Rapport d’activité journée 3 Hackathon

Aujourd’hui nous avons avancé sur la récupération des métriques, la fonction heuristique et l’interface graphique.

**Récupération des métriques**

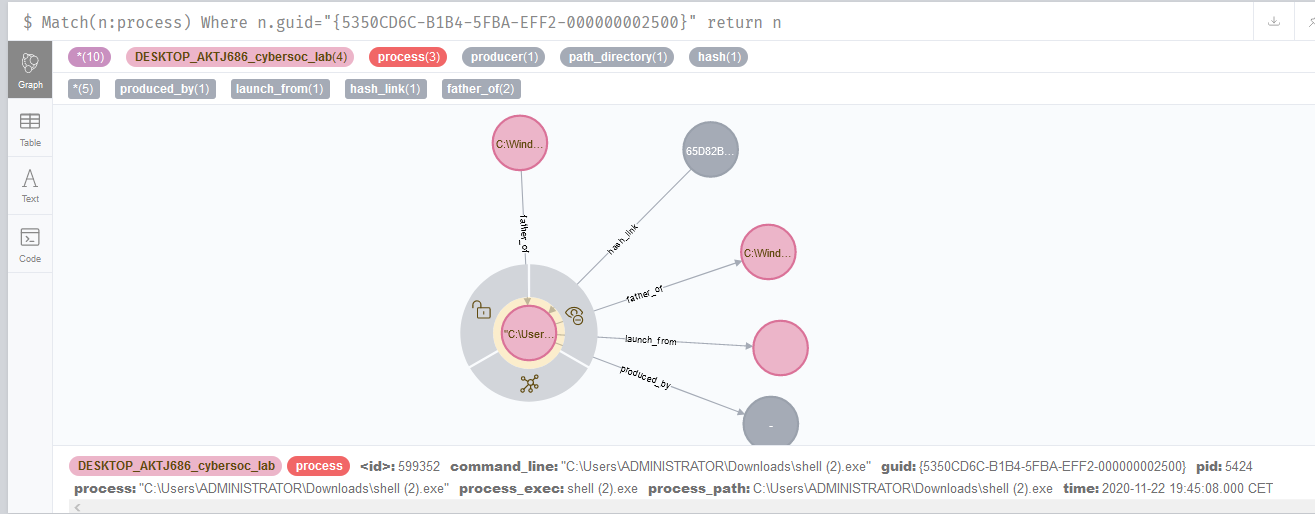
Nous avons terminé de construire les fonctions de récupération des métriques sur la base. Nous n’en n’avons pas rajouté pour l’instant.

**Fonction de scoring d’anomalie**

Nous avons ajouté une nouvelle classe à notre solution : la classe Threat Hunting, elle construit un score pour chaque processus.

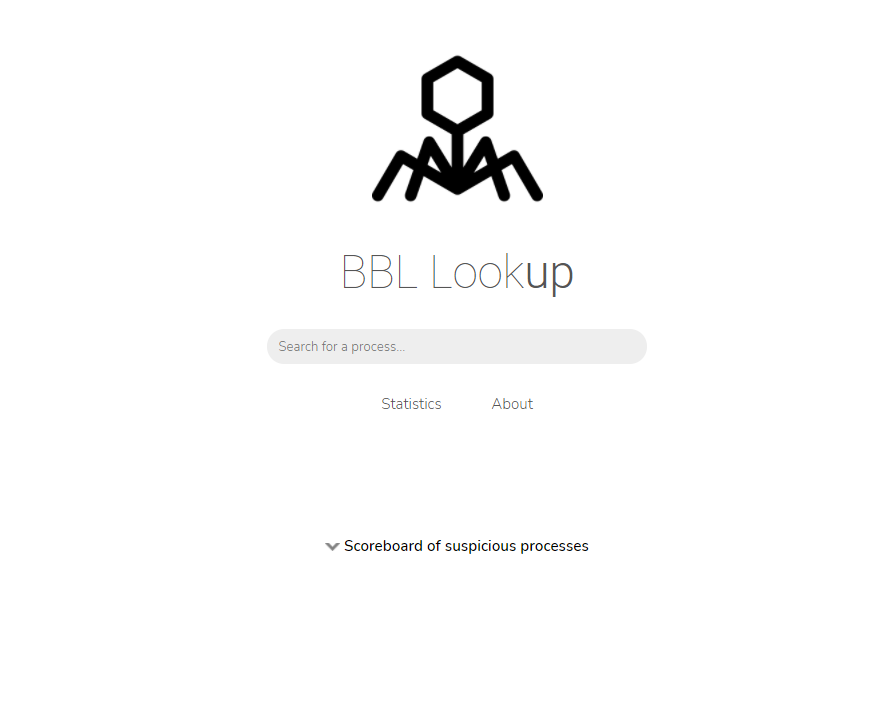
On a choisi de créer un score qui sera compris entre 0 et 6. Toutes les métriques ne sont pas encore utilisées. Ce score est construit en faisant la somme de 6 métriques, toutes normalisées, avec des coefficients particuliers. On va tenter de jouer avec ces coefficients pour peut-être améliorer la performance.

