



Centre de la sécurité  
des télécommunications

Communications  
Security Establishment

# CENTRE CANADIEN POUR LA **CYBERSÉCURITÉ**

## Certifications dans le domaine de la cybersécurité

© Gouvernement du Canada

Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

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 étudiantes et étudiants potentiels et aux professionnelles et 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 employées et employés à progresser sur le plan professionnel dans le domaine de la cybersécurité.

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

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

## HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première version	Novembre 2020
2	Ajout de nouvelles certifications et retrait de fournisseurs de formation	Juillet 2022
3	Mise à jour de l'information relative à Rogers Cybersecure Catalyst	Avril 2023
4	Changement du nom d'une équipe et ajout de nouvelles certifications	Novembre 2023
5	Certifications mises à jour et OSDA ajouté	Juin 2024

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

# TABLE DES MATIÈRES

<b>1.0</b>	<b>Introduction.....</b>	<b>5</b>
1.1	Le Centre canadien pour la cybersécurité .....	5
1.2	Objet.....	5
<b>2.0</b>	<b>Organismes de certification reconnus mondialement .....</b>	<b>6</b>
2.1	CertNexus .....	6
2.2	Cisco Systems.....	6
2.3	Computing Technology Industry Association .....	7
2.4	Council for Registered Ethical Security Testers .....	7
2.5	Certified Wireless Network Professionals .....	8
2.6	EC-Council .....	8
2.7	Global Information Assurance Certification .....	8
2.8	International Information Systems Security Certification Consortium.....	9
2.9	ISACA .....	9
2.10	itSM Solutions.....	10
2.11	McAfee Institute.....	10
2.12	Offensive Security .....	11
2.13	PECB .....	11
2.14	SECO INSTITUTE .....	12
<b>3.0</b>	<b>Cyber Credentials Collaborative .....</b>	<b>12</b>
<b>4.0</b>	<b>ROGERS CYBERSECURE CATALYST .....</b>	<b>13</b>
<b>5.0</b>	<b>Liste et description des certifications en cybersécurité .....</b>	<b>14</b>
5.1	CertNexus .....	14
5.2	Cisco Systems.....	17
5.3	CompTIA.....	19
5.4	Council for Registered Ethical Security Testers (CREST).....	22
5.5	Certified Wireless Network Professions (CWNP).....	24
5.6	EC-Council .....	25
5.7	Global Information Assurance Certification (GIAC).....	35
5.8	International Information Systems Security Certification Consortium.....	46
5.9	ISACA .....	49
5.10	itSM Solutions.....	51
5.11	McAfee Institute.....	52

5.12	Offensive Security .....	54
5.13	PECB .....	57
5.14	SECO Institute .....	66
<b>6.0</b>	<b>Contenu complémentaire .....</b>	<b>69</b>
6.1	Liste d'abréviations, d'acronymes et de sigles .....	69
6.2	Références.....	70

## LISTE DES TABLEAUX

Tableau 1 :	Liste et description des certifications de CertNexus .....	14
Tableau 2 :	Liste et description des certifications de Cisco Systems.....	17
Tableau 3 :	Liste et description des certifications de CompTIA.....	19
Tableau 4 :	Liste et description des certifications de CREST.....	22
Tableau 5 :	Liste et description des certifications de CWNP .....	24
Tableau 6 :	Liste et description des certifications de l'EC-Council.....	25
Tableau 7 :	Liste et description des certifications de GIAC .....	35
Tableau 8 :	Liste et description des certifications de l'association (ISC)2 .....	46
Tableau 9 :	Liste et description des certifications de ISACA .....	49
Tableau 10 :	Liste et description des certifications d'itSM Solutions.....	51
Tableau 11 :	Liste et description des certifications du McAfee Institute.....	52
Tableau 12 :	Liste et description des certifications d'Offensive Security .....	54
Tableau 13 :	Liste et description des certifications de PECB .....	57
Tableau 14 :	Liste et description des certifications du SECO Institute .....	66

## 1.0 INTRODUCTION

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

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

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

### 1.1 LE CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) a été mis sur pied sous l'égide du Centre de la sécurité des télécommunications (CST) en octobre 2018. L'équipe de Développement de cybercompétences du Centre pour la cybersécurité travaille de concert avec les universités, les collèges, les associations éducatives, les comités ministériels à vocation éducative et des membres du corps professoral du secteur privé afin d'accroître les capacités et le bassin de candidates et candidats talentueux en cybersécurité au Canada. L'équipe collabore aussi avec les professeures et 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 des étudiantes, des étudiants des professionnelles ou professionnels éventuels de la cybersécurité qui cherchent à faire progresser leur carrière dans le domaine. Le guide met en lumière certaines des certifications les plus demandées et reconnues mondialement qu'offrent des fournisseurs à travers le monde. Une liste complète des certifications se trouve à la fin du guide (tableaux 1 à 14).

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

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

## 2.0 ORGANISMES DE CERTIFICATION RECONNUS MONDIALEMENT

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

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

### 2.1 CERTNEXUS

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

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

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

### 2.2 CISCO SYSTEMS

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

- **Débutant** : Le point de départ pour les personnes qui désirent entamer une carrière de professionnel des réseaux.
- **Associé** : Les candidates et candidats maîtrisent les éléments essentiels requis pour entreprendre une carrière et élargir leurs perspectives d'emploi grâce aux plus récentes technologies.
- **Professionnel** : Les candidates et candidats choisissent un volet en technologie de base et un examen axé sur une concentration afin de personnaliser leur certification de niveau professionnel.

- **Expert** : La certification est reconnue partout dans le monde comme étant la certification la plus prestigieuse de l'industrie des technologies.
- **Architecte** : Ce niveau permet de démontrer l'expertise architecturale d'un concepteur de réseaux.

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

## 2.3 COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION

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

- La certification **CompTIA Advanced Security Practitioner (CASP+)** est axée sur le rendement et elle s'adresse davantage aux praticiennes et 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 professionnelles et professionnels en cybersécurité chargés des tests de pénétration et de la gestion des vulnérabilités. Les titulaires de cette certification ont démontré que leurs connaissances et leurs compétences pratiques sont à jour et qu'ils sont en mesure de tester des dispositifs dans de nouveaux environnements (p. ex. en nuage ou mobiles), ainsi que des ordinateurs et des serveurs traditionnels.
- La certification **CompTIA Security+** est une certification de premier échelon. Les titulaires de cette certification sont des expertes et 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 candidates et candidats doivent posséder deux années d'expérience en sécurité des réseaux et avoir déjà obtenu leur certification **Network+**.

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

## 2.4 COUNCIL FOR REGISTERED ETHICAL SECURITY TESTERS

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

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

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

## 2.5 CERTIFIED WIRELESS NETWORK PROFESSIONALS

---

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

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

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

## 2.6 EC-COUNCIL

---

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

- Le titre de compétence **Certified Ethical Hacker (ANSI)** atteste les compétences des candidates et candidats dans cinq phases du piratage contrôlé : la reconnaissance, l'énumération, l'obtention de l'accès, le maintien de l'accès et le brouillage de pistes. Cette certification exige de passer un examen de quatre heures comportant 125 questions.
- La certification **Certified Ethical Hacker (Practical)** cible l'application des compétences CEH dans le cadre de défis concrets d'audit de sécurité et d'autres scénarios connexes. Les candidates et 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 candidates et 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 versées et versés dans les domaines de l'antipiratage, de la criminalistique numérique et des tests de pénétration.
- Les titulaires de la certification **Certified Network Defender (CND)** démontrent une connaissance approfondie de la sécurité axée sur la défense et l'expertise nécessaire pour sécuriser des données.
- Les titulaires de la certification **EC-Council Disaster Recovery Professional (EDRP)** disposent des bases nécessaires pour leur permettre de sécuriser et de rétablir des réseaux en cas de catastrophe, comme lors d'attaques malveillantes.

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

## 2.7 GLOBAL INFORMATION ASSURANCE CERTIFICATION

---

Le programme **Global Information Assurance Certification** (GIAC), fondé par le SANS Institute, est spécialisé dans la certification technique et pratique. Les certifications offertes sont liées à des cours de formation dispensés par le SANS Institute. Elles sont reconnues dans le monde entier. Les candidates et candidats qui demandent une certification de

**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.



catégorie *Expert Status* doivent uniquement passer un examen pour l'obtention de la certification, celle-ci étant valide pendant quatre ans. Pour être admissibles à un renouvellement à la fin de la période de quatre ans, les titulaires de la certification doivent avoir accumulé 36 crédits de formation continue et avoir payé les frais de renouvellement de la certification ou avoir repassé l'examen. Les personnes désirant obtenir une certification de catégorie *Gold Status* doivent faire des recherches et rédiger un rapport technique ou un livre blanc. Cette catégorie démontre que les titulaires ont des connaissances plus approfondies dans un domaine particulier.

- La certification **GIAC Security Essential Certification** (GSEC) atteste que les connaissances des candidates et 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 praticiennes et 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 candidates et candidats de détecter les incidents liés à la sécurité informatique, d'y intervenir et de les régler en faisant appel à un large éventail de compétences essentielles en sécurité. Les titulaires d'une certification GCIH possèdent une connaissance approfondie des techniques courantes de cyberattaque et des mécanismes de défense contre celles-ci.

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

## 2.8 INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM

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

L'association (ISC)<sup>2</sup> 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)<sup>2</sup>, ou quatre années d'expérience et un diplôme universitaire ou des certificats accrédités. Les candidates et candidats doivent également passer un examen écrit de trois heures. Le renouvellement de la certification est requis tous les trois ans. Pour renouveler leur certification, les candidates et 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)<sup>2</sup> se trouve à la section 5.8.

## 2.9 ISACA

L'**ISACA**, anciennement Information Systems Audit and Control Association, est une association professionnelle internationale axée sur la gouvernance des TI. Elle compte plus de 140 000 membres, professionnelles 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.

**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.

Les candidates et 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 professionnelles et professionnels des TI chargés de la gestion, du développement et de la surveillance des systèmes de sécurité de l'information dans les applications d'entreprise, ou de l'élaboration de pratiques exemplaires en matière de sécurité organisationnelle. Outre l'examen écrit, les candidates et 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 candidates et candidats d'identifier, d'évaluer et de répondre aux risques liés aux TI. Les candidates et 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 premières intervenantes et premiers intervenants lors d'incidents de sécurité. Créée en 2015, cette certification évalue la capacité des candidates et candidats d'exécuter des vérifications de cybersécurité validées mondialement et couvrant les cinq fonctions de base du cadre de cybersécurité du NIST (NCSF pour *NIST Cyber Security Framework*) : identification, protection, détection, intervention et récupération. Pour obtenir la certification, les candidates et candidats doivent passer un examen de quatre heures basé sur le rendement et comportant des simulations d'incidents de sécurité. À la fin de la période de certification de trois ans, les titulaires doivent passer la version la plus récente de l'examen donnant droit au renouvellement de la certification.

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

## 2.10 ITSM SOLUTIONS

---

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

- **NCSF Foundation** : Pour les cadres, les professionnelles et les professionnels du milieu informatique et des affaires qui doivent connaître les principes de base du NCSF 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 NCSF et à savoir comment l'adapter et l'opérationnaliser.

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

## 2.11 MCAFFEE INSTITUTE

---

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

- La certification **Certified Cyber Intelligence Professional (CCIP)** a été conçue en parallèle avec le National Cyber Security Workforce Framework du département de la Sécurité intérieure. Cette certification démontre que des

employées et employés peuvent identifier des personnes d'intérêt, mener rapidement des enquêtes de cybersécurité et poursuivre en justice des cybercriminels. Les candidates et candidats doivent détenir un baccalauréat ou un diplôme de niveau supérieur, et avoir trois années d'expérience dans les secteurs des enquêtes, des TI, de la fraude, de l'application de la loi, de la criminalistique, de la justice pénale, du droit et de la prévention des pertes.

