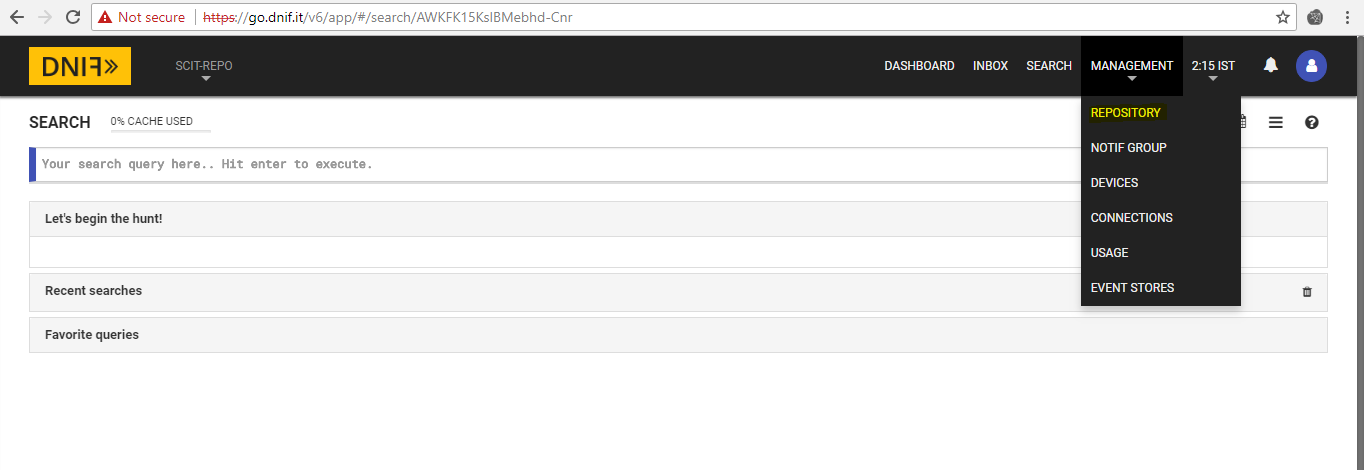
**Creating Alerts with DNIF**

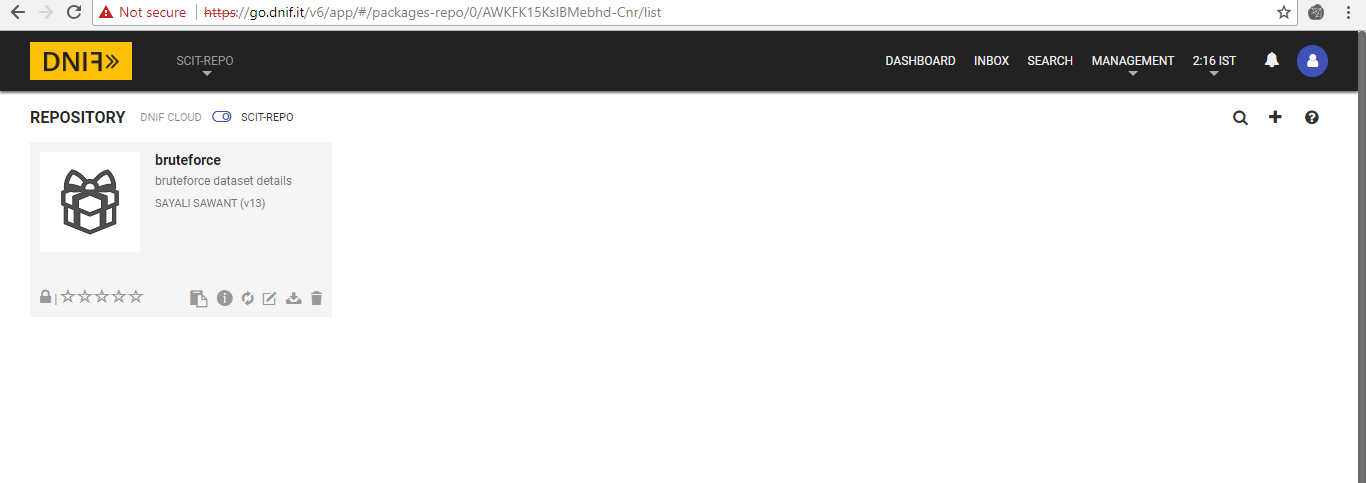
Dnif provides feature to create alerts which enable users to trigger reports if the specified conditions in the query are met.

In order to create reports, follow the steps mentioned below:

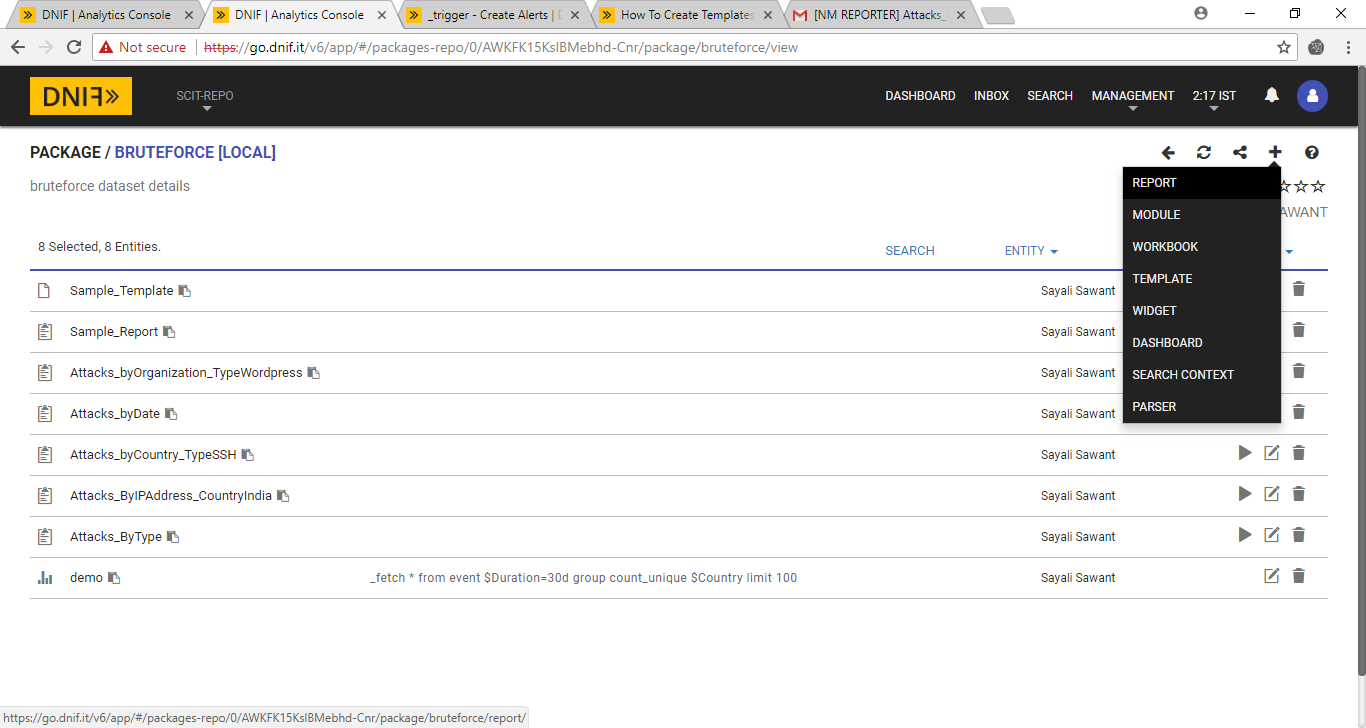
Under “Management” Tab, click on Repository option



Create a new repository in order to create and visualize reports within the created repository.



In order to add a new Report , Click on “+” icon within the repository , and click on “Report” option from the given menu.



