



CERTIFIED NETWORK DEFENDER V3

Formez-vous au seul programme entièrement axé sur la sécurité et la défense des réseaux !

Code : CNDv3

Le Certified Network Defender – CND – est un cours indépendant des fabricants, pratique, donné par un formateur accrédité et qui permettra aux étudiants de se certifier dans le domaine de la sécurité des réseaux. Avec un programme intensif de labs, la formation a été créée sur des compétences précises, directement liées à l'analyse des fiches de poste et au cadre de formation en cybersécurité donné par la National Initiative of Cybersecurity Education (NICE). La formation a également été adaptée aux différentes missions et responsabilités du poste d'administrateur système/réseau publiées par le Department of Defense (DoD).

Afin d'obtenir des compétences solides en sécurité défensive des réseaux, la formation prépare les administrateurs réseaux aux dernières technologies et pratiques de sécurité réseau.

Le programme Certified Network Defender v3 a été mis à jour pour vous donner les armes nécessaires afin d'aider les Blue Teams à se défendre. Les particuliers et les entreprises qui cherchent à renforcer leurs compétences en matière de défense de réseau trouveront la CND v3 indispensable.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% exercices pratiques : labs) et formalisés par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Network Attacks and Defense Strategies
- **Module 2 :** Administrative Network Security
- **Module 3 :** Technical Network Security
- **Module 4 :** Network Perimeter Security
- **Module 5 :** Endpoint Security – Windows Systems
- **Module 6 :** Endpoint Security – Linux Systems
- **Module 7 :** Endpoint Security – Mobiles Devices
- **Module 8 :** Endpoint Security – IoT Devices
- **Module 9 :** Administrative Application Security
- **Module 10 :** Data Security
- **Module 11 :** Enterprise Virtual Security
- **Module 12 :** Enterprise Cloud Security
- **Module 13 :** Enterprise Wireless Security
- **Module 14 :** Network Traffic Monitoring and Analysis
- **Module 15 :** Network Logs Monitoring and Analysis
- **Module 16 :** Incident Response and Forensic Investigation
- **Module 17 :** Business Continuity and Disaster Recovery

- **Module 18 :** Risk Anticipation with Risk Management
- **Module 19 :** Threat Assessment with Attack Surface Analysis
- **Module 20 :** Threat Prediction with Cyber Threat Intelligence

PASSAGE DE L'EXAMEN

L'examen CND 312-38 aura lieu à distance.

- **Titre de l'examen :** Certified Network Defender (ANSSI)
- **Format de l'examen :** QCM
- **Nombre de questions :** 100
- **Durée :** 4 heures
- **Langue :** anglais
- **Score requis :** 70% minimum de bonnes réponses

RÉSULTAT

Directement disponible en fin d'examen.

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.



PROCHAINES DATES

24 février 2025
14 avril 2025
7 juillet 2025
20 octobre 2025



OBJECTIFS

- Appréhender les fonctionnalités de protection, de détection, de réponse et de prévision de la sécurité des réseaux
- Être capable de sécuriser les conteneurs et les réseaux définis par logiciel
- Prévenir les menaces
- Être préparé(e) à l'examen Certified Network Defender (ANSI)



INFORMATIONS GÉNÉRALES

Code : CNDv3

Durée : 5 jours

Prix : 3 890 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Examen : inclus. Valable 12 mois à date de réception.

Passage de l'examen à distance.

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel



PUBLIC VISÉ

- Administrateur réseau / Administrateur sécurité réseau
- Ingénieurs sécurité réseau
- Techniciens défense réseau
- Analystes CND / Sécurité
- Responsable sécurité
- Toute personne impliquée dans des opérations de réseau



PRÉ-REQUIS

- 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.



RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 50% d'exercices pratiques
- 1 PC par personne