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.

Level up Your Response Actions:

Hands-on Building Splunk® SOAR Apps Using the Splunk® SOAR App Wizard
SEC1332C

Scott McCarthy

SOAR Technical Team Lead | National Grid

splunk> .conf23

Scott McCarthy

SOAR Technical Team Lead
National Grid

We want to automate, but we can't.

Introduction and Purpose

1) Build custom SOAR app

2) Ingest paginated data from an authenticated REST API source

3) POST data to an authenticated REST API source

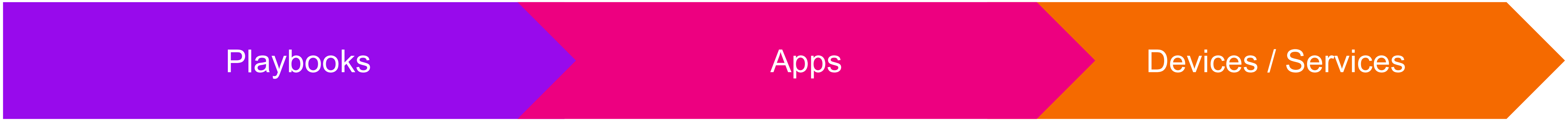
4) Understand the basics of app development inside SOAR

Getting introduced to the Splunk® SOAR App Dev Process

splunk> .conf23

Splunk® SOAR app architecture

Playbooks trigger **Actions** on the App



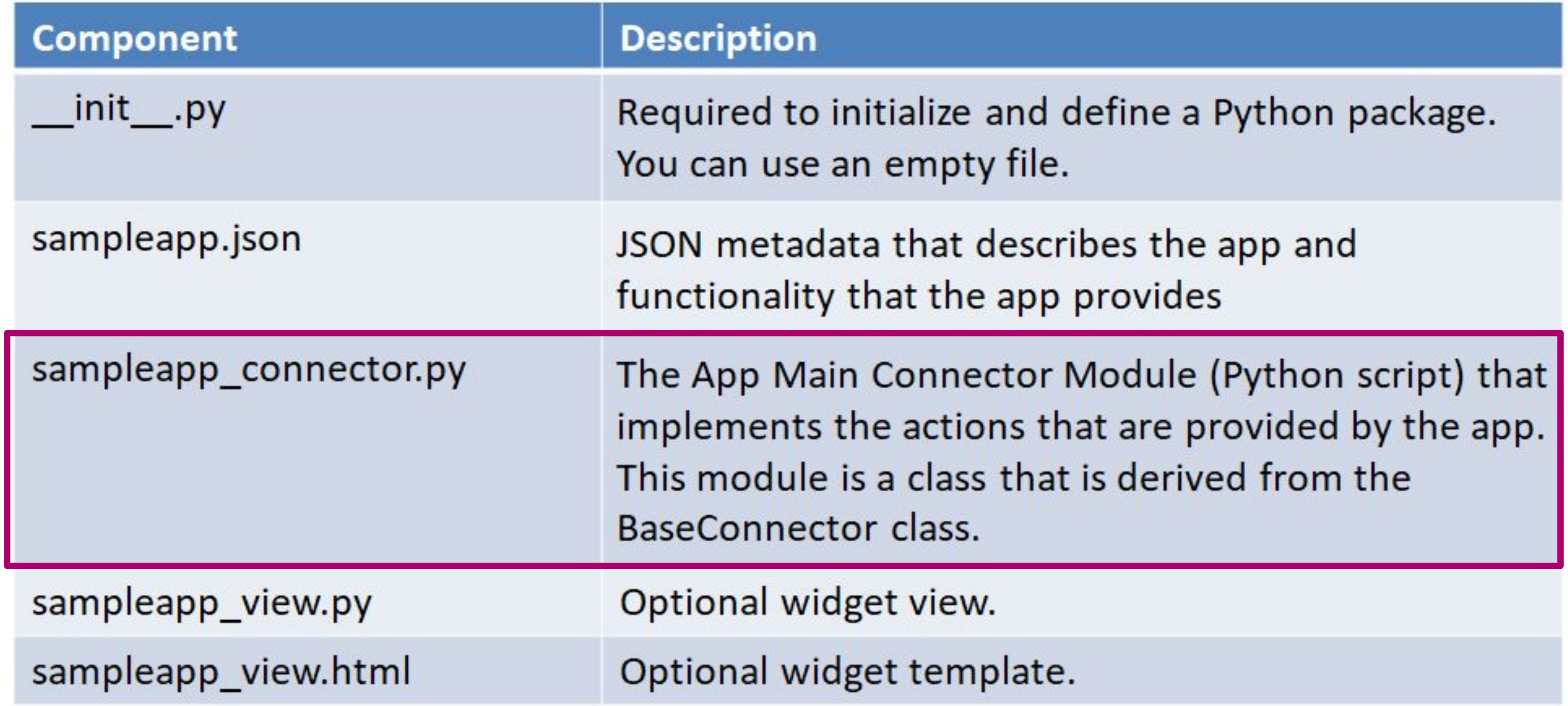
Playbooks

Apps

Devices / Services

Splunk® SOAR app components

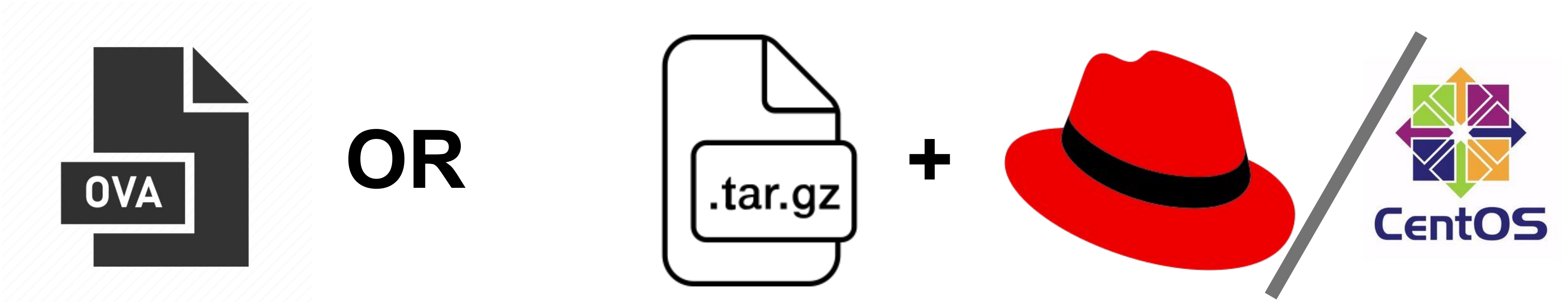
A Splunk® SOAR app consists of a number of components.



