GROUPE MDA

PROGRAMME DE FORMATION

Formation Cybersécurité

Programme individuel 100 % personnalisé · séances d'une heure en hybride avec votre expert dédié. Construire les bons réflexes de sécurité numérique à partir de vos usages réels, sans jargon technique superflu.

DURÉE
65 séances · 65 h

TARIF HT
À partir de 9 750 € HT

FORMAT
Hybride

CATÉGORIE
Cybersécurité

DURÉE	TARIF HT	FORMAT	SESSIONS
65 séances · 65 h	**À partir de 9 750 € HT**	**Hybride**	**65 séances**

CUMUL DE VOTRE SÉLECTION

4 niveaux sélectionnés · **65 séances individuelles** de **1 heure** en visio · **65 heures** au total · **À partir de 9 750 € HT** .

01 Présentation

séances individuelles. Un seul expert. Zéro cours générique.

La cybersécurité n'est pas qu'un sujet pour les DSI. Chaque collaborateur qui ouvre un email, se connecte à un WiFi public ou partage un fichier représente un point d'entrée potentiel pour une attaque. Ce programme débutant transforme vos usages numériques quotidiens en pratiques sécurisées, sans vous noyer dans la théorie.

Avant la première séance, votre expert dédié passe 30 minutes avec vous pour cartographier vos outils, vos habitudes et vos risques réels. Il adapte ensuite l'ensemble des séances individuelles à votre contexte précis : secteur d'activité, stack applicative, niveau de maturité. Si vous utilisez Gmail et Google Drive, on travaille sur Gmail et Google Drive. Si votre entreprise est sous contrainte RGPD, on y consacre les séances nécessaires.

Chaque heure de travail avec votre expert produit un livrable concret : liste de mots de passe à changer, politique de partage à mettre en place, procédure d'alerte à rédiger. Pas de slides théoriques envoyées par email après la séance.

Ce programme couvre les fondamentaux essentiels : reconnaître et déjouer le phishing, sécuriser son poste et ses appareils mobiles, gérer ses accès et ses mots de passe, comprendre les obligations RGPD liées à votre rôle, savoir quoi faire en cas d'incident. À l'issue des séances individuelles, vous disposez d'une routine de cyberhygiène personnalisée et d'un plan d'action concret pour votre contexte professionnel.

Financement possible via OPCO, CPF ou AGEFICE selon votre statut et les critères d'éligibilité en vigueur.

02 Objectifs pédagogiques

À l'issue de la formation, le stagiaire est capable de :

- Identifier les principales menaces cyber et comprendre comment elles fonctionnent
- Adopter une gestion rigoureuse des mots de passe et de l'authentification
- Sécuriser son poste de travail, ses appareils mobiles et sa connexion réseau
- Reconnaître et déjouer les tentatives de phishing et d'ingénierie sociale
- Comprendre ses obligations RGPD liées à la sécurité des données
- Construire une routine quotidienne de cyberhygiène adaptée à son contexte
- Savoir réagir et signaler un incident de sécurité efficacement

03 Public & prérequis

PUBLIC CONCERNÉ

Collaborateurs non spécialistes souhaitant sécuriser leurs usages numériques professionnels. Dirigeants de TPE/PME, assistants, commerciaux, chefs de projet · tout profil exposé au risque cyber sans formation préalable. Aucun prérequis technique requis.

PRÉREQUIS

Aucun prérequis technique. Accès à un ordinateur connecté et aux outils numériques utilisés au quotidien dans votre contexte professionnel.

04 Programme par séance

65 séances individuelles d'1 heure en visio avec votre expert dédié. Chaque séance débute par un point d'avancement et se termine par un livrable concret · pas de cours générique.

Programme cumulé sur 4 niveaux : Débutant, Intermédiaire, Confirmé, Expert.

NIVEAU DÉBUTANT

SÉANCE 01 Séance 1 · Audit de vos usages et cadrage personnalisé — 1H

- Cartographie de vos outils et de vos pratiques numériques
- Identification de vos 3 risques prioritaires
- Adaptation du programme aux séances individuelles suivantes

SÉANCE 02 Séance 2 · Panorama des menaces cyber actuelles — 1H

- Types d'attaques : phishing, ransomware, BEC, credential stuffing
- Comment les hackers choisissent leurs cibles
- Statistiques sectorielles adaptées à votre activité

SÉANCE 03 Séance 3 · Anatomie d'une attaque : du clic à la compromission — 1H

- Simulation commentée d'une attaque phishing réelle
- Les étapes de la kill chain simplifiée
- Pourquoi les bonnes pratiques coupent la chaîne

