



Automation for everyone

Agenda

00:00 - 00:45 Introduction - What is Shuffle and security automation

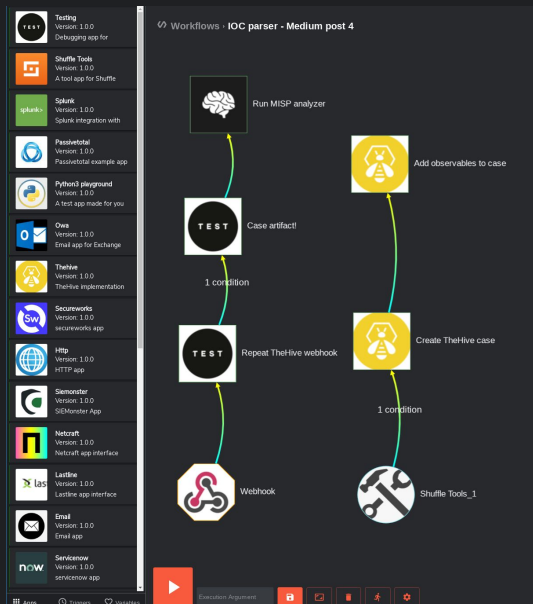
01:00 - 01:45 Workflows: creation, using and sharing

02:00 - 02:45 Integrations: creation, using and sharing

03:00 - 03:45 Use-case solving: we'll help solve your use-case in class

Workshop goals

Playbook editor



App editor

The screenshot shows the App editor interface for 'TheHive OpenAPI'. The top section is 'General information', which includes a name field (TheHive OpenAPI), a description field (API description for TheHive - https://github.com/TheHive-Project/TheHiveDocs/tree/), and an API information section with a base URL field (https://api.example.com) and an authentication dropdown (Bearer auth). The bottom section is 'Actions', which lists tasks performed by the app: GET - ApiAlert - List alerts, POST - ApiAlert - Create an alert, and POST - ApiAlertSearch - Find alerts. Each action has 'Duplicate' and 'Delete' buttons.

Organization control

The screenshot displays the Organization control interface. The top navigation bar includes links for ORGANIZATION, USERS, APP AUTHENTICATION, ENVIRONMENTS, SCHEDULES, HYBRID, and ORGANIZATIONS. The main section is 'Organization overview', which includes a name field (Shuffle AS), a description field (Creating security automation solutions for the good of the general public), and a 'STOP SYNC' button. Below this is a 'Cloud synchronization' section with a table of cloud sync features. The table has columns for 'Webhook', 'Schedules', 'User Input', 'Send Mail', 'Send Sms', 'Updates', 'Notifications', 'Email Trigger', 'App Executions', 'Workflow Executions', 'Apps', and 'Authentication'. Each feature has a status indicator (green checkmark or red X).

Webhook	Schedules	User Input	Send Mail	Send Sms	Updates	Notifications	Email Trigger	App Executions	Workflow Executions	Apps	Authentication
✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗

Shuffle - built from real-world experience

- Worked in multiple incident response & SOC environments
- Developers in bluetams are “unicorns”
- Built for accessibility and standardization
- Started after a blogpost on NSA WALKOFF (2019)

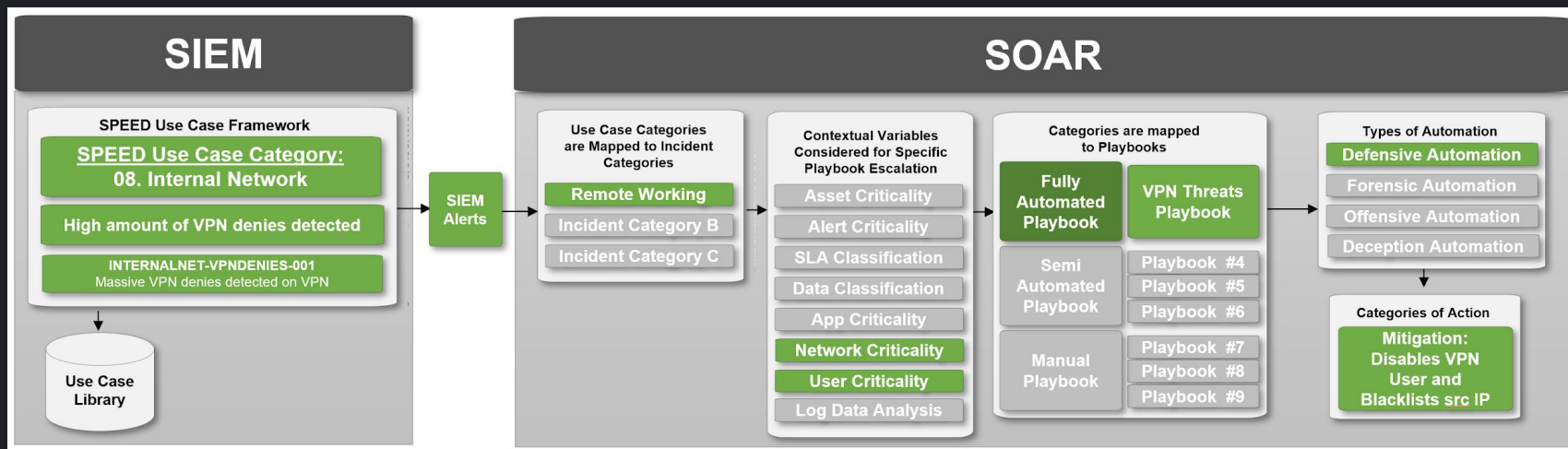
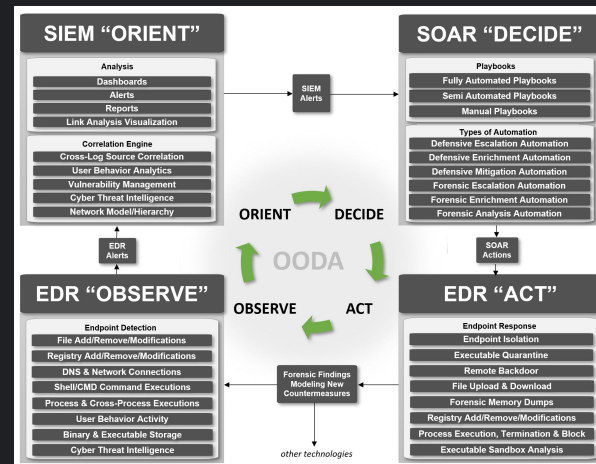
What is Shuffle today

- Automation platform
- Open Source Software
- Workflow editor
- Integrations builder
- Code generator
- Authentication overview
- ...

