Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Certifications dans le domaine de la cybersécurité

Canada

AVANT-PROPOS

La publication *Certifications dans le domaine de la cybersécurité* est un document NON CLASSIFIÉ. Ce document se veut un guide qui fournit de l'information sur plusieurs des certifications offertes aux étudiants potentiels et aux professionnels de la cybersécurité. Son objectif n'est pas de recommander un organisme de certification ou une certification en particulier, mais plutôt d'offrir une liste de différentes certifications pouvant aider des employés à progresser sur le plan professionnel dans le domaine de la cybersécurité.

L'information est tirée des sites Web des organismes de certification mentionnés dans le présent guide.

Avis de non-responsabilité : Le Centre de la sécurité des télécommunications n'approuve ni ne recommande aucune des certifications ou aucun des organismes de certification proposés dans le présent document. L'information fournie se veut un résumé général de renseignements accessibles au public et elle est offerte à titre d'information seulement.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première version	Novembre 2020
2	Ajout de nouvelles certifications et retrait de fournisseurs de formation	Juillet 2022

Avis de non-responsabilité : Le Centre de la sécurité des télécommunications n'approuve ni ne recommande aucune des certifications ou aucun des organismes de certification proposés dans le présent document. L'information fournie se veut un résumé général de renseignements accessibles au public et elle est offerte à titre d'information seulement.

TABLE DES MATIÈRES

Avis de non-responsabilité : Le Centre de la sécurité des télécommunications n'approuve ni ne recommande aucune des certifications ou aucun des organismes de certification proposés dans le présent document. L'information fournie se veut un résumé général de renseignements accessibles au public et elle est offerte à titre d'information seulement.

LISTE DES TABLEAUX

1.0 INTRODUCTION

La demande de professionnels et de praticiens compétents dans le domaine de la cybersécurité continue d'augmenter au Canada et à travers le monde. Face à cette demande croissante, la valeur accordée à la certification en technologies de l'information (TI) est également en hausse. Une certification adéquate peut donner aux titulaires un avantage par rapport à d'autres candidats. Dans cette optique, les organisations recherchent des personnes compétentes ayant reçu une formation de haut niveau et possédant une expérience concrète.

L'obtention d'une certification démontre à d'éventuels employeurs qu'une personne est compétente, qualifiée et expérimentée dans certains domaines. En outre, compte tenu du temps et de l'investissement financier qu'exigent de nombreuses certifications, certains employeurs considèrent que la certification démontre un engagement professionnel dans le domaine.

Les certifications sont non seulement un excellent complément à d'autres compétences professionnelles, mais elles peuvent également conduire à des augmentations salariales. Selon une étude menée par Global Knowledge, une personne détenant une certification peut toucher un revenu jusqu'à 15 % supérieur à celui d'employés qui n'en possèdent pas (1). De plus, conserver une certification implique souvent de poursuivre une formation continue ce qui permet aux titulaires de rester à l'affût des nouvelles technologies et de continuer à protéger leurs organisations contre les menaces émergentes pour la cybersécurité.

1.1 LE CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a été mis sur pied sous l'égide du Centre de la sécurité des télécommunications (CST) en octobre 2018. L'équipe Collaboration avec le milieu de l'éducation et développement des cybercompétences travaille de concert avec les universités, les collèges, les associations éducatives, les comités ministériels à vocation éducative et des professeurs du secteur privé afin d'accroître les capacités et le bassin de candidats talentueux en cybersécurité au Canada. L'équipe collabore aussi avec les professeurs afin d'améliorer la compréhension de la collectivité en matière de cybersécurité. Sa mission consiste à s'assurer que le Canada demeure un leader mondial en cybersécurité et, pour ce faire, il est essentiel de renforcer la formation en cybersécurité au pays.

1.2 OBJET

Le présent guide a comme principal public cible d'éventuels étudiants ou professionnels de la cybersécurité qui cherchent à faire progresser leur carrière dans le domaine. Le guide met en lumière certaines des certifications les plus demandées et reconnues mondialement qu'offrent des fournisseurs à travers le monde. Une liste complète des certifications se trouve à la fin du guide (tableaux 1 à 14).

Avis de non-responsabilité : Le CST n'approuve ni ne recommande aucune des certifications ou aucun des organismes de certification proposés dans le présent document. L'information fournie se veut un résumé général de renseignements accessibles au public et elle est offerte à titre d'information seulement.

Toutes les mesures nécessaires pour s'assurer de l'exactitude des renseignements ont été prises; toutefois, en raison de la nature dynamique des programmes et de la cybersécurité, le présent guide sera révisé régulièrement afin de s'assurer qu'il reflète les offres de certification les plus récentes. De nouvelles certifications ainsi que d'autres modifications proposées peuvent être envoyées par courriel à l'adresse academicoutreach-collaborationacademique@cyber.gc.ca.

2.0 ORGANISMES DE CERTIFICATION RECONNUS MONDIALEMENT

Les sections suivantes présentent des certifications en cybersécurité parmi les plus populaires et les plus connues, classées par ordre alphabétique. Une liste plus complète de certifications se trouve dans les tableaux ci-joints. **Le CST n'approuve, n'appuie ou ne favorise aucune des certifications ou aucun des organismes de certification suivants. Le présent guide est fourni à titre d'information seulement. Il ne devrait être utilisé que comme point de départ par les personnes intéressées à obtenir une certification. En outre, ces personnes devraient faire des recherches plus approfondies, en prenant en considération leurs intérêts et objectifs de carrière, le temps qu'elles devront y consacrer et leurs ressources financières, avant de choisir la certification qui leur convient.**

Il faut également souligner que même si la plupart des organismes de certification sont américains, leurs certifications sont reconnues dans le monde entier. De plus, les candidats ont la possibilité de recevoir leur formation auprès de fournisseurs locaux et, dans plusieurs cas, de passer les examens dans des centres d'examen, comme le centre Pearson VUE, ou en ligne.

2.1 CERTNEXUS

Le programme **CertNexus** offre des certifications et des microcompétences en technologies émergentes, comme l'Internet des objets (IdO), l'intelligence artificielle et les interfaces homme-machine. Les quatre certifications offertes en cybersécurité sont valides pendant trois ans.

- La certification **Certified First Responder** (CRF) atteste les connaissances et les compétences requises pour protéger l'information et les systèmes essentiels avant, pendant et après un incident.
- La certification **Cyber Safe** démontre que ses titulaires peuvent déterminer les risques les plus courants associés à l'utilisation de technologies mobiles ou en nuage, et qu'ils sont aptes à se protéger, eux ainsi que leur organisation, contre des cybermenaces.
- Les titulaires d'une certification **Cyber Secure Coder** (CSC) ont été initiés aux vulnérabilités qui compromettent la sécurité, à l'établissement et à la correction de ces vulnérabilités, ainsi qu'aux stratégies de gestion des problèmes de sécurité.
- La microcompétence **IRBIZ** s'adresse aux leaders et aux cadres en TI qui sont tenus de respecter la législation en matière d'intervention en cas d'incident. Un cours et un examen réussis attestent que les candidats possèdent les compétences nécessaires pour évaluer les menaces pour la sécurité et intervenir face à celles-ci, et qu'ils sont aptes à faire fonctionner une plateforme d'analyse de la sécurité des systèmes et des réseaux.

Une liste complète des certifications en cybersécurité offertes par le programme CertNexus se trouve à la section 5.1.

2.2 CISCO SYSTEMS

Cisco Systems est un leader mondial en matière de solutions et de matériel de mise en réseau. La majorité du trafic Internet passe par des chemins d'accès réseau conçus par Cisco. L'obtention de l'une de ses certifications démontre que les candidats savent comment travailler avec les solutions Cisco. On compte cinq niveaux de certification dans le programme Cisco :

- **Débutant** : Le point de départ pour les personnes qui désirent entamer une carrière de professionnel des réseaux.
- **Associé** : Les candidats maîtrisent les éléments essentiels requis pour entreprendre une carrière et élargir leurs perspectives d'emploi grâce aux plus récentes technologies.

- **Professionnel** : Les candidats choisissent un volet en technologie de base et un examen axé sur une concentration afin de personnaliser leur certification de niveau professionnel.
- **Expert** : La certification est reconnue partout dans le monde comme étant la certification la plus prestigieuse de l'industrie des technologies.
- **Architecte** : Ce niveau permet de démontrer l'expertise architecturale d'un concepteur de réseaux.

Une liste complète des certifications en cybersécurité offertes par Cisco Systems se trouve à la section 5.2.

2.3 COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION

La **Computing Technology Industry Association** (CompTIA) délivre des certifications dans plus de 120 pays. Elle compte plus de 2,2 millions de titulaires. L'organisation publie également chaque année 50 études par secteur d'activités qui permettent de faire un suivi des tendances et des changements. Les certifications proposées couvrent une vaste gamme de domaines TI, dont la cybersécurité. Pour renouveler une certification, il faut satisfaire aux exigences en matière de formation continue et payer des frais annuels.

- La certification **CompTIA Advanced Security Practitioner** (CASP+) est axée sur le rendement et elle s'adresse davantage aux praticiens qu'aux gestionnaires. Elle touche un niveau avancé de compétence en cybersécurité. Les titulaires de la certification CASP+ possèdent des connaissances avancées en gestion des risques, en opérations et architecture de sécurité intégrée, ainsi qu'en recherche et en collaboration.
- La certification **CompTIA Cyber Security Analyst** (CySA+) s'adresse aux analystes de la cybersécurité et couvre les menaces persistantes avancées dans un environnement de cybersécurité après 2014. Elle atteste l'expertise d'une personne en analyse de la sécurité, en détection des intrusions et en intervention en cas d'incident.
- La certification **CompTIA PenTest+** s'adresse aux professionnels en cybersécurité chargés des tests de pénétration et de la gestion des vulnérabilités. Les titulaires de cette certification ont démontré que leurs connaissances et leurs compétences pratiques sont à jour et qu'ils sont en mesure de tester des dispositifs dans de nouveaux environnements (p. ex. en nuage ou mobiles), ainsi que des ordinateurs et des serveurs traditionnels.
- La certification **CompTIA Security+** est une certification de premier échelon. Les titulaires de cette certification sont des experts dans différents domaines : gestion des menaces, cryptographie, gestion de l'identité, systèmes de sécurité, identification et atténuation des risques liés à la sécurité, contrôle d'accès réseau et infrastructure de sécurité. Les candidats doivent posséder deux années d'expérience en sécurité des réseaux et avoir déjà obtenu leur certification **Network+**.

Une liste complète des certifications en cybersécurité offertes par le programme CompTIA se trouve à la section 5.3.

2.4 COUNCIL FOR REGISTERED ETHICAL SECURITY TESTERS

Le **Council for Registered Ethical Security Testers** (CREST) est un organisme à but non lucratif qui décerne à des sociétés et à des particuliers des certifications et des attestations reconnues internationalement. Des sections régionales de cet organisme se trouvent au Royaume-Uni, aux États-Unis, en Australie, à Singapour et à Hong Kong. Elles proposent des examens dont les sujets concernent les tests de pénétration, le renseignement sur les menaces, l'intervention en cas d'incident et l'architecture de la sécurité. Le Government Communications Headquarters (GCHQ) du Royaume-Uni a approuvé l'examen sur l'intervention en cas d'incident. Les examens CREST comportent trois niveaux d'attestation pour les particuliers :

- **Praticien** – admissible à l'exercice de la profession
- **Autorisé** – apte à travailler de manière autonome sans supervision
- **Certifié** – compétent sur le plan technique pour gérer de grands projets et des équipes de premier plan

Une liste complète des certifications en cybersécurité se trouve à la section 5.4.

2.5 CERTIFIED WIRELESS NETWORK PROFESSIONALS

Le programme **Certified Wireless Network Professionals** (CWNP) est un programme de certification WLAN (pour *Wireless Local Area Network*; réseau local sans fil) non rattaché à un fournisseur donné. Il offre quatre niveaux de certification WLAN (débutant à expert). Le programme de certification prépare les professionnels des TI et les administrateurs de WLAN à définir, à concevoir et à gérer les applications et l'infrastructure WLAN.