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

## 2.12 OFFENSIVE SECURITY

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

- La certification **Offensive Security Certified Professional (OSCP)** est considérée comme l'une des plus difficiles à obtenir en raison du degré de difficulté de son examen. Les candidates et candidats doivent réussir, en 24 heures, à attaquer et à pénétrer des systèmes opérationnels dans des conditions d'essai en laboratoire sécuritaires. En raison de son caractère pratique, cet examen s'adresse aux testeuses et testeurs de pénétration possédant un solide bagage technique et en piratage contrôlé. Avant d'essayer de passer l'examen, les candidates et 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)<sup>2</sup>. Contrairement à beaucoup des autres certifications en cybersécurité, la certification OSCP n'expire jamais.
- La **certification OSDA (Security Operations and Defensive Analysis)** est conçue sur mesure pour les professionnelles et professionnels des TI comme les analystes de centres des opérations de sécurité, les analystes des cybermenaces et du renseignement, ainsi que d'autres professionnelles et professionnels participant à la protection de l'environnement TI d'une organisation. Cette certification englobe plusieurs domaines d'importance critique, comme la gestion des incidents, qui permet aux candidates et aux candidats d'apprendre comment détecter les incidents de sécurité, intervenir en cas d'incident et assurer la reprise des activités, le tout efficacement. Elle aborde aussi le renseignement sur les menaces, qui nécessite une compréhension des menaces émergentes et l'application des connaissances qui les concernent, de même que la surveillance en matière de sécurité, où l'accent est mis sur l'identification des activités suspectes grâce à l'analyse des réseaux et des journaux. La gestion des vulnérabilités et les techniques de cyberdéfense sont aussi traitées, en vue de munir les professionnelles et professionnels des compétences voulues pour évaluer et atténuer les vulnérabilités, et mettre en œuvre de robustes stratégies de défense contre les cybermenaces. En outre, cette certification permet de gagner en aisance à configurer et surveiller un dispositif GIES pour détecter des attaques actives contre le réseau, et d'apprendre à inspecter manuellement des journaux en vue de différencier les activités normales des activités anormales. Le processus de certification nécessite que les participants mènent à bien une formation approfondie, suivi d'un examen rigoureux qui met à l'épreuve tant leurs connaissances théoriques que leurs compétences pratiques dans les domaines susmentionnés. Avant de tenter d'obtenir cette certification, les candidates et candidats éventuels doivent avoir suivi les cours Linux, Windows et Network Basics de l'entreprise Offensive Security.

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

## 2.13 PECB

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

personnes certifiées, présent dans plus de 150 pays. PECB détient un agrément de l'International Accreditation Service (IAS) et du United Kingdom Accreditation Service (UKAS).

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

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

## 2.14 SECO INSTITUTE

Le **Security & Continuity Institute** (SECO) est un institut européen qui offre des certifications de haut niveau touchant la sécurité et la continuité. Le programme de certification du SECO comporte sept volets de certification, chacun axé sur un domaine d'expertise particulier comme la sécurité des TI, la confidentialité des données et le piratage contrôlé. Les volets commencent au niveau de base (*Foundation*), et se poursuivent avec les niveaux praticien (*Practitioner*) et expert (*Expert*). Les candidates et 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 professionnelles et professionnels qui désirent faire carrière dans le domaine. Les titulaires de cette certification comprennent les principes fondamentaux du piratage contrôlé et sont en mesure d'effectuer des tests de pénétration de base. Bien qu'il n'y ait pas de préalables pour cette certification, une connaissance de base de Linux est recommandée.
- La certification **Ethical Hacking Practitioner** (S-EHP) s'adresse aux professionnelles et professionnels qui ont déjà une connaissance solide des fondements du piratage contrôlé. L'obtention préalable de la certification S-EHF est recommandée. Les titulaires de cette certification ont démontré qu'elles et ils comprennent pleinement le processus de test de pénétration et qu'ils connaissent les techniques courantes de test de pénétration.

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

## 3.0 CYBER CREDENTIALS COLLABORATIVE

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

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

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

## 4.0 ROGERS CYBERSECURE CATALYST

Rogers Cybersecure Catalyst et le centre national d'innovation et de collaboration en cybersécurité de l'Université métropolitaine de Toronto ont établi un partenariat avec le SANS Institute pour offrir un programme intensif de certification et de formation en cybersécurité. Le programme [Certifications for Leadership in Cybersecurity \(CLIC\)](#) (offert en anglais seulement) est un programme virtuel à temps partiel de 6 mois permettant aux étudiantes et étudiants d'apprendre les compétences dont ils ont besoin pour entreprendre une carrière dans le domaine de la cybersécurité. Les diplômées et diplômés obtiendront les deux certifications GIAC suivantes :

GIAC Foundational Cybersecurity Technologies (GFACT);

GIAC Security Essentials Certification (GSEC).

Outre les certifications, les participantes et participants recevront des instructions liées la Catalyst Cyber Range, un mentorat professionnel avec des spécialistes de premier plan en cybersécurité, un soutien professionnel et des contacts avec des employeuses et employeurs.

Le programme (offert en anglais seulement) est financé par le gouvernement du Canada, Rogers Communications et la Banque Royale du Canada.

## 5.0 LISTE ET DESCRIPTION DES CERTIFICATIONS EN CYBERSÉCURITÉ

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

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

### 5.1 CERTNEXUS

**Tableau 1 : Liste et description des certifications de CertNexus<sup>1</sup>**

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified First Responder (CFR)	<ul style="list-style-type: none"> <li>• Atteste les connaissances des candidates et candidats en matière d'analyse des menaces, de conception d'environnements réseau et informatiques sécurisés, de détection proactive des défaillances réseau, d'intervention en cas d'incidents de cybersécurité et d'enquête sur ces incidents</li> <li>• Les candidates et candidats doivent avoir de trois à cinq années d'expérience de travail dans un environnement informatique, à protéger les systèmes d'information essentiels avant, pendant et après un incident</li> <li>• L'examen comporte 100 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Deux options possibles pour le renouvellement de la certification : <ul style="list-style-type: none"> <li>○ Passer la plus récente version de l'examen</li> <li>○ Obtenir 90 crédits de formation continue pendant la période de trois ans et payer les frais annuels</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de système</li> <li>• Administratrices et administrateurs de réseau</li> <li>• Intervenantes et intervenants en cas d'incident informatique</li> <li>• Enquêteuses et enquêteurs en cybercriminalité</li> <li>• Vérificatrices et vérificateurs des TI</li> <li>• Analystes de la sécurité</li> <li>• Analystes de réseau</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
		<ul style="list-style-type: none"> <li>Ingénieures et ingénieurs en sécurité des systèmes d'information</li> </ul>
Certified IoT Security Practitioner (CIoTSP)	<ul style="list-style-type: none"> <li>Atteste que les candidates et candidats possèdent les connaissances, les compétences et les capacités nécessaires pour sécuriser des environnements réseau pour les dispositifs de l'Internet des objets (IdO), analyser les vulnérabilités et déterminer les mesures de contrôle raisonnables à prendre pour contrer les menaces, surveiller efficacement les dispositifs de l'IdO et intervenir en cas d'incident</li> <li>Les candidates et candidats doivent avoir une compréhension fondamentale des écosystèmes de l'IdO</li> <li>L'examen comporte 100 questions à choix multiples</li> </ul>	<ul style="list-style-type: none"> <li>Administratrices et administrateurs de réseau</li> <li>Ingénieures et ingénieurs en développement logiciel</li> <li>Architectes de solutions</li> <li>Analystes de la cybersécurité</li> <li>Développeuses et développeurs Web</li> <li>Ingénieures et ingénieurs en nuage</li> </ul>
Cyber Secure Coder (CSC)	<ul style="list-style-type: none"> <li>Démontre que les titulaires de cette certification ont été initiées et 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</li> <li>Les candidates et candidats doivent avoir une certaine expérience en programmation (développement d'applications de bureau, mobiles, Web ou infonuagiques)</li> <li>L'examen comporte 80 questions à choix multiples</li> <li>Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>Programmeuses et programmeurs en chef</li> <li>Programmeuses débutantes et programmeurs débutants</li> <li>Testeuses et testeurs d'application</li> <li>Testeuses et testeurs de l'assurance de la qualité</li> <li>Conceptrices et concepteurs de logiciels</li> <li>Architectes de logiciels</li> </ul>
CyberSafe	<ul style="list-style-type: none"> <li>Atteste que les candidates et candidats peuvent identifier les risques les plus courants associés à l'utilisation de technologies mobiles ou infonuagiques, et qu'ils peuvent assurer leur protection et celle de leur organisation contre des cybermenaces</li> </ul>	<ul style="list-style-type: none"> <li>Utilisatrices et utilisateurs finaux sans connaissances techniques de l'informatique</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Aucun préalable n'est exigé pour l'examen, mais les candidates et candidats doivent avoir une certaine expérience de la technologie de base (ordinateurs, téléphones intelligents, courriel, Internet, etc.)</li> <li>• L'examen ne comporte que dix questions et n'impose aucune limite de temps</li> </ul>	
Microcompétence IRBIZ	<ul style="list-style-type: none"> <li>• Atteste que les candidates et 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</li> <li>• Les candidates et candidats doivent avoir une compréhension générale de la cybersécurité</li> <li>• L'examen comporte dix questions à choix multiples et de type vrai ou faux</li> <li>• Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Leaders et cadres en TI responsables d'assurer le respect de la législation en matière d'intervention en cas d'incident</li> </ul>



## 5.2 CISCO SYSTEMS

**Tableau 2 : Liste et description des certifications de Cisco Systems<sup>2</sup>**

Certification	Aperçu de la certification	Candidates et candidats ciblés
Cisco Certified CyberOps Associate	<ul style="list-style-type: none"> <li>• Prépare les candidates et candidats à travailler avec des analystes associées et associés de la cybersécurité au sein de centres des opérations de sécurité (COS)</li> <li>• Aucun préalable n'est exigé</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige d'avancer au prochain niveau de certification, d'accumuler des crédits de formation continue ou une combinaison de ces deux exigences</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes de la cybersécurité</li> <li>• Membres de l'équipe du COS</li> </ul>
Cisco Certified CyberOps Professional	<ul style="list-style-type: none"> <li>• Nouvelle certification créée en 2021</li> <li>• Atteste les connaissances des candidates et candidats en matière de sécurité infonuagique, de gestion des risques et d'analyse du renseignement sur les menaces</li> <li>• Aucun préalable n'est exigé</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige d'avancer au prochain niveau de certification, d'accumuler des crédits de formation continue ou une combinaison de ces deux exigences</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes de la sécurité de l'information</li> <li>• Intervenantes et intervenants en cas d'incident informatique</li> <li>• Gestionnaires des incidents</li> <li>• Ingénieures et ingénieurs de réseau</li> </ul>
Cisco Certified Internetwork Expert (CCIE) Security	<ul style="list-style-type: none"> <li>• Atteste les connaissances des candidates et candidats en matière d'infrastructure de sécurité, notamment la sécurité des réseaux, la sécurité infonuagique, la sécurité du contenu, la protection et la détection des points terminaux, l'accès sécurisé aux réseaux, la visibilité et les mesures de renforcement de la sécurité</li> <li>• Aucun préalable n'est exigé</li> <li>• On recommande aux candidates et candidats d'avoir de cinq à sept ans d'expérience dans la conception, le déploiement, l'exploitation et l'optimisation de technologies et solutions de sécurité</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels chevronnés de la réseautique avec de cinq à sept ans d'expérience</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• La certification exige la réussite d'un examen de qualification et d'un examen pratique en laboratoire de huit heures</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige d'avancer au prochain niveau de certification, d'accumuler des crédits de formation continue ou une combinaison de ces deux exigences</li> </ul>	
Cisco Certified Network Professional (CCNP) Security	<ul style="list-style-type: none"> <li>• Atteste des connaissances des candidates et candidats en matière d'infrastructure d'entreprise, de virtualisation, d'assurance, de sécurité et d'automatisation</li> <li>• Aucun préalable n'est exigé</li> <li>• On recommande aux candidates et candidats d'avoir de trois à cinq ans d'expérience dans la mise en œuvre de solutions de sécurité</li> <li>• La certification nécessite la réussite d'un examen de base et d'un examen de concentration</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige d'avancer au prochain niveau de certification, d'accumuler des crédits de formation continue ou une combinaison de ces deux exigences</li> </ul>	<ul style="list-style-type: none"> <li>• Les professionnelles et professionnels avec de trois à cinq ans d'expérience dans la mise en œuvre de solutions de sécurité</li> <li>• Ingénieures et ingénieurs de réseau</li> <li>• Ingénieures et ingénieurs de système</li> <li>• Techniciennes et techniciens de réseau</li> </ul>
Cisco Certified Support Technician (CCST) Cybersecurity	<ul style="list-style-type: none"> <li>• Nouvelle certification créée en 2023</li> <li>• Certification de premier échelon</li> <li>• Aucun préalable n'est exigé</li> <li>• Atteste les compétences et les connaissances des candidates et candidats pour ce qui est des concepts et des domaines de base en matière de cybersécurité, ce qui comprend les principes de la sécurité, les concepts de la sécurité des réseaux et des points terminaux, l'évaluation des vulnérabilités, la gestion des risques et le traitement des incidents</li> <li>• La certification ne vient jamais à expiration et il n'est pas nécessaire d'obtenir une nouvelle certification</li> </ul>	<ul style="list-style-type: none"> <li>• Étudiantes et étudiants en fin d'études secondaires ou postsecondaires</li> <li>• Étudiantes et étudiants dans des écoles techniques</li> <li>• Professionnelles et professionnels débutants en réseautique et en TI</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Cisco Certified Support Technician (CCST) Networking	<ul style="list-style-type: none"> <li>Nouvelle certification créée en 2023</li> <li>Certification de premier échelon</li> <li>Aucun préalable n'est exigé</li> <li>Atteste les compétences et les connaissances des candidates et candidats pour ce qui est des concepts et des domaines de base en matière de réseautique, ce qui comprend le fonctionnement des réseaux, ainsi que les dispositifs, les supports et les protocoles qui permettent aux réseaux de communiquer</li> <li>La certification ne vient jamais à expiration et il n'est pas nécessaire d'obtenir une nouvelle certification</li> </ul>	<ul style="list-style-type: none"> <li>Étudiantes et étudiants en fin d'études secondaires ou postsecondaires</li> <li>Étudiantes et étudiants dans des écoles techniques</li> <li>Professionnelles et professionnels débutants en réseautique et en TI</li> </ul>

