+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 30/09/2025

S'inscrire

Formation Parcours introductif à la Cybersécurité

10 jours (70 heures)

PRÉSENTATION

Notre formation « Parcours introductif à la cybersécurité » s'adresse aux techniciens et administrateurs systèmes et réseaux qui souhaitent acquérir une vision globale et opérationnelle de la sécurité informatique et évoluer vers les métiers de la cybersécurité.

Au fil de ces dix journées, vous développerez une vision globale de la cybersécurité et de son environnement, en découvrant les enjeux économiques et sociétaux, les acteurs de la menace et l'écosystème institutionnel et réglementaire. Vous apprendrez à connaître et utiliser les principaux référentiels, normes et outils de cybersécurité (ISO, NIST CSF, CIS Controls, ANSSI, SIEM, EDR, scanners de vulnérabilités), tout en intégrant les obligations juridiques essentielles (RGPD, NIS2, LPM).

La formation vous permettra également d'appréhender les différents métiers liés à la cybersécurité et leurs trajectoires professionnelles, afin de mieux situer votre rôle et vos perspectives d'évolution dans ce domaine en forte croissance. Vous serez formés à identifier les principaux risques et menaces (malwares, ransomwares, phishing, APT, erreurs de configuration Cloud/IoT) et à mettre en place les mesures de protection adaptées (défense en profondeur, Zero Trust, IAM, supervision, gestion d'incidents).

Enfin, vous apprendrez à intégrer les bonnes pratiques de sécurité informatique dans vos activités quotidiennes, à sensibiliser les utilisateurs et à contribuer à la construction d'une véritable culture cybersécurité au sein de votre organisation.

À l'issue de la formation, vous serez capable de mettre en œuvre les principes fondamentaux, les normes et les outils de cybersécurité dans un cadre opérationnel.

OBJECTIFS

- Détenir une vision globale de la cybersécurité et son environnement (enjeux, écosystème…)
- Connaître les différents référentiels, normes et outils de la cybersécurité
- Appréhender les métiers liés à la cybersécurité

- Connaître les obligations juridiques liées à la cybersécurité
- Comprendre les principaux risques et menaces ainsi que les mesures de protection
- Identifier les bonnes pratiques en matière de sécurité informatique

PUBLIC VISÉ

- Toutes personnes souhaitant s'orienter vers les métiers de la cybersécurité
- Les techniciens et administrateurs systèmes et réseaux

Pré-requis

Avoir des connaissances générales dans les systèmes d'information et connaître le guide d'hygiène sécurité de l'ANSSI

PROGRAMME DE NOTRE FORMATION : PARCOURS INTRODUCTIF À LA CYBERSÉCURITÉ

[Jour 1 - Matin]

Introduction et contexte

- Pourquoi la cybersécurité est stratégique : enjeux économiques & sociétaux
- Incidents majeurs récents et impacts métiers
- Acteurs de la menace : cybercrime, hacktivisme, espionnage

[Jour 1 - Après-midi]

Fondamentaux de la sécurité

- Modèle CIA (Confidentialité, Intégrité, Disponibilité)
- Surfaces d'attaque et vecteurs d'intrusion
- « Misuse cases » et approche par les risques
- Rappels sur la cryptographie : chiffrement, hachage, signatures, certificats
- Atelier pratique : Cartographier les actifs critiques d'une organisation.

Écosystème juridique et cadre légal

- ANSSI, CERT-FR, ENISA, CNIL : rôles & interactions
- Panorama RGPD, NIS2, LPM : obligations clés
- Responsabilités juridiques & sanctions
- Atelier pratique : Etude de cas. Impacts d'une violation RGPD.

[Jour 2 - Matin]

Référentiels internationaux

- ISO/IEC 27001 & 27002, ISO 27035 (incidents)
- NIST CSF & CIS Controls : comparatif
- Guide d’hygiène informatique de l’ANSSI

[Jour 2 - Après-midi]

Gouvernance et PSSI

- Élaborer une Politique de Sécurité (PSSI)
- Rôles, responsabilités, comités de sécurité
- Indicateurs & tableaux de bord
- Atelier pratique : Créer une mini-PSSI pour une PME.

Conformité et audit

- Méthodologie d’audit sécurité
- Gestion de la dette de sécurité
- Plan de remédiation et suivi
- Atelier pratique : Simulation d’un audit basique.

[Jour 3 - Matin]

Métiers de la cybersécurité

- Panorama des rôles : RSSI, analyste SOC, pentester, auditeur, forensic
- Interactions clés : équipes internes, prestataires, CERT/ANSSI
- Compétences essentielles selon les filières (techniques, organisationnelles, transverses)
- Atelier pratique : cartographier un parcours professionnel en cybersécurité.

[Jour 3 - Après-midi]

Certifications & trajectoires

- Voies professionnelles : offensive (pentest), défensive (SOC/Blue Team), gouvernance (RSSI/consultant)
- Panorama certifications : Security+, eJPT, CEH (débutants), CISSP, OSCP, ISO Lead (avancés)
- Construire son plan de carrière : étapes, spécialisation, veille continue

Outils du quotidien

- SIEM, EDR, IDS/IPS, IAM
- Scanners de vulnérabilités (SCA/SAST/DAST)
- Alerting, corrélation & triage
- Atelier pratique : Prise en main d’un scanner simple.

[Jour 4 - Matin]

Typologie des menaces

- Malware, ransomware, APT, supply chain
- Ingénierie sociale & risques humains
- IoT, mobilité, cloud : nouveaux vecteurs
- Atelier pratique : Simulation de phishing & débrief.

