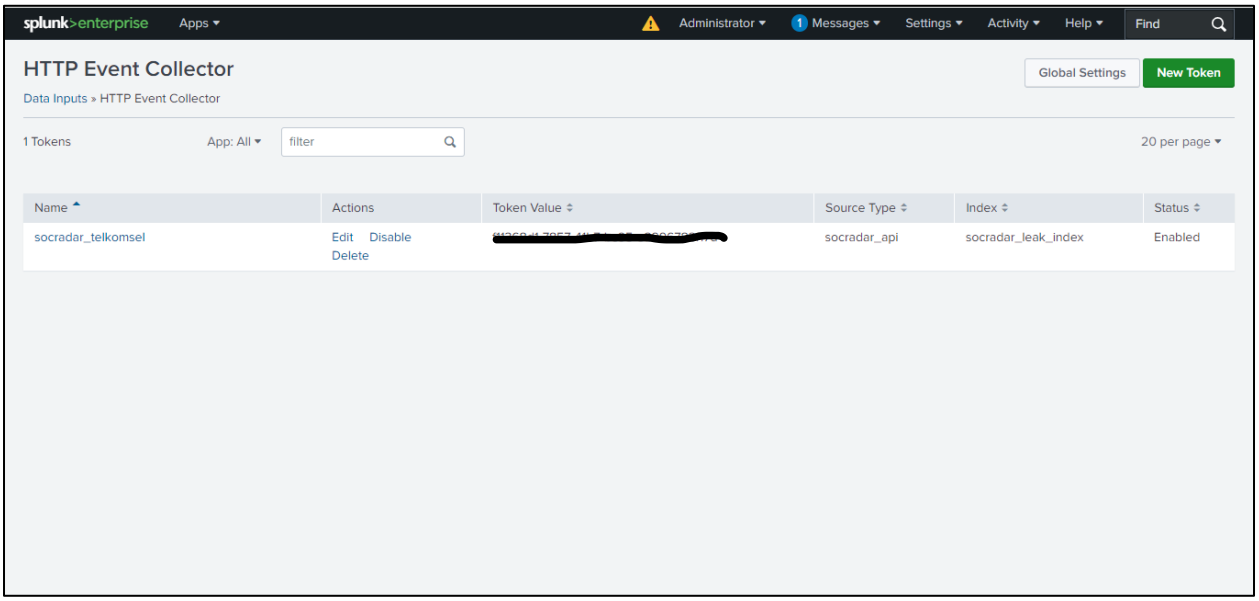
SOCRadar and Splunk Integration

I. Requirement (Pre-Installation)

- Splunk HTTP Event Collector (HEC)
- Splunk New Indexes (optional)
- Splunk New Source Type
- Splunk Alert Setup
- HEC URL and Token
- SOCRadar API token
- SOCRadar API path
- Python Script to pull data from SOCRadar API and send to Splunk HEC (Python 3.13 or higher)

II. Installation

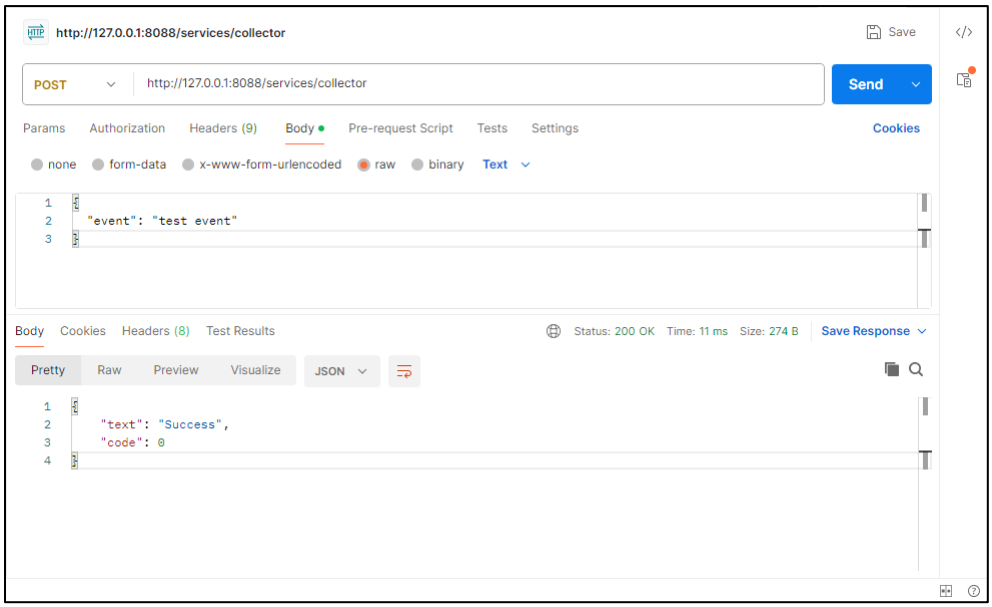
1. Create Splunk HTTP Event Collector (HEC)
    - Login to Splunk Dashboard
    - Go to **Settings --> Data --> Data Inputs --> HTTP Event Collector**
    - Choose **New Token** and create New HEC, you can choose the Source Type and index or create the new one.
    - When creating new HEC proccess are done, the token will appears or you can find the token in **Data Inputs --> HEC** menu as shown on the pictures below.



