

Fonction

ADMINISTRATEUR SOLUTIONS DE SECURITE 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'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.

Une évolution professionnelle est possible vers les fonctions d'Analyste SOC - Analyste réponse à incidents - Pentesteur - Correspondant Sécurité de Projet - Analyste Menace

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

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

Méthodes et outils d'intégration de logiciels

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 10 à 49