- La certification **Certified Wireless Network Expert** (CWNE) est la certification de plus haut niveau du programme CWNP. Les titulaires de cette certification disposent des compétences les plus avancées dans le marché actuel de la technologie Wi-Fi d'entreprise. Les candidats doivent réussir quatre examens de certification, procéder à des déploiements de WLAN commerciaux, fournir trois recommandations, satisfaire aux exigences en matière d'expérience et de publication, et faire l'objet d'un examen par les pairs dirigé par le comité consultatif de la certification CWNE.
- La certification **Certified Wireless Security Professional** (CWSP**)** est une certification WLAN de niveau professionnel faisant partie du programme CWNP. Elle atteste la capacité des candidats d'évaluer les vulnérabilités d'un réseau et d'aider à prévenir les attaques, d'effectuer des audits de sécurité de WLAN et de mettre en œuvre des solutions de surveillance de la conformité, et de concevoir l'architecture de sécurité d'un réseau. Les candidats doivent obtenir la certification **Certified Wireless Network Administrator** (CWNA) avant de recevoir la certification CWNP.

Une liste complète des certifications en cybersécurité offertes par le programme CWNP se trouve à la section 5.5.

2.6 EC-COUNCIL

L'**EC-Council** est un comité de certification technique en cybersécurité établi dans 145 pays. Il est approuvé par le gouvernement américain, la National Security Agency et le Committee on National Security Systems (CNSS).

- Le titre de compétence **Certified Ethical Hacker (ANSI)** atteste les compétences des candidats dans cinq phases du piratage contrôlé : la reconnaissance, l'énumération, l'obtention de l'accès, le maintien de l'accès et le brouillage de pistes. Cette certification exige de passer un examen de quatre heures comportant 125 questions.
- La certification **Certified Ethical Hacker (Practical)** cible l'application des compétences CEH dans le cadre de défis concrets d'audit de sécurité et d'autres scénarios connexes. Les candidats doivent passer un examen de six heures comportant 20 études de cas. La note de passage est de 70 %.
- La certification **Certified Ethical Hacker (Master)** est décernée aux candidats qui ont obtenu les certifications ANSI et Practical.
- Une autre certification universellement reconnue est la **Computer Hacking Forensics Investigator (CHFI)**. Elle atteste que ses titulaires sont versés dans les domaines de l'antipiratage, de la criminalistique numérique et des tests de pénétration.
- Les titulaires de la certification **Certified Network Defender (CND)** démontrent une connaissance approfondie de la sécurité axée sur la défense et l'expertise nécessaire pour sécuriser des données.
- Les titulaires de la certification **EC-Council Disaster Recovery Professional (EDRP)** disposent des bases nécessaires pour leur permettre de sécuriser et de rétablir des réseaux en cas de catastrophe, comme lors d'attaques malveillantes.

Une liste complète des certifications en cybersécurité offertes par l'EC-Council se trouve à la section 5.6.

2.7 GLOBAL INFORMATION ASSURANCE CERTIFICATION

Le programme **Global Information Assurance Certification** (GIAC), fondé par le SANS Institute, est spécialisé dans la certification technique et pratique. Les certifications offertes sont liées à des cours de formation dispensés par le SANS Institute. Elles sont reconnues dans le monde entier. Les candidats qui demandent une certification de catégorie *Expert Status* doivent uniquement passer un examen pour l'obtention de la certification, celle-ci étant valide pendant quatre ans. Pour être admissibles à un renouvellement à la fin de la période de quatre ans, les titulaires de la certification doivent avoir accumulé 36 crédits de formation continue et avoir payé les frais de renouvellement de la certification ou avoir repassé l'examen. Les personnes désirant obtenir une certification de catégorie *Gold Status* doivent faire des recherches et rédiger un rapport technique ou un livre blanc. Cette catégorie démontre que les titulaires ont des connaissances plus approfondies dans un domaine particulier.

- La certification **GIAC Security Essential Certification** (GSEC) atteste que les connaissances des candidats en sécurité de l'information vont au-delà de notions simples de terminologie et de concepts. Les titulaires ont les compétences nécessaires en défense active, en cryptographie, en politiques et plans sur la sécurité, en traitement des incidents, en protection de réseau, etc.
- La certification **GIAC Certified Intrusion Analyst** (GCIA) atteste les connaissances des praticiens en matière de surveillance de réseau et d'hôte, d'analyse de trafic et de détection d'intrusion. Les titulaires de la certification sont aptes à configurer et à surveiller des systèmes de détection d'intrusion, et à analyser le trafic sur un réseau.
- La certification **GIAC Certified Incident Handler** (GCIH) démontre la capacité des candidats de détecter les incidents liés à la sécurité informatique, d'y intervenir et de les régler en faisant appel à un large éventail de compétences essentielles en sécurité. Les titulaires d'une certification GCIH possèdent une connaissance approfondie des techniques courantes de cyberattaque et des mécanismes de défense contre celles-ci.

Une liste complète des certifications en cybersécurité offertes par le programme GIAC se trouve à la section 5.7.

2.8 INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM

L'**International Information Systems Security Certification Consortium**, ou (ISC)2, est un organisme membre sans but lucratif qui apporte un soutien à ses membres pour tout ce qui touche les titres de compétence, les ressources et le leadership sur le plan de la cybersécurité et de la sécurité de l'information, des logiciels et des infrastructures. Cette grande organisation de sécurité des TI compte plus de 140 000 membres à l'échelle mondiale, dont près de 6 000 au Canada.

L'association (ISC)2 offre l'une des certifications en cybersécurité les plus populaires :

- La certification **Certified Information Systems Security Professional** (CISSP) est souvent exigée pour les emplois les plus recherchés en cybersécurité. On la considère d'ailleurs comme la « référence absolue » en matière de certifications en sécurité. Pour obtenir cette certification de niveau avancé, il faut notamment posséder un minimum de cinq années d'expérience dans au moins deux des huit corpus de connaissances communes de l'association (ICS)2, ou quatre années d'expérience et un diplôme universitaire ou des certificats accrédités. Les candidats doivent également passer un examen écrit de trois heures. Le renouvellement de la certification est requis tous les trois ans. Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation professionnelle continue pendant la période de trois ans et payer des frais annuels.

Une liste complète des certifications en cybersécurité offertes par l'association (ISC)2 se trouve à la section 5.8.

2.9 ISACA

L'**ISACA,** anciennement Information Systems Audit and Control Association, est une association professionnelle internationale axée sur la gouvernance des TI. Elle compte plus de 140 000 membres et professionnels détenant des certifications ISACA dans 180 pays. L'association, répartie en plus de 200 sections locales, donne de la formation aux membres, en plus d'offrir des occasions de réseautage et de partage de ressources.

Les candidats doivent passer des examens écrits pour obtenir les certifications professionnelles de l'ISACA.
Ces certifications sont toutes valides pendant une période de trois ans. Pour conserver leur certification, les titulaires de titres de compétence doivent obtenir au moins 120 crédits de formation professionnelle continue sur la période de trois ans, et payer une cotisation annuelle, ou ils doivent repasser l'examen. Voici une liste des certifications en cybersécurité qu'offre le programme ISACA :

- La compétence **Certified Information Security Manager** (CISM) s'adresse aux responsables des équipes de cybersécurité et aux professionnels des TI chargés de la gestion, du développement et de la surveillance des systèmes de sécurité de l'information dans les applications d'entreprise, ou de l'élaboration de pratiques exemplaires en matière de sécurité organisationnelle. Outre l'examen écrit, les candidats doivent avoir un minimum de cinq années d'expérience dans le domaine de la sécurité. Ils doivent de plus présenter une demande écrite.
- La certification **Certified in Risk and Information Systems Control** (CRISC) démontre la capacité des candidats d'identifier, d'évaluer et de répondre aux risques liés aux TI. Les candidats doivent avoir trois années d'expérience en contrôle et en gestion des risques dans un environnement professionnel et être en mesure d'accomplir les tâches dans au moins deux domaines du programme CRISC. Pour cette certification, l'éducation ne remplace pas l'expérience professionnelle.
- La certification **Cyber Security Nexus Practitioner** (CSX-P) reconnaît les personnes qui peuvent agir en tant que premiers intervenants lors d'incidents de sécurité. Créée en 2015, cette certification évalue la capacité des candidats d'exécuter des vérifications de cybersécurité validées mondialement et couvrant les cinq fonctions de base du cadre de cybersécurité du NIST (NCFS pour *NIST Cyber Security Framework*) : identification, protection, détection, intervention et récupération. Pour obtenir la certification, les candidats doivent passer un examen de quatre heures basé sur le rendement et comportant des simulations d'incidents de sécurité. À la fin de la période de certification de trois ans, les titulaires doivent passer la version la plus récente de l'examen donnant droit au renouvellement de la certification.

Une liste complète des certifications en cybersécurité offertes par le programme ISACA se trouve à la section 5.9.

2.10 ITSM SOLUTIONS

Les certifications **itSM Solutions** s'appuient sur le cadre de cybersécurité du NIST (NCSF). Elles attestent que les professionnels de la cybersécurité possèdent les compétences de base nécessaires pour concevoir, établir, tester et gérer un programme de cybersécurité au moyen du NCSF.

- **NCSP Foundation :** Pour les cadres et les professionnels du milieu informatique et des affaires qui doivent connaître les principes de base du NCSF pour s'acquitter de leurs tâches.
- **NCSP Practitioner :** La formation enseigne comment créer et concevoir une technologie axée sur un programme de cybersécurité et un programme de gestion des risques. Elle aide à mieux comprendre le NCSF et à savoir comment l'adapter et l'opérationnaliser.

Une liste complète des certifications en cybersécurité offertes par le programme itSM Solutions se trouve à la section 5.10.

2.11 MCAFFEE INSTITUTE

Le **McAfee Institute** offre plusieurs certifications de comités reconnus par l'industrie dans les domaines du renseignement et des enquêtes en matière de cybersécurité, de la criminalistique numérique et des enquêtes sur la cryptomonnaie. Les titulaires de certification viennent des plus grands organismes gouvernementaux et d'application de la loi, comme la US Air Force et la US Army, le Federal Bureau of Investigation (FBI) et le New York Police Department (NYPD).

- La certification **Certified Cyber Intelligence Professional** (CCIP) a été conçue en parallèle avec le National Cyber Security Workforce Framework du département de la Sécurité intérieure. Cette certification démontre que des employés peuvent identifier des personnes d'intérêt, mener rapidement des enquêtes de cybersécurité et poursuivre en justice des cybercriminels. Les candidats doivent détenir un baccalauréat ou un diplôme de niveau supérieur, et avoir trois années d'expérience dans les secteurs des enquêtes, des TI, de la fraude, de l'application de la loi, de la criminalistique, de la justice pénale, du droit et de la prévention des pertes.

Une liste complète des certifications en cybersécurité offertes par le McAfee Institute se trouve à la section 5.11.

2.12 OFFENSIVE SECURITY

Offensive Security est une société internationale qui propose des services de consultation et de formation aux entreprises spécialisées dans la technologie. Elle offre, entre autres, des programmes de certification basés sur un cadre pratique du rendement, un accès à des laboratoires virtuels et des projets de source ouverte.

- La certification **Offensive Security Certified Professional** (OSCP) est considérée comme l'une des plus difficiles à obtenir en raison du degré de difficulté de son examen. Les candidats doivent réussir, en 24 heures, à attaquer et à pénétrer des systèmes opérationnels dans des conditions d'essai en laboratoire sécuritaires. En raison de son caractère pratique, cet examen s'adresse aux testeurs de pénétration possédant un solide bagage technique et en piratage contrôlé. Avant d'essayer de passer l'examen, les candidats doivent avoir suivi le cours de formation sur les tests de pénétration qu'offre Offensive Security. L'obtention de la certification permet aussi aux titulaires d'obtenir 40 crédits de formation continue (ISC)2. Contrairement à beaucoup des autres certifications en cybersécurité, la certification OSCP n'expire jamais.

Une liste complète des certifications en cybersécurité offertes par Offensive Security se trouve à la section 5.12.

2.13 PECB

PECB est un organisme de certification qui propose des services d'éducation et de certification selon la norme 17024 de l'Organisation internationale de normalisation (ISO pour *International Organization for Standardization*) et de la Commission électrotechnique internationale (CEI) (*Évaluation de la conformité – Exigences générales pour les organismes de certification procédant à la certification de personnes*), dans un large éventail de disciplines, y compris en sécurité de l'information et du nuage. Le réseau PECB est un réseau mondial de distributeurs, de revendeurs, de formateurs et de personnes certifiées, présent dans plus de 150 pays. PECB détient un agrément de l'International Accreditation Service (IAS) et du United Kingdom Accreditation Service (UKAS).

- La certification **Certified Lead Ethical Hacker** démontre la capacité des titulaires à évaluer légalement la sécurité des systèmes de leur organisation et à découvrir leurs vulnérabilités.

