Shuffle

Overview

Shuffle is am open source SOAR (Security Orchestration, Automation and Response) platform.
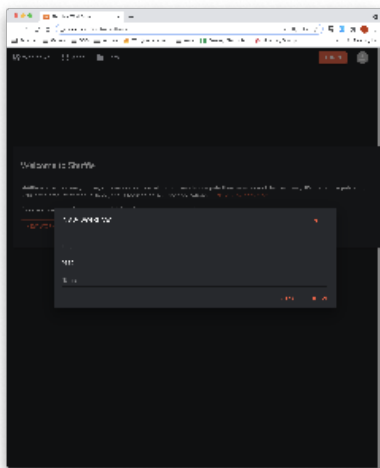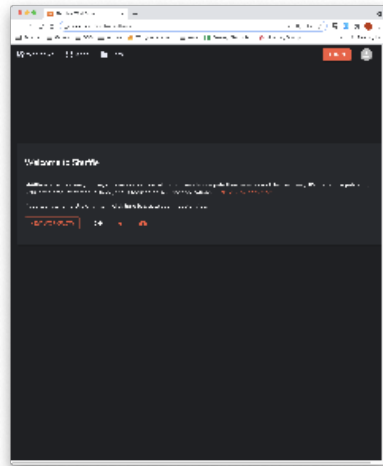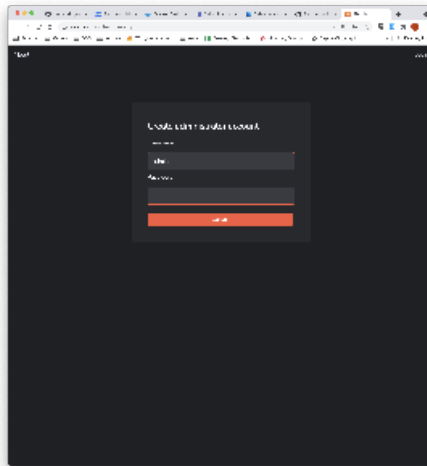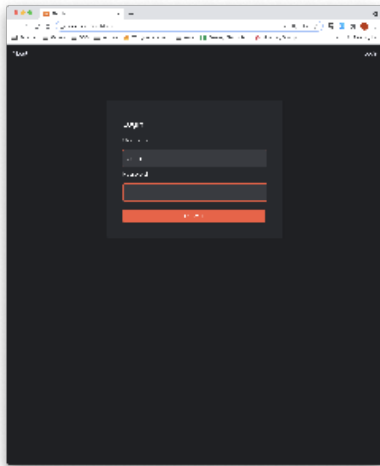
The point of a SOAR platform is to handle an incident end-to-end — automating before, during and after the incident.

Installation

```
git clone https://github.com/frikky/Shuffle
cd Shuffle
docker-compose up -d
```
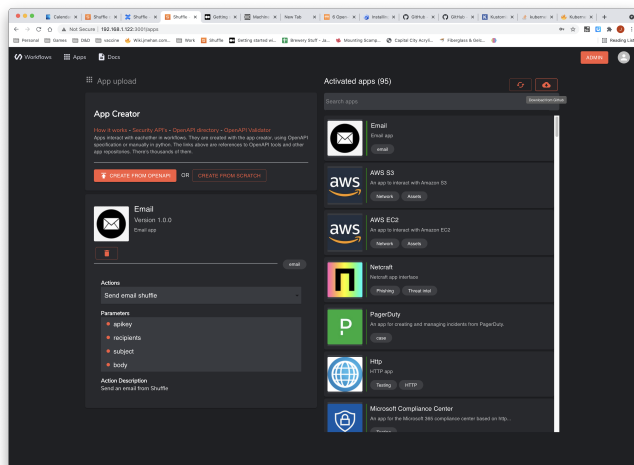
Navigate to http://localhost:3001/adminsetup
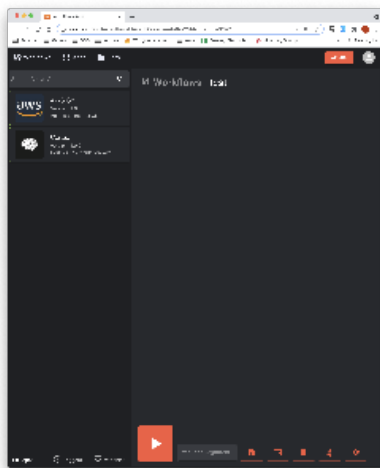
Download Apps

Shuffle doesn't come with all of the apps as part of the install.

