

Technicien des opérations de cybersécurité

Cadre de référence de la NICE	Protection et défense, PR-INF-001, soutien aux infrastructures de défense en matière de cybersécurité	
Description fonctionnelle	Le titulaire met à l'essai, met en œuvre, déploie, entretient et administre le matériel et les logiciels de l'infrastructure des opérations de sécurité.	
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 de sécurité ou une compromission du système qui peut avoir un impact important sur les systèmes, les capacités ou les fonctions informatiques de l'organisation.	
Parcours de perfectionnement	Il s'agit souvent d'un emploi de premier échelon dans le domaine de la sécurité après avoir acquis de l'expérience dans des fonctions techniques, administratives de réseau ou autres fonctions similaires. Avec une formation et une expérience supplémentaires, il existe un potentiel pour des rôles plus techniques ou plus opérationnels ainsi que des possibilités de gestion.	
Autres titres	▪ Spécialiste/technicien du soutien aux infrastructures de sécurité ▪ Analyste des systèmes de sécurité ▪ Technicien en systèmes de sécurité ▪ Analyste du contrôle de la sécurité	
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2281 – Techniciens/techniciennes de réseau informatique 2282 – Agents/agentes de soutien aux utilisateurs	
Tâches	▪ Surveiller activement le rendement du système de sécurité, dépanner et résoudre les problèmes d'interopérabilité matérielle ou logicielle, ainsi que les pannes et les défauts du système ▪ Installer, configurer et entretenir les logiciels, le matériel et les équipements périphériques du système de sécurité ▪ Élaborer, rédiger et tenir à jour des rapports d'incidents et des évaluations de vulnérabilité et d'impact ▪ Développer et maintenir une base de données de suivi et de solutions ▪ Analyser et recommander des améliorations et des changements pour soutenir l'amélioration des opérations de sécurité ▪ Auditer, enregistrer et signaler des activités de gestion du cycle de vie ▪ Administrer les comptes, les privilèges et l'accès aux systèmes et équipements de sécurité ▪ Effectuer la gestion des actifs ou le contrôle de l'inventaire des ressources des systèmes et des équipements ▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs	
Qualifications requises	Éducation	Études postsecondaires (diplôme en informatique ou dans un domaine des TI connexe)
	Formation	Formation aux systèmes de cybersécurité, au fonctionnement des systèmes de sécurité et aux outils basés sur les fournisseurs (par exemple, systèmes de détection des intrusions, pare-feu, antivirus, gestion des incidents, etc.)

	Expérience professionnelle	2 à 3 ans dans l'exploitation et la sécurité des réseaux
Outils et technologie	▪ Outils, journaux et procédures des systèmes de cybersécurité ▪ Politiques et directives organisationnelles ▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents	
Compétences	Les CCH s'appliquent au niveau de base : ☐ Menaces pour les systèmes d'information et leur sécurité ☐ Concepts, protocoles, composants et principes de l'architecture de sécurité des réseaux (par exemple, application de la défense en profondeur) ☐ Techniques de base de renforcement des systèmes, des réseaux et des systèmes d'exploitation ☐ Enregistrements et modes de transmission (par exemple, Bluetooth, identification par radiofréquence [RFID], réseau infrarouge [RI], technologie Wi-Fi, radiomessagerie, cellulaire, antennes paraboliques, voix par IP [VoIP]) ☐ Analyse du trafic du réseau (outils, méthodologies, processus) ☐ Architectures et normes de gestion de l'identité, des justificatifs d'identité et de l'accès ☐ Politique, procédures et pratiques de gestion des incidents de cybersécurité ☐ Analyse organisationnelle des tendances des utilisateurs et des affaires ☐ Consultation des clients et résolution des problèmes Les CCH sont appliquées à un niveau avancé : ☐ Procédures, principes et méthodologies d'essai des systèmes de cybersécurité ☐ Outils et applications du système de détection d'intrusion (SDI)/système de prévention d'intrusion (SPI) ☐ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ☐ Dépannage, analyse et réparation des infrastructures de cybersécurité ☐ Politiques, gestion des comptes et contrôles des systèmes de 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 dans la gestion des systèmes 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 les processus de gestion de l'identité et de l'accès, y compris les changements techniques et de processus connexes.	

	▪ 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.
--	---