### 5.3 COMPTIA

**Tableau 3 : Liste et description des certifications de CompTIA<sup>3</sup>**

Certification	Aperçu de la certification	Candidates et candidats ciblés
Advanced Security Practitioner (CASP+)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> <li>La seule certification axée sur le rendement qui s'adresse davantage aux praticiennes et praticiens qu'aux gestionnaires, travaillant à un niveau avancé de cybersécurité</li> <li>Atteste les compétences de niveau avancé des candidates et 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</li> <li>Les candidates et candidats doivent avoir dix années d'expérience en administration des TI; dont cinq années d'expérience pratique en sécurité technique</li> <li>L'examen comporte 90 questions à choix multiples et des questions axées sur le rendement</li> <li>Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>Architectes de la sécurité</li> <li>Analystes techniques en chef</li> <li>Ingénieures et ingénieurs de la sécurité</li> <li>Ingénieures et ingénieurs de la sécurité des applications</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>Le renouvellement de la certification exige l'obtention de 75 crédits de formation continue pendant la période de trois ans</li> </ul>	
Cyber Security Analyst (CySA+)	<ul style="list-style-type: none"> <li>Certification d'analyste de la cybersécurité de niveau intermédiaire</li> <li>La certification d'analyste de la sécurité la plus à jour qui couvre les menaces persistantes avancées dans un environnement de cybersécurité après 2014</li> <li>Atteste l'expertise des candidates et candidats en analyse de la sécurité, en détection des intrusions et en intervention</li> <li>Les candidates et 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</li> <li>Approuvée par le département de la Défense des États-Unis</li> <li>L'examen comporte 85 questions à choix multiples et des questions axées sur le rendement</li> <li>Valide pendant trois ans</li> <li>Le renouvellement de la certification exige l'obtention de 60 crédits de formation continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>Analystes de la sécurité des TI</li> <li>Analystes du COS</li> <li>Analystes de la cybersécurité</li> <li>Analystes du renseignement sur les menaces</li> <li>Ingénieures et ingénieurs de la sécurité</li> <li>Analystes de la cybersécurité</li> </ul>
Network+	<ul style="list-style-type: none"> <li>Atteste les connaissances et les compétences des candidates et candidats en conception et en mise en œuvre de réseaux fonctionnels</li> <li>Les préalables sont la certification A+ et neuf à douze mois d'expérience en réseautique</li> <li>Elle s'avère utile pour les personnes désirant suivre une carrière en infrastructure des TI (dépannage, configuration, gestion des réseaux)</li> <li>L'examen comporte 90 questions à choix multiples et des questions axées sur le rendement</li> <li>Valide pendant trois ans</li> <li>Le renouvellement de la certification exige l'obtention de 30 crédits de formation continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>Postes de premier échelon</li> <li>Administratrices et administrateurs de réseau débutants</li> <li>Techniciennes et techniciens en informatique</li> <li>Ingénieures et ingénieurs de système débutants</li> </ul>
PenTest+	<ul style="list-style-type: none"> <li>Certification de niveau intermédiaire</li> <li>Atteste que les candidates et 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</li> </ul>	<ul style="list-style-type: none"> <li>Testeuses et testeurs de pénétration</li> <li>Testeuses et testeurs de vulnérabilité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Les candidates et candidats doivent avoir trois ou quatre années d'expérience en sécurité de l'information ou une expérience connexe</li> <li>• L'examen comporte 85 questions à choix multiples et des questions axées sur le rendement</li> <li>• Le renouvellement de la certification exige l'obtention de 60 crédits de formation continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes de la sécurité</li> <li>• Opératrices et opérateurs de la sécurité réseau</li> </ul>
Security+	<ul style="list-style-type: none"> <li>• Certification de premier échelon</li> <li>• Atteste les compétences de base en cybersécurité nécessaires pour exécuter les fonctions essentielles en sécurité</li> <li>• Les titulaires de la certification sont des expertes et experts en gestion des menaces, en contrôle d'accès réseau et en infrastructure de sécurité</li> <li>• Les candidates et candidats doivent posséder deux années d'expérience en sécurité réseau et avoir obtenu la certification Network+</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige l'obtention de 50 crédits de formation continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de système</li> <li>• Administratrices et administrateurs de réseau</li> <li>• Administratrices et administrateurs de la sécurité</li> <li>• Vérificatrices et vérificateurs des TI débutants</li> <li>• Testeuses et testeurs de pénétration</li> <li>• Ingénieures et ingénieurs de la sécurité</li> </ul>

## 5.4 COUNCIL FOR REGISTERED ETHICAL SECURITY TESTERS (CREST)

Tableau 4 : Liste et description des certifications de CREST<sup>4</sup>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Infrastructure Tester	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats ont les capacités requises pour accéder à un réseau afin de trouver des failles et des vulnérabilités dans la couche du réseau et du système d'exploitation</li> <li>• L'examen comporte une partie écrite à choix multiples et deux volets pratiques de six heures</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de système</li> <li>• Testeuses et testeurs de pénétration</li> <li>• Gestionnaires de la sécurité de l'information</li> <li>• Gestionnaires des incidents</li> </ul>
Certified Web Application Tester	<ul style="list-style-type: none"> <li>• Évalue la capacité des candidates et candidats de trouver des vulnérabilités dans des applications Web sur mesure</li> <li>• L'examen comporte une partie écrite à choix multiples et deux volets pratiques de six heures</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Testeuses et testeurs de pénétration</li> <li>• Spécialistes du piratage contrôlé</li> </ul>
CREST Certified Wireless Specialist (CCWS)	<ul style="list-style-type: none"> <li>• Atteste les connaissances et les compétences des candidates et candidats liées à la réalisation d'examens de la sécurité sans fil, et aux technologies d'identification par radiofréquences (RFID), Bluetooth et autres technologies sans fil traditionnelles</li> <li>• Le préalable exigé est d'avoir réussi l'un des examens de certification CREST de base</li> <li>• Examen en deux volets : 120 questions à choix multiples et tâches pratiques</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels de haut niveau</li> </ul>
Practitioner Security Analyst (CPSA)	<ul style="list-style-type: none"> <li>• Certification de premier échelon</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de système</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Atteste les connaissances des candidates et candidats liées à l'évaluation des systèmes d'exploitation et des services réseau courants à un niveau de base</li> <li>• Les candidates et candidats doivent démontrer qu'ils possèdent les connaissances nécessaires pour faire des analyses de base des vulnérabilités dans les infrastructures et les applications Web, et pour interpréter les résultats afin de localiser les failles de sécurité</li> <li>• L'examen comporte des questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Testeuses et testeurs de pénétration</li> <li>• Gestionnaires de la sécurité de l'information</li> <li>• Gestionnaires des incidents</li> </ul>
Registered Penetration Tester (CRT)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats d'effectuer des tâches de base relatives à l'évaluation des vulnérabilités et aux tests de pénétration</li> <li>• Lors de l'examen, les candidates et candidats doivent trouver des vulnérabilités connues dans des technologies de réseaux, d'applications et de bases de données courantes; l'examen comporte une section à choix multiples</li> <li>• La certification CPSA est un préalable</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de système</li> <li>• Testeuses et testeurs de pénétration</li> <li>• Gestionnaires de la sécurité de l'information</li> <li>• Gestionnaires des incidents</li> </ul>

## 5.5 CERTIFIED WIRELESS NETWORK PROFESSIONS (CWNP)

Tableau 5 : Liste et description des certifications de CWNP<sup>5</sup>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Wireless Network Expert (CWNE)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• On compte moins de 200 titulaires de la certification CWNE dans le monde</li> <li>• Atteste que les candidates et 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</li> <li>• Les candidates et candidats doivent avoir trois années d'expérience dans les réseaux Wi-Fi</li> <li>• 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)</li> <li>• Les candidates et candidats doivent passer quatre examens et effectuer des déploiements de WLAN commerciaux</li> <li>• Valide pendant trois ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes occupant des postes supérieurs liés au WLAN</li> </ul>
Certified Wireless Security Professional (CWSP)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats d'évaluer les vulnérabilités d'un réseau et d'aider à prévenir les attaques, d'effectuer des vérifications de sécurité de WLAN et de mettre en œuvre des solutions de surveillance de la conformité</li> <li>• Les candidates et candidats doivent déjà avoir obtenu la certification Certified Wireless Network Administrator (CWNA)</li> <li>• L'examen comporte 60 questions à choix multiples</li> <li>• Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels des réseaux TI</li> </ul>

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



Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>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</li> </ul>	