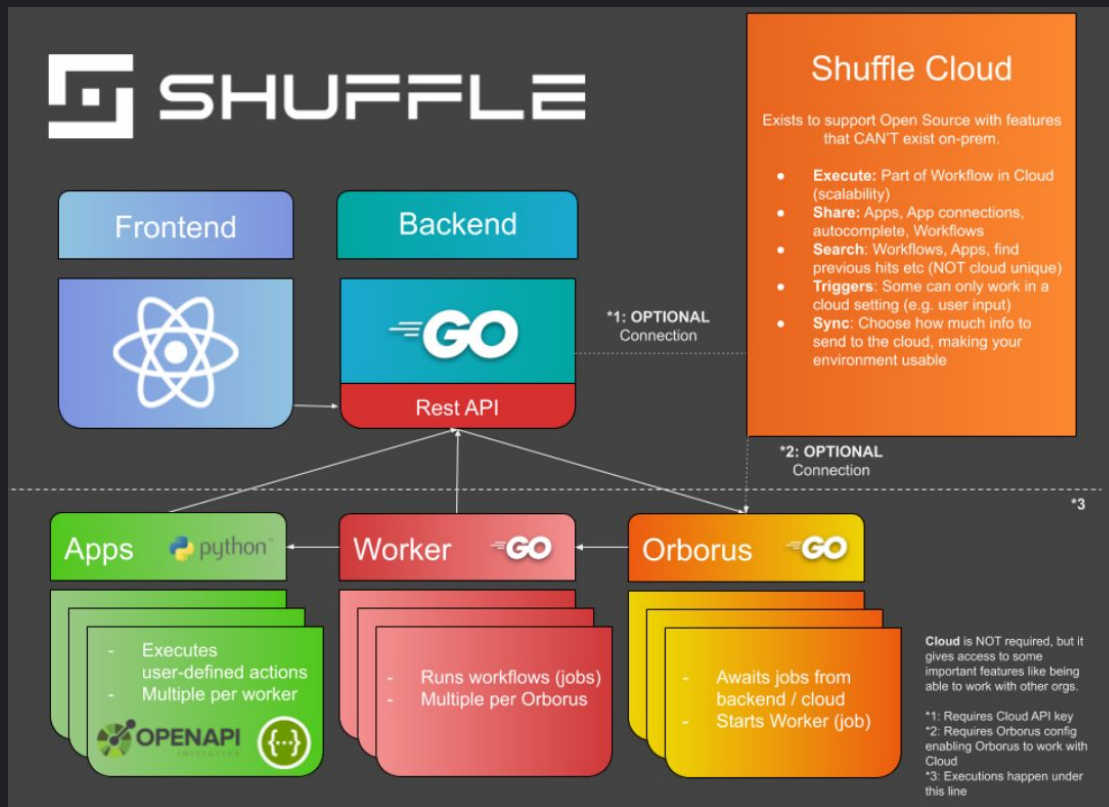
Practical examples

- [Ransomware cryptolocker](#)
- [New domain admin](#)
- [Website defacement](#)
- [Multiple failed logins detected](#) -> block user
- S3 bucket access -> block IP
- Phishing happened -> automate triage
- SSL certificate validation -> email on error
- Automatically enrich cases
- Automatically analyze and run emails

OODA driven SOAR



Architecture



Let's get started

 Workflows  Apps  Docs

[SETTINGS](#)

Log

Login

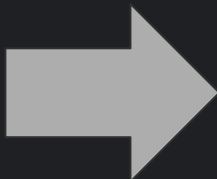
Username



Password



SUBMIT



Welcome to Shuffle


Shuffle is a flexible, easy to use, automation platform allowing users to integrate their services and devices freely. It's made to significantly reduce the amount of manual labor, and is focused on security applications. [Click here to learn more.](#)

If you want to jump straight into it, click here to create your first workflow:

[NEW WORKFLOW](#)

..OR



 Workflows

 Apps

 Docs

ADMIN

SETTINGS

Logout

Workflows

Workflows (35)



Executions: Hook test



Execution Timeline



Collapse results

Hook test



EDIT



hook



EC2 testing_copy_copy



EDIT



test



EC2 testing_copy



EDIT



test



EC2 testing



EDIT



test



Execute subworkflow



EDIT



sub

test



#170: Nested loop testing



EDIT



#170

test



Status: FINISHED

Actions: 1/1

Started: 2020-12-20T07:18:34.000Z

ABOUT

Status: FINISHED

Actions: 1/1

Started: 2020-12-20T07:18:01.000Z

ABOUT

Status: FINISHED

Actions: 1/1

Started: 2020-12-20T07:17:25.000Z

ABOUT

Status: FINISHED

Actions: 1/1

Started: 2020-12-20T07:06:21.000Z

ABOUT

Status: FINISHED

Actions: 1/1

Started: 2020-12-20T07:05:45.000Z

ABOUT

Status: FINISHED

Actions: 1/1

Started: 2020-12-20T06:55:34.000Z

ABOUT

Status: FINISHED

Started: 2020-12-20T07:18:34.000Z

Finished: 2020-12-20T07:18:34.000Z

▶ "Execution argument / webhook": { ... } 6 items

Name: Start node

App: Testing, Version: 1.0.0

Action: repeat_back_to_me, Environment: Shuffle, Status: SUCCESS

Started: 2020-12-20T07:18:38.000Z

▶ "Results for Start node": { 6 items

"color": "warning"

"pretext": "WAZUH Alert"

"title":

"Listened ports status (netstat) changed (new port opened or closed)."

"text":

"ossec: output: 'netstat listening ports ': tcp 0.0.0.0:22 0.0.0.0:* 1052/sshd tcp6 :::22 :::* 1052/sshd tcp 127.0.0.1:25 0.0.0.0:* 1013/master tcp6 :::1:25 :::* 1013/master udp 0.0.0.0:68 0.0.0.0:* 810/dhclient udp 127.0.0.1:323 0.0.0.0:* 19308/chronyd udp6 :::1:323 :::* 19308/chronyd tcp 0.0.0.0:1514 0.0.0.0:* 11664/ossec-remoted tcp 0.0.0.0:1515 0.0.0.0:* 11548/ossec-authd tcp 0.0.0.0:55000 0.0.0.0:* 11503/python3"

▶ "fields": [3 items

0: { 2 items

"title": "Agent"

"value": "(000) - wazuh"

1: { 2 items

"title": "Location"

"value": "netstat listening ports"

2: { 2 items

"title": "Rule ID"

"value": "533 _(Level 7)_"

"ts": "1608446832.7860573"

Apps

App upload

App Creator

How it works - [Security API's](#) - [OpenAPI directory](#) - [OpenAPI Validator](#)
Apps interact with eachother in workflows. They are created with the app creator, using OpenAPI specification or manually in python. The links above are references to OpenAPI tools and other app repositories. There's thousands of them.

 CREATE FROM OPENAPI OR [CREATE FROM SCRATCH](#)



Siemonster

Version 1.0.0
SIEMonster App



[Testing](#) [Search](#) [SIEM](#)

Actions

Ping

Arguments

- username
- password
- url

Action Description

Returns Greetings from the APP. Is used to make sure, that APP works.

Your apps (49)



Search apps



Siemonster

SIEMonster App

[Testing](#) [Search](#) [SIEM](#)



NLP

An NLP app to classify text



AWS EC2

An app to interact with Amazon EC2



AWS S3

An app to interact with S3



Shuffle Tools

A tool app for Shuffle

[Shuffle](#) [Testing](#)



Hoxhunt

Hoxhunt app interface

Documentation

API

About

App creation

Apps

Architecture

Configuration

Features

Getting started

Organizations

Privacy policy

Triggers

Workflows

About

Shuffle started as a project in mid-2019 because of a few automation related problems that needed more attention in the **CERT/SIRT** community. Available automation solutions in the security industry are trying to do everything at once; handle tickets, indicators, threat intel and much more in a single platform, while our goal is to build the best solution to fit all your existing tools following the **Unix philosophy**: "Do One Thing and Do It Well".

