Analyste en investigation informatique numérique

Cadre de référence de la NICE	Enquête, analyste en investigation informatique de cyberdéfense, INV-FOR-002
Description fonctionnelle	**La description suivante, basée sur les rôles, concerne uniquement les opérations de sécurité et ne comprend pas les fonctions d'investigation informatique numérique ou d'audit qui sont prévues dans le cadre des professions connexes liées à l'application de la loi ou à l'audit**. Le titulaire effectue des investigations informatiques numériques pour analyser les preuves provenant d'ordinateurs, de réseaux et d'autres dispositifs de stockage de données. Il s'agit notamment d'enquêter sur les preuves électroniques et de les conserver, de planifier et de développer des outils, de hiérarchiser les activités et de soutenir les opérations de reprise et l'analyse après l'incident.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes, le manque d'attention aux détails ou un mauvais jugement peuvent entraîner l'incapacité à déterminer la source et à atténuer une compromission, mais peuvent également avoir des répercussions sur les systèmes d'information des organisations, notamment en ce qui concerne les accusations criminelles ou les litiges civils.
Parcours de perfectionnement	Il s'agit souvent d'un poste de niveau 2/3 dans un environnement des opérations de cybersécurité qui est normalement précédé d'un minimum de 2 à 3 ans dans un rôle de sécurité des réseaux ou de sécurité opérationnelle, y compris analyste des logiciels malveillants. Cela peut conduire à une spécialisation accrue dans les activités d'investigation informatique numérique ou d'évaluation de la sécurité, ainsi qu'à des rôles de chef d'équipe rouge/bleue, de testeur de pénétration ou de gestionnaire.
Autres titres	▪ Investigateur en investigation informatique numérique (normalement réservé à l'environnement de la cybercriminalité) ▪ Examinateur en investigation informatique numérique (normalement réservé aux environnements de cyberaudit)
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 enquêtes en temps réel sur les incidents de cyberdéfense (par exemple, collectes de preuves, corrélation et suivi des intrusions, et analyse des menaces) ▪ Enquêter sur les incidents de sécurité conformément au mandat ▪ Planifier des activités d'investigation informatique numérique pour les cyberincidents ▪ Collecter et analyser les artefacts d'intrusion (par exemple, le code source, les logiciels malveillants et la configuration du système) et utiliser les données découvertes pour permettre d'atténuer les incidents potentiels de cyberdéfense ▪ Identifier et rendre compte avec précision des artefacts d'investigation informatique numérique ▪ Capturer et analyser le trafic du réseau associé aux activités malveillantes à l'aide d'outils de surveillance du réseau

<table>
<tr><td></td><td colspan="2">▪ Contribuer à la post-analyse des incidents de sécurité et formuler des recommandations basées sur les activités d'investigation
▪ Élaborer et tenir à jour des rapports d'enquête et des rapports techniques
▪ Fournir une assistance technique sur les questions de preuves numériques au personnel approprié
▪ Rassembler des preuves pour les affaires judiciaires et fournir des témoignages d'experts lors des procédures judiciaires
▪ Gérer les preuves numériques conformément aux exigences appropriées de la chaîne de possession
▪ Établir et gérer une infrastructure/un laboratoire d'analyse sécurisé
▪ Exploiter des systèmes d'investigation informatique numérique (selon les besoins et les fonctions et systèmes disponibles)
▪ Préparer et examiner les politiques, normes, procédures et lignes directrices en matière d'investigation
▪ 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'investigation informatique numérique. En outre, en fonction du contexte technique de l'organisation et des systèmes/dispositifs utilisés, une formation spécialisée en matière d'investigation informatique numérique peut être nécessaire (par exemple, appareil mobile, média numérique, etc.)</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 de l'analyse des logiciels malveillants dans des environnements actifs et de la « boîte morte ».</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, techniques et procédures d'investigation informatique numérique
▪ Outils d'analyse des logiciels malveillants
▪ Système de gestion des événements et incidents de sécurité
▪ Bases de données des vulnérabilités communes
▪ Mandats, responsabilités et limites de l'autorité en matière d'enquêtes de sécurité</td></tr>
<tr><td>Compétences</td><td colspan="2">Les CCH sont appliquées à un niveau avancé :
☐ Outils, techniques et procédures des acteurs de menace
☐ Méthodes de réponse aux incidents et de traitement des incidents
☐ Système de gestion des événements et incidents de sécurité
☐ Méthodes, processus et pratiques d'investigation informatique numérique
☐ Tactiques, techniques et procédures de lutte contre la cybercriminalité
☐ Processus de collecte, d'emballage, de transport et de stockage des preuves électroniques pour éviter l'altération, la perte, les dommages physiques ou la destruction des données
☐ Capture et préservation des preuves numériques</td></tr>
</table>

	☐ Lois, règlements, politiques et éthiques applicables en matière d'enquêtes et de gouvernance ☐ Règles juridiques de preuve et procédures judiciaires, présentation de preuves numériques, témoignage en tant que témoin expert ☐ Expertise judiciaire spécifique à un système ou à un appareil (par exemple, mémoire, directeur actif, appareil mobile, réseau, ordinateur [boîte morte], etc.) ☐ Outils et techniques d'analyse des logiciels malveillants ☐ Rétroingénierie ☐ Capacités déployables en matière d'investigation informatique numérique ☐ Types d'investigation informatique numérique, y compris les outils, les techniques et les procédures (en fonction de l'organisation et du système d'information) qui peuvent inclure les investigations informatiques numériques suivantes : o l'ordinateur o le réseau et le répertoire actif o les appareils mobiles o les médias numériques (image, vidéo, audio) o la mémoire
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 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. ▪ 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 que les outils, techniques et protocoles des acteurs de menace liés aux attaques de l'informatique quantique et la manière de s'en défendre.