Analyste des systèmes de technologie opérationnelle

Cadre de référence de la NICE	Aucun.
Description fonctionnelle	Le titulaire est responsable de fournir des conseils et d'assurer une cybersécurité efficace dans les contextes de technologie opérationnelle (TO)(SCI/SCO/SCADA). Il travaille de concert avec les ingénieurs systèmes/technologues de différentes disciplines qui sont associés aux systèmes gérés par la TO (par exemple, les ingénieurs en mécanique des fluides, les ingénieurs spécialistes des systèmes de puissance, les ingénieurs de systèmes mécaniques).
Conséquence des erreurs ou risque	Les erreurs, la négligence, les renseignements obsolètes ou un mauvais jugement pourraient entraîner une défaillance catastrophique de la TO et des systèmes connexes qu'ils utilisent pour la gestion. Dans de nombreux cas, cela peut avoir une incidence importante sur les opérations organisationnelles et, dans certains cas, peut directement entraîner des dommages importants pour les êtres humains (par exemple dans les systèmes d'infrastructures critiques).
Parcours de perfectionnement	Après une formation technique, le titulaire est souvent employé dans des activités liées aux systèmes de TI ou de TO qui constituent la base d'un travail de cybersécurité plus spécialisé dans l'environnement de TO. De même, les professionnels de la cybersécurité qui travaillent normalement dans un environnement informatique peuvent passer aux systèmes de TO en bénéficiant d'une formation et d'un enseignement spécialisés en TO et en intégration de systèmes.
Autres titres	Conseiller en sécurité de la TO Technicien en sécurité de la TO Analyste de la sécurité – SCI/SCO/SCADA
CNP connexes	2133 – Ingénieurs électriciens et électroniciens/ingénieures électriciennes et électroniciennes 2147 – Ingénieurs informaticiens/ingénieures informaticiennes (sauf ingénieurs/ingénieures et concepteurs/conceptrices en logiciel) 2171 – Analystes et consultants/consultantes en informatique 2241 – Technologues et techniciens/techniciennes en génie électronique et électrique
Tâches	▪ Collaborer avec les intervenants clés pour mettre en place un programme efficace de gestion des risques liés à la cybersécurité dans l'environnement de TO. ▪ Rechercher et soutenir la conception de solutions de cybersécurité dans le contexte de la TO ▪ Assurer la conformité avec les lois et règlements en vigueur ▪ Rédiger, mettre en œuvre et maintenir les politiques, normes et procédures de sécurité des TI/TO ▪ Surveiller et gérer les exigences et les contrôles de cybersécurité dans l'environnement de TO ▪ Évaluer et analyser la position en matière de cybersécurité dans les systèmes de TO et recommander des mesures correctives/de gestion des risques pour les vulnérabilités ▪ Travailler avec d'autres parties prenantes, soutenir la conception et le développement de solutions de sécurité pour répondre aux exigences commerciales et techniques dans l'environnement de TO

<table>
<tr><td></td><td colspan="2">▪ Gérer l'intégration technique entre les TI et les TO
▪ Définir et maintenir des ensembles d'outils et des procédures qui soutiennent le suivi et la gestion des TO
▪ En concertation avec les autres parties prenantes, élaborer des plans d'intervention en cas d'incident de cybersécurité définissant clairement le rôle des personnes chargées de la gestion et de la maintenance des systèmes de TO
▪ Préparer des rapports techniques
▪ Élaborer, fournir et superviser le matériel de formation sur la cybersécurité et les efforts éducatifs liés aux TO</td></tr>
<tr><td rowspan="3">Qualifications requises</td><td>Éducation</td><td>Baccalauréat en informatique, en génie informatique ou dans une discipline connexe ou formation et expérience équivalentes</td></tr>
<tr><td>Formation</td><td>Formation spécialisée associée à la cybersécurité de la TO ainsi qu'aux outils et techniques spécifiques aux systèmes requis</td></tr>
<tr><td>Expérience professionnelle</td><td>L'expérience préférée pour le rôle de premier échelon requiert une expérience modérée de 2 à 3 ans dans l'environnement de TO</td></tr>
<tr><td>Outils et technologie</td><td colspan="2">▪ Plans stratégiques et d'affaires
▪ Évaluation de la menace et des risques
▪ Processus de gestion de vulnérabilité et évaluations de vulnérabilité des TO
▪ Processus et procédures de gestion des incidents
▪ Systèmes de gestion des événements et incidents de sécurité ou systèmes et réseaux de signalement des incidents qui peuvent être utilisés pour les incidents de cybersécurité de TO
▪ 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 et procédures de sécurité des TO</td></tr>
<tr><td>Compétences</td><td colspan="2">Tout en sachant que tous les analystes de TO n'auront pas nécessairement une formation en TI, il convient de se référer aux applications de base des CCH suivantes :

☐ Systèmes de télémétrie, communication de données, acquisition de données et contrôle de processus
☐ Concepts de systèmes d'exploitation, de réseaux et de systèmes de communication
☐ Réseaux de distribution électrique, équipement du système électrique, fonctionnement des stations de transformation et théorie de l'électricité
☐ Procédures de dépannage et de maintenance des ordinateurs et des réseaux
☐ Principes et pratiques de l'administration des réseaux
☐ Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels
☐ Applications et systèmes de gestion de bases de données
☐ Administration et optimisation des bases de données
☐ Méthodes et processus d'essai et d'évaluation des systèmes
☐ Mesures ou indicateurs du rendement, de la disponibilité, de la capacité ou des problèmes de configuration du système</td></tr>
</table>

	☐ Outils d'analyse et protocoles de réseau ☐ Outils de diagnostic et techniques d'identification des défauts Application avancée des CCH suivantes : ☐ Logiciels et matériel des systèmes de TO, contrôleurs logiques programmables, relais numériques et analogiques ☐ Évaluation de la menace et des risques liés à la TO connectée à Internet (y compris les implications et l'évaluation des dispositifs IdO) ☐ Exigences juridiques et de conformité, y compris les responsabilités organisationnelles en matière de sécurité du lieu de travail et du public liées à la TO/production ☐ Normes et meilleures pratiques de l'industrie, notamment en ce qui concerne les environnements industriels dans l'espace de cybersécurité ☐ Gestion, mesures et suivi du programme de cybersécurité Systèmes de contrôle – applicables à l'industrie/aux environnements de production ☐ Intégration et convergence des TI/TO ☐ Sécurité des processus et analyse des dangers ☐ Analyse et intégration de système ☐ Résolution de problèmes dans les environnements de systèmes complexes ☐ Communications techniques, y compris la rédaction de rapports pour traiter des questions techniques interdisciplinaires
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, et plus particulièrement ceux liés aux TO et à l'exploitation et l'accès à distance. ▪ 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 surveillance et des opérations à distance par l'IdO et les dispositifs. ▪ 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 les exigences, les procédures et les politiques de TO. ▪ 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. Pour le chiffrement au sein des systèmes de TO, cela nécessitera des connaissances et des compétences liées à la mise en œuvre d'une stratégie de sécurité quantique au sein de l'organisation.