SÉANCE 04

Séance 4 · Mots de passe et authentification

1H

- Gestionnaire de mots de passe : choix et mise en place
- Authentification à deux facteurs : méthodes et priorités
- Livrable : politique de mots de passe personnelle

SÉANCE 05

Séance 5 · Sécurité du poste de travail

1H

- Mises à jour OS et applications : pourquoi et comment
- Chiffrement du disque dur
- Antivirus et EDR : ce qu'il faut vraiment installer

SÉANCE 06

Séance 6 · Reconnaître et déjouer le phishing

1H

- Checklist de détection sur vos emails réels
- Spear phishing et usurpation d'identité
- Livrable : procédure interne de signalement

SÉANCE 07

Séance 7 · Sécurité réseau et déplacements

1H

- WiFi public : risques et bonnes pratiques
- VPN : pourquoi, lequel, comment l'utiliser
- Hotspot mobile versus réseau d'entreprise

SÉANCE 08

Séance 8 · Gestion des données sensibles

1H

Classification des données de votre organisation

- Partage sécurisé de fichiers (Drive, WeTransfer, email)
- Suppression sécurisée et gestion des archives

SÉANCE 09

Séance 9 · Cloud et stockage sécurisé

1H

- Droits d'accès et partage sur votre cloud pro
- Synchronisation entre appareils : risques méconnus
- Livrable : audit de vos partages et permissions actives

SÉANCE 10

Séance 10 · Appareils mobiles et télétravail

1H

- Sécurisation du smartphone professionnel
- BYOD : risques et règles minimales
- Poste à domicile : isoler le pro du perso

SÉANCE 11

Séance 11 · RGPD et responsabilités individuelles

1H

- Ce que la loi impose à chaque collaborateur
- Violations de données : délais de notification et conséquences
- Livrable : fiche réflexe RGPD adaptée à votre poste

SÉANCE 12

Séance 12 · Réseaux sociaux et identité professionnelle

1H

- Fuites d'information via LinkedIn, Twitter, Facebook
- OSINT : ce que vos données publiques révèlent

Paramètres de confidentialité à configurer

SÉANCE 13 · Séance 13 · Ingénierie sociale et manipulation — 1H

- Scénarios réels : vishing, smishing, pretexting
- Techniques de manipulation psychologique utilisées par les attaquants
- Réflexes de vérification avant toute action sensible

SÉANCE 14 · Séance 14 · Sécurité des outils collaboratifs — 1H

- Teams, Slack, Drive, Notion : paramètres de sécurité clés
- Gestion des bots et intégrations tierces
- Risques liés aux réunions visio et au partage d'écran

SÉANCE 15 · Séance 15 · Sauvegardes et continuité personnelle — 1H

- Stratégie 3-2-1 adaptée à votre contexte
- Test de restauration : souvent oublié, toujours utile
- Plan personnel de reprise après incident

SÉANCE 16 · Séance 16 · Signalement et gestion des incidents — 1H

- Quoi signaler, à qui, dans quel délai
- Collecte des preuves sans contaminer la scène
- Votre rôle dans la chaîne de réponse interne

SÉANCE 17

Séance 17 · Simulation d'attaque phishing

1H

- Exercice pratique sur un email fictif préparé par l'expert
- Débriefing sur les signaux manqués
- Mise à jour de votre checklist de détection

SÉANCE 18

Séance 18 · Emails avancés : BEC et fraude au président

1H

- Anatomie d'une fraude au virement
- Processus de vérification à 2 canaux
- Livrable : procédure d'alerte adaptée à votre organisation

SÉANCE 19

Séance 19 · Construction de votre routine de cyberhygiène

1H

- Checklist quotidienne, hebdomadaire, mensuelle
- Outils gratuits de surveillance (HaveIBeenPwned, etc.)
- Veille sécurité : 3 sources pour rester à jour sans y consacrer plusieurs heures par jour

SÉANCE 20

Séance 20 · Bilan et plan d'action post-formation

1H

- Consolidation des apprentissages clés
- Évaluation finale sur cas réel apporté par le stagiaire
- Plan d'action personnalisé à 30 jours

NIVEAU INTERMÉDIAIRE

SÉANCE 21

Séance 1 · Audit de l'existant et cartographie des risques

1H

- Inventaire des actifs numériques (hardware, software, données)
- Identification des points d'entrée et des flux sensibles
- Priorisation des risques selon votre contexte

SÉANCE 22

Séance 2 · Gestion des identités et des accès (IAM)

1H

- Principe du moindre privilège appliqué à votre annuaire
- Revue des accès actifs et suppression des comptes orphelins
- Livrable : matrice des droits d'accès documentée