Une liste complète des certifications en cybersécurité offertes par le programme PECB se trouve à la section 5.13

2.14 SECO INSTITUTE

Le **Security & Continuity Institute** (SECO) est un institut européen qui offre des certifications de haut niveau touchant la sécurité et la continuité. Le programme de certification du SECO comporte sept volets de certification, chacun axé sur un domaine d'expertise particulier comme la sécurité des TI, la confidentialité des données et le piratage contrôlé. Les volets commencent au niveau de base (*Foundation*), et se poursuivent avec les niveaux praticien (*Practitioner*) et expert (*Expert*). Les candidats peuvent ensuite faire une demande de certification de niveau agent autorisé (*Certified Officer*) qui représente la plus haute distinction de compétence dans chacun des volets.

- La certification **Ethical Hacking Foundation** (S-EHF) en est une de premier échelon s'adressant aux professionnels qui désirent faire carrière dans le domaine. Les titulaires de cette certification comprennent les principes fondamentaux du piratage contrôlé et sont en mesure d'effectuer des tests de pénétration de base. Bien qu'il n'y ait pas de préalables pour cette certification, une connaissance de base de Linux est recommandée.
- La certification **Ethical Hacking Practitioner** (S-EHP) s'adresse aux professionnels qui ont déjà une connaissance solide des fondements du piratage contrôlé. L'obtention préalable de la certification S-EHF est recommandée. Les titulaires de cette certification ont démontré qu'ils comprennent pleinement le processus de test de pénétration et qu'ils connaissent les techniques courantes de test de pénétration.

Une liste complète des certifications en cybersécurité offertes par le programme SECO se trouve à la section 5.14.

3.0 CYBER CREDENTIALS COLLABORATIVE

L'organisation Cyber Credentials Collaborative (C3) a été créée en 2011 afin de promouvoir les avantages des certifications dans le développement des compétences des professionnels de la sécurité de l'information, partout dans le monde.
Elle offre du soutien sous forme de sensibilisation et préconise les compétences non rattachées à un fournisseur donné dans les secteurs de la sécurité de l'information, de la vie privée et d'autres domaines des TI. En proposant aux membres une plateforme qui favorise la collaboration sur des enjeux d'intérêt commun, C3 a pour objectif de promouvoir les carrières en TI, de mieux préparer la main-d'œuvre et de s'assurer que les certifications en TI sont conçues de façon à répondre aux besoins des gouvernements, des organisations privées et des établissements d'enseignement.

Les organismes de certification indiqués ci-dessous sont tous membres de l'organisation C3 :

- (ISC)2
- CertNexus
- CompTIA
- Global Information Assurance Certification
- ISACA

4.0 FORMATION ACCÉLÉRÉE EN CYBERSÉCURITÉ

Rogers Cybersecure Catalyst et le centre national d'innovation et de collaboration en cybersécurité de l'Université Ryerson ont récemment établi un partenariat avec le SANS Institute pour offrir un programme intensif de certification et de formation en cybersécurité. Le Accelerated Cybersecurity Training Program a été conçu afin de pallier le manque de professionnels en cybersécurité au Canada. Les participants à ce programme de sept mois obtiendront trois certifications GIAC :

- GIAC Foundational Cybersecurity Technologies (GFACT)
- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Incident Handler (GCIH)

Outre les certifications, les participants recevront un certificat délivré par Rogers Cybersecure Catalyst pour attester qu'ils ont achevé le programme, un mentorat professionnel avec des experts et des contacts avec des employeurs.

Le programme comprend également quatre volets qui visent à favoriser la participation des groupes sous-représentés au sein de l'industrie, comme les femmes, les nouveaux Canadiens et les travailleurs déplacés : Royal Bank of Canada (RBC) Women in Cyber, RBC New Careers in Cyber, Rogers New Canadians in Cyber et Peel Region Young Workers in Cyber.

Le programme est financé par le gouvernement du Canada, Rogers Communications et la Banque Royale du Canada (RBC).

5.0 LISTE ET DESCRIPTION DES CERTIFICATIONS EN CYBERSÉCURITÉ

Les tableaux ci-dessous dressent une liste plus complète des différentes certifications en cybersécurité offertes aux particuliers, classées par ordre alphabétique.

Avant d'essayer de passer l'examen de certification, les candidats peuvent acheter des cours de formation (en classe, en ligne ou individualisés) et d'autres matériels pédagogiques de préparation, comme des examens de simulation. Ils peuvent se les procurer auprès des vendeurs et des fournisseurs de cours de formation. Certains fournisseurs proposent des offres groupées de cours qui comprennent les frais d'examen. Pour en savoir plus sur les fournisseurs et les options de formation en vue de la certification, veuillez consulter le site Web de l'organisme de certification.

5.1 CERTNEXUS

Tableau 1 Liste et description des certifications de CertNexus[1]

Certification	Aperçu de la certification	Candidats ciblés

Certified First Responder (CFR)	• Atteste les connaissances des candidats en matière d'analyse des menaces, de conception d'environnements réseau et informatiques sécurisés, de détection proactive des défaillances réseau, d'intervention en cas d'incidents de cybersécurité et d'enquête sur ces incidents
	• Les candidats doivent avoir de trois à cinq années d'expérience de travail dans un environnement informatique, à protéger les systèmes d'information essentiels avant, pendant et après un incident
	• L'examen comporte 100 questions à choix multiples
	• Valide pendant trois ans
	• Deux options possibles pour le renouvellement de la certification :
	  ○ Passer la plus récente version de l'examen
	  ○ Obtenir 90 crédits de formation continue pendant la période de trois ans et payer les frais annuels
		• Administrateurs de système
		• Administrateurs de réseau
		• Intervenants en cas d'incident informatique
		• Enquêteurs en cybercriminalité
		• Vérificateurs des TI
		• Analystes de la sécurité
		• Analystes de réseau
		• Ingénieurs en sécurité des systèmes d'information

[1] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

Certified IoT Security Practitioner (CIoTSP)	• Atteste que les candidats possèdent les connaissances, les compétences et les capacités nécessaires pour sécuriser des environnements réseau pour les dispositifs de l'Internet des objets (IdO), analyser les vulnérabilités et déterminer les mesures de contrôle raisonnables à prendre pour contrer les menaces, surveiller efficacement les dispositifs de l'IdO et intervenir en cas d'incident • Les candidats doivent avoir une compréhension fondamentale des écosystèmes de l'IdO • L'examen comporte 100 questions à choix multiples	• Administrateurs de réseau • Ingénieurs en développement logiciel • Architectes de solutions • Analystes de la cybersécurité • Développeurs Web • Ingénieurs en nuage
Cyber Secure Coder (CSC)	• Démontre que les titulaires de cette certification ont été initiés aux vulnérabilités qui compromettent la sécurité, à l'identification et à l'atténuation de ces vulnérabilités, ainsi qu'aux stratégies de gestion des défauts de sécurité • Les candidats doivent avoir une certaine expérience en programmation (développement d'applications de bureau, mobiles, Web ou infonuagiques) • L'examen comporte 80 questions à choix multiples • Valide pendant trois ans	• Programmeurs en chef • Programmeurs débutants • Testeurs d'application • Testeurs de l'assurance de la qualité • Concepteurs de logiciels • Architectes de logiciels
CyberSafe	• Atteste que les candidats peuvent identifier les risques les plus courants associés à l'utilisation de technologies mobiles ou infonuagiques, et qu'ils peuvent assurer leur protection et celle de leur organisation contre des cybermenaces • Aucun préalable n'est exigé pour l'examen, mais les candidats doivent avoir une certaine expérience de la technologie de base (ordinateurs, téléphones intelligents, courriel, Internet, etc.) • L'examen ne comporte que dix questions et n'impose aucune limite de temps	• Utilisateurs finaux sans connaissances techniques de l'informatique
Microcompétence IRBIZ	• Atteste que les candidats possèdent les compétences nécessaires pour évaluer les menaces à la sécurité et intervenir en cas de telles menaces, et qu'ils sont aptes à faire fonctionner une plateforme d'analyse de la sécurité des systèmes et des réseaux • Les candidats doivent avoir une compréhension générale de la cybersécurité • L'examen comporte dix questions à choix multiples et de type vrai ou faux • Valide pendant trois ans	• Leaders et cadres en TI responsables d'assurer le respect de la législation en matière d'intervention en cas d'incident

5.2 CISCO SYSTEMS

Tableau 2 Liste et description des certifications de Cisco Systems[2]

Certification	Aperçu de la certification	Candidats ciblés
Cisco Certified CyberOps Associate	• Prépare les candidats à travailler avec des analystes associés de la cybersécurité au sein de centres des opérations de sécurité (COS) • Aucun préalable n'est exigé • Valide pendant trois ans • Le renouvellement de la certification exige d'avancer au prochain niveau de certification, d'accumuler des crédits de formation continue ou une combinaison de ces deux exigences	• Analystes de la cybersécurité • Membres de l'équipe du COS
Cisco Certified CyberOps Professional	• Nouvelle certification créée en 2021 • Atteste les connaissances des candidats en matière de sécurité infonuagique, de gestion des risques et d'analyse du renseignement sur les menaces • Aucun préalable n'est exigé • Valide pendant trois ans • Le renouvellement de la certification exige d'avancer au prochain niveau de certification, d'accumuler des crédits de formation continue ou une combinaison de ces deux exigences	• Analystes de la sécurité de l'information • Intervenants en cas d'incident informatique • Gestionnaires des incidents • Ingénieurs de réseau
Cisco Certified Network Associate Security (CCNA Security)	• Atteste la capacité des candidats de développer une infrastructure de sécurité, de reconnaître les menaces et les vulnérabilités auxquelles font face les réseaux, et d'atténuer les menaces à la sécurité • Les candidats doivent déjà avoir une certification valide Cisco CCENT, CCNA Routing and Switching ou toute certification CCIE • Valide pendant trois ans • Le renouvellement de la certification exige d'avancer au prochain niveau de certification, d'accumuler des crédits de formation continue ou une combinaison de ces deux exigences	• Administrateurs de réseau • Ingénieurs de réseau

[2] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

5.3 COMPTIA

Tableau 3 Liste et description des certifications de CompTIA[3]

Certification	Aperçu de la certification	Candidats ciblés
Advanced Security Practitioner (CASP+)	• Certification de niveau avancé • La seule certification axée sur le rendement qui s'adresse davantage aux praticiens qu'aux gestionnaires, travaillant à un niveau avancé de cybersécurité • Atteste les compétences de niveau avancé des candidats en gestion des risques, en opérations et architecture de sécurité intégrée, en recherche et en collaboration, ainsi qu'en intégration de la sécurité d'entreprise • Les candidats doivent avoir dix années d'expérience en administration des TI; dont cinq années d'expérience pratique en sécurité technique • L'examen comporte 90 questions à choix multiples et des questions axées sur le rendement • Valide pendant trois ans • Le renouvellement de la certification exige l'obtention de 75 crédits de formation continue pendant la période de trois ans	• Architectes de la sécurité • Analystes techniques en chef • Ingénieurs de la sécurité • Ingénieurs de la sécurité des applications
Cyber Security Analyst (CySA+)	• Certification d'analyste de la cybersécurité de niveau intermédiaire • La certification d'analyste de la sécurité la plus à jour qui couvre les menaces persistantes avancées dans un environnement de cybersécurité après 2014 • Atteste l'expertise des candidats en analyse de la sécurité, en détection des intrusions et en intervention • Les candidats doivent avoir trois ou quatre années d'expérience en sécurité de l'information ou dans un domaine connexe, et détenir une certification Network+ ou Security+, ou avoir des connaissances équivalentes • Approuvée par le département de la Défense des États-Unis • L'examen comporte 85 questions à choix multiples et des questions axées sur le rendement • Valide pendant trois ans	• Analystes de la sécurité des TI • Analystes du COS • Analystes de la cybersécurité • Analystes du renseignement sur les menaces • Ingénieurs de la sécurité • Analystes de la cybersécurité

