Analyste de la sécurité de la chaîne d'approvisionnement

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Le titulaire est le principal responsable de la collecte et de l'analyse des données pour cibler les failles et les vulnérabilités de la cybersécurité dans les opérations de la chaîne d'approvisionnement d'une organisation, et fournit des conseils et des orientations pour aider à réduire ces risques de la chaîne d'approvisionnement.
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou le mauvais jugement peuvent entraîner des décisions organisationnelles qui peuvent avoir une incidence importante sur l'entreprise. L'absence d'une appréciation complète des besoins opérationnels en matière de sécurité mettra en péril la posture de sécurité de l'organisation face à l'évolution des menaces.
Parcours de perfectionnement	Généralement tiré de rôles d'analyse de la cybersécurité (par exemple, analyste des opérations de cybersécurité, analyste de vulnérabilité, etc.), ce rôle peut néanmoins être assumé par un large éventail de professionnels qui peuvent évaluer et fournir des renseignements sur les menaces potentielles pesant sur la chaîne d'approvisionnement. Cela inclut ceux qui peuvent se spécialiser dans les aspects liés aux facteurs humains de la chaîne d'approvisionnement (par exemple, accès proche, menace interne).
Autres titres	Analyste de la cybersécurité Analyste de l'intégrité de la chaîne d'approvisionnement
CNP connexes	2171 – Analystes et consultants/consultantes en informatique 2174 – Programmeurs/programmeuses et développeurs/développeuses en médias interactifs
Tâches	▪ Collaborer avec les intervenants clés pour établir un programme efficace de gestion des risques liés à la cybersécurité ▪ Assurer la conformité avec les lois et règlements en vigueur ▪ Élaborer et mettre en œuvre des plans alignés sur les objectifs organisationnels et les exigences de sécurité ▪ Recueillir et analyser les renseignements relatifs à la chaîne d'approvisionnement afin de cibler et d'atténuer les défauts et les vulnérabilités, y compris l'intégrité des composants, dans les réseaux ou les systèmes informatiques d'une organisation ▪ Analyser les configurations matérielles et logicielles des systèmes ▪ Recommander du matériel, des logiciels et des contre-mesures à installer ou à mettre à jour en fonction des cybermenaces et des vulnérabilités en matière de sécurité ▪ Collaborer avec les collègues pour mettre en œuvre les changements et les nouveaux systèmes ▪ Suivre et signaler les cybermenaces et les vulnérabilités de sécurité qui ont des répercussions sur le rendement de la chaîne d'approvisionnement ▪ Définir, développer, mettre en œuvre et maintenir des plans, des politiques et des procédures de cybersécurité ▪ Veiller au respect des politiques, réglementations et procédures de cybersécurité de l'organisation

	▪ Assurer la conformité aux exigences de sécurité des réseaux et systèmes de l'organisation ▪ Élaborer et tenir à jour des évaluations des risques et des rapports connexes sur les fournisseurs, les produits et les services ▪ Définir et maintenir des ensembles d'outils et des procédures qui soutiennent l'intégrité de la chaîne d'approvisionnement ▪ Préparer des rapports techniques ▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés à la cybersécurité et à l'intégrité de la chaîne d'approvisionnement	
Qualifications requises	Éducation	Études postsecondaires dans un domaine lié à la cybernétique ou aux TI (par exemple : génie informatique, informatique, technologies de l'information, gestion des technologies des affaires – sécurité numérique ou équivalent)
	Formation	Outre une formation structurée à l'analyse de la cybersécurité, une formation spécialisée et des compétences en matière d'analyse de vulnérabilité et des menaces pesant sur la chaîne d'approvisionnement sont nécessaires.
	Expérience professionnelle	Les personnes employées dans ce rôle peuvent avoir différents niveaux d'expertise en matière de cybersécurité. L'expérience requise dépendra du besoin organisationnel et de la complexité des systèmes à analyser.
Outils et technologie	▪ Plans stratégiques et d'affaires ▪ Évaluation de la menace et des risques ▪ Processus de gestion de vulnérabilité et outils et applications d'évaluation de vulnérabilité ▪ Processus et procédures de gestion des incidents ▪ Infrastructure de sécurité organisationnelle et systèmes de compte rendu Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents ▪ Processus et politiques de gestion des risques de cybersécurité dans la chaîne d'approvisionnement ▪ Accords et contrats de tiers et de niveau de service	
Compétences	Application de base des CCH suivantes : ☐ Concepts, principes et pratiques de sécurité intégrée/organisationnelle (logiciels, systèmes, données, matériel et personnel) ☐ Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles ☐ Menaces, besoins opérationnels et infrastructures techniques liés au secteur/contexte ☐ Gestion de projet et exigences de sécurité tout au long du cycle de vie du projet ☐ Processus d'approvisionnement et exigences de sécurité Application avancée des CCH suivantes : ☐ Infrastructure de sécurité organisationnelle, y compris les systèmes de protection et de défense tout au long de la chaîne d'approvisionnement	

	☐ Situation de la menace à la cybersécurité et sources de renseignements sur la menace liée à la chaîne d'approvisionnement ☐ Exigences juridiques et de conformité alors qu'elles s'étendent aux accords avec des tiers ☐ Analyse de vulnérabilité et outils ☐ Analyse et techniques avancées de sécurité des renseignements et des données ☐ Conception fonctionnelle et technique des réseaux et des systèmes, et solutions de cybersécurité ☐ Processus, responsabilités et pouvoirs de gestion des risques au sein de l'organisation et tout au long de la chaîne d'approvisionnement ☐ Gestion des risques et responsabilité des tiers ☐ Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels ☐ Processus actuels de la chaîne d'approvisionnement nationale
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. ▪ L'utilisation accrue des outils automatisés, aidée par l'intelligence artificielle, nécessitera de comprendre comment ces outils seront intégrés dans l'infrastructure de sécurité organisationnelle et les implications pour le personnel, les ressources, les procédures et les politiques. ▪ 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. ▪ 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. ▪ 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 au sein de l'organisation.