Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Devenir défenseur de réseau certifié (C|ND)

Date et durée

Code formation : CND-V2
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

C|ND : Certified Network Defender

Description

La **formation CND v2** est un cours particulièrement poussé qui permet aux administrateurs réseau de renforcer leurs compétences techniques sur le plan de la défense des réseaux, de la détection et des réponses en cas d'attaques. De plus, elle permet d'obtenir la prestigieuse certification **Certified Network Defender** mise place par notre partenaire EC-Council.
Pendant 5 jours intensifs, vous découvrirez comment réduire les menaces informatiques et comment mieux **protéger les infrastructures réseau des entreprises**. Dès les premiers modules, vous serez initié aux bases de la défense des réseaux. Ensuite, vous aborderez les contrôles de sécurité réseau, les protocoles, la sécurité des équipements, la mise en place de **systèmes de détection d'intrusions** et de VPN sécurisés ainsi que le paramétrage des pare-feu.
Enfin, les derniers modules seront consacrés aux aspects techniques avec les signatures de trafic réseau, l'analyse des vulnérabilités, la mise en place d'une politique de sécurité réseau et d'un plan de réponse aux incidents. Après avoir suivi ce programme de formation, vous pourrez **passer l'examen officiel** et obtenir le titre de Certified Network Defender v2 (*plus d'infos dans l'onglet certification*).

Objectifs

En participant à la **formation en sécurité réseau CND v2**, vous atteindrez les objectifs suivants :

- comprendre le fonctionnement des réseaux informatiques et maîtriser les principes fondamentaux des systèmes de défense ;
- mettre en œuvre des contrôles de sécurité réseau en appliquant des protocoles strictes, en déployant des périmètres sécurisés avec des systèmes de détection d'intrusion (IPS), en créant des réseaux privés virtuels (VPN) et en configurant des pare-feu ;
- comprendre les particularités des signatures du trafic réseau, de l'analyse et du balayage des vulnérabilités ;
- maîtriser la conception d'architectures réseau sécurisées ;
- savoir protéger, détecter, répondre et prédire face à des attaques réseaux sur des infrastructure d'entreprise ;
- établir une vraie politique de défense des réseaux et de la sécurité informatique ;
- réussir l'examen 312-38 et obtenir la certification C|ND.

Oo2 est accrédité par EC-Council pour dispenser la formation CND. Ce statut garantit la prestation d'un formateur agréé, des supports de cours officiels et des examens de certifications organisés immédiatement en fin de formation.

Points forts

Une formation très avancée et complète sur la sécurité des réseaux comprenant le passage de l'examen CND v2 (312-38). Des cours théoriques et pratiques dispensés par un formateur certifié en cybersécurité.

Certification

Information général

Ce programme de formation vous permet de **passer l'examen officiel CDN disponible en ligne** sur la plateforme EC-Council ECC Exam. Les frais d'inscription sont inclus dans le prix de cette formation et vous recevrez un bon d'examen (voucher). Une fois l'examen réussi, vous obtiendrez le titre de Certified Threat Intelligence Analyst.
Le titre de CDN v2 mis au point par des spécialistes de la cybersécurité, vise notamment à fournir aux professionnels de l'informatique les moyens de **lutter contre les cyber-menaces**, de les détecter, d'y répondre et surtout de les prédire avant qu'elles ne surgissent. La certification est aussi destinée à guider les organisations dans la mise en place et le déploiement de leur propre système de défense réseau.

Détail de l'examen C|DN

Code de l'examen : 312-38
Nombres de questions : 100 QCM
Durée : 4 heures
Score de réussite : entre 60 et 85 %
Validité de la certification : permanente

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

Suivre la **formation en sécurité réseau CND v2**, nécessite les prérequis suivants :

- avoir des connaissances avancées sur les systèmes d'exploitation Windows et Linux (systèmes de fichiers, permissions, sécurité, pare-feu, etc.) ;

- maîtriser les fondamentaux des réseaux, tels que les protocoles TCP/IP ;
- connaître les rôles et les services qui sont utilisés par les serveurs au niveau du réseau.

Public

Cette formation s'adresse aux publics suivants :

- les administrateurs réseau, les ingénieurs en sécurité réseau, les techniciens de défense réseau, les analystes réseaux, les responsables informatique et toute autre professionnels chargées de sécuriser un réseau.

Cette formation s'adresse aux profils suivants

Administrateur réseaux - télécoms
Administrateur système
Ingénieur réseaux - télécoms
Ingénieur système
Analyste de données

Programme

Module 1

- Les attaques réseau et les stratégies de défense.

Module 2

- La sécurité administrative des réseaux.

Module 3

- La sécurité technique des réseaux.

Module 4

- La sécurité du périmètre réseau.

Module 5

- La sécurité des points de terminaison pour les systèmes Windows.

Module 6

- La sécurité des points de terminaison pour les systèmes Linux.

Module 7

- La sécurité des points de terminaison pour les appareils mobiles.

Module 8

- La sécurité des points de terminaison pour les appareils IoT.

Module 9

- La sécurité des applications administratives.

Module 10

- La sécurité des données.

Module 11

- La sécurité des réseaux virtuels d'entreprise.

Module 12

- La sécurité des réseaux d'entreprise dans le cloud.

Module 13

- La sécurité des réseaux sans fil d'entreprise.

Module 14

- La surveillance et l'analyse du trafic réseau.

Module 15

- La surveillance et l'analyse des journaux du réseau.

Module 16

- La réponse aux incidents et aux enquêtes judiciaires.

Module 17

- La continuité des activités et la reprise après sinistre.

Module 18

- L'anticipation des risques et la gestion des risques.

Module 19

- L'évaluation des menaces via l'analyse de la surface d'attaque.

Module 20

- La prédiction des menaces via le renseignement sur les cybermenaces.