[3] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

	• Le renouvellement de la certification exige l'obtention de 60 crédits de formation continue pendant la période de trois ans	
Network+	• Atteste les connaissances et les compétences des candidats en conception et en mise en œuvre de réseaux fonctionnels • Les préalables sont la certification A+ et neuf à douze mois d'expérience en réseautique • Elle s'avère utile pour les personnes désirant suivre une carrière en infrastructure des TI (dépannage, configuration, gestion des réseaux) • L'examen comporte 90 questions à choix multiples et des questions axées sur le rendement • Valide pendant trois ans • Le renouvellement de la certification exige l'obtention de 30 crédits de formation continue pendant la période de trois ans	• Postes de premier échelon • Administrateurs de réseau débutants • Techniciens en informatique • Ingénieurs de système débutants
PenTest+	• Certification de niveau intermédiaire • Atteste que les candidats ont les capacités et les compétences nécessaires pour tester des dispositifs dans de nouveaux environnements (en nuage ou mobiles), ainsi que des ordinateurs et des serveurs traditionnels • Les candidats doivent avoir trois ou quatre années d'expérience en sécurité de l'information ou une expérience connexe • L'examen comporte 85 questions à choix multiples et des questions axées sur le rendement • Le renouvellement de la certification exige l'obtention de 60 crédits de formation continue pendant la période de trois ans	• Testeurs de pénétration • Testeurs de vulnérabilité • Analystes de la sécurité • Opérateurs de la sécurité réseau
Security+	• Certification de premier échelon • Atteste les compétences de base en cybersécurité nécessaires pour exécuter les fonctions essentielles en sécurité • Les titulaires de la certification sont des experts en gestion des menaces, en contrôle d'accès réseau et en infrastructure de sécurité • Les candidats doivent posséder deux années d'expérience en sécurité réseau et avoir obtenu la certification Network+ • Valide pendant trois ans • Le renouvellement de la certification exige l'obtention de 50 crédits de formation continue pendant la période de trois ans	• Administrateurs de système • Administrateurs de réseau • Administrateurs de la sécurité • Vérificateurs des TI débutants • Testeurs de pénétration • Ingénieurs de la sécurité

5.4 COUNCIL FOR REGISTERED ETHICAL SECURITY TESTERS (CREST)

Tableau 4 Liste et description des certifications de CREST[4]

Certification	Aperçu de la certification	Candidats ciblés
Certified Infrastructure Tester	• Atteste que les candidats ont les capacités requises pour accéder à un réseau afin de trouver des failles et des vulnérabilités dans la couche du réseau et du système d'exploitation • L'examen comporte une partie écrite à choix multiples et deux volets pratiques de six heures • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent repasser l'examen	• Administrateurs de système • Testeurs de pénétration • Gestionnaires de la sécurité de l'information • Gestionnaires des incidents
Certified Web Application Tester	• Évalue la capacité des candidats de trouver des vulnérabilités dans des applications Web sur mesure • L'examen comporte une partie écrite à choix multiples et deux volets pratiques de six heures • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent repasser l'examen	• Testeurs de pénétration • Spécialistes du piratage contrôlé
CREST Certified Wireless Specialist (CCWS)	• Atteste les connaissances et les compétences des candidats liées à la réalisation d'examens de la sécurité sans fil, et aux technologies d'identification par radiofréquences (RFID), Bluetooth et autres technologies sans fil traditionnelles • Le préalable exigé est d'avoir réussi l'un des examens de certification CREST de base • Examen en deux volets : 120 questions à choix multiples et tâches pratiques • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent repasser l'examen	• Professionnels de haut niveau

[4] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

Practitioner Security Analyst (CPSA)	• Certification de premier échelon • Atteste les connaissances des candidats liées à l'évaluation des systèmes d'exploitation et des services réseau courants à un niveau de base • Les candidats doivent démontrer qu'ils possèdent les connaissances nécessaires pour faire des analyses de base des vulnérabilités dans les infrastructures et les applications Web, et pour interpréter les résultats afin de localiser les failles de sécurité • L'examen comporte des questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent repasser l'examen	• Administrateurs de système • Testeurs de pénétration • Gestionnaires de la sécurité de l'information • Gestionnaires des incidents
Registered Penetration Tester (CRT)	• Atteste la capacité des candidats d'effectuer des tâches de base relatives à l'évaluation des vulnérabilités et aux tests de pénétration • Lors de l'examen, les candidats doivent trouver des vulnérabilités connues dans des technologies de réseaux, d'applications et de bases de données courantes; l'examen comporte une section à choix multiples • La certification CPSA est un préalable • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent repasser l'examen	• Administrateurs de système • Testeurs de pénétration • Gestionnaires de la sécurité de l'information • Gestionnaires des incidents

5.5 CERTIFIED WIRELESS NETWORK PROFESSIONS (CWNP)

Tableau 5 Liste et description des certifications de CWNP[5]

Certification	Aperçu de la certification	Candidats ciblés
Certified Wireless Network Expert (CWNE)	• Certification de niveau avancé • On compte moins de 200 titulaires de la certification CWNE dans le monde • Atteste que les candidats maîtrisent toutes les notions pertinentes pour leur permettre d'administrer, d'installer, de configurer et de concevoir des réseaux sans fil, puis de résoudre les problèmes qui touchent ces réseaux, et qu'ils ont une connaissance approfondie de l'analyse de protocole, de la détection et de la prévention des intrusions • Les candidats doivent avoir trois années d'expérience dans les réseaux Wi-Fi • Les exigences relatives à la demande comprennent une lettre d'appui de la part de trois personnes et la présentation de documents (dissertations et publications) • Les candidats doivent passer quatre examens et effectuer des déploiements de WLAN commerciaux • Valide pendant trois ans • Le renouvellement de la certification exige le paiement des frais de renouvellement et l'obtention de 60 crédits de formation continue sur une période de trois ans	• Personnes occupant des postes supérieurs liés au WLAN
Certified Wireless Security Professional (CWSP)	• Atteste la capacité des candidats d'évaluer les vulnérabilités d'un réseau et d'aider à prévenir les attaques, d'effectuer des vérifications de sécurité de WLAN et de mettre en œuvre des solutions de surveillance de la conformité • Les candidats doivent déjà avoir obtenu la certification Certified Wireless Network Administrator (CWNA) • L'examen comporte 60 questions à choix multiples • Valide pendant trois ans • Le renouvellement de la certification exige d'avoir une certification CWNA valide et de passer la version actuelle de l'examen ou de passer l'examen CWNE	• Professionnels des réseaux TI

[5] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

5.6 EC-COUNCIL

Tableau 6 Liste et description des certifications de l'EC-Council[6]

Certification	Aperçu de la certification	Candidats ciblés
Certified Application Security Engineer (CASE)	• Deux volets : JAVA et .NET • Atteste que les candidats possèdent les compétences et les connaissances essentielles en sécurité qui sont nécessaires tout au long d'un cycle de développement logiciel type, en mettant l'accent sur l'importance de la mise en œuvre de pratiques et de méthodologies sécurisées dans l'environnement actuel d'exploitation non sécurisé • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • Valide pendant trois ans • Les examens comportent 50 questions à choix multiples • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Personnes responsables du développement, de la mise à l'essai, de la gestion ou de la protection d'une vaste gamme d'applications • Concepteurs qui aspirent à devenir des ingénieurs, des analystes ou des testeurs de la sécurité des applications
Certified Chief Information Security Officer (CCISO)	• Le programme CCISO reconnaît l'expérience concrète nécessaire pour réussir aux plus hauts échelons de la sécurité de l'information • Il vise à former des cadres supérieurs de haut niveau en sécurité de l'information • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins cinq années d'expérience de travail dans chacun des cinq domaines du programme CCISO et doivent présenter une demande d'admission à l'examen • Les candidats qui suivent la formation officielle doivent avoir 5 années d'expérience de travail dans au moins trois des domaines du programme CCISO	• Dirigeants principaux de la sécurité de l'information

[6] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

	• L'examen comporte 150 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	
Certified Cloud Security Engineer (CCSE)	• Atteste la capacité des candidats de créer et de mettre en œuvre des stratégies de sécurité pour protéger les applications et les infrastructures infonuagiques • Le programme offre des concepts de sécurité infonuagique propres à des fournisseurs précis et d'autres qui ne sont aucunement liés à des fournisseurs précis • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • L'examen comporte 125 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Analystes infonuagiques • Analystes de la cybersécurité • Administrateurs de la sécurité réseau • Administrateurs et ingénieurs infonuagiques • Professionnels des opérations de gestion infonuagique et réseau
Certified Cybersecurity Technician (CCT)	• Compétence de premier échelon en cybersécurité pour les personnes qui désirent entamer une carrière en cybersécurité ou en TI • Atteste les compétences techniques pratiques des candidats • Aucun préalable n'est exigé • L'examen comporte 60 questions à choix multiples et dix scénarios pratiques • Valide pendant trois ans • La certification CCT ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour *EC-Council Continuing Education*). Pour renouveler leur certification, les candidats doivent repasser l'examen	• Personnes qui désirent assumer des fonctions de premier échelon associées à la cybersécurité ou à la sécurité de l'information • Techniciens en cybersécurité • Administrateurs et ingénieurs de réseau • Spécialistes et gestionnaires du soutien TI • Techniciens et coordonnateurs de réseau
Certified Ethical Hacker (CEH) – ANSI	• Compétence de premier échelon • Atteste que les candidats savent comment trouver les faiblesses et les vulnérabilités dans les systèmes ainsi qu'utiliser les mêmes outils et connaissances que ceux d'un	• Agents de la sécurité de l'information

	pirate malveillant, mais de façon légitime et légale pour évaluer la posture de sécurité des systèmes • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • Ce titre de compétence atteste les compétences des candidats, d'un point de vue neutre, en matière de sécurité réseau dans le domaine du piratage contrôlé • L'examen comporte 125 questions • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Agents, gestionnaires, ingénieurs ou spécialistes en sécurité de l'assurance de l'information • Administrateurs de site • Vérificateurs de la sécurité de l'information • Analystes des risques, des menaces et des vulnérabilités
Certified Ethical Hacker (CEH) – Master	• Les candidats détiennent les certifications ANSI et Practical CEH • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Responsables de la sécurité • Vérificateurs des TI • Administrateurs de site
Certified Ethical Hacker (CEH) – Practical	• Atteste les connaissances des candidates liées aux techniques de piratage contrôlé telles que l'identification du vecteur de menace, le balayage réseau, la détection du système d'exploitation, l'analyse des vulnérabilités, le piratage de systèmes, le piratage d'applications Web, etc. • Aucun préalable n'est exigé, mais cette certification est généralement la prochaine étape après avoir obtenu la certification CEH ANSI • Examen de six heures comportant 20 études de cas • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Analystes ou administrateurs de la sécurité de l'information • Agents, gestionnaires, ingénieurs ou spécialistes en sécurité de l'assurance de l'information • Analystes des risques, des menaces et des vulnérabilités • Administrateurs de système • Administrateurs ou ingénieurs de réseau
Certified Network Defender (CND) – ANSI	• Démontre que les candidats possèdent l'expertise requise pour protéger le réseau contre les menaces, détecter les menaces sur le réseau et intervenir face à celles-ci	• Administrateurs de TI et de réseau

	• Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité des TI et doivent présenter une demande d'admission à l'examen • L'examen comporte 100 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Analystes de la sécurité des données • Ingénieurs et techniciens de réseau
Certified Penetration Testing Professional (CPENT)	• Atteste la capacité des candidats d'exécuter des tests de pénétration efficaces dans un environnement réseau d'entreprise, ce qui comprend la conduite d'activités d'attaque, d'exploitation, d'évitement et de défense • Aucun préalable n'est exigé • L'examen de 24 heures consiste en une évaluation pratique et la rédaction d'un rapport sur les tests de pénétration • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Testeurs de pénétration • Spécialistes du piratage contrôlé • Administrateurs de coupe-feu et de serveur réseau • Professionnels de l'évaluation des risques • Ingénieurs et analystes de la sécurité • Consultants en sécurité de l'information
Certified Secure Computer User (CSCU)	• Atteste que les candidats peuvent cerner des menaces à la sécurité de l'information et les atténuer efficacement • Aucun préalable n'est exigé • L'examen comporte 50 questions à choix multiples • Valide pendant trois ans • La certification CSCU ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour *EC-Council Continuing Education*). Pour renouveler leur certification, les candidats doivent repasser l'examen	• Toute personne âgée de treize ans et plus qui utilise un ordinateur pour travailler, étudier ou jouer • Utilisateurs finaux
Certified SOC Analyst (CSA)	• Atteste que les candidats ont une pleine compréhension des tâches que doit accomplir un analyste du centre des opérations de sécurité (COS) • Le programme met l'accent sur la création de nouvelles possibilités de carrière pour les candidats en leur donnant les compétences techniques, les connaissances et les	• Analystes du COS de niveau 1 et de niveau 2 • Analystes de la cybersécurité • Futurs analystes du COS

	capacités accrues qui sont en demande pour contribuer dynamiquement à une équipe du COS • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir une année d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • L'examen comporte 100 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Administrateurs ou ingénieurs de la sécurité et de réseau • Analystes et techniciens en défense des réseaux
Certified Threat Intelligence Analyst (CTIA)	• Démontre que les candidats ont les compétences pour cerner, atténuer et contrer les risques opérationnels en transformant les menaces internes et externes en entités malveillantes quantifiables • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • L'examen comporte 50 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Spécialistes du piratage contrôlé • Analystes de la criminalistique numérique et de logiciels malveillants • Analystes du renseignement sur les menaces • Membres de l'équipe d'intervention en cas d'incident • Professionnels du COS • Gestionnaires, architectes, analystes, ingénieurs et praticiens de la sécurité
Computer Hacking Forensics Investigator (CHFI) – ANSI	• Atteste que les candidats possèdent les compétences nécessaires pour enquêter de façon proactive sur les menaces de sécurité complexes, ce qui comprend l'enquête, l'enregistrement et le signalement des cybercrimes pour prévenir les attaques • Programme en laboratoire non rattaché à un fournisseur donné • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • L'examen comporte 150 questions à choix multiples	• Gestionnaires des TI • Fournisseurs de services de criminalistique numérique • Responsables de l'application de la loi • Responsables de la défense et de la sécurité

	• Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Organismes gouvernementaux
Digital Forensics Essentials (DFE)	• Compétence de premier échelon qui aide les candidats à renforcer leurs compétences et leur expertise en criminalistique numérique et en sécurité de l'information, de façon à ajouter de la valeur à leur milieu de travail et à leur employeur • Aucun préalable n'est exigé • L'examen comporte 75 questions à choix multiples • Valide pendant trois ans • La certification DFE ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour *EC-Council Continuing Education*). Pour renouveler leur certification, les candidats doivent repasser l'examen	• Personnes qui désirent assumer des fonctions de premier échelon associées à la cybersécurité ou à la sécurité de l'information • Techniciens du centre d'assistance • Administrateurs de réseau • Techniciens de réseau • Spécialistes du soutien informatique
EC-Council Disaster Recovery Professional (EDRP)	• Atteste la capacité des candidats de planifier, de mettre en œuvre et de tenir à jour un plan de continuité des activités et de reprise après sinistre • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • L'examen comporte 150 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Directeurs des TI et dirigeants principaux de la sécurité de l'information • Gestionnaires et consultants en matière de risques liés aux TI • Consultants en continuité des activités et en reprise après sinistre • Professionnels des TI dans les domaines de la reprise après sinistre, de la continuité des activités et de l'administration de système

EC-Council Certified Encryption Specialist (ECES)	• Certification de premier échelon qui initie les professionnels et les étudiants à la cryptographie en inculquant les rudiments de la cryptographie à clé symétrique moderne • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins une année d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • L'examen comporte 50 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Cryptanalystes • Cryptographes • Spécialistes du piratage contrôlé • Testeurs de pénétration
EC-Council Certified Incident Handler (ECIH) - ANSI	• Atteste que les candidats possèdent les connaissances et les compétences nécessaires pour gérer efficacement les conséquences à la suite d'une brèche de sécurité en réduisant les répercussions de l'incident sur les plans financier et de la réputation • Programme spécialisé • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins une année d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • L'examen comporte 100 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Administrateurs de l'évaluation des risques • Administrateurs et ingénieurs de système • Gestionnaires des TI et des réseaux • Ingénieurs de la sécurité des applications • Analystes et enquêteurs en criminalistique numérique • Analystes du COS • Testeurs de pénétration
Ethical Hacking Essentials (EHE)	• Compétence de premier échelon qui inculque les rudiments du piratage contrôlé et des tests de pénétration, et qui prépare les candidats à une carrière en cybersécurité • Aucun préalable n'est exigé • L'examen comporte 75 questions à choix multiples • Valide pendant trois ans • La certification ECE ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour *EC-Council Continuing Education*). Pour renouveler leur certification, les candidats doivent repasser l'examen	• Personnes qui désirent assumer des fonctions de premier échelon associées à la cybersécurité ou à la sécurité de l'information • Techniciens du centre d'assistance • Administrateurs de réseau • Techniciens de réseau

		• Spécialistes du soutien informatique
Industrial Control Systems and Supervisory Control and Data Acquisitions (ICS/SCADA) Cybersecurity	• Atteste les connaissances rudimentaires des candidats en matière de sécurité et leur capacité à défendre une architecture réseau • Les candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir une année d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen • L'examen comporte 75 questions à choix multiples • Valide pendant trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels	• Administrateurs et ingénieurs de système • Responsables des systèmes SCADA • Analystes des systèmes opérationnels assurant le soutien des interfaces SCADA • Consultants en sécurité réalisant les évaluations de la sécurité des systèmes SCADA ou des systèmes de contrôle industriels (SCI)
Network Defense Essentials (NDE)	• Compétence de premier échelon qui inculque les concepts fondamentaux de la sécurité de l'information et de la défense réseau, et qui est destiné principalement aux candidats qui désirent faire carrière en cybersécurité • Aucun préalable n'est exigé • L'examen comporte 75 questions à choix multiples • Valide pendant trois ans • La certification NDE ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour *EC-Council Continuing Education*). Pour renouveler leur certification, les candidats doivent repasser l'examen	• Personnes qui désirent assumer des fonctions de premier échelon associées à la cybersécurité ou à la sécurité de l'information • Techniciens du centre d'assistance • Administrateurs de réseau • Techniciens de réseau • Spécialistes du soutien informatique

5.7 GLOBAL INFORMATION ASSURANCE CERTIFICATION (GIAC)

Tableau 7 Liste et description des certifications de GIAC[7]

Certification	Aperçu de la certification	Candidats ciblés
GIAC Advanced Smartphone Forensics (GASF)	• Certification de niveau avancé • Atteste que les candidats possèdent les qualifications nécessaires pour effectuer des examens d'informatique judiciaire sur des appareils, comme des téléphones mobiles et des tablettes, et qu'ils ont une connaissance des principes de base en ce qui a trait aux interventions judiciaires sur les appareils mobiles, à l'analyse de système de fichiers d'appareils, au comportement des applications mobiles, à l'analyse des artefacts d'événement, ainsi qu'à l'identification et à l'analyse de maliciels qui s'attaquent aux appareils mobiles • Valide pendant quatre ans • L'examen comporte 75 questions • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Analystes de la criminalistique numérique et de logiciels malveillants • Analystes et enquêteurs judiciaires de la cyberdéfense • Testeurs de pénétration • Concepteurs d'exploit • Analystes en menaces informatiques
GIAC Assessing and Auditing Wireless Networks (GAWN)	• Certification de niveau avancé • Atteste que les candidats possèdent des connaissances des divers mécanismes de sécurité pour les réseaux sans fil, des outils et des techniques utilisés pour l'évaluation et l'exploitation des faiblesses, et des techniques servant à l'analyse des réseaux sans fil • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Vérificateurs • Spécialistes du piratage contrôlé • Testeurs de pénétration • Professionnels de la sécurité réseau • Ingénieurs de système sans fil

[7] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

GIAC Certified Detection Analyst (GCDA)	• Certification de niveau avancé • Atteste la capacité des candidats de recueillir, d'analyser et d'utiliser de façon tactique des sources de données modernes sur les réseaux et les terminaux pour détecter les activités malveillantes ou non autorisées • Les titulaires d'une certification GCDA ont les compétences pour occuper des postes de leadership en gestion de l'information et des événements de sécurité (GIES) • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Analystes de la sécurité • Architectes de la sécurité • Ingénieurs principaux de la sécurité • Ingénieurs et analystes du COS • Enquêteurs spécialisés dans les cybermenaces
GIAC Certified Enterprise Defender (GCED)	• Certification de niveau avancé • Atteste les connaissances et les compétences des candidats dans les domaines de l'infrastructure réseau de défense, de l'analyse de paquets, des tests de pénétration, du traitement des incidents et de la suppression de maliciels • L'examen comporte 115 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Intervenants en cas d'incident informatique • Testeurs de pénétration • Ingénieurs et analystes du COS • Professionnels de la sécurité réseau
GIAC Certified Forensic Analyst (GCFA)	• Certification de niveau avancé • Atteste que les candidats possèdent les connaissances, les compétences et les capacités nécessaires pour effectuer des enquêtes officielles sur des incidents et traiter des scénarios de gestion de niveau avancé • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Membres de l'équipe d'intervention en cas d'incident • Analystes du COS • Agents fédéraux et professionnels chargés de l'application de la loi • Analystes de la criminalistique numérique
GIAC Certified Forensic Examiner (GCFE)	• Certification de niveau intermédiaire	• Professionnels de la sécurité de l'information • Membres d'organismes d'application de la loi

	• Atteste les connaissances des candidats en analyse de la criminalistique informatique, ce qui comprend les compétences essentielles nécessaires pour recueillir et analyser des données à partir de systèmes d'exploitation Windows • L'examen comporte 115 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Analystes de la criminalistique numérique et de logiciels malveillants • Analystes et enquêteurs judiciaires de la cyberdéfense
GIAC Certified Incident Handler (GCIH)	• Certification de niveau intermédiaire • Atteste la capacité des candidats de détecter les incidents, d'intervenir en cas d'incident et de résoudre les incidents liés à la sécurité informatique au moyen d'une vaste gamme de compétences essentielles en sécurité • L'examen comporte de 100 à 150 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Membres de l'équipe d'intervention en cas d'incident • Intervenants en cas d'incident lié à la cyberdéfense
GIAC Certified Intrusion Analyst (GCIA)	• Certification de niveau avancé • Atteste les connaissances des candidats en matière de surveillance de réseau et d'hôte, d'analyse de trafic et de détection d'intrusion • Les titulaires de la certification sont aptes à configurer et à surveiller des systèmes de détection d'intrusion, et à analyser le trafic réseau • L'examen comporte de 100 à 150 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Personnes responsables de la surveillance de réseau et d'hôte, de l'analyse de trafic et de la détection d'intrusion • Analystes en menaces informatiques • Analystes du centre des opérations de sécurité • Membres de l'équipe d'intervention en cas d'incident
GIAC Certified Web Application Defender (GWEB)	• Certification de niveau avancé • Démontre que les candidats maîtrisent les connaissances et les compétences en matière de sécurité dont ils ont besoin pour traiter les erreurs courantes d'applications Web qui occasionnent la majorité des problèmes de sécurité • L'examen comporte 75 questions	• Développeurs d'applications • Analystes de la sécurité des applications • Architectes d'applications • Testeurs de pénétration

	• Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Personnes dont les responsabilités exigent la conformité aux normes de l'industrie des cartes de paiement (PCI pour *Payment Card Industry*)
GIAC Certified Windows Security Administrator (GCWN)	• Certification de niveau avancé • Atteste la capacité des candidats de sécuriser les clients et les serveurs Windows, et leurs connaissances en matière de configuration et de gestion de la sécurité des systèmes d'exploitation et des applications Microsoft • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Personnes responsables de l'installation, de la configuration et de la sécurisation des clients et des serveurs Microsoft Windows
GIAC Continuous Monitoring Certification (GMON)	• Certification de niveau avancé • Atteste la capacité des candidats de prévenir les intrusions et de détecter rapidement les activités suspectes • L'examen comporte 115 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Architectes de la sécurité • Analystes et gestionnaires du COS • Gestionnaires de la sécurité technique • Ingénieurs de la sécurité
GIAC Critical Controls Certification (GCCC)	• Certification de niveau avancé • La seule certification basée sur les contrôles de sécurité essentiels qui font appel à une approche priorisée de la sécurité fondée sur les risques • Atteste que les candidats possèdent les connaissances et les compétences nécessaires pour mettre en œuvre et exécuter les contrôles de sécurité essentiels recommandés par le Council on Cybersecurity, et pour effectuer des vérifications en fonction de la norme • Aucun préalable n'est exigé • L'examen comporte 75 questions	• Administrateurs des TI • Ingénieurs de la sécurité réseau • Fournisseurs de services de sécurité • Vérificateurs de la sécurité, dirigeants principaux de l'information et responsables de l'évaluation des risques

	• Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	
GIAC Critical Infrastructure Protection (GCIP)	• Certification de niveau avancé • Atteste que les candidats ont les connaissances et les compétences nécessaires pour comprendre la réglementation de la North American Electric Reliability Corporation (NERC) relative à la protection des infrastructures essentielles (CIP pour *Critical Infrastructure Protection*) et pour préparer des stratégies de mise en œuvre pratiques afin d'assurer la conformité à la réglementation • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Analystes des opérations de sécurité • Chefs et gestionnaires d'équipe • Analystes d'intervention en cas d'incident • Praticiens de la cybersécurité des systèmes de contrôle industriels (SCI)
GIAC Cyber Threat Intelligence (GCTI)	• Certification de niveau avancé • Atteste la capacité des candidats de comprendre et d'analyser des scénarios d'évaluation des menaces complexes; d'identifier, de créer et de valider les besoins en renseignement par la modélisation des menaces • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Membres de l'équipe d'intervention en cas d'incident • Analystes en menaces informatiques • Analystes du renseignement
GIAC Defending Advanced Threats (GDAT)	• Certification de niveau avancé • Atteste que les candidats ont des connaissances avancées de la façon dont les adversaires s'attaquent aux réseaux et des contrôles de sécurité efficaces pour les arrêter • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Architectes de la sécurité • Ingénieurs de la sécurité • Gestionnaires de la sécurité technique