Component	Description
__init__.py	Required to initialize and define a Python package. You can use an empty file.
sampleapp.json	JSON metadata that describes the app and functionality that the app provides
sampleapp_connector.py	The App Main Connector Module (Python script) that implements the actions that are provided by the app. This module is a class that is derived from the BaseConnector class.
sampleapp_view.py	Optional widget view.
sampleapp_view.html	Optional widget template.

Have a development environment

It is best to develop using a development environment with an on-prem instance of Splunk® SOAR.



See resources below on setting up a dev environment:

https://docs.splunk.com/Documentation/SOARonprem/latest/Install/Overview

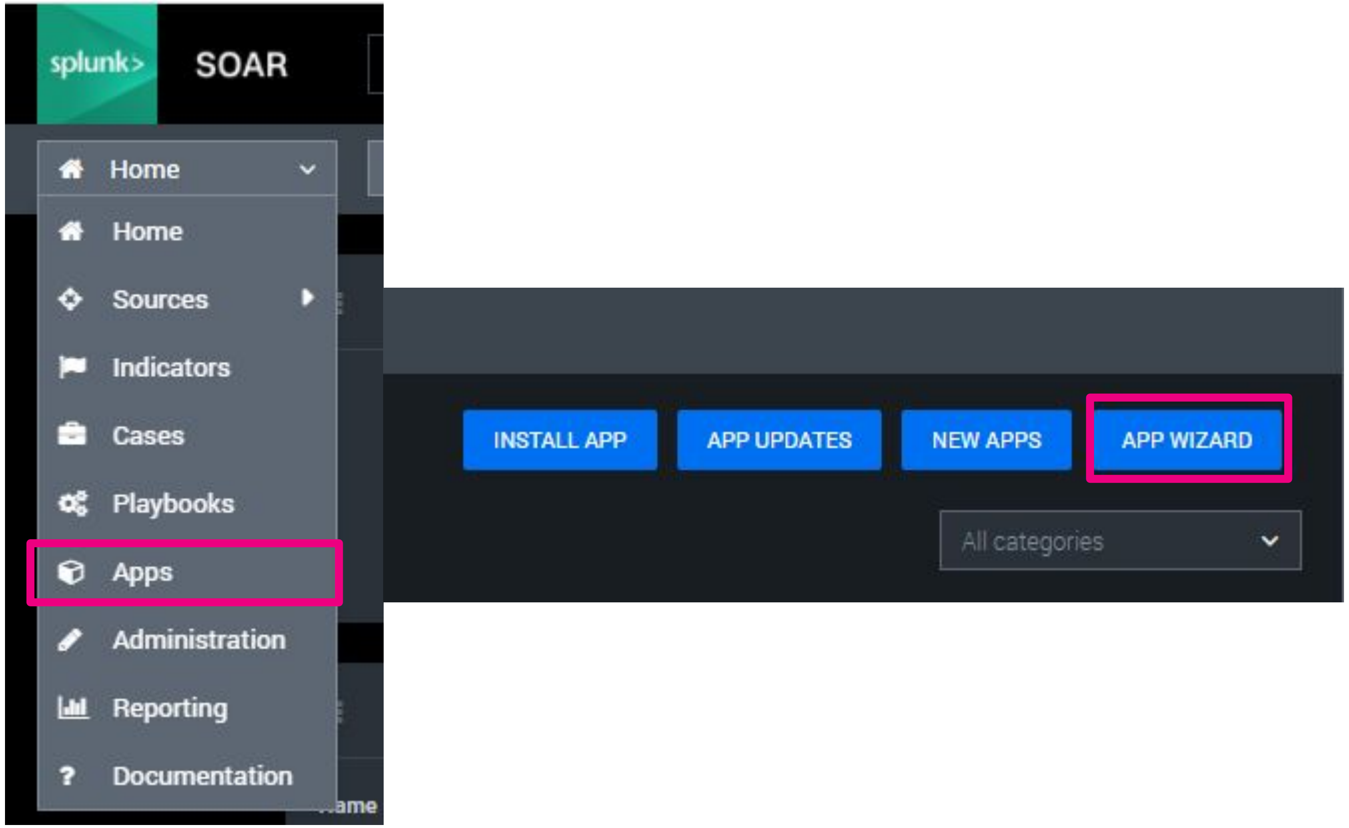
https://docs.splunk.com/Documentation/SOAR/current/DevelopApps/SetUpADevEnvironment

Using the App Wizard

Navigate to the **Main Menu**.

Select **Apps**.

