WALKOFF
Intermediate Workflow

1. Clone the IDS Automation Example:

```
git clone https://github.com/walkoffcyber/ids-automation-example.git
```

2. Run the image setup script which will pull the images from Docker Hub as well as add the Elastalert Kibana Plugin to the Kibana image:

```
./image_setup.sh
```

3. Deploy the "*SimpleIDS*" stack:

```
docker stack deploy --compose-file=simple-ids-compose.yml simpleids
```

4. This stack contains:
   - Zeek (formerly Bro)
     i. This will generate logs from live interface data if you are on Linux, or ingest pcaps on Windows.
   - Elastic 7.4.0 stack (Elasticsearch, Filebeat, Kibana).
     i. Filebeat will pick up the following logs from Zeek: http.log, files.log, ssl.log, notice.log.
     ii. These logs will be parsed into their component fields and can be displayed in Kibana with the built-in Zeek dashboard that comes with version 7.
   - Elastalert
     i. This container monitors Elasticsearch and can be used to generate alerts of various types. In this example, we will use it to trigger a WALKOFF workflow.

- TheHive stack (TheHive, Cortex, Elasticsearch)
  i. TheHive is an open-source incident-response-focused ticketing system which we will use as the human-in-the-loop component.
  ii. Cortex is the analytic and response companion to TheHive, and will be used to trigger a WALKOFF workflow in response.

5. When you start the stack, the Elastic stack will take some time to start up. To monitor for when it is ready, use:

```
docker service logs -f simpleids_kibana
```

6. Once Kibana is ready, you'll need to perform the following single-line command to initialize Elastalert:

```
docker exec -it $(docker ps -qf "name=elastalert") \
      elastalert-create-index --config /opt/elastalert/config.yaml
```

This will create an index for elastalert to write data back to.

Note: From this point on, `*hostname*` will substitute for the hostname or IP of where you have launched this stack.

- **For example:** use 127.0.0.1 if you're using the browser on the same host.

7. Open a new tab in your browser and navigate to

```
http://hostname:5601/app/elastalert-kibana-plugin
```

You should see an existing example rule.

WALKOFF Intermediate Workflow

8. Open a new tab in your browser and navigate to

```
https://hostname:8080/walkoff/login
```

9. Log in, and create a workflow called *"ElastAlertExample"*. From the *"basics"* app, place an *"echo_json"* action on to the canvas and give it a placeholder object. Save the workflow and execute it to verify it runs.

10. Open another tab in your browser and navigate to

```
http://hostname:5601/app/kibana
```

    Within one minute, you should see Zeek (Bro) log data populating the *`filebeat-*`* index. If you do not, verify that the *`zeek`* directory is being populated by logs.

11. Open a new tab in your browser and navigate to http://example.com (this should be an HTTP address and not HTTPS). Refresh the page a few times.

12. Open the rule and test it, after a couple minutes the query should state that it would trigger on the data you have seen.

13. Open the WALKOFF tab again and navigate to the execution page - you should see a few workflows that have run with your data.