

UI based Add-on creation

Show via demo

- UI Based Add-on creation
- Maintains a consistent look and feel while still making it easy for you to add branding
- Upload your add-on Logo and pick your color theme



Create Add-on ×

* Add-on name: Add-on name

Version: 1.0.0

Author: Splunk

Description: Add-on description

Visible: □

Icon: Upload my icon No file selected

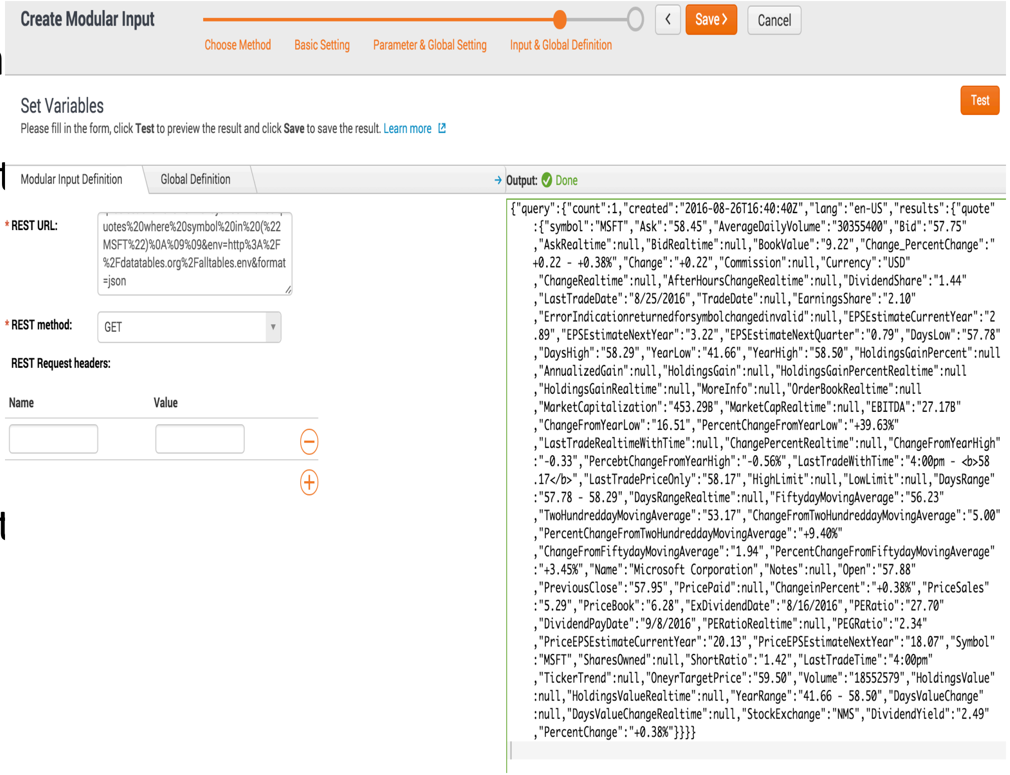
Theme color: #65a637

Cancel Create

Modular Input

Show via demo

- Modular Input ease of creation
- If you have simple REST API:
  - We can generate the mod input for you without writing a single line of code.
  - Can be tokenized
- If you have shell command or script
  - We will generate the mod input for you
  - Can be tokenized
- Real time code validation



Set Variables

Please fill in the form, click **Test** to preview the result and click **Save** to save the result. Learn more

* REST URL: uotes%20where%20symbol%20in%20(%22MSFT%22)%0A%09%09&env=http%3A%2F%2Fdatatables.org%2Falltables.env&format=json

* REST method: GET

REST Request headers:

