Analyste des opérations de cybersécurité

Remarque : Ce rôle comprend les rôles suivants :

Analyste de niveau I – analyste des opérations de cybersécurité

Analyste de niveau II – spécialiste des logiciels malveillants

Analyste de niveau III – chercheur de la menace : gestion et défense active

Cadre de référence de la NICE	Protection et défense, analyste en cyberdéfense, PR-CDA-001
Description fonctionnelle	Opérateur de centre des opérations de cybersécurité de première ligne chargé de surveiller et d'entretenir les dispositifs de sécurité des TI et souvent responsable de la détection initiale, de la réponse aux incidents et de leur atténuation
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner une défaillance catastrophique des systèmes de TI et de données de l'organisation et des conséquences pour les fonctions organisationnelles qui dépendent de ces systèmes.
Parcours de perfectionnement	Il s'agit d'un emploi de premier échelon commun au sein du centre des opérations de sécurité (COS). Avec une formation et une expérience supplémentaires, il est possible de jouer des rôles plus techniques ou plus opérationnels dans les opérations de cybersécurité (p. ex. l'évaluation et la gestion de vulnérabilité, l'investigation informatique numérique, l'analyse de menace et des logiciels malveillants) ainsi que des possibilités de gestion. Il est à noter que les rôles de niveau II et III peuvent nécessiter une formation et une éducation plus approfondies en plus d'une expérience pertinente. Souvent, un diplôme en informatique ou en génie informatique est une condition préalable étant donné le niveau de connaissances et de compétences requis pour des tâches plus complexes. Toutefois, nombreux sont ceux qui ont progressé de postes d'analystes de la cybersécurité à des rôles avancés dans le domaine de la cybersécurité sans diplôme connexe.
Autres titres	▪ Opérateur du COS ▪ Opérateur de cybersécurité ▪ Analyste de la sécurité des infrastructures ▪ Analyste en sécurité des réseaux ▪ Administrateur de la sécurité des réseaux ▪ Analyste en sécurité des données
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Cibler et analyser les menaces techniques et les vulnérabilités des réseaux ▪ Déterminer, contenir, mener des mesures d'atténuation initiales et signaler les compromissions du système ▪ Examiner, analyser ou appliquer les protocoles de sécurité Internet, les algorithmes cryptographiques, les normes d'annuaire, les protocoles de réseau, le renforcement des réseaux, les contrôles techniques de sécurité des TI, les outils et techniques de sécurité des TI, les systèmes d'exploitation, les systèmes de détection et protection contre les

<table>
<tr><td></td><td colspan="2">intrusions, les pare-feu, les routeurs, les multiplexeurs et les commutateurs, et les dispositifs sans fil
▪ Analyser les données de sécurité et fournir des alertes, des conseils et des rapports
▪ Installer, configurer, intégrer, ajuster, faire fonctionner, surveiller le rendement et détecter les défauts des dispositifs et systèmes de sécurité
▪ Effectuer une analyse d'impact pour les nouvelles implémentations de logiciels, les changements majeurs de configuration et la gestion des correctifs
▪ Développer des modèles de validation et d'essais pour les produits et services de sécurité des TI
▪ Dépanner les produits de sécurité et les incidents
▪ Concevoir/élaborer des protocoles de sécurité des TI
▪ Effectuer des tâches liées à l'autorisation et à l'authentification dans des environnements physiques et logiques
▪ Élaborer des options et des solutions pour atteindre les objectifs du projet liés à la sécurité
▪ Choisir les produits de sécurité et leur configuration pour répondre aux objectifs du projet liés à la sécurité
▪ Mettre en œuvre et à l'essai les spécifications de configuration
▪ Créer des livres de configuration et de construction opérationnelle
▪ Examiner, élaborer et fournir du matériel de formation pertinent</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Diplôme d'études collégiales dans le domaine des technologies de l'information avec une spécialisation en TI/cybersécurité, sécurité des réseaux ou similaire.</td></tr>
<tr><td>Formation</td><td>Formation aux opérations de cybersécurité avec une certification de niveau industriel dans un domaine connexe (par exemple, opérations de sécurité, sécurité des réseaux, détection et atténuation des menaces, exploitation d'appareils de sécurité). Une formation spécialisée est nécessaire pour les analystes de niveau II et III.</td></tr>
<tr><td>Expérience professionnelle</td><td>L'expérience initiale requise est d'avoir réussi à travailler dans un environnement de TI et dans une équipe technique.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Processus et procédures de gestion des incidents
▪ Systèmes de défense, y compris les pare-feu, les logiciels et les systèmes antivirus, les systèmes de détection et de protection contre les intrusions, les scanneurs et les alarmes
▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents</td></tr>
<tr><td>Compétences</td><td colspan="2">Dans les COS plus importants, il peut y avoir la possibilité de passer d'analyste de niveau 1 à analyste de niveau 2. Les analystes de niveau 3 sont rares et presque exclusivement employés dans des contextes de sécurité nationale et militaire. Les compétences requises pour les niveaux 1 et 2 sont indiquées ci-dessous.

