Cybersécurité
Une initiative de l'AIT numérique
Présentée par le Conseil des technologies de l'information et des communications

Bienvenue dans l'AIT numérique du CTIC - La cybersécurité

L'AIT numérique du CTIC est un programme novateur d'apprentissage intégré au travail qui aide les étudiantes et les étudiants à acquérir des connaissances et des compétences pour faire progresser leur apprentissage et acquérir une expérience de travail enrichissante.

VUE D'ENSEMBLE DU COURS

Le cours sur la cybersécurité de l'AIT numérique est un programme innovant et collaboratif visant à développer la prochaine génération de talents en matière de cybersécurité, piloté par un réseau d'entreprises et de partenaires de pointe. Ce cours offre aux étudiantes et aux étudiants ainsi qu'aux jeunes diplômées/diplômés un parcours d'apprentissage très pratique, mais stratégique, et combine :

1. Apprentissage et expérience professionnelle sur le lieu de travail offerts par les entreprises qui exploitent activement ou utilisent les capacités de la **cybersécurité**;
2. Modules interactifs de cybersécurité numériques emplifiés, dirigés par l'industrie, complétant l'apprentissage sur le lieu de travail;
3. Activation du développement de carrière et des compétences d'autoapprentissage des étudiantes et des étudiants.

Ce cours en ligne en six modules servira à initier les étudiantes et les étudiants de l'enseignement supérieur à un ensemble de sujets liés au domaine de la cybersécurité. Il mettra en contexte, l'apprentissage des étudiantes et des étudiants sur le terrain et fournira un cadre pour la poursuite de l'apprentissage et le développement de leur carrière en leur apportant un aperçu stratégique et une expérience de l'industrie.

À l'issue de ce cours, les étudiantes et les étudiants auront une bonne compréhension des différentes catégories de cybersécurité, de la terminologie clé et d'une série d'applications industrielles. Le cours ne se veut pas une vue d'ensemble complète ou inclusive de l'industrie, mais plutôt un moyen pour les apprenantes et les apprenants non seulement d'essayer de comprendre la cybersécurité à un niveau élevé, mais de les équiper pour plonger plus profondément dans leurs domaines d'intérêt spécifiques grâce à des lectures supplémentaires, des ressources en ligne et un apprentissage sur le terrain.

PUBLIC CIBLE

Ce cours est conçu pour les étudiantes et les étudiants qui souhaitent développer des compétences fondamentales dans le domaine de la cybersécurité, en tant qu'introduction de base à ce sujet. Nous encourageons les étudiantes et les étudiants qui maîtrisent déjà ce sujet à prendre un autre des cours de l'AIT numérique disponibles, qui fournissent une excellente compréhension latérale des concepts associés à ce cours. Si vous souhaitez étudier une version plus approfondie de ce sujet, veuillez contacter votre animatrice ou votre animateur de cours pour connaître les options disponibles.

VUE D'ENSEMBLE DU SUJET

Chaque module est divisé en deux sections : pratique active et ressources industrielles. La section pratique active est hébergée par le leader du secteur, Field Effect, sur la plateforme Cyber Range. La section des ressources industrielles est conçue selon le cadre de la main-d'œuvre en cybersécurité de la NICE (National Initiative for Cybersecurity Education) de l'organisme canadien CyberNB. Le choix de ce cadre revient au premier avant étudiantes et aux étudiants de partager cette référence commune avec d'autres organismes du secteur public, du secteur privé et du monde universitaire lorsqu'il s'agit de comprendre les rôles et les responsabilités dans les carrières liées à la cybersécurité.

FORMAT DU COURS

Nous vous présenterons plusieurs types d'activités d'apprentissage tout au long du cours. Vous trouverez ci-dessous une liste de ces activités ainsi qu'une brève description de ce qu'elles impliquent et de ce que l'on attend de vous :

Module	Leçon	Description	Détails
1	**Fondements actifs de la cybersécurité**	• Renforcement de Windows • Fichiers suspects et cachés • Introduction au cadre de la main-d'œuvre en cybersécurité de la NICE	Difficulté : intermédiaire Âge : 18 ans et plus
2	**Le langage de la cybersécurité**	• Stéganographie • Encodage-décodage • Encodeur et régler	Durée : deux heures par module, dix heures par étude de cas
3	**Algorithmes d'enquête de la cybersécurité**	• Hachage • Analyser et enquêter	Détails de l'étude de cas : Les étudiantes et les étudiants passeront en revue les outils de cybercriminalistique et constitueront un dossier d'information sur l'empreinte numérique du personnage présenté (Matt). En privé, les étudiantes et les étudiants doivent appliquer les mêmes outils à leur propre empreinte numérique et réaliser une activité de réflexion sur la façon d'améliorer cette empreinte en vue d'un emploi futur.
4	**Défense essentielle en matière de cybersécurité**	• Analyse de base des réseaux • Recueillir, opérer et maintenir	
5	**Méthodes de cyberattaque**	• Pare-feu • Protéger et défendre	
6	**Méthodes stratégiques de cybersécurité**	• Défense active • Sécuriser l'approvisionnement	
Étude de cas	**Googlez-vous – Cybercriminalistique**	• Travail en petits groupes avec des présentations examinées par des juntes/jurés du secteur	

