Ingénieur/analyste en automatisation de la sécurité

REMARQUE : *Il s'agit d'un rôle de travail émergent. Il existe des échantillons limités de ce rôle de travail et les tâches et activités des experts en la matière varient en fonction des exigences organisationnelles. En conséquence, les renseignements ci-dessous se fondent sur des représentations actuelles basées sur les exigences de la demande et sur une compréhension de l'intelligence artificielle, de l'apprentissage machine et des exigences de la science des données pour soutenir l'ingénierie et l'analyse des processus automatisés*. *On s'attend à ce que le rôle évolue considérablement au cours des prochaines années.*

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Compte tenu des références, de la documentation sur la sécurité organisationnelle, des orientations en matière de sécurité des TI et des outils et ressources nécessaires, le titulaire recherche et définit les besoins opérationnels en matière de sécurité, détermine les besoins et conçoit des solutions automatisées qui soutiennent la sécurité organisationnelle.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou l'absence de prise en compte des exigences organisationnelles, des besoins opérationnels et des menaces peuvent entraîner une mauvaise conception des systèmes ou une mauvaise intégration des systèmes/dispositifs qui créent des vulnérabilités exploitables pouvant avoir des conséquences importantes sur les objectifs organisationnels, y compris le risque de défaillance catastrophique des systèmes.
Parcours de perfectionnement	Le titulaire du rôle a généralement suivi une éducation formelle et possède une expérience de 5 à 10 ans dans des fonctions connexes d'ingénierie des TI, de conception de systèmes ou d'intégration de systèmes. Formation supplémentaire, études ou expérience en automatisation des processus et activités connexes d'intelligence artificielle/d'ingénierie de l'apprentissage machine.
Autres titres	▪ Ingénieur automaticien de système ▪ Concepteur de systèmes automatisés ▪ Ingénieur en automatisation et contrôles de sécurité
CNP connexes	2133 – Ingénieurs électriciens et électroniciens/ingénieures électriciennes et électroniciennes 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel 2241 – Technologues et techniciens/techniciennes en génie électronique et électrique
Tâches	▪ Rechercher, développer, intégrer, mettre à l'essai et mettre en œuvre des solutions d'automatisation de la sécurité pour les nuages ou les systèmes ▪ Déterminer l'étendue et planifier les travaux d'automatisation afin de respecter les délais ▪ Gérer/surveiller les activités automatisées de solution de sécurité, y compris les correctifs, les mises à jour et les processus connexes ▪ Élaborer et tenir à jour des outils et des processus pour soutenir les activités d'automatisation de la sécurité ▪ Examiner et mettre à l'essai les scripts d'automatisation de la sécurité avant la mise en œuvre ▪ Dépanner tout problème survenant au cours des essais, de la production ou de l'utilisation

	▪ Créer, utiliser et maintenir une documentation de référence ▪ Déterminer, acquérir et superviser la gestion des ressources financières, techniques et humaines nécessaires pour soutenir les activités d'automatisation de la sécurité ▪ Examiner, approuver et superviser les modifications des politiques et contrôles en matière de cybersécurité et leurs implications pour les activités automatisées ▪ Programmer et superviser les évaluations et les audits de sécurité ▪ Superviser et gérer les relations avec les fournisseurs de produits et services de sécurité des TI acquis ▪ Veiller à ce que les exigences de sécurité soient déterminées pour tous les systèmes de TI tout au long de leur cycle de vie ▪ Superviser ou gérer les mesures préventives ou correctives lorsqu'un incident ou une vulnérabilité en matière de cybersécurité est découvert ▪ Évaluer les menaces et élaborer des contre-mesures et des stratégies d'atténuation des risques contre les vulnérabilités des systèmes automatisés ▪ Effectuer une analyse des risques et faire des essais chaque fois qu'un système automatisé subit un changement ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés au rôle	
Qualifications requises	Éducation	Diplôme pertinent d'ingénieur ou d'informatique avec une formation de troisième cycle ou équivalente en automatisation des systèmes, apprentissage artificiel ou apprentissage machine.
	Formation	Formation pertinente en matière de cybersécurité pour soutenir les fonctions d'ingénieur en sécurité.
	Expérience professionnelle	Expérience modérée (3 à 5 ans) dans le domaine de la sécurité et de la conception, de l'intégration, des essais et du soutien des systèmes associés. Expérience en programmation et en essai d'applications. 2 à 3 ans d'expérience pratique dans l'automatisation des processus du système.
Outils et technologie	▪ Outils et méthodologies d'évaluation de la menace et des risques ▪ Systèmes de protection et de défense, y compris les pare-feu, les logiciels et 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 ▪ Outils et techniques d'essai et d'évaluation de la sécurité ▪ Outils, techniques et procédures d'automatisation des processus ▪ Langages de programmation applicables	
Compétences	Niveau d'application avancé des CCH suivantes : ☐ Automatisation des processus dans un cadre de sécurité ☐ API, automatisation et langages de script ☐ Fonctions SDN, NFV et VNF ☐ Modèles d'ingénierie de la sécurité	

	☐ Définition et communication des approches de sécurité qui soutiennent les exigences organisationnelles ☐ Normes de sécurité internationales et conformité ☐ Concepts d'architecture de la sécurité et modèles de référence pour l'architecture d'entreprise ☐ Sécurité des systèmes pendant l'intégration et la configuration ☐ Processus d'évaluation de la sécurité et d'autorisation ☐ Méthodes et processus d'essais et d'évaluation de la sécurité ☐ Sécurité tout au long du cycle de vie de développement du système/logiciel ☐ Méthodes et applications d'évaluation de vulnérabilité et d'essais de pénétration ☐ Méthodes d'essais et d'évaluation des systèmes et des logiciels ☐ Conception de la sécurité basée sur les preuves ☐ Création et essai des modèles de menace ☐ Gestion de projet et évaluation de la sécurité tout au long du cycle de vie du projet ☐ Processus d'achat et évaluations de l'intégrité de la chaîne d'approvisionnement ☐ 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)
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. ▪ Si le rôle est exercé au sein de l'organisation, il sera nécessaire de comprendre pleinement les implications en matière de sécurité de l'option « apportez votre équipement personnel de communication » (AVEC) et de la gestion des risques associés. ▪ Si des outils de sécurité automatisés sont utilisés, il faudra définir les exigences en matière d'essai, d'intégration et de contrôle et conseiller/former les responsables de ces activités sur les changements de processus et de procédures qui en résulteront. En outre, en tant que responsable technique potentiel de l'automatisation de la sécurité, il peut être nécessaire de former les responsables des organisations aux avantages et aux risques de l'automatisation et à la gestion des changements nécessaires. ▪ 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 nécessitera une bien meilleure appréciation des capacités des acteurs de menace et des contre-mesures potentielles. ▪ 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. Cela nécessitera des connaissances et des compétences liées à la mise en œuvre d’une stratégie de sécurité quantique et la compréhension des implications sur les mécanismes de sécurité basés sur l’IA.