Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Certifications dans le domaine de la cybersécurité

2020

TLP:WHITE

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

TABLE DES MATIÈRES

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 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 ne sont pas 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 CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Centre canadien pour la cybersécurité (CCC) a été mis sur pied sous l'égide du Centre de la sécurité des télécommunications (CST) en octobre 2018. L'équipe Relations et collaboration avec le milieu universitaire du Centre pour la cybersécurité travaille de concert avec les universités, les collèges, les associations et les comités ministériels à vocation éducative, ainsi qu'avec les professeurs du secteur privé afin d'accroître les capacités et le bassin de candidats talentueux en cybersécurité au Canada. L'équipe collabore 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 (tableau 1).

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.

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

---

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

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 contact@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 en ordre alphabétique. Une liste plus complète de certifications se trouve dans les tableaux joints. **Le Centre de la sécurité des télécommunications 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, l'intelligence artificielle et les interfaces homme-machine. Les quatre certifications offertes en cybersécurité sont valides pour une période de trois ans.

- La certification ***Certified First Responder*** (CRF) atteste les connaissances et les compétences requises pour protéger les renseignements et les systèmes essentiels avant, pendant et après un incident. Elle est approuvée conformément à la directive 8140 du département de la Défense.
- 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'identification 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 des 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 de systèmes et de réseaux.

Une liste complète des certifications en cybersécurité offertes par le programme CertNexus se trouve à la section 3.1.

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 réseaux de connexions conçus par Cisco. L'obtention d'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 toutes 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 centré 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 technologique.
- ***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 3.2.

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 branche d'activité qui permettent de faire un suivi des tendances et des changements. Les certifications proposées couvrent une vaste gamme de domaines informatiques, dont la cybersécurité. Certaines certifications sont approuvées conformément aux exigences de la directive 8140 du département de la Défense. Pour renouveler, 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 (en nuage ou mobiles), ainsi que des ordinateurs et des serveurs traditionnels.
- La certification ***CompTIA Security+*** en est une 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 de réseau et avoir déjà obtenu leur certification Network+.

Une liste complète des certifications en cybersécurité offertes par le programme CompTIA se trouve à la section 3.3.

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 accréditations 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. L'intervention en cas d'incident a été approuvée par le Government Communications Headquarters (GCHQ). Les examens CREST comportent trois niveaux d'accréditation 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 3.4.

2.5 CERTIFIED WIRELESS NETWORK PROFESSIONALS

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

- 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 des entreprises. Les candidats doivent réussir quatre examens de certification, procéder à des déploiements du RL sans fil commercial, 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 CWNE.
- La certification ***Certified Wireless Security Professional*** (CWSP**)** est une certification de RL 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 avant qu'elles ne se produisent, d'effectuer des vérifications de sécurité de RL sans fil et de mettre en œuvre des solutions de surveillance de la conformité, et de concevoir une architecture de sécurité de 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 3.5.

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 des défis concrets de la vérification 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 du test 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.
- La certification ***Licensed Penetration Tester* (LPT)** n'est accordée qu'aux personnes maîtrisant les techniques de cybersécurité. Elle représente sans doute le summum en matière de certifications en cybersécurité.

Une liste complète des certifications en cybersécurité offertes par le programme EC Council se trouve à la section 3.6.

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* ne sont tenus que de passer un examen pour l'obtention de la certification; celle-ci est valide pour une période de 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 ils doivent repasser 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*** (GIAC) 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, d'intervenir en cas d'incident et de régler les incidents liés à la sécurité informatique 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 3.7.

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 informatique compte plus de 140 000 membres à l'échelle mondiale, dont près de 6 000 au Canada.

Les certifications (ISC)2 satisfont à la directive *Cyber Workforce Management* (directive 8140) du département de la Défense (DoD) des États-Unis[2]. 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 d'une durée 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 3.8.

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 du développement 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

[2] La directive *Cyber Workforce Management* du DoD (anciennement DoD 8750) s'adresse au personnel soutenant les missions du DoD relatives au renseignement, à la sécurité et à l'application de la loi dans le cyberespace. Elle vise à consolider la main-d'œuvre du cyberespace et à établir des éléments précis de celle-ci pour ainsi normaliser les rôles professionnels, les qualifications et les exigences de formation dans le cyberespace.

base du cadre de cybersécurité du NIST (*Cyber Security Framework*) : identification, protection, détection, intervention et récupération. Pour obtenir la certification, les candidats doivent passer un examen d'une durée 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 3.9.

2.10 ITSM SOLUTIONS

Les certifications **itSM Solutions** s'appuient sur le cadre de cybersécurité du NIST (NCSF pour *Cyber Security Framework*). 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 de ce cadre de cybersécurité.

- ***NCSF Foundations* :** Pour les cadres et les professionnels du milieu informatique et des affaires qui doivent connaître les principes de base du cadre de cybersécurité du NIST pour s'acquitter de leurs tâches.
- ***NCSF 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 cadre de cybersécurité du NIST 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 3.10.

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. Le McAfee Institute se trouve sur la liste des fournisseurs de certifications professionnelles en cybersécurité de la National Initiative for Cyber Security Careers and Studies (NICCS) du département de la Sécurité intérieure des États-Unis. Les titulaires de certification viennent des plus grands organismes gouvernementaux et d'application de la loi, comme la US Air Force et la United States Army, le Federal Bureau of Investigation (FBI) et le New York Police Department (NYPD).

- La certification **Certified Cyber Intelligence Professional** (CCIP) a été développée 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 3.11.

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 à 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 à attaquer et à pénétrer des systèmes opérationnels dans des conditions d'essai en laboratoire sécuritaires, sur une période de 24 heures. 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 3.12.

2.13 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 spécifique, comme la sécurité des technologies de l'information, 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 du système d'exploitation Linux est recommandée.
- La certification ***Ethical Hacking Practitioner*** (S-EHP) s'adresse aux professionnels qui ont déjà une solide connaissance des fondements du piratage contrôlé. L'obtention préalable de la certification S-EHF est recommandée. Obtenir la certification démontre que les candidats comprennent pleinement le processus du test de pénétration et qu'ils maîtrisent les techniques communes de ce test.

Une liste complète des certifications en cybersécurité offertes par le SECO se trouve à la section 3.13.

2.14 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 milite pour les compétences non rattachées à un vendeur 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 développées 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 :

- CertNexus
- Computing Technology Industry Association
- EC-Council
- Global Information Assurance Certification
- International Information Systems Security Certification Consortium
- ISACA

3.0 LISTES ET DESCRIPTIONS DES CERTIFICATIONS EN CYBERSÉCURITÉ

Les tableaux ci-dessous dressent une liste plus complète des différentes certifications en cybersécurité offertes aux particuliers, classées en 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 qui figurent dans la dernière colonne. Certains fournisseurs proposent des offres groupées de cours qui comprennent les frais d'examen.