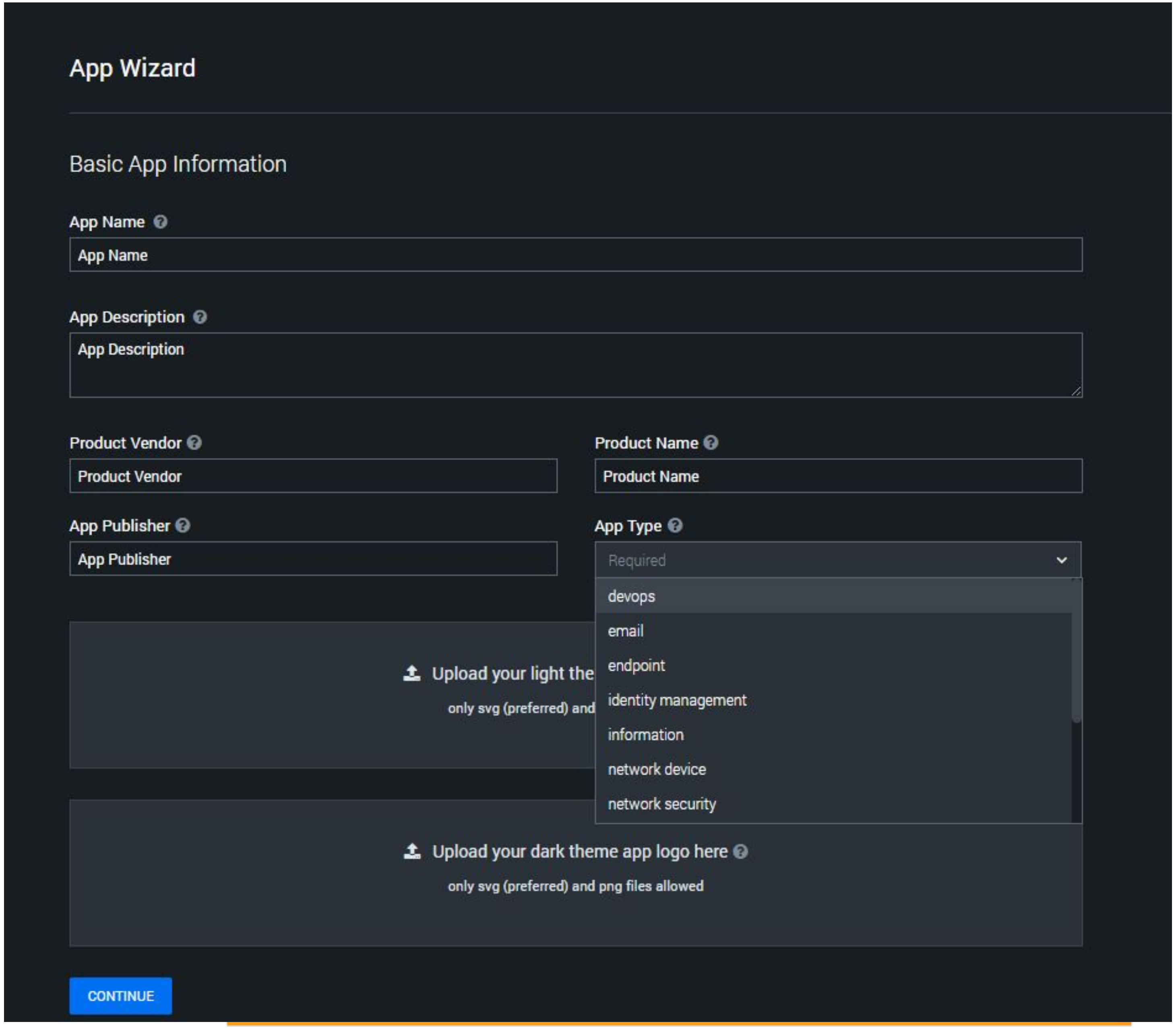
Click **App Wizard**.