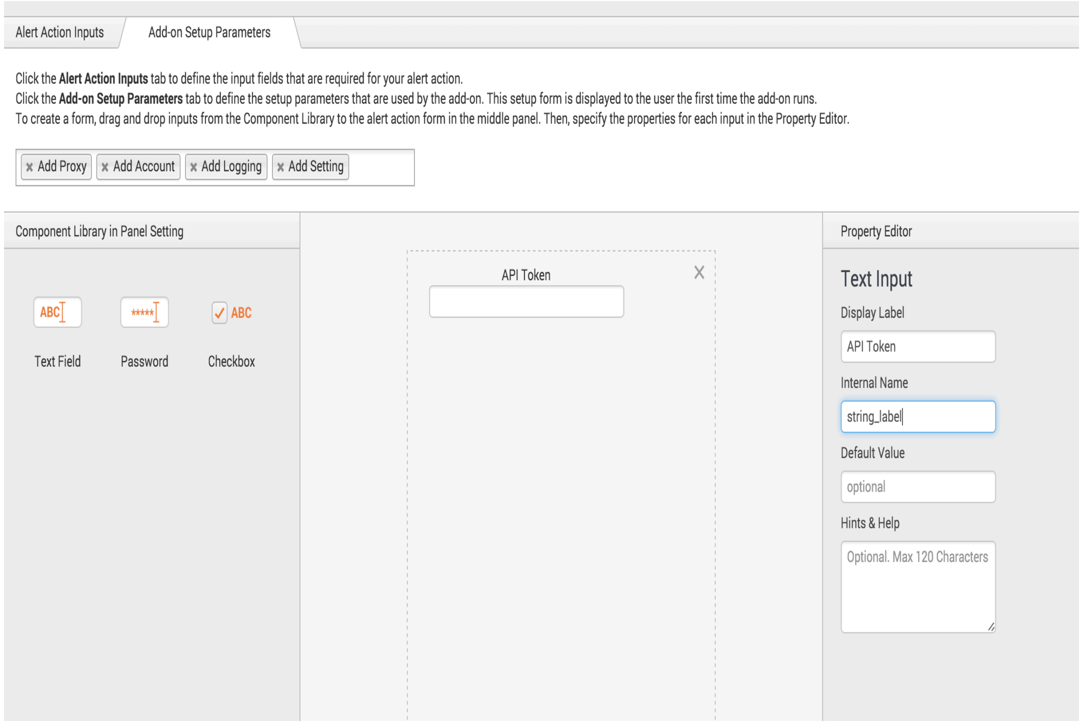
Output: ✓ Done

```
{"query":{"count":1,"created":"2016-08-26T16:40:40Z","lang":"en-US","results":{"quote"
    :{"symbol":"MSFT","Ask":"58.45","AverageDailyVolume":"30355400","Bid":"57.75"
    ,"AskRealtime":null,"BidRealtime":null,"BookValue":"9.22","Change_PercentChange":"
    +0.22 - +0.38%","Change":"+0.22","Commission":null,"Currency":"USD"
    ,"ChangeRealtime":null,"AfterHoursChangeRealtime":null,"DividendShare":"1.44"
    ,"LastTradeDate":"8/25/2016","TradeDate":null,"EarningsShare":"2.10"
    ,"ErrorIndicationreturnedforsymbolchangedinvalid":null,"EPSEstimateCurrentYear":"2
    .89","EPSEstimateNextYear":"3.22","EPSEstimateNextQuarter":"0.79","DaysLow":"57.78"
    ,"DaysHigh":"58.29","YearLow":"41.66","YearHigh":"58.50","HoldingsGainPercent":null
    ,"AnnualizedGain":null,"HoldingsGain":null,"HoldingsGainPercentRealtime":null
    ,"HoldingsGainRealtime":null,"MoreInfo":null,"OrderBookRealtime":null
    ,"MarketCapitalization":"453.29B","MarketCapRealtime":null,"EBITDA":"27.17B"
    ,"ChangeFromYearLow":"16.51","PercentChangeFromYearLow":"+39.63%"
    ,"LastTradeRealtimeWithTime":null,"ChangePercentRealtime":null,"ChangeFromYearHigh"
    :"-0.33","PercebtChangeFromYearHigh":"-0.56%","LastTradeWithTime":"4:00pm - <b>58
    .17</b>","LastTradePriceOnly":"58.17","HighLimit":null,"LowLimit":null,"DaysRange"
    :"57.78 - 58.29","DaysRangeRealtime":null,"FiftydayMovingAverage":"56.23"
    ,"TwoHundreddayMovingAverage":"53.17","ChangeFromTwoHundreddayMovingAverage":"5.00"
    ,"PercentChangeFromTwoHundreddayMovingAverage":"+9.40%"
    ,"ChangeFromFiftydayMovingAverage":"1.94","PercentChangeFromFiftydayMovingAverage"
    :"+3.45%","Name":"Microsoft Corporation","Notes":null,"Open":"57.88"
    ,"PreviousClose":"57.95","PricePaid":null,"ChangeinPercent":"+0.38%","PriceSales"
    :"5.29","PriceBook":"6.28","ExDividendDate":"8/16/2016","PERatio":"27.70"
    ,"DividendPayDate":"9/8/2016","PERatioRealtime":null,"PEGRatio":"2.34"
    ,"PriceEPSEstimateCurrentYear":"20.13","PriceEPSEstimateNextYear":"18.07","Symbol"
    :"MSFT","SharesOwned":null,"ShortRatio":"1.42","LastTradeTime":"4:00pm"
    ,"TickerTrend":null,"OneyrTargetPrice":"59.50","Volume":"18552579","HoldingsValue"
    :null,"HoldingsValueRealtime":null,"YearRange":"41.66 - 58.50","DaysValueChange"
    :null,"DaysValueChangeRealtime":null,"StockExchange":"NMS","DividendYield":"2.49"
    ,"PercentChange":"+0.38%"}}}}
```

