



Mise à jour févr. 2025

# Les essentiels de la cybersécurité

21 juil.-25 juil.  
18 août-22 août  
01 sept.-05 sept.  
17 nov.-21 nov.

Nantes / Rennes : 3350 € HT  
Brest / Le Mans : 3350 € HT  
Certification : NON

**Durée** 5 jours (35 heures)

« Délai d'accès maximum 1 mois »

## OBJECTIFS PROFESSIONNELS

- Présentation des Cyber-menaces actuelles et sites de référence sur la cybersécurité
- Directives et exigences de conformité
- Cyber rôles nécessaires à la conception de systèmes sûrs
- Cycle des attaques processus de gestion des risques
- Stratégies optimales pour sécuriser le réseau d'entreprise
- Zones de sécurité et solutions standards de protection

## PARTICIPANTS

- Professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en sécurité

## PRE-REQUIS

- Connaissances en réseaux TCP/IP

## MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Remise d'un support de cours.

## MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

## MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

## MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré. Nous préconisons 4 personnes maximum par action de formation en classe à distance

## ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

## PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

**A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP**

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

**Programme de formation****Le champ de bataille (02h45)**

- La croissance d'Internet dans le monde entier
- Principes et objectifs de sécurité
- Terminologie des menaces et de l'exposition
- Documents et procédures de gestion des risques

**Structure de l'Internet et TCP/IP (01h45)**

- Normes de conformité juridique
- Internet Leadership IANA
- Modèle TCP/IP

**Évaluation de la vulnérabilité et outils (01h45)**

- Vulnérabilités et exploits
- Outils d'évaluation de la vulnérabilité
- Techniques d'attaques avancées, outils et préventions

**Sensibilisation à la cyber sécurité (01h00)**

- Ingénierie sociale : objectifs de l'ingénierie sociale, cibles, attaque, hameçonnage
- Sensibilisation à la cyber sécurité : politiques et procédures

**Cyber-attaques : Footprinting et scannage (01h45)**

- Footprinting
- Identification du réseau cible et sa portée
- Techniques de scannage de port

**Cyberattaques : effraction (01h00)**

- Attaque des mots de passe, escalade des privilèges
- Authentification et décodage du mot de passe

**Cyberattaques : Porte dérobée et cheval de Troie****(Backdoor and Trojans) (02h15)**

- Logiciels malveillants, Cheval de Troie, Backdoor et contre-mesures
- Communications secrètes
- Logiciel anti-espion
- Pratiques de lutte contre les logiciels malveillants

**Évaluation et gestion des risques cybernétiques (02h15)**

- Actifs protégés : CIA Triad
- Processus de détermination de la menace
- Catégories de vulnérabilités
- Actifs de l'entreprise vs risques

**Gestion des politiques de sécurité (01h00)**

- Politique de sécurité
- Références de politiques

**Sécurisation des serveurs et des hôtes (02h15)**

- Types d'hôtes
- Directives de configuration générale et correctifs de sécurité
- Renforcement des serveurs et périphériques réseau
- Renforcement de l'accès sans fil et sécurité des VLAN

**Sécurisation des communications (01h00)**

- Application de la cryptographie au modèle OSI
- Tunnels et sécurisation des services

**Authentification et solutions de chiffrement (02h15)**

- Authentification par mot de passe de systèmes de chiffrement
- Fonctions de hachage
- Avantages cryptographiques de Kerberos
- Composants PKI du chiffrement à clef symétrique, du chiffrement asymétrique, des signatures numériques

**Pare-feu et dispositifs de pointe (01h45)**

- Intégration de la sécurité générale
- Prévention et détection d'intrusion et défense en profondeur
- Journalisation

**Analyse criminalistique (01h00)**

- Gestion des incidents
- Réaction à l'incident de sécurité

**Reprise et continuité d'activité (02h15)**

- Types de catastrophes et Plan de reprise d'activité (PRA)
- Haute disponibilité
- Documentation de collecte de données
- Plan de Reprise d'Activité et Plan de Continuité d'Activité

## Cyber-révolution (00h30)

- Cyberforces, Cyberterrorisme et Cybersécurité : crime, guerre ou campagne de peur ?

## LABS (08h30)

- Lab 1 : Installation du lab
- Lab 2 : Comprendre TCP/IP
- Lab 3 : Evaluation de la vulnérabilité
- Lab 4 : Sensibilisation à la cybersécurité
- Lab 5 : Scannage
- Lab 6 : Cyber-attaques et mots de passe
- Lab 7 : Cyber-attaques et portes dérobées
- Lab 8 : Évaluation des risques
- Lab 9 : Stratégies de sécurité
- Lab 10 : Sécurité hôte
- Lab 11 : Communications secrètes
- Lab 12 : Authentification et cryptographie
- Lab 13 : Snort IDS
- Lab 14 : Analyse criminalistique
- Lab 15 : Plan de continuité des affaires