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.
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
All Data is Relevant
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*
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
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
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
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
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
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.
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
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
Map To Any Data Model

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

Don't forget to rate this session in the .conf2017 mobile app
Where Can I Download This App?

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