# Introduction

To reduce risks for an organization or its customers, one needs to ensure that vulnerabilities are identified, analyzed, and resolved quickly. The identification is easy due to reporting & nature of the vulnerabilities, however, analyzing and resolution are the two main time-consuming tasks. The security engineer have to use his expertise and during this process, he will be rely on various security repositories for analyzing similar attacks in order to develop a resolution. One of the rich and publicly available attack repositories is Common Attack Pattern Enumeration (**CAPEC**) https://capec.mitre.org/. It is a community resource for

identifying and understanding various attacks. It not only contains attack descriptions and attack patterns that adversaries use to exploit but also provides mitigations.

Here, we propose a machine learning NLP technique using the transformers model encoding with TensorFlow framework to search the reported vulnerability-related CAPEC patterns in fraction of a second. The method is not only limited to existing or reported but can also be used for unknown and internal vulnerabilities.

# High level architecture

# Method Flow details:

We used the text similarity NLP technique to trace the related CAPECs from a given CVE. The prediction of the CAPECs is calculated in the following way:

* Create the encoding of all CAPECS by using the sentence transformer model and store it in the local vector store
* Next, CVE is inputted. For example, CVE-2018-18442 is used as the input data
* We connect to the CVE site and scrape the description of it and create the encoding by using the same sentence transformer model
* Iterate through all CAPECS encodings and compare the similarity score between the input CVE encoding to the CAPECs encodings
* Finally, the top 10 CAPECS are sorted by the similarity score

# Resources

Demo: ⁃ [http://ec2-55-187-46-69.us-west-2.compute.amazonaws.com:8082](http://ec2-54-187-46-69.us-west-2.compute.amazonaws.com:8082/)

As an API : [http://ec2-55-187-46-69.us-west-2.compute.amazonaws.com:8082/capecs/CVE-2018-18442/](http://ec2-54-187-46-69.us-west-2.compute.amazonaws.com:8082/capecs/CVE-2018-18442/)