Fonction
ADMINISTRATEUR SOLUTIONS DE SECURITE III.3 (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 IV.A (H/F)
- ANALYSTE SOC III.2 (H/F)
- ANALYSTE SOC III.3 (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’administrateur de solutions de sécurité installe, met en production, administre et exploite des solutions de sécurité (antivirus, sondes, firewalls, IAM, etc.).

Il participe au bon fonctionnement des solutions de sécurité en garantissant le maintien en conditions opérationnelles et de sécurité.

Les administrateurs de solutions de sécurité peuvent évoluer vers d’autres fonctions de sécurité opérationnelle comme Analyste SOC, Analyste Réponse à Incidents, Pentesteur, Expert Cyber

Missions

Administration

- S’assurer du fonctionnement optimal des solutions de sécurité dont il a la charge
- Contribuer au paramétrage des solutions de sécurité, gérer les changements
- Configurer les solutions en conformité avec les normes et standards définis par les experts du domaine, effectuer des revues régulières des règles et paramétrages mis en place
- Mettre en place la collecte des logs et des alertes issues des solutions vers un service de détection d’incidents
- Assurer un suivi des actions et une documentation des processus

Maintenance

- Maintenir et faire évoluer les solutions de sécurité de son périmètre, dans un objectif de qualité, de productivité et de sécurité globale
- Assurer le suivi et la remédiation des vulnérabilités identifiées

Exploitation

- Valider l’installation des outils dans l’environnement de production
- Gérer les droits d’accès aux solutions en fonction des profils
- Traiter les incidents ou anomalies ainsi que les exceptions
- Veiller au bon fonctionnement de la remontée des logs et des alertes

Communication

- Contribuer à la sensibilisation et à la formation des utilisateurs aux solutions de sécurité

Compétences

COMPORTEMENTALES

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.

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.

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.

Culture RSE
: Acquérir et/ou développer des connaissances sur la RSE (Responsabilité Sociétale des Entreprises) et connaitre les enjeux et les actions du groupe La Poste en la matière (sujets environnementaux, sociaux, sociétaux, et/ou de gouvernance)

Cyber Sécurité

Politiques de cybersécurité
: Créer, intégrer et appliquer des politiques qui répondent aux objectifs de sécurité de l'organisation. Maitriser le corpus documentaire cybersécurité existant.

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)

Techniques SI

Gestion des incidents et des problèmes
: Identifier et qualifier les incidents et les problèmes. Maîtriser la méthode ITIL / GDI. Gérer la résolution des incidents (Priorisation/arbitrage, mobilisation des moyens et compétences nécessaires, escalade, activation mode dégradé. . .). Réaliser un rapport sur les incidents et les problèmes dans le cadre des processus et contrats définis.

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)

Procédures et outils du système qualité

Définir un Plan d'Assurance Qualité (PAQ)

Méthodes et outils d'intégration de logiciels

Combiner et tester les différents modules ou composants d'un logiciel afin de s'assurer qu'ils fonctionnent correctement ensemble et qu'ils répondent aux exigences spécifiées. Détecter les incompatibilités, les erreurs de communication et les problèmes d'intégration.

Méthodes et principes de mise en production

Connaître les Normes et Standards Informatiques Internes (SNI), les méthodes, principes, contraintes de mise en production et d'exploitation ainsi que les méthodes suivant un processus itératif (méthode agile, devops) ou cycle en V. . .

Famille

Filière

Métier

Répartition des effectifs

- Banque postale
- Groupe - siege

Effectif de la fonction

De 1 à 9