

Organisation et sécurité du Système d'Information

Durée: 4 Jours **Réf de cours: CYBTO** **Version: 2** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

Cette formation est délivrée en synchrone à distance tout en garantissant l'accès à un environnement d'apprentissage complet! Ce module de formation permet de présenter les bases d'une organisation ainsi que la sécurité des SI dans le domaine de la Cybersécurité. Il sert d'introduction aux modules avancés en Cybersécurité.

Public visé:

Cette formation s'adresse à toute personne ayant des connaissances techniques des systèmes d'information et souhaitant se former aux fondamentaux techniques de la Cybersécurité ou souhaitant s'orienter vers les métiers de la Cybersécurité.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
 - Expliquer l'enjeu humain et matériel autour de la cyber sécurité.
 - Identifier l'organisation technique des SI.
-

Pré-requis:

- Avoir suivi le MOOC de l'ANSSI
 - Connaître le guide d'hygiène informatique.
 - CYBER - Les essentiels de la Cybersécurité
-

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- CYBNR - Cybersécurité : conformité et évolution des normes
-

Contenu:

Partie I : organisation

technique

- Réponse légale à un incident (Forensic)
- L'analyse de risques : EBIOS/MEHARI
- La protection des infrastructures
- La gestion des identités et des accès
- La surveillance

Labs

- Lab : Sensibilisation
- Lab : Ingénierie sociale

Partie II: la sécurité du SI

La sécurité physique

- Les équipements du réseau : Switch, Routeurs, Pare-feu, Sondes HIDS/HIPS et NIDS/NIPS, Honeybots
- Accès aux équipements avec authentification AAA
- Contrôler les interfaces

La gestion des accès

- Identification et authentification
- Les méthodes d'authentification : Biométrie, certificats, token
- Gestion des mots de passe
- Authentification forte (two-factor authentication)
- SSO (Single Sign-on)
- Principes d'autorisation et modèles d'autorisation : ACM, DAC, MAC, RBAC, ABAC

La supervision

- Traçabilité
- Gestion des événements (logs)

La sécurité des applications

- Les enjeux de sécurité tout au long du cycle de développement
- Les failles les plus courantes
- Sécurisation des applications Web et OWASP
- Utilisation de pare-feu applicatif : WAF (Web Application Firewall)

La sécurité du cloud

- Les principaux acteurs
- La sécurité selon le type de cloud (public, privé, hybride)
- La sécurisation des environnements virtuels
- Confidentialité et emplacement des données
- Niveaux de disponibilité et de services (Besoins de SLA)
- Respect des lois et réglementations

Labs

- Lab : Escalade des privilèges
- Lab : sécurité physique
- Lab : Analyse des Flux réseau
- Lab : Sécuriser Web server, FTP et Poste de travail
- Lab : Protection des données
- Lab : PKI
- Lab : Gestion des mots de passe

Préparation au passage de la certification CISEF Cyber ; IT Security Foundation (Exin)

?

Méthodes pédagogiques :

Suivi de cette formation à distance depuis un site client équipé. Il suffit de disposer de : une bonne connexion internet un casque avec microphone au calme pour en profiter pleinement

Une fiche explicative est adressée en amont aux participants pour leur permettre de vérifier leur installation technique et de se familiariser avec la solution technologique utilisée.

L'accès à l'environnement d'apprentissage (support de cours officiel CYBTO en français, labs, ainsi qu'aux feuilles d'émargement et d'évaluation est assuré.

Glossaire Français/Anglais permettant la préparation de la certification remis aux participants.

En savoir plus : <https://www.globalknowledge.com/fr-fr/solutions/methodes-d'apprentissage/classe-a-distance>

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
- Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.