RDV – Monsieur Gregory Blanc

Articles NIDS (SAE model) (détection d'intrusion) et DL4MD proposant des solutions d'IA pour la détection et l'analyse de malwares.

COMPTE-RENDU DE RDV – PROPOSITION D'UN SUJET CASSIOPEE

17 Nov 2017 - 9:30 - 10:20
Avec Gregory Blanc, Charles Mure et Félix Molina

Sujet : Détection d'intrusion ou analyse de malwares ? Les deux ? A définir plus précisement par la suite. Les deux sont intéressants et implémentables.

Tuteur projet Cassiopée : M. Gregory Blanc

But du projet : implementation d'algo de détection et/ou d'analyse malwares.

- Récupération de log data concernant l'analyse et la détection des malwares :
    → LOG http://www.unb.ca/cic/datasets/index.html
    → LOG http://www.netresec.com/?page=PcapFiles
    → Log provenant d'un collègues de M. Blanc (environ 1 To de données)

- A vérifier : les papiers de recherche cités (liés) à la détection et l'analyse de malwares sur reseau SDN via Google Scholar.

- Solution d'apprentissage streaming : à rechercher
    → Online Algorithm
    → Streaming Algorithm

- Simulation des menaces/attaques (si besoin) : BotNetSimulator.

- Envoi du sujet Cassiopée à Mme Kohlenberg pour acceptation.

- Choix d'une nouvelle date de RDV si le projet est accepté.