Cybersécurité pour les systèmes d’information

Durée
4 jours

Lieu
ENSICAEN

Prochaines sessions :
3 décembre 2024
4 février 2025

Effectif minimum
4 personnes

Tarif
3800 €
net de taxe par personne, accueil et déjeuner inclus

Cybersécurité pour les systèmes d’information d’entreprise, ses réseaux et technologies modernes

Les cyberattaques prennent de plus en plus d’ampleur et touche aujourd’hui aussi bien les particuliers que les professionnels passant par les entreprises, les administrations publiques dans tous les pays. La cybersécurité devient donc un enjeu majeur face à ce phénomène.

Objectifs de la formation

- Étudier les vulnérabilités et vecteurs d'attaques cyber d'un système informatique dans l'environnement du travail
- Comprendre les éléments de base pour concevoir une architecture de sécurité pour l'entreprise
- Étudier les outils et solutions du contrôle d'accès sécurisé, sécurité réseaux et résilience
- Comprendre les principes de sécurité des technologies modernes pour l'entreprise (WiFi, Cloud, blockchains, IoT et systèmes connectés et embarqués)

Public

Toute personne souhaitant être sensibiliser à la cybersécurité et accroître ses connaissances dans le domaine

Prérequis

Pas de prérequis nécessaire

Modalités pédagogiques

Distanciel ou Présentiel

Durée modifiable selon les besoins

Contenu de la formation

Module 1 : Sécurité des SI et du réseau d'entreprise

1. Vulnérabilités et menaces sur la sécurité des SI des entreprises

2. Panorama des attaques dans l'entreprise, vecteurs d'attaques contre les réseaux et infrastructures

3. Services de cybersécurité

4. Introduction à la cryptographie de point du vue Réseau

5. Notions de base d'une architecture sécurisée pour l'entreprise

6. Techniques d'authentification

Module 2 : Outils de sécurité et contrôle d'accès

1. Outils et mécanismes de sécurité :
    - Introduction aux concepts de sécurité suivants : IDS/IPS, Firewall, IP SEC, SSL/TLS, DMZ, SIEM, VLAN, Top Ten OWASP (web et API), outils de vulnérabilités (metasploit, …)
2. Contrôle d’accès, résilience :
    - Notions de bases du contrôle d’accès, introduction aux modèles de contrôle d’accès (RBAC, DAC, MAC, …), IAM, PAM, SOC, PDIS…

Module 3 : Sécurité des technologies modernes de l’entreprise

1. Sécurité dans le Cloud
    - Principes et modèles du cloud, vulnérabilités et attaques dans le cloud/big data, cycle de vie, techniques d’anonymisation, solution de sécurité
2. Blockchains
    - Principes de Blockchains, Blockchain publique et prive, algorithmes de consensus, smart contracts
3. WiFi, IoT, systèmes connectés et embarqués
    - Architectures, vulnérabilités, et solutions de sécurité

Évaluation des acquis

Les acquis des apprenants seront évalués au travers d’exercices réalisés tout au long de la formation.

Attestation de formation

Une attestation de formation est transmise aux apprenants à l’issue de la formation professionnelle. Elle certifie le suivi de la formation et l’acquisition des compétences.

Satisfaction des apprenants

Au terme de la formation, les apprenants renseigneront un formulaire de satisfaction.

Financements

Le plan de développement des compétences