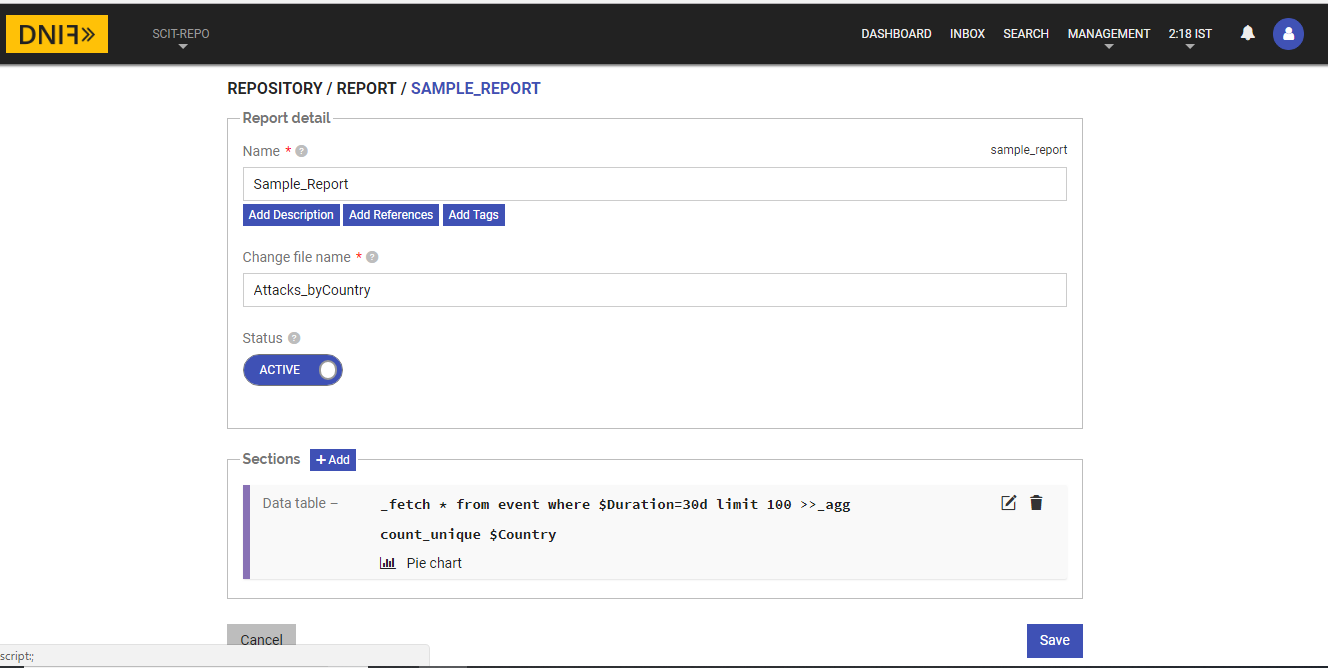
Enter the mandatory fields :

Name of the Report

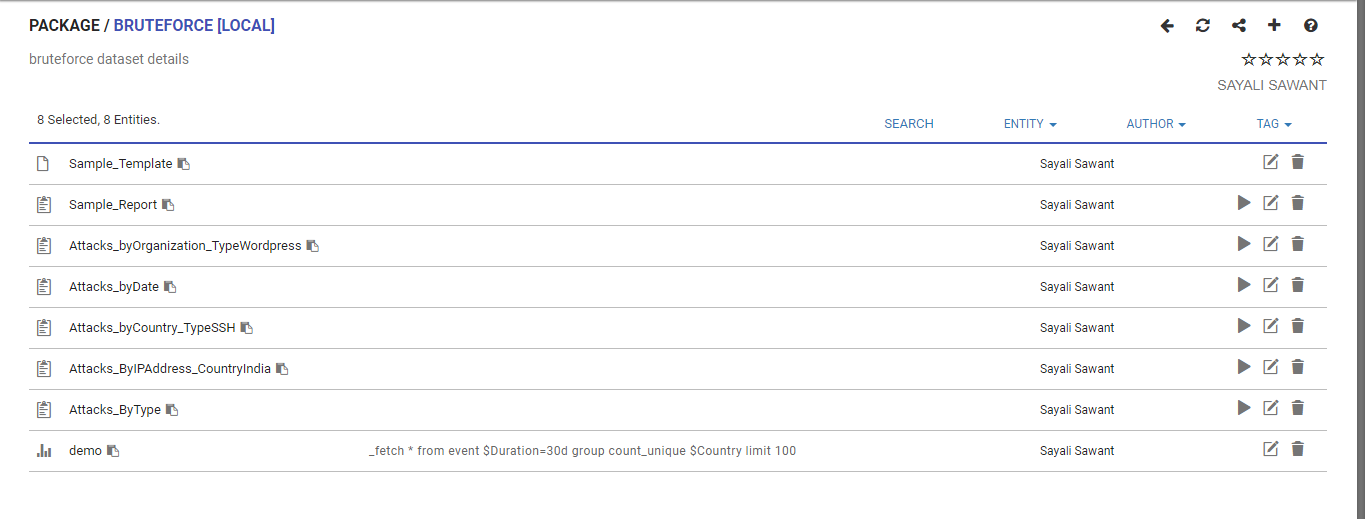
Add Data Table using DQL queries as shown below in order to retrieve the required results in the Report. Here report is generated to count the unique number of attacks occurred based on Country field within the last one month.

Query : \_fetch \* from event where $Duration=30d limit 100

count\_unique $Country



Click on “Save” button, created Report will be visible as shown below under the repository

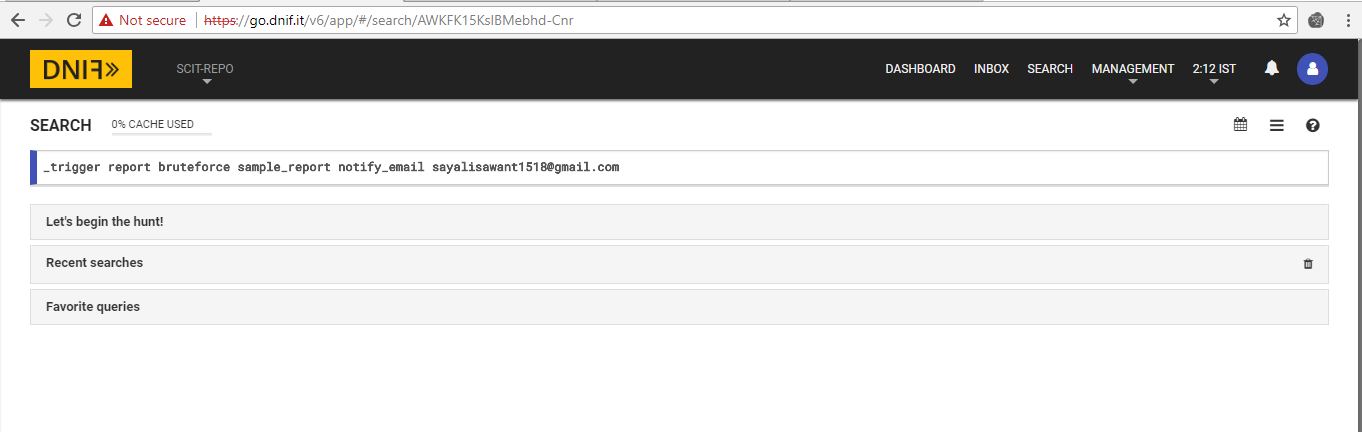


In order to trigger email alerts for the created report use the following query:

\_trigger report bruteforce sample\_report notify\_email [sayalisawant1518@gmail.com](mailto:sayalisawant1518@gmail.com)

Where,

* **bruteforce** is a slug name of the package which contains the required report template.
* **Sample\_report** is a slug name of report template.
* **notify\_email** is a parameter to send an email.
* **sayalisawant1518@gmail.com.com** is the target email address to whom the report needs to be sent.



