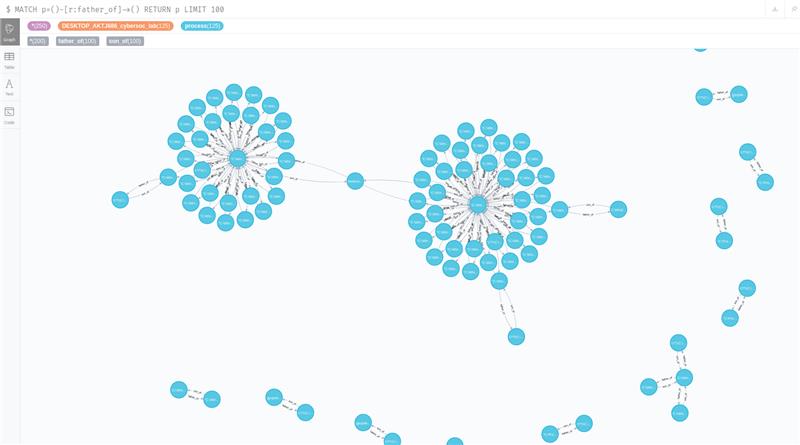
Rapport d’activité journée 1 Hackathon

Durant cette première journée nous avons décidé de construire un premier graphe pour les processus de la base de données que nous avons reçu. Lors de la recherche d’une clef primaire, élément que nous avons jugé nécessaire à la construction du graphe, nous nous sommes intéressés au *guid* de chaque processus, en espérant que couplé au nom de l’ordinateur, nous obtenions une clef composée unique.

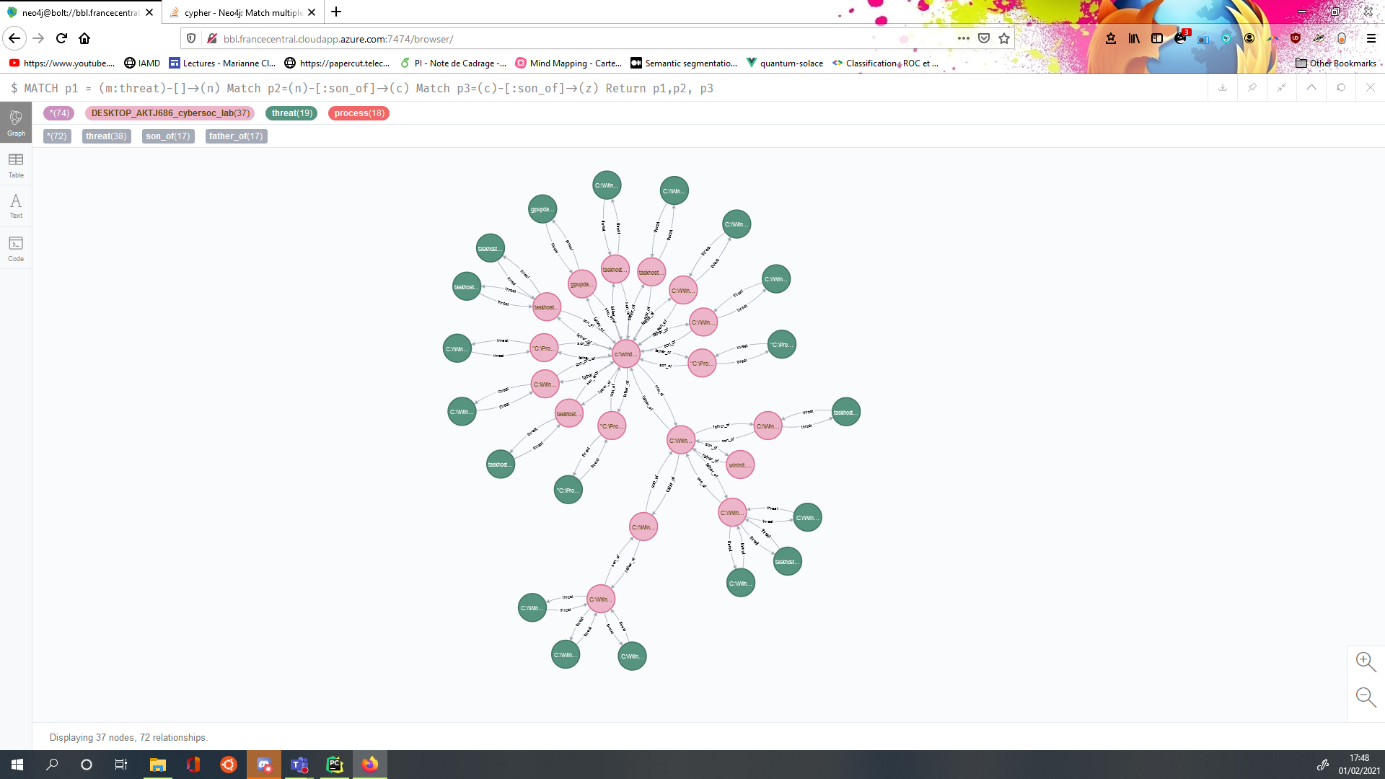
Cependant, nous avons trouvé plusieurs processus qui arboraient le même *guid*. Nous avons donc décidé dans notre graphe de séparer ces processus en créant un nouveau type de nœud que nous avons baptisé ‘*Menace*’.

Mis à part cela, nous avons réussi à remplir une base de données Neo4j dans laquelle chaque nœud standard représente un processus. Ce nœud comporte toutes les informations que l’on a retrouvé dans le fichier csv fourni comme le *Hash* ou l’*id*.

Nous avons aussi créé les liens de parenté entre les processus pères et fils, ce qui donne une représentation semblable à celle-ci-dessous.



Nous avons donc mis dans le graphe les nœuds ‘Menaces’ qui sont alors liés au processus avec lequel il partage un guid commun. On obtient alors ce genre de graphe :



On peut voir ici que certains nœuds que l’on a classé naïvement comme ‘Menaces’ proviennent d’un nombre réduit de processus pères.