CYCLE CERTIFIANT « CYBER RESILIENCE A L'HEURE DU DEVELOPPEMENT DE LA DATA ET DU CLOUD »

10 jours-60 heures
TARIF
30 000 Dhs HT

ANIMATEUR(S)

Didier SPELLA
Ex-Commandant de l'Armée de l'Air Française en charge des Systèmes d'Informations
Ex-Expert Sécurité SI chez IBM
Habilité par l'ANSSI à labelliser les formations continues en sécurité numérique

Taib DEBBAGH
Ex-Secrétaire Général du Ministère marocain en charge des Technologies de l'Information et Diplomate auprès de l'Union Internationale des Télécommunications (UIT), organisation des Nations Unies à Genève. Docteur en Informatique des Organisations de l'Université Paris-Dauphine.

Anass DOUKKALI
Professeur de l'enseignement supérieur habilité, chargé de mission auprès de l'Université Mohamed V de Rabat pour le développement de l'innovation en e-santé et e-emploi.
Ex-Ministre de la Santé
Ex-Directeur Général de l'ANAPEC
Ex-Député à la Chambre des Représentants

Yahya ARROUBAT
Responsable du département de la sécurité SI au sein de Bourse de Casablanca.
Membre de l'AUSIM. Auteur en 2017, du livre blanc « DNSSI, Conformité avec le Décret 02-15-712. Apport de la Norme internationale ISO 27001 »

Hicham FAIK
Expert cyber sécurité
Certifié CISSP, CCSP, SANS GSTRT, CISM, ISO27001, ISO27005
Ingénieur EHTP

Abdessamad KAHIR
Consultant Senior en sécurité de l'information (CISA,CEH,COBIT, CRISC, ITIL, ISO27001 LA & LI)
Ingénieur Ecole Mohammadia

Le cabinet Mouvement Conseil organise en partenariat avec l'AUSIM (Association des Utilisateurs des Systèmes d'Information au Maroc) et avec MorTrust (première association professionnelle au service de la cybersécurité et de la confiance numérique au Maroc) un cycle certifiant au sujet de la Cyber résilience à l'heure du développement de la Data et du Cloud.

Cette formation a pour objectif d'acquérir une vision globale, théorique et pratique, de la sécurité et de sa gouvernance sur le plan des lois mais aussi des outils, concepts et mécanismes permettant de faire face aux attaques visant la sécurité des systèmes d'informations.

Cette formation permettra d'apprendre les mesures de sécurité susceptibles d'être prises pour se défendre contre des attaques d'un système d'information. Sont abordés également les aspects légaux et règlementaires.

Public visé

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

Méthodes pédagogiques

- Support de séminaires,
- Etude de cas
- Application et atelier de travail (workshops)
- Témoignages de personnalités connues et reconnues dans le domaine
- Simulation d'une Situation de Crise suite à une Cyberattaque
- Attestation de formation

Modules

Module 1 : Contexte et enjeux de la Cyber sécurité, les menaces et les techniques de réduction des cyber-risques
Module 2 : Uses Cases
Module 3 : Mettre en place un système de management de la sécurité de l'Information selon la norme ISO 27001 V 2022 / 27002
Module 4 : Cyber résilience, Gouvernance de la Data et du Cloud
Module 5 : Corpus Réglementaire Marocain et Cyber Résilience Oversight Expectations (CROE)

Dates & Lieu

27 et **28 Avril 2023** Au Grand Mogador Casablanca
11 et **12 Mai 2023** Au Sofitel Jardin Des Roses Rabat
25 et **26 Mail 2023** Au Sofitel Jardin Des Roses Rabat
08 et **09 Juin 2023** Au Sofitel Jardin Des Roses Rabat
22 et **23 Juin 2023** Au Sofitel Jardin Des Roses Rabat

RENSEIGNEMENTS
TEL : 06 63 62 08 02

12 Avenue Michlifen 4ème étage APT N°9 Agdal RABAT Email : contact@mouvement.ma
Tél : 05 37 70 32 17 Fax : 05 37 67 51 44 RC : 122439 Patente : 25102377 IF : 20722985 CNSS :5258711