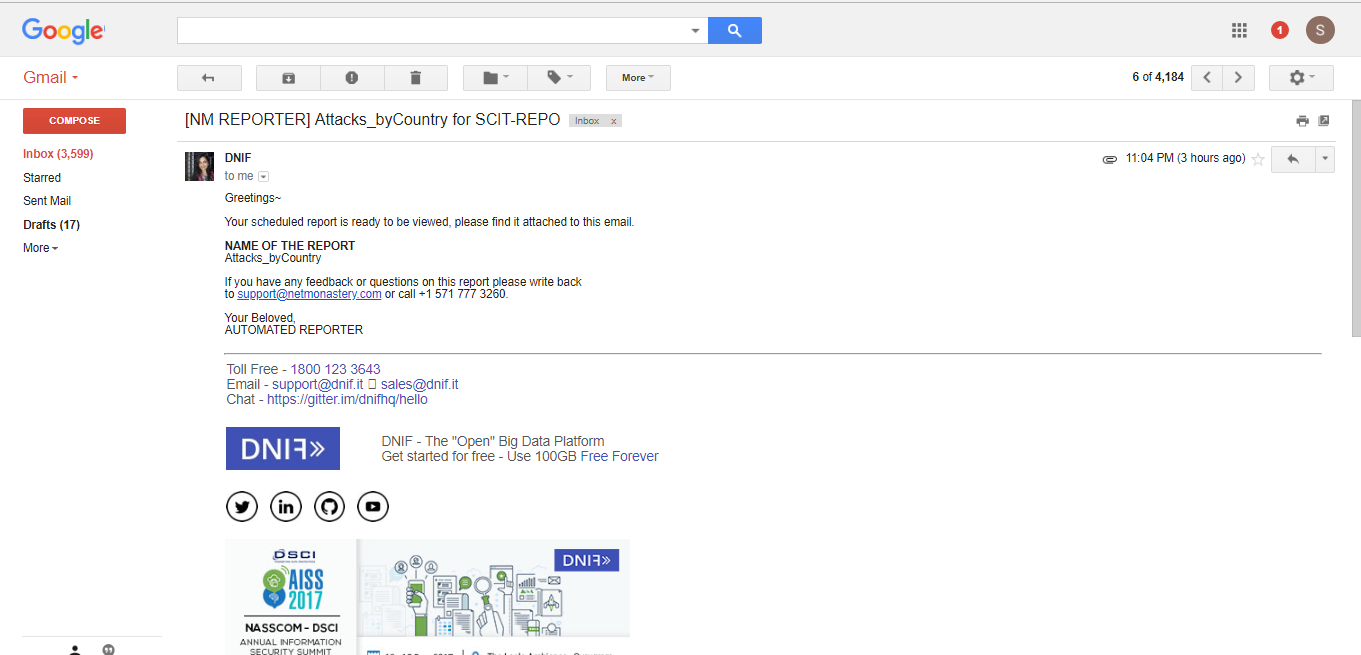
Similarly , alerts can be generated as demonstrated below for different conditions using queries and notify the user via email for the same.

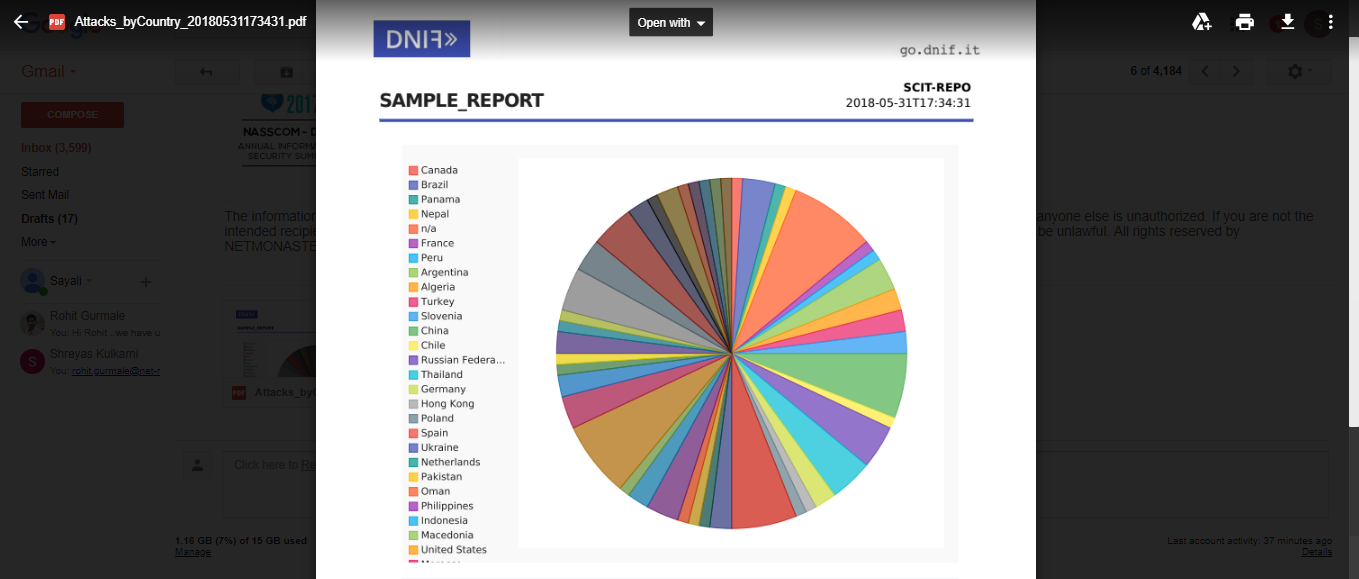
1.

Email Trigger: Generating email as shown below to record the list of attacks occurred country-wise in the past one month.