3.1 CERTNEXUS

Table 1 Listes et descriptions des certifications de CertNexus[3]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Certified First Responder (CFR)	• Elle atteste les connaissances des candidats en matière d'analyse de menaces, de conception informatique sécurisée et d'environnement réseau, de détection proactive de défaillances de réseaux et d'intervention et d'enquête sur des incidents liés à la cybersécurité • Approuvée conformément à la directive 8140 du département de la Défense • Les candidats doivent avoir de trois à cinq années d'expérience dans un environnement informatique où le travail implique la protection de systèmes d'information essentielle avant, pendant et après un incident	• Administrateurs de système • Administrateurs de réseau • Intervenants en cas d'incident informatique • Enquêteurs de la cybercriminalité • Vérificateurs des TI • Analystes de la sécurité • Analystes de réseau • Ingénieurs de sécurité pour les systèmes d'information	• Fast Lane • Global Knowledge • Learning Tree • New Horizons Fournisseurs offrant aussi des cours en français : • Eccentrix

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

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.

	• L'examen comporte 100 questions à choix multiples
	• Valide pour une période de trois ans
	• Deux options possibles pour le renouvellement de la certification :
	  ○ Passer l'examen en utilisant la plus récente version
	  ○ Obtenir 90 crédits de formation continue pendant la période de trois ans et payer les frais annuels		

Certified IoT Security Practitioner (CIoTSP)	• Elle 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 des menaces, de surveiller efficacement les dispositifs de l'IdO et d'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 de développement logiciel • Architectes de solutions • Analystes de la cybersécurité • Développeurs Web • Ingénieurs de l'infonuagique	• Deloitte • Global Knowledge • New Horizons Fournisseurs offrant aussi des cours en français : • Eccentrix
Cyber Secure Coder (CSC)	• Elle 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 de la programmation (développement d'applications de bureau, mobiles, Web ou infonuagiques) • L'examen comporte 80 questions à choix multiples • Valide pour une période de trois ans	• Programmeurs en chef • Programmeurs débutants • Testeurs d'application • Testeurs de l'assurance de la qualité • Concepteurs de logiciels • Architectes de logiciels	• Global Knowledge • New Horizons Fournisseurs offrant aussi des cours en français : • Eccentrix
CyberSafe	• Elle 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	• Utilisateurs finaux sans connaissances techniques de l'informatique	• New Horizons • Saskatoon Business College

	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		Fournisseurs offrant aussi des cours en français : • Eccentrix
Microcompétence IRBIZ	• Elle 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 pour une période de trois ans	• Leaders et cadres des TI responsables d'assurer le respect de la législation en matière d'intervention en cas d'incident	• New Horizons Fournisseurs offrant aussi des cours en français : • Eccentrix

3.2 CISCO SYSTEMS

Table 2 Listes et descriptions des certifications de Cisco Systems[4]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Cisco Certified CyberOps Associate	• La certification prépare les candidats à travailler avec des analystes associés de la sécurité informatique au sein de centres des opérations de sécurité • Aucun préalable n'est exigé • Elle est approuvée conformément à la directive 8570 du département de la Défense • Les candidats doivent passer deux examens pour recevoir la certification • Valide pour une période de trois ans • Le renouvellement de la certification exige de passer un examen de recertification, ou de réaliser des activités d'apprentissage et d'obtenir 30 crédits de formation continue	• Analystes de la cybersécurité • Membres de l'équipe du centre des opérations de sécurité	• Global Knowledge • Centennial College • NetCom Learning
Cisco Certified Network Associate Security (CCNA Security)	• Elle 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 • Elle est approuvée conformément à la directive 8570.01 du	• Administrateurs de réseau • Ingénieurs de réseau	• Cybrary • InfoSec • Centennial College • NetCom Learning Fournisseurs offrant aussi des cours en français :

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

	département de la Défense • Valide pour une période de trois ans • Le renouvellement de la certification exige de passer un examen de recertification, ou de réaliser des activités d'apprentissage et d'obtenir 30 crédits de formation continue		• AFI Expertise • Collège de Maisonneuve • Eccentrix

3.3 COMPTIA

Table 3 Listes et descriptions des certifications de CompTIA[5]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
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 la cybersécurité • Elle 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 • Elle est approuvée conformément aux directives 8140/8570 du département de la Défense • Les candidats doivent avoir dix années d'expérience en administration des TI; dont cinq années d'expérience pratique en sécurité technique	• Architectes de la sécurité • Analystes techniques en chef • Ingénieurs de la sécurité • Ingénieurs de la sécurité des applications	• Global Knowledge • Intrinsec • Learn IT Canada • SecureNinja • SkillsBuild Canada • Ultimate IT Courses Fournisseurs offrant aussi des cours en français : • Eccentrix

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

	• L'examen comporte 90 questions à choix multiples et des questions axées sur le rendement • Valide pour une période de trois ans • Le renouvellement de la certification exige l'obtention de 75 crédits de formation continue pendant la période de trois ans		
Cyber Security Analyst (CySA+)	• Certification d'analyste de la cybersécurité de niveau intermédiaire • La certification d'analyste de la sécurité la plus récente qui couvre les menaces persistantes avancées dans un environnement de cybersécurité après 2014 • Elle 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 • Elle est 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 pour une période de trois ans • Le renouvellement de la certification nécessite l'obtention de 60 crédits de formation continue pendant la période de trois ans	• Analystes de la sécurité informatique • Analystes du centre des opérations de sécurité • Analystes de la cybersécurité • Analystes du renseignement sur les menaces • Ingénieurs de la sécurité • Analystes de la cybersécurité	• CertFirst • CLC Technical Training • New Horizons • SecureNinja Fournisseurs offrant aussi des cours en français : • Eccentrix
Network+	• Elle 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	• Postes de premier échelon • Administrateurs de réseau débutants • Techniciens en informatique • Ingénieurs de système débutants	• AFI Expertise • CertFirst • CLC Technical Training • Global Knowledge Fournisseurs offrant aussi des cours en français :

	questions axées sur le rendement • Valide pour une période de trois ans • Le renouvellement de la certification nécessite l'obtention de 30 crédits de formation continue pendant la période de trois ans		• AFI Expertise • Collège de Maisonneuve • Eccentrix
PenTest+	• Certification de niveau intermédiaire • Elle 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 nécessite l'obtention de 60 crédits de formation continue pendant la période de trois ans	• Testeurs de pénétration • Testeurs de la vulnérabilité • Analystes de la sécurité • Opérateurs de la sécurité de réseau	• Global Knowledge • Learning Tree • Udemy Fournisseurs offrant aussi des cours en français : • Eccentrix
Security+	• Certification de premier échelon • Elle 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 de réseau et avoir obtenu la certification Network+ • Valide pour une période de trois ans • Le renouvellement de la certification nécessite l'obtention de 50 crédits de formation continue pendant la période de trois ans	• Administrateurs de système • Administrateurs de réseau • Administrateurs de la sécurité informatique • Vérificateurs des TI débutants • Testeurs de pénétration • Ingénieurs de la sécurité	• CertFirst • CLC Technical Training • Cybrary • New Horizons • SecureNinja Fournisseurs offrant aussi des cours en français : • AFI Expertise • Eccentrix • Global Knowledge