Cybersécurité
Une initiative de l'AIT numérique
Présentée par le Conseil des technologies de l'information et des communications

1.1 Renforcement de Windows

Aperçu de la section

Dans cette section, les étudiantes et les étudiants apprendront à mieux protéger un système informatique Windows contre les menaces et les vulnérabilités de base en identifiant les risques de sécurité et en appliquant des techniques courantes de renforcement pour atténuer ladite menace.

Cette section est conçue comme une expérience d'apprentissage pratique destinée aux étudiantes et aux étudiants qui s'intéressent à la cybersécurité. Elles et ils doivent avoir une connaissance pratique de base d'un ordinateur Windows pour pouvoir compléter cette section.

Attentes en matière de charge de travail

L'étudiante ou l'étudiant devrait être capable de réaliser le laboratoire 1 de la section en 30 à 45 minutes. Cependant, le temps réel investi dépendra des connaissances préalables et du temps passé à étudier les ressources suggérées et à effectuer les tâches facultatives. Le laboratoire 2 est facultatif.

Résultats d'apprentissage et objectifs

À l'issue de cette section, les étudiantes et les étudiants seront capables de :

- Évaluer et configurer les paramètres de sécurité Windows de base sur une machine Windows 10 Professionnel selon les pratiques exemplaires.
- Connexion automatique (désactivée) et paramètres de l'économiseur d'écran (définition du mot de passe de l'économiseur d'écran).
- Paramètres de sécurité de la politique des comptes (paramètres de la politique des mots de passe et de la politique de verrouillage des comptes) en fonction des ressources et/ou des exigences du scénario.
- Windows Update (mise à jour automatique).
- Paramètres du pare-feu Windows Defender (par défaut).
- Détection des virus et des menaces (par défaut).
- Accès à distance (désactivé).
- Évaluer et configurer les comptes et les privilèges d'utilisateurs et d'utilisateurs appropriés sur un ordinateur Windows 10.
  - Configurer les comptes d'utilisateurs, d'utilisateurs et d'invités/d'invités avec des droits d'utilisation appropriés afin de réduire les risques de cybersécurité.
  - Désactiver ou renommer les comptes d'utilisateurs, d'utilisateurs, d'invités/invités ainsi que d'administrateurs ou d'administrateurs pour réduire les risques de cybersécurité.
- Détecter les risques et les menaces de sécurité de base et appliquer les stratégies de renforcement appropriées pour atténuer les risques.

Format de la section

Les étudiantes et les étudiants se verront présenter deux scénarios dans lesquels elles et ils devront mieux sécuriser un ordinateur Windows 10 sur la base des informations données dans le scénario. Chaque scénario est présenté dans un laboratoire qui contient une machine virtuelle (VM) Windows 10. Cette VM n'a pas d'accès à Internet.

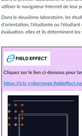
Dans le premier laboratoire, le scénario guidera les étudiantes et les étudiants à travers les étapes de base du renforcement de Windows 10 en leur faisant effectuer plusieurs tâches. Des ressources sont fournies. Si la ressource est un lien, les étudiantes et les étudiants doivent utiliser le navigateur Internet de leur propre système pour y accéder.

Dans le deuxième laboratoire, les étudiantes et les étudiants sont confrontés/confrontés à un nouveau scénario et à la VM qui l'accompagne. Les défis à relever dans ce laboratoire seront les mêmes que ceux du premier laboratoire. Cependant, la grande différence est qu'il n'y a pas d'orientation; l'étudiante ou l'étudiant doit se fier aux connaissances et aux compétences nouvellement acquises ainsi qu'à ses capacités de recherche pour relever le défi. Les étudiantes et les étudiants doivent lire le scénario et évaluer les risques de sécurité. Sur la base de leur évaluation, elles et ils déterminent les stratégies à appliquer pour atténuer ces risques de sécurité.

FIELD EFFECT

Cliquez sur le lien ci-dessous pour lancer le module et entrez votre nom d'utilisatrice ou d'utilisateur et votre mot de passe dans la page de connexion :

https://ctc-cyberrange.fieldeffect.net/CyberRace/login



Renforcement de la sécurité de Windows

Apprendre à mieux protéger un système Windows contre les menaces et vulnérabilités de base en identifiant les risques et en effectuant des techniques standardisées de renforcement de sécurité.