Add-on Setup

Show via demo

- Allows you to generate and build setup page without having to deal with setup.xml.
- Create you setup parameters or select default ones.
- Support multi-account
- Interactive
- Out of the box proxy support, password encryption, logging



Click the **Alert Action Inputs** tab to define the input fields that are required for your alert action.
Click the **Add-on Setup Parameters** tab to define the setup parameters that are used by the add-on. This setup form is displayed to the user the first time the add-on runs.
To create a form, drag and drop inputs from the Component Library to the alert action form in the middle panel. Then, specify the properties for each input in the Property Editor.

Display Label: API Token

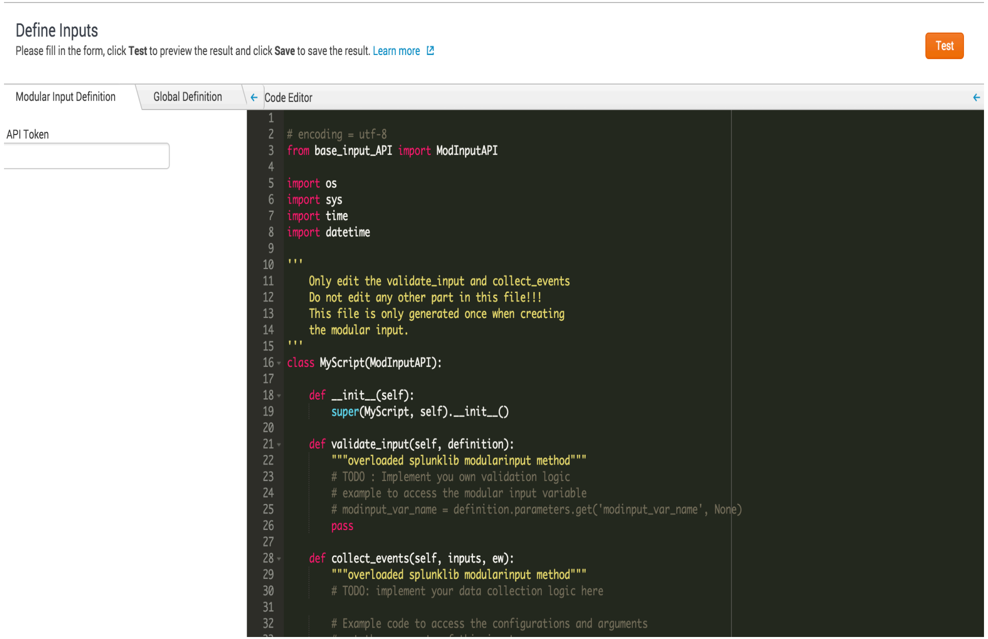
Internal Name: string_label

Default Value: optional

Advanced Modular Input

Show via demo

- If you have more advanced data collection logic
- Real time code validation
- Includes library:
  - Checkpointing
  - Reading encrypted password from storage/password endpoint
  - Proxy
  - Accessing parameter values from setup page



Define Inputs

Please fill in the form, click **Test** to preview the result and click **Save** to save the result. Learn more

