SOCRadar integration with Wazuh

Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance. **[1]**

Alarms and **Threat Feed** data that is provided by SOCRadar can be retrieved by Wazuh. We have provided sample code snippets written in **Python 3.7** that can be used to integrate SOCRadar and Wazuh.

There are 2 different code snippets for every supported APIs those produce 2 different output formats:

- **JSON**
- **CSV**

For the **Alarms** data there is an additional code snippet that produces in following output format:

- **CEF**

For the **Threat Feed** data there are additional code snippets that produce in following output format:

- **TXT**
- **XLSX**

Depending on your preferences one of the output format can be selected for the SOCRadar API output and can be provided to the Wazuh.

[1] https://wazuh.com/

External Libraries

For this integration the library named, requests is required. You may install it by running this command in your environment's terminal:

```
sudo pip install requests
```

Demonstration

SOCRadar's Alarms integration with Wazuh by using the script written in **Python 3.7** with **CSV** output format will be demonstrated under this section.

Navigate to **Integrations** page under the menu. After choosing **Wazuh section** select **CSV** format from dropdown and later click to **Copy to Clipboard button:**

Paste it into a **.py** file, for instance **socradar_alarms-wazuh.py.**

Set the necessary environment variable:

- **SOCRADAR_ALARMS_INTEGRATION_FOLDER**

After you set your environment variables successfully, you can proceed to execute the script that you have copied before.

```
python3 socradar_alarms-wazuh.py
```

This script will continuously collect data from SOCRadar API by sending GET requests in every 60 seconds and will create log files under the **SOCRADAR_ALARMS_INTEGRATION_FOLDER** until there will be any exceptions/keyboard interruptions. Log files will be created in an interval of 1 day. You can provide this folder to Wazuh and it can track down the log files consist of the SOCRadar alarms in CSV format. The interval of the log files creation and 60 seconds period of SOCRadar API requests can be changed to longer/shorter periods.

Scripts should run in VM Crontab.

```
Crontab_working_frequency cd Path_of_File && path_of_python file_name.py
```

```
E.g.: 5 6 * * * cd /home/socradar && /usr/bin/python file_name.py For feed
```

E.g.: 0 1 * * * cd /home/socradar && /usr/bin/python file_name.py For Alarm