Ref. SEC-CYBINTRO

Parcours introductif à la cybersécurité

10 jours (70 heures) | Perfectionnement | Présentiel ou classe à distance

à partir de
6 000 € HT par personne (TVA en vigueur)

Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Mettre en oeuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Etudiants en sécurité informatique, administrateurs système, développeurs, chefs de projets.

Prérequis

Avoir des connaissances générales en système et système d'information.

Programme

1 Pendant votre formation

Parcours introductif à la cybersécurité

Phase 1 : Etat de l'art cyber

Jour 1 - Matin

Les tendances de la cybercriminalité

- L'évolution de la cybercriminalité en France et dans le monde
- L'impact économique de la cybercriminalité
- Le modèle économique HaaS (Hacking as a Service)
- Caractéristiques, coûts, usages

Base de la sécurité de l'information

- SSI et SI
- DICP et les critères de sécurité
- La sécurité en profondeur
- La "security by design"
- Approche par les risques
- Vulnérabilités et menaces

Gestion des cyberattaques

- Tests d'intrusion, mesure d'anticipation incontournable
- SOC (Security Operation Center)
- La gestion des incidents
- Les plans de continuité d'activité
- Métier de la gouvernance cyber
- Les exercices Red Team, Blue Team et Purple Team
- Recourir à une société spécialisée de détection des incidents

Jour 1 - Après-midi

Gestion d'incidents et riposte face à une cyberattaque

- La notion de preuve dans le monde informatique
- Recherche, collecte et structuration de preuves
- Méthodologie de gestion d'incidents
- Les CERT (Computer Emergency Response Teams) : des organismes qui facilitent la tâche
- Le cadre juridique des ripostes à une cyberattaque
- Organiser et gérer une cellule de crise
- Importance de la veille en cybersécurité
- Gestion des vulnérabilités et patch management

Jour 2 - Matin

Identifier les acteurs de la lutte contre la cybercriminalité

- Cyber-délits en France et en Europe : quel dispositif ?
- Les services spécialisés du ministère de l'Intérieur
  - OCLCTIC, BEFTI, IRCGN, BFMP, DGSI...

Les bonnes pratiques

- Gouvernance de la cybersécurité
- Défense en profondeur
- Gestion des incidents de cybersécurité

Jour 2 - Après-midi

Loi, normes, référentiels, organismes qui régissent la cybersécurité

- RGPD
- Article 321 du code pénal
- ISO/IEC 27001/2
- Guide d'hygiène ANSSI, CIS, MITRE
- Prestataires certifiés obligatoires (PDIS, PRIS)
- Audit de sécurité par l'ANSSI
- Auditeurs certifiés (PASSI, LPM)
- Le rôle spécifique de l'ANSSI, la CNIL, l'ARJEL et l'ENISA
- Directive européenne : Network and Information Security
- Règlement européen : Cybersecurity Act
- Loi de programmation militaire (2016)
- Les organismes de l'Union européenne
- Les associations
- Les entreprises privées au service de la lutte contre la cybercriminalité

Phase 2 : Introduction aux différents métiers de la cyber offensive
Jour 3 - Matin

La sécurité offensive et le pentesting

- Principes de la sécurité de l'information
- Les différentes phases d'une attaque
- Définition d'un test d'intrusion
- Aspects légaux et réglementaires liés aux tests d'intrusion
- Méthodes et framework pour un test d'intrusion

Exemples de travaux pratiques (à titre indicatif)

- *Framework pentest*
- *Questionnaire de pré-engagement*
- *Rédaction d'un contrat de pré-engagement*

Préparer son test d'intrusion

- Préparation d'une machine pour test d'intrusion
- Automatisation et scripting
- Outils matériel connus
- Templating de documents

Exemples de travaux pratiques (à titre indicatif)

- *Rubber Ducky*
- *Suivi test d'intrusion*

Collecte d'informations

- Ingénierie des sources publiques (OSINT)
- Relevé passif et actif d'informations sur l'organisation cible

Exemples de travaux pratiques (à titre indicatif)

