

## EC-Council Certified Network Defender (CND) + Voucher d'examen

**Durée: 5 Jours**    **Réf de cours: CND**    **Version: 2.0**    **Méthodes d'apprentissage: Virtual Learning**

### Résumé:

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour se préparer efficacement à la certification à la certification en sécurité. Il s'agit d'une formation basée sur les compétences, intensive et conçue pour incorporer les compétences critiques en matière de sécurité des réseaux - Protéger, Détecter, Répondre et Prédire. Elle intègre les outils, technologies et techniques les plus récents, déploie une approche pratique de l'apprentissage et met l'accent sur la prévision des menaces, la continuité des activités et la reprise après sinistre. La formation est conçue et développée après des études de marché et des enquêtes approfondies. Cette formation est délivrée en synchrone à distance tout en garantissant l'accès à un environnement d'apprentissage complet!

*Mise à jour : 18.12.2023*

### Public visé:

Cette formation s'adresse à ceux qui travaillent dans le domaine de l'administration des réseaux et de la cybersécurité en tant qu'administrateur/ingénieur réseau, administrateur/ingénieur/analyste de sécurité réseau, ingénieur en cybersécurité, analyste de sécurité, technicien de défense réseau, opérateur de sécurité. La formation s'adresse à toutes les opérations de cybersécurité, à tous les rôles et à toute personne souhaitant faire carrière dans la cybersécurité.

### Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Prévenir les menaces
- Appréhender les fonctionnalités de protection, de détection, de réponse et de prévision de la sécurité des réseaux
- Se préparer à la certification

### Pré-requis:

Les participants doivent 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 et connaître les rôles et les services qui sont utilisés par les serveurs au niveau du réseau.

## Contenu:

|  |  |  |
|--|--|--|
| Attaques de réseaux et stratégies de défense     | Sécurité des points finaux - Dispositifs IoT | Surveillance et analyse des journaux de réseau                   |
| Sécurité administrative des réseaux              | Sécurité des applications administratives    | Réponse aux incidents et investigations judiciaires              |
| Sécurité technique des réseaux                   | Sécurité des données                         | Continuité des activités et reprise après sinistre               |
| Sécurité du périmètre du réseau                  | Sécurité des réseaux virtuels d'entreprise   | Anticipation des risques et gestion des risques                  |
| Sécurité des points finaux - Systèmes Windows    | Sécurité des réseaux en nuage d'entreprise   | Évaluation des menaces avec l'analyse de la surface d'attaque    |
| Sécurité des points finaux - Systèmes Linux      | Sécurité des réseaux sans fil                | Prévision des menaces avec le renseignement sur les cybermenaces |
| Sécurité des points finaux - Dispositifs mobiles | Surveillance et analyse du trafic réseau     |  |

## Méthodes pédagogiques :

Support de cours officiel remis aux participants.

## Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via [moncompteformation.gouv.fr](http://moncompteformation.gouv.fr).

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur [globalknowledge.fr/handicap](http://globalknowledge.fr/handicap)
- Le Règlement intérieur est disponible sur [globalknowledge.fr/reglement](http://globalknowledge.fr/reglement)