Cybersecurity Essentials 1.0
Cadre et déroulement du cours

Dernière mise à jour 29 mars 2017

Profil des participants

Le cours *Cybersecurity Essentials 1.0* est conçu pour les élèves souhaitant poursuivre des études plus approfondies dans le domaine de la cybersécurité. Ce cours préparatoire apporte une vue d'ensemble du domaine de la cybersécurité. Le programme présente les caractéristiques des cybercriminels et les tactiques qu'ils utilisent. Il aborde ensuite les technologies, les produits et les procédures utilisés par les professionnels de la cybersécurité pour lutter contre la cybercriminalité. Il s'adresse à des étudiants issus de divers niveaux de formation et types d'établissement, notamment de lycées, de collèges, d'universités, de grandes écoles, d'établissements d'enseignement technologique et professionnel, ou d'autres organismes de formation.

Prérequis

Pour acquérir les compétences appropriées, les élèves doivent être familiarisés avec le contenu et les compétences décrits dans le cours prérequis :

- Introduction à la cybersécurité 2.0

Certifications visées

Il n'y a aucune certification visée pour ce cours.

Description du cursus

Le cours comporte de nombreuses fonctionnalités pour aider les élèves à comprendre ces concepts :

- Les contenus multimédias riches, notamment des activités interactives, des vidéos, des jeux et des questionnaires, proposent des méthodes d'apprentissage variées pour favoriser l'assimilation des connaissances.
- Les travaux pratiques et les exercices de simulation dans Packet Tracer aident les élèves à développer un esprit critique et à acquérir de solides aptitudes en matière de dépannage.
- Les évaluations innovantes permettent de recevoir instantanément le feedback de l'instructeur et de mieux évaluer le niveau de connaissances et de compétences atteint.
- Les concepts techniques sont expliqués de façon à ce que les élèves de tous les niveaux puissent les comprendre. Par ailleurs, les activités interactives s'insèrent dans les cours magistraux et favorisent l'assimilation des connaissances.
- Le programme encourage les élèves à envisager une formation supplémentaire en informatique, mais favorise également les compétences mises en œuvre et l'expérience pratique.

Les exercices Cisco Packet Tracer sont conçus pour Packet Tracer 6.3 ou ultérieur.

Objectifs du cursus

Cybersecurity Essentials 1.0 présente les connaissances de base et les compétences essentielles associées aux domaines de la sécurité du monde virtuel : sécurité des informations, sécurité des systèmes, sécurité du réseau, sécurité mobile, sécurité physique, éthique et lois, technologies associées, techniques de protection et de réduction utilisées dans les entreprises.

À l'issue du cours *Cybersecurity Essentials 1.0*, les élèves seront en mesure d'effectuer les tâches suivantes :

- Décrire les caractéristiques des criminels et des héros dans le domaine de la cybersécurité.
- Décrire comment les principes de confidentialité, d'intégrité et de disponibilité sont liés aux états des données et aux contre-mesures prises en matière de cybersécurité.
- Décrire les tactiques, les techniques et les procédures utilisées par les cybercriminels.
- Décrire comment les technologies, les produits et les procédures sont utilisés pour protéger la confidentialité.
- Décrire comment les technologies, les produits et les procédures sont utilisés pour garantir l'intégrité des données.
- Décrire comment les technologies, les produits et les procédures garantissent la haute disponibilité.
- Expliquer comment les professionnels de la cybersécurité utilisent les technologies, les processus et les procédures pour protéger tous les composants du réseau.
- Expliquer l'objectif des lois liées à la cybersécurité.

Équipements et installation recommandés

Pour offrir les meilleures conditions d'apprentissage, nous recommandons 12 à 15 étudiants par classe et un ordinateur par personne. Tout au plus, deux étudiants peuvent utiliser le même ordinateur dans le cadre des travaux pratiques. Certains exercices nécessitent que les ordinateurs soient connectés au réseau local.

Configuration matérielle requise pour les ordinateurs utilisés lors des TP

- Un ordinateur avec un minimum de 2 Go de mémoire vive et 8 Go d'espace disque disponible
- Un accès Internet haut débit pour télécharger Oracle VirtualBox et le fichier image de la machine virtuelle

Présentation du programme

Avec le cours *Cybersecurity Essentials 1.0*, les élèves peuvent :

- Connaître les acteurs du monde de la cybersécurité et la motivation des cybercriminels et des spécialistes de la cybersécurité.
- Apprendre à identifier les attaques de sécurité, les symptômes, les processus et les mesures mises en place.
- Acquérir des connaissances fondamentales dans divers domaines de la sécurité.
- Acquérir des compétences dans les technologies de gestion de la sécurité, de contrôle, de protection et de réduction des risques.
- Connaître les lois et l'éthique en matière de sécurité, et apprendre à développer des politiques de sécurité.
- Apprendre les rôles des différents professionnels de la cybersécurité et les options de carrière.

