Supply Chain Risk Related Classification Challenge Series - (01/03): NLP-based Threat Detection

Code Machine Learning Data Science Linux Recommended Challenges Recommended THRIVE Articles

Key Information

1st	2nd	3rd	4th	5th
$2,000	$1,000	$500	$300	$200

Unregister

Submit

Next Deadline: Review | 3d 7h until current deadline ends

Show Deadlines

DETAILS REGISTRANTS (130) SUBMISSIONS (24) CHALLENGE FORUM

Challenge Overview

Challenge Objective

The supply chain risk management department receives many incident feeds from different sources in the form of emails and news subscriptions for reporting potential risks. However, the majority of them are in fact false alarms.

In this challenge, we need to classify the received incident feeds as a real threat/relevant or not/ irrelevant from tons of emails based on (1) vendor-provided categories (e.g.,category), (2) vendor-provided severity, (3) supply chain related node/location proximity distance, & type of node, (4) geocode & geography details of the nodes and (5) titles and description. In addition, email contains other information also, That also can be used for the classification.

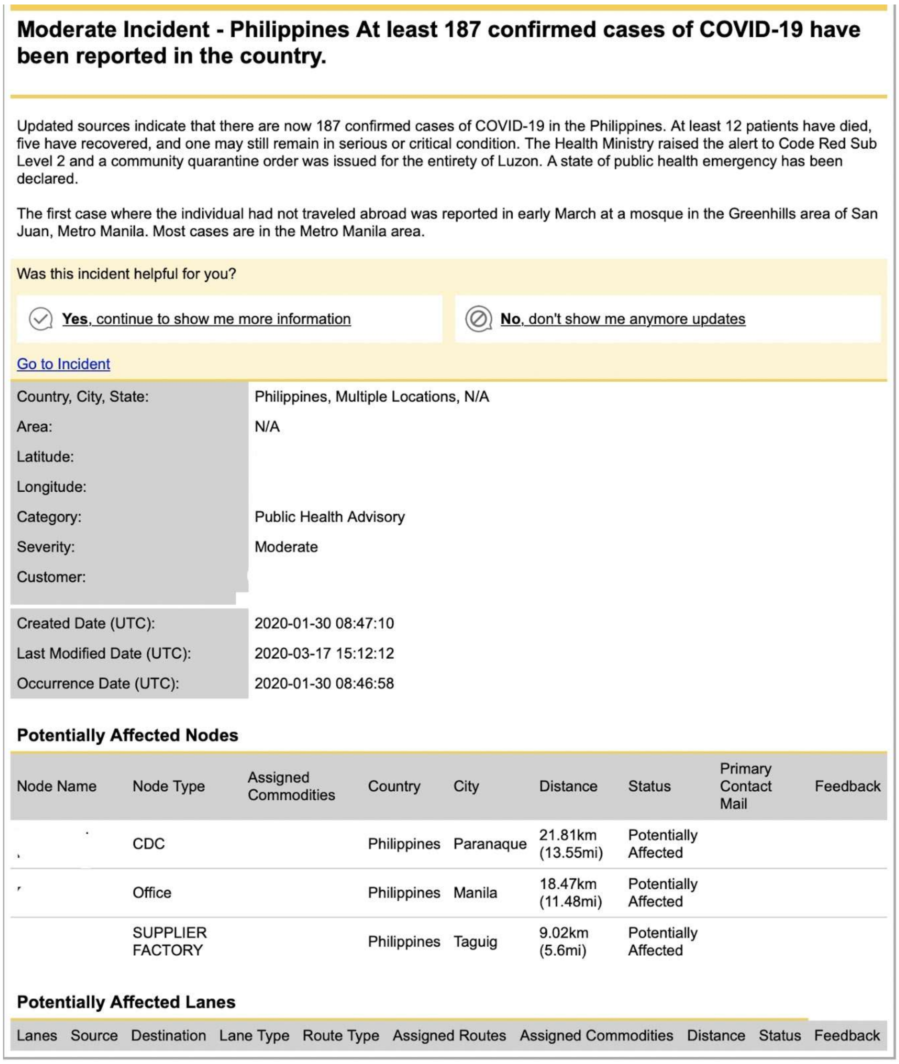
We expect your models must leverage (1) keyword-based rules & mapping rules(heuristic) and/or (2) text analytic models using NLP techniques 3. Continuous learning capabilities. Your models should be able to incorporate feedback from users for continuous learning purposes.. In this challenge, your model is only learned from the historical data. However, when it comes to online, models should be able to learn continuously based on the user-provided feedback on its prediction.. For example, the user may provide real threat/relevant or not / irrelevant feedback on all of the predictions; the user may also provide the mode some new keywords/rules.

