+33 1 81 69 35 70 | contact@devforma.com | www.devforma.com

devforma
DÉVELOPPEMENT & FORMATION

Techniques d'Attaques en réseau et les contre-mesures

Plus de 75% de la formation est constituée d'exercices pratiques et de projets sur GNS3.

À qui s'adresse la formation ?

- Techniciens, administrateurs et ingénieurs systèmes/réseaux/sécurité.

+33 1 81 69 35 70 | contact@devforma.com | www.devforma.com

devforma
DÉVELOPPEMENT & FORMATION

Informations clés

Jours de formations	**3**
Lieu	**Présentiel / Distanciel**
Horaires	**9h - 12h30 / 13h30 - 17h00.**
Prix global	**2400 €**
Eligibilité aux OPCO	**Oui**
Eligibilité aux CPF	**Lien CPF**
Langue	**Français**
Vidéos	**Non**
Durée de l'examen	**Selon la certification demandée**

+33 1 81 69 35 70 | contact@devforma.com | www.devforma.com

devforma
DÉVELOPPEMENT & FORMATION

Objectifs de la formation

- Comprendre et sécuriser les réseaux d'entreprise contre les vulnérabilités modernes.
- Déployer des configurations robustes et appliquer des bonnes pratiques actualisées.
- Protéger efficacement les utilisateurs et les points d'entrée extérieurs.
- Configurer correctement les équipements de protection avec les dernières technologies.

Approche pédagogique

Cette formation comporte plusieurs ateliers pratiques sur des environnements techniques. Les sessions "A distance" sont réalisées avec un outil de visioconférence, permettant au formateur d'adapter sa pédagogie.

L'évaluation se fait en continue au fils des travaux pratiques.

Prérequis

- Compréhension des concepts de réseau et de sécurité.
- Connaissance en configuration de routeurs et d'équipements réseau Cisco.
- Connaissance de l'utilisation de Linux et des lignes de commande.
- Connaissance de l'utilisation de GNS3.

+33 1 81 69 35 70 | contact@devforma.com | www.devforma.com

Programme de la formation

Jour 1

Fondamentaux de la sécurité réseau et défense de niveau 2

1. Introduction aux enjeux actuels de la sécurité réseau

- Tendances récentes en cybersécurité.
- Analyse des risques et typologie des attaques modernes.

2. Attaques et défenses sur les équipements de niveau 2

- Approfondissement sur les switchs de niveau 2 et 3.
- Étude de cas sur ARP Poisoning et VLAN Hopping, avec démonstrations pratiques.

Jour 2

Sécurité des protocoles et équipements de niveau 3

3. Attaques et protections de niveau 3

- Exploration des vulnérabilités dans IPv4 & IPv6.
- Analyses pratiques d'attaques sur RIP, OSPF, et BGP avec contres mesures actualisées.

4. Sécurité des passerelles virtuelles

- Simulation d'attaques sur VRRP et HSRP.
- Mise en œuvre des stratégies de défense efficaces.

Jour 3

Sécurité VPN, chiffrement et outils de protection réseau

5. Attaques et défenses des VPN

- Techniques avancées pour cracker et protéger les VPN.
- Pratiques recommandées pour sécuriser les communications VPN.

6. Chiffrement et authentification

- Évolution de la cryptographie et son application dans les réseaux modernes.
- Mises en situation sur l'authentification sous Linux et Windows.

7. Outils de protection réseau

- Dernières innovations en matière de pare-feu, IDS/IPS, et serveurs mandataires.
- Ateliers pratiques sur la configuration et l'optimisation de ces outils.