Description de la formation

Tableau 1. Description de la formation Cybersecurity Essentials 1.0

Chapitre/Section	Objectifs
Chapitre 1. Cybersécurité : un monde de magiciens, de criminels et de héros	**Décrire les caractéristiques des criminels et des héros dans le domaine de la cybersécurité.**
1.1 Le monde de la cybersécurité	Décrire les caractéristiques communes de l'univers de la cybersécurité
1.2 Cybercriminels contre cyberhéros	Faire la différence entre les cybercriminels et les héros
1.3 Les menaces envers le royaume	Comparer la manière dont les menaces de cybersécurité affectent les individus et les entreprises.
1.4 Les forces obscures de la cybersécurité	Décrire les facteurs qui favorisent l'expansion et la croissance de la cybercriminalité.
1.5 Augmenter le nombre de héros	Décrire le comportement des entreprises et les efforts consentis pour augmenter les effectifs dédiés à la cybersécurité
Chapitre 2. Le cube magique de la cybersécurité	**Décrire comment les principes de confidentialité, d'intégrité et de disponibilité sont liés aux états des données et aux contre-mesures prises en matière de cybersécurité.**
2.1 Le cube magique de la cybersécurité	Décrire les trois dimensions du cube de McCumber.
2.2 La triade CID	Décrire les principes de confidentialité, d'intégrité et de disponibilité.
2.3 Les états des données	Expliquer la différence entre les trois états possibles pour des données.
2.4 Les mesures de cybersécurité	Comparer les différents types de contre-mesures en matière de cybersécurité.
2.5 Le cadre de gestion de la sécurité IT	Décrire le modèle de cybersécurité ISO.
Chapitre 3. Menaces pour la cybersécurité, vulnérabilités et attaques	**Décrire les tactiques, les techniques et les procédures utilisées par les cybercriminels.**
3.1 Malwares et codes malveillants	Différencier les types de malwares et de codes malveillants.
3.2 La supercherie	Comparer les différentes méthodes utilisées dans le cadre de l'ingénierie sociale.
3.3 Les attaques	Comparer les différents types de cyberattaques.
Chapitre 4. L'art de protéger les secrets	**Décrire comment les technologies, les produits et les procédures sont utilisés pour protéger la confidentialité.**
4.1 La cryptographie	Expliquer comment les techniques de chiffrement protègent la confidentialité.
4.2 Les contrôles d'accès	Décrire comment les techniques de contrôle d'accès protègent la confidentialité.
4.3 La dissimulation des données	Décrire le concept de dissimulation des données.

Chapitre 5. L'art de garantir l'intégrité	**Décrire comment les technologies, les produits et les procédures sont utilisés pour garantir l'intégrité des données.**
5.1 Les types de contrôles de l'intégrité des données	Expliquer les processus utilisés pour garantir l'intégrité des données.
5.2 Les signatures numériques	Expliquer l'objectif des signatures numériques.
5.3 Les certificats	Expliquer l'objectif des certificats numériques.
5.4 Protection de l'intégrité des bases de données	Expliquer la nécessité d'assurer l'intégrité des bases de données.
Chapitre 6. Le royaume des cinq neuf	**Décrire comment les technologies, les produits et les procédures garantissent la haute disponibilité.**
6.1 La haute disponibilité	Expliquer le concept de haute disponibilité.
6.2 Les mesures pour améliorer la disponibilité	Expliquer comment les mesures relatives à la haute disponibilité permettent d'améliorer la disponibilité.
6.3 Gestion des incidents	Décrire comment un plan de gestion des incidents améliore la haute disponibilité.
6.4 Reprise après sinistre	Décrire l'importance du plan de reprise après sinistre sur l'amélioration de la haute disponibilité.
Chapitre 7. Fortification du royaume	**Expliquer comment les professionnels de la cybersécurité utilisent les technologies, les processus et les procédures pour protéger tous les composants du réseau.**
7.1 Protéger les systèmes et les appareils	Expliquer comment les processus et les procédures protègent les systèmes.
7.2 Le renforcement du serveur	Expliquer comment protéger les serveurs sur un réseau.
7.3 Le renforcement du réseau	Expliquer comment mettre en place des mesures de sécurité pour protéger des appareils réseau.
7.4 Sécurité physique et environnementale	Expliquer comment les mesures de sécurité physique sont mises en place afin de protéger l'équipement réseau.
Chapitre 8. Rejoindre l'ordre des cyberhéros	**Expliquer l'objectif des lois liées à la cybersécurité.**
8.1 Les domaines de la cybersécurité	Décrire comment les domaines de cybersécurité sont utilisés dans la triade CID.
8.2 Comprendre le serment lié à l'adhésion	Expliquer dans quelle mesure l'éthique peut vous guider.
8.3 Étape suivante	Expliquer les étapes à suivre pour devenir un professionnel de la cybersécurité.

Siège social aux États-Unis
Cisco Systems, Inc.
San José, CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : www.cisco.com/go/offices.