Cybersécurité
Une initiative de l'AIT numérique
Présentée par le Conseil des technologies de l'information et des communications

2.3 Cadre de la NICE - Superviser et gouverner

Aperçu de la section

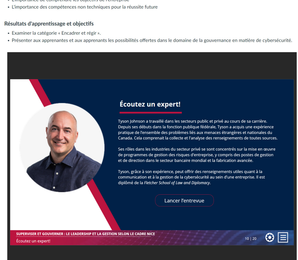
Cette section donnera à l'apprenante et à l'apprenant une bonne compréhension des rôles de direction dans la cybersécurité et des compétences clés qui sont les plus importantes dans ce type de poste.

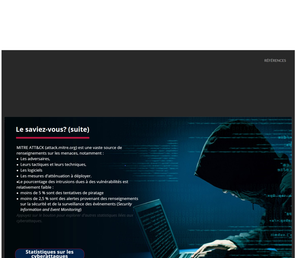
Thèmes clés

- L'importance de l'engagement des parties prenantes pour superviser, gérer et conseiller
- L'importance de comprendre les objectifs de l'entreprise
- L'importance des compétences non techniques pour la réussite future

Résultats d'apprentissage et objectifs

- Examiner la catégorie « Encadrer et régir ».
- Présenter aux apprenantes et aux apprenants les possibilités offertes dans le domaine de la gouvernance en matière de cybersécurité.





Cybersécurité
Une initiative de l'AIT numérique
Présentée par le Conseil des technologies de l'information et des communications

3.2 Cadre de la NICE - Analyser et enquêter

Aperçu de la section

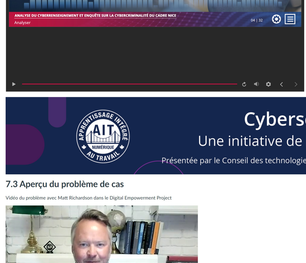
Cette section donnera l'apprenante et à l'apprenant une bonne compréhension des rôles qui effectuent un examen et une évaluation hautement spécialisés des informations cybernétiques entrantes afin de déterminer leur utilité pour le renseignement. L'apprenante ou l'apprenant apprendra également les principales compétences non techniques dont elle ou il a besoin lorsqu'elle ou qu'il enquête sur des cybercrimes.

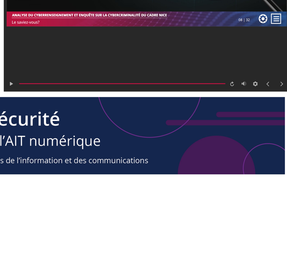
Thèmes clés

- Analyse du cyberrenseignement
- Disciplines d'enquête sur la cybercriminalité
- Conditions d'emploi
- Perspectives de carrière associées

Résultats d'apprentissage et objectifs

- Fournir aux apprenantes et aux apprenants les différents types d'analyse de la cybersécurité qui sont reconnus dans le cadre de la NICE.
- Fournir des cas d'utilisation et des parcours d'emploi liés aux cybercrimes et à leur prévention.

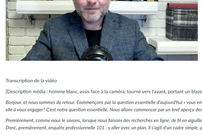




Cybersécurité
Une initiative de l'AIT numérique
Présentée par le Conseil des technologies de l'information et des communications

7.3 Aperçu du problème de cas

Vidéo du problème avec Matt Richardson dans le Digital Empowerment Project



Transcription de la vidéo

[Description média : homme blanc, assis face à la caméra, tourné vers l'avant, portant un blazer gris et une chemise noire. Derrière lui, des étagères blanches avec des livres.]

Bonjour, et nous sommes de retour. Commençons par la question essentielle d'aujourd'hui « vous embauchez-vous? ». Sur la base de ce que vous trouvez en ligne sur vous-même, votre comportement, votre attitude, vos compétences et qualifications. Votre empreinte ou votre image vous incitent-elle à vous engager? C'est notre question essentielle. Nous allons commencer par un bref aperçu des étapes à suivre.

Premièrement, comme nous le savons, lorsque nous faisons des recherches en ligne, de fil en aiguille, c'est très facile de s'écarter du chemin et de se retrouver dans des domaines sans rapport et de se perdre dans le vacarme qu'est Internet. Il y a beaucoup de données et beaucoup d'informations. Donc, premièrement, enquête professionnelle 101 : y aller avec un plan. Il s'agit d'un cadre simple, qui est pas besoin d'être compliqué. Commencez par collecter quelques informations de surface de haut niveau sur le sujet.

L'activité d'aujourd'hui : vous allez commencer par me chercher. Vous allez me rapiner en ligne. Vous allez faire une vérification de mes antécédentsbénévoles. Nous nous servons de moi comme exemple parce que je suis un cas facile. Il y a pas mal de choses sur moi et j'ai fait beaucoup de choses différentes. Il n'y a donc pas de pénurie d'informations sur moi, ma carrière et ma vie en ligne.