Open Source

Focus for Shuffle has moved to an entirely open ecosystem. This includes, but is not limited to; the Shuffle product, open workflows, open apps, open standards (OpenAPI, Swagger).

Roadmap

This roadmap is meant more as a guide than as the exact order of operations. **Current version: 0.8.1**

- 0.1 - 0.5: Created basic features for automation, as well as use cases and frontend. This was before the project was open sourced.
- 0.6 - Usability: High focus on the workflow and app editor, as well as bugfixing after open sourcing.
- 0.7 - Improve: First larger release of Shuffle. Focus on users, schedules, app authentication and a better overview in general through the admin view.
- **0.8 - Integrate (current)**: Hybrid cloud features and
- 0.9 - Features: Search engine for apps, workflows and other important items. File control possibilities available.
- 1.0 - Launch: Categorized apps, proper use-cases, dashboard control and a real tutorial
- 1.1 - Business: Reporting, Risk transparency, manager focus
- 1.2 - OSS: **Open Source tool expansion**

Organization

Multi-tenant control

Organization

ORGANIZATION

USERS

APP AUTHENTICATION

ENVIRONMENTS


SCHEDULES

FILES

HYBRID

Organization overview

On this page you can configure individual parts of your organization. [Learn more](#)



Name

Shuffle AS

Description

Creating security automation solutions for the good of the general public

SAVE CHANGES





























Cloud synchronization

What does **cloud sync** do? Cloud synchronization is a way of getting more out of Shuffle. Shuffle will **ALWAYS** make every option open source, but features relying on other users can't be done without a collaborative approach.

Cloud Apikey

STOP SYNC

Cloud sync features

 Webhook 	 Schedules 	 User Input 
 Send Mail 	 Send Sms 	 Updates 
 Notifications 	 Email Trigger 	 App Executions 
 Workflow Executions 	 Apps 	 Workflows 
 Autocomplete 	 Authentication 	



ORGANIZATION



USERS



APP AUTHENTICATION



ENVIRONMENTS



SCHEDULES



FILES



HYBRID



User management

Add, edit, block or change passwords. [Learn more](#)

[ADD USER](#)

Username	API key	Role	Active	Actions
admin	db0373c6-1083-4dec-a05d-3ba73f02ccd4	Admin	True	EDIT USER GET NEW API KEY
testing	887c003a-11be-4579-9e22-3cda3b5f67da	User	False	EDIT USER GET NEW API KEY
user101		User	True	EDIT USER GET NEW API KEY



ORGANIZATION



USERS



APP AUTHENTICATION



ENVIRONMENTS



SCHEDULES



FILES






HYBRID



App Authentication

Control the authentication options for individual apps. **Actions can be destructive!** [Learn more](#)

Icon	Label	App Name	Workflows	Action amount	Fields	Actions
	bedrift 3	IBM QRadar	1	0	url	DELETE
	Fredrik login	owa	1	1	username, password, server, build, account, verifyssl	DELETE
	VirusTotal app	VirusTotal v3	2	6	apikey	DELETE
	New auth Shuffle	thehive	1	1	apikey, url	DELETE

[ORGANIZATION](#)[USERS](#)[APP AUTHENTICATION](#)[ENVIRONMENTS](#)[SCHEDULES](#)[FILES](#)[HYBRID](#)

Environments

Decides what Orborus environment to execute an action in a workflow in. [Learn more](#)

[ADD ENVIRONMENT](#)[Show archived](#)

Name	Orborus running (TBD)	Type	Default	Actions	Archived
Hallo	TBD	onprem	SET DEFAULT	ARCHIVE	false
Shuffle	TBD	onprem	true	ARCHIVE	false



ORGANIZATION



USERS



APP AUTHENTICATION



ENVIRONMENTS



SCHEDULES



FILES



HYBRID



Schedules

Schedules used in Workflows. Makes locating and control easier. [Learn more](#)

Interval

Environment

Workflow

Argument

Actions

15 seconds

onprem

d25cdc7a-4f72-4fb7-9caf-2121fe9a112a

{"example": {"json": "is cool"}}

STOP SCHEDULE



ORGANIZATION



USERS



APP AUTHENTICATION



ENVIRONMENTS



SCHEDULES



FILES



HYBRID



Files

Files from Workflows. [Learn more](#)

Created	Name	Workflow	Md5	Status	Filesize	Actions
2020-12-18T02:35:36.000Z	testing5.txt		c33cc365889c4fc693f2e5509d0cc232	active	132	
2020-12-18T02:35:35.000Z	test6.txt		62fffd27816eb43392e1548626a7d1ad	active	135	
2020-12-18T02:35:34.000Z	filename.txt		7327c0b6c814d98c88c92803881323fe	active	32	
2020-12-18T02:34:46.000Z	testing5.txt		c33cc365889c4fc693f2e5509d0cc232	active	132	
2020-12-18T02:34:41.000Z	test6.txt		62fffd27816eb43392e1548626a7d1ad	active	135	
2020-12-18T02:34:38.000Z	filename.txt		7327c0b6c814d98c88c92803881323fe	active	32	
2020-12-18T02:33:00.000Z	test6.txt		62fffd27816eb43392e1548626a7d1ad	active	135	

Recap

- Apps
 - Actions
 - Parameters
 - Files
- App Creation
 - GUI - OpenAPI
 - CLI - Python
- Workflows
 - Files
 - Triggers
 - Webhook
 - Schedule
 - Subflow
 - User input
 - Authentication
 - Variables
 - Conditions
 - Autocompletion
- Organizations
 - Organization control
 - Cloud access
 - Users
 - Environments
 - Authentication
 - Schedules
 - Files

Workflows

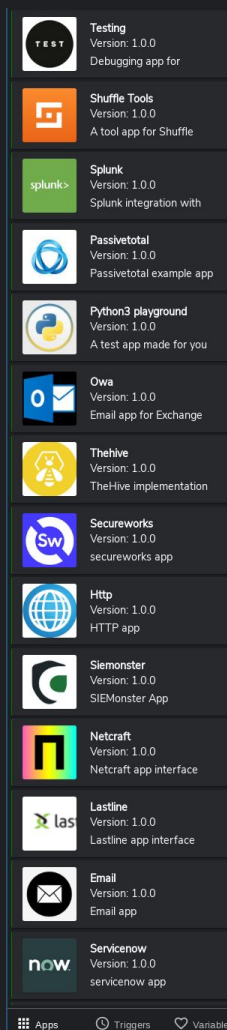
No-code automation

Use-case showcase

- SIEM SSH alert -> Block IP in AWS Firewall
- S3 honeypot -> Block IP and add to MISP
- Schedule mail -> TheHive alert with attachments

