CYCLE DE FORMATION

CYBERSÉCURITÉ ET CYBER-RÉSILIENCE DES SI : APPRENDRE DES FAILLES POUR ANTICIPER ET PROTÉGER

Dans un monde où chaque entreprise, chaque administration et chaque individu est potentiellement une cible, la cybersécurité n'est plus un luxe mais une nécessité stratégique. Le Maroc, à l'instar de nombreux pays, connaît une recrudescence inquiétante d'attaques informatiques – ransomware, hameçonnage, exfiltration de données – qui paralysent des institutions, compromettent des services publics et mettent en péril la souveraineté numérique. Trop souvent, ces incidents révèlent des failles techniques, organisationnelles… et humaines.
Ce cycle de formation intensif de 10 jours, animé par des experts reconnus, vous propose d'aller au-delà de la réaction pour construire une véritable posture de cyber-résilience. À travers des cas concrets, des retours d'expérience, des outils de pointe et une approche pluridisciplinaire, vous apprendrez à anticiper, à protéger, mais aussi à reconstruire après une attaque.

Durée	Lieu
10 jours	Hôtel Sofitel Jardin des roses Rabat

Tarif	Renseignement
30 000 Dhs HT	06 63 62 08 02

Dates

»03-04 juillet 2025
»11-12 septembre 2025
»25-26 septembre 2025
»09-10 octobre 2025
»13-14 Novembre2025

Public concerné

- Managers, Décideurs, Administrateurs d'entreprises, Responsables de la Sécurité des Systèmes d'Informations (RSSI), DSI, CDO, Administrateurs sécurité.

Objectifs Pédagogiques

- Comprendre les cybermenaces actuelles et maîtriser les bonnes pratiques de sécurisation des systèmes d'information, des environnements Cloud et des applications.
- Intégrer la sécurité dans toute la chaîne de développement (DevSecOps) et appliquer les normes de gouvernance et de conformité (ISO 27001, RGPD, Loi 09-08).
- Renforcer la résilience organisationnelle en développant une culture de cybersécurité et en sensibilisant aux risques humains (phishing, Shadow IT, IA).

Animateurs

M. Hicham EL FAIK
CEO / Founder - CYBRFORGE CyberSecurity Expert - Global CISO 🛡️ I Help My Customers Achieve Their Cybersecurity Strategy GIAC GSTRT, CISSP, CCSP, C|CISO, CISM, ISO CCSM, ISO27001 LA, ISO27005 SLRM, ISO22301 LI, CEH, PMP

M.Mohamed BENOUDA
Président Fondateur ABA TECHNOLOGY
Ex Directeur Général de la SNTL

M.Omar BASSIRI
Ingénieur - Analyste Java EE et Web - Java/J2EE, Javascript, Spring, Maven, Birt, DevOps Tech Lead - SpringBoot, Bitbucket, Jenkins, Helm(Go Templates), K8s, Rancher, AWS

M.Mehdi MOUNIR
Senior Manager IT Infrastructure - ISO 27001 LEAD AUDITOR

M.Radouane MRABET
Emeritus professor at Mohamed V University in Rabat, École Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS),

M.Amin LEMFADLI
Cybersecurity & Data Privacy Expert - PMP, CISSP, CCSP, HCISPP, SSCP, CDPSE, CISA, CISM, CDPO

Module 1: Panorama des cybermenaces au Maroc et sécurisation des Systèmes d'Information : analyses récentes et bonnes pratiques architecturales (2 jours)

Jour 1 : Panorama des cybermenaces et analyse des attaques récentes au Maroc

Objectifs :

- Contextualiser les menaces modernes.
- Étudier les attaques CNSS, DDoS54, SEO Hack japonais (plusieurs institutions Marocaines).

Contenus :

- Cartographie des menaces 2025 (APT, ransomware, exfiltration).
- Analyse détaillée des vecteurs des attaques au Maroc.
- Erreurs techniques et humaines observées.
- Table ronde : "Sommes-nous prêts ?"

Jour 2 : Sécurisation des Systèmes d'Information (SI) – Architecture et bonnes pratiques

Objectifs :

- Revoir les fondations : urbanisation, segmentation, durcissement.

Contenus :

- Zones de confiance et pare-feu applicatif (WAF).
- Bastion, segmentation réseau, cloisonnement des données.
- Typologie des SOCs
- Contrat SOC

Module 2: Culture DevSecOps : Fondamentaux, pratiques, outils et automatisation de la sécurité (2jours)

Jour 1 : Fondamentaux et culture DevSecOps

Objectifs :

- Comprendre les fondements, les enjeux, et la culture DevSecOps, ainsi que les bonnes pratiques d'intégration de la sécurité dans le cycle de vie du développement logiciel.

Contenus :

- Introduction à DevSecOps
- Culture, organisation et gouvernance
- Intégration de la sécurité dans le cycle de vie DevOps
- Menaces et vulnérabilités courantes
- Outils DevSecOps (intro)
- Cas d'usage et bonnes pratiques

Jour 2 : Pratique, outils et automatisation de la sécurité

Objectifs :

- Découvrir et manipuler les outils DevSecOps pour automatiser la sécurité dans les pipelines CI/CD, sécuriser le code, les conteneurs et l'infrastructure, et bâtir un pipeline sécurisé de bout en bout.

