Sujet : Analyse de bibliographie : utilisation pour la CTI

Tuteur : David Brosset (david.brosset@ecole-navale.fr)

Résumé :

Le renseignement sur la menace d'origine cyber (ou Cyber Threat Intelligence) est un domaine important de la cybersécurité qui vise à connaître les acteurs et les vecteurs d'attaque pour dimensionner les mécanismes de défense. Au niveau étatique, il est intéressant de connaître le niveau de compétence des autres nations. Les publications scientifiques sont une des sources pouvant être utilisées pour quantifier/qualifier ou plutôt faire émerger des tendances du niveau scientifique des pays par domaine.

Il s'agit d'OSINT (Open Source Intelligence) puisqu'il s'agit de recherche publique. Néanmoins, les publications reflètent nécessairement le niveau d'expertise des pays.

Dans ce cadre, un logiciel d'analyse de bibliographie sera développé. Il pourra à partir d'un domaine (défini par mots clés par exemple) et d'une cible (pays, université, chercheurs .etc.) générer un ensemble de représentations visuelles. Un outil d'analyse de bibliographie a déjà été développé et sera utilisé. L'interface graphique du logiciel permettra de spécifier le domaine et la cible afin de générer des statistiques et des représentations graphiques (sous forme de graphes).L'évolution des niveaux d'expertise est un élément important. Le logiciel produira des graphiques par année pour apprécier les tendances.

L'ensemble du projet devra être hébergé sur un serveur Git afin de permettre le développement collaboratif. Une attention particulière devra être portée à la documentation.

Étapes :

- Étude des différentes sources de publications scientifiques
- Développement d'un prototype de recensement automatique de publications
- Définition et modélisation des domaines et des cibles
- Création d'une base de données
- Connexion au programme fourni d'analyse de bibliographies
- Représentation graphique des résultats

Compétences :

- Programmation en Python
- Connaissances en bases de données
- Génération de la documentation de développement
- Connaissance et maîtrise de git

Références :

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.

Biryukov, M., & Dong, C. (2010). Analysis of computer science communities based on DBLP. In Research and Advanced Technology for Digital Libraries: 14th European Conference, ECDL 2010, Glasgow, UK, September 6-10, 2010. Proceedings 14 (pp. 228-235). Springer Berlin Heidelberg.

Burch, M., Pompe, D., & Weiskopf, D. (2015, July). An analysis and visualization tool for DBLP data. In 2015 19th International Conference on Information Visualisation (pp. 163-170). IEEE.
Le Format BibTex, https://fr.wikipedia.org/wiki/BibTeX