Cet appel à projets vise à stimuler l'innovation collaborative afin de proposer des solutions pour renforcer la sécurité numérique des entités de petite dimension, telles que les PME et les administrations communales, allant de l'évaluation des risques jusqu'à l'analyse des intrusions. Il est mené en collaboration avec la section forensique de la Police cantonale vaudoise.

Nous encourageons les chercheurs des Hautes Ecoles, les acteurs de l'innovation et les experts en cybersécurité à unir leurs forces pour répondre à l'ampleur des évolutions en cours et contribuer à la protection essentielle des petites organisations contre les menaces croissantes de cybercriminalité.

Contexte et enjeux

L'élargissement des périmètres numérisés dans tous les domaines d'activités est corrélé à une montée en puissance fulgurante de la cybercriminalité. Les organisations criminelles diversifient et professionnalisent leurs activités, exploitant les faiblesses d'un environnement numérique de plus en plus vaste et complexe (architecture des systèmes, objets connectés, évolution de leur *supply chain*, développements *open source*, techniques de virtualisation, bases d'apprentissage par *machine learning*). Pour atteindre leurs objectifs de compromission, les modèles d'attaques deviennent très sophistiqués, techniquement et socialement, car la manne financière est énorme.

Les petites structures organisationnelles, telles que les PME et les administrations communales, constituent l'ADN de notre tissu socio-économique. Elles sont vitales. Pourtant, ne disposant souvent pas des compétences et ressources nécessaires pour s'en prémunir efficacement, elles se trouvent particulièrement exposées aux cybermenaces. Le combat est inégal : alors que les défenseurs disposent de moyens financiers limités pour essayer de sécuriser l'ensemble des composants et systèmes, les attaquants disposent quant à eux d'importantes ressources pour essayer d'exploiter une seule faille.

Les conséquences d'une cyberattaque sur ces structures organisationnelles fragiles impactent souvent gravement leur fonctionnement et la confiance de leurs clients et partenaires, conduisant régulièrement à une cessation d'activités économiques dans la période qui suit l'attaque, respectivement à une perte d'efficience et de confiance des citoyens. Outre le risque de perte d'emploi, les répercussions humaines sont aussi de nature psychologiques et sociales pour les victimes d'une attaque informatique, qui se trouvent démunies dans un environnement non-maîtrisé.

Dans ce contexte, la protection numérique des petites organisations est un gage de compétitivité, voire de survie de notre tissu socio-économique. Il est primordial de promouvoir une culture et d'encourager une approche proactive de la cybersécurité afin de créer un écosystème cyber résilient et robuste, prenant en compte les défis spécifiques auxquels ces acteurs sont confrontés.

Objectifs

L'objectif de cet appel à projets est de contribuer au **développement de briques technologiques et à l'élaboration des méthodes et outils disruptifs pour l'évaluation de la sécurité, la prévention, la détection et l'analyse de vulnérabilités et d'intrusions sur des systèmes et réseaux informatiques spécifiques aux petites organisations**.

Nature des projets

Les projets attendus prendront en compte les caractéristiques propres aux organisations de taille réduite, telles que des ressources financières et humaines limitées, leurs systèmes organisationnels et leurs processus opérationnels. Ils visent des résultats réplicables ou industrialisables, à contrario de solutions personnalisées.

Les projets pourront être d'ordre logiciel, par la réalisation ou l'extension d'un logiciel en lien avec la sécurité informatique, **ou d'ordre organisationnel**, par la définition de nouveaux processus pour le fonctionnement des PME.

Les projets d'ordre logiciels impliqueront le **développement de nouveaux outils informatiques** ou d'extensions pour des outils existants. Les logiciels concernés sont variés et peuvent être regroupés en trois catégories :

- **Les logiciels spécifiquement relatifs à la sécurité** : pare-feu, antivirus, systèmes de détection ou de réaction aux intrusions (nouvelles heuristiques), système de récolte ou stockage des événements ou des traces (assurance de non-répudiation, ...), système d'évaluation de la sécurité informatique (d'un réseau, site web, ...)
- **Les logiciels orientés entreprise en lien avec les aspects de sécurité de l'information** : VPN, systèmes d'identification et gestion des accès des utilisateurs, système de gestion de secrets d'entreprise (mots de passe, certificats, …)
- **Les logiciels favorisant la résilience de l'organisation aux incidents informatiques** : système de sauvegarde et de restauration des données, réplication des services informatiques, système de gestion de la documentation des ressources informatiques, service de surveillance des ressources informatiques

De nouveaux processus organisationnels pourront également être créés pour réduire l'exposition aux risques de sécurité ou améliorer la résilience des PME face aux menaces. Par exemple, des programmes de formation ou de sensibilisation à la sécurité informatique ainsi que les bonnes pratiques relatives peuvent être constitués. Des listes de points faibles dans les architectures classiques des PME peuvent être définies, par retour d'expérience, afin d'orienter ou de faciliter l'évaluation des composantes de sécurité. Divers règlements, tels qu'une « Politique d'utilisation sécuritaire des ressources informatiques » (ordinateurs, services en ligne, e-mail, …) ou une « Politique d'utilisation des ordinateurs personnels dans le cadre professionnel » (ou inversement) peuvent être rédigés. Finalement, une proposition de standardisation pour les annonces d'incidents informatiques (attaques, fuites de données, …) aux administrations, tels que des modèles de déclaration d'incidents, peuvent faire l'objet d'un projet.

Domaines d'expertise

Les projets s'inscrivent notamment dans les domaines suivants (non-exhaustif) :

- Méthodes et outils interactifs pour l'évaluation et le réentraînement des compétences humaines basés notamment sur des briques technologiques de cyber-range et de simulation (plateformes éducatives, simulateurs d'attaque, etc.)
- Solutions d'évaluation et d'audit des composants et des systèmes explorant l'apport de l'intelligence artificielle et intégrant des technologies de *deep learning*, de virtualisation et de désagrégation
- Techniques de durcissement des produits, services ou systèmes de façon mesurable, répétable et industrialisable
- Briques de sécurisation modulaires et évolutives intégrables dans les infrastructures existantes, notamment pour les outils de communication à distance et collaboratifs
- Mécanismes et outils de recherche automatisée des vulnérabilités et de détection précoce des intrusions basés sur l'intelligence artificielle et le *machine learning,* automatisation de pentest
- Outils d'analyse des méthodologies d'attaque et des modèles comportementaux combinant potentiellement du matériel et du logiciel (modèles sémantiques dysfonctionnels, techniques de *reverse engineering*, analyse à base d'IA, algorithmes d'analyse d'impact à l'échelle des systèmes, techniques de visualisation et de navigation interactives, etc.)
- Méthodes et techniques d'investigation numérique et d'analyse forensique tenant compte de l'impact du cadre légal associé (investigation de failles matérielles pouvant être exploitées par logiciel, analyse d'images systèmes et de mémoires de systèmes embarqués, analyse sur dispositifs physiques, etc.)
- Outils favorisant la standardisation des rapports d'incidents et l'obligation juridique d'annonce des cyberattaques