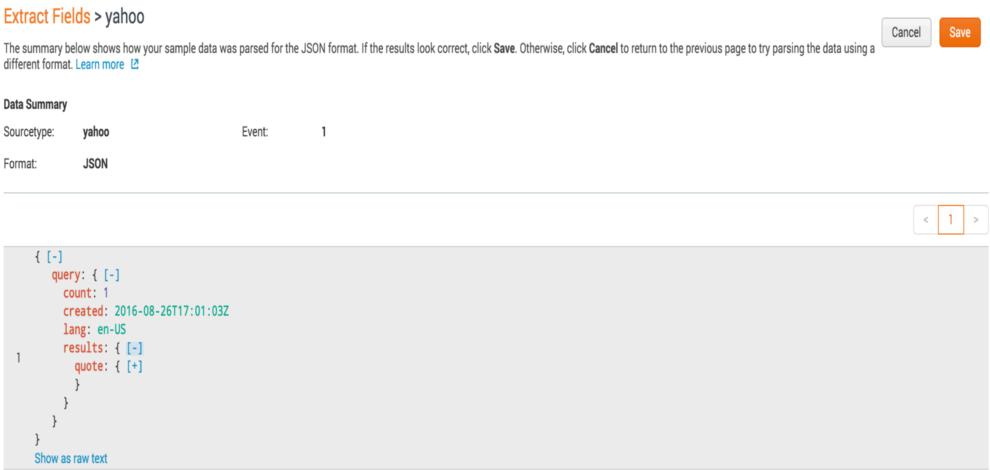
API Token

```

# encoding = utf-8
from base_input_API import ModInputAPI

import os
import sys
import time
import datetime

'''
    Only edit the validate_input and collect_events
    Do not edit any other part in this file!!!
    This file is only generated once when creating
    the modular input.
'''
class MyScript(ModInputAPI):

    def __init__(self):
        super(MyScript, self).__init__()

    def validate_input(self, definition):
        """overloaded splunklib modularinput method"""
        # TODO : Implement you own validation logic
        # example to access the modular input variable
        # modinput_var_name = definition.parameters.get('modinput_var_name', None)
        pass

    def collect_events(self, inputs, ew):
        """overloaded splunklib modularinput method"""
        # TODO: implement your data collection logic here

        # Example code to access the configurations and arguments
```

Field Extraction

Show via demo

- Support various format incl JSON
- Leverages machine learnin based on format similarity
- Automatically generate reg



Extract Fields > yahoo

The summary below shows how your sample data was parsed for the JSON format. If the results look correct, click **Save**. Otherwise, click **Cancel** to return to the previous page to try parsing the data using a different format. Learn more

Data Summary

Sourcetype: **yahoo** Event: 1

Format: **JSON**

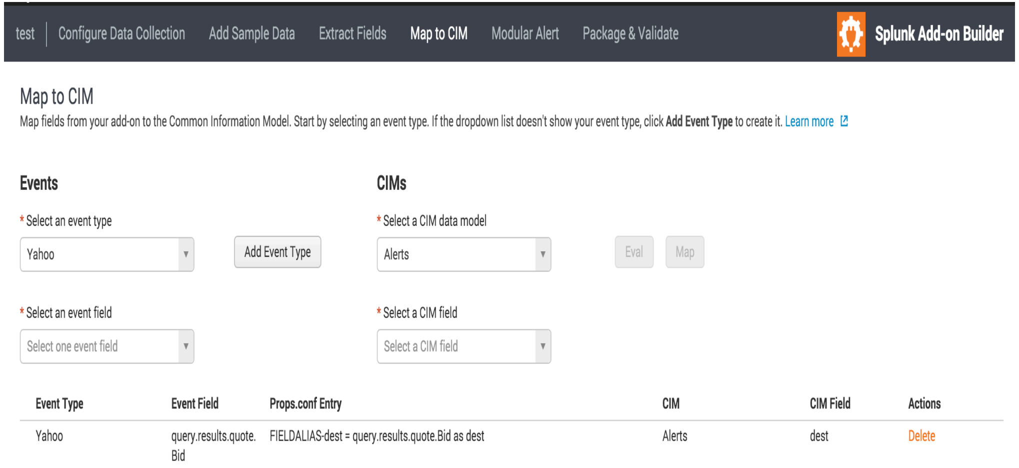
```
1   { [-]
      query: { [-]
        count: 1
        created: 2016-08-26T17:01:03Z
        lang: en-US
        results: { [-]
          quote: { [+]
          }
        }
      }
    }
```

Show as raw text

CIM Mapping

Show via demo

- UI based CIM mapping
- Map your Add-on fields to the Common information model in a click of a button



Map to CIM

Map fields from your add-on to the Common Information Model. Start by selecting an event type. If the dropdown list doesn't show your event type, click **Add Event Type** to create it. Learn more

Events

* Select an event type: Yahoo

Add Event Type

* Select an event field: Select one event field

CIMs

* Select a CIM data model: Alerts

Eval Map

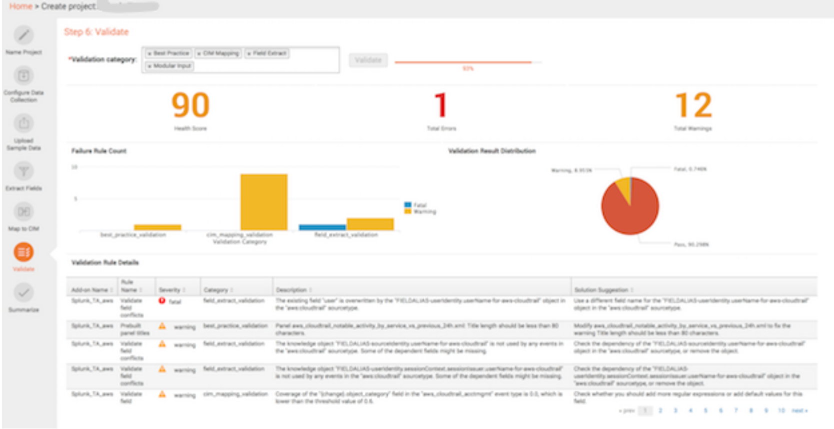
* Select a CIM field: Select a CIM field