Workflows

- What are they
- Who can make them
- How are they made
- How are they shared

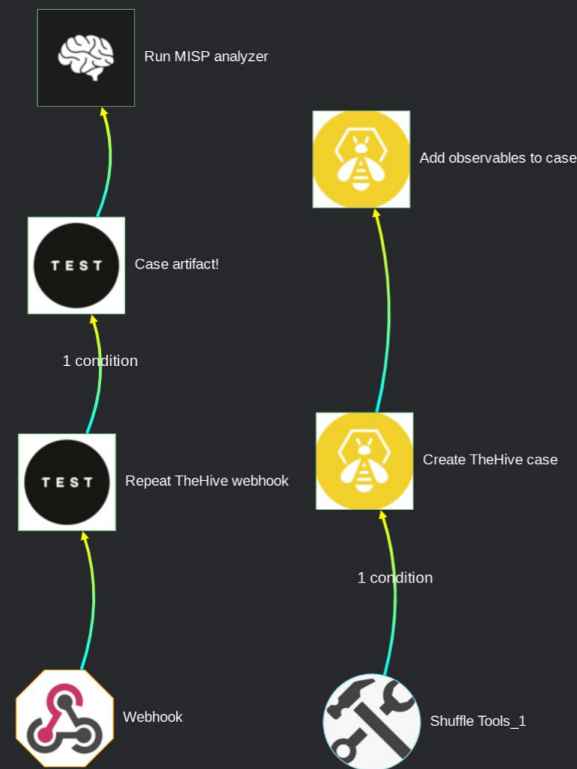


A screenshot of a workflow catalog interface. It displays a list of applications, each with an icon, a name, a version number, and a brief description. The applications listed are:

- Testing** (Version: 1.0.0): Debugging app for
- Shuffle Tools** (Version: 1.0.0): A tool app for Shuffle
- Splunk** (Version: 1.0.0): Splunk integration with
- Passivetotal** (Version: 1.0.0): Passivetotal example app
- Python3 playground** (Version: 1.0.0): A test app made for you
- Owa** (Version: 1.0.0): Email app for Exchange
- Thehive** (Version: 1.0.0): TheHive implementation
- Secureworks** (Version: 1.0.0): secureworks app
- Http** (Version: 1.0.0): HTTP app
- SIEMONSTER** (Version: 1.0.0): SIEMONSTER App
- Netcraft** (Version: 1.0.0): Netcraft app interface
- Lastline** (Version: 1.0.0): Lastline app interface
- Email** (Version: 1.0.0): Email app
- ServiceNow** (Version: 1.0.0): servicenow app

At the bottom of the catalog, there are tabs for 'Apps', 'Triggers', and 'Variables'.

Workflows - IOC parser - Medium post 4



Execution Argument



Downloading workflows

Workflows (35)



Hook test



EDIT



hook

EC2 testing_copy_copy



EDIT



test

EC2 testing_copy



EDIT



test

EC2 testing



Load workflows from github repo



Repository (supported: github, gitlab, bitbucket)

<https://github.com/frikky/shuffle-workflows>



Branch (default value is "master"):

master

Authentication (optional - private repos etc):

Username / APIkey (optional)

Password (optional)



CANCEL

SUBMIT

Your first Workflow

Workflows (35)



Hook test



EDIT



hook

EC2 testing_copy_copy



EDIT



test

EC2 testing_copy



EDIT



test

EC2 testing

New workflow



Demo Workflow

Description

Demo workflow



CANCEL

SUBMIT

Started: 2020-12-20T07:05:45.000Z



Testing
Version: 1.0.0
Debugging app for



Shuffle Tools
Version: 1.0.0
A tool app for Shuffle



AWS EC2
Version: 1.0.0
An app to interact with



Hoxhunt
Version: 1.0.0
Hoxhunt app interface



Email
Version: 1.0.0
Email app



Archive.today
Version: 1.0.0
Archive.Today app



Recordedfuture
Version: 1.0.0
Recordedfuture example



Python3 playground
Version: 1.0.0
A test app made for you



NLP
Version: 1.0.0
An NLP app to classify



ServiceNow
Version: 1.0.0
servicenow app

Workflows > Demo Workflow



Start node

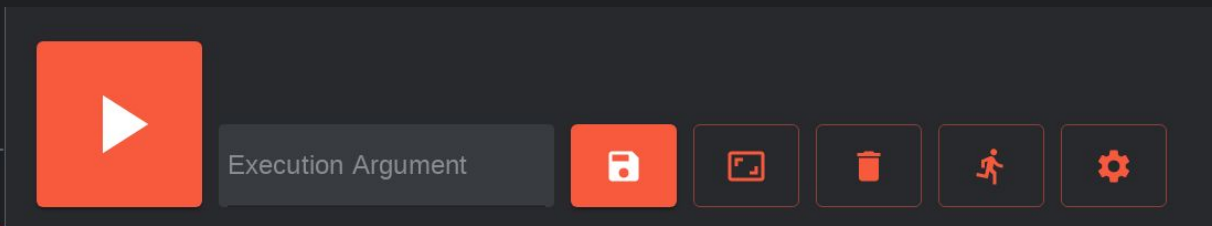


Execution Argument



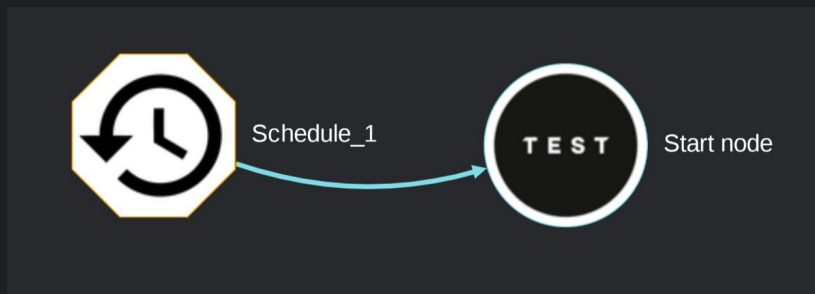
Features

- Save & Execute
 - See executions
 - Startnode
 - Workflow configuration
 - Execution Argument
 - Triggers
 - Variables
 - Delete nodes
- Apps
 - Actions
 - Parameters
 - Files
 - Autocompletion
 - Authentication



Execute

- Manual
- Execution Argument
- Variables
- Triggers
 - Schedule
 - Webhook
- Executions



A screenshot of the Airflow web interface for a workflow named "Demo Workflow". The interface is dark-themed. At the top, it says "Workflows › Demo Workflow". On the right side, there is a sidebar with a "Testing" tab selected, which has a red box around it. Below the tab, there is a dropdown menu with "What are actions?". Further down, there are fields for "Name" (containing "Start node") and "Environment" (containing "Shuffle"). Below these is an "Actions" section with a dropdown menu showing "Repeat back to me". Underneath is an "Arguments" section with a "Call" action selected, and a text input field containing "\$exec". At the bottom of the sidebar, there is a "Start node" label. In the main area, there is a black circular node with "TEST" in white, also labeled "Start node". A red arrow points from this node to the "Testing" tab in the sidebar. At the bottom of the interface, there is a red play button icon, a text input field containing "hello", and a row of icons for saving, refreshing, deleting, pausing, and settings.

Apps

- Draggable
- Contains actions
 - Containing arguments
 - Authentication



Testing
Version: 1.0.0
Debugging app for



Shuffle Tools
Version: 1.0.0
A tool app for Shuffle



Archive.today
Version: 1.0.0
Archive.Today app



Lastline
Version: 1.0.0
Lastline app interface



Splunk
Version: 1.0.0
Splunk integration with



Passivetotal
Version: 1.0.0
Passivetotal example



ServiceNow
Version: 1.0.0
servicenow app



AWS S3
Version: 1.0.0
An app to interact with
--



Siemonster
Version: 1.0.0
SIEMonster App



Hoxhunt
Version: 1.0.0
Hoxhunt app interface

Variables

- Execution Argument
- Triggers
- Previous actions
 - Successful
 - Failed
- Workflow Variables
- Execution Variables

What are **WORKFLOW** variables?