3.4 COUNCIL FOR REGISTERED ETHICAL SECURITY TESTERS (CREST)

Table 4 Listes et descriptions des certifications de CREST[6]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Certified Infrastructure Tester	• Elle atteste que les candidats ont les capacités requises pour accéder à un réseau afin de trouver des vulnérabilités informatiques dans la couche du réseau et du système d'exploitation • L'examen comporte une partie écrite à choix multiples et deux volets pratiques d'une durée de six heures • Valide pour une période de 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	• Accenture • CISCO • Firebrand
Certified Web Application Tester	• Elle 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 d'une durée de six heures • Valide pour une période de trois ans • Pour renouveler leur certification, les candidats doivent repasser l'examen	• Testeurs de pénétration • Spécialistes du piratage contrôlé	• Accenture • CISCO • Cobalt Labs • Cyber Management Alliance
CREST Certified Wireless Specialist (CCWS)	• Elle atteste les connaissances et les compétences des candidats liées à la réalisation d'examens de la sécurité sans fil, et aux	• Professionnels de haut niveau	• 7Safe • Cyberskills Training

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

	technologies RFID, Bluetooth et autres technologies sans fil traditionnelles • Le préalable exigé est d'avoir réussi un des examens de certification CREST de base • Examen en deux volets : 120 questions à choix multiples et tâches pratiques • Valide pour une période de trois ans • Pour renouveler leur certification, les candidats doivent repasser l'examen		
Practitioner Security Analyst (CPSA)	• Certification de premier échelon • Elle 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 faire la preuve 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 pour une période de 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	• Crucial Academy • ICSI Ltd • iHack Labs Ltd • Immersive Labs • Net Security Training Ltd • QA
Registered Penetration Tester (CRT)	• Elle 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 communes; l'examen comporte une section à choix multiples • La certification CPSA est un préalable	• Administrateurs de système • Testeurs de pénétration • Gestionnaires de la sécurité de l'information • Gestionnaires des incidents	• 6Point6 • Crucial Academy • ICSI Ltd • iHackLabs Ltd • Immersive Labs • Net Security Training Ltd • QA

	• Valide pour une période de trois ans • Pour renouveler leur certification, les candidats doivent repasser l'examen		• Trustwave Spider Labs

3.5 CERTIFIED WIRELESS NETWORK PROFESSIONS (CWNP)

Table 5 Listes et descriptions des certifications de CWNP[7]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Certified Wireless Network Expert (CWNE)	• Certification de niveau avancé • On compte moins de 200 titulaires de la certification CWNE dans le monde • Elle 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)	• Personnes occupant des postes supérieurs liés au RL sans fil	• Sans objet

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

	• Les candidats doivent passer quatre examens et effectuer des déploiements de RL sans fil commerciaux • Valide pour une période de 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		
Certified Wireless Security Professional (CWSP)	• Elle atteste la capacité des candidats d'évaluer les vulnérabilités d'un réseau et d'aider à prévenir les attaques avant qu'elles ne se produisent, d'effectuer des vérifications de sécurité de RL sans fil 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 pour une période de 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 informatiques	• NetCertExpert • WiFi Training

3.6 EC COUNCIL

Table 6 Listes et descriptions des certifications de l'EC Council[8]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Advanced Network Defence CAST 614	• Certification de niveau avancé • Elle atteste les connaissances des candidats en matière de défense de réseau, d'architecture d'entreprise sécurisée et de défense contre les logiciels malveillants • Les candidats doivent avoir deux années d'expérience connexe en sécurité de l'information • L'examen comporte 50 questions écrites et dix questions pratiques • Valide pour une période de 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 coupe-feux • Architectes de système • Administrateurs de système • Administrateurs Windows	• Firebrand • Global Knowledge
Advanced Penetration Tester (APT)	• Certification de niveau avancé • Elle atteste les compétences des candidats en matière de tests de pénétration avancés • Elle prépare les candidats à l'examen de catégorie maître *Licensed Penetration Tester (Master)* • Valide pour une période de trois ans • Pour renouveler leur certification, les candidats doivent accumuler	• Spécialistes du piratage contrôlé • Testeurs de pénétration • Administrateurs de serveur réseau • Professionnels de l'évaluation des risques	• iClass • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix

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

	120 crédits de formation continue pendant la période de trois ans et payer des frais annuels		
Certified Application Security Engineer (CASE)	• Deux volets : JAVA et .NET • Elle 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 • Les candidats doivent avoir deux années d'expérience dans un environnement de développement Java ou .NET • Valide pour une période de 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	• Global Knowledge • iClass • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix
Certified Chief Information Security Officer (CCISO)	• Les candidats doivent avoir cinq années d'expérience en gestion de la sécurité de l'information dans les cinq domaines du programme CCISO, ou avoir terminé le programme EC Council Information Security Manager (EISM) • La certification du programme CCISO vise à former des cadres supérieurs de haut niveau en sécurité de l'information • Elle est approuvée conformément à la directive 8140 du département de la Défense • Elle satisfait à la norme de formation certifiée du GCHQ • Valide pour une période de 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	• Dirigeants principaux de la sécurité de l'information	• Ferro Technics • iClass • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix
Certified Ethical Hacker	• Compétence de premier échelon	• Responsables de la sécurité	• CertBolt

(ANSI)	• Elle atteste les compétences des candidats dans les cinq phases du piratage contrôlé : la reconnaissance, l'énumération, l'obtention de l'accès, le maintien de l'accès et le brouillage de pistes • Les candidats doivent avoir deux années d'expérience en sécurité de l'information • Elle satisfait à la norme de formation certifiée du GCHQ • L'examen comporte 125 questions • Valide pour une période de 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	• Vérificateurs des TI • Administrateurs de site	• Global Knowledge • iClass • Learning Tree • SimpliLearn Fournisseurs offrant aussi des cours en français : • Eccentrix • Kereon
Certified Ethical Hacker (Master)	• Les candidats détiennent les certifications ANSI et Practical CEH • Elle satisfait à la norme de formation certifiée du GCHQ • Valide pour une période de 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	• CertBolt • Global Knowledge • iClass • Learning Tree • SimpliLearn Fournisseurs offrant aussi des cours en français : • Eccentrix
Certified Ethical Hacker (Practical)	• Compétence de premier échelon • Elle cible l'application de compétences CEH dans le cadre des défis concrets de la vérification de sécurité et d'autres scénarios connexes • Elle satisfait à la norme de formation certifiée du GCHQ • Examen d'une durée de six heures comportant 20 études de cas • Valide pour une période de trois ans • Pour renouveler leur certification, les candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans	• Responsables de la sécurité • Vérificateurs des TI • Administrateurs de site	• CertBolt • iClass • Learning Tree • SimpliLearn Fournisseurs offrant aussi des cours en français : • Eccentrix • Global Knowledge