Event Type	Event Field	Props.conf Entry	CIM	CIM Field	Actions
Yahoo	query.results.quote.Bid	FIELDALIAS-dest = query.results.quote.Bid as dest	Alerts	dest	Delete

Health Validation

Show via demo

- Validate you Add-on for:
  - Best practices
  - CIM compliance
- Detect any field extraction problems
- Detect any problems with you modular inputs
- Certification readiness on roadmap



Home > Create project [redacted]

Step 6: Validate

*Validation category: × Best Practice × CIM Mapping × Field Extract × Modular Input

90 Health Score

1 Total Errors

12 Total Warnings

Validation Rule Details

Add-on Name	Rule Name	Severity	Category	Description	Solution Suggestion
Splunk_TA_aws	Validate field conflicts	fatal	field_extract_validation	The existing field "user" is overwritten by the "FIELDALIAS-useridentity.userName-for-aws-cloudtrail" object in the "aws:cloudtrail" sourcetype.	Use a different field name for the "FIELDALIAS-useridentity.userName-for-aws-cloudtrail" object in the "aws:cloudtrail" sourcetype.
Splunk_TA_aws	Prebuilt panel titles	warning	best_practice_validation	Panel aws_cloudtrail_notable_activity_by_service_vs_previous_24h.xml: Title length should be less than 80 characters.	Modify aws_cloudtrail_notable_activity_by_service_vs_previous_24h.xml to fix the warning Title length should be less than 80 characters.
Splunk_TA_aws	Validate field conflicts	warning	field_extract_validation	The knowledge object "FIELDALIAS-sourceidentity.userName-for-aws-cloudtrail" is not used by any events in the "aws:cloudtrail" sourcetype. Some of the dependent fields might be missing.	Check the dependency of the "FIELDALIAS-sourceidentity.userName-for-aws-cloudtrail" object in the "aws:cloudtrail" sourcetype, or remove the object.
Splunk_TA_aws	Validate field conflicts	warning	field_extract_validation	The knowledge object "FIELDALIAS-useridentity.sessionContext.sessionIssuer.userName-for-aws-cloudtrail" is not used by any events in the "aws:cloudtrail" sourcetype. Some of the dependent fields might be missing.	Check the dependency of the "FIELDALIAS-useridentity.sessionContext.sessionIssuer.userName-for-aws-cloudtrail" object in the "aws:cloudtrail" sourcetype, or remove the object.
Splunk_TA_aws	Validate field	warning	cim_mapping_validation	Coverage of the "[change].object_category" field in the "aws_cloudtrail_acctmgmt" event type is 0.0, which is lower than the threshold value of 0.6.	Check whether you should add more regular expressions or add default values for this field.

« prev 1 2 3 4 5 6 7 8 9 10 next »