NEW WORKFLOW VARIABLE

What are **EXECUTION** variables?

NEW EXECUTION VARIABLE

Workflow Variable


Demo variable


Description

Demo data

CANCEL SUBMIT

 Apps

 Triggers

 Variables

Actions

- Name
- Authentication
- Environment
- Parameters
 - Required
 - Optional

Testing

SET STARTNODE

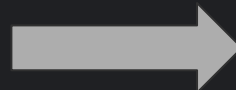
◀ What are actions?

Name

Start node

Actions

Hello world



thehive

SET
STARTNODE

◀ What are actions?

Name

thehive_1

Authentication

TheHive for Customer X - (1.0... +




Environment


Shuffle




Actions


Create alert




Parameters


● Type   

incident 

● Source   

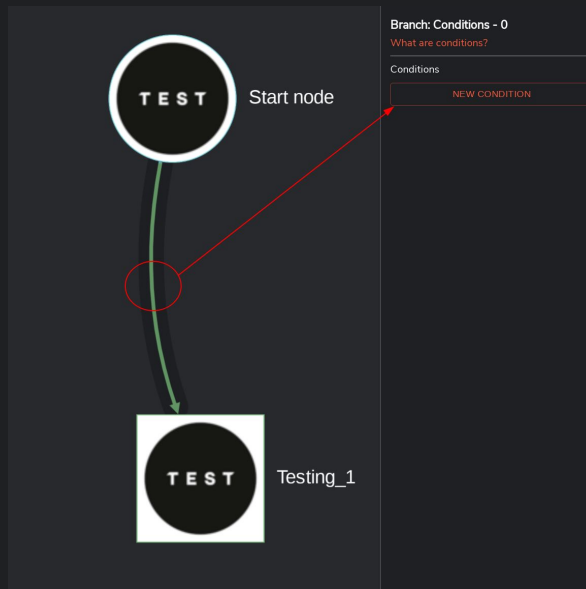
SIEM 

● Sourceref   

incident-1234 

Conditions

- If statements
- AND
- Loops



Condition

Condition

source destination

= Static value EQUALS Static value

Autocomplete Autocomplete

SUBMIT

Condition

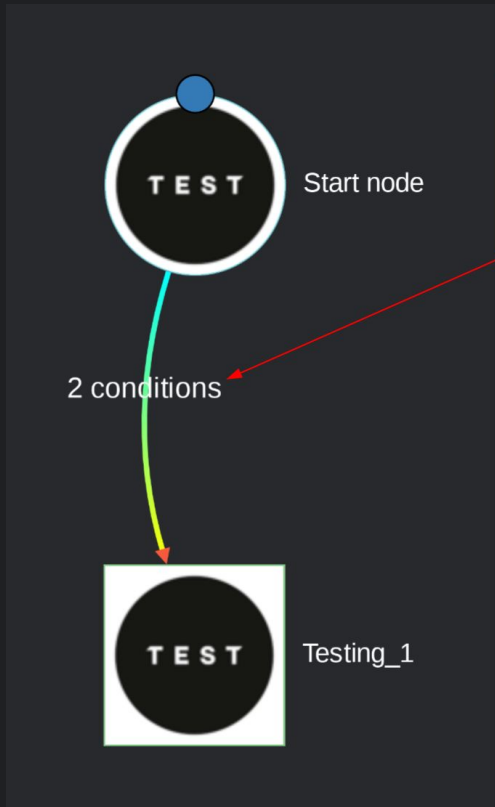
Condition

source destination

! true EQUALS false

Autocomplete Autocomplete

SUBMIT



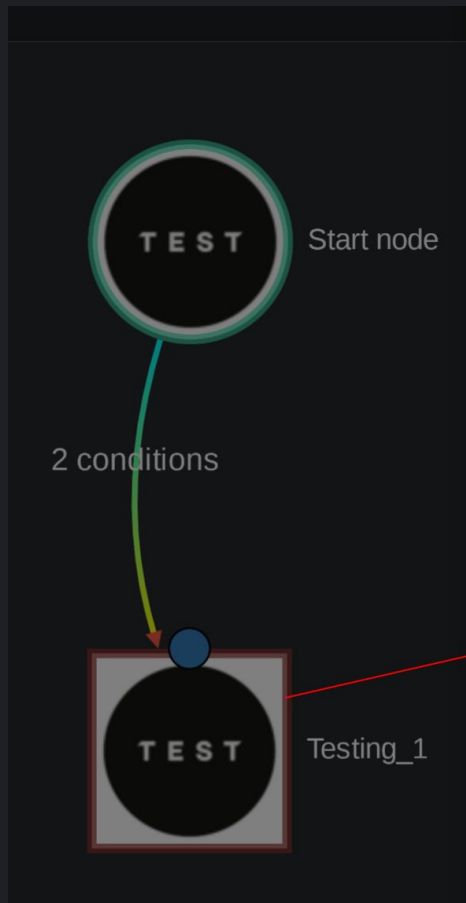
Branch: Conditions - 0

What are conditions?

Conditions

true	equals	false	⋮
DATA	matches regex	\w+	⋮

NEW CONDITION



← See other Executions

Executing Workflow

Status: FINISHED


Started: 2021-01-07T10:49:42.000Z

Finished: 2021-01-07T10:49:52.000Z

Source: default

☐ Show failed / skipped actions

Actions

◀  **Start node**
repeat_back_to_me

Status SUCCESS

Result

◀  **Testing_1**
hello_world

Status FAILURE

Result Failed condition: true equals false

Variable

- Triggers - \$exec
- Apps - \$node_name
- Variables - \$variable_name
- JSON

The screenshot displays the 'Demo Workflow' interface. In the center, a circular node labeled 'TEST' is identified as the 'Start node'. To the right, a 'Testing' sidebar contains a 'Parameters' section where the variable '\$exec' is highlighted with a red box. A red arrow points from this box to a plus icon in the bottom right corner of the workflow canvas. At the bottom of the canvas, a red play button is next to an 'Execution Argument' input field, which is also highlighted with a red box. Below the input field are icons for saving, viewing, deleting, running, and settings.

Nested variables (JSON)

- JSON

```
$exec = {"name": "Fredrik", "product": {"name": "Shuffle"}}
```

How do we get these?

- Fredrik
- Shuffle

Nested variables (JSON) 2

```
$exec = {"name": "Fredrik", "product": {"name": "Shuffle"}}
```

```
Fredrik: $exec.name
```

```
Shuffle: $exec.product.name
```

```
{"hashes": [  
  "7c401bde8cafc5b745b9f65effbd588f",  
  "177ae9a7fc02130009762858ad182678"  
]}
```

Loops

- ```
{"hashes": [
 "7c401bde8cafc5b745b9f65effbd588f",
 "177ae9a7fc02130009762858ad182678",
 "52f05ee28bcfec95577d154c62d40100"
]}
```
- `$exec.hashes.#`



Virustotal\_search

Virustotal

SET STARTNODE

What are  
actions?

