Sujet de thèse – Outils de visualisation pour la cybersécurité

L'Institut de Recherche Technologique (IRT) System X a pour ambition de devenir une référence mondiale dans le domaine de l'ingénierie numérique. Pour cela, il s'appuie sur la co-localisation des ressources à la fois industrielles et académiques lui permettant d'avoir une efficacité et une dynamique d'innovation. Cette dernière favorise le décloisonnement des mondes publics et privés en abordant des thématiques de R&D prometteuses et des sujets de recherche d'avenir.

DÉFINITION DU CADRE DE LA THÈSE

Intégré au sein de l'Institut de Recherche Technologique System X, situé à Saclay et en étroite collaboration avec des industriels et des académiques, vous êtes amené à prendre part et à contribuer au rayonnement scientifique de System X. Vous travaillerez dans un environnement stimulant avec les meilleurs laboratoires de recherche Français (Inria, CEA, Institut Mines-Télécom, UP11, UTT (Troyes), UVSQ,…) et en étroite collaboration, sur des projets scientifiques prometteurs, avec des industriels (Airbus Group, Gemalto, Engie, …).

DESCRIPTIF DU SUJET de RECHERCHE

Le projet EIC (Environnement d'Intégration et d'Interopérabilité en Cybersécurité) vise à mettre en œuvre une plateforme expérimentale et technique en cybersécurité appelée CHESS (Cybersecurity Hardening Environment for Systems of Systems) qui permettra d'évaluer le couplage de technologies de cybersécurité à travers des cas d'usage innovants dans le domaine des SmartGrids, de l'Usine du Futur, du Transport Connecté et Autonome et des nouveaux services de l'Internet des Objets.

Perçu par certains comme un espace à part entière, le cyberespace est bien plus difficile à cerner que les espaces traditionnels (air, terre, espaces maritimes) en raison de la superposition de ses couches physiques, logiques et cognitives. Que l'on soit dans une démarche de cyberdéfense, d'aménagement du territoire ou d'évaluation des capacités d'un pays, cartographier le cyberespace de façon dynamique est devenu un enjeu stratégique. Des outils de visualisation permettent d'associer plus efficacement les décideurs à la compréhension des enjeux de la cybersécurité pour la continuité de leurs activités et l'acceptation par leurs clients de leurs solutions. Ils aident à mieux comprendre les actions permanentes de protection et constituent, le cas échéant, une aide à la décision en cas de crise mineure ou majeure. Ces mêmes outils faciliteront le travail quotidien des analystes dans les plateformes opérationnelles de type SOC/NOC (Security and Network Operation Center) ainsi que celui des "risks manager" (responsables sécurité des systèmes d'information, Chief Data Officer).

Dans cette thèse, on cherche à mettre en place de nouvelles solutions et à développer des outils de visualisation facilitant l'analyse de données complexes et massives (architectures complexes et hétérogènes, traces de sécurité, comportements) pour mieux comprendre les agressions dont est victime le système et en assurer une meilleure protection et en garantir la résilience. Trois étapes pourront être franchies :

<u>1/ État de l'art des outils de visualisation en cybersécurité sur des architectures IT « classiques ».</u>

Depuis quelques années, de nombreuses applications apparaissent sur le marché permettant de mettre en œuvre la visualisation à partir de bases de données standard pour produire des représentations visuelles relativement familières et exploitables par des analystes.

Cette activité visera à réaliser des représentations et cartographies du cyber espace, des attaquants et des menaces :

- Cartographie générale : IP, DNS, média sociaux, acteurs, hacktivistes, cybergéographie, caractérisation du risque (au-delà de Maltego et autres)
- Carte des attaques sur un espace de représentation des AS et non géographique
- Cyber Visual Analytics : Aide à l'analyse au travers de nouvelles représentations/visualisations notamment dans l'investigation, la qualification et l'attribution des attaques.
- Vers une vision dynamique des cyber attaques

2/ Modèles de visualisation sur des architectures hyper connectées.

La visualisation analytique est apparue en 2004 et a progressé depuis avec des systèmes comme Jigsaw de Georgia Tech ou de la société Occulus de Toronto. Il s'agit de concevoir et de réaliser ici des composants semblables à ceux fournis par Jigsaw, permettant l'exploration de corpus étiquetés de manière fluide et expressive.

Des composants graphiques en client léger seront privilégiés : système orienté Web avec les technologies de visualisation incorporées aux navigateurs récents (Chrome, Firefox, Safari) : HTML5, JavaScript, CSS et XML/SVG. La performance sera évaluée comme facteur dominant.

Pour prendre un exemple, les composants de visualisation des données relatives à la cybersécurité des cas d'usages d'EIC et accessibles par les réseaux sociaux s'appuieront sur des librairies open sources à l'instar de D3.js (Data-Driven Documents).

3/ Applications à la plateforme CHESS pour les SOCs du futur.

Pour les activités opérationnelles de type SOC, il s'agit de faciliter la navigation dans les résultats des analyses et des requêtes réalisées dans des grands volumes de données pour aider l'analyste dans ses tâches (analyse de logs, suivi des échanges des hackers sur les média sociaux, dynamique des agressions …). Les principaux points à résoudre sont :

- La facilité d'utilisation par des analystes ;
- La gestion de la dynamicité des données ;
- Le passage à l'échelle.

Il s'agit également de proposer des nouvelles interfaces de visualisation de données et de démontrer des modalités innovantes d'interaction associées, par exemple avec des dispositifs comme « leap motion », « myo » et « kinect ».

COMPÉTENCES REQUISES

- Maîtrise de langages de programmation pour la manipulation de données (Java et/ou Python) et le développement Web (HTML5, JavaScript, CSS et XML/SVG) ;
- Capacité à appréhender rapidement les technologies de stockages de masse NoSQL (MongoDB, ElastiscSearch, Neo4j, OrientDB, Hadoop, …)
- Idéalement issu d'un Master de Data Mining
- Sensibilité à l'ergonomie et au design Web

APTITUDES PERSONNELLES

- Personne communicante et dynamique ;
- Autonome et bon esprit d'initiative

LOCALISATION ET CONTACTS

Ref : Thèse-EIC-1

Localisation: IRT System X, 8 Avenue de la Vauve, 91120, Palaiseau.

Contacts: Philippe Wolf : philippe.wolf@irt-systemx.fr
Nabil Bouzerna : nabil.bouzerna@irt-systemx.fr