SÉANCE 23

Séance 3 · Gestion des mots de passe et MFA à l'échelle

1H

- Déploiement d'un gestionnaire de mots de passe en équipe
- Authentification multi-facteur : choix des méthodes par profil
- Politique de mots de passe adaptée à votre annuaire

SÉANCE 24

Séance 4 · Sécurité réseau : firewall, segmentation, DMZ

1H

- Configuration du pare-feu : règles essentielles à auditer
- Segmentation réseau pour limiter le lateral movement
- Logs réseau : ce qu'il faut surveiller en priorité

SÉANCE 25

Séance 5 · Patch management et gestion des vulnérabilités

1H

Inventaire des systèmes non patchés et priorisation CVE

- Processus de mise à jour structuré (test, déploiement, validation)
- Outils gratuits de scan de vulnérabilités (OpenVAS basics)

SÉANCE 26

Séance 6 · Détection des intrusions et monitoring

1H

- Centralisation des logs (syslog, Windows Event Viewer)
- Indicateurs d'alerte à surveiller en priorité
- Mise en place d'alertes basiques sans SIEM dédié

SÉANCE 27

Séance 7 · Réponse à incident : procédures et communication

1H

- Construction de votre procédure de réponse à incident
- Chaîne de communication interne et externe en cas de crise
- Livrable : playbook de réponse adapté à votre organisation

SÉANCE 28

Séance 8 · Sécurité applicative : bases de l'OWASP Top 10

1H

- Les 10 vulnérabilités web les plus critiques expliquées
- Audit basique de vos applications web exposées
- Checklist de sécurité pour vos développements ou achats SaaS

SÉANCE 29

Séance 9 · Sécurité du cloud (AWS, Azure, GCP, SaaS)

1H

- Matrice de responsabilité partagée selon votre hébergement

Audit de vos buckets, permissions et configurations cloud

- Livrable : politique de sécurité cloud documentée

SÉANCE 30 · Séance 10 · Plan de continuité et reprise après sinistre · 1H

- RTO / RPO : définir vos objectifs de reprise concrets
- Tests de restauration : protocole et fréquence
- Scénarios de sinistre adaptés à votre infrastructure

SÉANCE 31 · Séance 11 · Conformité RGPD niveau responsable de traitement · 1H

- Registre des activités de traitement : état et mise à jour
- Analyse d'impact (AIPD) : quand et comment
- Livrable : cartographie des données personnelles traitées

SÉANCE 32 · Séance 12 · Sensibilisation et formation des équipes · 1H

- Kit de sensibilisation adapté à votre secteur
- Animation d'un exercice phishing en interne
- Construction d'un plan de sensibilisation annuel

SÉANCE 33 · Séance 13 · Sécurité des API et des flux de données · 1H

- Inventaire des API exposées et des flux entrants/sortants
- Authentification des API : tokens, OAuth 2.0 basics
- Risques liés aux intégrations SaaS tierces

SÉANCE 34

Séance 14 · Simulation d'incident et test de votre plan

1H

- Exercice tabletop sur un scénario ransomware adapté à votre structure
- Identification des failles dans votre plan de réponse actuel
- Mise à jour du playbook suite aux résultats du test

SÉANCE 35

Séance 15 · Bilan et feuille de route sécurité

1H

- Consolidation de tous les livrables produits
- Priorisation des actions selon effort / impact
- Plan de renforcement à 6 mois avec indicateurs de suivi

NIVEAU CONFIRMÉ

SÉANCE 36

Séance 1 · Audit technique de votre infrastructure et gap analysis

1H

- Cartographie technique : systèmes, réseaux, services exposés
- Identification des failles architecturales prioritaires
- Priorisation des séances individuelles selon vos gaps réels

SÉANCE 37

Séance 2 · Architecture Zero Trust : principes et mise en oeuvre

1H

- Modèle Zero Trust : never trust, always verify
- Segmentation micro-périmétrique et microsegmentation réseau
- Livrable : schéma d'architecture cible pour votre réseau

SÉANCE 38

Séance 3 · Pentest interne : méthodologie et outils légaux

1H

- Nmap : reconnaissance et fingerprinting de l'infrastructure
- OpenVAS / Nessus Essentials : scan de vulnérabilités
- Interprétation des résultats et priorisation des corrections

SÉANCE 39

Séance 4 · SIEM : déploiement et tuning des règles de détection

1H

- Architecture d'un SIEM (Wazuh, Elastic SIEM basics)
- Collecte des logs : sources prioritaires, formats, normalisation
- Livrable : 10 règles de détection personnalisées pour votre SI