Name

Virustotal\_search

Authentication

Virustotal API - (1.0.0)



Actions

Get hash

Parameters

Resource



`$exec.hashes.#`



Ssl\_verify



False - default=True



# Triggers - \$exec



## Webhook

Simple HTTP webhook



## Shuffle Workflow

Control another workflow



## User Input

Wait for user input



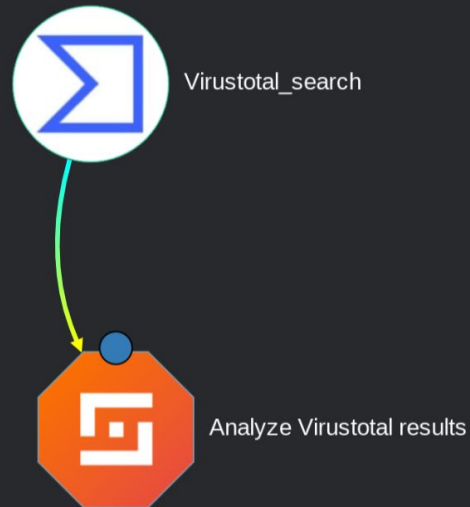
## Schedule

Schedule execution time

- Webhook
  - Best for instant workflow trigger integrations (e.g. from TheHive)
- Shuffle Workflow
  - Behaves like an Action
- User Input
  - Waits for user before continue
- Schedule
  - Executes workflow on a user-defined schedule

# Sub workflows

- Sub-flows - why?
- Use-case:
  - Many emails -> many attachments
  - Loop(s) within loop(s)
- Reusability



## Shuffle Workflow

What are subflows?

Name

Analyze Virustotal results

Parameters

Select a workflow to execute

IOC parser - Medium post 4

Explore selected workflow

Execution Argument:

`$VirusTotal_search`

API-key:

`db0373c6-1083-4dec-a05d-3ba73f02ccd4`



# Authentication

- Developer defined actions
- Organization wide

**Virustotal** SET STARTNODE

What are actions?

**Authenticate Virustotal:** +

**Actions**

**Parameters**

🔒 **Apikey** ✎ | 📱 | ❤️

+

● **Resource** ✎ | 📱 | ❤️

+

● **Ssl\_verify** ✎ | 📱 | ❤️

+

## Authentication for Virustotal

### What is this?

These are required fields for authenticating with Virustotal

### Name - what is this used for?

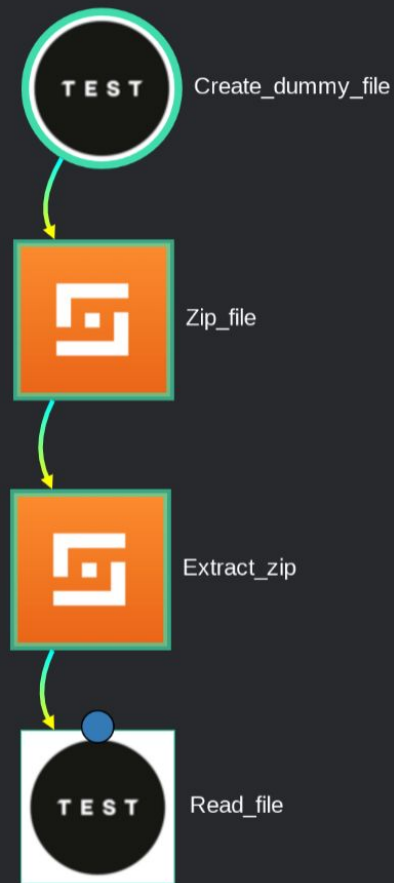
The API endpoint to use (URL) - predefined in the app

🔒 **apikey**

CANCEL SUBMIT

# Files

- Created by apps
- Abstracted by away ID
- Organization controlled



# Executions

- Why look at it again?
- Result exploration
- Result listing
- Trigger-view

**All Executions**

REFRESH EXECUTIONS

|   |                     |     |   |
|---|---------------------|-----|---|
| ▶ | 2021-01-13 13:53:15 | 6/6 | > |
| ▶ | 2021-01-13 13:51:55 | 5/5 | > |
| ▶ | 2021-01-13 13:51:04 | 5/5 | > |
| ▶ | 2021-01-13 13:48:10 | 5/5 | > |
| ▶ | 2021-01-13 13:44:48 | 5/5 | > |
| ▶ | 2021-01-13 13:43:33 | 5/5 | > |
| ▶ | 2021-01-13 09:28:14 | 4/4 | > |
| ▶ | 2021-01-13 09:24:44 | 4/4 | > |
| ▶ | 2021-01-13 04:14:13 | 4/4 | > |
| ▶ | 2021-01-13 04:12:56 | 4/4 | > |
| ▶ | 2021-01-13 04:11:00 | 4/4 | > |
| ▶ | 2021-01-13 04:08:47 | 2/2 | > |

← See other Executions

## Executing Workflow

**Status:** FINISHED  
**Started:** 2021-01-13T09:28:14.000Z  
**Finished:** 2021-01-13T09:28:27.000Z  
**Source:** default

### Actions

◀ **Create\_dummy\_file**  
upload\_file

**Status SUCCESS**

▶ "Results for Create\_dummy\_file" :  
{  
...} 2 items

◀ **Zip\_file**  
inflate\_archive

**Status SUCCESS**

▶ "Results for Zip\_file" : {...}  
} 2 items

# Executions - 2

- Movable
- Popout
- Discovery

**Testing**

What are actions?

SET STARTNODE

← See other Executions

**Testing Workflow**

Name

Create\_dummy\_file

**Actions**

Upload file

**Parameters**

Filename

testfile.txt

Data

some\_data\_here

**Status: FINISHED**

Started: 2021-01-13T09:28:14.000Z

Finished: 2021-01-13T09:28:27.000Z

Source: default

**Actions**

Create\_dummy\_file

upload\_file

**Status SUCCESS**

```
"Results for Create_dummy_file": {
 "result": "Successfully put your data in a file"
 "file_ids": [1 item
 0 : "34ab18a0-3883-4a62-98ca-22edf910e2ca"
]
}
```

**Create\_dummy\_file**

upload\_file

✓ ! 👁 ✕

**Status SUCCESS**

```
"Results for Create_dummy_file": { 2 items
 "result": "Successfully put your data in a file"
 "file_ids": [1 item
 0 : "34ab18a0-3883-4a62-98ca-22edf910e2ca"
]
}
```

# Executions - 3

- General:

- Copy values
- Copy autocompletion

- Buttons

- Success
- Error
- See execution
- Close



## Create\_dummy\_file

upload\_file



Status SUCCESS

```
▼ "Results for Create_dummy_file" : { 2 items
 "result" : "Successfully put your data in a file"
 ▼ "file_ids" : [1 item
 0 : "34ab18a0-3883-4a62-98ca-22edf910e2ca"
]
}
```

# Recap - Workflows

- Dashboard

- Import
- Export
- Cloud download
- Executions
- Execution results

- Workflow

- Save
- Execute
- Global Configuration
- Execution Argument
- Variables
- Node management
- Execution exploration

- Apps

- Actions
- Arguments
- Files
- Autocompletion
- Authentication

- Variables

- Workflow variables
- Execution variables

- Files

- List
- Upload
- Download

- Conditions

- Variables
- Nested JSON
- Loops

# Apps



## App upload

### App Creator

How it works - Security API's - OpenAPI directory - OpenAPI Validator  
Apps interact with eachother in workflows. They are created with the app creator, using OpenAPI specification or manually in python. The links above are references to OpenAPI tools and other app repositories. There's thousands of them.



