FORMATION PROFESSIONNELLE
CYBERSECURITE

Tel : 25 40 87 05 / 70 25 87 70 /78 85 35 74 Email : info@asntechnology.com
www.asntechnology.com

Le : 25 mars 2024 | **à Ouagadougou**

Tarifs:-
-Entreprise : 300.000 F/pers - Particulier: 200.000 F/pers SANS EXAMEN

Durée : 5 jours

OBJECTIFS DE LA FORMATION

- Installer des machines virtuelles afin de créer un environnement sécurisé pour la mise en œuvre et l'analyse des incidents de cyber sécurité.
- Expliquer le rôle de l'analyste de cyber sécurité dans l'entreprise
- Expliquer les fonctionnalités et les caractéristiques du système d'exploitation Windows nécessaires pour renforcer les analyses de cyber sécurité.
- Expliquer les fonctionnalités et les caractéristiques du système d'exploitation Linux.
- Analyser le fonctionnement des services et des protocoles réseau.
- Expliquer le fonctionnement de l'infrastructure de réseau.
- Classer les divers types d'attaques réseau
- Utiliser des outils de surveillance du réseau pour identifier les
- attaques contre les services et les protocoles réseau.
- Expliquer comment empêcher un accès malveillant aux réseaux informatiques, aux hôtes et aux données.
- Expliquer les effets de la cryptographie sur la surveillance de la sécurité du réseau.
- Expliquer comment enquêter sur les attaques et les vulnérabilités des terminaux.
- Évaluer les alertes de sécurité du réseau.
- Analyser les données liées aux intrusions réseau afin d'identifier les hôtes compromis et les vulnérabilités.
- Appliquer des modèles de gestion des incidents liés à la sécurité du réseau.

PREREQUIS

Avoir des notions en réseau informatique

Public cible

- Gestionnaires de système d'information,
- Administrateurs systèmes / réseaux/base de données
- Toute personne interessée par la sécurité..

Méthode pédagogique

- • formation participative et échange d'expériences
- • Théorie et Travaux pratiques

CONTENUS

Généralités

- Introduction
- Qu'est-ce que la cyber sécurité ?

- Fonctionnement de la cyber sécurité
- Professionnels de la cyber sécurité

Modules 1 : Acteurs de Menace et des Défenseurs

- Acteurs de menance
- Les defenseurs
- Travaux Pratiques

Module 2 : Présentation du Système d'Exploitation

- Le système d'exploitation Windows
- Le système d'exploitation Linux
- Travaux pratiques

Module 3 : Fondamentaux du Réseau

- Protocoles réseaux
- Ethernet et protocole IP
- Vérification de la connectivité
- Protocole ARP
- Couche Transport
- Services réseaux
- Travaux pratiques
- Module 4 : Sécurité de l'Infrastructure Réseau
- Les périphériques de communication réseau
- Infrastructure de sécurité réseau
- Travaux pratiques

Module 4 : Sécurité de l'infrastructure réseau

- Les périphériques de communication réseau
- Infrastructure de sécurité réseau

Module 5 : Menaces et Attaques

- Les hackers et leurs outils
- Menaces et attaques courantes
- Outils de surveillance réseau
- Attaques ciblant les fondamentaux du réseau
- Attaquer les actifs
- Travaux pratiques

Module 6 : Défense du Réseau

- Comprendre la défense
- Contrôle d'accès
- Renseignements sur les menaces
- Travaux pratiques

Module 7 : Cryptographie et Protection des Points d'Extrémité

- Cryptographie
- Protection des terminaux
- Évaluation des vulnérabilités des terminaux
- Travaux pratiques

Modules 8 : Protocoles et Fichiers Journaux

- Technologies et protocoles
- Données de sécurité réseau

1-Formation
2-Coaching après la formation et Examen

Faites valoir vos compétences
Obtenez :
- Une attestation de formation
-Un coaching GRATUIT après la formation
- Documents et cas pratiques GRATUITS

Modules 9 : Analyse des données de sécurité

- Évaluation des alertes
- Utilisation des données de sécurité réseau
- Analyse et réponse aux incidents numériques
- Travaux pratiques