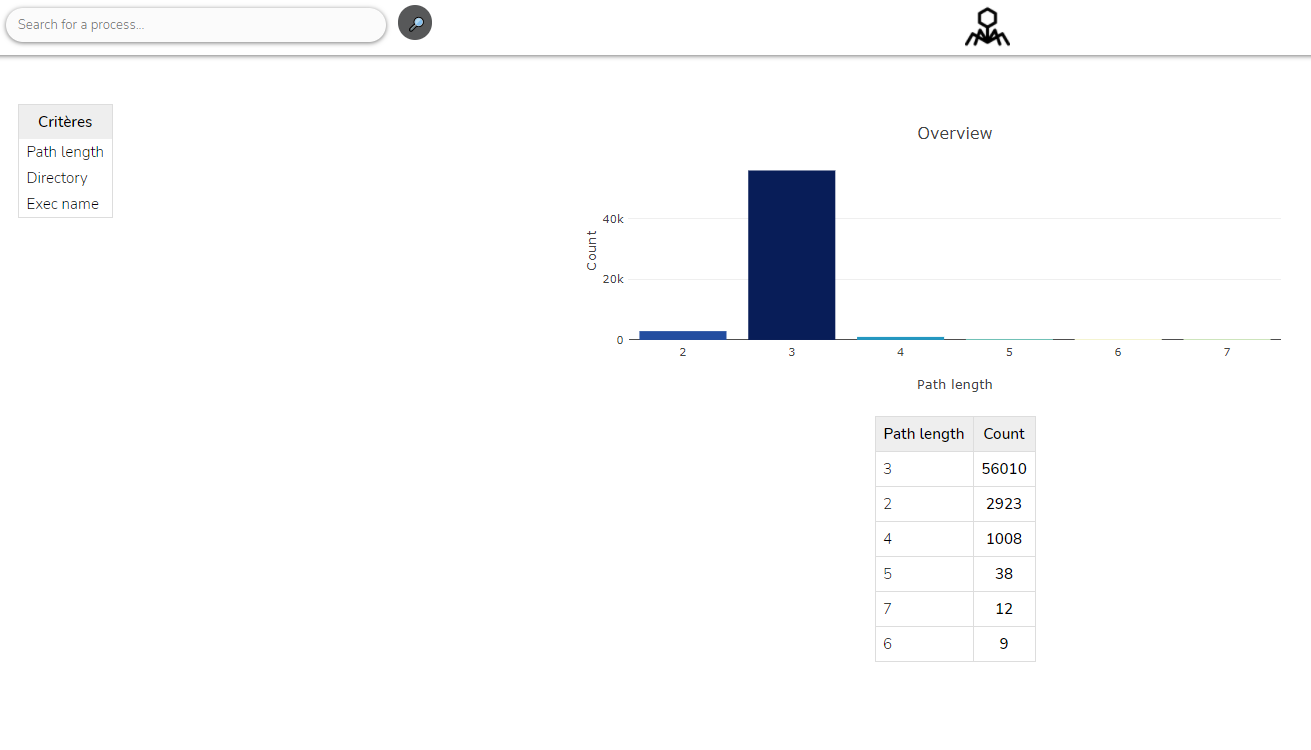
Nous avons déjà réussi à évaluer la base de données une première fois avec cette fonction, et nous avons trié les résultats.



Par exemple ce processus s’est retrouvé avec un score de 4.7, et nous paraît relativement suspicieux. Commande Shell dans le dossier Download. Nous avons aussi trouvé un exemple où Word.exe exécute des processus. Pour la suite nous voulons améliorer ce scoring en ajoutant les métriques manquantes.

**Interface graphique**

Page d’accueil de l’interface graphique. D’ici on doit pouvoir rechercher un processus particulier (à faire) et surtout afficher des statistiques sur les métriques. On obtient par exemple la page suivante.

Affichage de l’histogramme de la métrique « Path Length ».

**Quelques interrogations**

Pensez vous que nous puissions utiliser les Hashs labélisés par Virus Total pour évaluer notre scoring ? Sinon avez-vous une liste de logiciel malveillant que l’on pourra utiliser pour évaluer la qualité de notre fonction ?