	et payer des frais annuels		
Certified Network Defence Architect (CNDA)	• Certification de premier échelon spécialement conçue pour les organismes gouvernementaux et militaires partout dans le monde • Les candidats doivent avoir un minimum de deux années d'expérience en sécurité de l'information, détenir une certification CEH valide et être à l'emploi d'un organisme gouvernemental ou militaire, ou être des employés contractuels du gouvernement • Aucun examen n'est requis • Valide pour une période de 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	• MindHub • ProTech
Certified Network Defender (CND)	• Elle démontre que les candidats ont une connaissance approfondie de la sécurité axée sur la défense et l'expertise nécessaire pour sécuriser des données • Les candidats doivent avoir deux années d'expérience en sécurité informatique • L'examen comporte 100 questions à choix multiples • Valide pour une période de 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 réseau • Analystes de la sécurité • Opérateurs de la sécurité • Ingénieurs de la sécurité de réseau	• Global Knowledge • iClass • InfoSec • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix
Certified Secure Computer User (CSCU)	• Elle 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 pour une période de trois ans • Pour renouveler leur certification, les candidats doivent accumuler	• Toute personne âgée de treize ans et plus qui utilise un ordinateur pour travailler, étudier ou jouer	• Ethical Hacking • Interwork Fournisseurs offrant aussi des cours en français : • Eccentrix

	120 crédits de formation continue pendant la période de trois ans et payer des frais annuels		
Certified SOC Analyst (CSA)	• Les candidats doivent avoir une année d'expérience en administration et sécurité des réseaux • Elle atteste que les candidats ont une pleine compréhension des tâches que doit accomplir un analyste du COS • L'examen comporte 100 questions à choix multiples • Valide pour une période de 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 du centre des opérations de sécurité de palier 1 et de palier 2 • Analystes de la cybersécurité • Administrateurs de réseau et de la sécurité informatique	• Global Knowledge • iClass • Near Secure Fournisseurs offrant aussi des cours en français : • Eccentrix
Certified Threat Intelligence Analyst (CTIA)	• Elle démontre que les candidats maîtrisent les connaissances et les compétences nécessaires pour traiter le renseignement sur les menaces • Les candidats doivent avoir deux années d'expérience en sécurité informatique • L'examen comporte 50 questions à choix multiples • Valide pour une période de 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 en menaces informatiques • Analystes du renseignement sur les menaces • Membres de l'équipe d'intervention en cas d'incident	• Global Knowledge • iClass • InfoSec Fournisseurs offrant aussi des cours en français : • Eccentrix
Computer Hacking Forensics Investigator (CHFI)	• Certification universellement reconnue • Programme de niveau expert qui s'adresse aux personnes devant composer régulièrement avec des cybermenaces • Elle atteste que les candidats sont versés dans les domaines de l'antipiratage, de la criminalistique numérique et des tests de	• Spécialistes du piratage contrôlé • Analystes du renseignement sur les menaces • Analystes de la criminalistique numérique et	• Global Knowledge • iClass • InfoSec • Learning Tree Fournisseurs offrant aussi

	pénétration • Les candidats sont des professionnels des TI et de la criminalistique ayant une connaissance de base en cybersécurité des TI, en criminalistique informatique et en intervention en cas d'incident • Il est recommandé d'obtenir au préalable la certification CEH • Elle est approuvée conformément à la directive 8140 du département de la Défense • L'examen comporte 150 questions à choix multiples • Valide pour une période de 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	de logiciels malveillants • Responsables de l'application des lois	des cours en français : • Eccentrix • Kereon
EC Council Disaster Recovery Professional (EDRP)	• Elle atteste que les candidats ont la base nécessaire pour sécuriser et rétablir des réseaux en cas de catastrophe, comme lors d'attaques malveillantes • Valide pour une période de 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 des risques informatiques • Consultants en continuité des activités et en reprise après catastrophe	• Global Knowledge • iClass • Near Secure Fournisseurs offrant aussi des cours en français : • Eccentrix
EC-Council Certified Encryption Specialist (ECES)	• Certification de premier échelon • Elle démontre que les candidats maîtrisent les compétences et les techniques nécessaires pour protéger les systèmes et les données importantes • Les candidats doivent avoir au moins une année d'expérience connexe en sécurité de l'information • Sans être une obligation, l'obtention de la certification CEH est	• Cryptanalystes • Cryptographes • Spécialistes du piratage contrôlé • Testeurs de pénétration	• Global Knowledge • iClass • SimpliLearn Fournisseurs offrant aussi des cours en français : • Eccentrix

	recommandée avant d'essayer de passer la formation et l'examen ECES • L'examen comporte 50 questions à choix multiples • Valide pour une période de 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		
EC-Council Certified Incident Handler (ECIH)	• Elle atteste que les candidats sont en mesure de créer des politiques en matière de traitement des incidents et d'intervention en cas d'incident, de traiter divers types d'incidents liés à la sécurité informatique, comme les incidents concernant la sécurité de réseau, les codes malveillants et les menaces internes • Les candidats doivent avoir une année d'expérience en sécurité informatique • L'examen comporte 100 questions à choix multiples • Valide pour une période de 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	• Gestionnaires des incidents • Responsables de l'évaluation des risques • Testeurs de pénétration • Administrateurs de système • Gestionnaires de réseaux	• Global Knowledge • iClass • Learning Class • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix
EC-Council Certified Security Analyst (ECSA)	• Certification de premier échelon • Les candidats doivent avoir deux années d'expérience connexe en sécurité de l'information • Elle satisfait à la norme de formation certifiée du GCHQ • Valide pour une période de 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 • Testeurs de pénétration • Administrateurs de coupe-feu • Testeurs de la sécurité • Administrateurs de serveur réseau	• CertBolt • iClass • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix
EC-Council Certified	• Certification de premier échelon	• Personnes intéressées à	• Global Knowledge