GIAC Defensible Security Architecture (GDSA)	• Certification de niveau avancé • Atteste que les candidats ont les compétences pratiques et concrètes nécessaires pour s'occuper des approches axées sur les réseaux et les données d'une architecture de sécurité défendable, qu'ils peuvent se charger du renforcement des applications dans la pile TCP/IP (*Transmission Control Protocol/Internet Protocol*) ainsi que de la création d'un environnement sécurisé au moyen de nuages privés, hybrides ou publics • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Architectes de la sécurité • Ingénieurs de réseau • Analystes de la sécurité • Enquêteurs spécialisés dans les cybermenaces • Ingénieurs principaux de la sécurité • Analystes de la sécurité
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	• Certification de niveau avancé • Atteste la capacité des candidats de trouver et d'atténuer les vulnérabilités informatiques majeures dans des systèmes et des réseaux • L'examen comporte de 55 à 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Testeurs de vulnérabilités • Analystes de la sécurité • Analystes de l'évaluation des vulnérabilités
GIAC Information Security Fundamentals (GISF)	• Certification de niveau débutant • Atteste que les candidats ont des connaissances en ce qui a trait aux bases de la sécurité, aux fonctions informatiques et à la réseautique, à la cryptographie de base et aux technologies de cybersécurité • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Membres de la direction • Agents de la sécurité de l'information • Administrateurs de système • Professionnels qui ont besoin d'une introduction aux principes de base de la cybersécurité
GIAC Information Security Professional (GISP)	• Certification de niveau intermédiaire pour gestionnaires et leaders • Atteste que les candidats ont des connaissances dans les huit domaines de connaissance en matière de cybersécurité : sécurité des actifs, sécurité des télécommunications et des réseaux, gestion de l'identité et de l'accès, gestion de la	• Administrateurs de système • Administrateurs de la sécurité informatique • Administrateurs de réseau • Gestionnaires de la sécurité

	sécurité et des risques, évaluation de la sécurité et tests de sécurité, ingénierie de sécurité, opérations de sécurité, et sécurité du développement de logiciels • Les candidats doivent avoir une certaine expérience des systèmes d'information et de la réseautique • L'examen comporte 250 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	
GIAC Mobile Device Security Analyst (GMOB)	• Certification de niveau avancé • Atteste que les candidats sont aptes à sécuriser adéquatement des dispositifs mobiles ayant accès à de l'information vitale • Démontre que les candidats ont les connaissances nécessaires pour évaluer et gérer des dispositifs mobiles et la sécurité des applications, et pour atténuer les risques que posent les maliciels et les dispositifs volés • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Analystes de la sécurité de l'information • Testeurs de pénétration • Spécialistes du piratage contrôlé • Administrateurs de système et de réseau
GIAC Network Forensic Analyst (GNFA)	• Certification de niveau avancé • Atteste la capacité des candidats de procéder à des examens à l'aide d'une analyse d'artefacts judiciaires de réseau • L'examen comporte 50 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Membres d'organismes d'application de la loi • Analystes de la criminalistique numérique et de logiciels malveillants • Analystes de la cyberdéfense • Membres de l'équipe d'intervention en cas d'incident • Membres de l'équipe du COS
GIAC Penetration Tester (GPEN)	• Certification de niveau avancé	• Testeurs de pénétration • Concepteurs d'exploit

	• Atteste que les candidats ont la capacité d'effectuer adéquatement des tests de pénétration en se servant de techniques et de méthodologies répondant à des pratiques exemplaires • L'examen comporte jusqu'à 115 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Personnel de la sécurité réseau • Spécialistes du piratage contrôlé
GIAC Response and Industrial Defence (GRID)	• Certification de niveau avancé • Démontre que les candidats comprennent l'approche de défense active et les attaques propres aux SCI, et savent comment ces attaques guident les stratégies d'atténuation • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Chefs d'équipe et membres de l'équipe d'intervention en cas d'incident visant les systèmes de contrôle industriels (SCI) • Chefs d'équipe et analystes du centre des opérations de sécurité • Défenseurs actifs
GIAC Reverse Engineering Malware (GREM)	• Certification de niveau avancé • Atteste que les candidats possèdent les connaissances et les compétences nécessaires pour faire la rétro-ingénierie des maliciels qui ciblent des plateformes courantes comme Microsoft Windows et des navigateurs Web • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Administrateurs de système et de réseau • Vérificateurs • Gestionnaires de la sécurité • Enquêteurs judiciaires
GIAC Security Essentials Certification (GSEC)	• Certification de premier échelon • Atteste que les connaissances des candidats en sécurité de l'information vont au-delà des notions simples de terminologie et de concepts • Les titulaires ont de grandes compétences en défense active, en cryptographie, en politiques et plans relatifs à la sécurité, en traitement des incidents et en protection de réseau • L'examen comporte 180 questions	• Professionnels de la sécurité

	• Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	
GIAC Security Expert (GSE)	• On compte moins de 250 titulaires de la certification GSE dans le monde • Atteste que les candidats maîtrisent la vaste gamme de compétences dont ont besoin les meilleurs consultants et praticiens de la sécurité • Les préalables sont les certifications GSEC, GCIH, GCIA avec deux certifications de catégorie Or • L'examen comporte deux volets : 24 questions pratiques basées sur les machines virtuelles et un laboratoire pratique • Valide pendant quatre ans • Le renouvellement de la certification exige de passer la version actuelle de l'examen • Le renouvellement de la certification GSE permet de renouveler toutes les autres certifications GIAC actives	• Meilleurs consultants et praticiens de la sécurité
GIAC Security Leadership (GSLC)	• Certification de niveau avancé pour gestionnaires et leaders • Atteste les connaissances des candidats en matière de gouvernance et de contrôles techniques axés sur la protection et la détection des problèmes de sécurité ainsi que l'intervention face à ceux-ci • L'examen comporte 115 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Gestionnaires et superviseurs des équipes de la sécurité de l'information • Gestionnaires des TI
GIAC Systems and Network Auditor (GSNA)	• Certification de niveau avancé pour gestionnaires et leaders • Atteste la capacité des candidats d'appliquer des techniques d'analyse des risques de base et d'effectuer des vérifications techniques des systèmes d'information essentiels • L'examen comporte 115 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Personnel technique responsable de sécuriser et de vérifier les systèmes d'information • Vérificateurs • Administrateurs de réseau • Gestionnaires des équipes de vérification ou de sécurité

GIAC Web Application Penetration Tester (GWAPT)	• Certification de niveau avancé • Atteste que les candidats ont la capacité de mieux sécuriser les organisations au moyen de tests de pénétration et grâce à une compréhension des problèmes de sécurité liés aux applications Web • Démontre que les candidats ont une connaissance des exploits relatifs aux applications Web et des méthodologies de test de pénétration • L'examen comporte 75 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Testeurs de pénétration • Testeurs de vulnérabilités • Analystes de la sécurité • Analystes de l'évaluation des vulnérabilités • Spécialistes du piratage contrôlé • Concepteurs de site Web
Global Industrial Cyber Security Professional (GICSP)	• Certification de niveau avancé • Évalue les connaissances et la compréhension de base des candidats au sein d'un ensemble varié de professionnels qui conçoivent ou prennent en charge des systèmes de contrôle et partagent la responsabilité de la sécurité de ces environnements • Aucun préalable n'est exigé • L'examen comporte 115 questions • Valide pendant quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue pendant la période de quatre ans	• Ingénieurs de la sécurité • Gestionnaires d'entreprise • Analystes de la sécurité

5.8 INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM

Tableau 8 Liste et description des certifications de l'association (ISC)2[8]

Certification	Aperçu de la certification	Candidats ciblés
Certified Cloud Security Professional (CCSP)	• Développée en collaboration avec la Cloud Security Alliance (CSA) • Reconnaît les leaders de la sécurité des TI et de l'information qui ont des connaissances et des compétences en architecture, en conception, en exploitation et en orchestration des services de sécurité infonuagique • Les candidats doivent avoir un minimum de cinq années d'expérience professionnelle en TI, dont au moins trois années en sécurité de l'information et une année dans l'un des six domaines du corpus de connaissances communes menant à la certification CCSP • L'examen comporte 125 questions à choix multiples • Valide pendant trois ans • Le renouvellement de la certification exige l'obtention de 90 crédits de formation continue pendant une période de trois ans	• Architectes d'entreprise • Ingénieurs de système • Architectes de système • Administrateurs de la sécurité • Leaders de la sécurité des TI et de l'information
Certified Information Systems Security Professional (CISSP)	• Certification de niveau avancé • Les candidats doivent avoir au moins cinq années d'expérience professionnelle dans au moins deux des huit domaines du corpus de connaissances communes offert par l'association (ISC)2, ou quatre années d'expérience professionnelle et un diplôme universitaire ou tout autre certificat accrédité • L'examen comporte de 100 à 150 questions utilisant la stratégie du test adaptatif informatisé (TAI) • Valide pendant trois ans • Le renouvellement de la certification exige l'obtention de 120 crédits de formation professionnelle continue pendant une période de trois ans • Trois concentrations sont également offertes aux titulaires d'une certification CISSP valide :	• Dirigeants principaux de la sécurité de l'information • Dirigeant principal de la sécurité • Analystes et vérificateurs de la sécurité • Directeurs de la sécurité • Directeurs ou gestionnaires des TI

[8] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

	○ CISSP-ISSAP (architecture) ○ CISSP-ISSEP (ingénierie) ○ CISSP-ISSMP (gestion)	
Healthcare Information Security and Privacy Practitioner (HCISPP)	• Atteste que les candidats ont les connaissances et les compétences nécessaires pour mettre en œuvre, gérer ou évaluer les contrôles de sécurité et de confidentialité touchant les renseignements sur les soins de santé et sur les patients • Conçue pour les praticiens et les consultants dont le travail demande le respect de la sécurité et de la confidentialité des renseignements sur les soins de santé • Les candidats doivent avoir un minimum de deux années d'expérience professionnelle • L'examen comporte 125 questions à choix multiples • Valide pendant trois ans • Le renouvellement de la certification nécessite l'obtention de 60 crédits de formation continue pendant la période de trois ans	• Agents de conformité • Superviseurs des dossiers médicaux • Gestionnaires de la pratique • Gestionnaires de la sécurité de l'information • Gestionnaires de l'information sur la santé
Systems Security Certified Practitioner (SSCP)	• Certification mondiale en sécurité des TI • Certification de premier échelon • Démontre que les titulaires de cette certification possèdent les compétences et les connaissances techniques pour mettre en œuvre, surveiller et administrer une infrastructure TI • Conçue pour les praticiens qui remplissent des fonctions TI opérationnelles ou qui travaillent en sécurité de l'information • Les candidats doivent avoir une année d'expérience professionnelle cumulative dans au moins l'un des sept domaines du corpus de connaissances communes offerts par le programme SSCP; une reconnaissance équivalant à une année d'expérience sera accordée aux candidats détenant un baccalauréat ou une maîtrise en cybersécurité • L'examen comporte 125 questions à choix multiples • Valide pendant trois ans • Le renouvellement de la certification nécessite l'obtention de 60 crédits de formation continue pendant la période de trois ans	• Ingénieurs de la sécurité réseau • Administrateurs de système • Analystes de la sécurité • Analystes de système et de réseau • Consultants en sécurité • Administrateurs, directeurs ou gestionnaires des TI

5.9 ISACA

Tableau 9 Liste et description des certifications de ISACA[9]

