

Diplôme canadien international délocalisé délivré par un établissement public Québécois, dans le cadre du système collégial du Québec



Devenez Consultant international en Cybersécurité augmentée par l'IA

Passez de la compréhension des cybermenaces à la maîtrise opérationnelle de la sécurité des systèmes, du cloud et des données.

Apprenez à protéger les réseaux, les systèmes et les environnements Cloud des organisations face aux cyberattaques, en apprenant à exploiter l'intelligence artificielle pour renforcer la détection et la réponse aux menaces, et en construisant des compétences techniques reconnues et recherchées sur le marché du travail — en Tunisie et à l'international.

À l'issue du parcours, le participant sera mieux préparé à intervenir au sein d'une équipe de cybersécurité, à contribuer à la sécurisation des infrastructures et à évoluer progressivement vers des fonctions de consultant Cyber, Cloud & IA.

A.E.C. en Cyber sécurité & sécurité infonuagique (Cloud Computing) • LEA.EB — Diplôme Professionnel International Étatique du Cégep de Sherbrooke (Québec – Canada) délocalisé en Tunisie • **540 heures**

Voir le détails sur site Canadien : (https://cegepsherbrooke.qc.ca/formations/aec/cybersecurite-et-securite-infonuagique/?utm_source=chatgpt.com#couts-et-details)

Voici notre lien en tant que nous sommes partenaire officiel du cegep ; [Formations offertes à l'international | Cégep de Sherbrooke](#)

540 h de formation officielle	9 cours spécialisés	7 à 10 mois selon la formule choisie	++++ Préparations 4 Certifications internationales
--	-------------------------------	---	---

Un diplôme étatique Canadien délocalisé en Tunisie

Délivré par le Cégep de Sherbrooke, établissement public québécois — un diplôme qui valorise votre profil bien au-delà de la Tunisie.

Deux expertises, un seul profil

Sécurité des réseaux et des systèmes d'un côté, sécurité des environnements Cloud (inonuagique) de l'autre — les

	deux dans un seul cursus et Application des outils IA dans la cybersécurité
Ouvert aux Personnes voulant la reconversion professionnelle Accessible aux titulaires d'un baccalauréat scientifique, et plus, ou d'une formation jugée suffisante (BTP ou AEC dans le domaine de l'informatique au sein de notre de structure canadienne)	3 formules pour s'adapter à votre rythme Temps plein en 7 mois, ou temps partiel en 10 mois — en soirée en ligne ou le week-end en présentiel.
4 Préparations aux certifications internationales Le programme prépare aux référentiels ISO/IEC 27001 (PECB), Cisco CCNA, Cisco Cyber Ops Associate et Cisco Ethical Hacking.	Un secteur en forte expansion La cybersécurité est aujourd'hui au cœur des priorités du monde — un domaine porteur, avec des profils recherchés sur le marché national et international. Le marché mondial a besoin d'environ 4000 000 de personnes compétentes en cyber sécurité

01 — POURQUOI CHOISIR CETTE FORMATION

La cybersécurité, un enjeu incontournable pour les organisations

Les cyberattaques, les intrusions et les fuites de données sont devenues des menaces constantes pour les entreprises et les institutions, d'autant plus que l'intelligence artificielle est aujourd'hui utilisée aussi bien pour renforcer les défenses que pour sophistiquer les attaques.

Protéger les systèmes informatiques, les réseaux et les données n'est plus une option : c'est une priorité stratégique — et ce Diplôme international, vous prépare à y répondre concrètement, avec l'appui des outils d'IA les plus récents.

UN SECTEUR EN FORTE DEMANDE

La cybersécurité est un domaine **en pleine expansion**, au cœur des préoccupations numériques actuelles. Les entreprises recherchent activement des profils capables d'intervenir sur la sécurité des systèmes, des réseaux et des environnements Cloud — et de plus en plus, capables d'utiliser l'intelligence artificielle pour anticiper et contrer les cybermenaces.

Deux expertises complémentaires, un seul cursus

Sécurité des systèmes & réseaux Sécuriser les infrastructures réseau, administrer et durcir les systèmes Linux, gérer les identités et les accès, surveiller les événements de sécurité, et intervenir en réponse aux incidents — avec le soutien d'outils d'IA pour la détection des anomalies et l'automatisation de la surveillance.	Sécurité Cloud (infonuagique) Comprendre les infrastructures Cloud, détecter leurs vulnérabilités, comprendre les menaces qui leur sont propres et les sécuriser dans le cadre de la stratégie globale de l'organisation, notamment grâce à l'intelligence artificielle pour l'analyse prédictive des risques Cloud.
---	--

02 — À QUI S'ADRESSE LA FORMATION

Un programme conçu pour les personnes scientifiques et techniques

Ce programme s'adresse à toute personne souhaitant se spécialiser dans la protection des systèmes d'information, sans nécessairement disposer d'une expérience professionnelle préalable en cybersécurité car les fondamentaux en réseaux et Cloud sont incorporés dans le programme Canadien

03 — LES OBJECTIFS DE LA FORMATION

Construire une expertise opérationnelle en cybersécurité

À l'issue du programme, vous serez en mesure d'agir à titre de spécialiste technique en cybersécurité ou en sécurité informatique — que ce soit en sécurité applicative, en test d'intrusion, ou en réponse aux incidents.

- Comprendre les enjeux de la cybersécurité dans le contexte d'une organisation et le rôle des différentes parties prenantes.
- Maîtriser les fondamentaux des réseaux, des systèmes et des environnements Cloud, ainsi que leur sécurisation.
- Gérer les identités, les accès et les privilèges au sein d'un système d'information.
- Assurer une surveillance proactive et savoir réagir efficacement face à un incident de sécurité.
- Se préparer à des certifications professionnelles reconnues à l'international, tout en développant des compétences pratiques d'utilisation de l'intelligence artificielle appliquée à la cybersécurité

04 — LE PARCOURS DE FORMATION

540 heures de formation théorique et pratique, fondées sur les compétences, la gestion de projets et l'apprentissage autonome.

Parcours professionnalisant par compétences et projets

COURS ; Reference Canadienne	CE QUE VOUS Y APPRENEZ	DURÉE
310-CA1-SH Cyber sécurité dans le contexte d'une organisation	Fondamentaux de la cybersécurité, enjeux d'affaires et rôle des parties prenantes. Prépare les bases des référentiels ISO/IEC 27001 et des parcours Cisco. Introduction au rôle de l'intelligence artificielle dans la gouvernance des risques cyber.	60 h
420-CA2-SH Gestion des identités et des accès	Authentification, gestion des accès et des privilèges, non-répudiation, traçabilité des actes posés. Utilisation de l'IA pour détecter les comportements d'accès anormaux.	45 h
420-CA3-SH Sécurisation d'un environnement infonuagique 1	Compréhension des infrastructures Cloud, détection des vulnérabilités et des menaces, avec un premier contact avec les outils d'IA d'analyse des vulnérabilités Cloud.	45 h
420-CB1-SH Sécurisation d'une infrastructure réseau	Fondamentaux des réseaux (architectures, protocoles) puis sécurisation : contrôles, segmentation, configuration sécurisée des équipements. IA appliquée à la détection d'anomalies de trafic réseau.	60 h
420-CB2-SH Sécurisation des systèmes informatiques	Administration des systèmes Linux, puis durcissement des systèmes, gestion des correctifs, contrôle des accès et surveillance, incluant l'automatisation de certaines tâches grâce à l'IA.	75 h
420-CB3-SH Sécurisation d'un environnement infonuagique 2	Approfondissement de la sécurité Cloud et intégration à la stratégie de sécurité de l'organisation, avec usage de l'IA pour l'analyse prédictive des risques.	45 h
420-CC1-SH Surveillance proactive en cyber sécurité	Configuration des technologies de surveillance et mise en pratique des processus de détection et d'investigation des événements de sécurité, avec intégration de l'IA pour l'analyse des logs et la détection des cyberattaques au sein d'un SOC.	60 h
420-CC2-SH Techniques de sécurité offensive	Notions et pratiques de sécurité offensive, pour renforcer la compréhension globale des enjeux de sécurité, incluant l'usage responsable de l'IA générative pour assister les tests d'intrusion.	75 h
420-CC3-SH Techniques de réponse aux incidents de sécurité	Exécution des tâches critiques de réponse aux incidents, avec l'appui de l'IA pour l'analyse des incidents de sécurité. Cours de fin de formation, préparant aux certifications internationales.	75 h
TOTAL DU PROGRAMME	9 cours — du socle cybersécurité à la spécialisation Cloud, réseaux, systèmes et réponse aux incidents, intégrant l'usage de l'intelligence artificielle à chaque étape	540 h

05 — UNE PÉDAGOGIE ORIENTÉE PRATIQUE

Des cours concrets, ancrés dans le milieu professionnel

Le programme est conçu pour vous rendre opérationnel : chaque cours combine apports théoriques et mise en pratique, dans une progression cohérente qui va des fondamentaux vers la spécialisation, en intégrant progressivement l'usage d'outils d'intelligence artificielle propres à chaque domaine de la cybersécurité.

- Une **admission par test pratique et théorique**, garantissant un niveau homogène au sein des groupes.
- Un parcours structuré en **trois paliers** : fondamentaux de la cybersécurité, sécurisation des systèmes/réseaux/Cloud, puis surveillance et réponse aux incidents.
- Des cours **concrets et ancrés dans le milieu de travail**, en phase avec les besoins réels des entreprises.
- Un **programme actualisé**, conçu pour répondre aux exigences actuelles du marché de la cybersécurité.

06 — CERTIFICATIONS ET PARCOURS PROFESSIONNELS

Un Diplôme international qui prépare à des certifications reconnues mondialement

Les cours du programme comportent des préparations à des certifications internationales, reconnues dans le monde.

Ce diplôme international s'appuie également sur des outils d'intelligence artificielle pour accompagner la préparation et l'entraînement aux examens :

◇ Certification PECB ISO/IEC 27001



◇ Certification Cisco CCNA



◇ Certification Cisco CyberOps Associate



◇ Certification Cisco Ethical Hacking



Ces certifications viennent renforcer la valeur de votre diplôme sur le marché du travail, en complément de l'A.E.C. délivrée par le Cégep de Sherbrooke Canada

07 — Les débouchés professionnels et les métiers de ce diplôme international

Des métiers recherchés, dans un secteur en pleine expansion

Ce diplôme Canadien ouvre l'accès à des métiers techniques variés, au cœur de la protection des systèmes d'information des organisations :

Technicien(ne) en cybersécurité

Analyste en cybersécurité

Spécialiste sécurité applicative

Spécialiste sécurité Cloud

Testeur d'intrusion / Hacker éthique

Administrateur systèmes sécurisés

Formateur / Conseiller en cybersécurité

8 — LES POINTS FORTS DU DIPLOME CANADIEN

Pourquoi choisir ce diplôme ?

Diplôme public canadien ayant un code permanent attribué par le ministère de l'éducation du Québec Une AEC d'Études Collégiales délivrée par le Cégep de Sherbrooke, établissement public du Québec. Chaque apprenant admis à notre AEC reçoit un code permanent attribué par le ministère de l'Éducation du Québec. Ses résultats sont consignés dans un bulletin d'études collégiales officiel. Après la réussite de l'ensemble des compétences prévues, l'étudiant obtient son diplôme conformément au système collégial québécois. Voir site du ministère de l'enseignement supérieur Québécois ; Comportant le cegep de Sherbrooke www....Liste des cégeps et collèges privés du Québec Gouvernement du Québec	Programme actualisé tenant compte de l'IA Un contenu conçu pour répondre aux besoins actuels des entreprises en matière de cybersécurité, intégrant l'usage des outils d'intelligence artificielle dans les pratiques professionnelles.
Cours concrets Des enseignements ancrés dans le milieu de travail, pour un profil directement opérationnel.	Horaire flexible Trois formules (temps plein, temps partiel en ligne, temps partiel week-end) pour concilier travail et études.
Préparation à des certifications internationales Une préparation aux référentiels ISO/IEC 27001, Cisco CCNA, CyberOps Associate et Ethical Hacking.	Un secteur très porteur Une profession en forte demande, dans un domaine en pleine expansion partout dans le monde.

09 — INFORMATIONS PRATIQUES

Trois formules pour s'adapter à votre emploi du temps

1. Temps plein — présentiel

- Durée : **7 mois** — Début : une session chaque trimestre.
- Rythme : **5 heures par jour, du lundi au vendredi, de 8h30 à 13h30.**

2. Temps partiel en ligne (online)

- Durée : **10 mois** — Début : une session chaque trimestre.
- Rythme : **du mardi au vendredi, de 18h30 à 20h30**, entièrement à distance.

3. Temps partiel — présentiel, fin de semaine

- Durée : **10 mois** — Début : une session chaque trimestre.

- Rythme : les samedis et dimanches, de 9h00 à 13h00.

Diplôme délivré

A.E.C. du Cégep de Sherbrooke en Cyber sécurité & sécurité infonuagique (Cloud Computing) — Diplôme Professionnel International Étatique du Québec (Canada), délocalisé en Tunisie (LEA.EB).

Frais de scolarité, dates précises de session et modalités de règlement : nous consulter.

REJOIGNEZ LA PROCHAINE SESSION

Faites de la cybersécurité votre expertise

Développez des compétences recherchées sur le marché, construisez votre expertise en cybersécurité et en sécurité Cloud, et passez de la théorie à la pratique grâce à un programme concret, structuré et reconnu à l'international. Préparez-vous dès aujourd'hui aux défis de la cybersécurité de demain.

LA PROCHAINE SESSION DÉMARRE EN SEPTEMBRE 2026

Nos conseillers vous accompagnent dans le choix de votre formule, la constitution de votre dossier et la vérification des prérequis. Contactez-nous pour convenir d'un rendez-vous d'information.

Téléphone : (+216) 71 254 444 · (+216) 98 110 924

Courriel : admission@academiesherbrooke.com.tn

Adresse : 06, Rue Abou Baker Essedik, Cité Jardin – 1003 Tunis