

- *Fonctionnement de la sécurité*
- *Contrôle d'accès*
- *Cryptographie*
- *Modèles et architectures de la sécurité*
- *Sécurisation des télécommunications et des réseaux*
- *Sécurité des applications*
- *Plan de continuité d'activité*
- *Cadre légal, investigation et éthique*
- *Sécurité physique*
- *Sécurité des informations et gestion des risques*

OUTILS PÉDAGOGIQUES**MODALITÉS D'ÉVALUATION****MODALITÉS DE FINANCEMENT****MODALITÉS ET DÉLAIS D'ACCÈS****OBJECTIFS PÉDAGOGIQUES****ACCESSIBILITÉ****LES POINTS FORTS DE LA FORMATION****5****Prix : 3?690 € € / HT****PRÉ-REQUIS**

- Connaître les concepts de base de la sécurité
- Avoir une expérience dans l'administration des systèmes, une bonne compréhension des systèmes Unix, Linux et Windows

MODALITÉS ET DÉLAIS D'ACCÈS**ATTESTATION OBTENUE****EFFECTIF DE LA FORMATION****CERTIFICATION****MODALITÉ PÉDAGOGIQUE**

Cours dispensé en mode présentiel avec une alternance d'apports théoriques et méthodologiques, et de mises en situations pratiques

PROCHAINES SESSIONS

Le 07/02/2022
Le 28/03/2022
Le 25/04/2022
Le 16/05/2022
Le 27/06/2022
Le 07/02/2022
Le 28/03/2022
Le 25/04/2022
Le 16/05/2022
Le 27/06/2022
Le 07/02/2022
Le 28/03/2022
Le 25/04/2022
Le 16/05/2022
Le 27/06/2022

PROGRAMMES DE FORMATION CISSP PRÉPARATION À LA CERTIFICATION SÉCURITÉ

Cette formation prépare au passage de l'examen CISSP dans le cadre du cursus de certification Certified Information Systems Security Professional (CISSP). La certification n'est pas incluse dans la formation.

SECURITE ET GESTION DU RISQUE (LA SECURITE, LES RISQUES, LES LOIS, LES RÉGULATION, ET LA CONTINUITÉ DES AFFAIRES)

- Concepts de confidentialité, d'intégrité, et de disponibilité
- Les principes gouvernant la Sécurité
- La conformité
- Les problèmes légaux et liés aux Régulations
- L'éthique professionnelle
- Les politiques de Sécurité, les Standards, les procédures et les lignes de conduites

LA SECURITE DES BIENS / VALEURS

- La classification des biens et de l'information
- La propriété (ex: les propriétaires des données, des systèmes)
- Protéger les données privées (sensibles)
- Une conservation adéquate
- Les contrôles des données de Sécurité
- Besoins à remplir pour la manipulation des données (ex: marquer, mettre des labels, le stockage)

L'INGÉNIERIE LIÉE À LA SECURITE (INGÉNIERIE & GESTION DE LA SECURITE)

- Les processus d'ingénierie liés aux principes conception sécurisé
- Les concepts fondamentaux des modèles de Sécurité
- Capacité d'un système d'information en matière de Sécurité
- L'architecture de la Sécurité, sa conception et les faiblesses des éléments de solution
- Les faiblesses des systèmes basés sur le Web
- Les faiblesses des systèmes mobiles
- Les faiblesses des systèmes embarqués et des systèmes Cyber
- La cryptographie
- Les principes de conception de lieux et de bâtiments sécurisés
- La Sécurité Physique

LA SECURITE DE COMMUNICATION ET DES RÉSEAUX (CONCEPTION ET PROTECTION DE LA SECURITE DES RÉSEAUX)

- La conception de Réseaux sécurisés (ex: les protocoles basés sur IP & non basés sur IP, la segmentation)
- Les composants d'un réseau sécurisé
- Les canaux de communication sécurisé
- Les attaques réseaux

LA GESTION DE L'ACCÈS ET L'IDENTITÉ (CONTROLLER L'ACCES ET GÉRER LES IDENTITÉS)

- Les contrôles logiques et physique des biens/valeurs
- L'identification et l'authentification des personnes et des périphériques
- Les Services Identité (ex. l'identité des nuages)
- Les Services tiers de gestion de l'identité (ex. sur site)
- Les attaques utilisant le contrôle d'Accès
- Le cycle de l'identification et d'accorder l'accès ou non (concrètement, comment provisionner)

L'ÉVALUATION ET LE TEST DE LA SECURITE (CONCEVOIR, EXÉCUTER, ET ANALYSER LES TESTS DE SECURITE)

- L'évaluation et les stratégies de Tests
- Les données liées au processus de Sécurité (ex. gestion et contrôles d'opération)
- Les tests de contrôle liés à la Sécurité
- Les résultats de tests (ex. automatiques / manuel)
- Les failles/faiblesses des Architectures de Sécurité

L'OPÉRATIONNEL DE LA SECURITE (CONCEPTS FONDAMENTAUX, ENQUÊTES, GESTION DES INCIDENTS, AND RECOUVREMENT APRÈS CATASTROPHE)

- Les moyens / aides à l'enquêtes et ce qui est nécessaire
- Le traçage et le suivi des activités
- Provisionner pour les ressources
- Les concepts opérationnels fondamentaux liés à la Sécurité
- Les techniques pour Protéger les biens / valeurs
- Gestion des incidents
- Mesures préventives
- Gestion des patches et des faiblesses

- Le processus de gestion des changements
- Les stratégies de recouvrement
- Le processus de gestion et de planification des désastres, de leur mise en oeuvre
- La gestion de la Continuité des affaires et de leurs exercices
- La Sécurité physique
- La mise à niveau du personnel de Sécurité

LA SÉCURITÉ DU DÉVELOPPEMENT SÉCURISÉ (LA COMPRÉHENSION, LA GESTION DES DIFFICULTÉS LIÉ AUSSI À LA SÉCURITÉ DES LOGICIELS)

- La Sécurité tout au long des phases de développement logiciel
- Les contrôles liés à la Sécurité dans l'environnement
- L'efficacité des architectures de Sécurité
- La Sécurité des logiciels acquis et leurs impacts