\_fetch \* from event where $Duration=30d limit 100

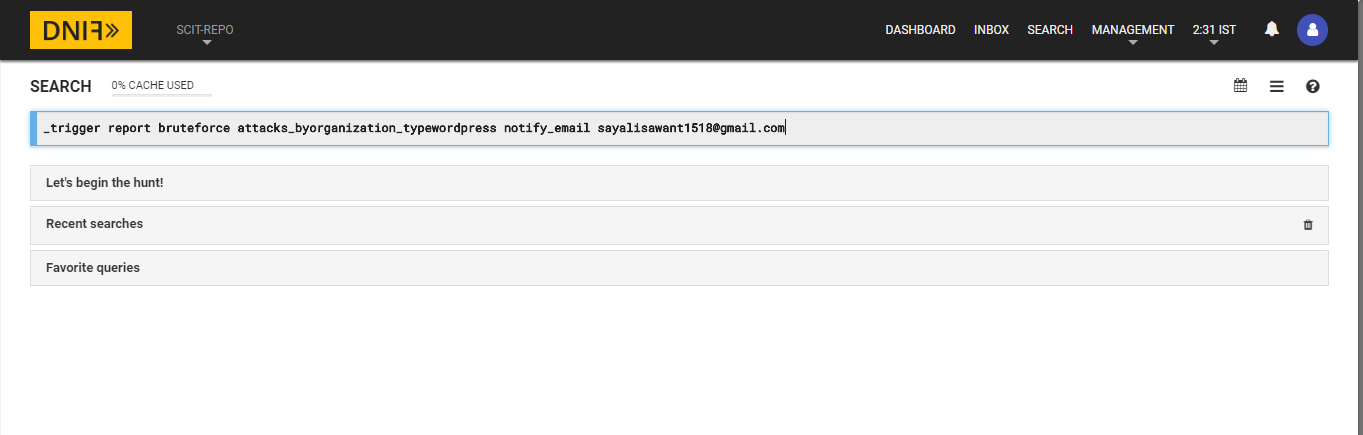
count\_unique $Country



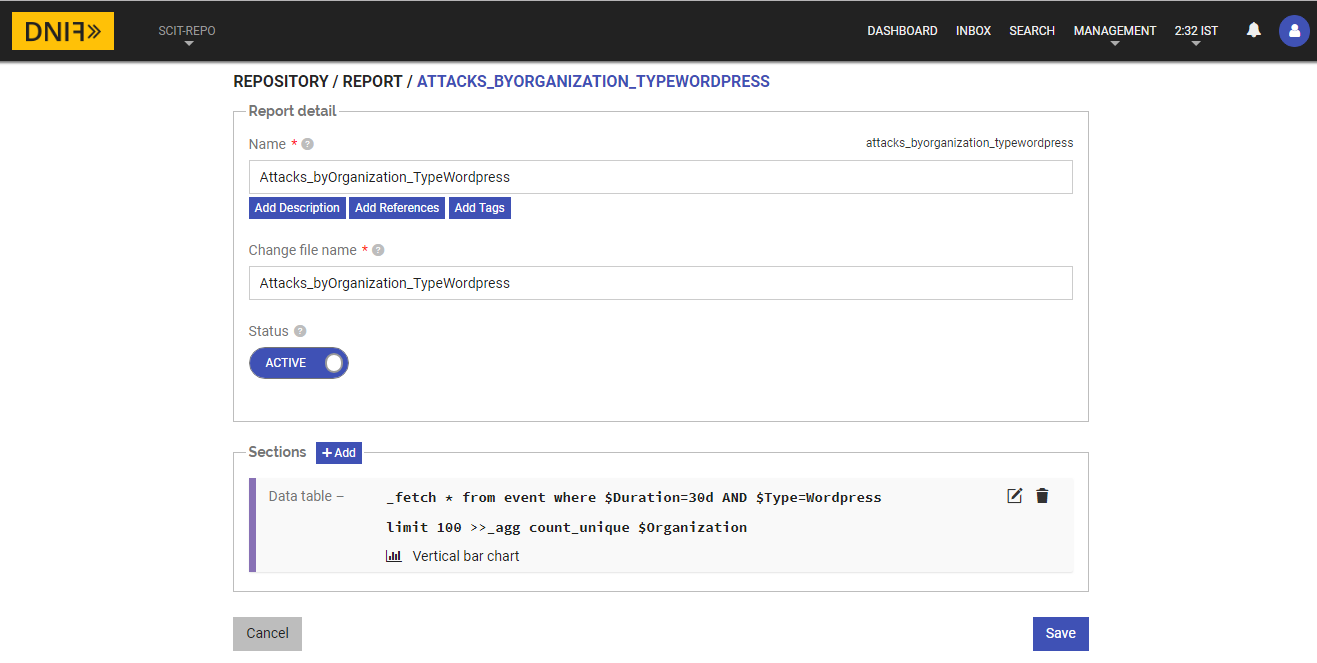


2. To trigger an email based on the organization based on the type of attack being Wordpress.

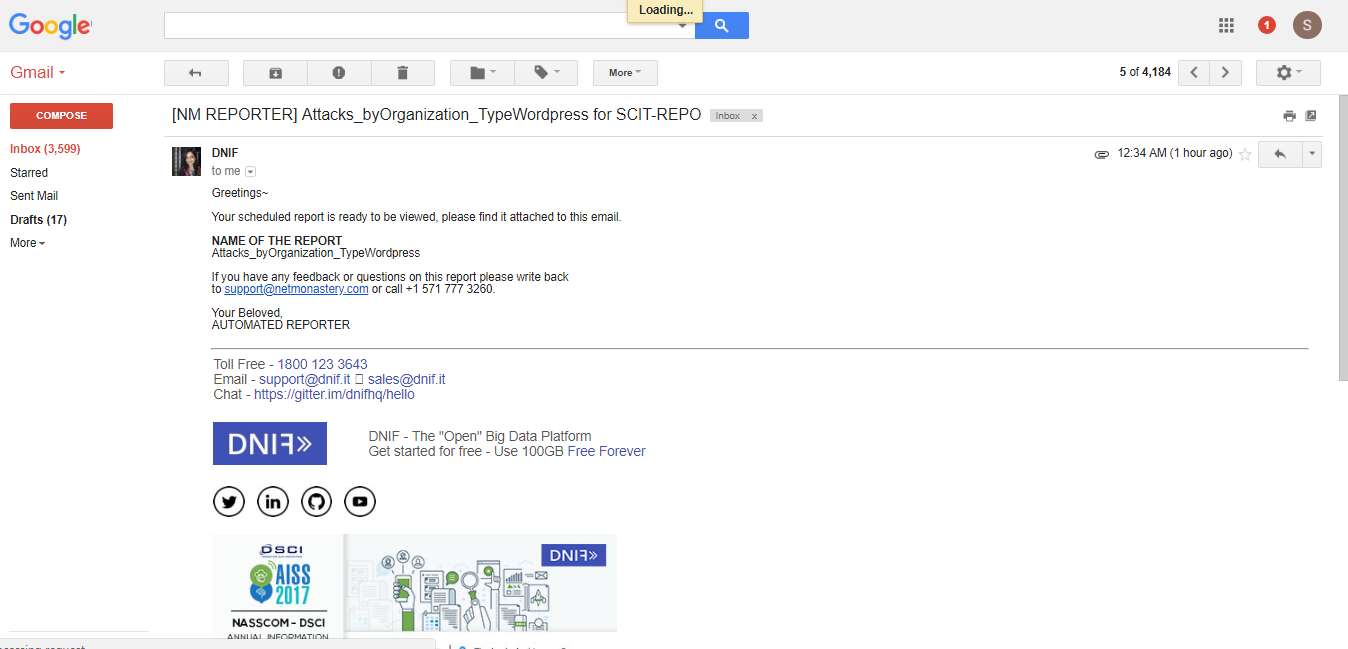
Query : \_trigger report bruteforce attacks\_byorganization\_typewordpress notify\_email sayalisawant1518@gmail.com

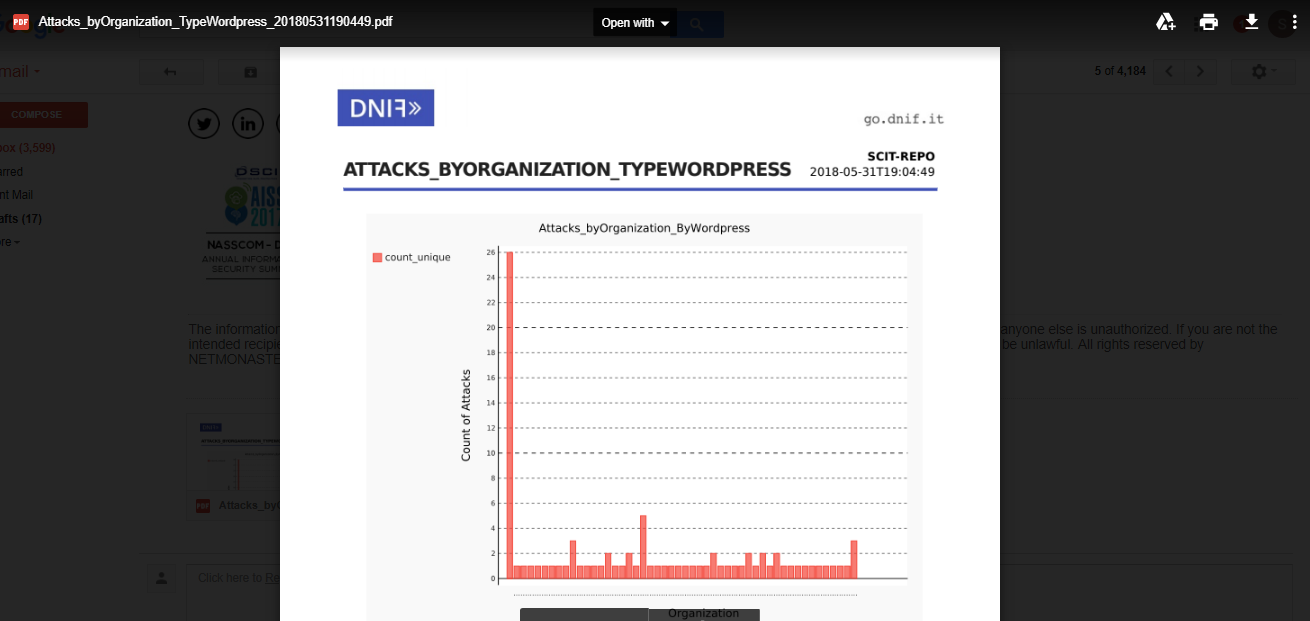


Report:



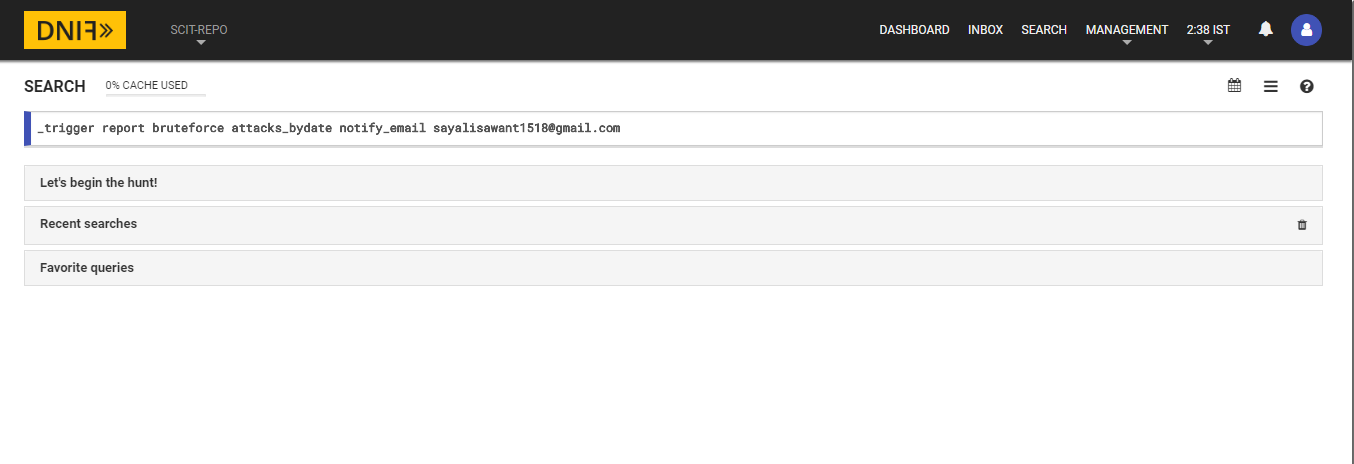
Email:



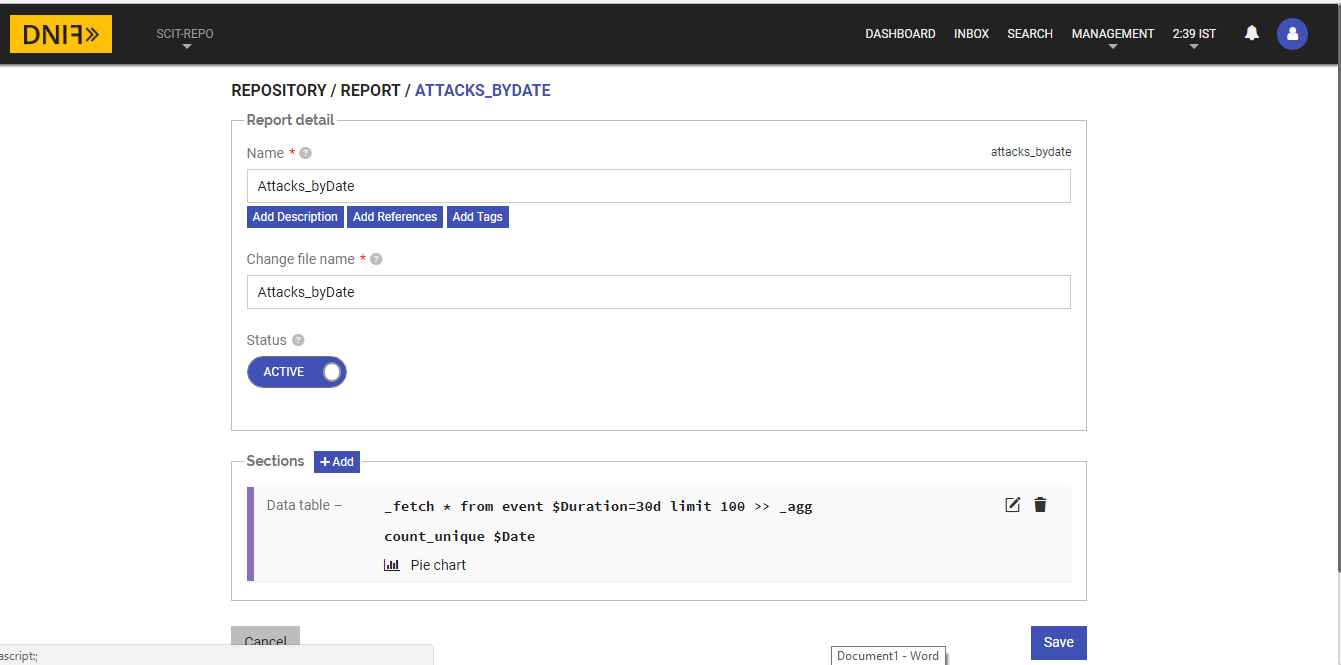


3. To trigger an alert based on the date of the originating attack.

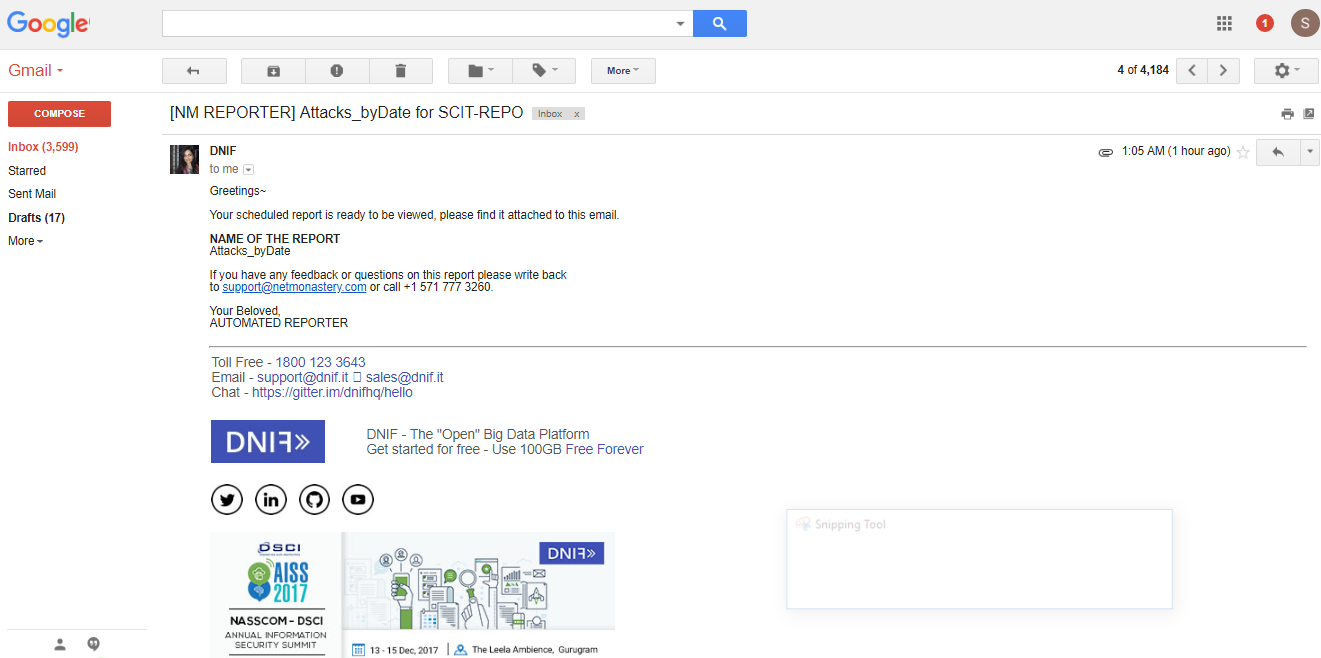
\_trigger report bruteforce attacks\_bydate notify\_email sayalisawant1518@gmail.com

