Spécialiste de la gestion de l’identité et du soutien à l’authentification

Rôle du cadre de la NICE	Aucun.
Description fonctionnelle	Le titulaire fournit un soutien continu à la gestion de l’identité, des justificatifs d’identité, de l’accès et de l’authentification afin de 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 ▪ Modéliser et associer les utilisateurs aux ressources (par exemple, en fonction de leur rôle) ▪ Installer, configurer, exploiter, maintenir et surveiller les applications connexes ▪ Déployer, configurer et gérer l’approvisionnement des utilisateurs, y compris la synchronisation de l’identité, l’approvisionnement automatique et la désactivation automatique de l’accès, le flux de travail d’approbation des demandes de sécurité en libre-service et les rapports consolidés ▪ Configurer et gérer les solutions de gestion des accès de l’entreprise sur le Web (authentification unique, gestion des mots de passe, authentification et autorisation, administration déléguée) ▪ Analyser les schémas ou les tendances des incidents en vue d’une résolution ultérieure ▪ 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

<table>
<tr><td></td><td colspan="2">▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés au rôle</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.</td></tr>
<tr><td>Formation</td><td>Formation sur les politiques, protocoles, outils et procédures d’identité, de justificatifs d’identité, de gestion de l’accès et d’authentification pertinents.
Développement et application d’un système de gestion des éléments d’identification de l’utilisateur.</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience dans la gestion de services d’annuaire et travail dans un environnement de sécurité.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Systèmes de gestion de l’identité et de l’accès
▪ Services d’annuaire
▪ Outils et services d’authentification
▪ 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">Les CCH s’appliquent au niveau de base :
☐ Architectures et normes de gestion de l’identité, des justificatifs d’identité et de l’accès
☐ Processus liés au cycle de vie des applications
☐ Mise en correspondance et modélisation des justificatifs d’identité
☐ Contrôles d’accès basés sur des politiques et adaptés aux risques
☐ Développement et application d’un système de gestion des éléments d’identification de l’utilisateur
☐ Analyse organisationnelle des tendances des utilisateurs et des affaires
☐ Consultation des clients et résolution des problèmes

Les CCH sont appliquées à un niveau avancé :
☐ Protocoles, outils et procédures d’accès au réseau, de gestion de l’identité et de l’accès
☐ Méthodes d’authentification, d’autorisation et de contrôle d’accès
☐ Installer, configurer, exploiter, maintenir et surveiller les applications connexes
☐ Développement et application des contrôles d’accès aux systèmes de sécurité
☐ Gestion des services d’annuaire
☐ 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)</td></tr>
<tr><td>Tendances futures ayant une incidence sur les compétences clés</td><td colspan="2">▪ 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.</td></tr>
</table>

	▪ 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 qu’une compréhension approfondie des implications pour les protocoles d’authentification et de la manière de se défendre contre les menaces potentielles de l’informatique quantique.