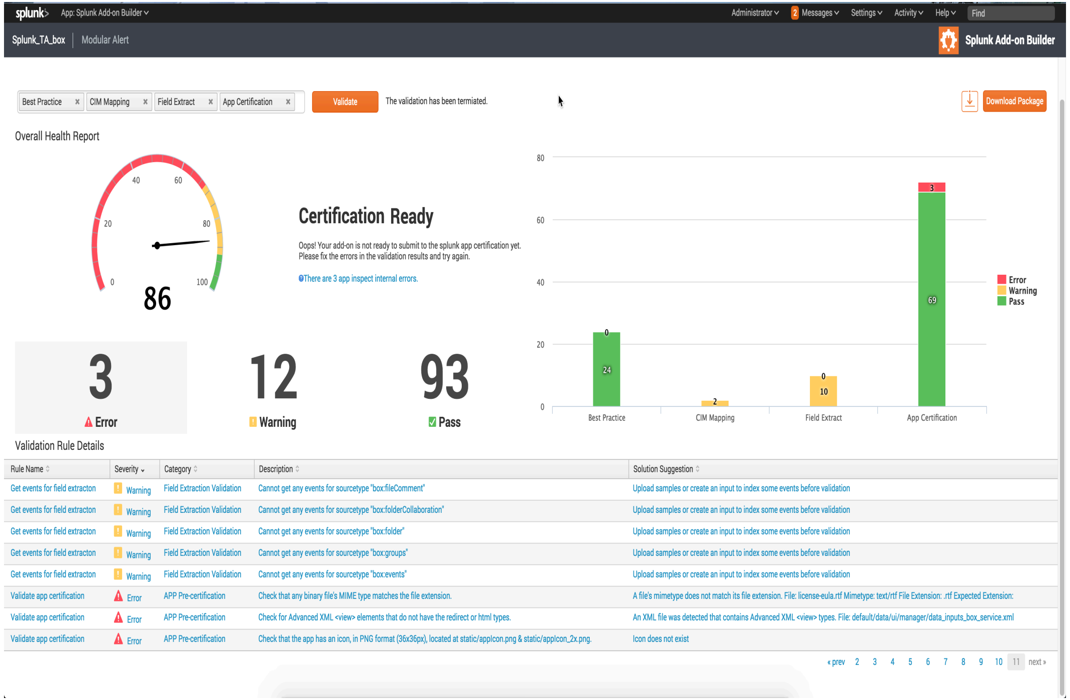
Whats new in Add-on Builder 2.0

- Version 2.0.0 Features Highlight

Certification check

Show via demo

- Get pre-certified with a click of a button
- Relies on backend online certification services to run check
- Add-on Builder pushes the Add-on package to the service and waits for results to be returned.
- Results are displayed on validation step in Add-on Builder.



The validation has been termiated.

Overall Health Report

86

Certification Ready

Oops! Your add-on is not ready to submit to the splunk app certification yet. Please fix the errors in the validation results and try again.

There are 3 app inspect internal errors.

3 Error

12 Warning

93 Pass

Validation Rule Details

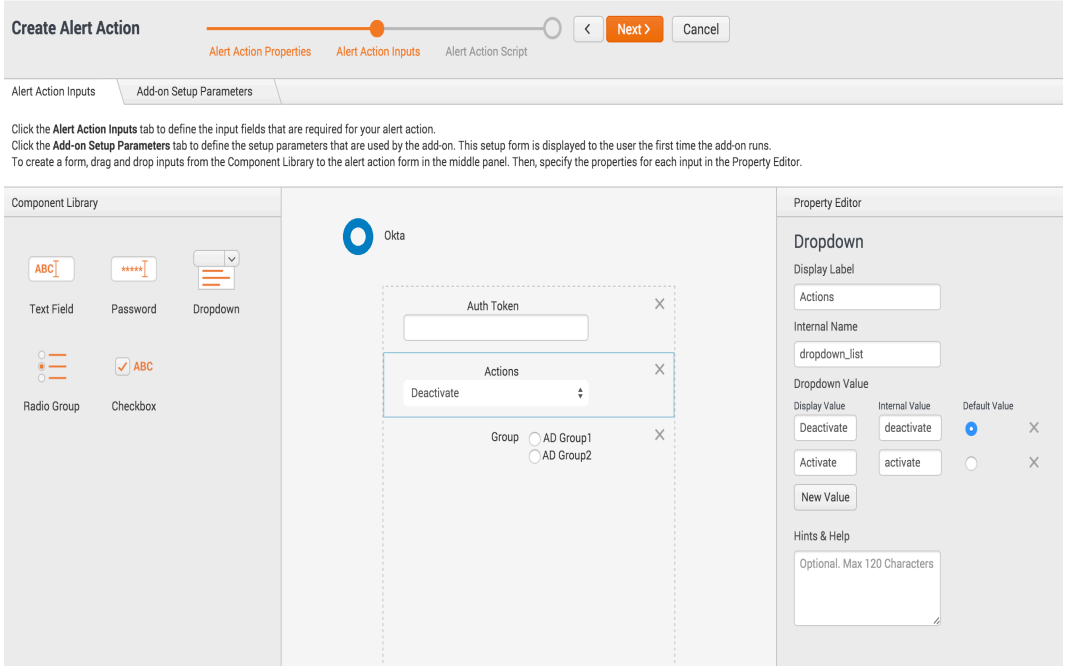
Rule Name	Severity	Category	Description	Solution Suggestion
Get events for field extracton	Warning	Field Extraction Validation	Cannot get any events for sourcetype "box:fileComment"	Upload samples or create an input to index some events before validation
Get events for field extracton	Warning	Field Extraction Validation	Cannot get any events for sourcetype "box:folderCollaboration"	Upload samples or create an input to index some events before validation
Get events for field extracton	Warning	Field Extraction Validation	Cannot get any events for sourcetype "box:folder"	Upload samples or create an input to index some events before validation
Get events for field extracton	Warning	Field Extraction Validation	Cannot get any events for sourcetype "box:groups"	Upload samples or create an input to index some events before validation
Get events for field extracton	Warning	Field Extraction Validation	Cannot get any events for sourcetype "box:events"	Upload samples or create an input to index some events before validation
Validate app certification	Error	APP Pre-certification	Check that any binary file's MIME type matches the file extension.	A file's mimetype does not match its file extension. File: license-eula.rtf Mimetype: text/rtf File Extension: .rtf Expected Extension:
Validate app certification	Error	APP Pre-certification	Check for Advanced XML <view> elements that do not have the redirect or html types.	An XML file was detected that contains Advanced XML <view> types. File: default/data/ui/manager/data_inputs_box_service.xml
Validate app certification	Error	APP Pre-certification	Check that the app has an icon, in PNG format (36x36px), located at static/applcon.png & static/applcon_2x.png.	Icon does not exist

