Sujet 1 : MISP - Plateforme de partage d'informations sur les menaces

Proposé par Francine Herrmann en collaboration avec Sami Mokaddem et Alexandre Dulaunoy du Circl, Luxembourg

Ce sujet peut être réalisé par 2 étudiants – Ce sujet peut donner lieu à un job d'été -

La communauté informatique est confrontée à des incidents de toutes sortes et de nouvelles menaces apparaissent quotidiennement. Combattre seul ces incidents de sécurité est presque impossible. Le partage d'informations sur les cybermenaces au sein de la communauté de la sécurité informatique est devenu un élément clé dans la réponse à un incident. Des sources d'information fiables, fournissant des informations crédibles, sont en effet indispensables à la communauté, voire à plus grande échelle, aux services de renseignement et aux groupes de détection des fraudes.

La plateforme de partage d'informations sur les menaces (MISP) est une plateforme de confiance, qui permet la collecte et le partage d'informations concernant les indicateurs de compromission (IoC), les attaques ciblées, mais aussi les menaces, les vulnérabilités ou des indicateurs financiers utilisés dans cas de fraude. Le but du MISP est d'aider à la mise en place de programmes de prévention d'attaques et de contre-mesures.

L'objectif de ce sujet d'IR est d'analyser les indicateurs techniques et non techniques existants au sein des plates-formes MISP et de concevoir et développer un prototype de logiciel permettant d'afficher des informations facilement accessibles aux utilisateurs non techniques jouant un rôle dans la sécurité de l'information, tels que les gestionnaires de risques ou les auditeurs internes ou externes.

Le candidat concevra et développera une interface Web permettant d'interroger l'API MISP et de créer une nouvelle superposition afin de permettre une vue synthétique des informations pour un non expert.

En plus de la vulgarisation et de la synthétisation des données, l'étudiant pourrait concevoir et développer un logiciel de génération de rapport en langage naturel. Un peu comme un `exporter en PDF`.

Dans une autre optique, en plus d'aider les non-experts, on pourrait fournir du support aux personnes plus technique en proposant des étapes de prévention ou des mesures à prendre. Par exemple, le système pourrait proposer automatiquement des règles pour bloquer une adresse IP délivrant beaucoup de malwares.

Le logiciel conçu sera un logiciel autonome (à publier en tant que logiciel libre) reposant sur l'API existante du MISP, ainsi que sur les autres API de CIRCL ou des services externes.

Le plan du travail à réaliser sera le suivant :

a. Etude Bibliographique de la plate-forme MISP et des informations obtenues à partir de MISP
b. Etude bibliographique des indicateurs et informations utiles aux utilisateurs non techniques
c. Proposition de différents indicateurs de sécurité synthétiques et conception de vues synthétiques sous formes d'écrans ou de rapport)
d. Développement d'une application de visualisation synthétique des informations de synthèse
e. Conception/proposition d'un algorithme d'aide à la prévention et aux contre-mesures à prendre
f. Développement de cet algorithme d'assistance

Point de départ de l'étude de bibliographique :

[1] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. 2016. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security* (WISCS '16). ACM, New York, NY, USA, 49-56. DOI: https://doi.org/10.1145/2994539.2994542

[2] Andras Iklody, Gérard Wagener, Alexandre Dulaunoy, Sami Mokaddem, Cynthia Wagner, Decaying Indicators of Compromise, Cornell University Lybrary, 2018, https://arxiv.org/abs/1803.11052