Formation Organisation et sécurité du Système d'Information

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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.

Référence	CYBTO
Durée	4 jours (28h)
Tarif	2 990 €HT
Repas	80 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 8 au 11 septembre 2025

PARIS

du 8 au 11 septembre 2025

VOIR TOUTES LES DATES

Objectifs

| Identifier l'organisation technique des SI.
| Expliquer l'enjeu humain et matériel autour de la cyber sécurité.

Public

| 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.

Prérequis

| Avoir suivi le MOOC de l'ANSSI
| Connaître le guide d'hygiène informatique de l'ANSSI.

Programme de la formation

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, Honeypots
| 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)

HUB Formation - 14 avenue de l'Opéra - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

La sécurité des applications
| Les enjeux de sécurité tout au long du cycle de développement
| Les failles les plus courantes
| Sécurisation des apllications 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 règlementations

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)

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.

Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.