

splunk> .conf2017

From API To Easy Street

Elias Haddad | Sr. Product Manager, Splunk

Gordon Wang | Sr. Software Engineer, Splunk

Cheney Li | Sr. Software Engineer, Splunk

September 26, 2017 | Washington, DC

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

1. Why Add-on Builder
2. What is Add-on Builder
3. Features Highlights
4. What's new in Add-on Builder
5. Demo
6. Q&A

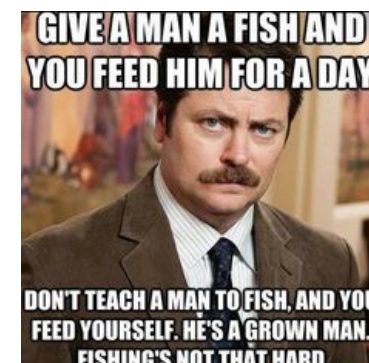
© 2017 SPLUNK INC.

© 2017 SPLUNK INC.

[illegible]

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**



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

```
130.60.4 - - [07/Jun 10:10:57:153] "GET /category.screen?category_id=G1F5&SESSIONID=5015L4FF10ADFF30 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=EST-5W-03"
128.241.220.82 - - [07/Jun 10:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5055L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=EST-5W-03"
131.27.160.0 - - [07/Jun 10:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-13&product_id=AV-CB-01&SESSIONID=5018L8FF2ADFF0 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-L1-02" 468 125.17 14 --
130.60.4 - - [07/Jun 10:10:57:153] "GET /category.screen?category_id=G1F5&SESSIONID=5015L4FF10ADFF30 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=EST-5W-03"
128.241.220.82 - - [07/Jun 10:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5055L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=EST-5W-03"
131.27.160.0 - - [07/Jun 10:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5055L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-13&product_id=AV-CB-01&SESSIONID=5018L8FF2ADFF0 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-L1-02" 468 125.17 14 --
```


Add-on Builder Feature Highlights

UI Based Add-On Creation

- ▶ 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

Author:

Add-on Author

Add-on Folder Name:

Edit

Version:

1.0.0


Description:

Add-on Description

Visible:

☐

Icon:



Upload my icon

No file selected

Theme Color:

Cancel

Create

Modular Input

► 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
- Support basic auth
- JSON data extraction

► If you have shell command or script

- We will generate the mod input for you
- Can be tokenized

► Real time code validation

The screenshot shows the 'Edit Data Input' window in the Splunk Add-on Builder. The 'Define & Test' tab is active. The 'Define the data input' section contains a form for defining a REST input. The 'REST URL' is set to 'https://api.nytimes.com/svc/search/v2/articlessearch.json? q=\${query}&api-key=\${_settings_additional_parameters.api_key}&sort=newest &begin_date=\${begin_date}'. The 'REST method' is set to 'GET'. The 'REST URL parameters' table lists 'q' as '\${query}', 'api-key' as '\${_settings_additional_parameters.api_key}', 'sort' as 'newest', and 'begin_date' as '\${begin_date}'. The 'REST request headers' section is empty. The 'Output' section shows a JSON response from the NYTimes API, including fields like 'status', 'copyright', 'docs', 'web_url', 'snippet', 'source', 'multimedia', 'headline', 'keywords', 'pub_date', 'document_type', 'new_desk', 'byline', 'original', 'type_of_material', 'id', 'word_count', 'score', and 'uri'.

Add-On Setup

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

Edit Data Input

Inputs & Parameters | Define & Test

Data Input Properties | Data Input Parameters | Add-on Setup Parameters

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. Select the type of parameters to add to the setup form from the list. Drag and drop input fields from the Component Library to add custom parameters. Then, specify the properties for each input in the Property Editor. [Learn More](#)

Preconfigured Parameters

- ☐ Proxy settings
- ☐ Global account settings
- ☒ Logging settings

Component Library in Panel Setting

- ☒ Text
- ☐ Password
- ☒ Checkbox

Property Editor

● To add a field to the form, drag one or more input fields from the Component Library to the center panel, then click a field to configure the details.

