Analyste d’évaluation de vulnérabilité

Cadre de référence de la NICE	Protection et défense, PR-VAM-001, analyste d’évaluation de vulnérabilité (VA)	
Description fonctionnelle	Le titulaire balaye les applications et les systèmes d’exploitation pour repérer les failles et les vulnérabilités; et effectue et présente des évaluations de vulnérabilité des réseaux et des systèmes d’une organisation.	
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d’attention aux détails ou le mauvais jugement peuvent entraîner une mauvaise identification ou une non-détection des vulnérabilités qui pourraient être comprises. Cela peut avoir un impact important sur les systèmes, les capacités et les fonctions informatiques de l’organisation.	
Parcours de perfectionnement	Il s’agit souvent d’un poste de niveau 2 dans un environnement des opérations de cybersécurité qui est normalement précédé de 2 à 3 ans dans un rôle de sécurité des réseaux ou de sécurité opérationnelle. Cela peut conduire à une spécialisation accrue comme analyste de vulnérabilité, chef d’équipe rouge/bleu, testeur de pénétration ou rôles de gestion.	
Autres titres	▪ Testeur de vulnérabilité ▪ Évaluateur de vulnérabilité ▪ Gestionnaire de l’évaluation de vulnérabilité	
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel	
Tâches	▪ Repérer les failles critiques des applications et des systèmes que les cyberacteurs pourraient exploiter ▪ Effectuer des évaluations de vulnérabilité des technologies concernées (par exemple, l’environnement informatique, le réseau et l’infrastructure de soutien, et les applications) ▪ Préparer et présenter des évaluations complètes de vulnérabilité ▪ Effectuer des audits et des balayages de sécurité des réseaux ▪ Maintenir un ensemble d’outils d’audit de cyberdéfense déployables (par exemple, des logiciels et du matériel spécialisés de cyberdéfense) pour soutenir les opérations de cyberdéfense ▪ Préparer des rapports d’audit qui tirent des conclusions techniques et procédurales, et faire des recommandations sur les stratégies et solutions correctives ▪ Mener ou soutenir les essais de pénétration autorisés sur les réseaux et systèmes des organisations ▪ Définir et revoir les exigences relatives aux solutions de sécurité de l’information ▪ Formuler des recommandations sur la sélection de contrôles de sécurité rentables pour atténuer les risques ▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs	
Qualifications requises	Éducation	Études postsecondaires (diplôme en informatique ou dans un domaine des TI connexe)
	Formation	Formation aux systèmes de cybersécurité, à l’évaluation et à l’analyse de vulnérabilité. Formation

		au système de vulnérabilité basé sur les fournisseurs.
	Expérience professionnelle	2 à 3 ans dans un rôle d'opérations de réseau ou de cybersécurité.
Outils et technologie	▪ Politiques, procédures et pratiques de sécurité organisationnelle ▪ Outils d'évaluation de vulnérabilité ▪ Politiques, processus et pratiques de gestion de vulnérabilité ▪ Bases de données des vulnérabilités communes	
Compétences	Les CCH s'appliquent au niveau de base : ☐ Outils, techniques et protocoles évolués pour les acteurs de menace ☐ Principes, outils et techniques d'essais de pénétration ☐ Processus de gestion des risques pour l'évaluation et l'atténuation des risques ☐ Concepts d'administration du système ☐ Concepts de gestion de la cryptographie et des clés cryptographiques ☐ Cryptologie ☐ Détermination des problèmes de sécurité sur la base de l'analyse de vulnérabilité et des données de configuration ☐ Politiques, processus et pratiques de gestion de vulnérabilité Les CCH sont appliquées à un niveau avancé : ☐ Planification et programmation d'évaluation de vulnérabilité, y compris les risques et les mesures d'atténuation du système ☐ Menaces à la sécurité des systèmes et des applications et vulnérabilités ☐ Techniques de renforcement de la sécurité de l'administration du système, du réseau et des systèmes d'exploitation ☐ Analyse des paquets à l'aide d'outils appropriés ☐ Exécution de balayages des vulnérabilités et reconnaissance des vulnérabilités des systèmes de sécurité ☐ Réalisation d'évaluations de la vulnérabilité/des impacts/des risques ☐ Examen des journaux du système pour identifier les preuves d'intrusions passées ☐ Utilisation d'outils d'analyse de réseau pour déterminer les vulnérabilités	
Tendances futures ayant une incidence sur les compétences clés	▪ 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 par rapport à la détection, à l'intervention et à la reprise en cas d'incident 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. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront	

	intégrés dans le COS, y compris la mise en œuvre de changements de personnel et de processus. ▪ 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 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 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, à la compréhension des vulnérabilités du système et à la manière d'atténuer les menaces liées à la sécurité quantique.

Testeur de pénétration

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Le titulaire effectue des essais formels et contrôlés et des évaluations de la sécurité physique des applications, réseaux et autres systèmes basés sur le Web, selon les besoins, afin de déterminer et d'exploiter les vulnérabilités de sécurité.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou le mauvais jugement peuvent entraîner une mauvaise identification ou une non-détection des vulnérabilités qui pourraient être comprises. Cela peut avoir un impact important sur les systèmes, les capacités et les fonctions informatiques de l'organisation.
Parcours de perfectionnement	Il s'agit souvent d'un poste de niveau 2 ou 3 dans un environnement des opérations de cybersécurité qui est normalement précédé d'une expérience importante (3 à 5 ans) dans un rôle d'opérations de cybersécurité, y compris un emploi dans l'analyse de vulnérabilité, l'analyse des logiciels malveillants ou l'analyse technique des systèmes de sécurité. Il s'agit d'un rôle technique avancé, qui peut conduire à une spécialisation technique croissante, à des rôles de direction ou de gestion d'une équipe rouge.
Autres titres	▪ Spécialiste d'essai et d'évaluation de sécurité ▪ Analyste spécialisé dans l'évaluation de la vulnérabilité
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2173 – Ingénieurs/ingénieures et concepteurs/conceptrices en logiciel
Tâches	▪ Effectuer des essais de pénétration sur les applications Web, les connexions réseau et les systèmes informatiques afin de cibler les cybermenaces et les vulnérabilités techniques

<table>
<tr><td></td><td colspan="2">▪ Effectuer des évaluations de la sécurité physique du réseau, des dispositifs, des serveurs et des systèmes d'une organisation
▪ Développer des essais de pénétration et les outils nécessaires à leur exécution (par exemple, normes, risques, atténuations)
▪ Rechercher des vulnérabilités et des faiblesses de sécurité inconnues dans les applications Web, les réseaux et les systèmes pertinents que les cyberacteurs peuvent facilement exploiter
▪ Élaborer et tenir à jour des documents sur les résultats des activités d'essais de pénétration
▪ Recourir à l'ingénierie sociale pour découvrir les lacunes en matière de sécurité
▪ Définir et revoir les exigences relatives aux solutions de sécurité de l'information
▪ Analyser, documenter et partager les résultats en matière de sécurité avec la direction et le personnel technique
▪ Fournir des recommandations et des lignes directrices sur la manière d'améliorer les pratiques de sécurité organisationnelle
▪ Élaborer, fournir et superviser le matériel de formation et les efforts éducatifs</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Études postsecondaires (diplôme en informatique ou dans un domaine des TI connexe)</td></tr>
<tr><td>Formation</td><td>Formation aux outils, techniques et procédures d'analyse de la vulnérabilité et d'essais de pénétration.</td></tr>
<tr><td>Expérience professionnelle</td><td>2 à 3 ans d'expérience dans un rôle avancé d'opérations de cybersécurité, de préférence avec une expérience en évaluation de vulnérabilité.</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Politiques, procédures et pratiques de sécurité organisationnelle
▪ Carte des systèmes organisationnels et architecture de réseau
▪ Outils d'évaluation de vulnérabilité
▪ Politiques, processus et pratiques de gestion de vulnérabilité
▪ Bases de données des vulnérabilités communes
▪ Outils et protocoles d'essais de pénétration</td></tr>
<tr><td>Compétences</td><td colspan="2">Les CCH sont appliquées à un niveau avancé :
☐ Architecture de sécurité des réseaux
☐ Outils, techniques et protocoles évolués pour les acteurs de menace
☐ Principes, outils et techniques d'essais de pénétration
☐ Processus de gestion des risques pour l'évaluation et l'atténuation des risques
☐ Concepts d'administration du système
☐ Concepts de gestion de la cryptographie et des clés cryptographiques
☐ Cryptologie
☐ Détermination des problèmes de sécurité sur la base de l'analyse de vulnérabilité et des données de configuration
☐ Politiques, processus et pratiques de gestion de vulnérabilité
☐ Planification et programmation des essais de pénétration, y compris les risques et les mesures d'atténuation du système
☐ Menaces à la sécurité des systèmes et des applications et vulnérabilités
☐ Techniques de renforcement de la sécurité de l'administration du système, du réseau et des systèmes d'exploitation</td></tr>
</table>

	☐ Analyse des paquets à l'aide d'outils appropriés ☐ Exécution de balayages des vulnérabilités et reconnaissance des vulnérabilités des systèmes de sécurité ☐ Réalisation d'évaluations de la vulnérabilité/des impacts/des risques ☐ Examen des journaux du système pour identifier les preuves d'intrusions passées ☐ Utilisation d'outils d'analyse de réseau pour déterminer les vulnérabilités
Tendances futures ayant une incidence sur les compétences clés	▪ 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 par rapport à la détection, à l'intervention et à la reprise en cas d'incident 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. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans le COS, y compris la mise en œuvre de changements de personnel et de processus. ▪ 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 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 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, à la compréhension des vulnérabilités du système et à la manière d'atténuer les menaces liées à la sécurité quantique.