Background

An electronic cellular device manufacturing company's supply chain risk management department subscribed to receive incident feeds from different vendors in the form of emails and news subscriptions to proactively monitor for their potential supply chain impacting risks.

The subscribed incident feeds are limited to the preconfigured radius from configured/interested locations only. These locations can be of various types like port, airport, supplier location, R&D etc., The radius can vary based on the location types or risk category type and it can be constant in other cases as well.

The received incident feed (email) would consist of the following contents to describe the threat.



Moderate Incident - Philippines At least 187 confirmed cases of COVID-19 have been reported in the country.

Updated sources indicate that there are now 187 confirmed cases of COVID-19 in the Philippines. At least 12 patients have died, five have recovered, and one may still remain in serious or critical condition. The Health Ministry raised the alert to Code Red Sub Level 2 and a community quarantine order was issued for the entirety of Luzon. A state of public health emergency has been declared.

The first case where the individual had not traveled abroad was reported in early March at a mosque in the Greenhills area of San Juan, Metro Manila. Most cases are in the Metro Manila area.

Was this incident helpful for you?

✓ **Yes**, continue to show me more information

⊘ **No**, don't show me anymore updates

Go to Incident

Country, City, State:	Philippines, Multiple Locations, N/A
Area:	N/A
Latitude:	
Longitude:	
Category:	Public Health Advisory
Severity:	Moderate
Customer:	
Created Date (UTC):	2020-01-30 08:47:10
Last Modified Date (UTC):	2020-03-17 15:12:12
Occurrence Date (UTC):	2020-01-30 08:46:58

Potentially Affected Nodes

Node Name	Node Type	Assigned Commodities	Country	City	Distance	Status	Primary Contact Mail	Feedback
	CDC		Philippines	Paranaque	21.81km (13.55mi)	Potentially Affected		
	Office		Philippines	Manila	18.47km (11.48mi)	Potentially Affected		
	SUPPLIER FACTORY		Philippines	Taguig	9.02km (5.6mi)	Potentially Affected		

Potentially Affected Lanes

Lanes	Source	Destination	Lane Type	Route Type	Assigned Routes	Assigned Commodities	Distance	Status	Feedback

Dataset:

The emails are extracted into the csv format and given in the challenge.

The extracted emails are available in the following files

1. Master.csv
2. Nodes.csv
3. Lanes.csv

The **Master.csv** file consists of the required key incident details and its affected node details are kept in **Nodes.csv**, its lane details are kept in the **Lanes.csv** files. All the three files are linked with the “id” column in those files.

Training_Jan_mar_2019_Master.csv: This file contains training data. The first row is the header. The first column, i.e., “Alert ID”, presents you the groundtruth label. When it is not empty in a row, this email should be treated as a real threat.

Training_Apr_jul_2019_Master.csv: Similar to the 1st quarter's csv; For the training purpose.

Testing_Aug_dec_2019_Master.csv: This file contains testing data. It is similar to the training csv files, except for

- The first column **"Alert ID"** is always empty. You are asked to fill in a binary value (i.e., an integer value 0 or 1) to each row denoting whether your model detects this email as a real threat. Here, 1 means it is a real threat.
- The second column **"Threat Level"** is always empty too. You are asked to fill in a confidence score (i.e., a floating number between 0 and 1) to each row, denoting how likely this email is a real threat. The higher, the more likely a real threat.

