Sigma UI for Kibana

Installation Guide

v.0.7.3

2018

Sigma UI for Kibana

Uncoder is using **sigmac** script to convert sigma to different SIEM languages. It requires **python3** with libraries:

PyYAML>=3.11

Details: https://github.com/Neo23x0/sigma/tree/master/tools

To install Sigma UI plugin for your Kibana

1. Copy the file sigma-ui-xxxxx.zip to Kibana server and run the command:

```
/usr/share/kibana/bin/./kibana-plugin install file:///PATH_TO_FILE/sigma-ui-xxxxx.zip
```

Wait until the installation finishes, it may take few minutes to optimize and cache browser bundles. Restart Kibana to apply the changes.

If you get error: “Plugin installation was unsuccessful due to error "Incorrect Kibana version in plugin [uncoder]. Expected [6.2.2]; found [6.2.1]“, please open zip archive and modify file “./kibana/uncoder/package.json”: put version of your Kibana to field "version".

2. **Restart Kibana** to apply the changes.

In case after restart Kibana you don’t see any changes, go to /usr/share/kibana/optimize. Delete all files in the folder ‘optimize’ including subfolders. And restart Kibana.This will make Kibana to refresh it’s cache.

3. Sigma UI plugin is using indices:

- “sigma_doc” - for sigma documents;

Create index templates for these index from file **index_template_sigme_doc.txt**
To fill sigma docs and to index:
Copy to server which has access to Elasticsearch database file **sigma_import.zip**.

- Unzip archive **sigma_import.zip**
- Modify script **es_config.py**, put there Elasticsearch hostname, user and password.
- Run command

```
python /PATH_TO_FILE/import_es_index.py
```

Indices will be created and filled with sigma rules.

4. Now you can use Sigma UI plugin.