CCNA Cybersecurity Operations

Cybersécurité

02/08/2025

RÉSUMÉ

De nos jours, les entreprises doivent détecter rapidement les cyberattaques et réagir efficacement en cas d'incident. Les centres opérationnels de sécurité (SOC) surveillent étroitement les systèmes de sécurité et protègent les entreprises en détectant et en stoppant les cyberattaques. CCNA Cybersecurity Operations prépare les candidats à travailler avec des analystes de la cybersécurité dans les centres opérationnels de sécurité.

CENTRES DE FORMATION

Saint-Nazaire, Laval, La Roche-sur-Yon, Cholet, Angers, Le Mans, Nantes

DURÉE DE LA FORMATION

55 jours / 71.5 heures

ACCUEIL PSH

Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.

PARTENAIRE

CISCO

PUBLIC ET PRÉREQUIS

Aucun prérequis nécessaire

LES OBJECTIFS

A l'issue de la formation, les stagiaires seront capables de :

- Installer des machines virtuelles afin de créer un environnement sécurisé pour la mise en œuvre et l'analyse des incidents liés à la cybersécurité
- Expliquer le rôle de l'analyste en cybersécurité dans l'entreprise
- Expliquer les fonctionnalités et les caractéristiques du système d'exploitation Windows nécessaires pour renforcer les analyses de cybersécurité
- Expliquer les fonctionnalités et caractéristiques du système d'exploitation Linux
- Analyser le fonctionnement des protocoles et des services réseau
- Expliquer le fonctionnement de l'infrastructure de réseau
- Classer les divers types d'attaques du réseau
- Utiliser des outils de surveillance du réseau pour identifier les attaques contre les services et les protocoles réseau
- Utiliser diverses méthodes pour empêcher les accès malveillants aux données, aux hôtes et aux réseaux informatiques
- Expliquer les impacts de la cryptographie sur la surveillance de la sécurité du réseau
- Expliquer comment enquêter sur les attaques et les vulnérabilités des terminaux
- Évaluer les alertes de sécurité du réseau
- Analyser les données liées aux intrusions réseau afin d'identifier les hôtes compromis et les vulnérabilités
- Appliquer des modèles de gestion des incidents liés à la sécurité du réseau

Les + Fab'Academy

• + de 1400 Jeunes formés en apprentissage chaque année
• + de 5300 salariés accompagnés en formation continue
• + de 1720 entreprises nous font confiance (TPE, PME, groupes industriels)
• Diplômes reconnus par l'Etat

• Pédagogie innovante (par projets, en îlots, parcours individualisés...)
• Equipement en machines modernes qui préparent aux métiers de demain
• 7 implantations en Pays de la Loire avec des campus neufs et modernes
• 24000m² de plateaux techniques et performants (outils numériques, cellules robotisées...)

OUTILS PÉDAGOGIQUES

Formation en distanciel avec apports théoriques et coaching individualisé réalisé par un formateur expert.
En début de formation : présentation du parcours, du calendrier et des jalons, prise en main de la plateforme e-learning et des outils d'échanges (forum, visioconférence).

Accès aux supports pédagogiques par notre plateforme de formation e-learning et accompagnement personnalisé en visioconférence et/ou forum par un formateur expert. Réponses aux questions sur la plateforme dans les 24 heures ouvrées de 9h00 à 17h.

MODALITÉ D'ÉVALUATION

Modalités d'évaluation des formations qualifiantes : Les connaissances et/ou capacités professionnelles de l'apprenant sont évaluées en cours et/ou en fin de formation par différents moyens : mises en situation, études de cas, QCM, ..

MODALITÉS D'ACCÈS

Délais d'accès de 6 mois maximum après confirmation via le bulletin d'inscription, sous réserve d'un nombre suffisant d'inscrits et dans la limite des places disponibles et sous réserve d'étude du dossier d'admissibilité

Modalités d'accès techniques : disposer d'un ordinateur, d'une tablette, équipé d'un accès internet et privilégier le navigateur Chrome

CONTENU DE LA FORMATION

Chapitre 1. Cybersécurité et centre opérationnel de sécurité

- Expliquer le rôle de l'analyste en cybersécurité dans l'entreprise.
- 1.1 Le danger Expliquer pourquoi les réseaux et les données sont la cible d'attaques.
- 1.2 Les combattants de la guerre contre la cybercriminalité
- Expliquer comment se préparer à une carrière dans les opérations de cybersécurité.

Chapitre 2. Système d'exploitation Windows Expliquer les fonctionnalités et caractéristiques du système d'exploitation Windows nécessaires pour renforcer les analyses de cybersécurité.

- 2.1 Présentation de Windows Expliquer le fonctionnement du système d'exploitation Windows.
- 2.2 Administration de Windows Expliquer comment sécuriser les terminaux Windows.

Chapitre 3. Système d'exploitation Linux Expliquer les fonctionnalités et caractéristiques du système d'exploitation Linux.

- 3.1 Utilisation de Linux Effectuer les opérations de base dans le shell Linux.
- 3.2 Administration de Linux Effectuer des tâches d'administration Linux basiques.
- 3.3 Clients Linux Effectuer des tâches de base liées à la sécurité sur un hôte Linux.

