Gestionnaire de la sécurité des systèmes d'information – opérations de cybersécurité

Cadre de référence de la NICE	Supervision et gouvernance, OV-MGT-001, gestionnaire de la sécurité des systèmes d'information
Description fonctionnelle	Le titulaire planifie, organise, dirige, contrôle et évalue les activités du centre des opérations de cybersécurité au sein d'une organisation. Employé dans les secteurs public et privé.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes 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	Le titulaire suit généralement une période de 5 à 10 ans dans des rôles connexes dans les opérations de TI ou de cybersécurité ou dans un emploi similaire. Ce rôle soutient l'augmentation des responsabilités au niveau de la gestion en fonction d'une base technique solide dans les opérations de cybersécurité ou d'un rôle de travail connexe (par exemple, évaluation et gestion de vulnérabilité, investigation informatique numérique, analyse de la cybersécurité).
Autres titres	▪ Gestionnaire des opérations de cybersécurité (GOC) ▪ Gestionnaire des opérations de sécurité (COS) ▪ Gestionnaire de la cybersécurité ▪ Gestionnaire de la sécurité des systèmes d'information (opérations de cybersécurité)
CNP connexes	0213 – Gestionnaires des systèmes informatiques
Tâches	▪ Diriger et gérer le personnel du COS, y compris l'embauche, la formation, le perfectionnement, la gestion du rendement et la réalisation d'examens annuels du rendement ▪ Demeurer à l'affût de la situation de la menace à la cybersécurité et des technologies de sécurité ▪ Élaborer et mettre en œuvre un programme de COS intégré qui répond aux exigences législatives et organisationnelles ▪ Élaborer et publier des mécanismes de gouvernance du COS (politiques, procédures et orientations) ▪ Élaborer et mettre en œuvre un programme de mesure et d'assurance qualité ▪ Surveiller l'efficacité du programme de COS et en rendre compte à la direction générale ▪ Surveiller et gérer les relations avec les fournisseurs de services et de technologies de sécurité ▪ Fournir des évaluations stratégiques sur le contexte des menaces, les tendances technologiques du COS et les technologies de sécurité émergentes ▪ Rechercher et interpréter les renseignements sur la menace en fonction des risques organisationnels ▪ Gérer les événements et incidents de cybersécurité au sein du COS ▪ Fournir des rapports, des exposés et des recommandations fondés sur les risques concernant les événements et incidents de cybersécurité courants et non courants, y compris la réponse aux crises organisationnelles (par exemple, les interruptions des systèmes d'entreprise)

<table>
<tr><td></td><td colspan="2">▪ Diriger et faciliter les leçons apprises, les activités rétrospectives et les meilleures pratiques concernant les événements et incidents liés à la cybersécurité
▪ Élaborer et superviser la mise en œuvre de plans d'action visant à soutenir l'amélioration continue de la position en matière de cybersécurité</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Baccalauréat en informatique ou dans une discipline connexe ou diplôme d'études collégiales dans le domaine des technologies de l'information.</td></tr>
<tr><td>Formation</td><td>Formation aux opérations de cybersécurité avec une certification de niveau industriel dans un domaine connexe (par exemple, sécurité des réseaux, traitement des incidents, détection et atténuation des menaces, investigation informatique numérique).
Formation à la gestion des équipes d'opérations de sécurité, ou perfectionnement et expérience équivalents.
Formation sur les outils et les technologies pertinents pour l'organisation qui soutiennent les opérations de cybersécurité.</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience significative (5 à 10 ans) dans le domaine des TI avec 3 à 5 ans d'expérience dans des opérations ou domaine connexe de la cybersécurité.</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
▪ Logiciels et systèmes d'authentification
▪ Processus de gestion de vulnérabilité et systèmes d'évaluation de vulnérabilité, y compris les essais de pénétration s'ils sont utilisés
▪ Services de sécurité fournis, le cas échéant</td></tr>
<tr><td>Compétences</td><td colspan="2">Cette profession repose sur les compétences démontrées pour un gestionnaire d'activité ainsi que pour le gestionnaire de la sécurité des systèmes d'information dans le cadre de la NICE. Plus précisément, ce travail exige ce qui suit :

Niveau d'application de base des CCH suivantes :
☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles

Niveau avancé d'application des CCH suivantes :
☐ Menaces et vulnérabilités organisationnelles, y compris :
o Situation de la menace à la cybersécurité et adaptation des processus du COS pour répondre à l'évolution de la menace
o Exigences en matière de gestion de vulnérabilité et gamme des mesures d'atténuation potentielles disponibles lorsqu'il n'existe pas de protocole de gestion de vulnérabilité
☐ Gestion des systèmes défensifs, y compris :
o Pare-feu, antivirus, systèmes de détection et de protection contre les intrusions
o Paramètres manuels et automatisés requis
o Exigences en matière de surveillance, d'essais et de maintenance
☐ Création, mise en œuvre et gestion :</td></tr>
</table>

	○ Processus et politiques de gestion des incidents ○ Responsabilités en matière de gestion des incidents ○ Pratiques de suivi et de signalement des incidents conformément aux exigences législatives et aux politiques organisationnelles ○ Analyses et rapports post-incident ○ Leçons organisationnelles tirées à l'appui de l'amélioration continue ☐ Gestion des fournisseurs (si les services de TI ou de sécurité sont externalisés) : ○ Rôles et responsabilités des contrôles de sécurité des services fournis ○ Rôles et responsabilités du fournisseur dans la gestion et le signalement des incidents ○ Exigences en matière de suivi, d'évaluation et de signalement des incidents pendant le cycle de vie du contrat ○ Responsabilités organisationnelles en réponse à une compromission/un manquement de la part du fournisseur ○ Gestion des communications et des relations avec les fournisseurs en cas de crise ☐ Offre de conseils sur les exigences, les politiques, les plans et les activités de sécurité ☐ Rédaction et fourniture des exposés et des rapports à différents niveaux d'auditoire (utilisateurs, gestionnaires, cadres) ☐ Maintien d'une plus grande conscience de la situation en matière de sécurité ☐ Conscience de soi concernant les connaissances, les compétences et les habiletés requises pour répondre aux changements commerciaux, techniques et aux menaces ☐ Apprentissage continu pour soutenir l'actualisation des connaissances sur les menaces émergentes, les innovations technologiques en matière de sécurité et l'évolution du paysage de la cybersécurité
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 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. Il sera nécessaire de comprendre les capacités de menace quantique et les connaissances et compétences liées à la mise en œuvre d'une stratégie de sécurité quantique.