اتحاد المصارف العربية
Union of Arab Banks

GPBM
المجموعة المهنية لبنوك المغرب
GROUPEMENT PROFESSIONNEL DES BANQUES DU MAROC
MOROCCAN BANKS ASSOCIATION

DÉVERROUILLER LES SECRETS DE LA CYBERSÉCURITÉ

Outils et Techniques avancés pour les Professionels de la Cybersécurité

26-28 JANVIER 2026

الدار البيضاء - المملكة المغربية
CASABLANCA - ROYAUME DU MAROC

DÉVERROUILLER LES SECRETS DE LA CYBERSÉCURITÉ

CONTEXTE

La probabilité et l'impact de l'exploitation des actifs des entreprises augmentent en raison de l'usage de l'intelligence artificielle, de la disponibilité d'outils publics et de l'émergence continue de nouvelles vulnérabilités. Une formation continue en cybersécurité est essentielle pour faire face à cette tendance croissante et réduire l'écart croissant entre les attaquants et les professionnels de la sécurité.

OBJECTIFS

L'objectif de cette formation est de mettre en lumière les menaces les plus récentes en 2025 ainsi que les principales préoccupations de l'industrie de la cybersécurité. Les sessions combinent les meilleures pratiques, des cadres de sécurité, des études de cas réels et des travaux pratiques permettant aux participants de comprendre la mentalité d'un hacker afin de se préparer à la bataille.

DÉVERROUILLER LES SECRETS DE LA CYBERSÉCURITÉ

PUBLIC CIBLE

- Directeurs de la sécurité des systèmes d'information (CISO)
- Auditeurs informatiques
- Responsables des risques informatiques
- Responsables des risques opérationnels
- Administrateurs systèmes
- Agents de support en technologies de l'information

PRÉREQUIS

Les participants doivent se munir d'un ordinateur portable avec les spécifications minimales suivantes :
- Windows 10 ou 11
- Mémoire : 16 Go de RAM
- Espace disque disponible : 200 Go
- Accès à Internet requis pour certains travaux pratiques

DÉVERROUILLER LES SECRETS DE LA CYBERSÉCURITÉ

AGENDA

JOUR 1

1. Principaux incidents de cybersécurité en 2025
2. Le panorama des menaces– État de la cybersécurité dans les pays arabes et au Maroc
3. Modèles de menace : MITRE ATT&CK et D3FEND
4. Contrôles de cybersécurité : SANS V8, ANSSI 42 règles d'hygiène
5. Outils GRC open source
6. Outils d'évaluation de la CISA
7. Analyse statique des fichiers PDF et Office
8. Analyse des modèles et cas d'usage des règles YARA
9. Études de cas réels :

a. Attaques sur plateformes OS
b. Attaques Web
c. Attaques par courriel
d. Ingénierie sociale
e. Attaques sans fil
f. Attaques par web shell
g. API et fuites d'information : cas de Facebook

10. Travaux pratiques : Simulation d'attaque sur DVWA

JOUR 2

1. Techniques de suppression et de récupération de données – démonstrations
2. Cryptographie et signatures numériques
3. Vulnérabilité de BitLocker et techniques de contournement
4. Cycle de vie d'une attaque
5. Contrôles et techniques préventives contre les APT
6. Outils & techniques de « Sandboxing » et d'évasion
7. Techniques avancées avec OWASP ZAP
8. Tests d'intrusion : démonstrations
9. Travaux pratiques : Utilisation d'outils open source pour scanner des applications Web et analyse dynamique d'une application Web ou mobile

DÉVERROUILLER LES SECRETS DE LA CYBERSÉCURITÉ

JOUR 3

10. Sécurité de l'infrastructure
11. Réaliser un test de préparation face aux rançongiciels
12. Attaques physiques et remédiation – « Rubber Ducky » et câbles O.MG
13. Durcissement des systèmes : outils et démonstrations
14. Enrichissement des logs avec SYSMON
15. L'IA en cybersécurité:
    a. Intégration de CHATGPT avec KALI
    b. Prompts CHATGPT pour la reconnaissance et le scan
    c. CHATGPT pour l'ingénierie sociale
    d. Réalisation d'attaques Web avec CHATGPT
    e. Cas d'usage de l'IA pour l'OSINT
16. Mise en œuvre, configuration et usage optimal de MISP (Malware Information Sharing Platform)
17. Solutions SIEM open source – WAZUH
18. IA appliquée à BURP et WAZUH
19. Clôture et recommandations

M. JEAN-MICHEL KAOUKABANI
ARCSHIELDS, DIRECTEUR

Jean-Michel est l'ancien responsable du Département de la Sécurité de l'Information au sein du Groupe Banque Byblos. Il est Auditeur Certifié des Systèmes d'Information (CISA) de l'ISACA, enseignant à l'Université Saint-Joseph – ESIB et à l'École Nationale d'Administration (ENA) au Liban, ainsi que formateur en cybersécurité et membre du comité technique auprès de l'Union des Banques Arabes.

Jean-Michel a successivement occupé les postes de Responsable de l'Audit Informatique, Responsable du MIS (Système d'Information de Gestion) et Responsable de la Sécurité de l'Information au sein du Groupe Banque Byblos. Il a récemment été nommé Directeur de la société de cybersécurité ArcShields. Il est diplômé de l'école d'ingénieurs française, l'École Nationale de la Statistique et de l'Analyse de l'Information (ENSAI), et titulaire d'un diplôme en Économie de l'Université Saint-Joseph.

Jean-Michel est un professionnel des systèmes d'information depuis plus de 20 ans, dont 19 années dans la sécurité de l'information et l'audit informatique dans le secteur financier. Il est certifié en scan de vulnérabilités, expert dans la mise en oeuvre d'une architecture de sécurité d'entreprise, l'évaluation des risques, les CSIRT, investigation informatique, l'audit informatique et les tests d'intrusion. Il enseigne et donne des conférences sur les normes de sécurité et les bonnes pratiques dans des universités et organismes gouvernementaux.