From the Apps screen, click the "Download from GitHub" cloud icon in the top right corner.

Components
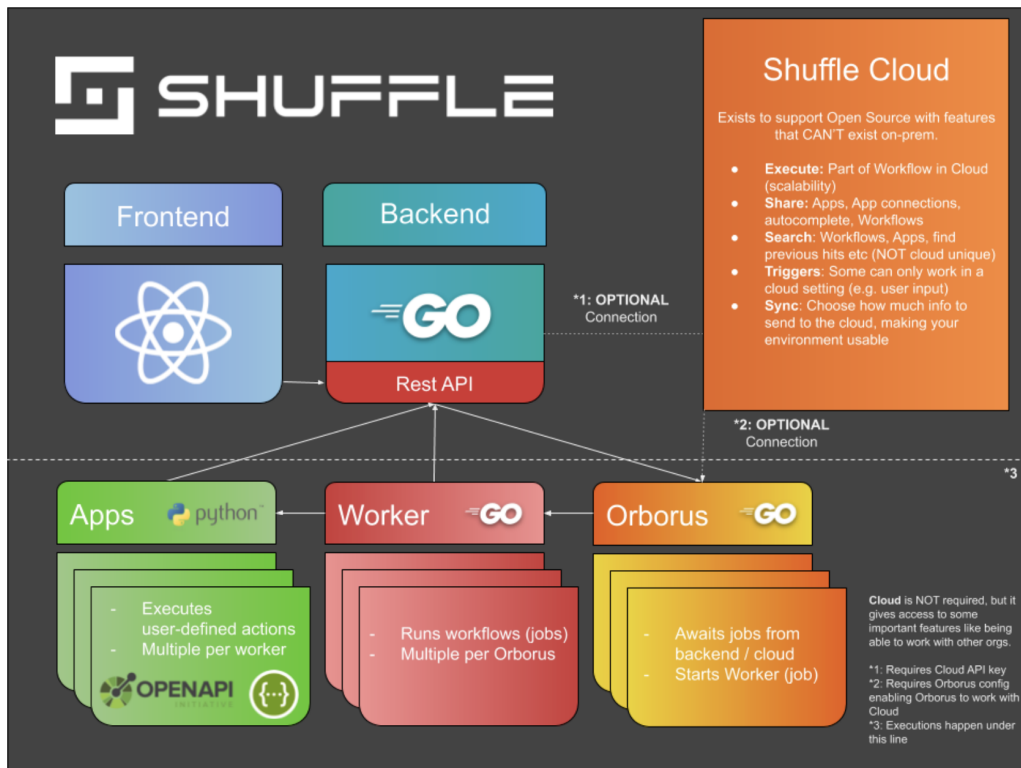
Typical Use Case

SIEM - Security information and event management -

- a set of tools and services offering a holistic view of an organization's information security.

SOAR - Security Orchestration, Automation and Response

Alert generated by SIEM is sent to SOAR for processing and response.

Shuffle includes:

- **Apps**
  - Actions
  - Parameters
  - Files

- **App Creation**
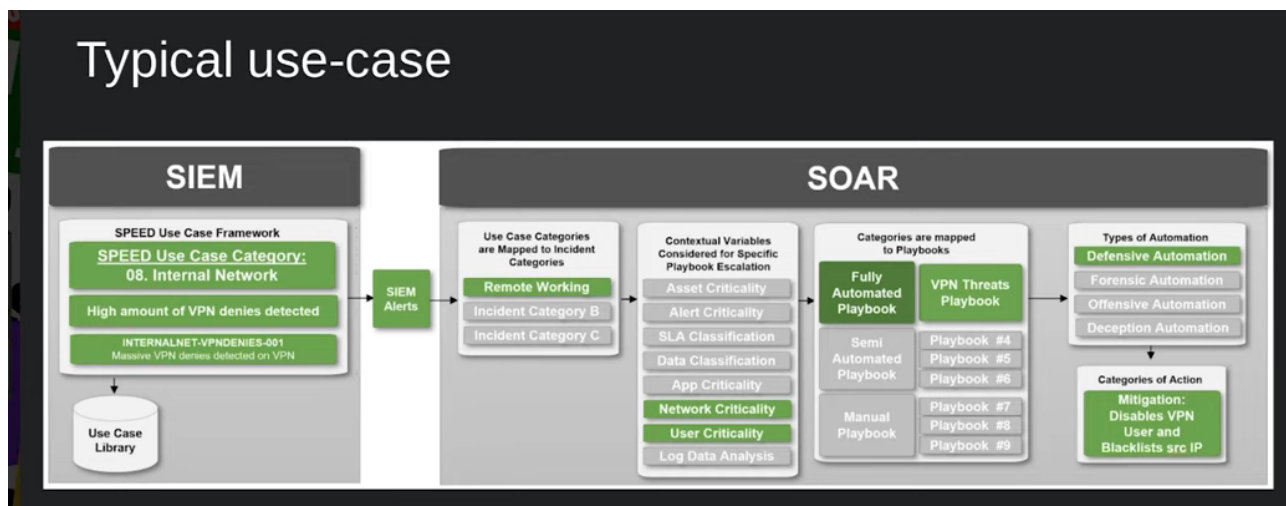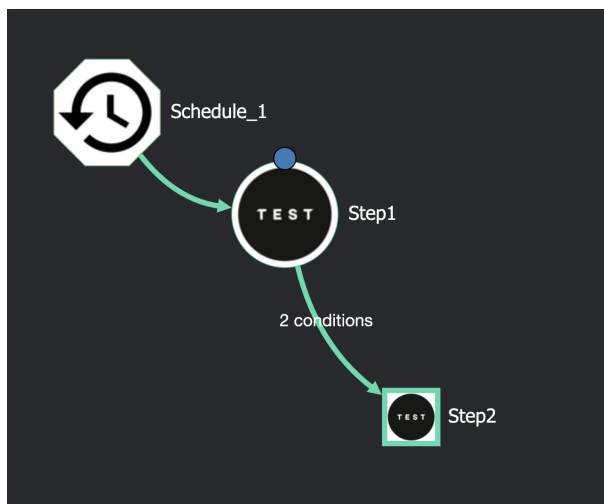 - GUI - OpenAPI
  - CLI - Python

- **Workflows**
  - Files
  - Triggers
    - Webhook
    - Schedule
    - Subflow
    - User input
  - Authentication
  - Variables
  - Conditions
  - Autocompletion

- **Organizations**
  - Organization control
  - Cloud access
  - Users
  - Environments
  - Authentication
  - Schedules
  - Files

Variables

Variable	Description
$exec	The variable passed to the executing workflow

Sample Workflow

Creating an App

Requirements

- Python3
- Pip3

Install WALKOFF

git clone https://github.com/nsacyber/WALKOFF.git

```
cd WALKOFF
```

```
./walkoff.sh up --build
```

References

Reference	URL
Shuffle - Open Source Plug and Play Security Automation	https://shuffler.io/
Repo	https://github.com/frikky/Shuffle
Introduction to Shuffle	https://medium.com/shuffle-automation/introducing-shuffle-an-open-source-soar-platform-part-1-58a529de7d12
Getting Started	https://medium.com/shuffle-automation/getting-started-with-shuffle-an-open-source-soar-platform-part-2-1d7c67a64244
[JSAC2021] Workshop: Shuffle the SOC - automating anything, anytime, anywhere	https://www.youtube.com/watch?v=PNuXCixYwDc&t=4144s
Creating Apps	https://shuffler.io/docs/apps
Open APIs	https://apis.guru/browse-apis/
App API	https://shuffler.io/docs/API
WALK OFF	https://github.com/nsacyber/WALKOFF
WALK OFF Doc	https://readthedocs.org/projects/walkoff/downloads/pdf/development/