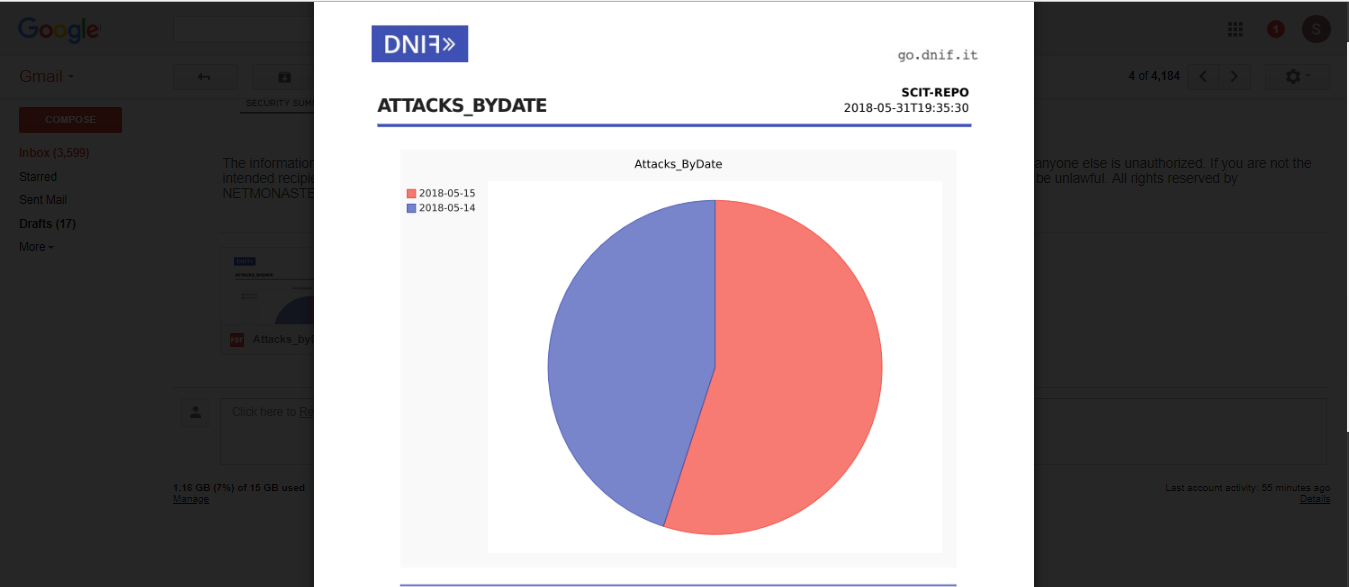


Report



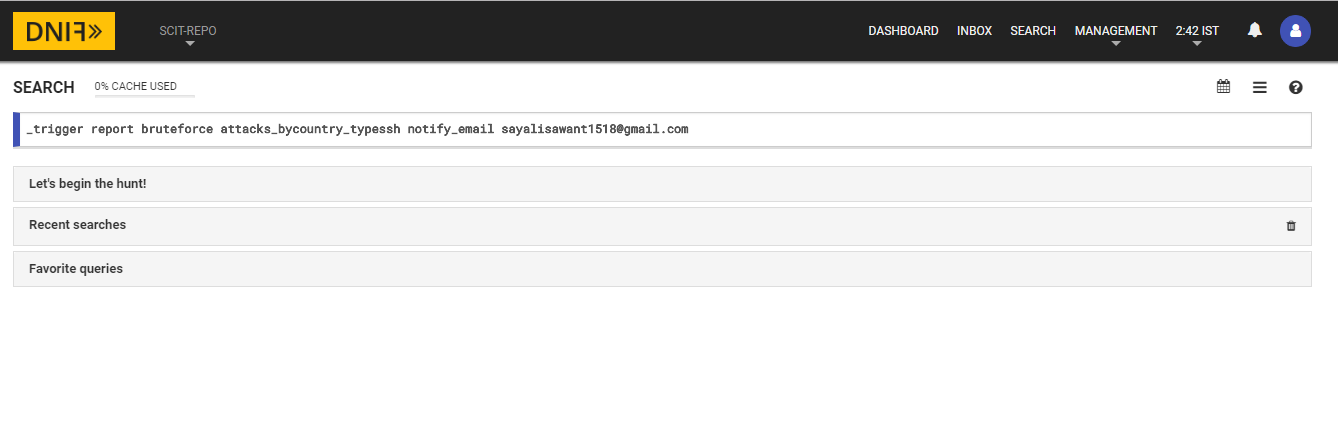
Email:



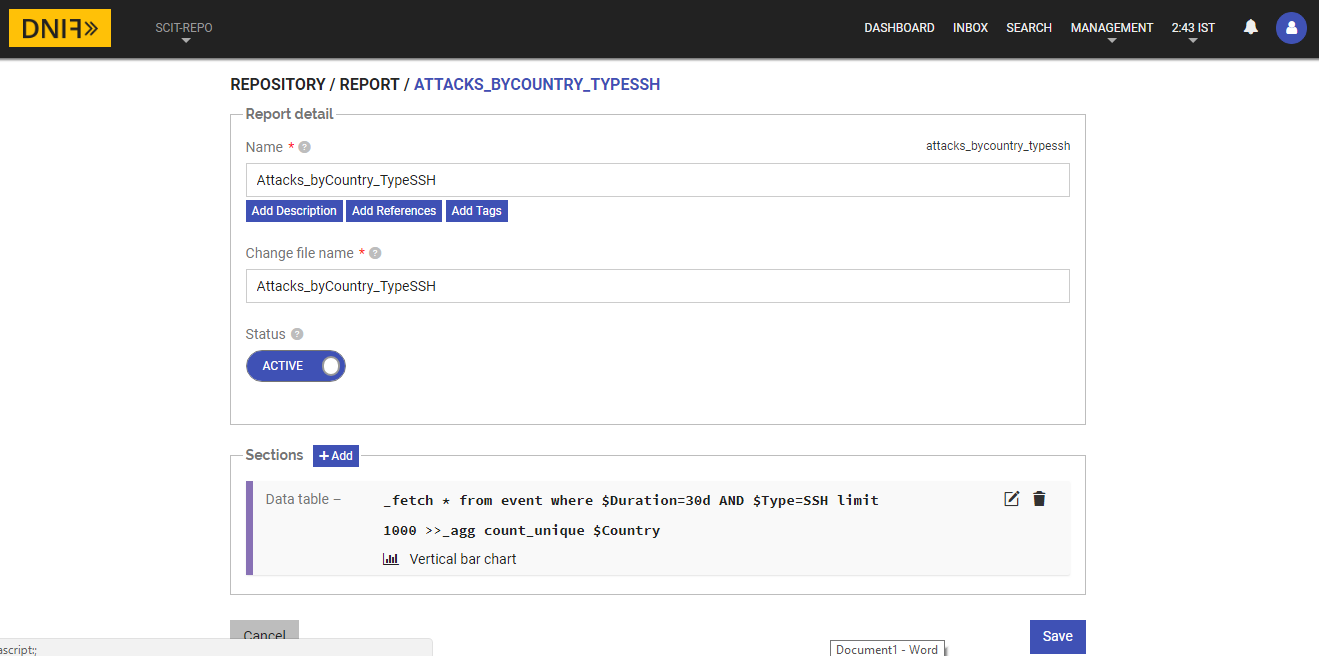


4. Query: To trigger an alert for the user based on Type of the attack originating countrywise.

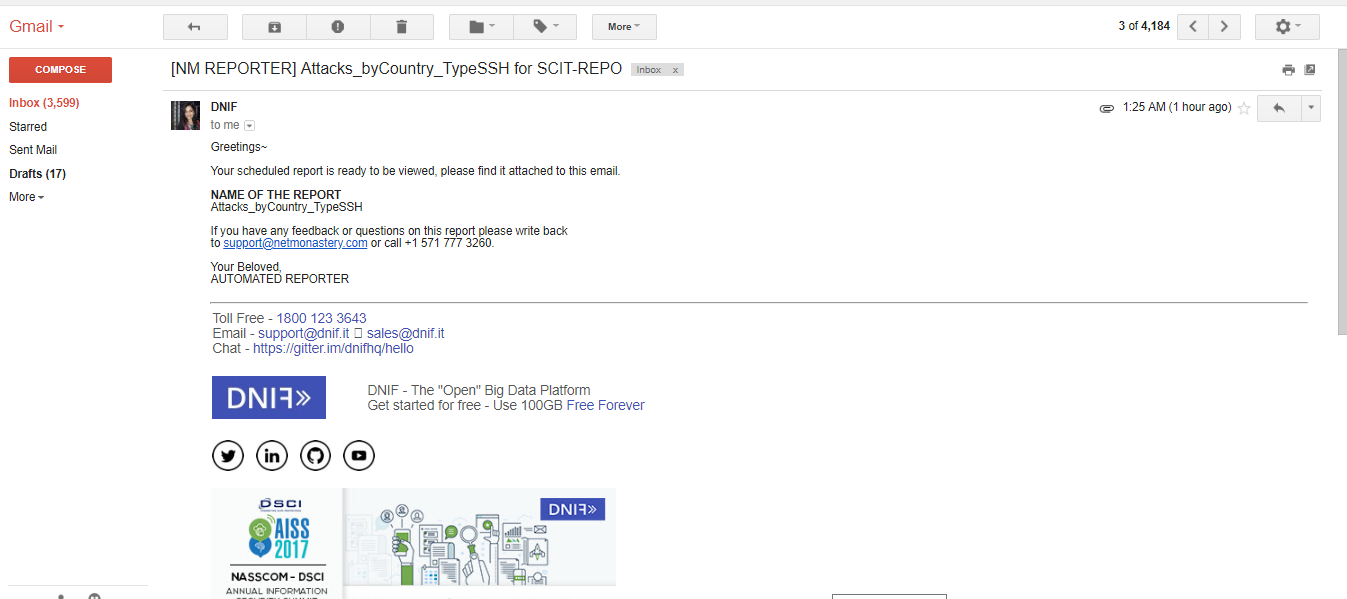
\_trigger report bruteforce attacks\_bycountry\_typessh notify\_email sayalisawant1518@gmail.com