Certification	Aperçu de la certification	Candidats ciblés
Certified Cybersecurity Practitioner (CSX-P)	• Nouvelle certification créée en 2015 • Reconnaît les personnes qui peuvent agir à titre de premiers répondants lors d'incidents de sécurité • La seule certification qui évalue la capacité des candidats d'exercer les compétences en cybersécurité validées mondialement et couvrant les cinq fonctions de base du cadre de cybersécurité du NIST (*Cyber Security Framework*) : identification, protection, détection, intervention et récupération • Les candidats doivent passer un examen basé sur le rendement comportant des simulations d'incidents de sécurité • Valide pendant trois ans • Le renouvellement de la certification exige l'obtention de 120 heures de formation professionnelle continue pendant la période de trois ans	• Praticiens de la sécurité • Gestionnaires des incidents
Certified in Risk and Information Systems Control (CRISC)	• Reconnaît les candidats qui identifient, évaluent et gèrent les risques par l'élaboration, la mise en œuvre et la maintenance des contrôles de systèmes d'information • Les candidats doivent avoir trois années d'expérience professionnelle en gestion et en contrôle des risques; l'éducation ne peut pas remplacer l'expérience • Valide pendant trois ans • Le renouvellement de la certification exige l'obtention de 120 heures de formation professionnelle continue pendant la période de trois ans	• Professionnels en TI et dans le milieu des affaires • Professionnels dans le domaine des risques et de la conformité • Analystes des activités • Gestionnaires de projets • Directeurs de la sécurité
Certified Information Security Manager (CISM)	• Certification axée sur la gestion	• Gestionnaires et directeurs de la sécurité de l'information

[9] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

	• Reconnaît les candidats qui gèrent, conçoivent, supervisent et évaluent la sécurité de l'information d'une entreprise • Les candidats doivent avoir un minimum de cinq années d'expérience en sécurité de l'information acquise sur une période de dix ans avant de pouvoir passer l'examen • Une demande écrite doit être présentée • L'examen comporte 150 questions à répondre en quatre heures • Valide pendant trois ans • Le renouvellement de la certification exige l'obtention de 120 heures de formation professionnelle continue pendant la période de trois ans	• Analystes de la sécurité des TI • Analystes des risques • Vérificateurs des TI • Gestionnaires de la sécurité des systèmes d'information
Certified Information Systems Auditor (CISA)	• Certification universellement reconnue • Atteste l'expérience, les compétences et les connaissances des candidats dans le domaine de la vérification, ainsi que la capacité d'évaluer les vulnérabilités, d'élaborer des rapports sur la conformité et de prévoir des mécanismes de contrôle au sein de l'entreprise • Les candidats doivent avoir cinq années d'expérience professionnelle en vérification, en contrôle ou en sécurité des systèmes d'information (SI); certains critères d'éducation peuvent remplacer l'expérience • L'examen comporte 150 questions • Les titulaires de cette certification doivent suivre au moins 120 heures de formation continue pendant la période de trois ans	• Professionnels du contrôle de vérification, de l'assurance de la qualité et de la sécurité des systèmes d'information

5.10 ITSM SOLUTIONS

Tableau 10 Liste et description des certifications d'itSM Solutions[10]

Certification	Aperçu de la certification	Candidats ciblés
NIST Cyber Security Professional (NCSP) Foundation	• Certification de premier échelon • Atteste que les candidats ont les connaissances et les capacités nécessaires pour opérationnaliser le cadre de cybersécurité du NIST (NCSF pour *NIST Cyber Security Framework*) • Aucun préalable n'est exigé, mais des compétences de base en informatique et des connaissances en sécurité sont recommandées • L'examen comporte 40 questions à choix multiples	• Professionnels de la sécurité, des TI ou de la gestion des risques • Vérificateurs • D'autres professionnels devant comprendre les rudiments de la cybersécurité, les composantes du NCSF et leur application dans le cadre de la gestion des risques
NCSP Practitioner	• Atteste que les candidats ont les compétences et les capacités nécessaires pour concevoir, établir, tester, gérer et améliorer un programme de cybersécurité basé sur le NCSF • Les candidats doivent avoir terminé la formation et l'examen NCSF Foundation avant d'essayer de passer l'examen • L'examen comporte 65 questions à choix multiples	• Professionnels des TI et de la cybersécurité

[10] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

5.11 MCAFEE INSTITUTE

Tableau 11 Liste et description des certifications du McAfee Institute[11]

Certification	Aperçu de la certification	Candidats ciblés
Certified Counterintelligence Threat Analyst (CCTA)	• Atteste la capacité des candidats d'identifier les cybercriminels et d'enquêter sur eux, de mener des enquêtes de contre-ingérence visant à atténuer les menaces, et d'enquêter et de poursuivre en justice les pirates informatiques et les cybercriminels • Préalables : baccalauréat ou diplôme de niveau supérieur et trois années d'expérience dans un domaine connexe, ou diplôme associé et quatre années d'expérience • Les candidats doivent se soumettre à une vérification des antécédents • L'examen comporte 200 questions • Valide pendant deux ans • Pour renouveler la certification, les candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue	• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes
Certified Cyber Intelligence Investigator (CCII)	• Atteste la capacité des candidats de mener des cyberenquêtes, d'utiliser des méthodologies afin de poursuivre en justice des cybercriminels, d'appliquer la criminalistique mobile et numérique, de reconnaître la fraude et le piratage, et de procéder à la collecte de renseignement • Préalables : baccalauréat ou diplôme de niveau supérieur et une année d'expérience dans un domaine connexe, ou diplôme associé et deux années d'expérience • Les candidats doivent se soumettre à une vérification des antécédents • L'examen comporte 200 questions • Valide pendant deux ans • Pour renouveler la certification, les candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue	• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes

[11] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

Certified Cyber Intelligence Professional (CCIP)	• Atteste la capacité des candidats de mener des cyberenquêtes, d'utiliser des méthodologies afin de poursuivre en justice des cybercriminels, de concevoir et de mettre en œuvre un programme de cybersécurité, de comprendre la criminalistique mobile et numérique, et de reconnaître la fraude et le piratage • Préalables : baccalauréat ou diplôme de niveau supérieur et trois années d'expérience dans un domaine connexe, ou diplôme associé et quatre années d'expérience • Les candidats doivent se soumettre à une vérification des antécédents • L'examen comporte 200 questions • Valide pendant deux ans • Pour renouveler la certification, les candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue	• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes
Certified Expert in Cyber Investigations (CECI)	• Atteste la capacité des candidats de reconnaître et d'identifier les cybercriminels, de mener des enquêtes de contre-ingérence visant à atténuer les menaces, de protéger les actifs et les renseignements d'une entreprise, et d'enquêter et de poursuivre en justice les pirates informatiques et les cybercriminels • Préalables : baccalauréat ou diplôme de niveau supérieur et quatre années d'expérience dans un domaine connexe, ou diplôme associé et six années d'expérience • Les candidats doivent se soumettre à une vérification des antécédents • L'examen comporte 200 questions de type vrai ou faux, des questions à choix multiples et des questions axées sur des scénarios • Valide pendant deux ans • Pour renouveler la certification, les candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue	• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes

5.12 OFFENSIVE SECURITY

Tableau 12 Liste et description des certifications d'Offensive Security[12]

Certification	Aperçu de la certification	Candidats ciblés
Offensive Security Certified Expert (OSCE)	• Démontre que les candidats maîtrisent des compétences avancées en test de pénétration; qu'ils peuvent analyser, corriger, modifier et adapter un code d'exploit; et créer des fichiers binaires pour échapper aux logiciels antivirus • Les candidats doivent avoir des connaissances préalables des techniques d'exploitation Windows, avoir de l'expérience avec Linux et posséder une connaissance approfondie du protocole TCP/IP et de la réseautique • Les candidats doivent avoir terminé le cours intitulé *Cracking the Perimeter* avant de passer l'examen • Le temps accordé pour l'examen est de 48 heures, et il comporte des tests de pénétration pratiques dans un réseau privé virtuel (RPV) isolé; les candidats doivent également présenter un rapport de test exhaustif	• Testeurs de pénétration • Professionnels de la sécurité
Offensive Security Certified Professional (OSCP)	• Atteste que les candidats ont les connaissances et les compétences nécessaires pour trouver les vulnérabilités et déployer des attaques organisées d'une manière contrôlée et ciblée • S'adresse aux testeurs de pénétration possédant un solide bagage technique et en piratage contrôlé, et une connaissance approfondie des réseaux TCP/IP • Les candidats doivent d'abord terminer le cours de formation intitulé *Penetration Testing* • La certification est difficile à obtenir en raison de l'examen qui est manifestement complexe • Les candidats doivent passer un examen de 24 heures au cours duquel ils doivent réussir à attaquer et à pénétrer des systèmes opérationnels dans un environnement de laboratoire sécuritaire; ils doivent également présenter un rapport de test de pénétration exhaustif • La certification n'expire jamais	• Testeurs de pénétration • Administrateurs de réseau • Professionnels de la sécurité réseau

[12] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

Offensive Security Exploitation Expert (OSEE)	• Exige beaucoup de temps • Atteste la capacité des candidats d'analyser les logiciels vulnérables, de trouver un code problématique et de développer des exploits sophistiqués dans divers systèmes d'exploitation Windows modernes • Les candidats doivent avoir de l'expérience en développement d'exploits dans Windows et ils doivent comprendre le fonctionnement d'un débogueur • Les candidats doivent avoir terminé le cours intitulé *Advanced Windows Exploitation* avant de passer l'examen • Les candidats devraient obtenir au préalable la certification OSCE • L'examen consiste à développer et à documenter des exploits pendant une période de 72 heures; les candidats doivent également présenter un rapport de test de pénétration exhaustif • La certification permet aux titulaires d'obtenir 40 crédits de formation continue (ISC)2 • La certification n'expire jamais	• Testeurs de pénétration
Offensive Security Web Expert (OSWE)	• Atteste que les candidats ont des connaissances pratiques de l'évaluation des applications Web et du processus de piratage; ainsi que leur capacité d'examiner du code source avancé dans des applications Web, de trouver des vulnérabilités et de les exploiter • Les candidats doivent bien connaître les langages de codage et Linux, être en mesure d'écrire des scripts et avoir de l'expérience avec les mandataires Web, une compréhension générale des vecteurs d'attaque des applications Web, en théorie et en pratique, et une connaissance approfondie du protocole TCP/IP et de la réseautique • Les candidats doivent réussir le cours intitulé *Advanced Web Attacks and Exploitation* avant de passer l'examen • Le temps accordé pour l'examen est de 48 heures, et il comporte une évaluation pratique d'applications Web dans un RPV isolé; les candidats qui réussissent doivent également présenter un rapport d'évaluation • La certification n'expire jamais	• Testeurs de pénétration • Spécialistes de la sécurité des applications Web • Ingénieurs de logiciel • Développeurs Web
Offensive Security Wireless Professional (OSWP)	• Atteste la capacité des candidats de trouver des vulnérabilités et des chiffrements en place dans des réseaux répondant à la norme 802.11 de l'Institute of Electrical and Electronics Engineers (IEEE), de contourner des restrictions liées à la sécurité et de récupérer les clés de chiffrement utilisées	• Administrateurs de réseau • Testeurs de pénétration

	• Les candidats doivent avoir une compréhension approfondie du protocole TCP/IP et du modèle OSI (*Open System Interconnection*), ainsi qu'une connaissance de Linux • Les candidats doivent avoir terminé le cours intitulé *Offensive Security Wireless Attacks* avant de passer l'examen • L'examen de quatre heures demande aux candidats de recueillir de l'information sans fil, et de mettre en œuvre diverses attaques afin d'avoir accès aux réseaux cibles; les candidats doivent également présenter un rapport sur les tests de pénétration • La certification n'expire jamais	

5.13 PECB

Tableau 13 Liste et description des certifications de PECB[13]

Certification	Aperçu de la certification	Candidats ciblés
Certified Lead Ethical Hacker	• Atteste que les candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc. • Les candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation • Les candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité • Les candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH • Examen de six heures à livre ouvert qui comprend deux parties : les candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit • Valide pendant trois ans • Pour renouveler la certification, les candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels	• Personnes responsables de la sécurité des systèmes d'information • Membres de l'équipe de sécurité de l'information
Computer Forensics Foundation	• Atteste que les candidats possèdent des connaissances en ce qui concerne les principes et concepts fondamentaux relatifs à l'informatique judiciaire, et les processus d'informatique judiciaire • Aucun préalable n'est exigé • Les candidats doivent signer le Code de déontologie de PECB	• Personnes souhaitant faire carrière en informatique judiciaire