Security Specialist (ECSS)	• Elle atteste que les candidats comprennent les concepts fondamentaux de la sécurité de l'information, de la criminalistique informatique et de la sécurité de réseau • Les candidats doivent avoir une année d'expérience en sécurité informatique • L'examen comporte 50 questions à choix multiples • Valide pour une période de 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	apprendre les principes de base de la sécurité de l'information, de la sécurité de réseau et de la criminalistique informatique	• Kaplan • Udemy Fournisseurs offrant aussi des cours en français : • Eccentrix
Licensed Penetration Tester (LTP)	• Certification de niveau avancé • Les titulaires de la certification maîtrisent les techniques de cybersécurité • L'examen est la dernière étape du volet sur la sécurité de l'information offert par EC Council • Valide pour une période de 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 • Testeurs de pénétration • Administrateurs de serveur réseau • Professionnels de l'évaluation des risques	• Global Knowledge • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix

3.7 GLOBAL INFORMATION ASSURANCE CERTIFICATION (GIAC)

Table 7 Listes et descriptions des certifications de GIAC[9]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
GIAC Advanced Smartphone Forensics (GASF)	• Certification de niveau avancé • Elle 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 services mobiles, à l'analyse de système de fichiers d'appareils, au comportement des applications mobiles, à l'analyse d'événements liés à des artefacts et à l'analyse de maliciels qui s'attaquent aux appareils mobiles • Valide pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Assessing and Auditing Wireless Networks (GAWN)	• Certification de niveau avancé • Elle atteste que les candidats ont 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	• Vérificateurs • Spécialistes du piratage contrôlé • Testeurs de pénétration • Professionnels de la sécurité	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux

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

	fil • L'examen comporte 75 questions • Valide pour une période de 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	de réseau • Ingénieurs de système sans fil	examens
GIAC Certified Detection Analyst (GCDA)	• Certification de niveau avancé • Elle 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 une activité malveillante ou non autorisée • Les titulaires d'une certification GCDA ont les compétences pour occuper des postes de leadership nécessitant la gestion de l'information et des événements (ou SIEM pour *Security Information and Event Management*) • L'examen comporte 75 questions • Valide pour une période de 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 centre des opérations de sécurité • Enquêteurs de la cybercriminalité	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Certified Enterprise Defender (GCED)	• Certification de niveau avancé • Elle atteste les connaissances et les compétences des candidats dans les domaines de l'infrastructure réseau de défense, de l'analyse de paquets, du test de pénétration, du traitement des incidents et de la suppression de maliciels • L'examen comporte 115 questions • Valide pour une période de quatre ans • Le renouvellement de la certification demande de passer la version actuelle de l'examen ou d'obtenir 36 crédits de formation continue	• Intervenants en cas d'incident informatique • Testeurs de pénétration • Ingénieurs et analystes du centre des opérations de sécurité • Professionnels de la sécurité de réseau	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens

	pendant la période de quatre ans		
GIAC Certified Forensic Analyst (GCFA)	• Certification de niveau avancé • Elle 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 comme lors d'intrusions impliquant une violation de données internes et externes ou des menaces persistantes avancées • Valide pour une période de 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 centre des opérations de sécurité • Agents fédéraux et professionnels chargés de l'application de la loi • Analystes de la criminalistique numérique	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Certified Forensic Analyst (GCFA)	• Certification de niveau avancé • Elle atteste la capacité des candidats d'effectuer des enquêtes officielles sur des incidents et de traiter des scénarios de gestion de niveau avancé comme lors d'intrusions impliquant une violation de données internes et externes, des menaces persistantes avancées et des cas d'informatique judiciaire complexes • L'examen comporte jusqu'à 115 questions • Valide pour une période de 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 COS • Analystes de la criminalistique numérique	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Certified Forensic Examiner (GCFE)	• Certification de niveau intermédiaire • Elle 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	• Analystes de la sécurité de l'information • Membres des forces de l'ordre • Analystes de la	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens

	• L'examen comporte 115 questions • Valide pour une période de 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	criminalistique numérique et de logiciels malveillants • Analystes et enquêteurs judiciaires de la cyberdéfense	
GIAC Certified Incident Handler (GCIH)	• Certification de niveau intermédiaire • Elle 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 pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Certified Intrusion Analyst (GCIA)	• Certification de niveau avancé • Elle atteste les connaissances du candidat en matière de surveillance de réseau et d'hôtes, 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 pour une période de 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'hôtes, 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Certified Perimeter	• Certification de niveau avancé	• Administrateurs de système	• Aucune formation

Protection Analyst (GPPA)	• Elle atteste que les candidats ont les connaissances, les compétences et les capacités nécessaires pour concevoir, configurer et surveiller les routeurs, les coupe-feux et les systèmes de défense du périmètre • 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 • Elle atteste les compétences des candidats dans les huit domaines de connaissance en matière de cybersécurité déterminés par l'association (ISC)2, qui constituent un élément essentiel de l'examen CISSP • Elle démontre que les candidats ont des connaissances dans plusieurs spécialités : sécurité des actifs, sécurité des télécommunications et des réseaux, gestion de l'identité et de l'accès, gestion de la sécurité et des risques, évaluation de la sécurité et tests de sécurité, ingénierie de sécurité, opérations de sécurité et sécurité du développement de logiciels • Une certaine expérience en systèmes d'information et en réseaux est exigée • L'examen comporte 250 questions • Valide pour une période de 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 la sécurité informatique • Administrateurs de réseau • Gestionnaires de la sécurité	n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Certified UNIX Security Administrator (GCUX)	• Certification de niveau avancé • Elle atteste les connaissances des candidats en ce qui concerne le renforcement de la sécurité des systèmes Linux/Unix, la sécurité des applications Linux et la criminalistique numérique Linux/UNIX • L'examen comporte 75 questions	• Personnes responsables de l'installation, de la configuration et de la surveillance des systèmes UNIX ou Linux • Vérificateurs	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens

	• Valide pour une période de 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	
GIAC Certified Web Application Defender (GWEB)	• Certification de niveau avancé • Elle démontre que les candidats maîtrisent les connaissances et les compétences 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 • Valide pour une période de 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	• Développeurs d'applications • Analystes de la sécurité des applications • Architectes d'applications • Testeurs de pénétration • Personnes dont les responsabilités exigent une conformité PCI	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Certified Windows Security Administrator (GCWN)	• Certification de niveau avancé • Elle atteste la capacité des candidats de protéger 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 pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Continuous Monitoring Certification (GMON)	• Certification de niveau avancé • Elle atteste la capacité des candidats de prévenir les intrusions et de détecter rapidement toute activité suspecte • L'examen comporte 115 questions	• Architectes de la sécurité • Analystes et gestionnaires du centre des opérations de sécurité	• Aucune formation n'est exigée, mais le SANS Institute offre des services de