Nous allons commencer le cadre de haut niveau, prendre quelques mots-clés, un style et du pupiter, les jeter dans un document texte. Des trucs qui incluent mon nom, Matt Richardson. Où je vis, où je travaille. Donc, je vais canna pour être dans la région de Belleville et Trenton, en Ontario. Aussi, quels types d'expérience j'ai, ce pour quoi je suis canna, une recherche rapide sur moi. Faire des choses clés que vous trouveriez est la sécurité sur Internet. Donc ma liste de mots clés, je pourrais commencer par quelque chose comme Matt ou dévoué. Matt Richardson, Belleville et la sécurité sur Internet. Une fois que j'ai mes mots clés, j'assemble quelques chaînes de recherche. Pour ceux qui ne sont pas familiers, nous allons utiliser des opérateurs de recherche booléens et créer des chaînes de recherche stratégiques qui excluront les résultats non pertinents et limiteront même le nombre de doublons. Le mot d'ordre ici est « exclure ». Vous voulez voir ce qu'il y a sur moi, mais vous ne voulez pas voir soit millions de résultats sur tous les Matt Richardson du monde.

Nous allons examiner certaines des principales plateformes sur lesquelles les gens vont vous chercher. Facebook, Instagram, Twitter, LinkedIn sont des plateformes très importantes. De toute évidence, Google. Bing et les résultats des moteurs de recherche vont être utiles dans leur prise de décision. Nous allons donc examiner les principales plateformes que les professionnels/professionnelles des RH vont utiliser pour nous rechercher en ligne afin de décider si nous sommes un bon candidat ou une bonne candidate pour leur organisation. Et aussi, vous savez, qu'est-ce que vous voulez rechercher. Certaines choses que vous ne voulez pas voir, c'est tout ce qui monte en mauvais jugement, le fils, tout ce qui est humiliant ou très important, méchant ou irrespectueux. C'est le moyen numéro un de torpiller vos chances. Les compétences, dans une certaine mesure, peuvent être enseignées. La compétence vient avec l'expérience, que ne vient qu'avec le temps. Mais le caractère ne s'apprend pas à facilement. Les personnes qui sont gentilles et respectueuses, qui font preuve de leadership, qui reconnaissent les autres, qui se montrent sous leur meilleur jour en ligne, vont se distinguer de manière positive.

Maintenant que nous disposons d'un cadre et d'un plan d'action avant d'entrer en ligne, nous allons vous présenter des techniques de recherche intermédiaires et avancées, directement issues du manuel d'instructions pour le renseignement de sources ouvertes ou OSINT. Nous allons également vous présenter de nouveaux outils gratuits qui ne nécessitent même pas de compte. Leur interface est simple, mais ils sont puissants. Nous allons également - vous allez commencer avec moi - travailler individuellement ou en groupe pour faire une vérification des antécédentsbénévoles de Matt Richardson Belleville, la sécurité sur Internet, comme discuté, et on peut vous demander de faire une présentation ou un compte rendu de ces conclusions. On vous demandera ensuite de retourner la lentille sur vous-même, de remplacer mon nom par le vôtre, de remplacer Belleville par votre ville ou village. Remplacez la sécurité sur Internet par un sujet pour lequel vous pourriez être connu. Comme entraîneur de hockey mineur, gagner une compétition académique ou une bourse d'études. Vous allez commencer à enlever les mains et à placer les vôtres. Et, très important, de réfléchir au peu. Des questions que vous pourriez vous poser - est-ce que je m'intimide? Suis-je une personne sympathique? Est-ce que je montre que j'ai des qualifications et des compétences, votre une curiosité intellectuelle? En tant qu'éducateur ou étudiante, est-ce que je fais des articles sur l'industrie, est-ce que je fais des commentaires sur ce que j'ai appris? Est-ce que je me montre sous un jour positif? Ou vous demandera donc de réfléchir sur moi, mais aussi sur vous-même.

Et surtout, nous avons tous fait des erreurs. Que faire si vous devez nettoyer ou corriger votre profil, votre empreinte, votre image en ligne? La bonne nouvelle est que ça se fait. Et entre, si vous êtes avec pas vraiment, n'êtes pas les seuls/seules. C'est toujours bien à savoir, car cela vous indique que vous l'accusion de commencer à construire une image en ligne positive et de faire sortir les plateformes qui seront consultées lorsque les gens décideront de votre avenir.

Financé par le gouvernement du Canada | Canada

Centre d'expertise national à but non lucratif pour l'économie numérique, nous sommes la source de confiance pour les conseils stratégiques fondés sur des données probantes, de recherches prospectives et de programmes de renforcement des capacités créatives.