TECHNO COMPÉTENCES

SYLLABUS

Formation « premier répondant » TI en cybersécurité

Introduction :

Le concept de « premier répondant » est déjà bien répandu au Québec, notamment grâce à la conscientisation croissante liée aux risques en milieu de travail ainsi que la valorisation des notions de santé et de sécurité. C'est dans cet esprit que la loi impose aux entreprises de former en secourisme une partie de ses employé·es, afin d'assurer une prise en charge en cas d'incident au travail et assister le personnel soignant. De même, lors de l'élaboration d'un plan de sécurité incendie, une entreprise doit désigner un ou plusieurs responsables en prévention d'une éventuelle évacuation.

En ce qui concerne la cybersécurité, il n'existe pour l'instant rien de semblable malgré le risque croissant que ces nouvelles menaces font peser sur tous les secteurs de l'économie québécoise et canadienne.

Afin de limiter le niveau de risque sur les entreprises et de limiter les conséquences néfastes du manque de main-d'œuvre en cybersécurité, TECHNOCompétences et Cybereco s'associent pour vous proposer la **formation « premier répondant » TI en cybersécurité**, offerte en ligne.

Elle permettra à une entreprise, un bureau ou une équipe de **se doter d'une personne-référente pouvant prendre en charge et solutionner des problématiques de base en cybersécurité.**

S'agissant d'un projet pilote, **les participant·es de la première cohorte bénéficieront de la formation gratuitement**, à condition de remplir le formulaire de pré-inscription et être l'un des **12 participant·es sélectionné·es.**

Présentation du responsable du cours :

Pierre-Martin Tardif est le formateur en charge de la formation.

Titulaire d'un MBA (UQAM) et d'un Ph.D en génie électrique (Université Laval), Pierre-Martin Tardif est Professeur à l'École de gestion de l'Université de Sherbrooke.

Au niveau de la sécurité de l'information, il s'intéresse à la gouvernance, à la gestion des risques, à la gestion de l'identité numérique, à la détection d'intrusion par intelligence artificielle et à la résilience des infrastructures essentielles.

Certifications complémentaires :

Certified in Enterprise Governance of IT (CGEIT®), Certified Information Systems Security Professional (CISSP®), CSX® Fundamentals, Project Manager Professional (PMP®), PMI Agile Certified Practitioner (PMI-ACP®), PMI Digital Agile Scrum Master (DASM®) et Lean Six-Sigma Black Belt (LSSBB et, Professional Scrum Master (PSM®).

Modalités de la formation :

Début de la formation : 8 septembre 2021

Fin de la formation : 8 octobre 2021

Classe virtuelle : 3h tous les mercredis (de 9h à 12h)

Travail en autonomie : estimé entre 12 et 26 heures selon la rapidité d'exécution des participants.

Clientèle visée :

La formation en ligne s'adresse à tout·e employé·e spécialiste des TI, ayant été désigné·e par son entreprise pour assurer la prise en charge des premiers gestes face à une cyberattaque.

Professionnels des TI ayant au **minimum** un :

- Niveau DEC en TI – Gestion de réseaux et sécurité ;
- Niveau DEC de l'informatique ;
- Niveau DEC gestion de réseau informatique, OU ;
- Niveau DEC conception et programmation.

Préalables nécessaires

Les personnes sélectionnées devront réaliser un travail de recherche préparatoire au sein de leur organisation afin de :

- Connaître le cadre légal régissant le secteur de sa propre organisation ;

- Connaître les procédures liées à la gestion de la qualité et à la gestion des risques ;
- Connaître les concepts de base (confidentialité, intégrité, disponibilité) ;
- Connaître les principes de stockage de données et de journalisation ;
- Connaître l'environnement et les utilisateurs de l'organisation.

Les objectifs de cette formation sont les suivants :

- Comprendre les risques cyber pour son entreprise ;
- Appliquer les meilleures pratiques pour protéger son entreprise ;
- Agir en tant que « premier répondant » TI lors d'une attaque.

Programme du cours :

La formation en ligne se divise en quatre (4) blocs. Chacun de ces blocs est composé de :

- Cours synchrone (avec participation du formateur) : 3h par semaine ;
- Cours asynchrone (en autonomie hors temps de travail) : 8h à 17h par semaine ;
- Travaux pratiques sur le lieu de travail : 4h à 9h par semaine.

SÉANCE 1 : Introduction aux concepts et risques liés à la cybersécurité

- Principales définitions en cybersécurité
- La gestion des risques en sécurité de l'information en entreprise
- La gestion des risques en sécurité de l'information en entreprise

SÉANCE 2 : Les menaces et leur protection

- Les principales menaces actuelles
- Une mesure de protection efficace pour un actif informationnel

SÉANCE 3 : Les mesures de protection des PME et la gestion des incidents

- Des comportements clés face à un incident de sécurité de l'information

SÉANCE 4 : Comportement et maturité

- Les facteurs humains influençant la sécurité de l'information

Mode d'évaluation des apprentissages :

Plusieurs modes d'évaluation seront proposés afin de favoriser le transfert des apprentissages :

- **Test de positionnement** (En autonomie)

Il permettra d'évaluer en début de formation les écarts à combler par la formation.

- **Quizz** (En autonomie)

Au cours de chaque séquence de formation, des quizz d'évaluation seront réalisés à partir de la plateforme d'évaluation B12.

- **Rapport technique** (Hors temps de travail) ;
- **Rapport exécutif** (Hors temps de travail).

Ces travaux, de type rapports devront être remis dans les délais prévus (avant la fin de la formation) afin d'être évalués par le formateur.

- **Entretiens individuels** (En autonomie) À l'issue de la formation, ces entretiens d'une durée de 15 minutes, porteront sur l'atteinte ou non des objectifs de formation par le participant ou la participante. Ils donneront au formateur l'occasion de faire le point, individuellement sur les travaux réalisés et l'atteinte des objectifs de la formation.

Validation de la formation :

À l'issue de la formation, une attestation de formation « premier répondant » TI en cybersécurité sera remise aux étudiants qui auront obtenu la note de passage de 55% aux différentes évaluations.

Règles de fonctionnement de la formation :

Travail personnel :

Des travaux personnels seront demandés aux participant·es. Ils devront être réalisés en autonomie sur une plateforme, en dehors des cours et du temps de travail. Ce temps varie de 8h à 17h, sur l'ensemble de la formation, selon l'implication et la rapidité d'exécution des participants.

Les participant·es auront deux rapports de recherche (rapport d'exécution, rapport technique) à réaliser et à présenter au formateur pour validation.

Engagement :

Au démarrage de la formation, les participant·es signeront un engagement à la formation. Cet engagement concerne :

- Le temps de travail personnel accordé aux travaux ;
- La réalisation des travaux en milieu de travail ;
- Le temps accordé à la pratique en milieu de travail ;
- La participation aux cours ;
- La remise des travaux prévus dans les délais.

Absentéisme :

La présence régulière au cours est indispensable afin de créer une cohésion de groupe, des échanges, mais également de favoriser les apprentissages nécessaires à l'obtention de l'attestation de formation **« premier répondant » TI en cybersécurité.**

Matériel requis :

- Une connexion Internet avec un débit minimal de 1,4 Mbps et une capacité de téléchargement mensuelle d'au moins 100 Mo pour la durée de la formation (connexion illimitée et bon débit) ;
- Un second écran est fortement suggéré, notamment lors de l'utilisation du Cyber Range. Au minimum, un écran d'un ordinateur portable et un écran externe.