Pour l'analyste des opérations de cybersécurité de niveau 1

Les CCH suivantes sont appliquées à un niveau de base :
☐ Administration et gestion de la sécurité des réseaux
☐ Architecture de sécurité des réseaux
☐ Sécurité du matériel et des microprogrammes</td></tr>
</table>

	☐ Sécurité définie par les logiciels et sécurité des applications ☐ Virtualisation et sécurité des réseaux privés virtuels (VPN) ☐ Sécurité basée sur l'infonuagique ☐ Sécurité des appareils sans fil/mobiles ☐ Zones de sécurité des TI ☐ Chiffrement et cryptographie, y compris les concepts et principes de gestion de clés ☐ Analyse et balayage des vulnérabilités ☐ Outils, processus et procédures de gestion de vulnérabilité ☐ Sécurité des applications Web ☐ Livres de configuration et de construction opérationnelle ☐ Acquisitions de systèmes et projets ☐ Responsabilités juridiques et éthiques associées aux opérations de cybersécurité, y compris la conduite des enquêtes, le respect de la vie privée et la préservation des preuves ☐ Rédaction et exposé sur des questions techniques (par exemple, rapports d'incidents, rapports techniques, etc.) pour une compréhension au niveau de la direction Les CCH suivantes sont appliquées à un niveau avancé : ☐ Concepts, opération et configuration des appareils de sécurité des réseaux (équipements spécifiques en fonction du rôle – systèmes ou appareils de cyberdéfense des réseaux, des serveurs et des postes de travail) ☐ Types d'intrusions et indicateurs de compromission ☐ Sources d'information sur la menace ☐ Tactiques, techniques et procédures (TTP) communes aux acteurs de menace ☐ Processus, responsabilités et autorités de gestion des incidents ☐ Méthodes, outils et systèmes de détection et de prévention d'intrusion ☐ Analyse des intrusions et techniques d'atténuation ☐ Analyse de base des logiciels malveillants **Pour l'analyste de niveau II – spécialiste des logiciels malveillants** Les CCH suivantes sont appliquées à un niveau avancé. Tout ce qui précède, en plus de ce qui suit : ☐ Menaces persistantes et sophistiquées aux TTP ☐ Outils, techniques et procédures de cyberdéfense ☐ Développement et essais des dispositifs de sécurité des réseaux (y compris les scripts et le codage). ☐ Analyse avancée des logiciels malveillants et rétroingénierie des logiciels malveillants ☐ Mise en œuvre des contrôles de sécurité avancés en réponse à des menaces persistantes ☐ Activités avancées de réponse aux incidents et de récupération **Pour l'analyste de niveau III – chercheur de la menace : gestion et défense active** Les CCH suivantes sont appliquées à un niveau avancé : ☐ Gestion avancée des menaces

	☐ TTP avancées pour les acteurs de menace, y compris la spécialisation des acteurs de menace persistante (par exemple, l'État-nation, le crime organisé) ☐ Interprétation/synthèse de renseignements classifiés/sensibles sur la menace provenant de sources multiples ☐ Responsabilités juridiques et éthiques liées aux techniques de défense active ☐ Analyse de l'exploitation ☐ Chasse aux menaces et cadres de défense active ☐ Élaboration de plans d'action complexes, y compris l'évaluation des risques et le plan d'atténuation ☐ Tactiques, outils et procédures de défense active, y compris des contre-mesures et des contre-contre-mesures avancées contre la menace ☐ Pensée antagoniste ☐ Développement, essai et déploiement d'outils techniques dans un cadre de défense active pour protéger les renseignements et les systèmes organisationnels à risque
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtualisés ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités par rapport à la détection, à l'intervention et à la reprise en cas d'incident de cybersécurité. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications des politiques « apportez votre équipement personnel de communication » (AVEC). Cela signifie que, quelles que soient les capacités de l'appareil, il faudra évaluer les risques posés pour l'organisation, les mesures d'atténuation pour tenir compte d'une éventuelle compromission par un appareil personnel, et les mesures qui seront requises par le centre des opérations de sécurité (COS) en cas d'incident. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans le COS, y compris la mise en œuvre de changements de personnel et de processus. ▪ L'utilisation accrue des outils automatisés par les acteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires. En conséquence, des stratégies d'atténuation créatives et pertinentes seront nécessaires localement. Cela exigera des capacités de réflexion critique et abstraite bien affinées. ▪ Des mécanismes visant à soutenir le niveau requis de confiance et de risque organisationnel devront être mis en place pour soutenir le suivi et la communication des résultats des outils automatisés. Par conséquent, il faudra mieux comprendre les risques organisationnels posés et les réponses potentielles dans l'environnement dynamique de la menace. ▪ L'émergence et l'utilisation des technologies quantiques par les acteurs de menace vont fondamentalement modifier la sécurité du chiffrement. Cela nécessitera des connaissances et des compétences liées à la mise en œuvre d'une stratégie de sécurité quantique ainsi que les outils, techniques et protocoles des acteurs de menace liés aux attaques de l'informatique quantique et la manière de s'en défendre.