## 5.6 EC-COUNCIL

**Tableau 6 : Liste et description des certifications de l'EC-Council<sup>6</sup>**

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Application Security Engineer (CASE)	<ul style="list-style-type: none"> <li>Deux volets : JAVA et .NET</li> <li>Atteste que les candidates et candidats possèdent les compétences et les connaissances essentielles en sécurité qui sont nécessaires tout au long d'un cycle de développement de logiciels (CDL) type, en mettant l'accent sur l'importance de la mise en œuvre de pratiques et de méthodologies sécurisées dans l'environnement actuel d'exploitation non sécurisé</li> <li>Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>Valide pendant trois ans</li> <li>Les examens comportent 50 questions à choix multiples</li> <li>Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>Personnes responsables du développement, de la mise à l'essai, de la gestion ou de la protection d'une vaste gamme d'applications</li> <li>Conceptrices et concepteurs qui aspirent à devenir des ingénieures, des ingénieurs, des analystes, des testeuses ou des testeurs de la sécurité des applications</li> </ul>
Certified Chief Information Security Officer (CCISO)	<ul style="list-style-type: none"> <li>Le programme CCISO reconnaît l'expérience concrète nécessaire pour réussir aux plus hauts échelons de la sécurité de l'information</li> </ul>	<ul style="list-style-type: none"> <li>Dirigeantes principales et dirigeants principaux de la sécurité de l'information</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Il vise à former des cadres supérieures et supérieurs de haut niveau en sécurité de l'information</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins cinq années d'expérience de travail dans chacun des cinq domaines du programme CCISO et doivent présenter une demande d'admission à l'examen</li> <li>• Les candidates et candidats qui suivent la formation officielle doivent avoir cinq années d'expérience de travail dans au moins trois des domaines du programme CCISO</li> <li>• L'examen comporte 150 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	
Certified Cloud Security Engineer (CCSE)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats de créer et de mettre en œuvre des stratégies de sécurité pour protéger les applications et les infrastructures infonuagiques</li> <li>• Le programme offre des concepts de sécurité infonuagique propres à des fournisseurs précis et d'autres qui ne sont aucunement liés à des fournisseurs précis</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>• L'examen comporte 125 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes infonuagiques</li> <li>• Analystes de la cybersécurité</li> <li>• Administratrices et administrateurs de la sécurité réseau</li> <li>• Administratrices, administrateurs, ingénieures et ingénieurs infonuagiques</li> <li>• Professionnelles et professionnels des opérations de gestion infonuagique et réseau</li> </ul>
Certified Cybersecurity Technician (CCT)	<ul style="list-style-type: none"> <li>• Compétence de premier échelon en cybersécurité pour les personnes qui désirent entamer une carrière en cybersécurité ou en TI</li> <li>• Atteste les compétences techniques pratiques des candidates et candidats</li> <li>• Aucun préalable n'est exigé</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes qui désirent assumer des fonctions de premier échelon associées</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• L'examen comporte 60 questions à choix multiples et dix scénarios pratiques</li> <li>• Valide pendant trois ans</li> <li>• La certification CCT ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour <i>EC-Council Continuing Education</i>). Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<p>à la cybersécurité ou à la sécurité de l'information</p> <ul style="list-style-type: none"> <li>• Techniciennes et techniciens en cybersécurité</li> <li>• Administratrices, administrateurs, ingénieures et ingénieurs de réseau</li> <li>• Spécialistes et gestionnaires du soutien TI</li> <li>• Techniciennes, techniciens, coordonnatrices et coordonnateurs de réseau</li> </ul>
Certified Ethical Hacker (CEH) – ANSI	<ul style="list-style-type: none"> <li>• Compétence de premier échelon</li> <li>• Atteste que les candidates et candidats savent comment trouver les faiblesses et les vulnérabilités dans les systèmes ainsi qu'utiliser les mêmes outils et connaissances que ceux d'une ou un pirate malveillant, mais de façon légitime et légale pour évaluer la posture de sécurité des systèmes</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>• Ce titre de compétence atteste les compétences des candidates et candidats, d'un point de vue neutre, en matière de sécurité réseau dans le domaine du piratage contrôlé</li> <li>• L'examen comporte 125 questions</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Agentes et agents de la sécurité de l'information</li> <li>• Agentes, agents, gestionnaires, ingénieures, ingénieurs ou spécialistes en sécurité de l'assurance de l'information</li> <li>• Administratrices et administrateurs de site</li> <li>• Vérificatrices et vérificateurs de la sécurité de l'information</li> <li>• Analystes des risques, des menaces et des vulnérabilités</li> </ul>
Certified Ethical Hacker (CEH) – Master	<ul style="list-style-type: none"> <li>• Les candidates et candidats détiennent les certifications ANSI et Practical CEH</li> <li>• Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Responsables de la sécurité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Vérificatrices et vérificateurs des TI</li> <li>• Administratrices et administrateurs de site</li> </ul>
Certified Ethical Hacker (CEH) – Practical	<ul style="list-style-type: none"> <li>• Atteste les connaissances des candidates et candidats liées aux techniques de piratage contrôlé telles que l'identification du vecteur de menace, le balayage réseau, la détection du système d'exploitation, l'analyse des vulnérabilités, le piratage de systèmes, le piratage d'applications Web, etc.</li> <li>• Aucun préalable n'est exigé, mais cette certification est généralement la prochaine étape après avoir obtenu la certification CEH ANSI</li> <li>• Examen de six heures comportant 20 études de cas</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes, administratrices ou administrateurs de la sécurité de l'information</li> <li>• Agentes, agents, gestionnaires, ingénieures, ingénieurs ou spécialistes en sécurité de l'assurance de l'information</li> <li>• Analystes des risques, des menaces et des vulnérabilités</li> <li>• Administratrices et administrateurs de système</li> <li>• Administratrices, administrateurs, ingénieures ou ingénieurs de réseau</li> </ul>
Certified Network Defender (CND) – ANSI	<ul style="list-style-type: none"> <li>• Démontre que les candidates et candidats possèdent l'expertise requise pour protéger le réseau contre les menaces, détecter les menaces sur le réseau et intervenir face à celles-ci</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité des TI et doivent présenter une demande d'admission à l'examen</li> <li>• L'examen comporte 100 questions à choix multiples</li> <li>• Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de TI et de réseau</li> <li>• Analystes de la sécurité des données</li> <li>• Ingénieures, ingénieurs, techniciennes et techniciens de réseau</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	
Certified Penetration Testing Professional (CPENT)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats d'exécuter des tests de pénétration efficaces dans un environnement réseau d'entreprise, ce qui comprend la conduite d'activités d'attaque, d'exploitation, d'évitement et de défense</li> <li>• Aucun préalable n'est exigé</li> <li>• L'examen de 24 heures consiste en une évaluation pratique et la rédaction d'un rapport sur les tests de pénétration</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Testeuses et testeurs de pénétration</li> <li>• Spécialistes du piratage contrôlé</li> <li>• Administratrices et administrateurs de pare-feu et de serveur réseau</li> <li>• Professionnelles et professionnels de l'évaluation des risques</li> <li>• Ingénieures, ingénieurs et analystes de la sécurité</li> <li>• Consultantes et consultants en sécurité de l'information</li> </ul>
Certified Secure Computer User (CSCU)	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats peuvent cerner des menaces à la sécurité de l'information et les atténuer efficacement</li> <li>• Aucun préalable n'est exigé</li> <li>• L'examen comporte 50 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• La certification CSCU ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour <i>EC-Council Continuing Education</i>). Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Toute personne âgée de treize ans et plus qui utilise un ordinateur pour travailler, étudier ou jouer</li> <li>• Utilisatrices ou utilisateurs finaux</li> </ul>
Certified SOC Analyst (CSA)	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats ont une pleine compréhension des tâches que doit accomplir un analyste du centre des opérations de sécurité (COS)</li> <li>• Le programme met l'accent sur la création de nouvelles possibilités de carrière pour les candidates et candidats en leur donnant les compétences techniques, les</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes du COS de niveau 1 et de niveau 2</li> <li>• Analystes de la cybersécurité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<p>connaissances et les capacités accrues qui sont en demande pour contribuer dynamiquement à une équipe du COS</p> <ul style="list-style-type: none"> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir une année d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>• L'examen comporte 100 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Futures et futurs analystes du COS</li> <li>• Administratrices, administrateurs, ingénieures ou ingénieurs de la sécurité et de réseau</li> <li>• Analystes, techniciennes et techniciens en défense des réseaux</li> </ul>
Certified Threat Intelligence Analyst (CTIA)	<ul style="list-style-type: none"> <li>• Démontre que les candidates et candidats ont les compétences pour cerner, atténuer et contrer les risques opérationnels en transformant les menaces internes et externes en entités malveillantes quantifiables</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>• L'examen comporte 50 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Spécialistes du piratage contrôlé</li> <li>• Analystes de la criminalistique numérique et de logiciels malveillants</li> <li>• Analystes du renseignement sur les menaces</li> <li>• Membres de l'équipe d'intervention en cas d'incident</li> <li>• Professionnelles et professionnels du COS</li> <li>• Gestionnaires, architectes, analystes, ingénieures, ingénieurs, praticiennes et praticiens de la sécurité</li> </ul>
Computer Hacking Forensics Investigator (CHFI) – ANSI	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent les compétences nécessaires pour enquêter de façon proactive sur les menaces de sécurité complexes, ce qui comprend l'enquête, l'enregistrement et le signalement des cybercrimes pour prévenir les attaques</li> <li>• Programme en laboratoire non rattaché à un fournisseur donné</li> </ul>	<ul style="list-style-type: none"> <li>• Gestionnaires des TI</li> <li>• Fournisseurs de services de criminalistique numérique</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>• L'examen comporte 150 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Responsables de l'application de la loi</li> <li>• Responsables de la défense et de la sécurité</li> <li>• Organismes gouvernementaux</li> </ul>
Digital Forensics Essentials (DFE)	<ul style="list-style-type: none"> <li>• Compétence de premier échelon qui aide les candidates et candidats à renforcer leurs compétences et leur expertise en criminalistique numérique et en sécurité de l'information, de façon à ajouter de la valeur à leur milieu de travail et à leur employeur</li> <li>• Aucun préalable n'est exigé</li> <li>• L'examen comporte 75 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• La certification DFE ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour <i>EC-Council Continuing Education</i>). Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes qui désirent assumer des fonctions de premier échelon associées à la cybersécurité ou à la sécurité de l'information</li> <li>• Techniciennes et techniciens du centre d'assistance</li> <li>• Administratrices et administrateurs de réseau</li> <li>• Techniciennes et techniciens de réseau</li> <li>• Spécialistes du soutien informatique</li> </ul>
EC-Council Disaster Recovery Professional (EDRP)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats de planifier, de mettre en œuvre et de tenir à jour un plan de continuité des activités et de reprise après sinistre</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins deux années d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>• L'examen comporte 150 questions à choix multiples</li> <li>• Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Directrices et directeurs des TI et dirigeantes principales et directeurs principaux de la sécurité de l'information</li> <li>• Gestionnaires, consultantes et consultants en matière de risques liés aux TI</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Consultantes et consultants en continuité des activités et en reprise après sinistre</li> <li>• Professionnelles et professionnels des TI dans les domaines de la reprise après sinistre, de la continuité des activités et de l'administration de système</li> </ul>
EC-Council Certified Encryption Specialist (ECES)	<ul style="list-style-type: none"> <li>• Certification de premier échelon qui initie les professionnelles, les professionnels, les étudiantes et les étudiants à la cryptographie en inculquant les rudiments de la cryptographie à clé symétrique moderne</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins une année d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>• L'examen comporte 50 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Cryptanalystes</li> <li>• Cryptographes</li> <li>• Spécialistes du piratage contrôlé</li> <li>• Testeuses et testeurs de pénétration</li> </ul>
EC-Council Certified Incident Handler (ECIH) - ANSI	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent les connaissances et les compétences nécessaires pour gérer efficacement les conséquences à la suite d'une brèche de sécurité en réduisant les répercussions de l'incident sur les plans financier et de la réputation</li> <li>• Programme spécialisé</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir au moins une année d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de l'évaluation des risques</li> <li>• Administratrices, administrateurs, ingénieures et ingénieurs de système</li> <li>• Gestionnaires des TI et des réseaux</li> </ul>



Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• L'examen comporte 100 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Ingénieures et ingénieurs de la sécurité des applications</li> <li>• Analystes, enquêteuses et enquêteurs en criminalistique numérique</li> <li>• Analystes du COS</li> <li>• Testeuses et testeurs de pénétration</li> </ul>
Ethical Hacking Essentials (EHE)	<ul style="list-style-type: none"> <li>• Compétence de premier échelon qui inculque les rudiments du piratage contrôlé et des tests de pénétration, et qui prépare les candidates et candidats à une carrière en cybersécurité</li> <li>• Aucun préalable n'est exigé</li> <li>• L'examen comporte 75 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• La certification ECE ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour <i>EC-Council Continuing Education</i>). Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes qui désirent assumer des fonctions de premier échelon associées à la cybersécurité ou à la sécurité de l'information</li> <li>• Techniciennes et techniciens du centre d'assistance</li> <li>• Administratrices et administrateurs de réseau</li> <li>• Techniciennes et techniciens de réseau</li> <li>• Spécialistes du soutien informatique</li> </ul>
Industrial Control Systems and Supervisory Control and Data Acquisitions (ICS/SCADA) Cybersecurity	<ul style="list-style-type: none"> <li>• Atteste les connaissances rudimentaires des candidates et candidats en matière de sécurité et leur capacité à défendre une architecture réseau</li> <li>• Les candidates et candidats qui désirent obtenir la certification sans suivre la formation officielle doivent avoir une année d'expérience de travail en sécurité de l'information et doivent présenter une demande d'admission à l'examen</li> <li>• L'examen comporte 75 questions à choix multiples</li> <li>• Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices, administrateurs, ingénieures et ingénieurs de système</li> <li>• Responsables des systèmes SCADA</li> <li>• Analystes des systèmes opérationnels assurant le</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Pour renouveler leur certification, les candidates et candidats doivent accumuler 120 crédits de formation continue pendant la période de trois ans et payer des frais annuels</li> </ul>	<p>soutien des interfaces SCADA</p> <ul style="list-style-type: none"> <li>• Consultantes et consultants en sécurité réalisant les évaluations de la sécurité des systèmes SCADA ou des systèmes de contrôle industriels (SCI)</li> </ul>
Network Defense Essentials (NDE)	<ul style="list-style-type: none"> <li>• Compétence de premier échelon qui inculque les concepts fondamentaux de la sécurité de l'information et de la défense réseau, et qui est destiné principalement aux candidates et candidats qui désirent faire carrière en cybersécurité</li> <li>• Aucun préalable n'est exigé</li> <li>• L'examen comporte 75 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• La certification NDE ne fait pas partie du schéma de formation continue d'EC-Council (ECE pour <i>EC-Council Continuing Education</i>). Pour renouveler leur certification, les candidates et candidats doivent repasser l'examen</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes qui désirent assumer des fonctions de premier échelon associées à la cybersécurité ou à la sécurité de l'information</li> <li>• Techniciennes et techniciens du centre d'assistance</li> <li>• Administratrices et administrateurs de réseau</li> <li>• Techniciennes et techniciens de réseau</li> <li>• Spécialistes du soutien informatique</li> </ul>