« prev 2 3 4 5 6 7 8 9 10 11 next »

Alert Action

Show via demo

- Alert Action allows Splunk admins to take automatic actions from Splunk alert
- Example of existing Custom Alert actions on Splunkbase: ServiceNow Incident creation, Hipchat notifications
- Add-on Builder allows you to build test and validate Custom Alert Action in a simple UI based workflow.



Click the **Alert Action Inputs** tab to define the input fields that are required for your alert action.
Click the **Add-on Setup Parameters** tab to define the setup parameters that are used by the add-on. This setup form is displayed to the user the first time the add-on runs.
To create a form, drag and drop inputs from the Component Library to the alert action form in the middle panel. Then, specify the properties for each input in the Property Editor.

Property Editor: Dropdown
- Display Label: Actions
- Internal Name: dropdown_list
- Dropdown Value:

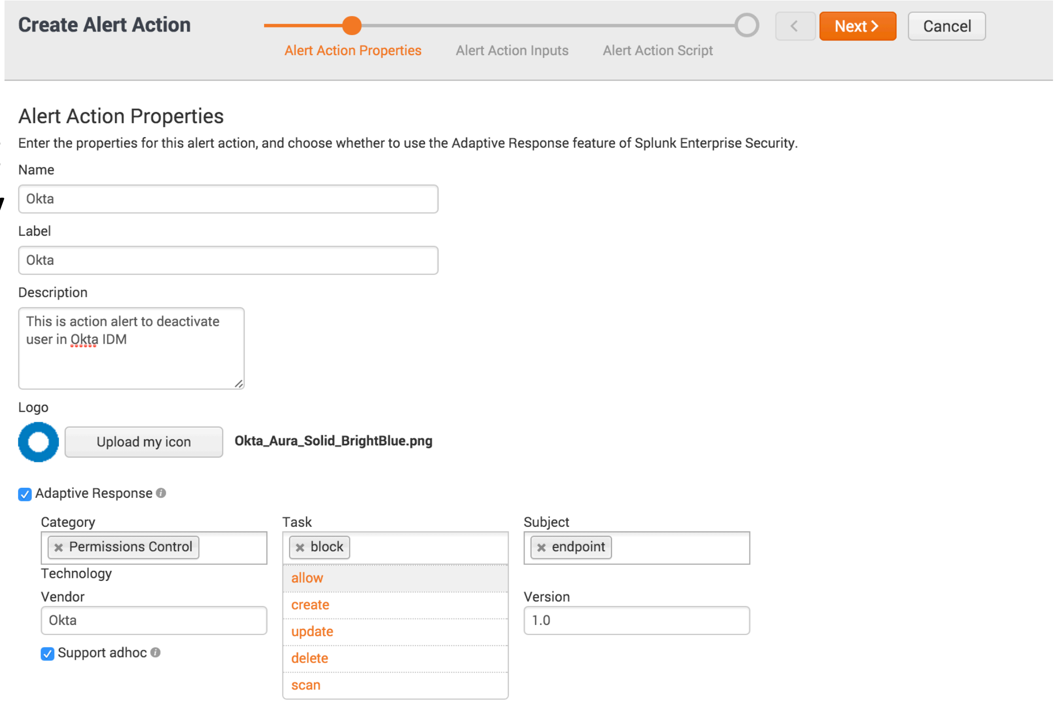
Display Value	Internal Value	Default Value
Deactivate	deactivate	●
Activate	activate	○

- Hints & Help: Optional. Max 120 Characters

Alert Action– Adaptive Response

Show via demo

- Splunk Enterprise Security developed the Adaptive Response initiative to connect Splunk with third part security systems
- Adaptive Response is built on top of action alert to define the interactions between Enterprise Security UI and the undelying action alert.
- Supports adhoc actions and alerts/automated



Alert Action Properties

Enter the properties for this alert action, and choose whether to use the Adaptive Response feature of Splunk Enterprise Security.