	• Valide pour une période de 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 de la sécurité technique • Ingénieurs de sécurité	préparation aux examens
GIAC Critical Controls Certification (GCCC)	• Certification de niveau avancé • La seule certification basée sur des contrôles de sécurité essentiels qui font appel à une approche priorisée de la sécurité fondée sur les risques • Elle atteste que les candidats possèdent les connaissances et les compétences nécessaires pour mettre en œuvre et exécuter les contrôles de sécurité 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 • Valide pour une période de 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 des TI • Personnel du département de la Défense • Ingénieurs de la sécurité de réseau • Fournisseurs de services de sécurité • Vérificateurs de la sécurité, dirigeants principaux de l'information et responsables de l'évaluation des risques	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Critical Infrastructure Protection (GCIP)	• Certification de niveau avancé • Elle 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 critiques (CIP pour *Critical Infrastructure Protection*) et pour préparer des stratégies d'exécution pratiques afin d'assurer la conformité à la réglementation • L'examen comporte 75 questions • Valide pour une 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)	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens

	• 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 Cyber Threat Intelligence (GCTI)	• Certification de niveau avancé • Elle 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 pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Defending Advanced Threats (GDAT)	• Certification de niveau avancé • Elle atteste que les candidats ont une bonne connaissance 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 pour une période de 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 sécurité • Gestionnaires de la sécurité technique	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Defensible Security Architecture (GDSA)	• Certification de niveau avancé • Elle 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 de protocoles TCP/IP ainsi que de la création d'un	• Architectes de la sécurité • Ingénieurs de réseau • Analystes de la sécurité • Enquêteurs de la cybercriminalité • Ingénieurs principaux de la	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens

	environnement sécurisé au moyen de nuages privés, hybrides ou publics • L'examen comporte 75 questions • Valide pour une période de 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	sécurité • Analystes de la sécurité	
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	• Certification de niveau avancé • Elle atteste la capacité des candidats de trouver et d'atténuer les vulnérabilités informatiques dans des systèmes et des réseaux • L'examen comporte de 55 à 75 questions • Valide pour une période de 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 la vulnérabilité • Analystes de la sécurité • Analystes de l'évaluation des vulnérabilités	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Information Security Fundamentals (GISF)	• Certification de niveau débutant • Elle atteste que les candidats ont des connaissances en ce qui a trait aux bases de la sécurité, aux fonctions informatiques et à la gestion de réseaux, à la cryptographie de base, et aux technologies de cybersécurité • L'examen comporte 75 questions • Valide pour une période de 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 gestion • Agents de la sécurité de l'information • Administrateurs de système • Professionnels qui ont besoin d'une introduction aux principes de base de la cybersécurité	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Information Security Professional (GISP)	• Certification de niveau intermédiaire pour gestionnaires et leaders • Elle atteste que les candidats ont des connaissances dans les huit domaines de connaissance en matière de cybersécurité : sécurité	• Administrateurs de système • Administrateurs de la sécurité informatique	• Aucune formation n'est exigée, mais le SANS Institute offre

	des actifs, sécurité des télécommunications et des réseaux, gestion de l'identité et de l'accès, gestion de la 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 gestion de réseaux • L'examen comporte 250 questions • Valide pour une période de 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 réseau • Gestionnaires de la sécurité	des services de préparation aux examens
GIAC Mobile Device Security Analyst (GMOB)	• Certification de niveau avancé • Elle atteste que les candidats sont aptes à sécuriser adéquatement des dispositifs mobiles ayant accès à de l'information vitale • Elle 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 pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Network Forensic Analyst (GNFA)	• Certification de niveau avancé • Elle 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	• Membres d'organismes d'application de la loi • Analystes de la criminalistique numérique et de logiciels malveillants	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux

	• Valide pour une période de 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 cyberdéfense • Membres de l'équipe d'intervention en cas d'incident • Membres de l'équipe du centre des opérations de sécurité	examens
GIAC Penetration Tester (GPEN)	• Certification de niveau avancé • Elle atteste que les candidats ont la capacité d'effectuer adéquatement un test de pénétration en se servant de techniques et de méthodologies répondant à des pratiques exemplaires • L'examen comporte jusqu'à 115 questions • Valide pour une période de 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 • Concepteurs d'exploit • Personnel de la sécurité de réseau • Spécialistes du piratage contrôlé	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Response and Industrial Defence (GRID)	• Certification de niveau avancé • Elle 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 pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Response and Industrial Defense (GRID)	• Certification de niveau avancé • Elle atteste que les candidats comprennent l'approche de défense active et les attaques propres aux SCI et qu'ils savent comment	• Membres de l'équipe d'intervention en cas d'incident sur les SCI	• Aucune formation n'est exigée, mais le SANS Institute offre

	ces attaques guident les stratégies d'atténuation • L'examen comporte 75 questions • Valide pour une période de 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	• Défenseurs actifs • Chefs d'équipe et analystes du centre des opérations de sécurité	des services de préparation aux examens
GIAC Reverse Engineering Malware (GREM)	• Certification de niveau avancé • Elle atteste que les candidats possèdent les connaissances et les compétences nécessaires pour faire la rétro-ingénierie des maliciels qui ciblent des plateformes communes comme Microsoft Windows et des navigateurs Web • L'examen comporte 75 questions • Valide pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Security Essentials Certification (GSEC)	• Certification de premier échelon • Elle 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 sur la sécurité, en traitement des incidents et en protection de réseau • L'examen comporte 180 questions • Valide pour une période de 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	• Professionnels de la sécurité	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens

GIAC Security Expert (GSE)	• On compte moins de 250 titulaires de la certification GSE dans le monde • Elle 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 pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Security Leadership (GSLC)	• Certification de niveau avancé pour gestionnaires et leaders • Elle atteste les connaissances des candidats en matière de gouvernance et de contrôles techniques axés sur la protection et la détection des problèmes de sécurité et l'intervention face à ceux-ci • L'examen comporte 115 questions • Valide pour une période de 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	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
GIAC Systems and Network Auditor (GSNA)	• Certification de niveau avancé pour gestionnaires et leaders • Elle 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	• Personnel technique responsable de sécuriser et de vérifier les systèmes d'information	• Aucune formation n'est exigée, mais le SANS Institute offre des services de

	• L'examen comporte 115 questions • Valide pour une période de 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 • Administrateurs de réseau • Gestionnaires des équipes de vérification ou de sécurité	préparation aux examens
GIAC Web Application Penetration Tester (GWAPT)	• Certification de niveau avancé • Elle 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 • Elle 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 pour une période de 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 la vulnérabilité • Analystes de la sécurité • Analystes de l'évaluation des vulnérabilités • Spécialistes du piratage contrôlé • Concepteurs de site Web	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens
Global Industrial Cyber Security Professional (GICSP)	• Certification de niveau avancé • Elle 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 pour une période de 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 en sécurité • Cadres industriels • Analystes de la sécurité	• Aucune formation n'est exigée, mais le SANS Institute offre des services de préparation aux examens

