Stagiaire – Ingénieur Cybersécurité (H/F)

durée : 4 à 6 mois
Vous devez impérativement disposer d'une convention de stage école couvrant toute la durée de la mission

Environnement de travail

L'équipe « IT Operational Security » est composée d'experts en Cyber Sécurité utilisant leurs compétences et leurs connaissances afin de répondre à 4 missions principales :

1. **Identifier** les déviations de sécurité le plus en amont possible des projets ou des installations
2. **Protéger** le système d'information BGL
3. **Maintenir** à jour le dispositif Cyber pour identifier de potentielles fuites de données et inversement, assurer que les informations/fichiers reçus de l'extérieur soient sûrs
4. **Répondre** aux évènements et incidents de sécurité détectés

Votre mission :

En intégrant l'équipe « IT Operational Security », vous serez amené à intervenir de manière transverse sur l'ensemble des activités. Vous aurez plus précisément les domaines d'intervention et responsabilités suivants.

IDENTIFIER

- ✓ *Architecture de domaine – sécurité opérationnelle :* Garantir la mise en place des projets/outils selon les normes et standards d'architectures « Cyber Security »

PROTEGER

- ✓ *Threat Intelligence :* Vous tenir à jour sur les nouveaux vecteurs d'attaque en lien direct avec le GCSIRT (Global Security Incident Response Team) qui nous alimente régulièrement sur des Patch Emergency/IOC, …
- ✓ *Vulnerability Management :* Réaliser les scans de vulnérabilités et de conformité, présenter les vulnérabilités et les non-conformités détectées, suivre leurs remédiations avec les équipes. Réaliser un reporting mensuel permettent de suivre l'activité.

DETECTER

- ✓ *Data Security :* Gérer les plates-formes DLP – In Motion et At Rest en implémentant les « Baselines de uses-cases Groupe/Locaux »
- ✓ *Malware Protection :* Gérer les outils de protection des flux entrants et sortants (Mails/Web)
- ✓ *Veille (transverse) :* Définition de nouveaux uses cases, Améliorations des processus
- ✓ *Communication/Coordination :* Liens avec les autres CSIRT du Groupe et avec d'autres acteurs de la place de Luxembourg (CIRCL, etc, …)

REPONDRE

- ✓ *Application Security :* Mettre en place le monitoring de sécurité adéquate afin d'évaluer périodiquement les applications de production et pouvoir détecter toute déviation (vulnérabilité/Non-Conformité) « Cyber ».
- ✓ *Cyber Incident Management :* Réaliser les investigations sur base des incidents ouverts et escalader en cas de doute ou de fraude potentielle
- ✓ *Forensics :* En cas d'une attaque réussie, réaliser les analyses « Forensics » afin de retracer la chaîne d'attaque et récolter les preuves
- ✓ *Cyber Crisis Management :* En cas de crise Cyber majeure, participer au comité en tant que consultant/expert Sécurité.

Apports du poste

En rejoignant notre équipe vous pourrez :

- ✓ Relever un nouveau challenge, élargir et renforcer vos compétences et connaissances Cyber
- ✓ Découvrir le métier d'experts/ingénieurs en Cyber Sécurité
- ✓ Evoluer au centre du dispositif Cyber et collaborer avec tous les acteurs de la Banque (IT, Métiers et d'autres entités du Groupe)
- ✓ Intégrer un domaine d'activité passionnant, en constance évolution et qui s'adapte en fonction des actualités

Formations /montée en compétences

Un catalogue/cursus de formations spécifique à l'activité de l'équipe « IT Operational Security » a été mis en œuvre afin de vous donner les repères nécessaires à votre « Onboarding » dans notre dispositif Cyber. Vous pourrez également compter sur le soutien de toute l'équipe pour vous guider dans vos premiers pas et répondre à vos questions.

Votre profil

Formation : Formation Universitaire Ingénieur ou Master en informatique / Sécurité de l'Information et des Systèmes (Bac +4/5)

Vous êtes à la recherche d'un stage ? Vous recherchez à intégrer une équipe jeune et dynamique ? Vous souhaitez apprendre un métier passionnant et qui a du sens ? Être accompagné par un tuteur inspirant et à l'écoute ?

Compétences comportementales :

- ✓ Capacité à collaborer / travail d'équipe
- ✓ Capacité à synthétiser / simplifier
- ✓ Capacité d'organisation
- ✓ Proactivité

Compétences techniques :

- ✓ Veille Cyber Sécurité : connaissances des framework de sécurité NIST, CIS
- ✓ Environnement d'exécution : Linux / Windows
- ✓ Outillage : Pack MS Office – Excel et Powerpoint, Service Now, …

Compétences linguistiques :

Pratique courante du français et bonne maîtrise de l'anglais à l'écrit et à l'oral