App Wizard

Set required fields

Upload icon svg or png file 200x150px to 400x300px



App Wizard

Basic App Information

App Name: App Name

App Description: App Description

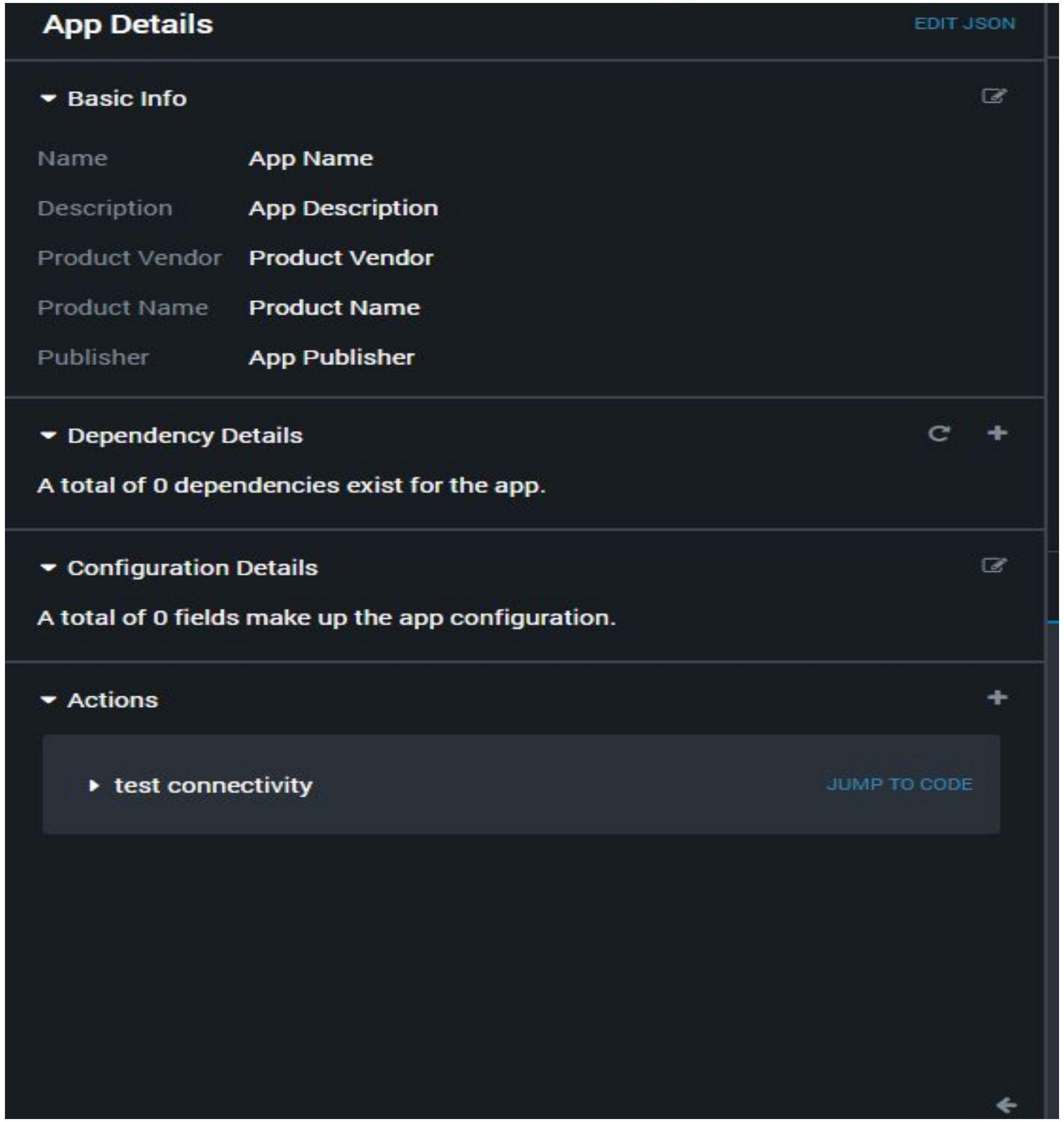
Product Vendor: Product Vendor

Product Name: Product Name

App Publisher: App Publisher

App Type: Required

https://docs.splunk.com/Documentation/SOAR/current/DevelopApps/CreateAnAppWithTheAppEditor



App Details

Basic Info

Name	App Name
Description	App Description
Product Vendor	Product Vendor
Product Name	Product Name
Publisher	App Publisher

Dependency Details

A total of 0 dependencies exist for the app.

Configuration Details

A total of 0 fields make up the app configuration.

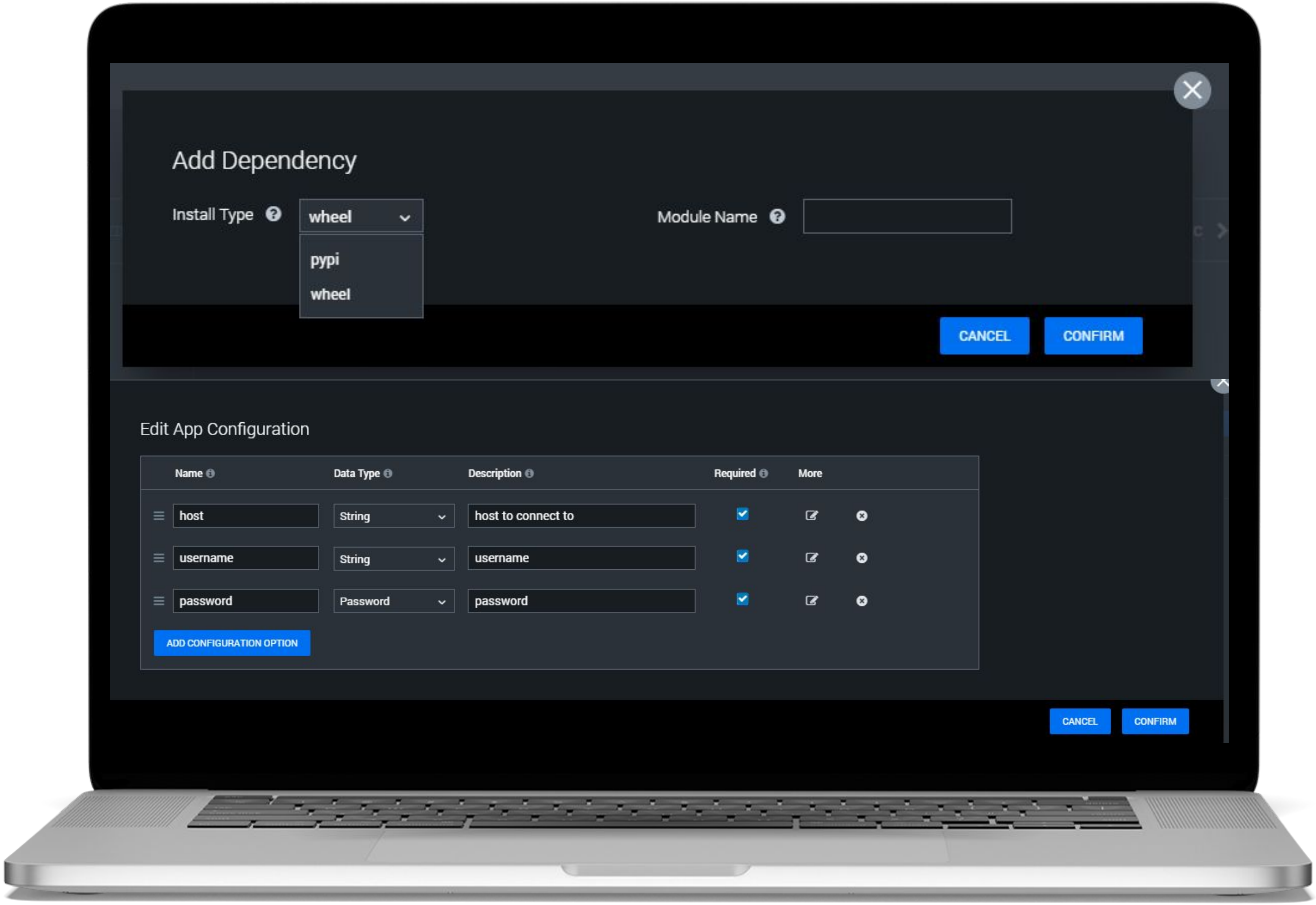
Actions

test connectivity

From App Details you can:

- Edit app basic information
- Add dependencies from PyPi/wheel files
- Edit app configuration (usually host and authentication information)
- Create actions

Adding dependencies and configurations



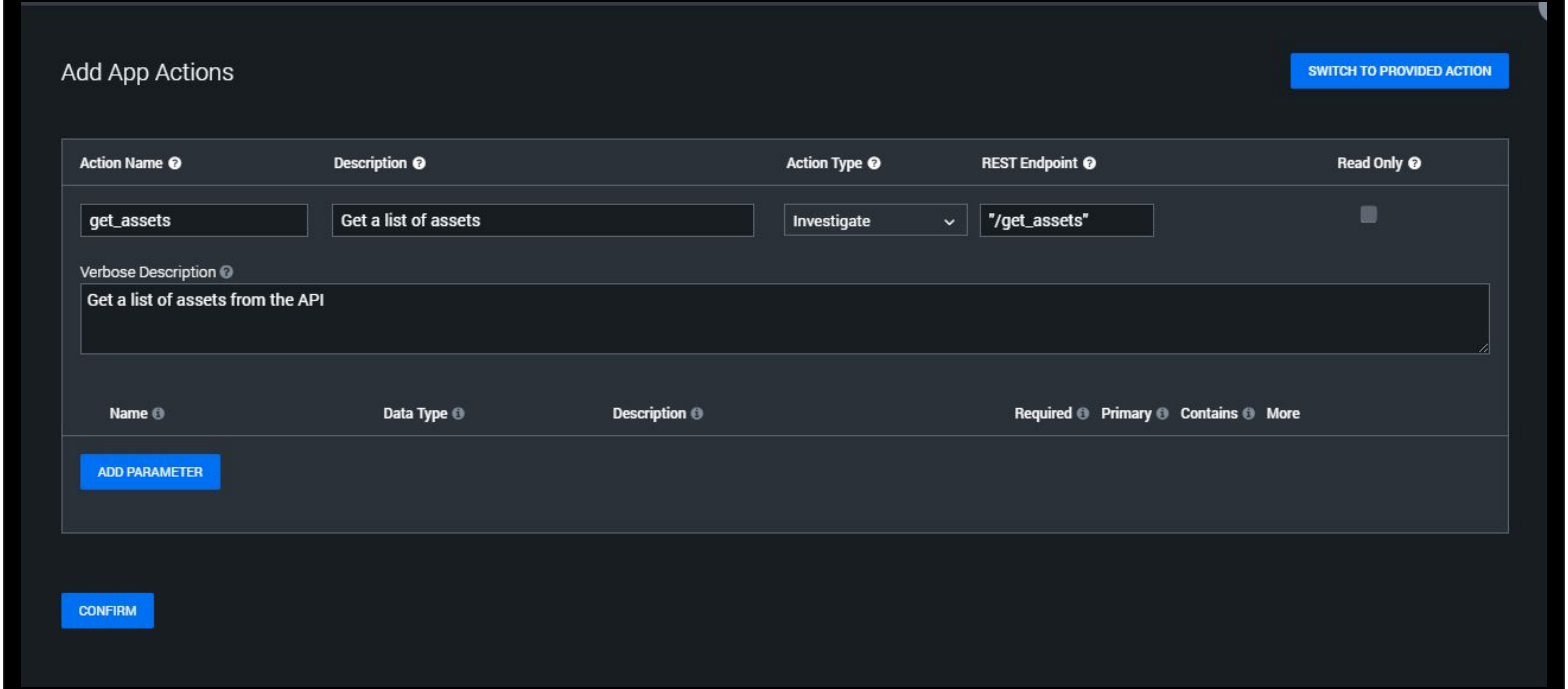
Add Dependency

Install Type: wheel

Module Name:

Edit App Configuration

Name	Data Type	Description	Required	More
host	String	host to connect to	☑	
username	String	username	☑	
password	Password	password	☑	