CREATE FROM OPENAPI

OR

CREATE FROM SCRATCH



**Siemonster**

Version 1.0.0

SIEMonster App



#### Actions

Ping

#### Parameters

- username
- password
- url

#### Action Description

Returns Greetings from the APP. Is used to make sure, that APP works.

#### Example return

SIEMonster welcomes from %hostname%

## Your apps (49)



Search apps



### Shuffle OpenAPI

Integrations to execute actions in Shuffle

SOAR

Automation

Shuffle



### Wazuh API REST

The Wazuh API is an open source RESTful API that allows for ...

API Info

Active-response

Agents



### Shodan

Automated generation of Shodan



### Recorded Future

Automated generation of Recorded Future



### UnpacMe

# Introduction Welcome to the UNPACME API! All the malware ...

public

unpacking

feed



### AIL framework

AIL framework - Framework for Analysis of Information Leaks

information leak



### CIRCL CVE Search



# App downloads

Your apps (49)



Load from github repo

Repository (supported: github, gitlab, bitbucket)



Branch (default value is "master"):

Authentication (optional - private repos etc):



CANCEL

FORCE UPDATE

SUBMIT



### AWS EC2

An app to interact with Amazon EC2

- Manually created (python)



### Virustotal

Based on <https://developers.virustotal.com/reference#file-ne...>



- Generated by Shuffle

- Active (usable) app



### Archive.org

Archive.org app

archive

search

- Inactive app



### Hashdd

API for <https://hashdd.com>

# App exploration

## App upload

### App Creator

How it works - Security API's - OpenAPI directory - OpenAPI Validator  
Apps interact with eachother in workflows. They are created with the app creator, using OpenAPI specification or manually in python. The links above are references to OpenAPI tools and other app repositories. There's thousands of them.



CREATE FROM OPENAPI

OR

CREATE FROM SCRATCH



### VirusTotal

Version 1.0.0

Based on <https://developers.virustotal.com/reference#file-network-traffic>

ACTIVATE APP



URL: <https://www.virustotal.com/vtapi/v2>

#### Actions

Get domain report

#### Parameters

- apikey
- domain
- ssl\_verify

## Your apps (49)



virustot



### VirusTotal

Based on <https://developers.virustotal.com/reference#file-network-traffic>



### VirusTotal

Based on <https://developers.virustotal.com/reference#file-network-traffic>

# App activation



**VirusTotal**

Version 1.0.0

Based on <https://developers.virustotal.com/reference#file-network-traffic>

ACTIVATE APP



URL: <https://www.virustotal.com/vtapi/v2>

## Actions

Get domain report ▼

## Parameters

- apikey
- domain
- ssl\_verify

# App activation - 1

Apps › Virustotalv2 - Demo

## General information

[Click here to learn more about app creation](#)



Name

Virustotalv2 - Demo

Description

Based on <https://developers.virustotal.com/reference#file-network-traffic>

# App activation - 2

## API information

Base URL - leave empty if user changeable

https://www.virustotal.com/vtapi/v2

Must start with http(s):// and CANT end with /.

## Authentication

API key

## API key

apikey

Can't be empty. Can't contain any of the following characters: !#\$%&'^+,-.\_~|]+\$

## Field type

Query

## Authentication for Virustotal

### What is this?

These are required fields for authenticating with Virustotal

### Name - what is this used for?

Auth july 2020

The API endpoint to use (URL) - predefined in the app

https://www.virustotal.com/vtapi/v2

 apikey

\*\*\*\*\*



CANCEL SUBMIT

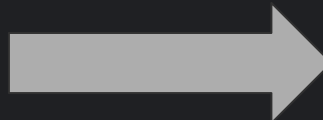
# App activation - 3

## Actions

Actions are the tasks performed by an app. Read more about actions and apps [here](#).

|   |      |                                    |           |        |
|---|------|------------------------------------|-----------|--------|
| ✓ | GET  | /comments/get - Get comments       | Duplicate | Delete |
| ✓ | POST | /comments/put - Write comment      | Duplicate | Delete |
| ✓ | GET  | /domain/report - Get domain report | Duplicate | Delete |
| ✓ | GET  | /ip-address/report - Get IP report | Duplicate | Delete |
| ✓ | GET  | /url/feed - Get URL feed           | Duplicate | Delete |
| ✓ | GET  | /url/report - Get URL report       | Duplicate | Delete |
| ✓ | POST | /url/scan - Get URL scan           | Duplicate | Delete |

NEW ACTION



VirusTotal2 -  
Demo

SET STARTNODE

What are  
actions?

Name

VirusTotal2 - Demo 1

- Get IP report
- Get URL feed
- Get URL report
- Get URL scan
- Get comments
- Get domain report
- Get hash
- Write comment

\*\*\*\*\*

Ssl\_verify

False - default=True

# App activation - 4

## Tags

Threat Intelligence

TI

TI

SAVE

App ready to build

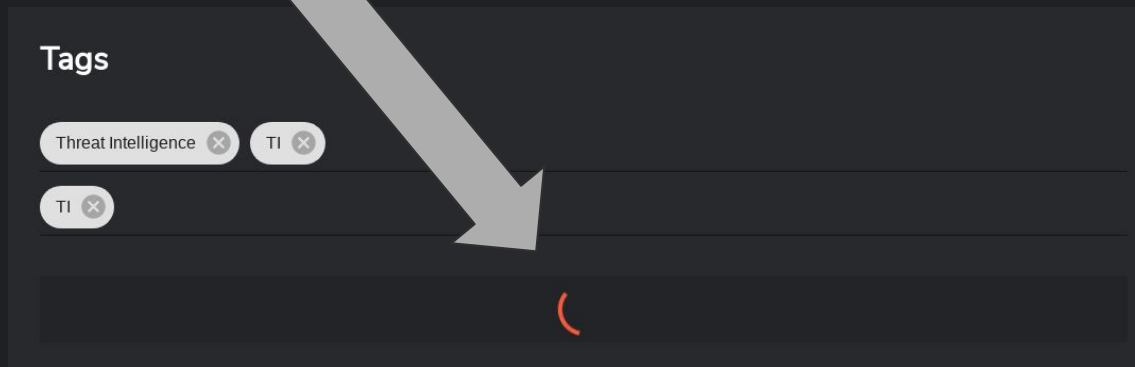
App building

## Tags

Threat Intelligence

TI






TI






# App usage

Workflows Apps Docs

-  **Testing**  
Version: 1.0.0  
Debugging app for
-  **Shuffle Tools**  
Version: 1.0.0  
A tool app for Shuffle
-  **VirusTotal2 - Demo**  
Version: 1.0.0  
Based on ...
-  **Archive.today**  
Version: 1.0.0  
Archive.Today app
-  **Lastline**  
Version: 1.0.0  
Lastline app interface