SÉANCE 40

Séance 5 · Threat intelligence opérationnelle

1H

- Sources d'IOC gratuites et payantes
- Intégration des IOC dans votre stack défensive
- Threat hunting basique : recherche proactive sur vos logs

SÉANCE 41

Séance 6 · Hardening des systèmes

1H

- Hardening Linux : CIS Benchmark appliqué à vos serveurs
- Windows Server : GPO de sécurité et audit des politiques
- Sécurisation des conteneurs Docker et Kubernetes basics

SÉANCE 42

Séance 7 · Active Directory : sécurisation et audit

1H

- Attaques AD courantes : Pass-the-Hash, Kerberoasting, DCSync
- BloodHound / PingCastle : audit de votre AD
- Livrable : plan de durcissement AD priorisé

SÉANCE 43

Séance 8 · DevSecOps : sécurité intégrée dans le CI/CD

1H

- Scan statique (SAST) et dynamique (DAST) dans la pipeline
- Gestion des secrets en pipeline : Vault, GitHub Secrets
- Audit des dépendances : SCA et gestion des CVE tiers

SÉANCE 44

Séance 9 · Analyse forensique post-incident

1H

- Acquisition d'une image disque et préservation des preuves
- Analyse mémoire : Volatility basics
- Timeline d'incident et rapport forensique synthétique

SÉANCE 45

Séance 10 · Cloud hybride : sécurité AWS / Azure / on-premise

1H

- IAM cloud : moindre privilège et revue des permissions
- Détection cloud : GuardDuty, Defender for Cloud, GCP SCC basics
- Sécurité du transit de données : VPN, PrivateLink, peering

SÉANCE 46

Séance 11 · Chiffrement avancé et infrastructure PKI

1H

PKI interne : CA racine, émission et révocation de certificats

- Chiffrement des données at rest et in transit
- Gestion du cycle de vie des certificats

SÉANCE 47

Séance 12 · Tests applicatifs : OWASP et Burp Suite

1H

- OWASP Top 10 : test manuel des 3 vulnérabilités prioritaires de vos apps
- Burp Suite Community : intercept, Repeater, Scanner basics
- Livrable : rapport de test applicatif sur votre webapp

SÉANCE 48

Séance 13 · ISO 27001 : démarche SMSI et audit interne

1H

- Périmètre du SMSI et analyse des risques (ISO 27005)
- Construction du plan de traitement des risques
- Livrable : matrice des risques et plan de traitement documenté

SÉANCE 49

Séance 14 · Gestion avancée des incidents et coordination

1H

- Rôles CERT/CSIRT : missions, organisation, outillage
- Coordination avec l'ANSSI et les parties prenantes externes
- Exercice tabletop avancé sur scénario APT

SÉANCE 50

Séance 15 · Bilan technique et plan de renforcement

1H

- Consolidation des livrables techniques produits

Scoring de maturité sécurité avant / après

- Plan de renforcement prioritaire à 3 mois avec KPIs

NIVEAU EXPERT

SÉANCE 51 · Séance 1 · Audit stratégique de la posture sécurité de votre organisation · 1H

- Évaluation de la maturité sécurité (CMMI, ISO 27001, NIS2)
- Identification des écarts stratégiques prioritaires
- Cadrage des séances individuelles sur vos enjeux réels

SÉANCE 52 · Séance 2 · Gouvernance de la cybersécurité · 1H

- Construction du RACI sécurité et du comité de pilotage
- Budget sécurité : justification, allocation, suivi
- Livrable : charte de gouvernance sécurité de votre organisation

SÉANCE 53 · Séance 3 · Conformité NIS2 : obligations et roadmap · 1H

- Champ d'application NIS2 : êtes-vous concerné ?
- Obligations clés : gestion des risques, signalement, continuité
- Livrable : roadmap de conformité NIS2 priorisée

SÉANCE 54 · Séance 4 · Red Team / Blue Team : organisation et pilotage · 1H

Définition du périmètre et des règles d'engagement

- Coordination des équipes et gestion des incidents détectés
- Débrief et intégration des enseignements dans la feuille de route

SÉANCE 55

Séance 5 · Threat modeling à l'échelle organisation

1H

- Méthodes STRIDE et PASTA appliquées à vos processus critiques
- Identification des scénarios d'attaque les plus probables
- Livrable : modèle de menaces documenté pour vos actifs critiques

SÉANCE 56

Séance 6 · Conception et pilotage d'un SOC

1H

- Architecture SOC : interne, externalisé ou hybride
- Dimensionnement, outillage, SLA et indicateurs de performance
- Sélection d'un prestataire MSSP : critères et grille d'évaluation