API key

Enter your New York Times API key

Advanced Modular Input

- ▶ If you have more advanced data collection logic
- ▶ Real-time code validation
- ▶ Includes library:
 - Check-pointing
 - Reading encrypted password from storage/password endpoint
 - Proxy
 - Accessing parameter values from setup page
 - Helper functions to send http requests

Create Data Input

Define Inputs
Fill out the form below to define your data input, enter variables to pass to the script, then click **Test** to preview the results. [Learn more](#)

Data Input Definition | **Add-on Setup Parameters** | **Code Editor**

Data input parameters

Enter a test value for the input parameters you defined in the previous step.

Text (text)

```

1 # encoding = utf-8
2
3
4 import os
5 import sys
6 import time
7 import datetime
8
9
10 '''
11     IMPORTANT
12     Edit only the validate_input and collect_events functions.
13     Do not edit any other part in this file.
14     This file is generated only once when creating the modular input.
15 '''
16
17 # For advanced users, if you want to create single instance mod input, uncomment this method.
18 def use_single_instance_mode():
19     return True
20
21 def validate_input(helper, definition):
22     """Implement your own validation logic to validate the input stanza configurations"""
23     # This example accesses the modular input variable
24     # text = definition.parameters.get('text', None)
25     pass
26
27 def collect_events(helper, ew):
28     """Implement your data collection logic here
29
30     # The following examples get the arguments of this input.
  
```

Field Extraction

- ▶ Support various formats including unstructured, KV, tabular and JSON
- ▶ Leverages machine learning clustering algorithm to group events based on format similarity
- ▶ Automatically generate regex for field extraction

New York Tim... | Configure Data Collection | Manage Source Types | **Extract Fields** | Map to Data Models | Create Alert Actions | Validate & Package | Splunk Add-on Builder

Extract Fields >> **demo:kv**

The summary below shows how your sample data was parsed for the Key Value format.

- Under **Pair Delimiter**, select the character used to separate key-value pairs.
- Under **Key Value**, select the character used to separate keys and values.
- Click **Other** to enter a different delimiter character.

When 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

Source type:	demo:kv	Event:	1000
Format:	Key Value	Coverage:	73.45%

Extraction Methods

Delimiters

Pair Delimiter

Comma Space Tab Pipe Other...

Key = Value

Equal Colon Semicolon Other...

All Matched Partially Matched Unmatched 1000 events, 0% matched, 100% partially matched, 0% unmatched.

1 2 3 4 5 >

InvoiceID=74877539, PayerAccountId=880758383673, LinkedAccountId=880758383673, RecordType=LineItem, RecordId=50239227869402047379697802, ProductName=AWS CloudTrail, RateId=10221961, SubscriptionId=214626710, PricingPlanId=791455, UsageType=APN1-FreeEventsRecorded, Operation=None, AvailabilityZone=, ReservedInstance=N, ItemDescription=0.0 per free event recorded in Asia Pacific (Tokyo) region, UsageStartDate=2016-05-31 01:00:00, UsageEndDate=2016-05-31 02:00:00, UsageQuantity=1680.00000000, Rate=0.000000000, Cost=0.00000000, ResourceId=, aws:autoscaling:groupName=, aws:cloudformation:logical-id=, aws:cloudformation:stack-id=, aws:cloudformation:stack-name=, user:Name=, user:elasticbeanstalk:environment-id=, user:elasticbeanstalk:environment-name=, user:name=, S3KeyLastModified="2016-06-04T20:15:09.000Z"

