Expert Sécurité Informatique (F/H)
(CDI / Temps Plein)

Rattachement :

Direction Sécurité des systèmes d'information (SSI) - RSSI

Localisation :

La Défense - Île de France

Qui sommes-nous ?

STET est un opérateur bancaire européen, leader sur le processing des paiements SEPA et des cartes. Nous proposons aux banques qui sont nos clientes un catalogue de 6 services distincts : la compensation inter-bancaire / le paiement instantané / l'autorisation bancaire / la digitalisation des moyens de paiement / la prévention de la fraude / l'authentification bancaire

Notre entreprise à taille humaine repose sur 4 valeurs : coopération, exemplarité, reconnaissance, cohésion.

Grâce à sa stratégie fondée sur l'innovation, STET est au cœur des révolutions dans le monde du paiement.
STET s'engage à favoriser des environnements de travail inclusif, respectueux de tous, propices à la créativité et équitable. Le développement professionnel comme une condition de notre performance collective et du bien-être de nos collaborateurs. La confiance au sein de nos équipes est un gage de la confiance que nous suscitons auprès de nos clients.

Qui êtes-vous ?

Diplômé d'une école d'ingénieurs ou équivalent (BAC+4/5) en sécurité informatique, vous avez au moins 8 ans d'expérience professionnelle dans les métiers liés à la sécurité des systèmes d'information.
Vous êtes idéalement doté d'une expérience de 10-12 ans dans la conception, la mise en œuvre et le suivi de la sécurité des systèmes critiques notamment dans le domaine des paiements interbancaires et les systèmes de place.
Une expérience des systèmes sensibles en termes de disponibilité, performance et sécurité serait un plus.

Votre Mission ?

Vous intervenez comme expert métier sur les processus de l'entreprise sur les questions de sécurité informatique. Vous assurez le maintien en condition de sécurité du système d'information et en particulier des périmètres d'autorisation et de compensation, dans l'activité de la Sécurité Opérationnelle et dans le cadre des directives définies par la Gouvernance.

Ce que nous pouvons accomplir ensemble :

- Piloter la conformité de l'architecture de l'infrastructure avec la politique de sécurité en place,
- Piloter le suivi des actions liées à la sécurité auprès des différentes équipes (spécificateurs, exploitants…)
- Coordonner et / ou piloter les projets liés à la sécurité
- Piloter la gestion et l'administration des activités liées aux opérations d'outils de sécurité (PKI, gestion d'outils spécifiques, …)
- Assurer la supervision des dispositifs de protection et de sécurité du SI
- Assurer la responsabilité du processus de veille technologique basée sur des outils de remontée d'alerte de sécurité s'appuyant sur des études d'impacts sur le système et la criticité de ses composants
- Assurer l'interface transverse et fournir un support pour assister les directions opérationnelles dans la mise en œuvre de la sécurité (phase de cadrage) dans les projets de l'entreprise
- Assurer une veille sécuritaire : maintient les abonnements de service de veille et s'assure que les différents correspondants disposent bien de l'information nécessaire.
- Organiser les tests de vulnérabilité : organise et réalise les tests de vulnérabilité sur les différents périmètres, avec les outils mise à disposition, en fonction de la politique d'entreprise et des normes auxquels ils sont assujettis.
- Tests d'intrusion : Être le contact privilégié des sociétés mandatés pour ses tests dans l'organisation, le suivi et la relation avec les différentes entités participantes.
- Analyser et qualifier les résultats de ces différentes sources d'information et informer les équipes concernées de ceux-ci.
- Communiquer les solutions possibles afin que les équipes puissent engagés les travaux de correction fonction des choix retenus et du niveau de priorité défini.
- Apporter son expertise sur l'architecture et la configuration d'équipements en matière de sécurité à la demande des entités l'exprimant.

Ce que vous savez faire :

Sur la partie métier :

- Cartographier les risques techniques et fonctionnels et estimer leur criticité
- Analyser et comprendre l'origine d'un dysfonctionnement, incident ou accident (spécifications physiques du produit, processus...)
- Vous disposez d'une bonne connaissance des systèmes d'exploitation, des équipements réseaux, des équipements et outils de sécurité.
- Elaborer des préconisations, proposer des solutions et scénarii d'amélioration
- Détecter, qualifier et traiter des incidents de sécurité
- Réaliser une analyse de risque en utilisant des normes et des méthodes standard
- Maitriser les règles de sécurité du Groupe applicable à son périmètre, les appliquer et les faire appliquer autour de soi
- Accompagner les projets de sécurité, définir les architectures sécuritaires,
- Participer à toutes les réunions techniques.

Vos compétences transverses :

- ✓ Vous savez communiquer de façon habile et fine dans des situations complexes (message sensible, public difficile, situation imprévue…)
- ✓ Vous savez Evaluer l'impact des changements et proposer les réponses ou les solutions adéquates ?
- ✓ Analyser l'information issue de différentes sources pour identifier les relations et les tendances ?
- ✓ Concevoir et mettre en œuvre des solutions nouvelles et efficaces ?
- ✓ Vous disposez d'un niveau d'anglais technique / courant à l'écrit et à l'oral ?
- ✓ Vous avez une bonne capacité d'analyse ainsi qu'un esprit de synthèse ?
- ✓ Vous avez une bonne connaissance des systèmes d'exploitation, des équipements réseaux, des équipements et outils de sécurité ?

Alors ce poste est fait pour vous !

Des déplacements sont envisageables dans les datacenters

Rejoignez-nous !

Rémunération : 70-80K

Mettez à profit vos compétences dans une organisation de système de paiement d'importance systémique qui souhaite recruter les talents de demain, pour répondre aux besoins de ses clients.

- Tous nos postes sont ouverts aux personnes en situation de handicap. (F/H)
- STET s'engage dans une dynamique d'évolution en matière d'égalité professionnelle pour renforcer la mixité à tous les niveaux de l'organisation.
- Nous accordons la plus haute importance à la protection des données personnelles de nos salariés et de nos candidats.

Pour envoyer votre candidature : Jean-Marc.Guichard@stet.eu

Pour plus d'informations retrouver nous sur www.stet.eu

A très vite !