HuMa, un outil pour l'analyse par l'humain de données de sécurité massives

Veronique Legrand*[1]

[1]CITI Centre of Innovation in Telecommunications and Integration of services (CITI) – INRIA, Institut National des Sciences Appliquées [INSA] - Lyon – CITI Laboratory, INSA Lyon Domaine Scientifique de la Doua Batiment Claude Chappe 6 avenue des Arts 69621 Villeurbanne Cedex Phone +33 4 7243 6415 Fax +33 4 7243 6227 E-Mail citi@insa-lyon.fr, France

Résumé

Jusqu'à présent, pour détecter des cyberattaques, les spécialistes de la sécurité opérationnelle utilisent des programmes qui analysent les traces informatiques, les comparent et les corrèlent face aux modes opératoires connus et aux modèles de menaces existants. Mais avec l'explosion des flux d'information et l'évolution des usages, ce travail est rendu plus difficile car il y a énormément de données à traiter et les sources d'information sont très hétérogènes. En effet, on constate une augmentation par an de 15% à 20% du volume des traces informatiques à analyser. Par ailleurs, un serveur moyen peut contenir 7 Go de logs par jour, une analyse humaine serait comparable à la lecture d'environ 11.000 livres de 300 pages par jour. Enfin, les cyberattaques peuvent se dérouler dans le temps avec une succession d'attaques et dans l'espace, sur plusieurs sites, sur différents supports ou sur des objets connectés.
Le but du projet Huma est donc de faciliter l'analyse des traces informatiques en créant des modèles d'attaque dynamiques qui seront ainsi plus facilement identifiables dans des flux massifs de données informatiques.

Mots-Clés: sécurité, big, data, SIEM, analyse

*Intervenant