ANNEX A

ENISA F-COD-20-T28 (Lot 3)

“Lot 3: Delivery of subscription services for tasks related to the Operational Cooperation of ENISA”

Business requirements for the purchase of Twitter Enterprise API subscription

Name: ENISA

Email: COD3@enisa.europa.eu

Legal Entity Name: European Union Agency for Cybersecurity

Organization's Website URL: www.enisa.europa.eu

Organization's Primary Location: Athens, Greece

Billing Address: Vasilisis Sofias 1, Marousi, Athens, 15124

Organization's Twitter Handle: @enisa_eu

Company description, including industries served and customer locations: ENISA is a European Union Agency. It is a public body serving the EU Institutions, Bodies and Agencies and the European Union Member States.

Please provide a thorough description in the form of a paragraph for each of the following:

- What is the purpose of your product or service?

OpenCSAM is a tool that provides trusted and up to date information to experts/analysts in cybersecurity. The information is indexed from multiple sources (Twitter being only one of them) and then processed to offer the most relevant available information to cybersecurity analysts, updated as close to real time as possible.

- What will you deliver to your users/customers?

The application delivers mostly search results which includes: documents, tweets, news articles. The users can see the indexed results as well as links to the original content. If the tweets contain links, we sometimes index those links as well and present their content the same way (see screenshots). We also envisage to offer our users an early warning capability (real time or near real time) for situational awareness on new cyber incidents, a historical evolution of published information regarding cybersecurity incidents, improve the analysis on “trending terms” and extend the knowledge graph with new terms related to cybersecurity.

- How do you intend to analyze Tweets, Twitter users, or their content?

We intend to index tweets based on hashtags or trusted Twitter users in order to discover new security threats and alert our users about them. Also we intend to discover new “trusted Twitter users” based on their activity and quality of their content.

Also we intend to use the Twitter hashtags to expand the knowledge graph that we use to model the cybersecurity domain. This we do through a combination of manual knowledge engineering and automated discovery of relevant hashtags through PageRank type algorithms.

Finally, we intend that in a future version of the platform to be able to track the appearance of a security threat based on the Twitter history of its mentions in order to better understand both the discovery but also of ways to optimize the notification process.

- How is Twitter data displayed to users of your product or service (e.g. will Tweets and content be displayed at row level or aggregated)?

The tweets are usually displayed at row level, distinct, as search results provided by a search engine. The tweets are enriched with tags added in our preprocessing phase. The tags are displayed below the tweet.

Do you (or do you plan to) make available an API that redistributes Twitter content to your customers, either as part of your product or as a complement? If so, please provide us with a sample payload.

We don’t plan to do this as of now**.**

Will your product, service, or analysis make Twitter content or derived information available to a government entity (or entity who serves government entities)?

If yes, please provide the following:

- A list of which government or public sector entities will have access to Twitter content, or information derived from Twitter content, under this use case. Please provide each entity's full name, along with the country's name they belong to.
- A description of which portion(s) of your overall use cases are applicable to each entity; or if they differ from the overall use case, a description of the specific use cases for these entities

ENISA is offering the OpenCSAM service to cybersecurity stakeholders from the European Commission as well as to public cybersecurity authorities across the 27 Member States.

Is your service currently accessing Standard or Premium API?

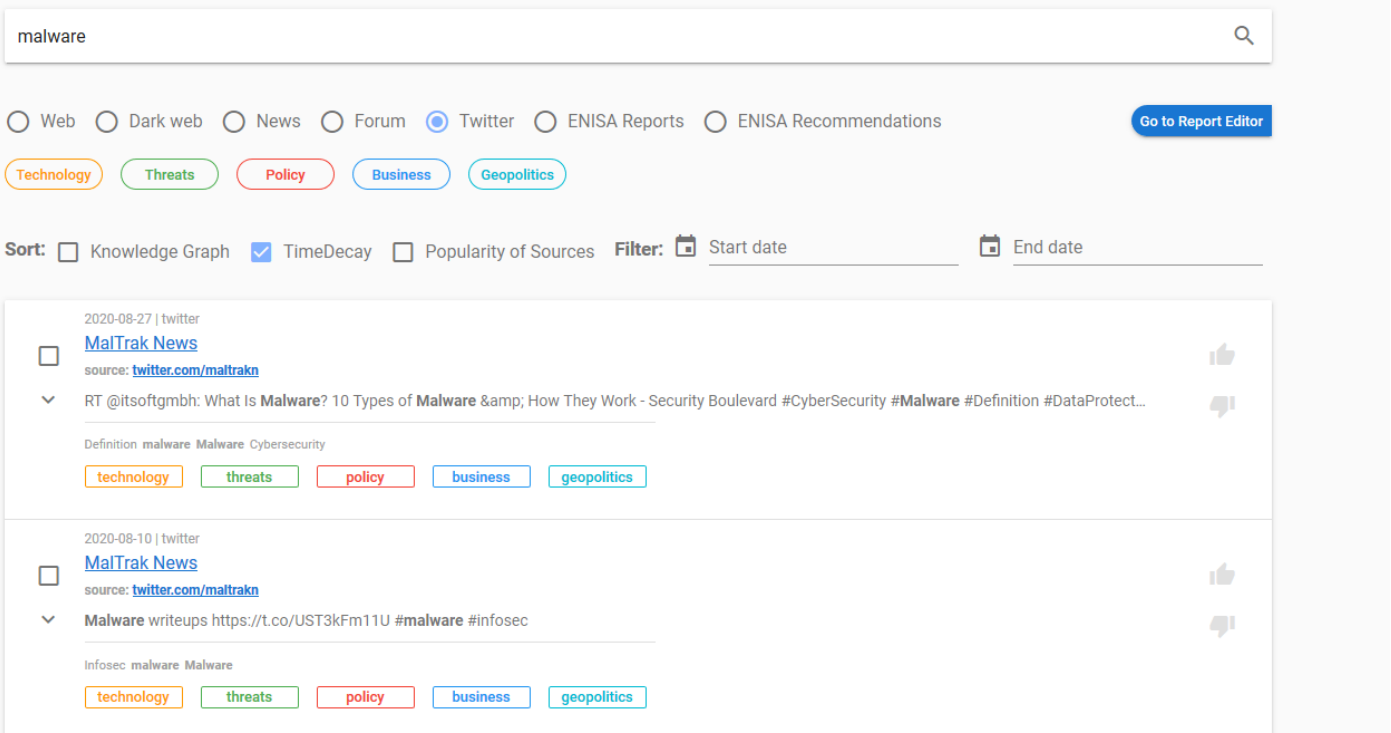
If yes, provide us with a list of your app IDs and/or a list of your developer accounts and the use cases for your apps in a few words.

