Spécialiste d’essai et d’évaluation de sécurité

Cadre de référence de la NICE	Fourniture sécurisée, essais et évaluation de la sécurité, SP-TST-001	
Description fonctionnelle	Le titulaire planifie, prépare et exécute des essais de dispositifs de sécurité, de systèmes d’exploitation, de logiciels et de matériel afin d’évaluer les résultats par rapport à des spécifications, des politiques et des exigences définies, et documente les résultats et fait des recommandations qui peuvent améliorer la confidentialité, l’intégrité et la disponibilité des renseignements.	
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou un mauvais jugement peuvent entraîner l’intégration et le déploiement de systèmes, de logiciels ou de services de TI présentant des vulnérabilités qui augmentent l’exposition aux menaces et le risque organisationnel. Les compromissions qui en résulteraient pourraient avoir une incidence importante sur l’entreprise.	
Parcours de perfectionnement	Le titulaire du rôle a généralement suivi une éducation formelle et possède une expérience de 5 à 10 ans dans le domaine de la sécurité des TI. Ce rôle nécessite souvent une formation spécialisée, des études ou une expérience en lien avec les essais et les mesures des systèmes.	
Autres titres	Évaluateur de la sécurité des systèmes	
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel)	
Tâches	▪ Mettre à l’essai, évaluer et vérifier les systèmes en cours de développement, les systèmes échangeant des renseignements électroniques avec d’autres systèmes, les logiciels et le matériel des systèmes d’exploitation associés, ainsi que les contrôles, et les dispositifs de sécurité utilisés au sein d’une organisation pour déterminer le niveau de conformité aux spécifications, aux politiques et aux exigences définies ▪ Analyser les résultats des essais des systèmes d’exploitation, des logiciels et du matériel et formuler des recommandations sur la base des résultats ▪ Élaborer des plans d’essai pour répondre aux spécifications, aux politiques et aux exigences ▪ Valider les spécifications, les politiques et les exigences en matière de testabilité ▪ Créer des preuves vérifiables des mesures de sécurité ▪ Préparer des évaluations qui documentent les résultats des essais et les éventuelles vulnérabilités en matière de sécurité ▪ Déployer, valider et vérifier le fonctionnement des dispositifs d’infrastructure de réseau ▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs ▪ Former et encadrer les membres de l’équipe de sécurité	
Qualifications requises	Éducation	Baccalauréat en informatique ou dans une discipline connexe ou formation et expérience équivalentes
	Formation	Formation à la mesure, à l’évaluation et aux essais de la sécurité des systèmes.

	Expérience professionnelle	Expérience importante (5-10 ans) dans le domaine des TI, avec une expérience de 3 à 5 ans dans un rôle de sécurité des systèmes à l'appui des évaluations de la sécurité et des audits des TI est préférable. Expérience de travail dans des environnements d'essais sécurisés.
Outils et technologie	▪ Plans stratégiques et d'affaires ▪ Évaluation de la menace et des risques ▪ Processus de gestion de vulnérabilité et évaluations de vulnérabilité ▪ Processus et procédures de gestion des incidents ▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Architecture de système ▪ Processus et politiques de gestion des risques en matière de cybersécurité ▪ Législation sur la protection de la vie privée et la sécurité ▪ Infrastructure de sécurité organisationnelle et systèmes de compte rendu ▪ Outils, techniques, procédures et protocoles des politiques d'essais et d'évaluation des systèmes ▪ Législation et exigences de conformité	
Compétences	Application de base des CCH suivantes : ☐ Processus d'achat en matière de sécurité et évaluations de l'intégrité de la chaîne d'approvisionnement ☐ Processus d'ingénierie des systèmes Application avancée des CCH suivantes : ☐ Processus d'évaluation de la sécurité et d'autorisation ☐ Stratégies d'essai et d'évaluation des systèmes de TI ☐ Infrastructure et ressources d'essai et d'évaluation des systèmes de TI ☐ Outils, procédures et pratiques d'essai et d'évaluation des systèmes de sécurité des TI ☐ Connaissance technique des réseaux, des composants informatiques, de la technologie d'alimentation électrique, des protocoles de système, des logiciels de cybersécurité ☐ Architecture et modèles de sécurité des réseaux ☐ Réalisation d'essais de sécurité indépendants de validation et de vérification ☐ Méthodes et techniques d'essai et d'évaluation des systèmes ☐ Conception d'essais, élaboration de scénarios et examen de l'état de préparation ☐ Essai d'intégration des systèmes ☐ Processus d'évaluation de la sécurité et d'autorisation ☐ Concepts d'architecture de sécurité et modèle d'architecture de sécurité des renseignements d'entreprise ☐ Détermination des politiques et exigences en matière d'essai et d'évaluation ☐ Collecte, analyse, vérification et validation des données d'essais et traduction des données et des résultats des essais en conclusion ☐ Conception et documentation des stratégies d'essai et d'évaluation ☐ Rédaction des rapports techniques et rapports d'essai et d'évaluation.	

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 ses responsabilités en matière de cybersécurité par rapport aux systèmes organisationnels, la manière dont ces systèmes sont intégrés et la manière dont ils peuvent être testés et évalués. ▪ 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 aux systèmes organisationnels. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment les outils seront intégrés dans l'infrastructure de sécurité organisationnelle et les implications sur les pratiques d'essais et d'évaluation. ▪ L'utilisation accrue des outils automatisés par les acteurs de menace pose des défis qui nécessiteront une évaluation continue des pratiques d'essai et d'évaluation et des outils requis. ▪ 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, ainsi que leurs implications sur les essais et l'évaluation de la sécurité. ▪ 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 permettant de mettre à l'essai et d'évaluer le chiffrement et le degré de résistance quantique.