Aperçu du cours

Ce programme a été révisé, enrichi et un module sur les réseaux a été ajouté. Les participants exploreront les principes de base de la cybersécurité, les menaces et attaques courantes, ainsi que les bonnes pratiques pour protéger les systèmes et les données. Ils apprendront à identifier les vulnérabilités et à adopter une approche proactive en matière de gestion des risques.

Tout au long de la formation, nous aborderons des sujets essentiels tels que la sécurité des réseaux, la gestion des identités et des accès (IAM), la sensibilisation aux attaques d'ingénierie sociale, ainsi que les fondements de l'audit et de la conformité.

Qu'il s'agisse de professionnels en reconversion, chef d'entreprise, d'étudiants en informatique ou de débutants curieux de découvrir le domaine de la cybersécurité, a l'issue de cette formation, vous maîtriserez les fondamentaux essentiels pour poursuivre l'examen Security+ de CompTIA

kozetek

Contenu du programme

Chapitre 1 - Introduction

- Métiers en cybersecurité
- Internet
- Architecture client-serveur
- Adresse IP
- DNS & DHCP
- Modèle OSI

Chapitre 2 - Réseaux informatique

- Firewal , Switch, Router, AP
- Firewall Statefull & stateless
- IDS & IPS
- IPSEC
- SSH
- WAF & nextGEN firewall
- Sécurité sans fil
- Routing
- VPN
- DMZ
- NAT

kozetek

Chapitre 3 - Attaques courantes

- DeepFake
- Malware
- Phishing/Vishing
- Baiting
- Tailgating
- Ingénierie sociale
- Ransomware
- Brute Force

Chapitre 4 - Concepts fondamentaux

- Triangle CIA
- Principle du privilège restreint
- Sécurité et cout
- Défense en profondeur
- Threat Modeling
- Sécurité physique
- Authorisation
- Authentification
- Accountability
- Active Directory
- Séparation des tâches

kozetek

Chapitre 5 - Sécurité des appareils

- Gestion des terminaux (endpoint)
- Gestions des terminaux mobiles (MDM)
- Endpoint Detection Response (EDR)
- Réduction surface attaque
- Zero-Trust Architecture

Chapitre 6 - Gouvernance, Risk , conformité

- Confirmité technologique
- Politique technologique
- Politique de mot de passe
- RTO - RPO -AIW
- DRP - IRP - BCP
- Gestion des vulnerabilités
- SIEM avec Nessus
- Audit informatique
- OWASP top 10
- Circulaire 126 BRH
- Test de pénétration

kozetek

Chapitre 7 - Conclusion

- Identification des besoins
- Politiques de sécurité
- Architecture réseau
- Monitoring réseau
- Contrôle d'accès
- Journalisation
- Dispositis réseaux
- Sensibilisation des utilisateurs

kozetek