SARL ONEO
1025 rue Henri Becquerel
Parc Club du Millénaire, Bât. 27
34000 MONTPELLIER
N° organisme : 91 34 0570434

Nous contacter :
04 67 13 45 45
www.ait.fr
contact@ait.fr

Référence	**4-IT-CYBA**
Durée	**5 jours (35 heures)**
Éligible CPF	**NON**
Mise à jour	**27/11/2023**

Les essentiels de la cybersécurité

Objectifs pedagogiques

- Présentation des cyber-menaces actuelles et sites de référence sur la cybersécurité
- Directives et exigences de conformité
- Cyber rôles nécessaires à la conception de systèmes sûrs
- Cycle des attaques processus de gestion des risques
- Stratégies optimales pour sécuriser le réseau d'entreprise
- Zones de sécurité et solutions standards de protection

Public concerne

Professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en sécurité

Prerequis

Connaissances en réseaux TCP/IP

Moyens pedagogiques

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
- Remise d'un support de cours.

Modalites d'evaluation

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Attestation de stage à chaque apprenant,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

Moyens techniques en presentiel

Accueil des stagiaires dans une salle dédiée à la formation équipée à minima d'un vidéo projecteur et d'un tableau blanc et/ou paperboard.

Pour les formations nécessitant un ordinateur, un PC est mis à disposition de chaque participant.

Moyens techniques en distanciel

A l'aide d'un logiciel (Teams, Zoom…), d'un micro et éventuellement d'une caméra les apprenants interagissent et communiquent entre eux et avec le formateur.

Sessions organisées en inter comme en intra entreprise.

L'accès à l'environnement d'apprentissage ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.

Pour toute question avant et pendant le parcours, assistance technique à disposition au 04 67 13 45 45.

Organisation

Délai d'accès : 5 jours ouvrés
(délai variable en fonction du financeur)

Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

Accessibilite

Les personnes en situation d'handicap sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

Pour tout renseignement, notre référent handicap reste à votre disposition : mteyssedou@ait.fr

Profil formateur

Nos formateur sont des experts dans leurs domaines d'intervention

Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

Certification possible

TOSA Cybercitizen
Certificateur ISOGRAD

Les essentiels de la cybersécurité

Le champ de bataille
- ☐ La croissance d'Internet dans le monde entier
- ☐ Principes et objectifs de sécurité
- ☐ Terminologie des menaces et de l'exposition
- ☐ Documents et procédures de gestion des risques

Structure de l'Internet et TCP/IP
- ☐ Normes de conformité juridique
- ☐ Internet Leadership IANA
- ☐ Modèle TCP/IP

Évaluation de la vulnerabilite et outils
- ☐ Vulnérabilités et exploits
- ☐ Outils d'évaluation de la vulnérabilité
- ☐ Techniques d'attaques avancées, outils et préventions

Sensibilisation a la cyber securite
- ☐ Ingénierie sociale : objectifs de l'ingénierie sociale, cibles, attaque, hameçonnage
- ☐ Sensibilisation à la cyber sécurité : politiques et procédures

Cyber-attaques : Footprinting et scannage
- ☐ Footprinting
- ☐ Identification du réseau cible et sa portée
- ☐ Techniques de scannage de port

Cyberattaques : effraction
- ☐ Attaque des mots de passe, escalade des privilèges
- ☐ Authentification et décodage du mot de passe

Cyberattaques : Porte derobee et cheval de Troie (Backdoor and Trojans)
- ☐ Logiciels malveillants, Cheval de Troie, Backdoor et contre-mesures
- ☐ Communications secrètes
- ☐ Logiciel anti-espion
- ☐ Pratiques de lutte contre les logiciels malveillants

Évaluation et gestion des risques cybernetiques
- ☐ Actifs protégés : CIA Triad
- ☐ Processus de détermination de la menace
- ☐ Catégories de vulnérabilités
- ☐ Actifs de l'entreprise vs risques

Gestion des politiques de securite
- ☐ Politique de sécurité
- ☐ Références de politiques

Securisation des serveurs et des hotes
- ☐ Types d'hôtes
- ☐ Directives de configuration générale et correctifs de sécurité
- ☐ Renforcement des serveurs et périphériques réseau
- ☐ Renforcement de l'accès sans fil et sécurité des VLAN

Securisation des communications
- ☐ Application de la cryptographie au modèle OSI
- ☐ Tunnels et sécurisation des services

Authentification et solutions de chiffrement
- ☐ Authentification par mot de passe de systèmes de chiffrage
- ☐ Fonctions de hachage
- ☐ Avantages cryptographiques de Kerberos
- ☐ Composants PKI du chiffrement à clef symétrique, du chiffrement asymétrique, des signatures numériques

Pare-feu et dispositifs de pointe
- ☐ Intégration de la sécurité générale
- ☐ Prévention et détection d'intrusion et défense en profondeur
- ☐ Journalisation

Analyse criminalistique
- ☐ Gestion des incidents
- ☐ Réaction à l'incident de sécurité

Reprise et continuite d'activite
- ☐ Types de catastrophes et Plan de reprise d'activité (PRA)
- ☐ Haute disponibilité
- ☐ Documentation de collecte de données
- ☐ Plan de Reprise d'Activité et Plan de Continuité d'Activité

Cyber-revolution
- ☐ Cyberforces, Cyberterrorisme et Cybersécurité : crime, guerre ou campagne de peur ?

LABS
- ☐ Lab1: Installation du lab
- ☐ Lab 2 : Comprendre TCP/IP
- ☐ Lab 3 : Evaluation de la vulnérabilité
- ☐ Lab 4 : Sensibilisation à la cybersécurité
- ☐ Lab 5 : Scannage
- ☐ Lab 6 : Cyber-attaques et mots de passe
- ☐ Lab 7 : Cyber-attaques et portes dérobées
- ☐ Lab 8 : Évaluation des risques
- ☐ Lab 9 : Stratégies de sécurité
- ☐ Lab 10 : Sécurité hôte
- ☐ Lab 11 : Communications secrètes
- ☐ Lab 12 : Authentification et cryptographie
- ☐ Lab 13 : Snort IDS
- ☐ Lab 14 : Analyse criminalistique
- ☐ Lab 15 : Plan de continuité des affaires