- *Présentation des outils d'OSINT*
- *Relevé d'informations et reconnaissance*

Jour 3 - Après-midi

Enumération de l'infrastructure

- Enumération du périmètre
- Evasion sur une infrastructure sécurisée
- Enumération des protocoles

Exemples de travaux pratiques (à titre indicatif)

- *Présentations des outils d'énumération*
- *Enumération de l'infrastructure*

Analyse des vulnérabilités

- Scan de vulnérabilités
- Présentation des différents outils
- Les vulnérabilités connues

Exemples de travaux pratiques (à titre indicatif)

- *Présentation OpenVAS*
- *Identification des vulnérabilités*

Jour 4 - Matin

Exploitation

- Recherche d'exploits
- Présentation des outils / frameworks d'attaques
- Déploiement et exécution de charges
- Ecoute passive et active des infrastructures
- Attaque par force brute (bruteforce attack)

Exemples de travaux pratiques (à titre indicatif)

- *Présentation metasploit*
- *Exploitation des vulnérabilités*

Jour 4 - Après-midi

Post-exploitation

- Désactivation des éléments de traçabilité
- Elévation de privilèges (méthodes, outils, vulnérabilités Linux)
- Etude des persistances (ADS, base de registre, planificateur de tâches, services)
- Mouvements latéraux et pivoting
- Nettoyage des traces

Phase 3 : Introduction aux différents métiers de la cyber défensive
Jour 5 - Matin

Métiers, support de travail et référentiels

- La Blue Team
- Ingénieur en sécurité, intégrateur de solution, le SOC, le CSIRT
- Le SOC (Security Operations Center) au coeur de la Blue Team
- Audit de la cybersécurité des systèmes d'information

Durcissement des infrastructures Windows

- Durcissement des postes et serveurs
- Durcissement des protocoles réseaux
- ATA, IA et threat intelligence
- Journalisation et surveillance avancée

Exemples de travaux pratiques (à titre indicatif)

- *Mettre en oeuvre un renforcement de sécurité en environnement Microsoft*
- *Auditer son architecture et préparer un plan de contre-mesure*

Jour 5 - Après-midi

Ouverture à l'investigation numérique avec la collecte de données

- Les outils du marché (Kape, Arsenal, FTK imager, Plaso, Hindsight…)
- Collecte des données physiques et virtualisation
- Présentation du Lab

Exemple de travaux pratiques (à titre indicatif)

- *Collecte de données (en continu)*

Jour 6 - Matin et après-midi

Recherche d'artéfacts et reporting

- Différents artéfacts Internet
  - Pièces jointes
  - Open/Save MRU (Most Recently Used)
  - Flux ADS (Alternate Data Stream) Zone.Identifier
  - Téléchargements
  - Historique Skype
  - Navigateurs Internet
  - Historique
  - Cache
  - Sessions restaurées
  - Cookies
- Différents artéfacts d'exécution
  - UserAssist
  - Timeline Windows 10
  - RecentApps
  - Shimcache
  - Jumplist
  - Amcache.hve
  - BAM/DAM
  - Last-Visited MRU
  - Prefetch

Exemples de travaux pratiques (à titre indicatif)

- *Analyse d'un disque*
- *Chaîne de custody et création d'un rapport sur une étude de cas*

Phase 4 : Introduction aux différents métiers de la cyber (risk manager)
Jour 7 - Matin

Etat de l'art du risk management

- Quelle est la définition d'un risque ?
- Quelle vision du risque ?
- L'ISO 31000
- L'AMRAE, le Club EBIOS
- Qu'est-ce qu'un bon risk manager ?
- Sensibilisation des dirigeants aux risques cybers

Créer un programme de gestion des risques

- L'importance de contextualiser
- Contexte interne, externe
- Recette du risque

- Assets
- Vulnérabilités
- Menaces
- Mesures
- Scénarios

Exemple de travaux pratiques (à titre indicatif)

- *A l'aide d'une étude de cas, identifier les scénarios de risques, vulnérabilités et menaces*

Jour 7 - Après-midi

Analyse et estimation des risques

- Approche qualitative vs quantitative
- Les différentes méthodes de calcul des risques
- Calcul des risques

