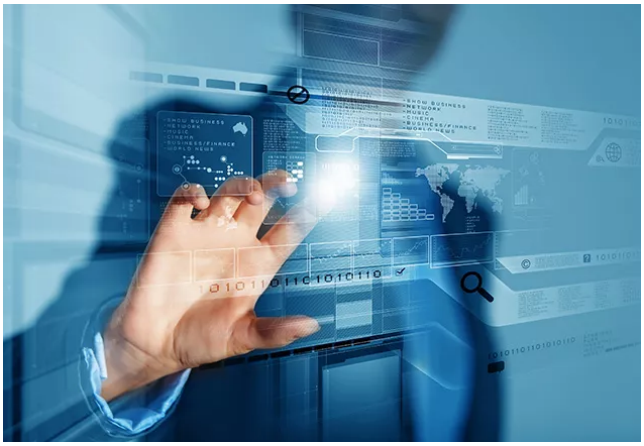
Formation cybersécurité : Devenir Lead Operational Security Officer (SECOPS)

Ref: PR-CYB-AT-LOSO

Maîtriser les principes et mécanismes techniques de la sécurité de l'information sur le plan opérationnel



DURÉE : **5 Jours** (35H)
Prix : **2 795,00 € HT**

PRÉSENTIEL
FORMATION QUALIFIANTE

Objectifs et compétences visés

- Maîtriser les principes techniques et les bonnes pratiques de la sécurité de l'information au sein d'une entreprise.
- Comprendre les mécanismes de sécurité généraux : architecture sécurisée, authentification, segmentation, outils de sécurité (IDS/IPS, NAC, firewalls, etc.), développement sécurisé, durcissement...
- Appréhender les audits techniques : audit d'architecture, audit de configuration, audit de code source, test d'intrusion...

À qui s'adresse la formation ?

Profils

- Chefs de projet maîtrise d’ouvrage et maîtrise d’œuvre.
- Membres d’une équipe de cybersécurité.
- Responsables de projet ou consultants souhaitant préparer et soutenir un organisme dans la mise en œuvre de la sécurité des systèmes d’information.

- Responsables des systèmes d’information ou de la sécurité du SI.
- Toute personne souhaitant maîtriser les principes techniques la sécurité des systèmes d’information.

Prérequis

Aucun prérequis nécessaire à cette formation. Il est nécessaire de venir muni d'un ordinateur portable.
Le suivi du MOOC de l'ANSSI (https://secnumacademie.gouv.fr/) n'est pas un prérequis mais est fortement recommandé.

Contenu de la formation

Dans un premier temps vous aborderez les principes de bases et les objectifs de la sécurité de l'information (module 1) :

- Notions de risque
- Les règles de base
- Le contrôle d'accès : AAA (Authentification, Autorisation, Traçabilité), la gestion des utilisateurs et la gestion des privilèges

Le deuxième volet de la formation pour devenir Lead Operational Security Officer est dédié à la cryptographie, au réseau et aux applications (modules 2, 3 et 4) :

- Concepts fondamentaux et modèles théoriques
- Fonctions de base (chiffrement, hachage, signature) et protocoles (TLS, IPSec,SSH)
- Attaques classiques, contrôle d'accès, segmentation et sécurisation
- Architecture, protocoles, authentification, OWASP et processus de développement

Le troisième volet se concentre sur les systèmes d'exploitation Linux (module 5) et Windows (module 6).

Enfin, la formation se termine par une approche théorique et pratique de la gestion des vulnérabilités et gestion des incidents (modules 7 et 8) :

- Sauvegarde et journalisation
- Veille sécurité
- SOC et CSIRT
- La gestion d'incidents et l'analyse inforensique

Modalités de la formation

Modalités d'évaluation

Cette formation se conclut par un examen de validation des acquis.

Nos plus

- Formation animée par un consultant CNPP spécialisé en sécurité opérationnelle et architecture sécurisée.
- Disponible également en visioconférence.

CNPP en quelques chiffres

21000
stagiaires / an


Des infrastructures pédagogiques uniques

+ de 500
diplômés / an

+ de 400
intervenants

98%
de stagiaires satisfaits en 2025

Nos formations complémentaires

Forensic et sécurité opérationnelle
Formation cybersécurité : Fondamentaux techniques de la sécurité de l'information
1 Jour
Présentiel
Appréhender les différentes facettes de la sécurité technique (authentification, développement, SI central...)

Forensic et sécurité opérationnelle
Formation cybersécurité : Devenir Lead Ethical Hacker
5,5 Jours
Présentiel
Acquérir une compréhension approfondie des concepts et méthodes employés par les professionnels de la cybersécurité en vue d'exécuter des tests d'intrusion.

Besoin d'informations sur une formation en cybersécurité ?

Nous sommes à votre écoute pour échanger sur votre prochaine formation en cybersécurité.

Contactez-nous !

+33 (0)8 06 00 03 80