InvoiceID=74877539, PayerAccountId=880758383673, LinkedAccountId=880758383673, RecordType=LineItem, RecordId=50238951168240941736172466, ProductName=AWS CloudTrail, RateId=10221966, SubscriptionId=214626710, PricingPlanId=791455, UsageType=APN2-FreeEventsRecorded, Operation=None, AvailabilityZone=, ReservedInstance=N, ItemDescription=0.0 per free event recorded in Asia Pacific (Tokyo) region, UsageStartDate=2016-05-31 01:00:00, UsageEndDate=2016-05-31 02:00:00, UsageQuantity=1680.00000000, Rate=0.000000000, Cost=0.00000000, ResourceId=, aws:autoscaling:groupName=, aws:cloudformation:logical-id=, aws:cloudformation:stack-id=, aws:cloudformation:stack-name=, user:Name=, user:elasticbeanstalk:environment-id=, user:elasticbeanstalk:environment-name=, user:name=, S3KeyLastModified="2016-06-04T20:15:09.000Z"

Alert Action

- ▶ 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.

Create Alert Action

Properties Inputs & Parameters Code & Test

Alert Action Inputs Add-on Setup Parameters

Define the input fields that are required for your alert action. 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. [Learn More](#)

Component Library

- Text
- Dropdown
- Radio Buttons
- Checkbox

alert_example

String label

Dropdown List

Property Editor

Dropdown

Display label

Dropdown List

Internal name

dropdown_list

Dropdown option

Display value	Internal value	Default value
Option1	option1	<input checked="" type="radio"/>
Option2	option2	<input type="radio"/>
Option3	option3	<input type="radio"/>

New Option

Help text

Optional. Max 200 Characters

☐ Required

Alert Action– Adaptive Response

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


Create Alert Action Properties Inputs & Parameters Code & Test < Next > Cancel

Alert Action Properties
Enter the properties for this alert action, and choose whether to use the Adaptive Response feature of Splunk Enterprise Security. [Learn more](#)

*Label
ARF example

*Name
arf_example

Description
This is a ARF example

Logo
 Upload my icon No file selected

☒ Support as an adaptive response action in Splunk Enterprise Security

Category <input type="text" value="Information Conveyance"/>	Task <input type="text" value="block"/>	Subject <input type="text" value="endpoint.printer"/>
Vendor <input type="text" value="Splunk"/>	Product <input type="text" value="ARF example"/>	Version <input type="text" value="1.0.0"/>

