

CISCO CYBER SÉCURITÉ

La cybersécurité est devenue un enjeu majeur pour les entreprises, les gouvernements et les particuliers à travers le monde.



Cette formation, conçue selon les standards de Cisco, offre une introduction complète aux principes fondamentaux de la cybersécurité. Il prépare le participant à identifier, évaluer et prévenir les menaces numériques tout en développant une compréhension approfondie des mécanismes de protection des systèmes informatiques.

Elle prépare le participant à devenir un expert capable de protéger efficacement les systèmes d'information dans un monde en constante évolution. Avec une combinaison parfaite de théorie et de pratique, il sera prêt à relever les défis modernes de la sécurité informatique.

OBJECTIFS

- Maîtriser les bases et les concepts avancés de la cybersécurité selon les normes Cisco.
- Identifier, analyser et répondre efficacement aux menaces numériques.
- Utiliser les outils Cisco pour la surveillance, la prévention et la résolution d'incidents.
- Garantir une sécurité alignée avec les réglementations et standards internationaux.
- Mettre en œuvre des stratégies de cybersécurité robustes au sein des organisations.

CONTENU

1. Introduction à la cybersécurité Cisco

- Importance de la cybersécurité dans un environnement numérique
- Présentation des menaces actuelles et futures

2. Fondamentaux de la sécurité réseau

- Modèles de sécurité et architecture réseau
- Protocoles de sécurité de base

3. Gestion des menaces

- Identification des types d'attaques (phishing, malwares, ransomwares, etc.)
- Méthodes de détection et de prévention

4. Solutions Cisco de sécurité

- Cisco Secure Firewall
- Cisco Umbrella
- Cisco Secure Endpoint et autres outils avancés

5. Stratégies de prévention des intrusions

- Configuration et gestion des systèmes de prévention des intrusions (IPS)
- Analyse et résolution des vulnérabilités

6. Sécurité des applications et des données

- Protection des bases de données et des applications critiques
- Gestion des accès et des identités

7. Réponse aux incidents et gestion des crises

- Élaboration de plans d'intervention en cas de cyberattaque
- Méthodes de remédiation et récupération

8. Conformité et gouvernance

- Règlements internationaux (RGPD, ISO 27001)
- Application des meilleures pratiques en cybersécurité

9. Atelier pratique

- Études de cas réels
- Simulations d'attaques et de réponses adaptées