CYCLE CERTIFIANT « CYBER RESILIENCE A L'HEURE DU DEVELOPPEMENT DE LA DATA ET DU CLOUD »

Les principaux points qui seront abordés

1. **Contexte et enjeux de la Cyber sécurité :**
- Définitions et enjeux.
- Les critères DICP (Disponibilité, Intégrité, Confidentialité, Preuve).
- Distinguer Vulnérabilités / Menaces / Attaques.
- Les 4 types de cyber-risques (cybercriminalité, atteinte à l'image, espionnage, sabotage).
- Avènement des Technologies Disruptives et leurs impacts sur les secteurs d'activité économiques
- Risques liés à l'adoption de ces nouvelles Technologies
- CyberSoc Watch

2. **Les menaces et les techniques de réduction des cyber-risques :**
- Panorama des menaces et des vulnérabilités.
- L'élément humain dans les cyber-risques.
- Panorama des techniques de réduction des cyber-risques.

3. **Cyber résilience, Gouvernance de la Data et du Cloud :**
- La Sécurité de la Data hébergée sur le Cloud
- La sécurité de l'Infrastructure Cloud
- La sécurité des applications Cloud
- Le Cloud et l'aspect réglementaire

4. **Mettre en place un système de management de la sécurité de l'Information selon la norme ISO 27001 V 2022**
- L'engagement de la direction.
- Définition d'une politique de cyber sécurité.
- Cartographie des actifs du SI.
- Identification, évaluation et traitement des risques.
- Le suivi des plans d'actions.
- La surveillance et le traitement des incidents.
- Les plans de reprise et de continuité d'activité.
- L'implication des parties prenantes.

5. **Corpus Réglementaire Marocain :**
- Revue de toutes les lois, règles, réglementations et circulaires
- Exigences, Responsabilités, portée de chaque cadre réglementaire

6. **Cyber Resilience Oversight Expectations (CROE) :**
- Présentation du cadre de référence
- Les trois niveaux de maturité
- Exigences, Responsabilités, portée…

Uses Cases

- Présentation de cas de Cyber-attaques :
- Secteur de la Santé
- Secteur de l'administration
- Secteur du Tourisme
- …

Simulation de crise suite à une cyber-attaque

12 Avenue Michlifen 4ème étage APT N°9 Agdal RABAT Email : contact@mouvement.ma
Tél : 05 37 70 32 17 Fax : 05 37 67 51 44 RC : 122439 Patente : 25102377 IF : 20722985 CNSS :5258711

CYCLE CERTIFIANT « CYBER RESILIENCE A L'HEURE DU DEVELOPPEMENT DE LA DATA ET DU CLOUD »

Programme des modules

Module 1 : Contexte et enjeux de la Cyber sécurité, Les menaces et les techniques de réduction des cyber-risques (2jours)

La Cybersécurité représente un enjeu nouveau et complexe pour le développement de systèmes, et ce premier séminaire abordera la façon de prendre en compte l'ensemble de ces contraintes, de la conception à la production du composant système.

Ce module traite des thématiques suivantes :

- L'intelligence Economique
- Définitions et objectifs, et stratégie d'entreprise en matière de Cybersécurité
- Le Cyber Monde, nouvel environnement technologique
- Les 4 paradigmes
- Les Principes de la sécurité
- Les quatre types d'attaques
- Les Principales Menaces
- Les 3 typologies d'attaques
- Notion de Base de la cybersécurité
- Cybersécurité, Sécurité des SI, Cyberdéfense, Cybercriminalité…

Module 2 : Uses Cases (2jours)

Ce module s'étale sur deux jours et présente les principaux risques dans un certain nombre de secteurs d'activités dont certains sont critiques, ou d'importance vitale comme les définit la Loi 05-20.

Les intervenants présentent les vulnérabilités, les menaces et quelques stratégies de traitement des risques afin de se prémunir contre les actes malveillants, dont l'objectif est de porter atteinte à la confidentialité, l'intégrité et la disponibilité des activités de ces secteurs.