[Jour 4 - Après-midi]

Vulnérabilités techniques

- Système, réseau, applicatif
- Cycle de vie d’une CVE
- Exemples : Heartbleed, Log4Shell

Analyse & gestion des risques

- Présentation rapide : EBIOS RM, MEHARI, FAIR
- Probabilités, impacts, appétence au risque
- Cartographie & priorisation
- Atelier pratique : Mini-EBIOS sur un SI fictif.

[Jour 5 - Matin]

Sécurité périmétrique

- Pare-feu, proxy, filtrage web/mail
- VPN & accès distants
- Bastion et DMZ
- Atelier pratique : Configurer un pare-feu logiciel.

[Jour 5 - Après-midi]

Défense en profondeur & Zero Trust

- Principes de couches successives
- Micro-segmentation & PoLP
- Contrôles d’accès dynamiques

Supervision & détection

- Collecte & corrélation de logs
- SIEM, SOC, UEBA
- Use cases de détection
- Atelier pratique : Analyser un journal système.

[Jour 6 - Matin]

Sécurité applicative : principes clés

- Principes du Secure Coding
- Comprendre les principales failles (OWASP Top 10)
- Validation d’entrées & gestion des erreurs
- Sessions & authentification forte
- Logging & chiffrement essentiels
- Présentation d’outils : OWASP ZAP, Burp Suite
- Atelier pratique : Prise en main d’OWASP Juice Shop (application volontairement vulnérable) et scan automatisé avec ZAP.

[Jour 6 - Après-midi]

Maîtriser les vulnérabilités critiques

- A01 Broken Access Control à A10
- Mécanismes de prévention & remédiation
- Checklists & revues de code
- Atelier pratique : Mapping OWASP sur une application de test. Mettre en pratique le OWASP Top 10 sur une application vulnérable, en reliant chaque faille rencontrée à sa catégorie et aux contre-mesures associées.

DevSecOps & « Shift Left »

- Principe du « Shift Left » : intégrer la sécurité dès les premières étapes
- Cycle de développement sécurisé (Secure SDLC)
- Introduction aux outils d’analyse automatique (SAST, DAST, SCA)
- Qualité & validation continue (tests, gates de sécurité)

[Jour 7 - Matin]

Sécurité du Cloud

- Partage de responsabilité (IaaS/PaaS/SaaS)
- Erreurs de configuration fréquentes
- Durcissement & surveillance
- Atelier pratique : Audit d'un environnement cloud simulé.

[Jour 7 - Après-midi]

Introduction aux Conteneurs & à Kubernetes

- Introduction : déploiement rapide et flexible, mais nouvelles surfaces d'attaque (images, secrets, réseau)
- Durcissement des images (hardening) : utiliser des images minimales, mises à jour et scannées pour vulnérabilités
- Gestion sécurisée des secrets : mots de passe, clés et certificats protégés
- Politiques réseau : contrôle et limitation des communications inter-conteneurs
- Bonnes pratiques de déploiement : moindre privilège, isolation des workloads, supervision continue

IAM & identité

- MFA, SSO, OAuth 2.1, OIDC
- Rôles, RBAC/ABAC
- Zero Trust appliqué aux identités
- Atelier pratique : Configurer un MFA sur un service cloud.

[Jour 8 - Matin]

Gestion d'incidents

- NIST SP 800-61 : workflow complet
- Playbooks & organisation CERT/CSIRT
- Automatisation & SOAR (principes)
- Atelier pratique : Exercice table-top d'incident.

[Jour 8 - Après-midi]

Forensic & preuves

- Chaîne de conservation & légalité
- Journalisation et timeline
- Outils & procédures

Communication de crise

- Interne vs externe : messages & canaux
- Rôle du management & IT
- Notifications aux autorités (CNIL, etc.)
- Atelier pratique : Simulation de communication post-incident.

[Jour 9 - Matin]

Facteur humain

- Mécanismes d’ingénierie sociale
- Programmes de sensibilisation continue
- Cas : phishing, prétexting, tailgating

[Jour 9 - Après-midi]

Bonnes pratiques utilisateurs

- Mots de passe & MFA
- Hygiène numérique (MAJ, sauvegardes)
- Postes de travail & mobiles
- Atelier pratique : Créer un kit de sensibilisation.

Culture cybersécurité

- Intégration à la culture d’entreprise
- Rituels, challenges, gamification
- Mesure de maturité & ROI
- Atelier pratique : Concevoir une campagne annuelle.

[Jour 10 - Matin]

Révisions & panorama global

- Points clés & synthèse transversale
- Retours d’expérience des participants
- Q/R guidée et auto-évaluation

[Jour 10 - Après-midi]

Étude de cas complète

- Scénario : entreprise victime d’un ransomware
- Analyse du vecteur d’attaque & confinement
- Plan de réponse & remédiations
- Atelier pratique : Gestion d’un incident de bout en bout (technique, organisationnel, communication)

Perspectives et parcours

- Opportunités métiers & spécialisations en cybersécurité
- Labs recommandés pour progresser : TryHackMe, HackTheBox, Blue Team Labs, LetsDefend, OWASP Juice Shop
- Recommandation d’un plan d’action individuel sur 90 jours (progression guidée via labs)

Formation Pentest Web

Formation Keycloak

Formation Keycloak Avancé

Formation Android Sécurité et Pentest

Formation OWASP Java

Formation OWASP avec .NET

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son

inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.