Certification

CYBERSÉCURITÉ POUR GESTIONNAIRES

Avec un développement numérique accéléré par la crise sanitaire, le risque d'une attaque informatique sur les organisations privées et publiques n'a jamais été aussi présent. Il n'y a pas un jour ou la presse ne fait pas mention de tentative d'hameçonnage, de logiciels rançons ou de fuites de données. Or, des méthodes s'offrent aux gestionnaires pour s'en prémunir, à commencer par la formation du personnel aux bonnes pratiques, et la compréhension des méthodes utilisées pour accéder à vos réseaux.

En partenariat avec

Québec

Clientèle

La formation s'adresse principalement aux :

- Dirigeants d'organisation, autant privée que publique,
- Responsables de départements et chefs d'équipe
- Responsables des ressources humaines

La formation s'adresse également aux membres d'ordres professionnels opérant dans le monde des affaires.

Compétences développées

La formation se présente comme une formation pratique, permettant aux dirigeants d'entreprise et de département de comprendre les risques associés aux services informatiques (techniques et humains), et recevoir les outils nécessaires pour minimiser les probabilités de cyberattaques, de même que de former le personnel aux bonnes pratiques.

Certification

Vous devez suivre les 6 modules obligatoires. Vos connaissances seront évaluées à la fin de chaque module. La réussite de l'ensemble des modules vous permettra d'obtenir une certification.

21 heures
À distance

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

Pour plus d'informations, veuillez contacter :
ESG+
esgplus@uqam.ca

Contenu

OBLIGATOIRE **OPTIONNEL**

MODULE 1

Gouvernance de la cybersécurité (6 heures)

Avant même de sélectionner les outils nécessaires à la protection de l'entreprise, il faut que celle-ci détermine, et mette en place, une politique de sécurité adaptée à l'activité et aux risques qu'elle encoure. Cette politique doit être appuyée par des règles de gouvernance pertinente, et évaluée par des audits réguliers.

MODULE 2

Ransomware, hameçonnage, cheval de Troie...: Comment assurer la protection des réseaux informatiques (3 heures)

Les ransomware (logiciels rançons) font depuis plusieurs mois la une de l'actualité mondiale, et les répercussions de cette nouvelle forme d'extorsion se calculent en centaine de milliers de dollars, si ce n'est en million (STM, hôpitaux, etc.). Ils ne sont cependant pas les seules menaces qui pèsent sur nos réseaux informatiques. Ici, nous analyseront les méthodes pour se protéger.

Ici, nous analyseront les méthodes pour se protéger via le développement de simulations d'attaques typiques auxquelles les participants seront soumis, afin de les sensibiliser concrètement aux risques et de les amener à une réflexion approfondie sur leur degré d'exposition. Inspirés de cas véritables, ces simulations d'attaque permettront d'illustrer en détail les mécanismes typiquement mis en place par les pirates pour se livrer à leurs méfaits, et serviront de point d'ancrage aux explications sur les mesures de protection qui viendront compléter la formation.

MODULE 3

Apprendre des cyberattaques et des systèmes de fraude : Une analyse de cas (3 heures)

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.

Ici, nous allons analyser les erreurs commises par les entreprises, sur le plan technique, mais surtout sur le plan humain, de même que nous analyserons le fonctionnement des organisations criminelles qui opèrent ces attaques.

MODULE 4

Objets connectés: Comment concevoir de manière sécurisée ? (3 heures)

Téléphone, montre, radio réveil, réfrigérateurs, voiture... de plus en plus de nous outils du quotidien sont désormais connectés. En revanche, il est régulièrement démontré que ceux-ci ne sont pas protégés contre des attaques pouvant avoir des répercussions désastreuses. Ici, nous comprendrons quelles sont les méthodes permettant de concevoir et développer les nouveaux outils du numérique de manière sécurisée.

Pour plus d'informations, veuillez contacter :
ESG+
esgplus@uqam.ca

MODULE 5

Télétravail et cybersécurité (3 heures)

Avec la pandémie, la révolution du télétravail est en marche et est là pour durer. Comment passer du travail au personnel, sur un même ordinateur en gardant la même sécurité ? Comment s'assurer à distance de conserver la même protection qu'en entreprise ? Quels sont les outils de travail coopératif sécuritaires et respectueux de vos données personnelles ? Nous y répondrons.

MODULE 6

Fuite de donnée: Responsabilités et gestion de crise (3 heures)

Que se passe-t-il en cas de fuite de données ? Comment doit-on régir ? Ce module a pour objectif d'explorer cette situation et d'offrir aux gestionnaires les outils de gestion de crise nécessaire pour traverser cette situation complexe et délicate.

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.

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.

Pour plus d'informations, veuillez contacter :
ESG+
esgplus@uqam.ca

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.

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 :
ESG+
esgplus@uqam.ca