Unsupervised adverse learning in the detection and countermeasure of advanced persistent threat campaigns

Mots clés :

- **Directeur de thèse** : Aurélien LATOUCHE
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire inconnu!
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal** : Divers

Résumé du projet de recherche (Langue 1)

This PhD is also supervised by Valérie Viet Triem Tong and Ludovic Mé from CentraleSupelec. In information security, attackers are an ever-growing and ever-changing menace, while protection systems are mostly stuck to looking for known attack patterns. This PhD is part of a project whose aim is to leverage machine learning technologies in order to detect unknown threats when they strike. In particular, this PhD will focus on finding Advanced Persistent Threats, which are highly focused and highly capable attacks. The main research topic will be the linking of related events occurring at different times and maybe on different machines inside the same entity, even if the events take place several years apart. The aim is to, whenever an attack is detected, find out where the attack originated and how it got wherever it is now. This would assist first line responders in assessing the severity of the attack as well as teams doing forensic analysis.