Add App Actions

SWITCH TO PROVIDED ACTION

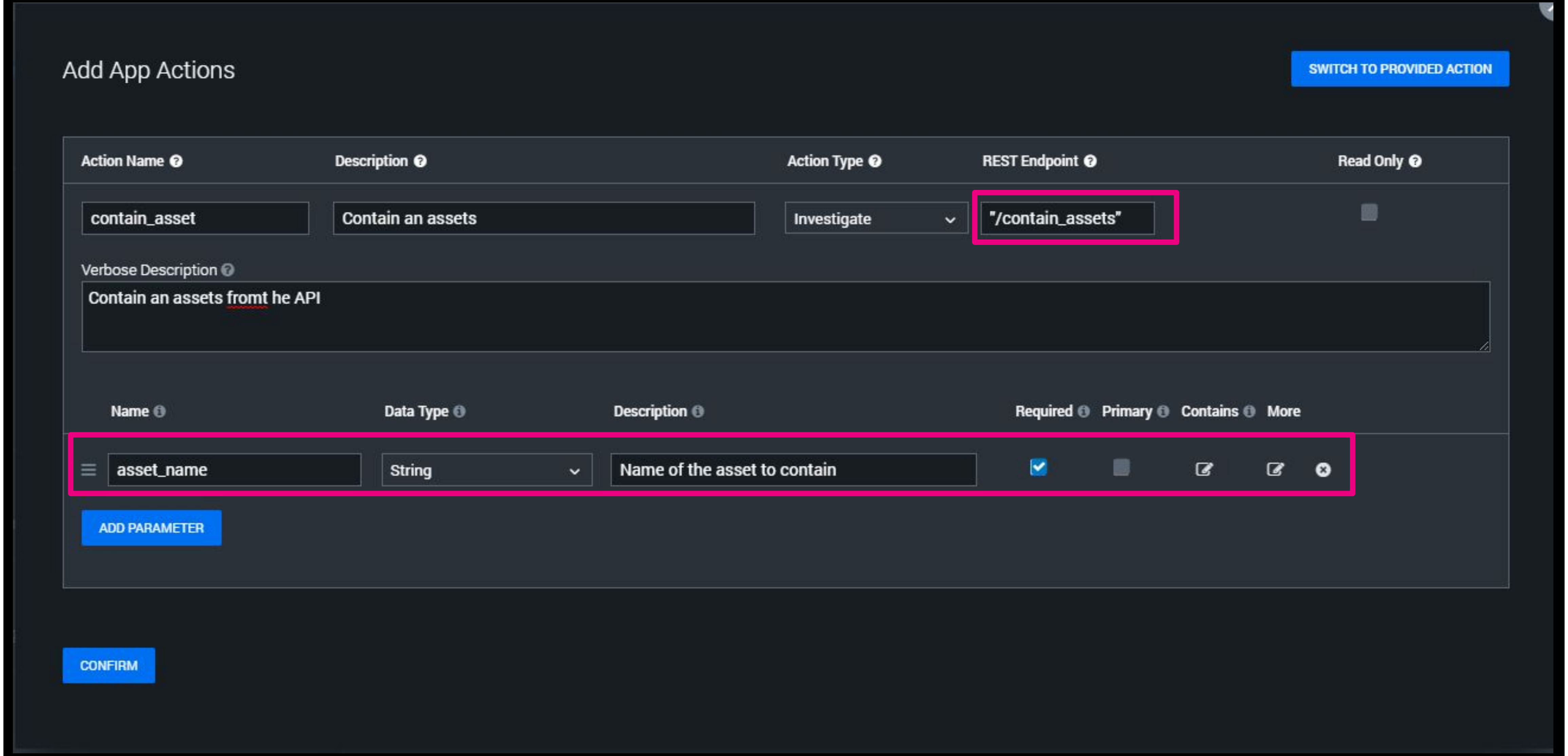
Action Name	Description	Action Type	REST Endpoint	Read Only
get_assets	Get a list of assets	Investigate	"/get_assets"	□

Verbose Description: Get a list of assets from the API

Name	Data Type	Description	Required	Primary	Contains	More

ADD PARAMETER

CONFIRM



Add App Actions

SWITCH TO PROVIDED ACTION

Action Name	Description	Action Type	REST Endpoint	Read Only
contain_asset	Contain an assets	Investigate	"/contain_assets"	□

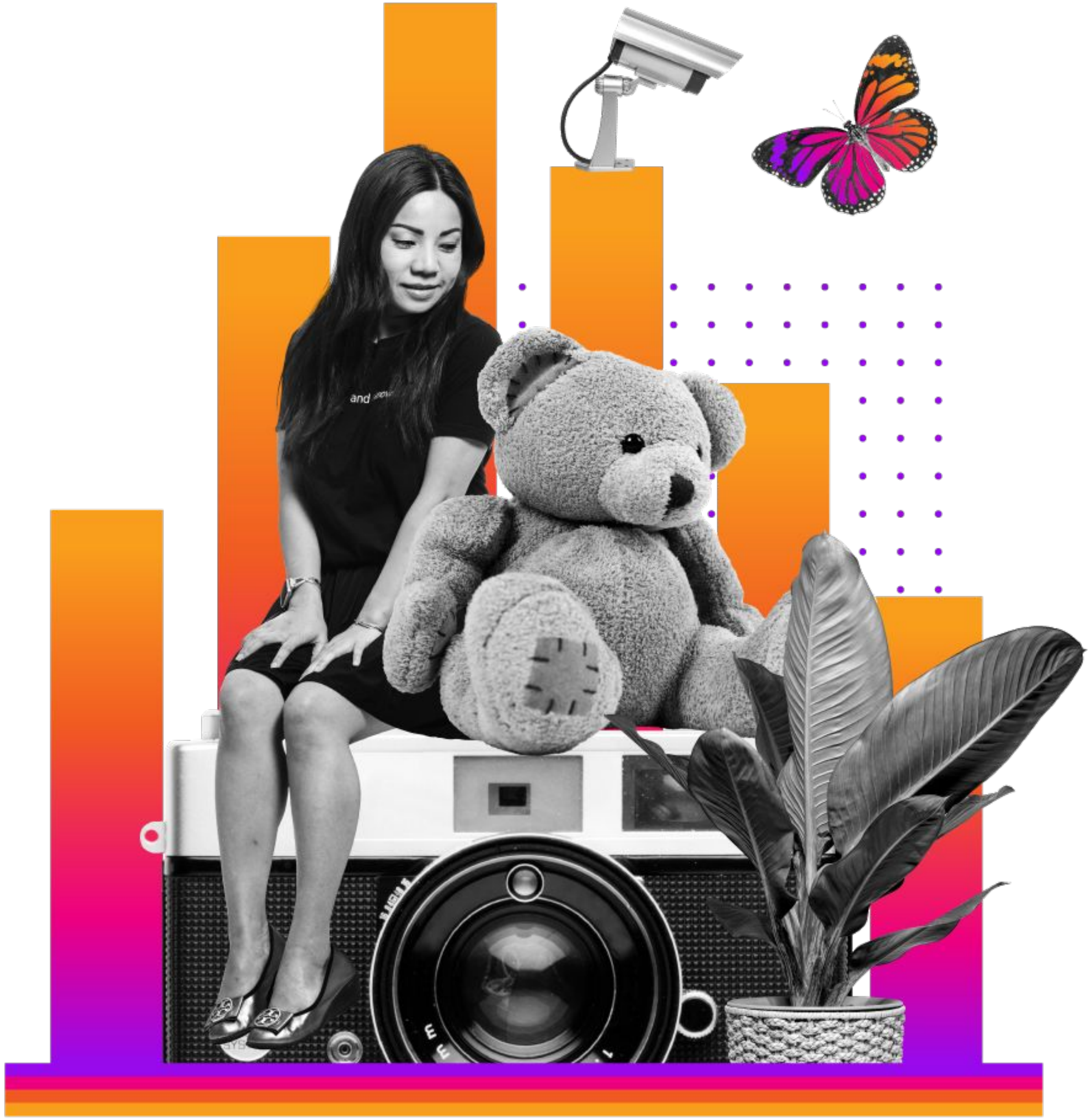
Verbose Description

Contain an assets fromt he API

	Name	Data Type	Description	Required	Primary	Contains	More
☰	asset_name	String	Name of the asset to contain	☑	□		

ADD PARAMETER

CONFIRM



Getting Hands-on

Let’s connect to home hosts and do this live.

