Évaluateur de logiciels sécurisés

Cadre de référence de la NICE	Dispositions relatives à la sécurité, SP Dev-001, Évaluateur de logiciels sécurisés
Description fonctionnelle	En fonction des références, de la documentation sur la sécurité organisationnelle, des orientations en matière de cybersécurité et des outils et ressources nécessaires, le titulaire analyse la sécurité des applications informatiques, des logiciels ou des programmes utilitaires spécialisés, nouveaux ou existants, et fournit des résultats exploitables.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes peuvent entraîner des vulnérabilités dans les logiciels et les outils sur le Web peuvent mettre en danger les systèmes et services organisationnels.
Parcours de perfectionnement	Le titulaire du rôle a généralement suivi une éducation formelle et possède une expérience de 5 à 10 ans d'expérience dans le domaine du développement de logiciels. Ce rôle nécessite souvent une formation spécialisée, des études ou une expérience correspondant aux logiciels sécurisés et aux activités d'évaluation de vulnérabilité pour la sécurité des logiciels/applications.
Autres titres	▪ Développeur/programmeur de logiciels sécurisés ▪ Spécialistes d'essai et d'évaluation de logiciels ▪ Analyste/évaluateur de vulnérabilité
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel 2174 – Programmeurs/programmeuses et développeurs/développeuses en médias interactifs
Tâches	▪ Définir/valider les besoins opérationnels en matière de sécurité et les exigences de sécurité ▪ Examiner et analyser les architectures et les documents de conception de la sécurité des TI, ainsi que les systèmes, protocoles, services, contrôles, appareils, applications, chiffrements et algorithmes de chiffrement connexes, en fonction des exigences de sécurité et des normes de l'industrie ▪ Rechercher, analyser et mettre en œuvre des processus et des techniques de développement d'applications sécurisées ▪ Analyser les données de sécurité et fournir des conseils et des rapports ▪ Élaborer et mener des procédures d'essais et de validation de systèmes ou d'applications logicielles, de programmation et de codage sécurisé, et faire rapport sur les fonctionnalités et la résilience ▪ Créer et examiner les cas d'utilisation du système ▪ Effectuer des balayages et des examens de vulnérabilité des systèmes ou des applications logicielles, et examiner les contrôles et les mesures nécessaires pour protéger les systèmes ou les applications logicielles ▪ Préparer des rapports sur les systèmes logiciels, le développement et les applications, les correctifs ou les versions qui laisseraient les systèmes vulnérables ▪ Développer des contre-mesures contre les exploitations potentielles des vulnérabilités des systèmes ▪ Effectuer une analyse des risques chaque fois qu'une application ou un système subit un changement

<table>
<tr><td></td><td colspan="2">Préparer des rapports techniques comme l’analyse des options de solutions de sécurité des TI et les plans de mise en œuvre
Fournir une vérification et validation par un tiers (VVT) sur les projets de logiciels
Fournir des conseils sur les politiques, plans et pratiques de sécurité logicielle
Examiner, élaborer et fournir du matériel de formation</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Diplôme en informatique pertinent lié à la programmation, à la conception ou au développement de logiciels</td></tr>
<tr><td>Formation</td><td>Certification valide au niveau de l’industrie pour le développement de logiciels sécurisés et les essais de sécurité logicielle</td></tr>
<tr><td>Expérience professionnelle</td><td>Expérience modérée (3 à 5 ans) dans le développement de logiciels, suivie d’une expérience modérée (3 à 5 ans) dans des activités de développement de logiciels sécurisés.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">Outils, processus et protocoles de développement de logiciels
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
Information sur la sécurité des logiciels et des applications à source ouverte (par exemple, OWASP)
Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents
Outils et techniques d’essai et d’évaluation de la sécurité des logiciels
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
Bases de données communes sur la vulnérabilité
Sites de collaboration sociale pour le développement de logiciels (par exemple GITHUB)
Services de sécurité fournis, le cas échéant</td></tr>
<tr><td>Compétences</td><td colspan="2">Application de base des CCH suivantes :
☐ Concepts d’architecture de sécurité et modèle d’architecture de sécurité des renseignements d’entreprise
☐ Processus d’évaluation de la sécurité et d’autorisation
☐ Processus d’achat de logiciels et évaluations de l’intégrité de la chaîne d’approvisionnement
☐ Outils, procédures et pratiques d’essai et d’évaluation des systèmes de sécurité des TI

Application avancée des CCH suivantes :
☐ Modèles, processus et principes du génie logiciel
☐ Cycle de vie du développement de logiciels et gestion de projets de logiciels
☐ Processus, procédures, pratiques, outils et techniques d’opérations de codage et de développement de logiciels sécurisés
☐ Besoins opérationnels en matière de sécurité, y compris les exigences de conformité
☐ Caractéristiques et exigences en matière de sécurité des données</td></tr>
</table>

	☐ Contrôles de sécurité pour le développement de logiciels ☐ Normes de développement de logiciels ☐ Normes de logiciels sécurisés ☐ Méthodes et processus sécurisés d'essai et d'évaluation des logiciels ☐ Méthodes et applications d'évaluation de vulnérabilité et d'essais de pénétration ☐ Création et essai des modèles de menace ☐ Analyse, évaluation et balayage des vulnérabilités ☐ Activités et techniques d'essais de pénétration ☐ Enquête et analyse sur les vulnérabilités et les failles des logiciels ☐ Mise en place et gestion de l'environnement sécurisé d'essais de logiciels et d'applications Web ☐ 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 des services à fournir, des systèmes logiciels et applications utilisés, et de la manière dont ils sont intégrés dans les réseaux organisationnels. ▪ 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 du dispositif, il faudra évaluer les risques posés pour l'organisation et mettre en œuvre des mesures d'atténuation au niveau de risque acceptable. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment les outils susceptibles de soutenir le développement, l'essai et l'intégration de logiciels seront utilisés ainsi que les implications potentielles en matière de sécurité. Si des outils de sécurité automatisés sont utilisés dans le développement et l'évaluation des logiciels, les responsabilités en matière d'essais, d'intégration et de suivi des exigences devront être définies et les responsables de ces activités devront être conseillés/formés sur les changements de processus et de procédures qui en résultent. ▪ 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, il faudra procéder à des évaluations créatives et localement pertinentes de la robustesse de la sécurité des logiciels/applications et des stratégies d'atténuation potentielles. Cela exigera des capacités de réflexion critique et abstraite bien affinées. ▪ 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 appliquée à l'environnement de logiciel/d'application.