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

Nous contacter :
+33 (0)4 67 13 45 45
www.ait.fr
contact@ait.fr

Référence	**3-SR-VPN**
Durée	**3 jours (21 heures)**
Éligible CPF	**NON**
Mise à jour	**26/12/2022**

VPN - Préserver ses informations sur internet

Objectifs pédagogiques

- Connaitre les menaces de vos communications internes, inter site, nomades
- Appréhender les opportunités technologiques
- Bonnes pratiques pour leur mise en service, leur suivi et leur contrôle

Public concerné

- Professionnels de la sécurité, les administrateurs, les ingénieurs réseau, les techniciens informatique

Prérequis

- Bonne compréhension des protocoles TCP/IP, pratique de l'Internet et des applications standards

Moyens pédagogiques

- 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.
- Alternance entre apports théoriques et exercices pratiques (en moyenne 30 à 50%)
- Remise d'un support de cours.

Modalités d'évaluation

- 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 présentiel

- 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

Accessibilité

- 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

- Aucune

VPN - Préserver ses informations sur internet

1. VPN : Assurer des communications sûres dans un environnement hostile

- Organisations étendues et mobilité
- Menaces sur les communications
- Objectifs de la sécurité des communications

2. Réseaux Virtuels Privés

- Qu'est-ce qu'un VPN ?
- Quelles utilisations ?
- Comment construire ou acquérir un VPN ?

3. Première approche de la cryptographie

- Transformation des messages - chiffrement et déchiffrement
- Deux types de chiffrement
- Signatures numériques
- Certificats numériques
- Implantation des protections
- Vieillissement et révocation automatique et manuelle des clés

5. Gestion de clés publiques (PKI)

- Objectif de la PKI
- Caractéristiques et éléments de la PKI
- Exemples de PKI

6. Première approche de l'encapsulation et de l'étiquetage

- TCP/IP et le modèle OSI
- Serial Line Interface Protocol (SLIP), « Point to point protocole » (PPP), « Point to point Tunneling Protocol» (PPTP)
- Level 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP)
- Multiprotocol Label Switching (MPLS)
- Protocole de réservation de ressource (RSVP), services différenciés (DiffServ), et services intégrés IETF (IntServ)

7. Sécurité du protocole IP (IPsec)

- Qu'est-ce que l´Ipsec ?
- Association de sécurité (SA), Base de données de sécurité (SADB), Base de données des procédures (SPD)
- Mode opératoire et services de sécurité d'Ipsec
- Phases et échange de clés Internet (IKE)
- Risques et limites d'IPSEC
- Principaux matériels/logiciels permettant de créer des VPN IPSEC

8. Sécurité des couches applicatives : SSL, SSH et TLS

- Qu'est-ce que SSL/TLS ?
- Mode opératoire et services de sécurité de SSL/TLS
- Risques et limites de SSL/SSH
- Principaux matériels/logiciels permettant de créer des VPN SSL/TLS/SSH

9. Modèles propriétaires : LEAP/WPA/VNC/...

- La sécurité nécessaire des communications sans fils
- Des solutions cryptographiques propriétaires controversées
- Quelle harmonisation ?

10. Architecture de communications sécurisées

- Applications à servir, répartition des risques, politique, et architecture
- Lieu d'installation des services de protection
- Sécurité des communications et disponibilité
- Approche de choix de solutions

11. Gestion et maintenance des communications sécurisées

- Principes pour maintenir et gérer des communications sécurisées
- Recherche et correction des fautes
- Performance
- Gestion des clés
- Directions futures
- Services de sécurité dans IPV6