Responsable des incidents de cybersécurité

Responsable en cas d'incident relatif à la TO

Cadre de référence de la NICE	Protection et défense, responsable des incidents de cyberdéfense, PR-CIR-001
Description fonctionnelle	Le titulaire fournit des activités de réponse immédiate et détaillée pour atténuer ou limiter les menaces et les incidents liés à la cybersécurité non autorisés au sein d'une organisation. Cela comprend la planification et l'élaboration de plans d'action, la hiérarchisation des activités et le soutien aux opérations de reprise et à l'analyse post-incident.
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, comme 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.
Autres titres	▪ Responsable des incidents de cybersécurité ▪ Responsable d'incidents – centre des opérations de sécurité ▪ Premier intervenant en matière de cybersécurité ▪ Responsable en cas d'incident de sécurité relatif à la technologie opérationnelle
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	Ces tâches s'appliquent aussi bien aux systèmes de TI qu'aux systèmes de TO. ▪ Effectuer des tâches de traitement des incidents de cyberdéfense en temps réel (par exemple, collecte de preuves, corrélation et suivi des intrusions, analyse de la menace et remédiation directe du système) ▪ Effectuer un triage de sécurité pour cibler et analyser les incidents et menaces cybernétiques ▪ Surveiller activement les réseaux et les systèmes pour détecter les incidents et menaces cybernétiques ▪ Procéder à une analyse des risques et à un examen de sécurité des journaux du système afin de repérer les éventuelles cybermenaces ▪ Procéder à des analyses et à des examens ou appliquer des scanneurs de réseau, des outils d'évaluation de vulnérabilité, des protocoles de réseau, des protocoles de sécurité Internet, des systèmes de détection d'intrusion, des pare-feu, des contrôleurs de contenu et des logiciels de point d'extrémité ▪ Collecter et analyser les données pour déterminer les failles et les vulnérabilités de la cybersécurité et formuler des recommandations permettant d'y remédier rapidement ▪ Élaborer et préparer l'analyse et le rapport des incidents de cyberdéfense ▪ Définir et maintenir des ensembles d'outils et des procédures

<table>
<tr><td></td><td colspan="2">▪ Élaborer, mettre en œuvre et évaluer les plans et activités de prévention et de réponse aux incidents, et s'adapter pour contenir, atténuer ou éradiquer les effets des incidents de cybersécurité
▪ Fournir un soutien à l'analyse des incidents dans le cadre des plans et activités de réponse
▪ Mener des activités de recherche et de développement sur les incidents de cybersécurité et les mesures d'atténuation
▪ Créer un plan de développement du programme qui comprend des évaluations des lacunes en matière de sécurité, des politiques, des procédures, des stratégies et des manuels de formation
▪ 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).

Formation spécialisée requise pour la technologie opérationnelle et les systèmes connexes.</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">Responsable des incidents de cybersécurité
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
☐ Sécurité définie par les logiciels et sécurité des applications
☐ Virtualisation et sécurité des 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</td></tr>
</table>

	☐ Rédaction et exposé sur des questions techniques (par exemple, rapports d'incidents, rapports techniques, etc.) pour une compréhension au niveau de la direction ☐ Bases de la continuité des activités et de la réponse aux catastrophes 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 ☐ Enquêtes de cybersécurité et préservation des preuves **Pour les responsables en cas d'incident relatif à la technologie opérationnelle** En plus des CCH pertinentes ci-dessus, les éléments suivants s'appliquent au niveau de base : ☐ Logiciels et matériel des systèmes de TO, contrôleurs logiques programmables, relais numériques et analogiques ☐ Évaluation de la menace et des risques liés à la TO connectée à Internet (y compris les implications et l'évaluation des dispositifs IdO) ☐ Exigences juridiques et de conformité, y compris les responsabilités organisationnelles en matière de sécurité du lieu de travail et du public liées à la TO/production ☐ Systèmes de télémétrie, communication de données, acquisition de données et contrôle de processus ☐ Concepts de systèmes d'exploitation, de réseaux et de systèmes de communication ☐ Réseaux de distribution électrique, équipement du système électrique, fonctionnement des stations de transformation et théorie de l'électricité ☐ Applications et systèmes de gestion de bases de données ☐ Mesures ou indicateurs du rendement, de la disponibilité, de la capacité ou des problèmes de configuration du système de TO ☐ Outils d'analyse et protocoles de réseau ☐ Outils de diagnostic et techniques d'identification des défauts
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.