- Présentation de cas de Cyber-attaques :
- Présentation de Mor Trust
- Etat des Lieux Cybersécurité
- Stat
- Use Cases

Module 3 : Mettre en place un système de management de la sécurité de l'Information selon la norme ISO 27001 V 2022 / 27002 (2jours)

Ce module permet de présenter la Norme ISO 27001 V 2022, avec les bonnes pratiques e matière de sécurité des Système d'Information. La démarche montre aussi comment réussir la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme, et comment le maintenir dans le temps.

- À l'issue de ces deux jours, le participant sera en mesure de : Expliquer les composants d'un système de management de la sécurité de l'information (SMSI) conforme à ISO 27001
- Expliquer le contenu et la corrélation entre ISO 27001 et 27002 ainsi qu'avec d'autres normes et cadres réglementaires
- Adapter les exigences de la norme ISO 27001 au contexte spécifique d'un organisme
- Interpréter les exigences d'ISO 27001 dans le cadre de l'audit d'un SMSI
- Aligner les différentes approches de la gouvernance SSI

Module 4 : Cyber résilience, Gouvernance de la Data et du Cloud (2jours)

Cyber Sécurité du Cloud : Concepts sécurité, Architecture et modèles de services, Risques, Résilience, Techniques de sécurité, Gouvernance,

Opérations du Cloud : Synthèse de la certification CCSP (ISC2 Certified Cloud Security Professional)

Module 5 : - Corpus Réglementaire Marocain
- Cyber Résilience Oversight Expectations (CROE)
(2jours)

Lors de cette journée l'intervenant présentera le corpus réglementaire en matière de sécurité et son évolution à travers le temps. L'expertise de l'intervenant qui a travaillé sur ce sujet que ce soit dans le secteur privé, public ou dans l'internationale permettra aux participants d'avoir une vision 360 sur l'apport de la réglementation dans la sécurisation des organisation public, semi-publics et privées.

Il sera aussi question de revenir sur l'évolution de la maturité de la stratégie de la Cyber sécurité au Maroc durant les 15 dernières années.

Cyber Resilience Oversight Expectations (CROE)

Le paysage des cybers menaces évolue constamment et atteint des niveaux de sophistication plus élevés.
À la lumière de cela, les organisations devraient redoubler d'efforts pour adapter, faire évoluer et améliorer leurs capacités de cyber-résilience.

Pour répondre à l'idée d'adaptation, d'évolution et d'amélioration continues, le CROE définit des niveaux d'attente qui fournissent aux superviseurs et aux contrôleurs une référence par rapport à laquelle ils peuvent évaluer le niveau actuel de cyber-résilience des organisations, mesurer la progression et établir des domaines d'amélioration prioritaires.

Le CROE établit trois niveaux d'attente : ***évolutif***, ***progressif*** et ***innovant***.
Ce module permet de présenter le cadre de référence CROE et la démarche de mise en place.

- **Simulation de crise « Attaque Cybercriminelle »**

Alors que le nombre de cyberattaques explose, ce module permet aux participants de se mettre dans une situation de "crises cyber".
L'objectif est de se préparer au mieux pour le jour où une attaque informatique frappera vraiment.

MODALITES D'INSCRIPTION AU CYCLE CERTIFIANT
« CYBER RESILIENCE A L'HEURE DU DEVELOPPEMENT DE LA DATA ET DU CLOUD »

Administration / Organisme

Raison Sociale _____

Adresse_____**Ville**_____

Le Responsable Formation

Nom_____

Prénom_____

Tél_____**E-mail**_____

Participants

Nom et Prénom	Fonction	Email	Tél

Tarif

30 000 Dhs HT soit 36 000 TTC Par Personne
Forfaits incluant les 10 jours du cycle, avec déjeuners et pauses café, ainsi que les supports de formation papier et électronique, et l'attestation de participation délivré conjointement par Mouvement Conseil, AUSIM et MorTrust, Et le certificat habilité par l'ANSSI en Cybercriminalité
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**

12 Avenue Michlifen 4ème étage APT N°9 Agdal RABAT Email : contact@mouvement.ma
Tél : 05 37 70 32 17 Fax : 05 37 67 51 44 RC : 122439 Patente : 25102377 IF : 20722985 CNSS :5258711