3.8 INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM

Table 8 Listes et descriptions des certifications de l'association (ISC)2[10]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Certified Cloud Security Professional (CCSP)	• Développée en collaboration avec la Cloud Security Alliance (CSA) • Elle reconnaît les chefs de la sécurité des technologies de l'information (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 un des six domaines du corpus de connaissances communes menant à la certification CCSP • L'examen comporte 125 questions à choix multiples • Valide pour une période de 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 informatique • Chefs de la sécurité des TI et de l'information	• Beyond20 • Cyper • Deloitte • Farro Technics • Global Knowledge • Knowledge Academy • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix
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	• Dirigeants principaux de la sécurité de l'information • Chefs de la sécurité	• Beyond 20 • Cyper • Deloitte

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

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.

	de connaissances communes offerts par l'association (ISC)2, ou quatre années d'expérience professionnelle et un diplôme universitaire ou tout autre certificat accrédité
	• Elle est approuvée conformément à la directive 8570.01 du département de la Défense des États-Unis
	• L'examen comporte 100 à 150 questions utilisant la stratégie du test adaptatif informatisé (TAI)
	• Valide pour une période de 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 personnes entreprenant des démarches pour l'obtention d'une certification CISSP valide
	  ○ CISSP-ISSAP (architecture)
	  ○ CISSP-ISSEP (ingénierie)
	  ○ CISSP-ISSMP (gestion)
		• Analystes ou vérificateurs de la sécurité
		• Directeurs de la sécurité
		• Directeurs ou gestionnaires des TI
			• Fanshaw College
			• Ferro Technics
			• Global Knowledge
			• Knowledge Academy
			• Learning Tree
			• Ryerson University
			• Seneca College
			• Université York
			Fournisseurs offrant aussi des cours en français :
			• Collège de Maisonneuve
			• Eccentrix
			• HEC Montréal

Healthcare Information Security and Privacy Practitioner (HCISPP)	• Elle atteste que les candidats ont les connaissances et les compétences nécessaires pour mettre en œuvre les contrôles de sécurité et de confidentialité touchant les renseignements sur la santé et les patients • Elle est conçue pour les praticiens et les consultants dont le travail demande le respect de la sécurité et de la confidentialité des renseignements • Les candidats doivent avoir un minimum de deux années d'expérience professionnelle • L'examen comporte 125 questions à choix multiples • Valide pour une période de trois ans • Le renouvellement de la certification exige 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	• Cyper • Intrinsec • Learning Tree

Systems Security Certified Practitioner (SSCP)	• Certification mondiale en sécurité informatique • Certification de premier échelon • Elle démontre que les titulaires de cette certification possèdent les compétences et les connaissances techniques pour mettre en œuvre, surveiller et administrer une infrastructure informatique • Elle est conçue pour les praticiens qui remplissent des fonctions informatiques opérationnelles ou qui travaillent en sécurité de l'information • Les candidats doivent avoir une année d'expérience professionnelle cumulative dans au moins 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 pour une période de 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 de réseau • Administrateurs de système • Analystes de la sécurité • Analystes de système et de réseau • Consultants en sécurité • Administrateurs, directeurs ou gestionnaires des TI	• Beyond20 • Cyper • Ferro Technics • Global Knowledge • Learning Tree Fournisseurs offrant aussi des cours en français : • Eccentrix

3.9 ISACA

Table 9 Listes et descriptions des certifications de l'association ISACA[11]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Certified Cybersecurity Practitioner (CSX-P)	• Cette nouvelle certification a été créée en 2015 • Elle 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 pour une période de trois ans • Le renouvellement de la certification exige l'obtention de 120 crédits de formation professionnelle continue pendant la période de trois ans	• Praticiens de la sécurité • Gestionnaires des incidents	• Global Knowledge • Intrinsec Security • Learning Tree
Certified in Risk and Information Systems Control (CRISC)	• Elle 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	• Professionnels du milieu informatique et des affaires • Professionnels spécialistes des risques et de la conformité	• Global Knowledge • Knowledge Academy • Learning Tree Fournisseurs offrant aussi des cours en français :

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

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.

	ne peut pas remplacer l'expérience • Valide pour une période de trois ans • Le renouvellement de la certification exige l'obtention de 120 crédits de formation professionnelle continue pendant la période de trois ans	• Analystes des activités • Gestionnaires de projet • Directeurs de la sécurité	• 2AB & Associates
Certified Information Security Manager (CISM)	• Certification axée sur la gestion • Elle reconnaît les candidats qui gèrent, conçoivent, coordonnent 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 pour une période de trois ans • Le renouvellement de la certification exige l'obtention de 120 crédits de formation professionnelle continue pendant la période de trois ans	• Gestionnaires et directeurs de la sécurité de l'information • Analystes de la sécurité informatique • Analystes des risques • Vérificateurs des TI • Gestionnaires de la sécurité des systèmes d'information	• Global Knowledge • Knowledge Academy • Learning Tree • Université de Toronto Fournisseurs offrant aussi des cours en français : • 2AB & Associates
Certified Information Systems Auditor (CISA)	• Certification universellement reconnue • Elle 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; certains critères d'éducation peuvent remplacer l'expérience • L'examen comporte 150 questions • Les titulaires de cette certification doivent suivre au moins	• Professionnels du contrôle de vérification, de l'assurance de la qualité et de la sécurité des systèmes d'information	• Ferro Technics • Global Knowledge • Knowledge Academy • Learning Tree • Netcom Learning • NobleProg • SimpliLearn Fournisseurs offrant aussi des cours en français : • 2AB & Associates

	120 heures de formation continue pendant la période de trois ans		

3.10 ITSM SOLUTIONS

Table 10 Listes et descriptions des certifications d'itSM Solutions[12]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
NCSF Foundation	• Certification de premier échelon • Elle atteste que les candidats ont les connaissances et les capacités nécessaires pour opérationnaliser le cadre de cybersécurité du NIST NIST Cyber Security Framework (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 100 questions à choix multiples	• Professionnels de la sécurité, des TI ou de la gestion des risques • Vérificateurs • D'autres professionnels devant comprendre les bases de la cybersécurité, les composantes du NCSF et leur application dans le cadre de la gestion des risques	• Knowledge Peak • LRS Education Services • University of Connecticut
NCSF Practitioner	• Elle atteste que les candidats ont les compétences et les capacités nécessaires pour concevoir, établir, tester, gérer et améliorer un programme de cybersécurité basé sur la certification NCSF • Les candidats doivent avoir terminé la formation et l'examen NCSF Foundation avant d'essayer de passer l'examen • L'examen comporte 100 questions à choix multiples	• Professionnels des TI et de la cybersécurité	• Knowledge Peak • LRS Education Services • University of Connecticut

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

3.11 MCAFEE INSTITUTE

Table 11 Listes et descriptions des certifications du McAfee Institute[13]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Certified Counterintelligence Threat Analyst (CCTA)	• Elle atteste la capacité des candidats d'identifier et d'enquêter les cybercriminels, 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 pour une période de deux ans • Pour renouveler, 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	• Sans objet
Certified Cyber Intelligence Investigator (CCII)	• Elle 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	• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes	• Sans objet

