Spécialiste du chiffrement/soutien à la gestion des clés

Cadre de référence de la NICE	Aucun.	
Description fonctionnelle	Le titulaire fournit un soutien continu à la gestion et à la maintenance des réseaux privés virtuels, du chiffrement, de l'infrastructure à clés publiques et, dans certains cas, de la sécurité des communications (SECOM) pour soutenir la sécurité organisationnelle des TI.	
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 compromission du système qui, selon le type, 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 la gestion de l'accès et des justificatifs d'identité pour l'administration du réseau ou du système. 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	▪ Analyste en gestion d'accès ▪ Analyste de système ▪ Spécialiste de la gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA)	
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2281 – Techniciens/techniciennes de réseau informatique 2282 – Agents/agentes de soutien aux utilisateurs	
Tâches	▪ Déterminer les besoins des clients et proposer des solutions techniques ▪ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ▪ Développer et appliquer des contrôles d'accès aux systèmes de sécurité ▪ Déployer, configurer et gérer les services de chiffrement/gestion de clés ▪ Mettre en place des VPN ▪ Analyser des modèles ou des tendances pour mieux les résoudre ▪ Gérer les processus d'approbation des demandes de changement d'identité ▪ Auditer, enregistrer et signaler les étapes de gestion du cycle de vie des utilisateurs par rapport à la liste de contrôle d'accès sur les plateformes gérées ▪ Configurer et gérer l'identité, les justificatifs d'identité et l'accès fédérés en conformité avec la politique, les normes et les procédures de sécurité ▪ Effectuer des tâches liées à l'autorisation et à l'authentification dans des environnements physiques et logiques ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés au rôle	
Qualifications requises	Éducation	Diplôme d'études collégiales dans le domaine des technologies de l'information.

	Formation	Formation aux technologies de chiffrement et de gestion des clés pertinentes au niveau appliqué.
	Expérience professionnelle	Expérience dans la gestion de services d'annuaire et travail dans un environnement de sécurité.
Outils et technologie	▪ Systèmes de gestion de l'identité et de l'accès ▪ Outils, processus et procédures de chiffrement et de gestion des clés ▪ Outils et procédures de chiffrement par VPN et Wi-Fi ▪ Outils et services d'authentification ▪ 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 : ☐ Cryptanalyse ☐ Concepts et méthodes de cryptographie et de chiffrement ☐ Cryptographie symétrique et asymétrique ☐ Stéganographie et stéganalyse ☐ Autorités cryptologiques nationales (Centre de la sécurité des télécommunications) ☐ Fournisseurs d'infrastructures à clés publiques Les CCH sont appliquées au niveau avancé : ☐ Politiques de sécurité des utilisateurs des technologies de la technologie de l'information (TI) de l'organisation (par exemple, création de compte, règles relatives aux mots de passe, contrôle d'accès) ☐ Protocoles, outils et procédures d'accès au réseau, de gestion de l'identité et de l'accès ☐ Normes nationales et internationales ☐ Méthodes d'authentification, d'autorisation et de contrôle d'accès ☐ ICP (infrastructure à clés publiques), MSM (module de sécurité matérielle), certificat numérique, protocole SSL/TLS (sécurité de la couche transport), protocole SSH, technologies de chiffrement actuelles ☐ Processus liés au cycle de vie des applications ☐ Signatures numériques, certificats numériques et gestion des certificats numériques ☐ Protocoles d'authentification ☐ VPN et protocoles ☐ Chiffrement des fichiers et des disques ☐ Algorithmes de chiffrement ☐ Analyse organisationnelle des tendances des utilisateurs et des affaires ☐ Consultation des clients et résolution des problèmes	
Tendances futures ayant une incidence sur les compétences clés	▪ La dépendance accrue sur les services virtuels ou « basés sur l'infonuagique » exigera une connaissance des responsabilités du fournisseur de services, notamment de ses responsabilités en matière de cybersécurité par rapport aux risques organisationnels en matière de cybersécurité, en particulier en ce qui concerne les exigences de chiffrement des données. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment les outils cryptographiques sont touchés et automatisés pour répondre aux besoins organisationnels.	

	▪ L'utilisation accrue des outils automatisés par les acteurs de menace pose des problèmes aux organisations qui ne disposent pas d'outils défensifs complémentaires pour assurer la robustesse des systèmes cryptographiques, des chiffres et des algorithmes. S'il existe des disparités connues entre la menace et la capacité de défense, des mesures d'atténuation doivent être définies et mises en œuvre. ▪ 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 comprendre les risques organisationnels posés, les mesures de sécurité et les politiques, processus ou procédures à mettre en place. ▪ 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 au sein de l'organisation. Cela comprend la connaissance et la compétence des algorithmes de sécurité quantique utilisés, l'intégration et la mise en œuvre de technologies de sécurité quantique au sein de l'organisation et les protocoles d'essai et d'évaluation du matériel, des logiciels et des protocoles de sécurité quantique et de résistance quantique.