ICTC CTIC

La Cybersécurité

Le cours d'AIT numérique du CTIC sur la cybersécurité est une introduction au cadre de la National Initiative for Cybersecurity Education (NICE). Les étudiantes et les étudiants découvriront les rôles et les carrières en cybersécurité dans divers secteurs. Ils apprendront l'analyse criminalistique numérique par le biais d'une étude de cas.

Modules		Leçons	Objectifs d'apprentissage	
Module 1	**Fondements actifs de la cybersécurité**	• Renforcement de Windows (labo virtuel) • Fichiers suspects et cachés (labo virtuel) • Introduction au cadre de la main-d'œuvre en cybersécurité de la NICE	• Évaluer et configurer les paramètres de sécurité Windows de base sur une machine Windows 10 Professionnel selon les pratiques exemplaires • Détecter les risques et les menaces de sécurité de base et appliquer les stratégies de renforcement appropriées pour atténuer les risques • Présenter aux apprenantes et aux apprenants le cadre de la NICE	Discussion sur Padlet Interrogation
Module 2	**Le langage de la cybersécurité**	• Stéganographie (labo virtuel) • Encodage-décodage (labo virtuel) • Encadrer et régir	• Détecter les fichiers contenant des données cachées à l'aide de Notepad, Strings, 7-Zip et Steghide • Cacher des données dans les fichiers avec 7-zip et Steghide • Reconnaître les types courants d'encodage : Base64, hexadécimal, URL et Rot13 • Passer en revue la catégorie « Encadrer et régir »	Discussion sur Padlet Interrogation
Module 3	**Algorithmes d'enquête de la cybersécurité**	• Hachage (labo virtuel) • Analyser et enquêter	• Déterminer l'objectif d'un hachage et ses cas d'utilisation courants • Être en mesure de créer des hachages • Fournir différents types d'analyse de la cybersécurité reconnus dans le cadre de la NICE	Discussion sur Padlet Interrogation
Module 4	**Défense essentielle en matière de cybersécurité**	• Analyse de base des réseaux (labo virtuel) • Recueillir, opérer et maintenir	• Découvrir les caractéristiques fondamentales des données relatives au réseau à l'aide de Wireshark • Analyser les données relatives au réseau pour établir certains protocoles • Acquérir une compréhension de base des philosophies de gestion des systèmes	Discussion sur Padlet Interrogation
Module 5	**Méthodes de cyberattaque**	• Pare-feu (labo virtuel) • Protéger et défendre	• Créer des règles de pare-feu en fonction de l'utilisation prévue d'un serveur • Explorer les perspectives de carrière et les exigences d'emploi liées à la protection et à la défense dans le domaine de la cybersécurité	Discussion sur Padlet Interrogation
Module 6	**Méthodes stratégiques de cybersécurité**	• Défense active (labo virtuel) • Sécuriser l'approvisionnement	• Comprendre l'importance de la mise en place et de l'exploitation de systèmes informatiques et de réseaux associés sécurisés. • Comprendre les défis auxquels les professionnelles/professionnels de l'informatique sont confrontées/confrontés	Discussion sur Padlet Interrogation

Financé par le programme de stages pratiques pour étudiants (PSPE) du gouvernement du Canada

Canada