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

	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 pour une période de deux ans • Pour renouveler, les candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue		
Certified Cyber Intelligence Professional (CCIP)	• Elle 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 pour une période de deux ans • Pour renouveler, 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	• Sans objet
Certified Expert in Cyber Investigations (CECI)	• Elle 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	• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes	• Sans objet

	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 pour une période de deux ans • Pour renouveler, les candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue		

3.12 OFFENSIVE SECURITY

Table 12 Listes et descriptions des certifications Offensive Security[14]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Offensive Security Certified Expert (OSCE)	• Elle 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 le système Linux, et posséder une connaissance approfondie des réseaux TCP/IP • 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 isolé; les candidats doivent également présenter un rapport de test exhaustif	• Testeurs de pénétration • Professionnels de la sécurité	• Sans objet
Offensive Security Certified Professional (OSCP)	• Elle 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 • Elle s'adresse aux testeurs de pénétration possédant un solide	• Testeurs de pénétration • Administrateurs de réseau • Professionnels de la sécurité de réseau	• Sans objet

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

	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 d'une durée de 24 heures au cours desquelles ils doivent réussir à attaquer et à pénétrer des systèmes opérationnels dans des conditions d'essai en laboratoire sécuritaires; ils doivent également présenter un rapport de test de pénétration exhaustif • La certification n'expire jamais		
Offensive Security Exploitation Expert (OSEE)	• Elle exige beaucoup de temps • Elle 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	• Sans objet

Offensive Security Web Expert (OSWE)	• Elle 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 un 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 le système Linux, être en mesure d'écrire des scripts et avoir de l'expérience avec les mandataires Web, une compréhension générale des vecteurs d'attaque, en théorie et en pratique, et une connaissance approfondie des réseaux TCP/IP • 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 réseau privé virtuel 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 en logiciels • Développeurs Web	• Sans objet
Offensive Security Wireless Professional (OSWP)	• Elle atteste la capacité des candidats de trouver des vulnérabilités et des chiffrements en place dans des réseaux répondant à la norme 802.11, de contourner des restrictions liées à la sécurité et de récupérer les clés de chiffrement utilisées • Les candidats doivent avoir une compréhension approfondie des réseaux TCP/IP et du modèle OSI, et avoir une connaissance du système Linux • Les candidats doivent avoir terminé le cours intitulé *Offensive Security Wireless Attacks* avant de passer l'examen • L'examen d'une durée 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 de test de pénétration	• Administrateurs de réseau • Testeurs de pénétration	• Sans objet

	• La certification n’expire jamais		

3.13 SECO INSTITUTE

Table 13 Listes et descriptions des certifications du SECO Institute[15]

Certification	Aperçu de la certification	Candidats ciblés	Fournisseurs/ Responsables de la formation
Certified Ethical Hacker (S-EHE)	• Le programme fait l'objet d'une restructuration	• Sans objet	• Sans objet
Dark Web Foundations	• Certification de premier échelon • Elle a été développée par la Netherlands Organisation for Applied Scientific Research en collaboration avec INTERPOL • Elle démontre que les candidats comprennent l'utilisation du Web invisible de manière sécuritaire • L'examen comporte 40 questions à choix multiples • Valide pour une période de trois ans	• Professionnels de la sécurité informatique • Employés d'organismes d'application de la loi • Responsables des politiques et représentants de gouvernement	• APMG International • Innovative Learning • Security Academy
Ethical Hacking Foundations (S-EHF)	• Certification de premier échelon • Elle atteste que les candidats ont une connaissance approfondie des techniques de base de test de pénétration et qu'ils comprennent les principes fondamentaux du piratage • L'examen comporte 40 questions à choix multiples	• Développeurs Web • Ingénieurs en logiciels • Administrateurs de la sécurité informatique • Ingénieurs de réseau • Spécialistes du piratage contrôlé	• Global Knowledge • Security Academy

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

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.

Ethical Hacking Practitioner (S-EHP)	• Elle atteste que les candidats comprennent pleinement le processus du test de pénétration et qu'ils maîtrisent les techniques communes de ce test • Les candidats doivent bien comprendre les principes de base du piratage contrôlé • Une certification S-EHF (ou l'équivalent) est recommandée • Examen en trois volets : Il comporte dix questions à choix multiples, cinq questions de type rédactionnel et une étude de cas • Pour un renouvellement, les candidats doivent payer une cotisation annuelle et obtenir 60 crédits de formation continue sur une période de trois ans	• Développeurs Web • Administrateurs de la sécurité informatique • Ingénieurs de réseau • Ingénieurs en logiciels • Testeurs de pénétration potentiels	• Global Knowledge • Security Academy
IT Security Expert/SOC (S-ITSE/SOC)	• Elle atteste que les candidats ont les connaissances et les compétences nécessaires pour prendre en charge la détection et l'analyse de menaces et l'intervention en cas de menaces, et pour améliorer l'ensemble de la sécurité d'une organisation • Les candidats doivent avoir une compréhension de base des protocoles TCP/IP, des principes fondamentaux des systèmes d'exploitation et des concepts de sécurité communs, et posséder deux années d'expérience dans un COS • Le préalable exigé est la certification S-ITSP ou l'équivalent • Valide pour une période de trois ans • Pour un renouvellement, les candidats doivent payer une cotisation annuelle et obtenir 120 crédits de formation continue sur la période de trois ans	• Personnes aspirant à devenir des analystes de COS de palier 1 et de palier 2 • Futurs gestionnaires du COS • Ingénieurs de système • Analystes de la sécurité	• Global Knowledge • Security Academy
IT Security Foundation (S-ITSF)	• Certification de premier échelon • Elle atteste que les candidats ont une connaissance de base de l'architecture informatique, des vulnérabilités matérielles communes et des mesures de sécurité • Aucun préalable n'est exigé; elle convient aux débutants qui ont	• Administrateurs de réseau ou de système • Personnes qui désirent entamer une carrière en sécurité informatique	• APMG International • Global Knowledge • Mangates • Security Academy

	quelques connaissances de base en informatique et en technologie • L'examen comporte 40 questions à choix multiples • Valide pour une période de trois ans		
IT Security Practitioner (S-ITSP)	• Elle 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 du principe de base de la sécurité informatique • Une 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 pour une période de trois ans • Pour un renouvellement, les candidats doivent payer une cotisation annuelle et obtenir 60 crédits de formation continue sur la période de trois ans	• Administrateurs de la sécurité informatique • Analystes de la sécurité • Architectes de la sécurité • Vérificateurs de la sécurité • Futurs analystes du centre des opérations de sécurité	• Global Knowledge • Security Academy