Fonction
ANALYSTE SOC 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’analyste SOC (Security Operation Center) assure la supervision du système d’information de l’organisation afin de détecter des activités suspectes ou malveillantes.

Il identifie, catégorise, analyse et qualifie les évènements de sécurité en temps réel ou de manière asynchrone sur la base de rapports d’analyse sur les menaces.

Il contribue au traitement des incidents de sécurité avérés en support des équipes de réponse aux incidents de sécurité.

L’analyste SOC pourra être amené à développer des compétences en **machine learning** afin de renforcer les capacités de détection.

Une évolution professionnelle est possible vers les fonctions d'Expert Cyber, Analyste Réponse à Incidents, Pentesteur, Administrateur Solution Sécurité, Correspondant Sécurité, Analyste Menace

Missions

Détection

- Identifier les évènements de sécurité en temps réel, les analyser et les qualifier
- Évaluer la gravité des incidents de sécurité
- Notifier les incidents de sécurité, escalader le cas échéant

Réaction

- Transmettre les plans d’action aux entités en charge du traitement et apporter un support concernant les correctifs ou palliatifs à mettre en œuvre
- Faire des recommandations sur les mesures immédiates
- Accompagner le traitement des incidents par les équipes d’investigation

Mise en place des cas d’usages et des outils

- Contribuer à la mise en place du service de détection (SIEM, etc.)
- Contribuer à la définition de la stratégie de collecte des journaux d'évènements
- Participer au développement et au maintien des règles de corrélation d'évènements

Veille et amélioration

- Collaborer à l'amélioration continue des procédures ; construire les procédures pour les nouveaux types d'incidents
- Contribuer à la veille permanente sur les menaces, les vulnérabilités et les méthodes d'attaques afin d'enrichir les règles de corrélation d'évènements

Reporting et documentation

- Renseigner les tableaux de bord rendant compte de l'activité opérationnelle
- Maintenir à jour la documentation
- Activités de recherche de compromissions (threat hunting)

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.

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

Techniques d'attaque et d'intrusion
: Maitriser les techniques employées par les attaquants pour compromettre un Système d'Information (ex : phishing via les réseaux sociaux, exploitation d'une vulnérabilité de l'OWASP), à toutes les étapes de la kill chain (reconnaissance, intrusion, exploitation, augmentation de privilèges, mouvement latéral,

persistance, exfiltration, etc.)

Investigation cyber

Maitriser les techniques et la démarche opérationnelle d'une investigation cyber au service de la détection ou de la réponse à incidents, permettant de mettre en évidence des preuves d'une attaque cyber en cours ou passée (analyse post-mortem, analyse de flux réseaux, analyse de journaux). S'assurer du respect du cadre légal, ainsi que de l'intégrité et la confidentialité des données à chaque investigation

Efficacité professionnelle

Synthèse

Savoir trier, analyser et isoler les informations essentielles des informations accessoires. Consolider des informations pour réaliser une synthèse.

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 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

Gestion des situations de tension organisationnelle ou humaine

Gestion des situations de tension organisationnelle ou humaine

Famille

Filière

Métier

Effectif de la fonction

De 1 à 9