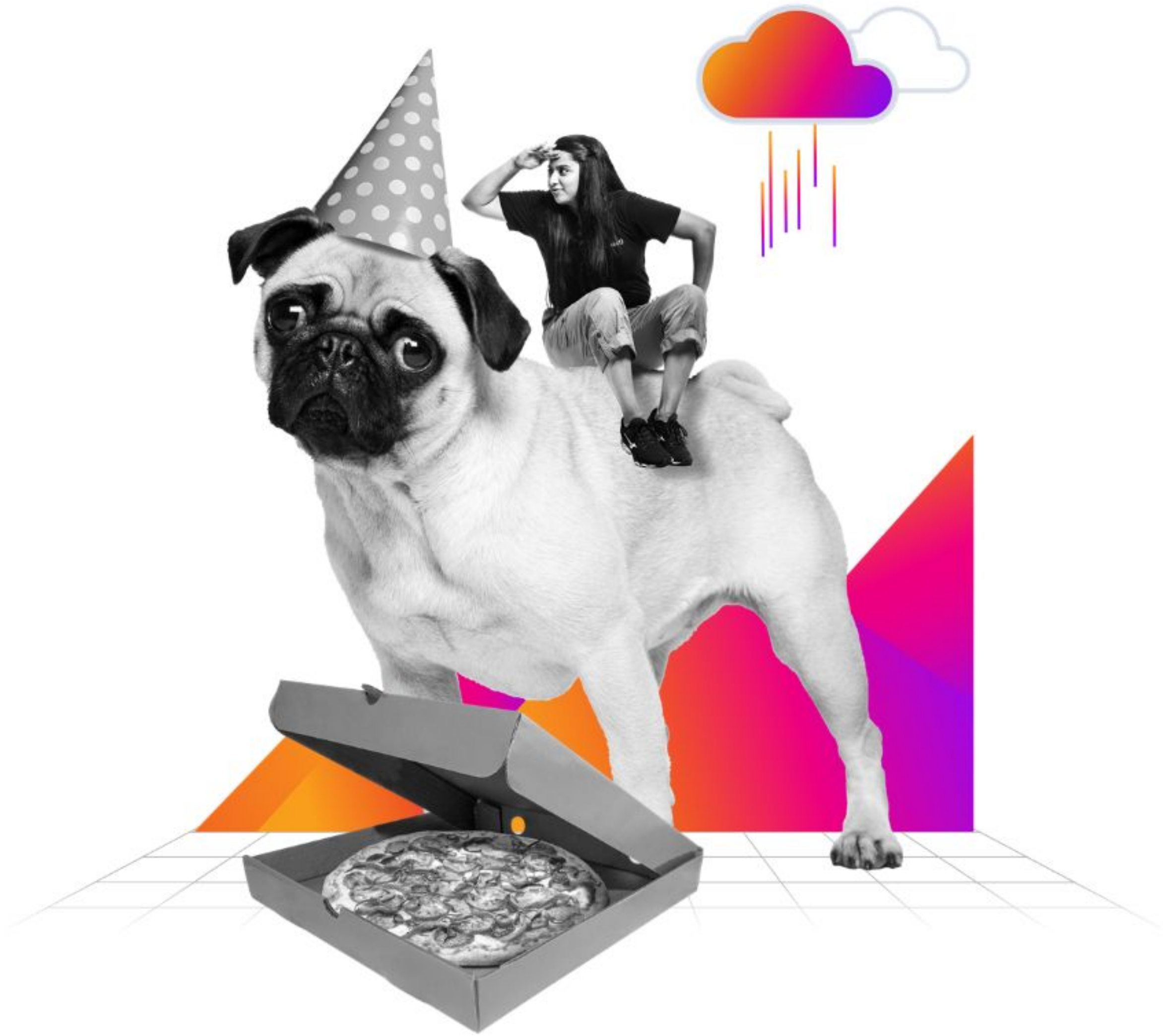
Audience Participation is encouraged

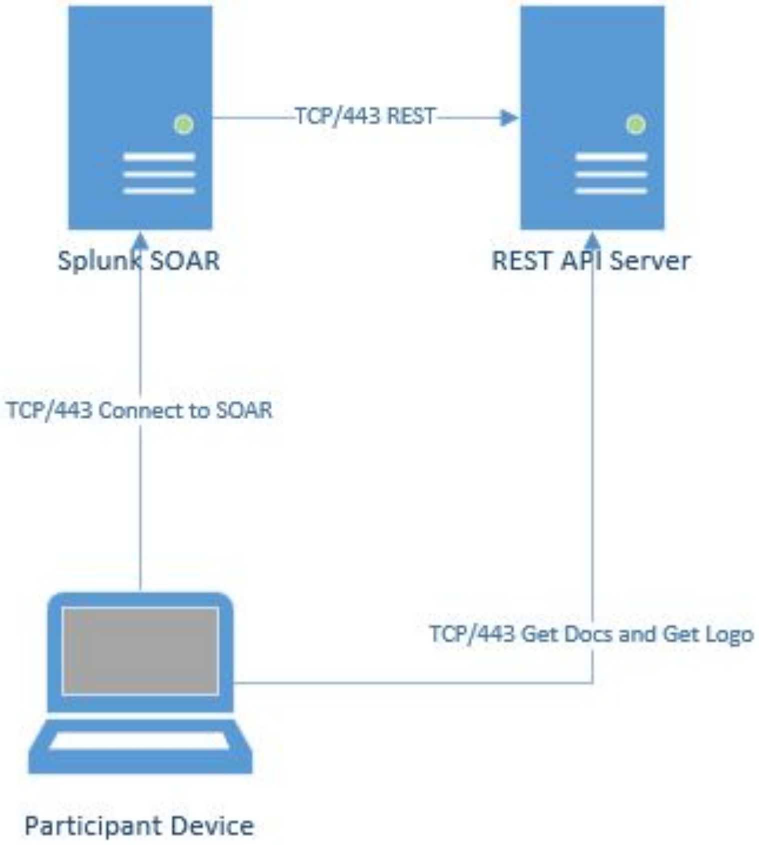
splunk> .conf23

Scenario

We have a new REST API source for managing endpoints and users that does not have an existing SOAR App.

- We need to get a list of users
- We need to contain an asset





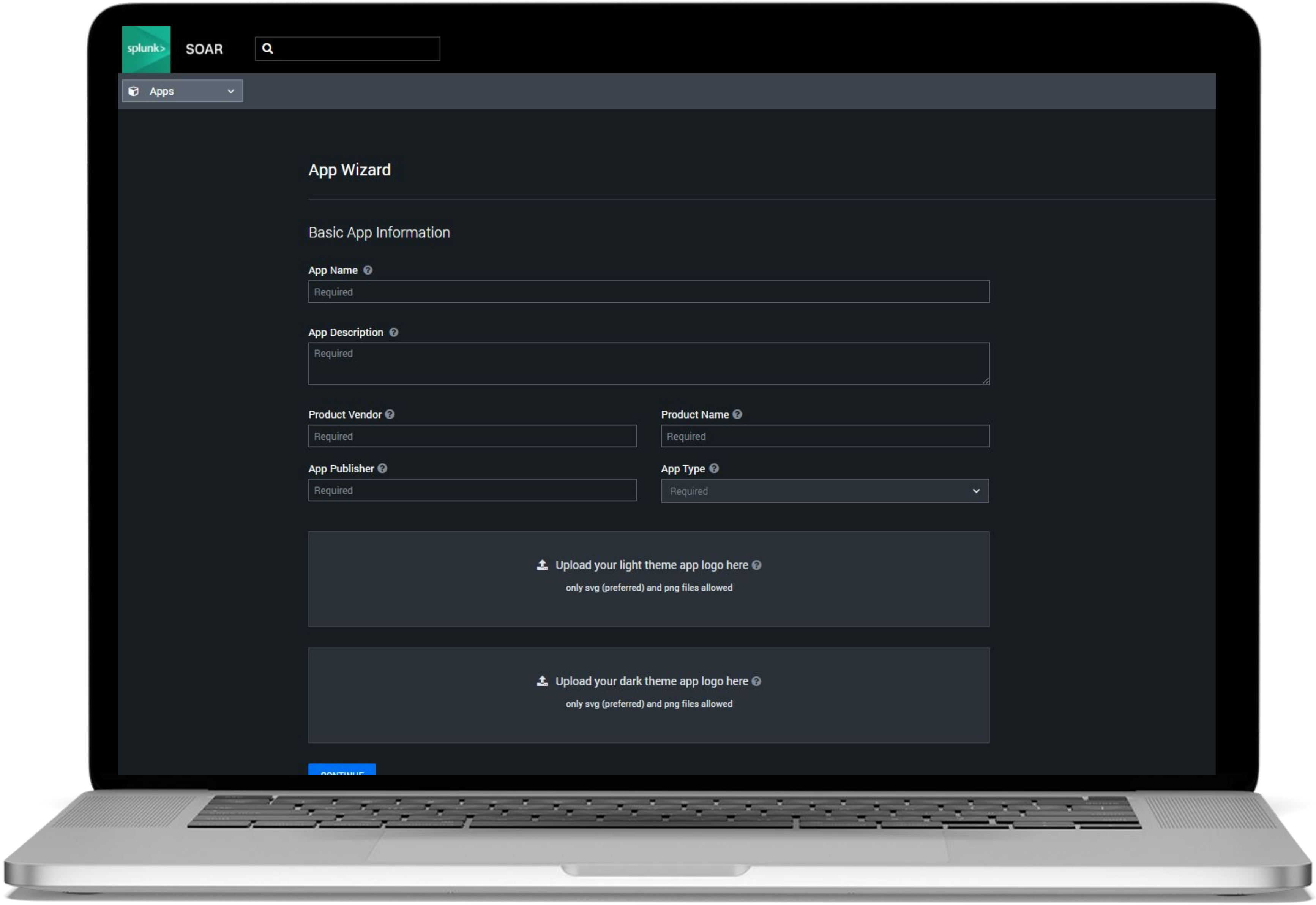
Rest API Server:
https://api.splunktools.net

Splunk SOAR Server:
https://soar.splunktools.net

GitHub Link:

https://github.splunktools.net

Let’s Build An App!



App Wizard

Basic App Information

App Name: Required

App Description: Required

Product Vendor: Required

Product Name: Required

App Publisher: Required

App Type: Required

Upload your light theme app logo here
only svg (preferred) and png files allowed

Upload your dark theme app logo here
only svg (preferred) and png files allowed

Q&A

splunk> .conf23

Resources

Splunk Official SOAR Development Documentation

Ingest Actions

App Github Repository

FastAPI GitHub Repository

splunktools.net

Related .Conf Talks

SEC1104C - Jump to Hyperspace - Publish Apps at Lightspeed with Open SOARce

SEC1700C - Ready, Set, SOAR: How Utility Apps Can Up Level Your Playbooks!

Make something tomorrow you couldn’t yesterday

Thank You

splunk> .conf23