## 5.7 GLOBAL INFORMATION ASSURANCE CERTIFICATION (GIAC)

Tableau 7 : Liste et description des certifications de GIAC<sup>7</sup>

Certification	Aperçu de la certification	Candidates et candidats ciblés
GIAC Advanced Smartphone Forensics (GASF)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste que les candidates et candidats possèdent les qualifications nécessaires pour effectuer des examens d'informatique judiciaire sur des appareils, comme des téléphones mobiles et des tablettes, et qu'ils ont une connaissance des principes de base en ce qui a trait aux interventions judiciaires sur les appareils mobiles, à l'analyse de système de fichiers d'appareils, au comportement des applications mobiles, à l'analyse des artefacts d'événement, ainsi qu'à l'identification et à l'analyse de maliciels qui s'attaquent aux appareils mobiles</li> <li>• Valide pendant quatre ans</li> <li>• L'examen comporte 75 questions</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes de la criminalistique numérique et de logiciels malveillants</li> <li>• Analystes, enquêteuses et enquêteurs judiciaires de la cyberdéfense</li> <li>• Testeuses et testeurs de pénétration</li> <li>• Conceptrices et concepteurs d'exploit</li> <li>• Analystes en menaces informatiques</li> </ul>
GIAC Assessing and Auditing Wireless Networks (GAWN)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste que les candidates et candidats possèdent des connaissances des divers mécanismes de sécurité pour les réseaux sans fil, des outils et des techniques utilisés pour l'évaluation et l'exploitation des faiblesses, et des techniques servant à l'analyse des réseaux sans fil</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Vérificatrices et vérificateurs</li> <li>• Spécialistes du piratage contrôlé</li> <li>• Testeuses et testeurs de pénétration</li> <li>• Professionnelles et professionnels de la sécurité réseau</li> <li>• Ingénieures et ingénieurs de système sans fil</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
GIAC Certified Detection Analyst (GCDA)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste la capacité des candidates et candidats de recueillir, d'analyser et d'utiliser de façon tactique des sources de données modernes sur les réseaux et les terminaux pour détecter les activités malveillantes ou non autorisées</li> <li>• Les titulaires d'une certification GCDA ont les compétences pour occuper des postes de leadership en gestion de l'information et des événements de sécurité (GIES)</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes de la sécurité</li> <li>• Architectes de la sécurité</li> <li>• Ingénieures principales et ingénieurs principaux de la sécurité</li> <li>• Ingénieures, ingénieurs et analystes du COS</li> <li>• Enquêteuses spécialisées et enquêteurs spécialisés dans les cybermenaces</li> </ul>
GIAC Certified Enterprise Defender (GCED)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste les connaissances et les compétences des candidates et candidats dans les domaines de l'infrastructure réseau de défense, de l'analyse de paquets, des tests de pénétration, du traitement des incidents et de la suppression de maliciels</li> <li>• L'examen comporte 115 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Intervenantes et intervenants en cas d'incident informatique</li> <li>• Testeuses et testeurs de pénétration</li> <li>• Ingénieures, ingénieurs et analystes du COS</li> <li>• Professionnelles et professionnels de la sécurité réseau</li> </ul>
GIAC Certified Forensic Analyst (GCFA)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste que les candidates et 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</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Membres de l'équipe d'intervention en cas d'incident</li> <li>• Analystes du COS</li> <li>• Agentes fédérales, agents fédéraux, professionnelles et professionnels chargés de l'application de la loi</li> <li>• Analystes de la criminalistique numérique</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
GIAC Certified Forensic Examiner (GCFE)	<ul style="list-style-type: none"> <li>• Certification de niveau intermédiaire</li> <li>• Atteste les connaissances des candidates et 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</li> <li>• L'examen comporte 115 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels de la sécurité de l'information</li> <li>• Membres d'organismes d'application de la loi</li> <li>• Analystes de la criminalistique numérique et de logiciels malveillants</li> <li>• Analystes, enquêteuses et enquêteurs judiciaires de la cyberdéfense</li> </ul>
GIAC Certified Incident Handler (GCIH)	<ul style="list-style-type: none"> <li>• Certification de niveau intermédiaire</li> <li>• Atteste la capacité des candidates et 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</li> <li>• L'examen comporte de 100 à 150 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Membres de l'équipe d'intervention en cas d'incident</li> <li>• Intervenantes et intervenants en cas d'incident lié à la cyberdéfense</li> </ul>
GIAC Certified Intrusion Analyst (GCIA)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste les connaissances des candidates et candidats en matière de surveillance de réseau et d'hôte, d'analyse de trafic et de détection d'intrusion</li> <li>• Les titulaires de la certification sont aptes à configurer et à surveiller des systèmes de détection d'intrusion, et à analyser le trafic réseau</li> <li>• L'examen comporte de 100 à 150 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes responsables de la surveillance de réseau et d'hôte, de l'analyse de trafic et de la détection d'intrusion</li> <li>• Analystes en menaces informatiques</li> <li>• Analystes du centre des opérations de sécurité</li> <li>• Membres de l'équipe d'intervention en cas d'incident</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
GIAC Certified Web Application Defender (GWEB)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Démontre que les candidates et candidats maîtrisent les connaissances et les compétences en matière de sécurité dont ils ont besoin pour traiter les erreurs courantes d'applications Web qui occasionnent la majorité des problèmes de sécurité</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Développeuses et développeurs d'applications</li> <li>• Analystes de la sécurité des applications</li> <li>• Architectes d'applications</li> <li>• Testeuses et testeurs de pénétration</li> <li>• Personnes dont les responsabilités exigent la conformité aux normes de l'industrie des cartes de paiement (PCI pour <i>Payment Card Industry</i>)</li> </ul>
GIAC Certified Windows Security Administrator (GCWN)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste la capacité des candidates et candidats de sécuriser les clients et les serveurs Windows, et leurs connaissances en matière de configuration et de gestion de la sécurité des systèmes d'exploitation et des applications Microsoft</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes responsables de l'installation, de la configuration et de la sécurisation des clients et des serveurs Microsoft Windows</li> </ul>
GIAC Continuous Monitoring Certification (GMON)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste la capacité des candidates et candidats de prévenir les intrusions et de détecter rapidement les activités suspectes</li> <li>• L'examen comporte 115 questions</li> <li>• Valide pendant quatre ans</li> </ul>	<ul style="list-style-type: none"> <li>• Architectes de la sécurité</li> <li>• Analystes et gestionnaires du COS</li> <li>• Gestionnaires de la sécurité technique</li> <li>• Ingénieures et ingénieurs de la sécurité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>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</li> </ul>	
GIAC Critical Controls Certification (GCCC)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> <li>La seule certification basée sur les contrôles de sécurité essentiels qui font appel à une approche priorisée de la sécurité fondée sur les risques</li> <li>Atteste que les candidates et candidats possèdent les connaissances et les compétences nécessaires pour mettre en œuvre et exécuter les contrôles de sécurité essentiels recommandés par le Council on Cybersecurity, et pour effectuer des vérifications en fonction de la norme</li> <li>Aucun préalable n'est exigé</li> <li>L'examen comporte 75 questions</li> <li>Valide pendant quatre ans</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>Administratrices et administrateurs des TI</li> <li>Ingénieures et ingénieurs de la sécurité réseau</li> <li>Fournisseurs de services de sécurité</li> <li>Vérificatrices et vérificateurs de la sécurité, dirigeantes principales et dirigeants principaux de l'information et responsables de l'évaluation des risques</li> </ul>
GIAC Critical Infrastructure Protection (GCIP)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> <li>Atteste que les candidates et candidats ont les connaissances et les compétences nécessaires pour comprendre la réglementation de la North American Electric Reliability Corporation (NERC) relative à la protection des infrastructures essentielles (CIP pour <i>Critical Infrastructure Protection</i>) et pour préparer des stratégies de mise en œuvre pratiques afin d'assurer la conformité à la réglementation</li> <li>L'examen comporte 75 questions</li> <li>Valide pendant quatre ans</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>Analystes des opérations de sécurité</li> <li>Chefs et gestionnaires d'équipe</li> <li>Analystes d'intervention en cas d'incident</li> <li>Praticiennes et praticiens de la cybersécurité des systèmes de contrôle industriels (SCI)</li> </ul>
GIAC Cyber Threat Intelligence (GCTI)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> </ul>	<ul style="list-style-type: none"> <li>Membres de l'équipe d'intervention en cas d'incident</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et 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</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Analystes en menaces informatiques</li> <li>• Analystes du renseignement</li> </ul>
GIAC Defending Advanced Threats (GDAT)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste que les candidates et candidats ont des connaissances avancées de la façon dont les adversaires s'attaquent aux réseaux et des contrôles de sécurité efficaces pour les arrêter</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Architectes de la sécurité</li> <li>• Ingénieures et ingénieurs de la sécurité</li> <li>• Gestionnaires de la sécurité technique</li> </ul>
GIAC Defensible Security Architecture (GDSA)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste que les candidates et candidats ont les compétences pratiques et concrètes nécessaires pour s'occuper des approches axées sur les réseaux et les données d'une architecture de sécurité défendable, qu'ils peuvent se charger du renforcement des applications dans la pile TCP/IP (<i>Transmission Control Protocol/Internet Protocol</i>) ainsi que de la création d'un environnement sécurisé au moyen de nuages privés, hybrides ou publics</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Architectes de la sécurité</li> <li>• Ingénieures et ingénieurs de réseau</li> <li>• Analystes de la sécurité</li> <li>• Enquêteuses spécialisées et enquêteurs spécialisés dans les cybermenaces</li> <li>• Ingénieures principales et ingénieurs principaux de la sécurité</li> <li>• Analystes de la sécurité</li> </ul>



Certification	Aperçu de la certification	Candidates et candidats ciblés
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste la capacité des candidates et candidats de trouver et d'atténuer les vulnérabilités informatiques majeures dans des systèmes et des réseaux</li> <li>• L'examen comporte de 55 à 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Testeuses et testeurs de vulnérabilités</li> <li>• Analystes de la sécurité</li> <li>• Analystes de l'évaluation des vulnérabilités</li> </ul>
GIAC Information Security Fundamentals (GISF)	<ul style="list-style-type: none"> <li>• Certification de niveau débutant</li> <li>• Atteste que les candidates et candidats ont des connaissances en ce qui a trait aux bases de la sécurité, aux fonctions informatiques et à la réseautique, à la cryptographie de base et aux technologies de cybersécurité</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Membres de la direction</li> <li>• Agentes et agents de la sécurité de l'information</li> <li>• Administratrices et administrateurs de système</li> <li>• Professionnelles et professionnels qui ont besoin d'une introduction aux principes de base de la cybersécurité</li> </ul>
GIAC Information Security Professional (GISP)	<ul style="list-style-type: none"> <li>• Certification de niveau intermédiaire pour gestionnaires et leaders</li> <li>• Atteste que les candidates et candidats ont des connaissances dans les huit domaines de connaissance en matière de cybersécurité : sécurité des actifs, sécurité des télécommunications et des réseaux, gestion de l'identité et de l'accès, gestion de la sécurité et des risques, évaluation de la sécurité et tests de sécurité, ingénierie de sécurité, opérations de sécurité, et sécurité du développement de logiciels</li> <li>• Les candidates et candidats doivent avoir une certaine expérience des systèmes d'information et de la réseautique</li> <li>• L'examen comporte 250 questions</li> <li>• Valide pendant quatre ans</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de système</li> <li>• Administratrices et administrateurs de la sécurité informatique</li> <li>• Administratrices et administrateurs de réseau</li> <li>• Gestionnaires de la sécurité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>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</li> </ul>	
GIAC Mobile Device Security Analyst (GMOB)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> <li>Atteste que les candidates et candidats sont aptes à sécuriser adéquatement des dispositifs mobiles ayant accès à de l'information vitale</li> <li>Démontre que les candidates et 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</li> <li>L'examen comporte 75 questions</li> <li>Valide pendant quatre ans</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>Analystes de la sécurité de l'information</li> <li>Testeuses et testeurs de pénétration</li> <li>Spécialistes du piratage contrôlé</li> <li>Administratrices et administrateurs de système et de réseau</li> </ul>
GIAC Network Forensic Analyst (GNFA)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> <li>Atteste la capacité des candidates et candidats de procéder à des examens à l'aide d'une analyse d'artefacts judiciaires de réseau</li> <li>L'examen comporte 50 questions</li> <li>Valide pendant quatre ans</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>Membres d'organismes d'application de la loi</li> <li>Analystes de la criminalistique numérique et de logiciels malveillants</li> <li>Analystes de la cyberdéfense</li> <li>Membres de l'équipe d'intervention en cas d'incident</li> <li>Membres de l'équipe du COS</li> </ul>
GIAC Penetration Tester (GPEN)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> <li>Atteste que les candidates et candidats ont la capacité d'effectuer adéquatement des tests de pénétration en se servant de techniques et de méthodologies répondant à des pratiques exemplaires</li> <li>L'examen comporte jusqu'à 115 questions</li> <li>Valide pendant quatre ans</li> </ul>	<ul style="list-style-type: none"> <li>Testeuses et testeurs de pénétration</li> <li>Conceptrices et concepteurs d'exploit</li> <li>Personnel de la sécurité réseau</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>Spécialistes du piratage contrôlé</li> </ul>
GIAC Response and Industrial Defence (GRID)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> <li>Démontre que les candidates et candidats comprennent l'approche de défense active et les attaques propres aux SCI, et savent comment ces attaques guident les stratégies d'atténuation</li> <li>L'examen comporte 75 questions</li> <li>Valide pendant quatre ans</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>Chefs d'équipe et membres de l'équipe d'intervention en cas d'incident visant les systèmes de contrôle industriels (SCI)</li> <li>Chefs d'équipe et analystes du centre des opérations de sécurité</li> <li>Responsables de défense active</li> </ul>
GIAC Reverse Engineering Malware (GREM)	<ul style="list-style-type: none"> <li>Certification de niveau avancé</li> <li>Atteste que les candidates et candidats possèdent les connaissances et les compétences nécessaires pour faire la rétro-ingénierie des maliciels qui ciblent des plateformes courantes comme Microsoft Windows et des navigateurs Web</li> <li>L'examen comporte 75 questions</li> <li>Valide pendant quatre ans</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>Administratrices et administrateurs de système et de réseau</li> <li>Vérificatrices et vérificateurs</li> <li>Gestionnaires de la sécurité</li> <li>Enquêteuses et enquêteurs judiciaires</li> </ul>
GIAC Security Essentials Certification (GSEC)	<ul style="list-style-type: none"> <li>Certification de premier échelon</li> <li>Atteste que les connaissances des candidates et candidats en sécurité de l'information vont au-delà des notions simples de terminologie et de concepts</li> <li>Les titulaires ont de grandes compétences en défense active, en cryptographie, en politiques et plans relatifs à la sécurité, en traitement des incidents et en protection de réseau</li> <li>L'examen comporte 180 questions</li> <li>Valide pendant quatre ans</li> </ul>	<ul style="list-style-type: none"> <li>Professionnelles et professionnels de la sécurité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>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</li> </ul>	
GIAC Security Expert (GSE)	<ul style="list-style-type: none"> <li>On compte moins de 250 titulaires de la certification GSE dans le monde</li> <li>Atteste que les candidates et candidats maîtrisent la vaste gamme de compétences dont ont besoin les meilleurs consultants, consultantes, praticiens et praticiennes de la sécurité</li> <li>Les préalables sont les certifications GSEC, GCIH, GCIA avec deux certifications de catégorie Or</li> <li>L'examen comporte deux volets : 24 questions pratiques basées sur les machines virtuelles et un laboratoire pratique</li> <li>Valide pendant quatre ans</li> <li>Le renouvellement de la certification exige de passer la version actuelle de l'examen</li> <li>Le renouvellement de la certification GSE permet de renouveler toutes les autres certifications GIAC actives</li> </ul>	<ul style="list-style-type: none"> <li>Meilleurs consultants, consultantes, praticiens et praticiennes de la sécurité</li> </ul>
GIAC Security Leadership (GSLC)	<ul style="list-style-type: none"> <li>Certification de niveau avancé pour gestionnaires et leaders</li> <li>Atteste les connaissances des candidates et candidats en matière de gouvernance et de contrôles techniques axés sur la protection et la détection des problèmes de sécurité ainsi que l'intervention face à ceux-ci</li> <li>L'examen comporte 115 questions</li> <li>Valide pendant quatre ans</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>Gestionnaires, superviseurs et superviseurs des équipes de la sécurité de l'information</li> <li>Gestionnaires des TI</li> </ul>
GIAC Systems and Network Auditor (GSNA)	<ul style="list-style-type: none"> <li>Certification de niveau avancé pour gestionnaires et leaders</li> <li>Atteste la capacité des candidates et candidats d'appliquer des techniques d'analyse des risques de base et d'effectuer des vérifications techniques des systèmes d'information essentiels</li> </ul>	<ul style="list-style-type: none"> <li>Personnel technique responsable de sécuriser et de vérifier les systèmes d'information</li> <li>Vérificatrices et vérificateurs</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• L'examen comporte 115 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de réseau</li> <li>• Gestionnaires des équipes de vérification ou de sécurité</li> </ul>
GIAC Web Application Penetration Tester (GWAPT)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Atteste que les candidates et 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</li> <li>• Démontre que les candidates et candidats ont une connaissance des exploits relatifs aux applications Web et des méthodologies de test de pénétration</li> <li>• L'examen comporte 75 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Testeuses et testeurs de pénétration</li> <li>• Testeuses et testeurs de vulnérabilités</li> <li>• Analystes de la sécurité</li> <li>• Analystes de l'évaluation des vulnérabilités</li> <li>• Spécialistes du piratage contrôlé</li> <li>• Conceptrices et concepteurs de site Web</li> </ul>
Global Industrial Cyber Security Professional (GICSP)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Évalue les connaissances et la compréhension de base des candidates et 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</li> <li>• Aucun préalable n'est exigé</li> <li>• L'examen comporte 115 questions</li> <li>• Valide pendant quatre ans</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Ingénieures et ingénieurs de la sécurité</li> <li>• Gestionnaires d'entreprise</li> <li>• Analystes de la sécurité</li> </ul>