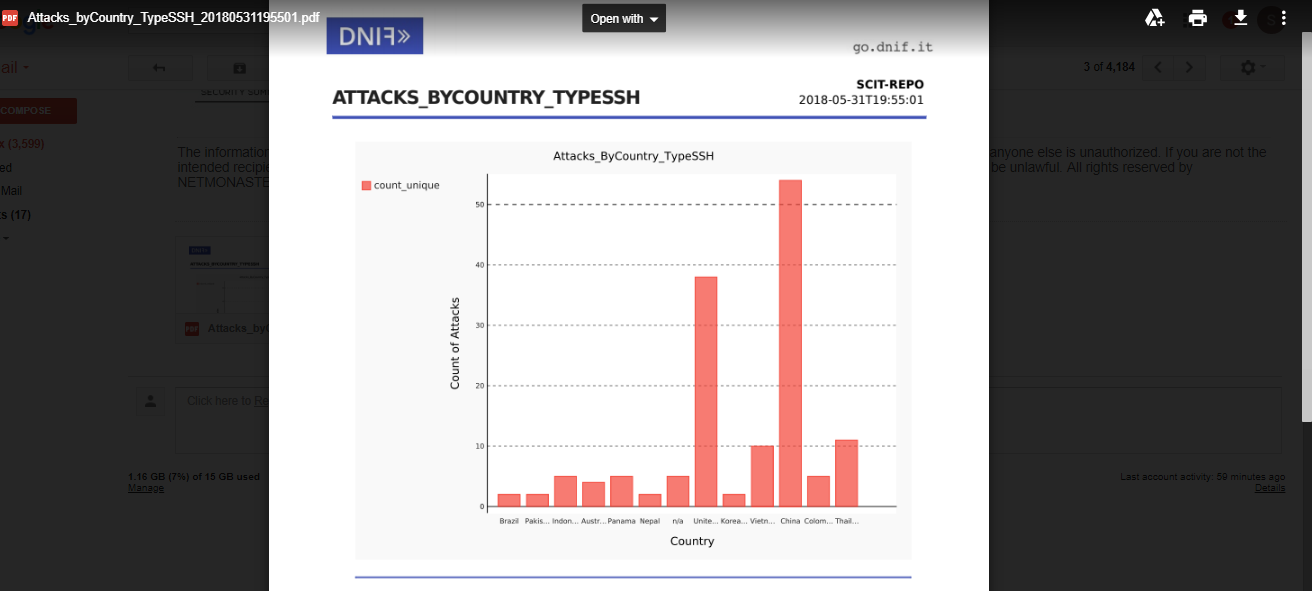


Report:



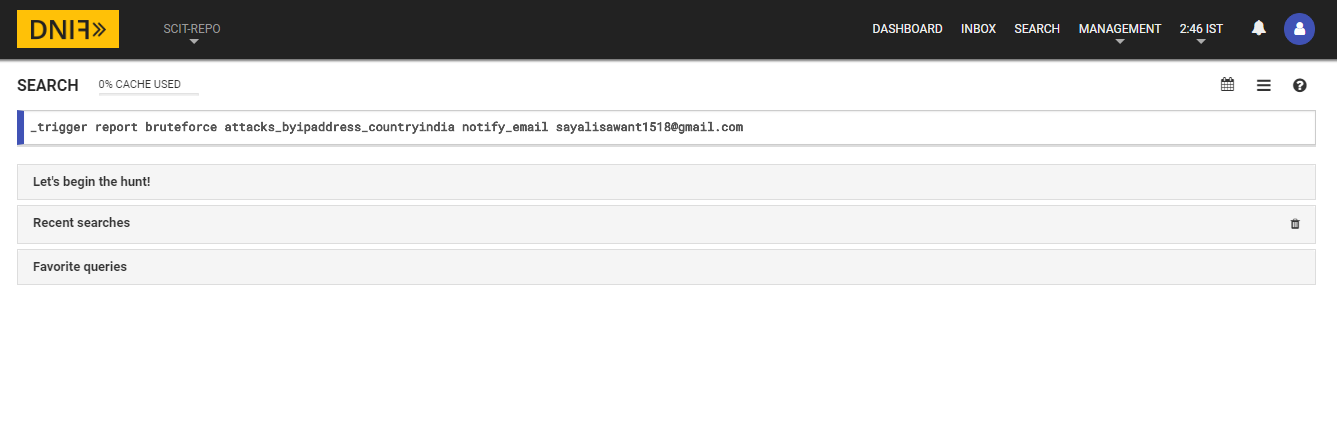
Email:



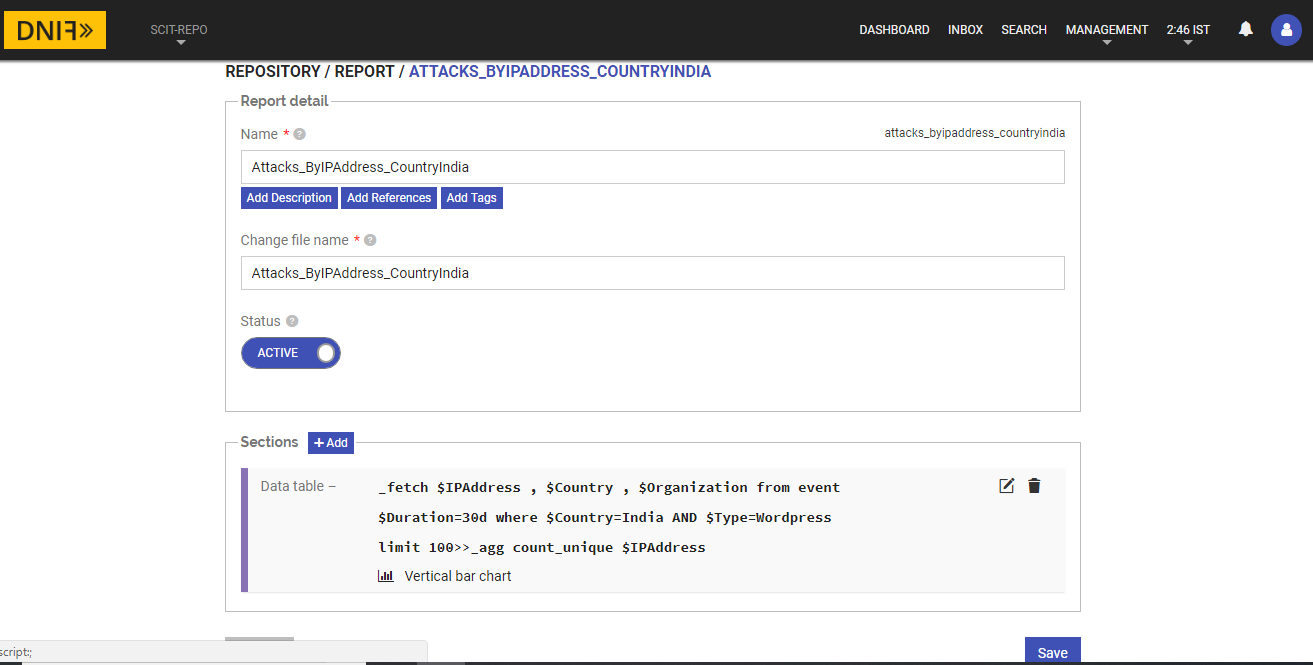


5. To trigger an alert based on attacks occurring in India and report the count of IP Addresses for originating attacks in the last 30 days.