Workflows > Demo Workflow

 VirusTotal2 - Demo\_1

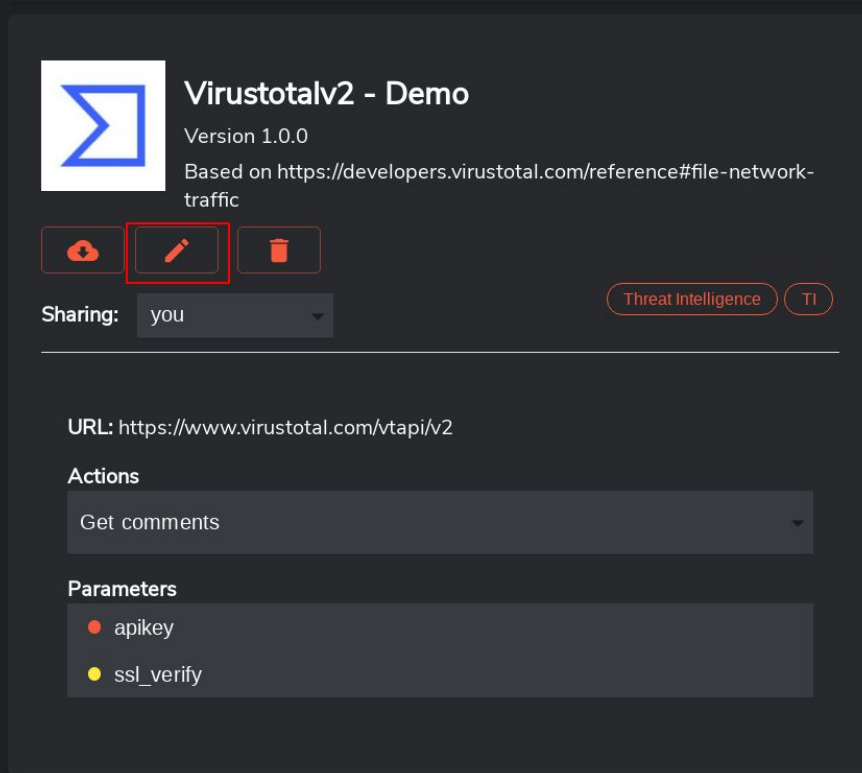
Build finished:  
instantly usable

# Further development

- Download app
- Edit app
- Delete app

## Requirements:

- Basic HTTP understanding



The screenshot shows the interface of the 'Virustotalv2 - Demo' application. At the top left is a logo consisting of a blue square with a white stylized 'Σ' inside. To the right of the logo, the text 'Virustotalv2 - Demo' is displayed, followed by 'Version 1.0.0' and a description: 'Based on <https://developers.virustotal.com/reference#file-network-traffic>'. Below this, there are three icons in a row: a cloud with a download arrow, a pencil (highlighted with a red box), and a trash can. To the right of these icons is a 'Sharing:' label followed by a dropdown menu showing 'you'. Further right are two orange buttons labeled 'Threat Intelligence' and 'TI'. Below a horizontal line, the 'URL:' is shown as 'https://www.virustotal.com/vtapi/v2'. Under the 'Actions' section, there is a dropdown menu currently showing 'Get comments'. Under the 'Parameters' section, there are two items: 'apikey' with a red dot and 'ssl\_verify' with a yellow dot.

**Virustotalv2 - Demo**  
Version 1.0.0  
Based on <https://developers.virustotal.com/reference#file-network-traffic>

Sharing: you

URL: <https://www.virustotal.com/vtapi/v2>

**Actions**  
Get comments

**Parameters**  
• apikey  
• ssl\_verify

# App development - add action

- Actions
  - POST
  - GET
  - DELETE
  - ...
- Name & Description

Virustotal File search

### Actions

Actions are the tasks performed by an app. Read more about actions and apps [here](#).

|                                     |      |                                    |                           |                        |
|-------------------------------------|------|------------------------------------|---------------------------|------------------------|
| <input checked="" type="checkbox"/> | GET  | /comments/get - Get comments       | <a href="#">Duplicate</a> | <a href="#">Delete</a> |
| <input checked="" type="checkbox"/> | POST | /comments/put - Write comment      | <a href="#">Duplicate</a> | <a href="#">Delete</a> |
| <input checked="" type="checkbox"/> | GET  | /domain/report - Get domain report | <a href="#">Duplicate</a> | <a href="#">Delete</a> |
| <input checked="" type="checkbox"/> | GET  | /ip-address/report - Get IP report | <a href="#">Duplicate</a> | <a href="#">Delete</a> |
| <input checked="" type="checkbox"/> | GET  | /url/feed - Get URL feed           | <a href="#">Duplicate</a> | <a href="#">Delete</a> |
| <input checked="" type="checkbox"/> | GET  | /url/report - Get URL report       | <a href="#">Duplicate</a> | <a href="#">Delete</a> |
| <input checked="" type="checkbox"/> | POST | /url/scan - Get URL scan           | <a href="#">Duplicate</a> | <a href="#">Delete</a> |
| <input checked="" type="checkbox"/> | GET  | /file/report - Get hash            | <a href="#">Duplicate</a> | <a href="#">Delete</a> |

NEW ACTION

# App development - autocomplete

## /file/search

Search for files

GET <https://www.virustotal.com/vtapi/v2/file/search>

cURL Python

```
curl --request GET \
--url 'https://www.virustotal.com/vtapi/v2/file/search?apikey=<apikey>&query=<query>'
```

### QUERY PARAMS

**apikey\*** string

Your API key

**query\*** string

Search query

**offset** string

The offset value returned by a previous identical query, allows you to paginate over the results.

Copy curl

### New action

[Learn more about actions](#)

**Name**

Search for files

**Description**

Description

**Request**

GET

URL path / Curl statement

`u.virustotal.com/vtapi/v2/file/search?apikey=<apikey>&query=<query>'`

The path to use. Must start with /. Use {variablename} to have path variables

**Queries**

Required: bool Delete

query

Click required switch

- <https://developers.virustotal.com/reference#file-search>

# App development - finishing touches

## Request

GET

URL path / Curl statement

/file/search?query={query}

The path to use. Must start with /. Use {variablename} to have path variables

Queries

Required: ☒

Delete

query

Click required switch

NEW QUERY

Headers: static for the action

Accept: application/json  
Content-Type: application/json

Headers that are part of the request. Default: EMPTY

Example success response

```
{
 "email": "testing@test.com",
}
```

Helps with autocompletion and understanding of the endpoint

CANCEL

SUBMIT



GET

/file/report - Get hash

Duplicate

Delete



GET

/file/search?query={query} - Search for files

Duplicate

Delete

NEW ACTION

## Tags

Threat Intelligence

TI

Threat Intelligence

TI

SAVE

# Recap - Apps

- App Listing

- OpenAPI
- Python
- Tags
- Import
- Export
- Active / Inactive
- Search

- Selected App

- Edit
- Delete
- Activate
- Actions
- Parameters

- App Editor

- Name
- Description
- Image
- Base URL
- Authentication
  - Header
  - Query
- Tags

- App Editor Actions

- Name
- Description
- GET/POST/DELETE/...
- URL Path



# What we did NOT cover

- Debugging in depth

- Docker containers
- Execution issues
- Build issues
- Development issues

- Manual app creation

- Python
- Api.yaml <-> src/app.py
- Dockerfiles
- Hot Loading apps
- Testing apps

- Contributing

- Main repo
- Apps
- Workflows

- Shuffle cloud

- What's different?
- How is it useful for you?

- Configuration

- How to deploy
- How to configure it for scale

- Roadmap



# Use-case solving

Solving use-cases in class