Chapitre 4. Protocoles et services réseau Analyser le fonctionnement des services et protocoles réseau.

- 4.1 Protocoles réseau Expliquer comment les protocoles permettent d'exploiter le réseau.
- 4.2 Protocoles Ethernet et IP Expliquer comment les protocoles Ethernet et IP assurent la communication réseau.
- 4.3 Vérification de la connectivité Appliquer des utilitaires de test pour vérifier et tester la connectivité réseau.
- 4.4 Protocole de résolution d'adresse Expliquer comment le protocole de résolution d'adresse permet de communiquer sur un réseau
- 4.5 Couche de transport et services réseau Expliquer comment les protocoles de couche de transport et les services réseau prennent en charge les fonctionnalités réseau.
- 4.6 Services réseau Expliquer comment les services réseau rendent possibles les fonctionnalités réseau.

Chapitre 5. Infrastructure de réseau Expliquer le fonctionnement de l'infrastructure réseau.

- 5.1 Périphériques de communication réseau Expliquer comment les périphériques réseau assurent les communications réseau filaires et sans fil.
- 5.2 L'infrastructure de sécurité du réseau Expliquer comment les périphériques et les services renforcent la sécurité du réseau.
- 5.3 Les représentations du réseau Expliquer comment les réseaux et les topologies réseau sont représentés.

Chapitre 6. Principes de sécurité du réseau Classer les divers types d'attaques du réseau.

- 6.1 Les hackers et leurs outils Expliquer comment les réseaux sont attaqués.
- 6.2 Attaques et menaces fréquentes Expliquer les divers types de menaces et d'attaques.

Chapitre 7. Tout savoir sur les attaques réseau Utiliser des outils de surveillance réseau pour identifier les attaques contre les services et les protocoles réseau.

- 7.1 Observation du fonctionnement du réseau Expliquer la surveillance du trafic réseau.
- 7.2 Attaques ciblant les fondements du réseau Expliquer comment les vulnérabilités TCP/IP favorisent attaques réseau.
- 7.3 Attaques ciblant les activités Expliquer pourquoi les applications et les services réseaux fréquemment utilisés sont vulnérables face aux attaques.

Chapitre 8. Protection du réseau Utiliser diverses méthodes pour empêcher les accès malveillants aux données, aux hôtes et aux réseaux d'ordinateurs.

- 8.1 Comprendre les mécanismes de défense Expliquer les approches en matière de protection du réseau.
- 8.2 Le contrôle d'accès Expliquer comment le contrôle d'accès peut protéger un réseau.
- 8.3 Pare-feu du réseau et prévention des intrusions Expliquer comment les pares-feux et d'autres empêchent les intrusions réseau.
- 8.4 Filtrage du contenu Expliquer comment le filtrage de contenu empêche les données indésirables d'entrer sur le réseau.
- 8.5 Threat Intelligence Utiliser diverses sources d'informations pour localiser les menaces actuelles.

Chapitre 9. Cryptographie et infrastructure à clé publique

- Expliquer les effets de la cryptographie sur la surveillance de la sécurité du réseau.
- 9.1 Cryptographie Utiliser des outils pour chiffrer et déchiffrer des données.
- 9.2. Cryptographie à clé publique Expliquer comment l'infrastructure à clé publique (PKI) assure la sécurité du réseau.

Chapitre 10. Analyse et sécurité des terminaux Expliquer comment enquêter sur les attaques et les vulnérabilités des terminaux.

- 10.1 Protection des terminaux Utiliser un outil pour générer un rapport d'analyse des programmes malveillants.
- 10.2 Évaluation des vulnérabilités des terminaux Classer les informations sur l'évaluation des vulnérabilités des terminaux.

Chapitre 11. Surveillance de la sécurité Évaluer les alertes de sécurité du réseau.

- 11.1 Les technologies et les protocoles Expliquer l'incidence des technologies de protection sur la surveillance de la sécurité.
- 11.2 Les fichiers journaux Expliquer les types de fichiers journaux utilisés dans les activités de sécurité.

Chapitre 12. Analyse des données relatives aux intrusions

- Analyser les données liées aux intrusions réseau afin d'identifier les hôtes compromis et les vulnérabilités
- 12.1 Collecte de données Expliquer comment les données liées à la sécurité sont recueillies.
- 12.2 Préparation des données Organiser divers fichiers journaux en préparation de l'analyse des données liées aux intrusions.
- 12.3 : Analyse des données Analyser les données liées aux intrusions afin de déterminer la source des attaques.

Chapitre 13. Gestion des incidents Expliquer comment les équipes CSIRT traitent les incidents liés à la sécurité du réseau.

- 13.10 Modèles de gestion des incidents Appliquer des modèles de gestion des incidents à une intrusion.
- 13.2 Équipes CSIRT et NIST 800-61r2 Appliquer les standards NIST 800-61r2 à un incident lié à la sécurité informatique.
- 13.3 Exercices basés sur des cas pratiques À l'aide d'un ensemble de journaux, isolez un hacker et recommandez un plan de réponse aux incidents.

VALIDATION ET CERTIFICATION

Certification de compétences pro

DATE DE MISE À JOUR

29/07/2022

VERSION DOCUMENTAIRE

V2