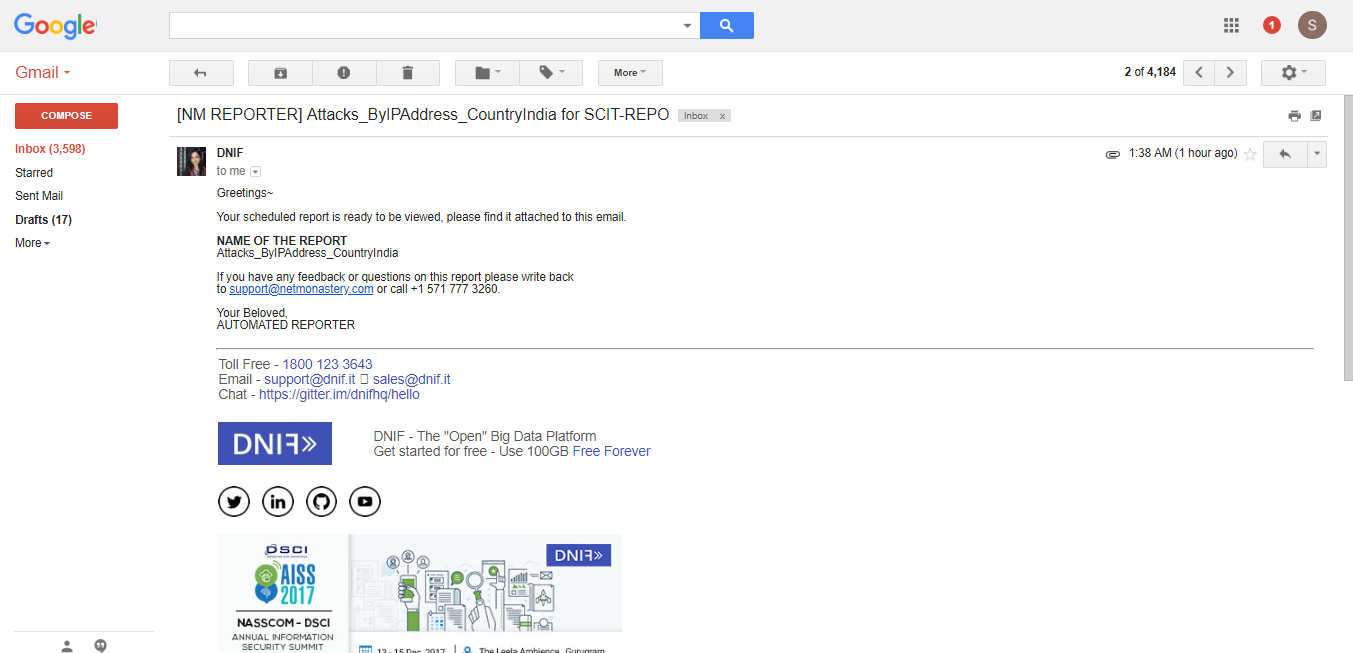
Query: \_trigger report bruteforce attacks\_byipaddress\_countryindia notify\_email sayalisawant1518@gmail.com

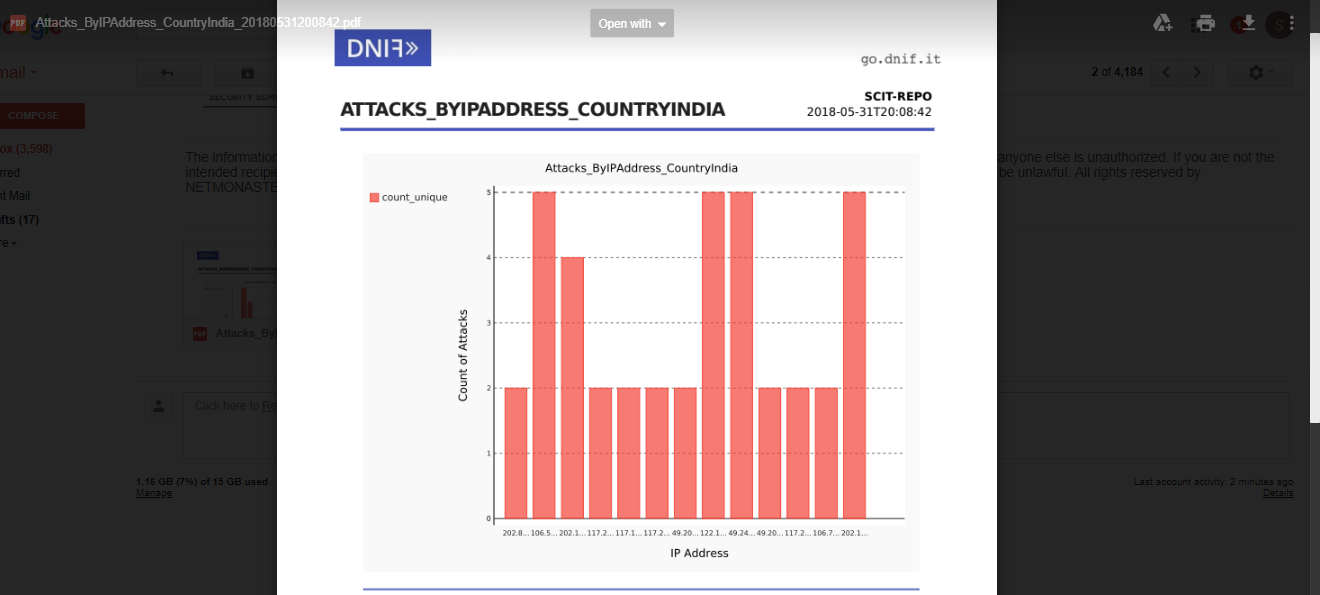


Report:



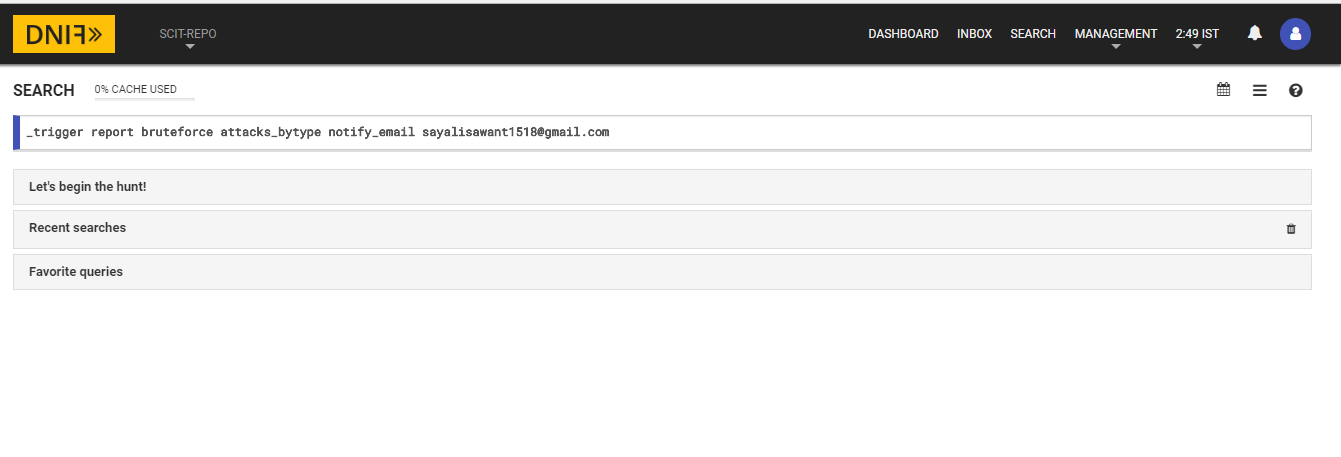
Email:



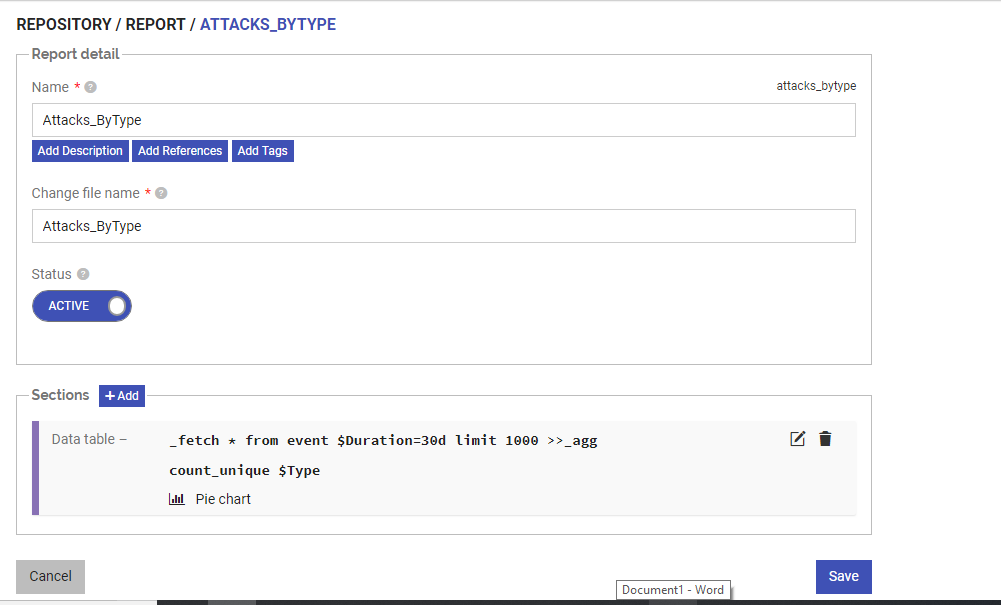


6. To trigger an alert based on Type of attack in the last 30 days.

Query : \_trigger report bruteforce attacks\_bytype notify\_email sayalisawant1518@gmail.com



Report:



Email:

