Fonction
EXPERT CYBER IV.A (H/F)

Évolutions possibles

Au sein du métier

- RSSI IV.A (H/F)
- RSSI IV.B (H/F)
- ADMINISTRATEUR SOLUTIONS DE SECURITE III.3 (H/F)
- ADMINISTRATEUR SOLUTIONS DE SECURITE IV.A (H/F)
- ANALYSTE DE LA MENACE III.3 (H/F)
- ANALYSTE DE LA MENACE IV.A (H/F)
- ANALYSTE REPONSE INCIDENT III.3 (H/F)
- ANALYSTE REPONSE INCIDENT IV.A (H/F)
- ANALYSTE SOC III.2 (H/F)
- ANALYSTE SOC III.3 (H/F)
- ANALYSTE SOC IV.A (H/F)
- CORRESPONDANT SECURITE III.2 (H/F)
- CORRESPONDANT SECURITE III.3 (H/F)
- CORRESPONDANT SECURITE IV.A (H/F)
- EXPERT CYBER IV.B (H/F)
- PENTESTEUR III.3 (H/F)
- PENTESTEUR IV.A (H/F)
- RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.A (H/F)
- RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.B (H/F)
- RESPONSABLE PROJET DE SECURITE III.3 (H/F)
- RESPONSABLE PROJET DE SECURITE IV.A (H/F)
- EXPERT CYBER IV.A (H/F)

Raisons d'être

L’Expert Cybersécurité se tient en permanence au fait de l’état de l’art dans son domaine d’expertise et maintient le savoir-faire dans l’entreprise.

Il est en appui des Spécialistes et des autres acteurs de la Filière SI.

Il définit la politique d’évolution dans le domaine de la Cybersécurité et veille à sa mise en œuvre.

Il assure l’optimisation de l’architecture SI (fonctionnelle, technique, applicative, données, sourcing …) et contribue dans le domaine de la Cybersécurité à la pertinence et à l’efficience de l’architecture SI.

L'expert Cyber peut évoluer vers des fonctions de RSSI – Responsable détection et réponse – Analyste réponse incident – Pentesteur – Administrateur solution sécurité – Responsable projet de sécurité – Correspondant sécurité de projet

Missions

Être en appui des spécialistes et des autres acteurs de la filière SI

En tant que référent dans le domaine de la Cybersécurité il :

- Informe les spécialistes sur les aspects les plus pointus et novateurs de son domaine
- Aide et conseille les équipes techniques sur les problématiques les plus complexes

Se tenir au fait de l’état de l’art dans le domaine de la Cybersécurité

- Réalise la veille technologique et réglementaire : connaît l’état de l’art et des déploiements du Groupe et capitalise sur les retours d’expérience
- Connaît et s’informe sur les évolutions du marché et recherche les solutions répondant au mieux à la politique d’évolution du SI de l’entreprise
- Participe aux colloques, forums et groupes de travail dans son domaine d’expertise
- Sollicite, le cas échéant, les interlocuteurs et les ressources DSGG, achats, juridiques, RH…pour

bénéficier de leur appui.

Définir la politique d’évolution du SI relativement au domaine de la Cybersécurité

- Analyse et anticipe les impacts des évolutions de la Cybersécurité sur le SI de l’entreprise
- Assure les meilleures conditions de ressources humaines, matérielles, méthodologiques, logicielles… pour garantir la meilleure efficience.
- Définit la politique d’évolution du SI dans le domaine de la Sécurité SI et/ou du make or buy
- Participe à la définition et à l’élaboration des solutions envisagées, en particulier pour les parties complexes et/ou sensibles
- Réalise les évaluations, les qualifications, les intégrations et les tests dans le domaine de la Sécurité SI

Contribuer à l’élaboration des standards techniques

- Participe à l’élaboration des normes et standards techniques et veille à leur mise en œuvre

Compétences

Comportementales Socles

Orientation client
: Enrichir l'expérience client en adoptant une posture de service et de conseil et développer une relation de confiance durable. Anticiper, analyser, comprendre les besoins et attentes de ses clients pour apporter des réponses personnalisées. S'appliquer à améliorer la satisfaction client et mesurer son niveau de satisfaction.

Culture du changement et de l'innovation
: Encourager et accompagner le changement et les initiatives d'amélioration dans un environnement complexe et incertain. Expérimenter, tester, évaluer en s'appuyant sur de nouvelles méthodes, y compris numériques. Comprendre et susciter l'innovation en remettant en question les usages et en osant être pionnier. Etre dans une dynamique d'identification et d'apport de nouveautés dans son activité en osant sortir du cadre pour penser le problème en dehors de ses limites et de ses moyens lorsque la situation le demande.

Coopération et ouverture
: Construire et faire vivre des réseaux informels ou structurés d'individus ou de groupes en s'appuyant sur les outils collaboratifs comme les réseaux sociaux internes. Participer individuellement à l'atteinte d'un résultat collectif en favorisant l'entraide et le partage de connaissances. Savoir fédérer les parties prenantes d'un projet autour d'un objectif commun et établir des partenariats. Faire preuve d'écoute active vis-à-vis de ses interlocuteurs et prendre en compte leurs problématiques et les objections émises dans ses actions et prises de décision. Etre ouvert(e) d'esprit et curieux(se) au sein de son environnement.

Orientation résultats
: Engager des actions et mobiliser en toute autonomie des ressources (financières, matérielles, techniques, numériques et humaines) pour atteindre des performances durables dans le respect des principes éthiques, de qualité de vie et de RSE. Savoir être proactif et fixer, pour soi et/ou pour d'autres, des objectifs ambitieux et exploiter des opportunités pour aller au-delà des attendus.

Cyber Sécurité

Compréhension des menaces cybersécurité
: Etre capable de d'identifier, analyser et anticiper les cybermenaces susceptibles de mettre en péril les intérêts de l'organisation et/ou des partenaires (ex : groupe d'attaquants, menace étatique, etc.)

Vulnérabilités des environnements
: Maitriser les principes, méthodes et outils d'évaluation des vulnérabilités et identifier les contre-mesures appropriées

Sécurité des systèmes d'exploitation
: Maitriser la sécurité des systèmes d'exploitation (poste de travail, serveur, mobile) connus sur le marché (Windows, Linux, iOS, Android, etc.) : méthodes de durcissement, connaissance des outils de sécurité natifs, connaissance des principales attaques.

Sécurité des réseaux et protocoles
: Mettre en place, maintenir et améliorer les pratiques établies en matière de sécurité des réseaux (ex : NIPS, anti-malware, restriction/empêchement dispositifs externes, filtres anti-spam) et des protocoles. Maitriser des outils d'analyse de réseau pour identifier les vulnérabilités (ex : fuzzing, nmap, etc.). Reconnaitre et interpréter une activité réseau malveillante dans le trafic. Maitriser l'utilisation d'analyseurs de protocoles. Maitriser la configuration et l'utilisation des composants de protection des réseaux (par exemple, pare-feu, VPN, systèmes de détection des intrusions dans les réseaux)

Sécurité des architectures
: Concevoir des architectures de sécurité qui répondent aux besoins fonctionnels et techniques exprimés par les projets, en respectant le modèle d'architecture de l'entreprise et la PSSI. Supporter les équipes

de conception et intégration des solutions jusqu'à la mise en oeuvre. Contribuer aux analyses de risques. Partager ses connaissances pour la rédaction de politiques

Sécurité applicative

Maitriser les techniques de sécurisation des applications : gestion des identités et des habilitations, sécurité dans les développements, chiffrement des données pendant l'échange et au stockage, gestion des certificats

Efficacité professionnelle

Veille / innovation / tendances

Se tenir informé(e) des tendances, des évolutions technologiques et des innovations en vigueur dans son domaine d'intervention en lien avec les enjeux de l'entreprise et attentes des clients / partenaires et à les intégrer dans son activité.

Techniques SI

Cartographie, principes et composants de l'architecture technique et de production

Maîtriser les cartographies, principes et composants de l'architecture technique et de production : - Cartographie réseaux, impression, services de messagerie, bus applicatif... - Architecture de partage, serveurs et outils distribués, implémentation CCU et RSE - SI internes/externes et cartographies des déploiements des services sur le Cloud - Référentiels d'entreprise - Urbanisation à l'échelle de l'entreprise, vision globale - Coexistence des processus internes et de l'outsourcing (BPO, ITO)

Cartographie, principes et composants de l'architecture fonctionnelle et applicative

Maîtriser la cartographie, les principes et composants de l'architecture fonctionnelle et applicative : - Cartographies : fonctionnelles, applicatives, de flux, de référentiel et d'utilisateurs - Couverture fonctionnelle d'un domaine Métier et des éléments communs aux autres domaines - Référentiels de données et applications partagées par plusieurs domaines

Innovation technologique

Identifier, créer et prototyper des nouveaux concepts et idées, produits ou services porteurs de valeur pour l'Entreprise notamment à travers une veille et la réalisation de pilotes en lien avec les clients et les opérationnels. Synergie, développement Agile, collaboration et animation avec les éco-systèmes numériques (Open Innovation, French Tech, Start Up . . .)

Famille

Filière

Métier

Répartition des effectifs

- Services-Courrier-Colis
- Banque postale
- Bgpn reseau
- Groupe - siege

Effectif de la fonction

De 10 à 49