Exemple de travaux pratiques (à titre indicatif)

- *A l'aide d'une étude de cas, analyser et estimer les scénarios de risques*

Jour 8 - Matin

EBIOS

- Différence entre EBIOS 2010 et EBIOS Risk Manager
- Notions de socle de sécurité
- Visions ateliers
- Les 5 ateliers

MEHARI

- Le Clusif
- Fonctionnement de MEHARI
- Les différentes phases de la méthode MEHARI

OCTAVE

- Les trois phases d'OCTAVE
  - Vue organisationnelle : création des profils de menaces sur les biens de l'entreprise
  - Vue technique : identification des vulnérabilités d'infrastructure
  - Développement de la stratégie : analyse de risques, mise en place des mesures de sécurité

Jour 8 - Après midi

La méthode Bow-Tie

- Représenter les relations entre les dangers, leurs causes et leurs effets
- Evaluer la contribution de chaque cause et la gravité de chaque risque
- Positionner des barrières de prévention et de protection

- Evaluer les facteurs aggravants diminuant l'efficacité des barrières
- Evaluer la robustesse et la contribution des barrières à l'atténuation des risques
- Evaluer l'impact de ces barrières sur la cotation générale du risque

Phase 5 : Introduction aux différents métiers de la cyber (assistance au RSSI)
Jour 9 - Matin

Métier de RSSI (Responsable de la Sécurité des Systèmes d'Information)

- Les différentes tâches d'un RSSI
- RSSI et non-directeur cyber
- Les associations des RSSI
- Quelle fonction pour l'assistant RSSI
- Conformité et gestion des risques

Savoir interpréter les référentiels, normes du marché

- ISO/IEC 27001/2
- Quelle méthode de travail pour implémenter la norme ISO
- Gestion des risques et programme GDR
- Comment monter une PSSI (Politique de Sécurité du Système d'Information)

Exemple de travaux pratiques (à titre indicatif)

- *Exemple de PSSI*

Jour 9 - Après-midi

NIST Cybersecurity Framework

- Les phases et les activités du NIST Cybersecurity Framework
  - Identify
  - Protect
  - Detect
  - Respond

Jour 10 - Matin

Guide d'hygiène de l'ANSSI

- 42 règles de sécurité
- Comment identifier la maturité
- Modèle de maturité avec CMMI (Capability Maturity Model Integration)
- Recommandations de l'ANSSI
- Comprendre les schémas de labellisation

Exemple de travaux pratiques (à titre indicatif)

- *Créer un fichier de suivi*

Jour 10 - Après-midi

Création d'un tableau de bord

- Quels indicateurs
- Maturity model vs process model
- Créer ses outils de veille

Quid de la gouvernance du DevOps

- Quel modèle pour la sécurité d'application
- SDLC de Microsoft
- Stride, threat modeling et approche SSI du DevSec
- Les outils
  - L'OWASP ASVS, SAMM, code review

La sécurité du monde industriel

- Les enjeux
- Différences entre SIE et SII
- Recommandations de l'ANSSI pour les industriels
- Mode opératoire des attaquants et APT sur les réseaux industriels

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.
Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques…) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 4 janvier 2027 au 15 janvier 2027 (10 jours / 70 heures)

À distance

Du 4 janvier 2027 au 15 janvier 2027 À distance

- 4 janvier 2027 ---------- 9h00 - 17h00
- 5 janvier 2027 ---------- 9h00 - 17h00
- 6 janvier 2027 ---------- 9h00 - 17h00
- 7 janvier 2027 ---------- 9h00 - 17h00
- 8 janvier 2027 ---------- 9h00 - 17h00
- 9 janvier 2027 ---------- 9h00 - 17h00
- 10 janvier 2027 ---------- 9h00 - 17h00
- 11 janvier 2027 ---------- 9h00 - 17h00
- 12 janvier 2027 ---------- 9h00 - 17h00
- 13 janvier 2027 ---------- 9h00 - 17h00
- 14 janvier 2027 ---------- 9h00 - 17h00
- 15 janvier 2027 ---------- 9h00 - 17h00