Name: Okta

Label: Okta

Description: This is action alert to deactivate user in Okta IDM

Logo: Okta_Aura_Solid_BrightBlue.png

☑ Adaptive Response

Category: Permissions Control

Task: block (allow, create, update, delete, scan)

Subject: endpoint

Technology

Vendor: Okta

Version: 1.0

☑ Support adhoc

Questions

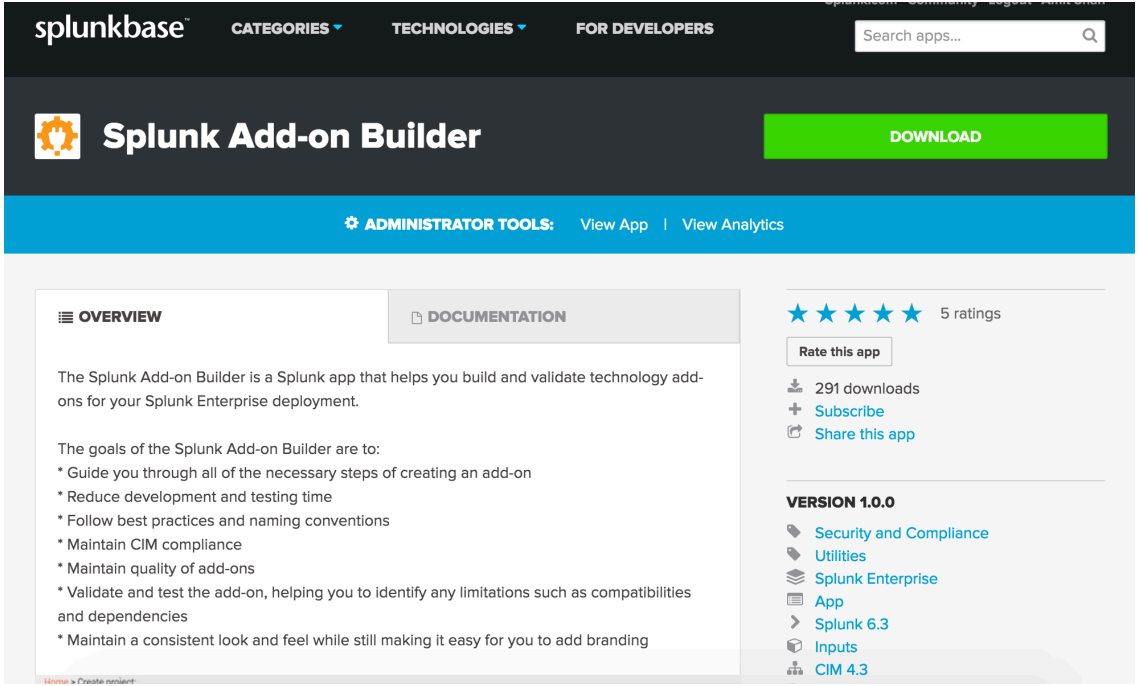
- Version 2.0.0 Features Highlight

THANK YOU

.conf2016

splunk>

Where can I download this app?



Splunk Add-on Builder

The Splunk Add-on Builder is a Splunk app that helps you build and validate technology add-ons for your Splunk Enterprise deployment.

The goals of the Splunk Add-on Builder are to:
* Guide you through all of the necessary steps of creating an add-on
* Reduce development and testing time
* Follow best practices and naming conventions
* Maintain CIM compliance
* Maintain quality of add-ons
* Validate and test the add-on, helping you to identify any limitations such as compatibilities and dependencies
* Maintain a consistent look and feel while still making it easy for you to add branding

★★★★★ 5 ratings

291 downloads

VERSION 1.0.0

Security and Compliance
Utilities
Splunk Enterprise
App
Splunk 6.3
Inputs
CIM 4.3

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

Data models covered by CIM

- Alerts
- Application State
- Authentication
- Change Analysis
- Databases
- Email
- Interprocess Messaging
- Intrusion Detection/ Prevention
- Inventory
- Java Virtual Machines
- Malware
- Network Sessions
- Network Traffic
- Performance
- Splunk Audit Logs
- Vulnerabilities
- Web