SÉANCE 57

Séance 7 · Gestion de crise cyber : cellule, communication, RETEX

1H

- Construction de la cellule de crise et des rôles
- Communication de crise : interne, clients, régulateurs, presse
- Livrable : plan de gestion de crise cyber documenté

SÉANCE 58

Séance 8 · Supply chain security : risques fournisseurs

1H

- Cartographie des fournisseurs critiques et de leurs accès SI

Audit et qualification sécurité des prestataires

- Clauses contractuelles de sécurité : ce qui est exigible

SÉANCE 59

Séance 9 · Cyber-résilience et exercices de simulation

1H

- Stratégie de reprise : RTO/RPO critiques, ordre de restauration
- Exercice de simulation de crise full-scope (tabletop avancé)
- Plan d'amélioration continue issu des exercices

SÉANCE 60

Séance 10 · IA et cybersécurité : risques émergents

1H

- Deepfake, prompt injection, adversarial attacks : menaces concrètes
- IA dans la défense : UEBA, détection d'anomalies, automatisation SOC
- Gouvernance de l'IA : shadow AI et sécurité des données organisationnelles

SÉANCE 61

Séance 11 · Construction et animation d'un CSIRT interne

1H

- Missions, périmètre et positionnement du CSIRT dans l'organisation
- Coordination avec l'ANSSI, le CERT-FR et les homologues sectoriels
- Outillage minimal pour un CSIRT efficace sans budget dédié

SÉANCE 62

Séance 12 · ISO 27001 : audit blanc et revue de direction

1H

- Simulation d'audit de certification sur votre périmètre SMSI
- Revue de direction : présentation, indicateurs, décisions
- Livrable : plan d'action post-audit blanc priorisé

SÉANCE 63

Séance 13 · Reporting COMEX et communication dirigeants

1H

- Construction du tableau de bord sécurité à destination du COMEX
- Langage du risque business versus langage technique
- Livrable : kit de présentation sécurité COMEX prêt à l'emploi

SÉANCE 64

Séance 14 · Transmission et culture sécurité durable

1H

- Programme de sensibilisation annuel : conception et animation
- Identification et développement des ambassadeurs sécurité internes
- Indicateurs de culture sécurité : comment mesurer les progrès

SÉANCE 65

Séance 15 · Bilan stratégique et plan de gouvernance transmissible

1H

- Consolidation de tous les livrables stratégiques
- Plan de gouvernance cybersécurité à 3 ans
- Document de passation : ce qu'un successeur doit savoir

05 Modalités

PÉDAGOGIE	Format individuel et personnalisé. séances d'une heure, planifiées à votre rythme, en visioconférence ou en présentiel selon vos contraintes. Avant la première séance, un cadrage gratuit avec votre expert permet d'identifier vos cas d'usage réels et d'adapter le programme à votre poste et à vos outils. L'expert reste le même du premier au dernier entretien : aucun roulement, aucun intervenant de remplacement. Chaque séance produit un livrable que vous pouvez appliquer dès le lendemain. Si vos priorités évoluent en cours de parcours, le programme s'adapte sans délai.
ÉVALUATION	Un questionnaire de positionnement avant la première séance évalue vos connaissances actuelles et oriente les priorités du programme. À chaque séance, un quiz de consolidation valide l'acquisition des notions clés. À mi-parcours, un bilan intermédiaire permet d'ajuster le programme si vos besoins ont évolué. En fin de parcours, une mise en situation sur un cas réel apporté par le stagiaire valide les réflexes acquis. La satisfaction est mesurée à chaud (J+1) et à froid (J+30). Un certificat de réalisation Qualiopi est remis à l'issue du parcours.

ACCESSIBILITÉ

Cette formation est accessible aux personnes en situation de handicap. Avant le démarrage, un entretien avec notre référent handicap, Benjamin Berrous, identifie les adaptations nécessaires : supports de cours en grands caractères ou en version audio, durée des séances modulée, pauses supplémentaires intégrées, accompagnement par un interprète LSF sur demande. Le format individuel facilite ces ajustements sans démarche administrative complexe. Les séances se déroulent dans l'environnement de travail habituel du stagiaire, ce qui supprime les obstacles liés aux déplacements. Toute demande d'adaptation est traitée en amont de la première séance, sans délai Contact référent handicap · benjamin.berrous@mda-performance.fr.

Prêt à démarrer ?

Premier échange de cadrage gratuit avec votre futur expert. Programme adapté à votre contexte, sans engagement.

VOUS POUVEZ ME RETROUVER ICI

groupe-mda.fr/formations/formation-cybersecurite