- Save the **HEC Token.**
- Test HEC Connection and open port using **curl** command :

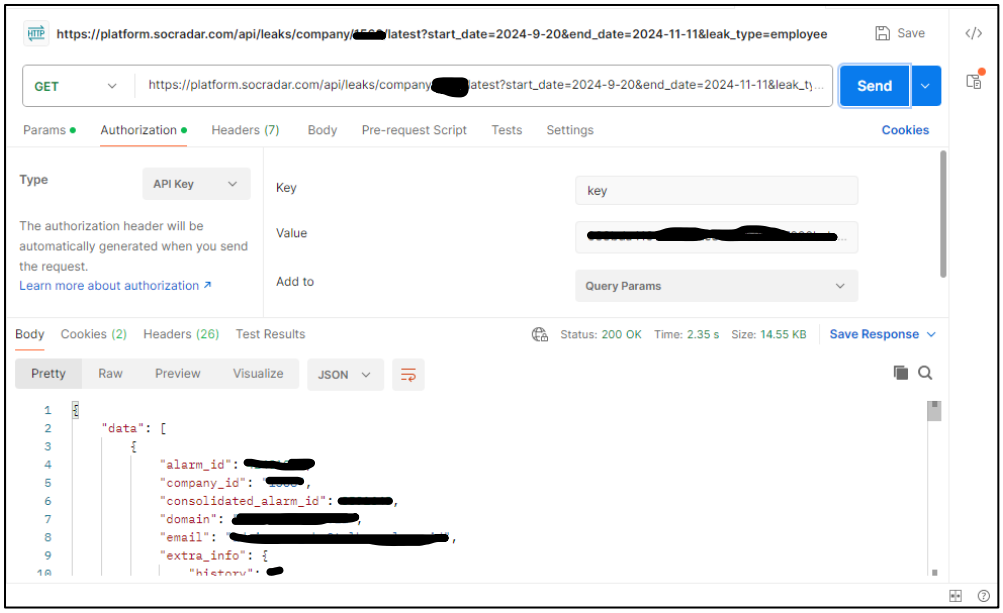
```
curl -k https://<domain>:8088/services/collector -H "Authorization: Splunk <TOKEN>"
-d '{"event": "test event"}'
```

- Or test by using Postman as shown below :



- Success Status in Postman output means HEC was configure successfully.

2. Generate API Token in SOCRadar
   - Go to **SOCRadar Dashboard --> Settings --> API Options**
   - In "**Company API Key**" field, copy the API key or regenerate it by click the key ico button
   - Save SOCRadar API key
   - Test SOCRadar API key using Postman as shown pictures below :



- Response Status 200 means API key was successfully pull the data.

3. Python Script for Pull data from SOCRadar API and Send to Splunk HEC (Kode Terlampir)

III. Run The Script

- Execute python script with python 3.13 or higher
- Or make python script execution as a .services
- Perform Query Search on Splunk and save it as Alarm :

```
index="socradar_leak_index" sourcetype="socradar_api" earliest=-5m
```

- Now python script will pull data from SOCRadar API every 5 minutes and if there's new data it would be send to Splunk HEC and trigger the Alert on Splunk Dashboard.