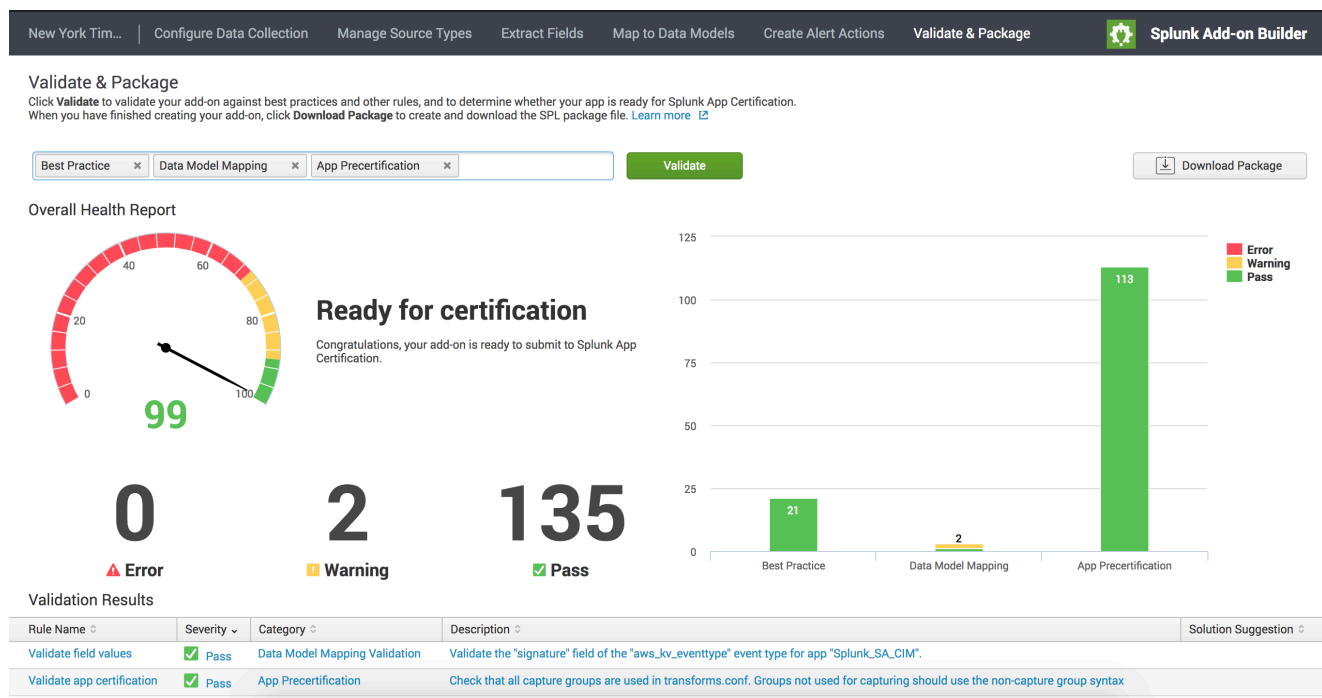
☒ Support as an ad-hoc action

Custom Drilldown

Source type

Health Validation

- ▶ Validate your Add-on for:
 - Best practices
- ▶ Detect any field extraction problems
- ▶ Detect any problems in modular inputs
- ▶ Certification readiness on roadmap



What's New – Latest Releases

REST Connect... With Check-Pointing

- Complexity with poll based ingestion – aka mod inputs
 - Check-pointing: mechanism to keep track of last ingested event
 - Encryption of passwords and sensitive information used by mod inputs
 - Payload can be returned in arrays of multiple events
- Solution: REST Connect in Add-on Builder
 - Ingest data from REST endpoint without writing code
 - Automatically handle encryption of passwords in a click of a button
 - Check-pointing is as easy as a check-box
 - Break REST endpoint payload into multiple events before indexing data

Poll Based Ingestion From REST is a Breeze

Define the data input

Fill out the form below to define your data input, enter variables to pass to the script, then click **Test** to preview the results. [Learn more](#)

REST URL parameters

Name	Value
q	\$(query)
api-key	\$_settings__additional_parameters.api
sort_by	newest
begin_date	\$(begin_date)

[New parameter](#)

REST request headers

Name	Value

[New header](#)

Data input parameters

Enter a test value for the input parameters you defined in the previous step.

query (query)?

snow

Event extraction settings

Checkpoint settings

Use checkpoints for incremental data collection. [Learn more](#)

☒ Enable checkpointing

• Checkpoint parameter name

begin_date

• Checkpoint field path

response.docs[-1].pub_date

Output: Done

```
{
  "response": {
    "meta": {
      "hits": 288,
      "time": 34,
      "offset": 0
    },
    "docs": [
      {
        "web_url": "http://www.nytimes.com/interactive/2017/02/09/nyregion/09snow-video-callout.html",
        "snippet": "The New York Times would like to see video from New Yorkers about how they're spending a day in the snow...",
        "lead_paragraph": "The New York Times would like to see video from New Yorkers about how they're spending a day in the snow",
        "abstract": null,
        "print_page": null,
        "blog": {},
        "source": "The New York Times",
        "multimedia": [
          {
            "width": 190,
            "url": "images/2017/02/09/nyregion/10weather-videocallout/10weather-videocallout-thumbWide.jpg",
            "height": 126,
            "subtype": "wide",
            "legacy": {
              "width": "images/2017/02/09/nyregion/10weather-videocallout/10weather-videocallout-thumbWide.jpg",
              "height": "126",
              "width": "190"
            },
            "type": "image"
          },
          {
            "width": 600,
            "url": "images/2017/02/09/nyregion/10weather-videocallout/10weather-videocallout-articleLarge.jpg",
            "height": 400,
            "subtype": "xlarge",
            "legacy": {
              "xlargewidth": "600",
              "xlarge": "images/2017/02/09/nyregion/10weather-videocallout/10weather-videocallout-articleLarge.jpg",
              "xlargeheight": "400"
            },
            "type": "image"
          },
          {
            "width": 75,
            "url": "images/2017/02/09/nyregion/10weather-videocallout/10weather-videocallout-thumbStandard.jpg",
            "height": 75,
            "subtype": "thumbnail"
          }
        ]
      }
    ]
  }
}
```