## 5.8 INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM

**Tableau 8 : Liste et description des certifications de l'association (ISC)2<sup>8</sup>**

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Cloud Security Professional (CCSP)	<ul style="list-style-type: none"> <li>• Développée en collaboration avec la Cloud Security Alliance (CSA)</li> <li>• Reconnaît les leaders de la sécurité des TI et de l'information qui ont des connaissances et des compétences en architecture, en conception, en exploitation et en orchestration des services de sécurité infonuagique</li> <li>• Les candidates et candidats doivent avoir un minimum de cinq années d'expérience professionnelle en TI, dont au moins trois années en sécurité de l'information et une année dans l'un des six domaines du corpus de connaissances communes menant à la certification CCSP</li> <li>• L'examen comporte 125 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige l'obtention de 90 crédits de formation continue pendant une période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Architectes d'entreprise</li> <li>• Ingénieurs et ingénieurs de système</li> <li>• Architectes de système</li> <li>• Administratrices et administrateurs de la sécurité</li> <li>• Leaders de la sécurité des TI et de l'information</li> </ul>
Titulaires d'une certification en cybersécurité	<ul style="list-style-type: none"> <li>• Certification de premier échelon</li> <li>• Ne requiert aucun préalable et aucune expérience de travail</li> <li>• Démontre que les candidates et candidats possèdent les connaissances, les compétences et les aptitudes fondamentales pour assumer des rôles liés à la cybersécurité de premier échelon et de niveau débutant</li> <li>• L'examen comporte 100 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige l'obtention de 45 crédits de formation continue pendant une période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels des TI</li> <li>• Étudiantes et étudiants de cycles supérieurs, nouvelles diplômées et nouveaux diplômés</li> <li>• Personnes en réorientation</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Information Systems Security Professional (CISSP)	<ul style="list-style-type: none"> <li>• Certification de niveau avancé</li> <li>• Les candidates et candidats doivent avoir au moins cinq années d'expérience professionnelle dans au moins deux des huit domaines du corpus de connaissances communes offert par l'association (ISC)2, ou quatre années d'expérience professionnelle et un diplôme universitaire ou tout autre certificat accrédité</li> <li>• L'examen comporte de 100 à 150 questions utilisant la stratégie du test adaptatif informatisé (TAI)</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige l'obtention de 120 crédits de formation professionnelle continue pendant une période de trois ans</li> <li>• Trois concentrations sont également offertes aux titulaires d'une certification CISSP valide : <ul style="list-style-type: none"> <li>○ CISSP-ISSAP (architecture)</li> <li>○ CISSP-ISSEP (ingénierie)</li> <li>○ CISSP-ISSMP (gestion)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Dirigeantes principales et dirigeants principaux de la sécurité de l'information</li> <li>• Dirigeantes principales et dirigeants principaux de la sécurité</li> <li>• Analystes, vérificatrices et vérificateurs de la sécurité</li> <li>• Directrices et directeurs de la sécurité</li> <li>• Directrices, directeurs ou gestionnaires des TI</li> </ul>
Healthcare Information Security and Privacy Practitioner (HCISPP)	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats ont les connaissances et les compétences nécessaires pour mettre en œuvre, gérer ou évaluer les contrôles de sécurité et de confidentialité touchant les renseignements sur les soins de santé et sur les patients</li> <li>• Conçue pour les praticiennes, les praticiens, les consultantes et les consultants dont le travail demande le respect de la sécurité et de la confidentialité des renseignements sur les soins de santé</li> <li>• Les candidates et candidats doivent avoir un minimum de deux années d'expérience professionnelle</li> <li>• L'examen comporte 125 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification nécessite l'obtention de 60 crédits de formation continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Agentes et agents de conformité</li> <li>• Superviseuses et superviseurs des dossiers médicaux</li> <li>• Gestionnaires de la pratique</li> <li>• Gestionnaires de la sécurité de l'information</li> <li>• Gestionnaires de l'information sur la santé</li> </ul>
Systems Security Certified Practitioner (SSCP)	<ul style="list-style-type: none"> <li>• Certification mondiale en sécurité des TI</li> <li>• Certification de premier échelon</li> </ul>	<ul style="list-style-type: none"> <li>• Ingénieures et ingénieurs de la sécurité réseau</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Démontre que les titulaires de cette certification possèdent les compétences et les connaissances techniques pour mettre en œuvre, surveiller et administrer une infrastructure TI</li> <li>• Conçue pour les praticiennes et praticiens qui remplissent des fonctions TI opérationnelles ou qui travaillent en sécurité de l'information</li> <li>• Les candidates et candidats doivent avoir une année d'expérience professionnelle cumulative dans au moins l'un des sept domaines du corpus de connaissances communes offerts par le programme SSCP; une reconnaissance équivalant à une année d'expérience sera accordée aux candidates et candidats détenant un baccalauréat ou une maîtrise en cybersécurité</li> <li>• L'examen comporte 125 questions à choix multiples</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification nécessite l'obtention de 60 crédits de formation continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de système</li> <li>• Analystes de la sécurité</li> <li>• Analystes de système et de réseau</li> <li>• Consultantes et consultants en sécurité</li> <li>• Administratrices, administrateurs, directrices, directeurs ou gestionnaires des TI</li> </ul>



## 5.9 ISACA

Tableau 9 : Liste et description des certifications de ISACA<sup>9</sup>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Cybersecurity Practitioner (CSX-P)	<ul style="list-style-type: none"> <li>• Nouvelle certification créée en 2015</li> <li>• Reconnaît les personnes qui peuvent agir à titre de premières intervenantes et premiers intervenants lors d'incidents de sécurité</li> <li>• 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 (<i>Cyber Security Framework</i>) : identification, protection, détection, intervention et récupération</li> <li>• Les candidates et candidats doivent passer un examen basé sur le rendement comportant des simulations d'incidents de sécurité</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige l'obtention de 120 heures de formation professionnelle continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Praticiennes et praticiens de la sécurité</li> <li>• Gestionnaires des incidents</li> </ul>
Certified in Risk and Information Systems Control (CRISC)	<ul style="list-style-type: none"> <li>• Reconnaît les candidates et candidats qui identifient, évaluent et gèrent les risques par l'élaboration, la mise en œuvre et la maintenance des contrôles de systèmes d'information</li> <li>• Les candidates et candidats doivent avoir trois années d'expérience professionnelle en gestion et en contrôle des risques; l'éducation ne peut pas remplacer l'expérience</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige l'obtention de 120 heures de formation professionnelle continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels en TI et dans le milieu des affaires</li> <li>• Professionnelles et professionnels dans le domaine des risques et de la conformité</li> <li>• Analystes des activités</li> <li>• Gestionnaires de projets</li> <li>• Directrices et directeurs de la sécurité</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Information Security Manager (CISM)	<ul style="list-style-type: none"> <li>• Certification axée sur la gestion</li> <li>• Reconnaît les candidates et candidats qui gèrent, conçoivent, supervisent et évaluent la sécurité de l'information d'une entreprise</li> <li>• Les candidates et 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</li> <li>• Une demande écrite doit être présentée</li> <li>• L'examen comporte 150 questions à répondre en quatre heures</li> <li>• Valide pendant trois ans</li> <li>• Le renouvellement de la certification exige l'obtention de 120 heures de formation professionnelle continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Gestionnaires, directrices et directeurs de la sécurité de l'information</li> <li>• Analystes de la sécurité des TI</li> <li>• Analystes des risques</li> <li>• Vérificatrices et vérificateurs des TI</li> <li>• Gestionnaires de la sécurité des systèmes d'information</li> </ul>
Certified Information Systems Auditor (CISA)	<ul style="list-style-type: none"> <li>• Certification universellement reconnue</li> <li>• Atteste l'expérience, les compétences et les connaissances des candidates et 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</li> <li>• Les candidates et candidats doivent avoir cinq années d'expérience professionnelle en vérification, en contrôle ou en sécurité des systèmes d'information (SI); certains critères d'éducation peuvent remplacer l'expérience</li> <li>• L'examen comporte 150 questions</li> <li>• Les titulaires de cette certification doivent suivre au moins 120 heures de formation continue pendant la période de trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels du contrôle de vérification, de l'assurance de la qualité et de la sécurité des systèmes d'information</li> </ul>

## 5.10 ITSM SOLUTIONS

Tableau 10 : Liste et description des certifications d'itSM Solutions<sup>10</sup>