An email consists of threat details for a location along with its occurrence date, geocode of the location, city, country etc., In addition, the email would consist of probability affected node list and its lane details as well.

DHL Risk solution - Configuration Information.xlsx: Presents you some explanation and sample rules for some types of threats.

All datasets can be downloaded https://www.dropbox.com/s/hnaiautc18dw87c/To%20Community.zip?dl=1.

Evaluation Metric

We are going to mainly evaluate your method based on the F1 score. We would like to see a model achieving a great balance between precision and recall. And please keep in mind that "about 98% of emails are not real threats".

Precision = **TP** / (**TP** + **FP**)

Recall = **TP** / (**TP** + **FN**)

F1 = 2 * **Precision** * **Recall** / (**Precision** + **Recall**)

If you are not familiar with F1, please check out https://en.wikipedia.org/wiki/F1_score.

We will evaluate the F1 scores based on your binary predictions and your confidence scores.

Given your binary predictions, we will compute your F1 score directly. Given your confidence scores, we will try to tune the threshold and see what's the best F1 score we can achieve.

Your final score will be (80% * Your F1 Score + 20% * Your Best F1 Score)

As the provided data set has enough data to identify the non relevant feed, the Accuracy expected should be minimum around 75%.

Final Submission Guidelines

Submission Format

You submission must include the following items

- The filled test data. We will evaluate the results quantitatively.
- **Working Python code** which works on the different sets of training/testing data in the same format. **No dataset-specific hardcoding** in the code is allowed. We will run the code on some different csv files of the same format (i.e., the header).
- All models in one code with clear inline comments.
- A report about your model, including data analysis, model details, and local cross validation results.
- A deployment instructions about how to install required libs and how to run.

Judging Criteria

Your solution will be evaluated in a hybrid of quantitative and qualitative way.

- Effectiveness (80%)
  - We will evaluate your prediction by comparing it to the ground truth data. Please check the "Evaluation Metric" section for details. The bigger final score, the better.
  - The capability of continuous learning based on user-provided feedback is important.
- Clarity (10%)
  - The model is clearly described, with reasonable justifications about the choice.
- Reproducibility (10%)
  - The results must be reproducible. We understand that there might be some randomness for ML models, but please try your best to keep the results the same or at least similar across different runs.

Hint /reference for the development:

1. **Transfer learning in NLP**
   1. https://becominghuman.ai/transfer-learning-in-nlp-using-fastai-a21ab5929759
   2. https://towardsdatascience.com/machine-learning-text-classification-language-modelling-using-fast-ai-b1b334f2872d
   3. https://towardsdatascience.com/transfer-learning-in-nlp-for-tweet-stance-classification-8ab014da8dde
   4. https://nlp.fast.ai/
   5. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/09/DLforNLP_Xiaodong_He.v5.partA_.pdf
2. Email Text Classification
   1. http://www.diva-portal.org/smash/get/diva2:1189491/FULLTEXT01.pdf

    2. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8864974

3. Word cloud

    1. https://www.datacamp.com/community/tutorials/wordcloud-python

Payments

Topcoder will compensate members in accordance with our standard payment policies, unless otherwise specified in this challenge. For information on payment policies, setting up your profile to receive payments, and general payment questions, please refer to https://www.topcoder.com/thrive/articles/Payment%20Policies%20and%20Instructions

Reliability Rating and Bonus

For challenges that have a reliability bonus, the bonus depends on the reliability rating at the moment of registration for that project. A participant with no previous projects is considered to have no reliability rating, and therefore gets no bonus. Reliability bonus does not apply to Digital Run winnings. Since reliability rating is based on the past 15 projects, it can only have 15 discrete values.
Read more.

REVIEW STYLE:

Final Review:
Community Review Board ?

Approval:
User Sign-Off ?

CHALLENGE LINKS:

Review Scorecard ?

CHALLENGE TERMS:

Standard Terms for Topcoder Competitions v2.2
Competition Non-Disclosure Agreement

SHARE: