ESG Accélérateur de croissance

Certification

CYBERSÉCURITÉ

Alors que la crise sanitaire de la COVID-19 aura contribué à l'accélération du développement numérique des organisations, celles-ci demeurent plus que jamais vulnérables au risque d'une attaque informatique.

Que l'on parle de tentatives d'hameçonnage, de logiciels rançons ou de fuites de données, le risque n'a jamais été aussi présent. Il représente tout un défi pour les gestionnaires qui doivent prendre des décisions avec une compréhension souvent partielle des enjeux relatifs à la cybersécurité.

En tant que dirigeant.e d'entreprise ou gestionnaire, apprenez à identifier les failles de vos réseaux informatiques grâce à une meilleure maitrise des outils et méthodes utilisées pour sécuriser votre organisation.

Nos certifications sont reconnues par le programme Scale AI qui permet d'obtenir un rabais de 50% sur le tarif régulier.

FORMATION ACCRÉDITÉE — AI — SUBVENTIONNÉE PAR SCALE AI

En partenariat avec Québec

OBJECTIFS

- Comprendre les risques techniques et humains associés aux services informatiques afin de mieux les appréhender.
- Développer les réflexes nécessaires pour minimiser les probabilités de cyberattaques.
- Former le personnel aux bonnes pratiques.

39 heures
À distance

3000 $ tarif régulier
1500 $ tarif Scale AI

Formation certifiante *

* *Pour être éligibles à l'obtention de leur attestation de certification, les participant.e.s doivent : (1) Suivre les modules obligatoires du programme ; (2) Compléter avec succès les différents tests de validation des connaissances*

PROGRAMME

OBLIGATOIRE OPTIONNEL

MODULE 1

Gouvernance de la cybersécurité

Avant de sélectionner les outils nécessaires à sa protection, une entreprise doit déterminer et mettre en place une politique de sécurité adaptée à son activité et aux risques auxquels elle s'expose. Ce module présente les différents enjeux à considérer afin que la politique de sécurité de votre entreprise soit appuyée par des règles de gouvernance pertinente et évaluée des par des audits périodiques.

MODULE 2

La protection des réseaux informatiques

Les logiciels rançons, appelés aussi ransomware, sont une nouvelle forme d'extorsion qui fait la une de l'actualité mondiale de ces derniers mois. Ce module s'intéresse aux méthodes pour se protéger contre tout type d'attaque informatique en soumettant les participants à des simulations d'attaques inspirées de cas réels.

MODULE 3

Données personnelles : leur importance et leur sécurisation

Les données personnelles sont des informations à la fois précieuses et extrêmement sensibles. Des nos jours, elles peuvent permettre à une entreprise d'accroître ses revenus si celles-ci sont collectées et utilisées dans le respect des lois. Cependant, une utilisation hasardeuse ou frauduleuse peut avoir des conséquences graves sur les entreprises.

MODULE 4

Apprendre des cyberattaques et des systèmes de fraude : une analyse de cas

Malgré les moyens toujours plus importants mis dans la protection des réseaux informatiques, le nombre de cyberattaques et de vols de données et d'identités augmente fortement. Ce module analyse les erreurs commises par les entreprises sur le plan technique, mais surtout sur le plan humain.

MODULE 5

Sécurité des objets connectés

Facilitant l'exécution du travail et la collecte des données, les objets connectés prennent de plus en plus de place en entreprise mais peuvent présenter un risque pour la sécurité en cas de mauvaise utilisation. Ce module vous présentera les bases de la technologie des objets connectés, les risques possibles et les différentes façons de s'en prémunir.

MODULE 6

Télétravail et cybersécurité

Sur la frontière entre vie privée et vis professionnelle, le télétravail soulève des problématiques majeures en matière de sécurité. Ce module permettra d'étudier les bonnes pratiques à respecter pour permettre aux participants de mettre en place un télétravail sécuritaire avec leurs équipes.

MODULE 7

La protection des données confidentielles

Les entreprises se tournent vers les technologies infonuagiques pour organiser et stocker leurs informations tout en les transmettant volontairement à des entreprises tierces sans connaître les conséquences que cela peut entraîner sur les secrets de l'entreprise. Ce module vous informera sur les risques liés à l'utilisation de certaines outils, de même que les alternatives à considérer.

MODULE 8

Gestion des incidents

Malgré l'instauration de règles préventives en matière de protection informatique, le risque zéro n'existe pas. De ce fait, les gestionnaires doivent savoir comment réagir en cas d'incidents, évaluer l'étendue de la situation et déterminer comment réagir et communiquer. Ce module fournit aux gestionnaires les bonnes pratiques à mettre en place en amont, afin de pouvoir gérer la crise le moment venu.

CONFÉRENCE

L'avenir de la cybersécurité

Introduction aux technologies futures qui amélioreront profondément notre rapport à la cybersécurité, à commencer par l'intelligence artificielle.

FORMATEURS

Jude Jacob Nsiempba

M. Nsiempba est professeur associé au département de didactique des langues, diplômé d'un baccalauréat en sciences appliquées, d'une maîtrise en informatique de gestion, d'un MBA et EMBA en gestion des technologies à l'UQAM, ainsi qu'un doctorat en génie industriel de Polytechnique Montréal. À l'UQAM, M. Nsiempba enseigne le cours de sécurité des systèmes, données et contrats.

Pour plus d'informations, veuillez contacter :
Alexandre LUIGGI
Conseiller principal, partenariats et développement des affaires
438 526-5824
luiggi.alexandre@uqam.ca

Guy Bégin
M. Bégin est professeur au département d'informatique de l'UQAM depuis trente ans, et est diplômé d'un doctorat en génie électrique de Polytechnique Montréal. M. Bégin enseigne notamment à l'UQAM le cours de sureté et sécurités des systèmes embarqués.

Benoît Gagnon
M. Gagnon est chargé de cours à l'Université de Montréal sur la cybercriminalité, le renseignement et les technologies de sécurité, ainsi que chercheur associé à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand en études stratégiques et diplomatiques.

Ancien analyste et conseiller stratégique de la Sûreté du Québec, il est diplômé d'une maîtrise en relations internationales, d'un doctorat en criminologie et d'un EMBA de l'UQAM.

Ygal Bendavid
Ygal Bendavid est professeur au département d'analytique, opérations et technologies de l'information de l'UQAM, de même que directeur du laboratoire de l'Internet des objets. M. Bendavid est diplômé d'un bac en gestion des opérations de HEC, d'une maîtrise en Management de la technologie ainsi que d'un doctorat en génie industriel de Polytechnique Montréal.

Christian Kengne
Christian Kengne est diplômé d'un Master of Engineering de l'École Polytechnique de Yaoundé, de même que d'une maîtrise de l'Université de Sherbrooke en Artificial Intelligence. Il a également obtenu de nombreux certificats en nouvelles technologies d'universités de renom tel que l'Université of Hong Kong, la Northwestern University, la Rochester Institute of Technology ou encore le MILA.

Son expertise principale comprend la gestion des menaces et des vulnérabilités, la surveillance et l'analyse de la sécurité, la sécurité du Cloud, les risques de sécurité et la conformité. Il a travaillé avec plusieurs organisations dans les services financiers, les services publics, l'industrie du transport, l'industrie des télécommunications, les entreprises d'énergie et de gaz, les laboratoires d'informatique et d'intelligence artificielle en Afrique centrale, au Canada et aux États-Unis.

Pour plus d'informations, veuillez contacter :
Alexandre LUIGGI
Conseiller principal, partenariats et développement des affaires
438 526-5824
luiggi.alexandre@uqam.ca

Dominic Jaar

Dominic Jaar est avocat, membre du Barreau du Québec et employé de KPMG, ou il occupe le poste d'associé et leader régional, Services-conseils en management. L'équipe que dirige Me Jaar répond aux besoins informationnels des professionnels responsables des affaires juridiques, de la conformité, des risques et des TI dans des sociétés ouvertes et fermées incluant l'administration de la preuve électronique, la récupération de preuves, la gestion des documents et de l'information, l'analyse de données et les cyberenquêtes. Me Jaar enseigne l'investigation informatique, la preuve électronique, la méthodologie des enquêtes et la protection des renseignements personnels dans diverses universités nord-américaines et dans le cadre de congrès internationaux.

Flare Systems

Depuis 2017, Flare Systems a développé de solides technologies axées sur l'IA qui automatisent la détection et la prévention des fraudes, en analysant le dark et le deep web, le tout pour aider les institutions financières et les compagnies à protéger leurs données sensibles.

Nareg Froundjian

Nareg Froundjian est actuellement membre du groupe Confidentialité des données et cybersécurité de Deloitte Legal Canada où il conseille des institutions canadiennes en matière de confidentialité des données, de cybersécurité et de droit des technologies. Préalablement à la pratique privée, il a dirigé des projets novateurs visant à améliorer l'accès à la justice au moyen de la technologie avec le Laboratoire de cyberjustice de l'Université de Montréal. De plus, M. Froundjian est conférencier dans de nombreux évènements entourant la cybersécurité.

Pour plus d'informations, veuillez contacter :
Alexandre LUIGGI
Conseiller principal, partenariats et développement des affaires
438 526-5824
luiggi.alexandre@uqam.ca