We are currently using the Standard API for the development of OpenCSAM. Our ID is ENISA_COD3

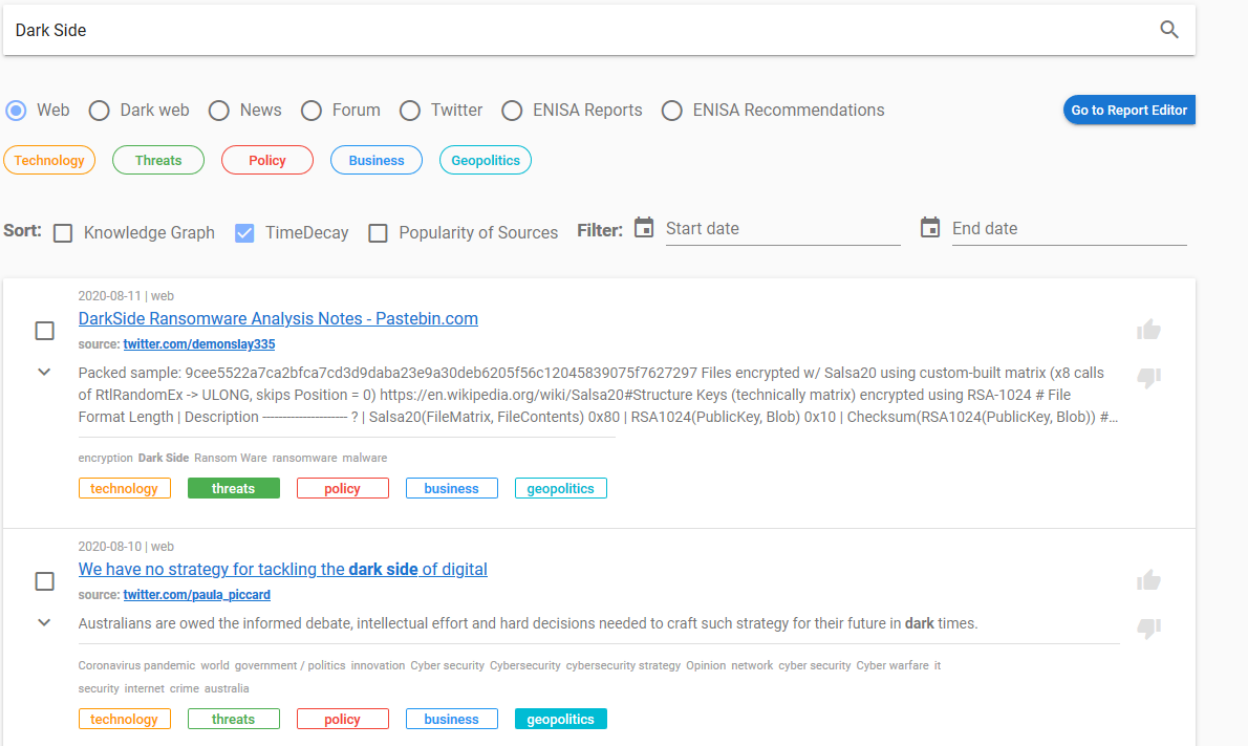
- Please include any relevant screenshots of your product or services.

The current version of OpenCSAM uses the standard access for use cases similar with the ones described above:

- Search results in tweets of monitored users. The results are presented to users and they might use the information in different types of reports



- Use of links discovered from tweets to enhance the document repository and as an alternative form of news



- Trending terms analysis within our monitored trusted users' posts

Twitter

Start date 2020-08-25

End date 2020-09-01

- Identifying possible trusted users that we might want to monitor

ADD NEW ITEM

Search

1 2 3 ... 445 446 447

Link	Type	Status	Added by	Popularity
https://twitter.com/evrentombul	twitter	pending	-	0.50
https://twitter.com/arrow_dot_com	twitter	pending	-	0.54