[13] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

	• Examen d'une heure à livre ouvert qui comporte cinq questions de type rédactionnel • Valide pendant trois ans • Pour renouveler la certification, les candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels	
ISO/IEC 27032 Foundation	• Atteste que les candidats ont des connaissances en ce qui a trait aux principes et aux concepts fondamentaux de cybersécurité, et une compréhension des approches, des méthodes et des techniques utilisées en cybersécurité • Aucun préalable n'est exigé • Les candidats doivent signer le Code de déontologie de PECB • Examen d'une heure qui comporte 40 questions à choix multiples • Valide pendant trois ans • Pour renouveler la certification, les candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels	• Professionnels en cybersécurité et en sécurité de l'information • Personnes souhaitant poursuivre une carrière en cybersécurité
ISO/IEC 27032 Lead Cybersecurity Manager • Certified Provisional • Certified • Certified Lead • Certified Senior Lead	• Atteste que les candidats possèdent des connaissances en ce qui concerne les principes et concepts fondamentaux de la cybersécurité, les rôles et responsabilités des parties prenantes, la gestion des risques liés à la cybersécurité, les mécanismes d'attaque et les contrôles en cybersécurité, l'échange d'information et la coordination, l'intégration d'un programme de cybersécurité à la gestion de la continuité des activités, et la gestion des incidents de cybersécurité et la mesure du rendement • Les candidats doivent avoir une compréhension fondamentale de la norme ISO/IEC 27032 et des connaissances approfondies en cybersécurité • Les candidats doivent signer le Code de déontologie de PECB • Examen de trois heures à livre ouvert qui comporte douze questions de type rédactionnel • Les candidats qui ont réussi l'examen peuvent postuler pour l'un des quatre titres de compétence en fonction du nombre d'années d'expérience de travail, d'expérience en	• Professionnels en cybersécurité et en sécurité de l'information • Responsables du développement ou de la gestion d'un programme de cybersécurité

	cybersécurité et du nombre total d'heures consacrées à des activités de cybersécurité • Valide pendant trois ans • Pour renouveler la certification, les candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels	
Lead Cloud Security Manager • Certified Provisional • Certified • Certified Lead • Certified Senior Lead	• Atteste que les candidats possèdent des connaissances en ce qui a trait aux principes et aux concepts de l'informatique en nuage, à la gestion des risques et des incidents de sécurité infonuagique, et aux tests, à la surveillance et à l'amélioration continue de la sécurité infonuagique • Les candidats doivent avoir une compréhension fondamentale des normes ISO/IEC 27017 et ISO/IEC 27018, et une connaissance générale des concepts de l'informatique en nuage • Les candidats doivent signer le Code de déontologie de PECB • Examen de trois heures à livre ouvert qui comporte 80 questions à choix multiples • Les candidats qui ont réussi l'examen peuvent postuler pour l'un des quatre titres de compétence en fonction du nombre d'années d'expérience de travail, du nombre d'années d'expérience en cybersécurité et du nombre total d'heures consacrées à des activités de projets CCSMS • Valide pendant trois ans • Pour renouveler la certification, les candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels	• Professionnels de la sécurité infonuagique et de la sécurité de l'information • Personnes chargées de maintenir et de gérer un programme de sécurité infonuagique Conseillers spécialisés en sécurité infonuagique
Lead Forensics Examiner • Certified Provisional • Certified • Certified Lead	• Atteste que les candidats possèdent des connaissances en ce qui concerne les principes et concepts fondamentaux relatifs à l'informatique judiciaire, les exigences relatives aux laboratoires de criminalistique numérique, les enquêtes sur les crimes informatiques et les examens d'informatique judiciaire, et le maintien de la chaîne de possession • Les candidats doivent avoir des connaissances en informatique judiciaire • Les candidats doivent signer le Code de déontologie de PECB	• Spécialistes et consultants en informatique judiciaire • Professionnels de la cybersécurité • Analystes de cyberrenseignement • Professionnels chargés de l'application de la loi

	• Examen de trois heures à livre ouvert qui comporte quatorze questions de type rédactionnel • Les candidats qui ont réussi l'examen peuvent postuler pour l'un des trois titres de compétence en fonction du nombre d'années d'expérience de travail, du nombre d'années d'expérience en cybersécurité et du nombre total d'heures consacrées à des activités d'informatique judiciaire • Valide pendant trois ans • Pour renouveler la certification, les candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels	• Analystes de données électroniques
Lead Pen Test Professional • Certified Provisional • Certified • Certified Lead	• Atteste que les candidats possèdent des connaissances en ce qui concerne les principes et concepts fondamentaux relatifs aux tests de pénétration, les bases techniques pour les tests de pénétration, les types de tests, et l'analyse des résultats et du processus de rapport • Les candidats doivent avoir une compréhension fondamentale des tests de pénétration, et des connaissances approfondies en cybersécurité • Les candidats doivent signer le Code de déontologie de PECB • Examen de trois heures qui comporte 150 questions à choix multiples • Les candidats qui ont réussi l'examen peuvent postuler pour l'un des trois titres de compétence en fonction du nombre d'années d'expérience de travail, du nombre d'années d'expérience dans le domaine des tests de pénétration et du nombre total d'heures consacrées à des activités de tests de pénétration • Valide pendant trois ans • Pour renouveler la certification, les candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels	• Professionnels des TI • Vérificateurs • Gestionnaires des TI et des risques • Testeurs de pénétration • Spécialistes du piratage contrôlé

5.14 SECO INSTITUTE

Tableau 14 Liste et description des certifications du SECO Institute[14]

Certification	Aperçu de la certification	Candidats ciblés
Certified Ethical Hacker (S-EHE)	• Le programme fait l'objet d'une restructuration	• s.o.
Dark Web Foundations	• Certification de premier échelon • Développée par la Netherlands Organisation for Applied Scientific Research en collaboration avec l'International Criminal Police Organization (INTERPOL) • Démontre que les candidats comprennent l'utilisation du Web invisible de manière sécuritaire • L'examen comporte 40 questions à choix multiples • Aucune limite de validité et aucune exigence de renouvellement de la certification ne s'appliquent	• Professionnels de la sécurité des TI • Application de la loi • Responsables des politiques et représentants de gouvernement
Ethical Hacking Foundations (S-EHF)	• Certification de premier échelon • Atteste que les candidats ont une connaissance approfondie des techniques de base liées aux tests de pénétration et qu'ils comprennent les principes fondamentaux du piratage • L'examen comporte 40 questions à choix multiples • Aucune limite de validité et aucune exigence de renouvellement de la certification ne s'appliquent	• Développeurs Web • Ingénieurs de logiciel • Administrateurs de la sécurité • Ingénieurs de réseau • Spécialistes du piratage contrôlé
Ethical Hacking Leader (S-EHL)	• La plus haute distinction de compétence dans le volet *Ethical Hacking* • Démontre que les candidats ont d'excellentes compétences dans le domaine des tests de pénétration, ainsi que de l'expérience de la direction de tests de pénétration	• Professionnels souhaitant valider l'expertise acquise dans le cadre de leur expérience pratique de travail

[14] Toutes les mesures nécessaires ont été prises pour s'assurer de l'exactitude des renseignements contenus dans ce tableau; toutefois, ces renseignements peuvent être modifiés à tout moment.

	• Les candidats doivent avoir des connaissances d'expert (certificat de niveau expert du SECO Institute ou l'équivalent) et au moins trois années d'expérience professionnelle pertinente • Aucun examen n'est requis • Valide pour une période d'un an • Pour renouveler la certification, les candidats doivent payer une cotisation annuelle et obtenir 40 crédits de formation continue durant l'année	
Ethical Hacking Practitioner (S-EHP)	• Atteste que les candidats comprennent pleinement le processus de test de pénétration et qu'ils connaissent les techniques courantes liées aux tests de pénétration • Les candidats doivent bien comprendre les principes de base du piratage contrôlé • La certification S-EHF (ou l'équivalent) est recommandée • Examen en trois volets : dix questions à choix multiples, cinq questions de type rédactionnel et une étude de cas • Valide pour une période d'un an • Pour renouveler la certification, les candidats doivent payer une cotisation annuelle et obtenir 20 crédits de formation continue durant l'année	• Développeurs Web • Administrateurs de la sécurité • Ingénieurs de réseau • Ingénieurs de logiciel • Testeurs de pénétration potentiels
IT Security Expert/SOC (S-ITSE/SOC)	• Atteste que les candidats ont les connaissances et les compétences nécessaires pour prendre en charge la détection et l'analyse des menaces et l'intervention en cas de menace, et pour améliorer l'ensemble de la sécurité d'une organisation • Les candidats doivent avoir une compréhension de base du protocole TCP/IP, des principes fondamentaux des systèmes d'exploitation et des concepts de sécurité courants, et posséder deux années d'expérience dans un COS • Le préalable exigé est la certification S-ITSP ou l'équivalent • Les candidats peuvent choisir l'une de deux spécialisations : gestionnaire de COS (*Manager SOC*) ou gestionnaires de la sécurité des TI (*IT Security Manager*) • Valide pendant un an • Pour renouveler la certification, les candidats doivent payer une cotisation annuelle et obtenir 40 crédits de formation continue durant l'année	• Personnes aspirant à devenir des analystes de COS de niveau 1 et de niveau II • Futurs gestionnaires de COS • Ingénieurs de système • Analystes de la sécurité
IT Security Foundation (S-ITSF)	• Certification de premier échelon	• Administrateurs de réseau ou de système

	• Atteste que les candidats ont une connaissance de base de l'architecture informatique, des vulnérabilités matérielles courantes et des mesures de sécurité • Aucun préalable n'est exigé; convient aux débutants qui ont quelques connaissances de base en informatique et en technologie • L'examen comporte 40 questions à choix multiples • Aucune limite de validité et aucune exigence de renouvellement de la certification ne s'appliquent	• Personnes qui désirent entamer une carrière en sécurité des TI
IT Security Practitioner (S-ITSP)	• Atteste les compétences techniques des candidats en gestion des vulnérabilités, en sécurité de coupe-feu et de réseau, en architecture de sécurité et en test de pénétration • Les candidats doivent avoir une bonne connaissance des termes, des concepts et des principes de base de la sécurité des TI • La certification *IT Security Foundation* (ou l'équivalent) est recommandée • L'examen comporte dix questions à choix multiples, cinq questions ouvertes et une étude de cas • Valide pendant un an • Pour renouveler la certification, les candidats doivent payer une cotisation annuelle et obtenir 60 crédits de formation continue durant l'année	• Administrateurs de la sécurité • Analystes de la sécurité • Architectes de la sécurité • Vérificateurs de la sécurité • Futurs analystes du COS

6.0 CONTENU COMPLÉMENTAIRE

6.1 LISTE DES ACRONYMES, DES ABRÉVIATIONS ET DES SIGLES

Acronyme, abréviation ou sigle	Expression au long
(ICS)2	*International Information Systems Security Certification Consortium*
C3	*Cyber Credentials Collaborative*
CCSMS	*Central Configuration Setting Management System*
CEI	Commission électrotechnique internationale
Centre pour la cybersécurité	Centre canadien pour la cybersécurité
CNSS	*Committee on National Security Systems*
CompTIA	*Computing Technology Industry Association*
COS	Centre des opérations de sécurité
CREST	*Council for Registered Ethical Testers*
CSA	*Cloud Security Alliance*
CST	Centre de la sécurité des télécommunications
CWNP	*Certified Wireless Network Professionals*
GCHQ	*Government Communications Headquarters*
GIAC	*Global Information Assurance Certification*
GIES	Gestion des informations et des événements de sécurité
IAS	*International Accreditation Service*
IdO	Internet des objets
IEEE	*Institute of Electronic Engineers*
INTERPOL	*International Criminal Police Organization*
ISACA	*Information Systems Audit and Control Association*
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
NERC CIP	*North American Electric Reliability Corporate Critical Infrastructure Protection*
NICCS	*National Initiative for Cyber Security Careers and Studies*
NIST	*National Institute of Standards and Technology*
NSA	*National Security Agency*
OSI	*Open Systems Interconnection*
PCI	Industrie des cartes de paiement (*Payment Card Industry*)
RBC	Banque Royale du Canada (*Royal Bank of Canada*)
RFID	Identification par radiofréquence (*Radio Frequency Identification*)
RPV	Réseau privé virtuel

SCADA	Télésurveillance et acquisition de données (*Supervisory Control and Data Acquisition*)
SCI	Système de contrôle industriel
SECO	*Security and Continuity Institute*
SI	Système d'information
TCP/IP	Protocole TCP/IP (*Transmission Control Protocol/Internet Protocol*)
TI	Technologies de l'information
UKAS	*United Kingdom Accreditation Service*
WLAN	Réseau local sans fil

6.2 RÉFÉRENCES

Numéro	Référence
1	MORGAN, Steve. *10 Hot Cybersecurity Certifications for IT Professionals to Pursue in 2020*, Cyber Crime Magazine, 24 mai 2020. https://cybersecurityventures.com/10-hot-cybersecurity-certifications-for-it-professionals-to-pursue-in-2019/