Certification	Aperçu de la certification	Candidates et candidats ciblés
NIST Cyber Security Professional (NCSP) Foundation	<ul style="list-style-type: none"> <li>• Certification de premier échelon</li> <li>• Atteste que les candidates et candidats ont les connaissances et les capacités nécessaires pour opérationnaliser le cadre de cybersécurité du NIST (NCSF pour <i>NIST Cyber Security Framework</i>)</li> <li>• Aucun préalable n'est exigé, mais des compétences de base en informatique et des connaissances en sécurité sont recommandées</li> <li>• L'examen comporte 40 questions à choix multiples</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels de la sécurité, des TI ou de la gestion des risques</li> <li>• Vérificatrices et vérificateurs</li> <li>• D'autres professionnelles et professionnels devant comprendre les rudiments de la cybersécurité, les composantes du NCSF et leur application dans le cadre de la gestion des risques</li> </ul>
NCSP Practitioner	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats ont les compétences et les capacités nécessaires pour concevoir, établir, tester, gérer et améliorer un programme de cybersécurité basé sur le NCSF</li> <li>• Les candidates et candidats doivent avoir terminé la formation et l'examen NCSF Foundation avant d'essayer de passer l'examen</li> <li>• L'examen comporte 65 questions à choix multiples</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels des TI et de la cybersécurité</li> </ul>

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

## 5.11 MCAFEE INSTITUTE

**Tableau 11 : Liste et description des certifications du McAfee Institute<sup>11</sup>**

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Counterintelligence Threat Analyst (CCTA)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats d'identifier les cybercriminelles et cybercriminels et d'enquêter sur eux, de mener des enquêtes de contre-ingérence visant à atténuer les menaces, et d'enquêter et de poursuivre en justice les pirates informatiques, les cybercriminelles et les cybercriminels</li> <li>• Préalables : baccalauréat ou diplôme de niveau supérieur et trois années d'expérience dans un domaine connexe, ou diplôme associé et quatre années d'expérience</li> <li>• Les candidates et candidats doivent se soumettre à une vérification des antécédents</li> <li>• L'examen comporte 200 questions</li> <li>• Valide pendant deux ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes</li> </ul>
Certified Cyber Intelligence Investigator (CCII)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats de mener des cyberenquêtes, d'utiliser des méthodologies afin de poursuivre en justice des cybercriminelles et cybercriminels, d'appliquer la criminalistique mobile et numérique, de reconnaître la fraude et le piratage, et de procéder à la collecte de renseignement</li> <li>• Préalables : baccalauréat ou diplôme de niveau supérieur et une année d'expérience dans un domaine connexe, ou diplôme associé et deux années d'expérience</li> <li>• Les candidates et candidats doivent se soumettre à une vérification des antécédents</li> <li>• L'examen comporte 200 questions</li> <li>• Valide pendant deux ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Cyber Intelligence Professional (CCIP)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats de mener des cyberenquêtes, d'utiliser des méthodologies afin de poursuivre en justice des cybercriminelles et 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</li> <li>• Préalables : baccalauréat ou diplôme de niveau supérieur et trois années d'expérience dans un domaine connexe, ou diplôme associé et quatre années d'expérience</li> <li>• Les candidates et candidats doivent se soumettre à une vérification des antécédents</li> <li>• L'examen comporte 200 questions</li> <li>• Valide pendant deux ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes</li> </ul>
Certified Expert in Cyber Investigations (CECI)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats de reconnaître et d'identifier les cybercriminelles et 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, les cybercriminelles et les cybercriminels</li> <li>• Préalables : baccalauréat ou diplôme de niveau supérieur et quatre années d'expérience dans un domaine connexe, ou diplôme associé et six années d'expérience</li> <li>• Les candidates et candidats doivent se soumettre à une vérification des antécédents</li> <li>• L'examen comporte 200 questions de type vrai ou faux, des questions à choix multiples et des questions axées sur des scénarios</li> <li>• Valide pendant deux ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent payer des frais de renouvellement et obtenir des crédits de formation continue</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes qui travaillent dans les domaines de la cybersécurité, de l'application de la loi et de la prévention des pertes</li> </ul>

## 5.12 OFFENSIVE SECURITY

Tableau 12 : Liste et description des certifications d'Offensive Security<sup>12</sup>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Offensive Security Certified Expert (OSCE)	<ul style="list-style-type: none"> <li>Démontre que les candidates et 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</li> <li>Les candidates et candidats doivent avoir des connaissances préalables des techniques d'exploitation Windows, avoir de l'expérience avec Linux et posséder une connaissance approfondie du protocole TCP/IP et de la réseautique</li> <li>Les candidates et candidats doivent avoir terminé le cours intitulé <i>Cracking the Perimeter</i> avant de passer l'examen</li> <li>Le temps accordé pour l'examen est de 48 heures, et il comporte des tests de pénétration pratiques dans un réseau privé virtuel (RPV) isolé; les candidates et candidats doivent également présenter un rapport de test exhaustif</li> </ul>	<ul style="list-style-type: none"> <li>Testeuses et testeurs de pénétration</li> <li>Professionnelles et professionnels de la sécurité</li> </ul>
Offensive Security Certified Professional (OSCP)	<ul style="list-style-type: none"> <li>Atteste que les candidates et candidats ont les connaissances et les compétences nécessaires pour trouver les vulnérabilités et déployer des attaques organisées d'une manière contrôlée et ciblée</li> <li>S'adresse aux testeuses et testeurs de pénétration possédant un solide bagage technique et en piratage contrôlé, et une connaissance approfondie des réseaux TCP/IP</li> <li>Les candidates et candidats doivent d'abord terminer le cours de formation intitulé <i>Penetration Testing</i></li> <li>La certification est difficile à obtenir en raison de l'examen qui est manifestement complexe</li> <li>Les candidates et candidats doivent passer un examen de 24 heures au cours duquel ils doivent réussir à attaquer et à pénétrer des systèmes opérationnels dans un environnement de laboratoire sécuritaire; ils doivent également présenter un rapport de test de pénétration exhaustif</li> </ul>	<ul style="list-style-type: none"> <li>Testeuses et testeurs de pénétration</li> <li>Administratrices et administrateurs de réseau</li> <li>Professionnelles et professionnels de la sécurité réseau</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
Offensive Security Exploitation Expert (OSEE)	<ul style="list-style-type: none"> <li>• La certification n'expire jamais</li> <li>• Exige beaucoup de temps</li> <li>• Atteste la capacité des candidates et candidats d'analyser les logiciels vulnérables, de trouver un code problématique et de développer des exploits sophistiqués dans divers systèmes d'exploitation Windows modernes</li> <li>• Les candidates et candidats doivent avoir de l'expérience en développement d'exploits dans Windows et ils doivent comprendre le fonctionnement d'un débogueur</li> <li>• Les candidates et candidats doivent avoir terminé le cours intitulé <i>Advanced Windows Exploitation</i> avant de passer l'examen</li> <li>• Les candidates et candidats devraient obtenir au préalable la certification OSCE</li> <li>• L'examen consiste à développer et à documenter des exploits pendant une période de 72 heures; les candidates et candidats doivent également présenter un rapport de test de pénétration exhaustif</li> <li>• La certification permet aux titulaires d'obtenir 40 crédits de formation continue (ISC)2</li> <li>• La certification n'expire jamais</li> </ul>	<ul style="list-style-type: none"> <li>• Testeuses et testeurs de pénétration</li> </ul>
Offensive Security Web Expert (OSWE)	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats ont des connaissances pratiques de l'évaluation des applications Web et du processus de piratage; ainsi que leur capacité d'examiner du code source avancé dans des applications Web, de trouver des vulnérabilités et de les exploiter</li> <li>• Les candidates et candidats doivent bien connaître les langages de codage et Linux, être en mesure d'écrire des scripts et avoir de l'expérience avec les mandataires Web, une compréhension générale des vecteurs d'attaque des applications Web, en théorie et en pratique, et une connaissance approfondie du protocole TCP/IP et de la réseautique</li> <li>• Les candidates et candidats doivent réussir le cours intitulé <i>Advanced Web Attacks and Exploitation</i> avant de passer l'examen</li> <li>• Le temps accordé pour l'examen est de 48 heures, et il comporte une évaluation pratique d'applications Web dans un RPV isolé; les candidates et candidats qui réussissent doivent également présenter un rapport d'évaluation</li> </ul>	<ul style="list-style-type: none"> <li>• Testeuses et testeurs de pénétration</li> <li>• Spécialistes de la sécurité des applications Web</li> <li>• Ingénieures et ingénieurs en logiciel</li> <li>• Développeuses et développeurs Web</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• La certification n'expire jamais</li> </ul>	
Offensive Security Wireless Professional (OSWP)	<ul style="list-style-type: none"> <li>• Atteste la capacité des candidates et candidats de trouver des vulnérabilités et des chiffrements en place dans des réseaux répondant à la norme 802.11 de l'Institute of Electrical and Electronics Engineers (IEEE), de contourner des restrictions liées à la sécurité et de récupérer les clés de chiffrement utilisées</li> <li>• Les candidates et candidats doivent avoir une compréhension approfondie du protocole TCP/IP et du modèle OSI (<i>Open System Interconnection</i>), ainsi qu'une connaissance de Linux</li> <li>• Les candidates et candidats doivent avoir terminé le cours intitulé <i>Offensive Security Wireless Attacks</i> avant de passer l'examen</li> <li>• L'examen de quatre heures demande aux candidates et candidats de recueillir de l'information sans fil, et de mettre en œuvre diverses attaques afin d'avoir accès aux réseaux cibles; les candidates et candidats doivent également présenter un rapport sur les tests de pénétration</li> <li>• La certification n'expire jamais</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de réseau</li> <li>• Testeuses et testeurs de pénétration</li> </ul>
Security Operations and Defensive Analysis (OSDA)	<ul style="list-style-type: none"> <li>• Valide que les candidats peuvent reconnaître les méthodologies communes pour les chaînes d'attaque de bout en bout (framework MITRE ATT&amp;CK®)</li> <li>• Les candidats peuvent effectuer des audits guidés de systèmes compromis sur plusieurs systèmes d'exploitation.</li> <li>• Les candidats démontreront leur capacité à utiliser un SIEM pour identifier et évaluer une attaque au fur et à mesure qu'elle se déroule en direct.</li> <li>• Les candidats valides peuvent inspecter manuellement les journaux afin de pouvoir reconnaître les activités normales et anormales ou bénignes et malveillantes.</li> <li>• La certification doit être renouvelée tous les trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Testeuses et testeurs de pénétration</li> <li>• Professionnelles et professionnels de la sécurité réseau</li> </ul>



## 5.13 PECB

Tableau 13 : Liste et description des certifications de PECB<sup>13</sup>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
Computer Forensics Foundation	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les principes et concepts fondamentaux relatifs à l'informatique judiciaire, et les processus d'informatique judiciaire</li> <li>• Aucun préalable n'est exigé</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes souhaitant faire carrière en informatique judiciaire</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
	<ul style="list-style-type: none"> <li>• Examen d'une heure à livre ouvert qui comporte cinq questions de type rédactionnel</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</li> </ul>	
ISO/IEC 27032 Foundation	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats ont des connaissances en ce qui a trait aux principes et aux concepts fondamentaux de cybersécurité, et une compréhension des approches, des méthodes et des techniques utilisées en cybersécurité</li> <li>• Aucun préalable n'est exigé</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB</li> <li>• Examen d'une heure qui comporte 40 questions à choix multiples</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels en cybersécurité et en sécurité de l'information</li> <li>• Personnes souhaitant poursuivre une carrière en cybersécurité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
	<ul style="list-style-type: none"> <li>• Valide pendant trois ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</li> </ul>	
ISO/IEC 27032 Lead Cybersecurity Manager <ul style="list-style-type: none"> <li>• Certified Provisional</li> <li>• Certified</li> <li>• Certified Lead</li> <li>• Certified Senior Lead</li> </ul>	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les principes et concepts fondamentaux de la cybersécurité, les rôles et responsabilités des parties prenantes, la gestion des risques liés à la cybersécurité, les mécanismes d'attaque et les contrôles en cybersécurité, l'échange d'information et la coordination, l'intégration d'un programme de cybersécurité à la gestion de la continuité des activités, et la gestion des incidents de cybersécurité et la mesure du rendement</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels en cybersécurité et en sécurité de l'information</li> <li>• Responsables du développement ou de la gestion d'un programme de cybersécurité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
	<ul style="list-style-type: none"> <li>• Les candidates et candidats doivent avoir une compréhension fondamentale de la norme ISO/IEC 27032 et des connaissances approfondies en cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB</li> <li>• Examen de trois heures à livre ouvert qui comporte douze questions de type rédactionnel</li> <li>• Les candidates et candidats qui ont réussi l'examen peuvent postuler pour l'un des quatre titres de compétence en fonction du nombre d'années d'expérience de travail, d'expérience en cybersécurité et du nombre total d'heures consacrées à des activités de cybersécurité</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le</li> </ul>	