Contenus :

- Sécurité du code et des dépendances
- Tests de sécurité dynamiques
- Sécurité des conteneurs & de l'infrastructure
- Surveillance, audit, traçabilité
- Automatisation dans les pipelines CI/CD

Module 3: Sécurité des applications mobiles, des API et du Cloud : risques, configurations critiques et enjeux de souveraineté (2jours)

Jour 1 : Sécurité des applications mobiles et API

Objectifs :

- Sécuriser les applications iOS/Android et les APIs exposées.

Contenus :

- OWASP Mobile Top 10.
- Problèmes fréquents : stockage local, interception, tokens JWT mal gérés.
- Tests de sécurité mobile avec MobSF.
- Bonnes pratiques DevSecOps dans le mobile.

Jour 2 : Sécurité Cloud & DaaS – Risques, erreurs de configuration souveraineté

Objectifs :

- Identifier les failles dans le Cloud et les services exposés.

Contenus :

- Sécurité dans AWS / Azure / GCP.
- DaaS et exposition des données par API.
- Cas pratiques : buckets S3 ouverts, secrets dans le code.
- Stratégies multicloud résilientes.

Module 4: Cybersécurité des infrastructures critiques et gouvernance de la sécurité : outils open source, conformité (ISO 27001, RGPD) et politiques de protection (2jours)

Jour 1 : Cybersécurité des infrastructures critiques (DNS, VPN, mail, AD) + Open Source Tools

Objectifs :

- Comprendre les points de rupture des SI.

Contenus :

- Vulnérabilités dans Active Directory.
- Dangers d'un DNS mal protégé.
- Spoofing, phishing, spear phishing sur les emails gouvernementaux.
- Etude des attaques DDoS sur ministères marocains.

Jour 2 : Gouvernance, conformité, politiques de sécurité (ISO 27001, RGPD, DLP)

Objectifs :

- Construire des politiques solides de sécurité et de gestion de crise.

Contenus :

- Structure du SMSI (Système de Management de la Sécurité).
- Sensibilité des données et classification.
- RGPD, gestion des consentements et DLP.
- Retex : gouvernance manquante dans les attaques au Maroc.

Module 5: Sécurité dans le Cloud selon les principes du CCSP (ISC2) et culture de sécurité : sensibilisation, phishing, Shadow IT et IA (2jours)

Jour 1 : La Sécurité dans le Cloud ou ce que prône le CCSP du ISC2

Objectifs :

- .Valider une expertise avancée en sécurité du cloud en maîtrisant les principes, les risques, les normes et les bonnes pratiques pour concevoir, gérer et sécuriser des environnements cloud.

Contenus :

- Cloud Concepts, Architecture and Design (Concepts, architecture et conception du Cloud)
- Cloud Data Security (Sécurité des données dans le Cloud)
- Cloud Platform and Infrastructure Security (Sécurité des plateformes et de l'infrastructure Cloud)
- Cloud Application Security (Sécurité des applications dans le Cloud)
- Cloud Security Operations (Opérations de sécurité dans le Cloud)
- Legal, Risk and Compliance (Aspects juridiques, gestion des risques et conformité)

Jour 2 : Culture de sécurité et sensibilisation humaine – Phishing, Shadow IT, IA

Objectifs :

- Former les humains, facteur #1 d'exposition.

Contenus :

- Scénarios de phishing ciblé (technique et narratif).
- Shadow IT et BYOD : leviers de compromission silencieux.
- Utilisation défensive de l'IA contre les cybermenaces.
- Conclusion : vers une gouvernance nationale résiliente ?

MODALITES D'INSCRIPTION AU CYCLE DE FORMATION

Cybersécurité et cyber résilience des SI :
apprendre des failles pour anticiper et protéger

Administration/Organisme

Raison sociale .....

Adresse .....**Ville** .....

Le responsable formation

Nom : .....

Prénom : .....

Tél : .....**E-mail :** .....

Participants

Nom et Prénom	Fonction	Email	Tél

Tarif

30 000 DH/HT soit36 000 DH/TTC par personne
Forfaits incluant les dix jours de formation avec déjeuners et pauses café, ainsi que les supports de formation papier et électronique, et le certificat délivré par Mouvement Conseil.
Possibilités d'hébergements à des tarifs préférentiels (nous contacter pour plus d'informations)
Le Cabinet Mouvement Conseil est éligible au remboursement OFPPT.

Règlement

Par virement bancaire au compte : Attijariwafa bank
Dar Al Moukawil Rabat N° 007 810 0014993000000402 83
Merci de remplir la présente fiche et nous la renvoyer en version scannée par email sur : contact@mouvement.ma ou par Fax N° : 05 37 67 51 44

Date **Signature et cachet de l'organisme**