Map To Any Data Model

- Map to any data model – CIM or ITSI
- Map data at run-time

CIM Mapping >> CIM Mapping Details

The CIM Mapping List shows all the mappings for the source types in the current event type.
Starting by selecting the CIM models and datasets you want to use, then click **New Knowledge Object** to map event type fields to CIM model fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. [Learn more](#)

Event Type Fields: **akamai_general_web**
Event Type Search: **sourcetype = akamai:cm:json**

CIM Mapping List

Source Type	Object Type	Event Type Field or Expression	CIM Field	Actions
akamai:cm:json	EVAL	urldecode(message.UA)	http_user_agent	Edit Delete
akamai:cm:json	EVAL	if(cacheStatus == 1 OR cacheStatus == 2, "true", "false")	cached	Edit Delete
akamai:cm:json	FIELDALIAS	cp	status	Edit Delete
akamai:cm:json	FIELDALIAS	message.reqMethod	http_method	Edit Delete
akamai:cm:json	FIELDALIAS	message.reqLen	bytes_in	Edit Delete
akamai:cm:json	EVAL	len(message.proto + "/" + "message.reqHost" + ":" + me...	url_length	Edit Delete
akamai:cm:json	FIELDALIAS	message.UA	http_user_agent	Edit Delete
akamai:cm:json	EVAL	len(urldecode(message.UA))	http_user_agent_length	Edit Delete
akamai:cm:json	FIELDALIAS	netPerf.downloadTime	duration	Edit Delete
akamai:cm:json	FIELDALIAS	message.respLen	bytes_out	Edit Delete
akamai:cm:json	FIELDALIAS	netPerf.cacheStatus	cacheStatus	Edit Delete
akamai:cm:json	EVAL	urldecode(message.reqQuery)	url_query	Edit Delete
akamai:cm:json	EVAL	"Akamai Cloud Monitor"	vendor_product	Edit Delete
akamai:cm:json	EVAL	if(cacheStatus > 0, "true", "false")	request_cacheable	Edit Delete
akamai:cm:json	EVAL	"cloud monitor"	app	Edit Delete
akamai:cm:json	FIELDALIAS	message.reqHost	dest	Edit Delete
akamai:cm:json	EVAL	'message.proto' + '/' + 'message.reqHost' + ':' + 'messa...	url	Edit Delete
akamai:cm:json	FIELDALIAS	date_hour	category	Edit Delete

CIM Model Fields

Select CIM Models

Search model fields

Proxy

- action
- app
- bytes
- bytes_in
- bytes_out
- cached
- category
- cookie
- dest
- duration
- http_content_type
- http_method
- http_referer
- http_user_agent
- http_user_agent_length
- response_time
- site
- src
- status
- uri_path
- url_query

Q&A



© 2017 SPLUNK INC.

Thank You

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk> .conf2017

Where Can I Download This App?

Splunk Add-on Builder

★★★★★ 19 ratings

Splunk Built

ADMINISTRATOR TOOLS: Manage App | View App | View Analytics

Overview Details

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
- Build alert actions and adaptive response actions for Splunk Enterprise Security
- Reduce development and testing time
- Follow best practices and naming conventions
- Maintain CIM compliance
- Maintain quality of add-ons

1,077 Installs 7,438 Downloads

Download

Rate this App

VERSION

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