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
	nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels	
Lead Cloud Security Manager <ul style="list-style-type: none"> <li>• Certified Provisional</li> <li>• Certified</li> <li>• Certified Lead</li> <li>• Certified Senior Lead</li> </ul>	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui a trait aux principes et aux concepts de l'informatique en nuage, à la gestion des risques et des incidents de sécurité infonuagique, et aux tests, à la surveillance et à l'amélioration continue de la sécurité infonuagique</li> <li>• Les candidates et candidats doivent avoir une compréhension fondamentale des normes ISO/IEC 27017 et ISO/IEC 27018, et une connaissance générale des concepts de l'informatique en nuage</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB</li> <li>• Examen de trois heures à livre ouvert qui comporte 80 questions à choix multiples</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels de la sécurité infonuagique et de la sécurité de l'information</li> <li>• Personnes chargées de maintenir et de gérer un programme de sécurité infonuagique</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
	<ul style="list-style-type: none"> <li>• Les candidates et candidats qui ont réussi l'examen peuvent postuler pour l'un des quatre titres de compétence en fonction du nombre d'années d'expérience de travail, du nombre d'années d'expérience en cybersécurité et du nombre total d'heures consacrées à des activités de projets CCSMS</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</li> </ul>	Conseillères spécialisées et conseillers spécialisés en sécurité infonuagique
Lead Forensics Examiner <ul style="list-style-type: none"> <li>• Certified Provisional</li> <li>• Certified</li> </ul>	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les principes et concepts fondamentaux relatifs à l'informatique judiciaire, les exigences relatives aux laboratoires de criminalistique numérique, les enquêtes</li> </ul>	<ul style="list-style-type: none"> <li>• Spécialistes, consultantes et consultants en informatique judiciaire</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
<ul style="list-style-type: none"> <li>• Certified Lead</li> </ul>	<p>sur les crimes informatiques et les examens d'informatique judiciaire, et le maintien de la chaîne de possession</p> <ul style="list-style-type: none"> <li>• Les candidates et candidats doivent avoir des connaissances en informatique judiciaire</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB</li> <li>• Examen de trois heures à livre ouvert qui comporte quatorze questions de type rédactionnel</li> <li>• Les candidates et candidats qui ont réussi l'examen peuvent postuler pour l'un des trois titres de compétence en fonction du nombre d'années d'expérience de travail, du nombre d'années d'expérience en cybersécurité et du nombre total d'heures consacrées à des activités d'informatique judiciaire</li> <li>• Valide pendant trois ans</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels de la cybersécurité</li> <li>• Analystes de cyberrenseignement</li> <li>• Professionnelles et professionnels chargés de l'application de la loi</li> <li>• Analystes de données électroniques</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
	<ul style="list-style-type: none"> <li>• Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</li> </ul>	
<p>Lead Pen Test Professional</p> <ul style="list-style-type: none"> <li>• Certified Provisional</li> <li>• Certified</li> <li>• Certified Lead</li> </ul>	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les principes et concepts fondamentaux relatifs aux tests de pénétration, les bases techniques pour les tests de pénétration, les types de tests, et l'analyse des résultats et du processus de rapport</li> <li>• Les candidates et candidats doivent avoir une compréhension fondamentale des tests de pénétration, et des connaissances approfondies en cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB</li> <li>• Examen de trois heures qui comporte 150 questions à choix multiples</li> </ul>	<ul style="list-style-type: none"> <li>• Professionnelles et professionnels des TI</li> <li>• Vérificatrices et vérificateurs</li> <li>• Gestionnaires des TI et des risques</li> <li>• Testeuses et testeurs de pénétration</li> </ul>



Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Lead Ethical Hacker	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats possèdent des connaissances en ce qui concerne les outils et techniques de collecte d'information, la modélisation des menaces et l'identification des vulnérabilités, les techniques d'exploitation, les rapports, etc.</li> <li>• Les candidates et candidats doivent avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation</li> <li>• Les candidates et candidats doivent avoir deux années d'expérience en matière de tests de pénétration et de cybersécurité</li> <li>• Les candidates et candidats doivent signer le Code de déontologie de PECB et le Code de conduite pour les PECB CLEH</li> <li>• Examen de six heures à livre ouvert qui comprend deux parties : les candidates et candidats doivent d'abord compromettre au moins deux machines cibles au moyen des tests de pénétration, puis documenter le processus dans un rapport écrit</li> <li>• Valide pendant trois ans</li> </ul> <p>Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</p>	<ul style="list-style-type: none"> <li>• Personnes responsables de la sécurité des systèmes d'information</li> <li>• Membres de l'équipe de sécurité de l'information</li> </ul>
	<ul style="list-style-type: none"> <li>• Les candidates et candidats qui ont réussi l'examen peuvent postuler pour l'un des trois titres de compétence en fonction du nombre d'années d'expérience de travail, du nombre d'années d'expérience dans le domaine des tests de pénétration et du nombre total d'heures consacrées à des activités de tests de pénétration</li> <li>• Valide pendant trois ans</li> <li>• Pour renouveler la certification, les candidates et candidats doivent démontrer qu'ils continuent d'exécuter les tâches relatives à la certification, qu'ils ont obtenu le nombre requis de crédits de formation professionnelle continue (FPC) et qu'ils paient les frais de maintien annuels</li> </ul>	<ul style="list-style-type: none"> <li>• Spécialistes du piratage contrôlé</li> </ul>

## 5.14 SECO INSTITUTE

Tableau 14 : Liste et description des certifications du SECO Institute<sup>14</sup>

Certification	Aperçu de la certification	Candidates et candidats ciblés
Certified Ethical Hacker (S-EHE)	<ul style="list-style-type: none"> <li>Le programme fait l'objet d'une restructuration</li> </ul>	<ul style="list-style-type: none"> <li>s.o.</li> </ul>
Dark Web Foundations	<ul style="list-style-type: none"> <li>Certification de premier échelon</li> <li>Développée par la Netherlands Organisation for Applied Scientific Research en collaboration avec l'International Criminal Police Organization (INTERPOL)</li> <li>Démontre que les candidates et candidats comprennent l'utilisation du Web invisible de manière sécuritaire</li> <li>L'examen comporte 40 questions à choix multiples</li> <li>Aucune limite de validité et aucune exigence de renouvellement de la certification ne s'appliquent</li> </ul>	<ul style="list-style-type: none"> <li>Professionnelles et professionnels de la sécurité des TI</li> <li>Application de la loi</li> <li>Responsables des politiques et représentantes et représentants de gouvernement</li> </ul>
Ethical Hacking Foundations (S-EHF)	<ul style="list-style-type: none"> <li>Certification de premier échelon</li> <li>Atteste que les candidates et candidats ont une connaissance approfondie des techniques de base liées aux tests de pénétration et qu'ils comprennent les principes fondamentaux du piratage</li> <li>L'examen comporte 40 questions à choix multiples</li> <li>Aucune limite de validité et aucune exigence de renouvellement de la certification ne s'appliquent</li> </ul>	<ul style="list-style-type: none"> <li>Développeuses et développeurs Web</li> <li>Ingénieures et ingénieurs de logiciel</li> <li>Administratrices et administrateurs de la sécurité</li> <li>Ingénieures et ingénieurs de réseau</li> <li>Spécialistes du piratage contrôlé</li> </ul>
Ethical Hacking Leader (S-EHL)	<ul style="list-style-type: none"> <li>La plus haute distinction de compétence dans le volet <i>Ethical Hacking</i></li> </ul>	<ul style="list-style-type: none"> <li>Professionnelles et professionnels souhaitant</li> </ul>

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

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Démontre que les candidates et candidats ont d'excellentes compétences dans le domaine des tests de pénétration, ainsi que de l'expérience de la direction de tests de pénétration</li> <li>• Les candidates et candidats doivent avoir des connaissances de spécialiste (certificat de niveau expert du SECO Institute ou l'équivalent) et au moins trois années d'expérience professionnelle pertinente</li> <li>• Aucun examen n'est requis</li> <li>• Valide pour une période d'un an</li> <li>• Pour renouveler la certification, les candidates et candidats doivent payer une cotisation annuelle et obtenir 40 crédits de formation continue durant l'année</li> </ul>	<p>valider l'expertise acquise dans le cadre de leur expérience pratique de travail</p>
Ethical Hacking Practitioner (S-EHP)	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats comprennent pleinement le processus de test de pénétration et qu'ils connaissent les techniques courantes liées aux tests de pénétration</li> <li>• Les candidates et candidats doivent bien comprendre les principes de base du piratage contrôlé</li> <li>• La certification S-EHP (ou l'équivalent) est recommandée</li> <li>• Examen en trois volets : dix questions à choix multiples, cinq questions de type rédactionnel et une étude de cas</li> <li>• Valide pour une période d'un an</li> <li>• Pour renouveler la certification, les candidates et candidats doivent payer une cotisation annuelle et obtenir 20 crédits de formation continue durant l'année</li> </ul>	<ul style="list-style-type: none"> <li>• Développeuses et développeurs Web</li> <li>• Administratrices et administrateurs de la sécurité informatique</li> <li>• Ingénieures et ingénieurs de réseau</li> <li>• Ingénieures et ingénieurs de logiciel</li> <li>• Testeuses et testeurs de pénétration potentiels</li> </ul>
IT Security Expert/SOC (S-ITSE/SOC)	<ul style="list-style-type: none"> <li>• Atteste que les candidates et candidats ont les connaissances et les compétences nécessaires pour prendre en charge la détection et l'analyse des menaces et l'intervention en cas de menace, et pour améliorer l'ensemble de la sécurité d'une organisation</li> <li>• Les candidates et candidats doivent avoir une compréhension de base du protocole TCP/IP, des principes fondamentaux des systèmes d'exploitation et des concepts de sécurité courants, et posséder deux années d'expérience dans un COS</li> <li>• Le préalable exigé est la certification S-ITSP ou l'équivalent</li> </ul>	<ul style="list-style-type: none"> <li>• Personnes aspirant à devenir des analystes de COS de niveau 1 et de niveau II</li> <li>• Futures et futurs gestionnaires de COS</li> <li>• Ingénieures et ingénieurs de système</li> <li>• Analystes de la sécurité</li> </ul>

Certification	Aperçu de la certification	Candidates et candidats ciblés
	<ul style="list-style-type: none"> <li>• Les candidates et candidats peuvent choisir l'une de deux spécialisations : gestionnaire de COS (<i>Manager SOC</i>) ou gestionnaires de la sécurité des TI (<i>IT Security Manager</i>)</li> <li>• Valide pour une période d'un an</li> <li>• Pour renouveler la certification, les candidates et candidats doivent payer une cotisation annuelle et obtenir 40 crédits de formation continue durant l'année</li> </ul>	
IT Security Foundation (S-ITSF)	<ul style="list-style-type: none"> <li>• Certification de premier échelon</li> <li>• Atteste que les candidates et candidats ont une connaissance de base de l'architecture informatique, des vulnérabilités matérielles courantes et des mesures de sécurité</li> <li>• Aucun préalable n'est exigé; convient aux débutantes et débutants qui ont quelques connaissances de base en informatique et en technologie</li> <li>• L'examen comporte 40 questions à choix multiples</li> <li>• Aucune limite de validité et aucune exigence de renouvellement de la certification ne s'appliquent</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de réseau ou de système</li> <li>• Personnes qui désirent entamer une carrière en sécurité des TI</li> </ul>
IT Security Practitioner (S-ITSP)	<ul style="list-style-type: none"> <li>• Atteste les compétences techniques des candidates et candidats en gestion des vulnérabilités, en sécurité de pare-feu et de réseau, en architecture de sécurité et en test de pénétration</li> <li>• Les candidates et candidats doivent avoir une bonne connaissance des termes, des concepts et des principes de base de la sécurité des TI</li> <li>• La certification <i>IT Security Foundation</i> (ou l'équivalent) est recommandée</li> <li>• L'examen comporte dix questions à choix multiples, cinq questions ouvertes et une étude de cas</li> <li>• Valide pour une période d'un an</li> <li>• Pour renouveler la certification, les candidates et candidats doivent payer une cotisation annuelle et obtenir 60 crédits de formation continue durant l'année</li> </ul>	<ul style="list-style-type: none"> <li>• Administratrices et administrateurs de la sécurité informatique</li> <li>• Analystes de la sécurité</li> <li>• Architectes de la sécurité</li> <li>• Vérificatrices et vérificateurs de la sécurité</li> <li>• Futures et futurs analystes du COS</li> </ul>

## 6.0 CONTENU COMPLÉMENTAIRE

### 6.1 LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

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

Acronyme, abréviation ou sigle	Définition
RFID	Identification par radiofréquence ( <i>Radio Frequency Identification</i> )
RPV	Réseau privé virtuel
SCADA	Télésurveillance et acquisition de données ( <i>Supervisory Control and Data Acquisition</i> )
SCI	Système de contrôle industriel
SE	Système d'exploitation
SECO	Security and Continuity Institute
SI	Système d'information
TCP/IP	Protocole TCP/IP ( <i>Transmission Control Protocol/Internet Protocol</i> )
TI	Technologies de l'information
UKAS	United Kingdom Accreditation Service
WLAN	Réseau local sans fil ( <i>Wireless Local Area Network</i> )

## 6.2 RÉFÉRENCES

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