Union of Arab Banks

EN COLLABORATION AVEC

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

SÉMINAIRE

DÉVERROUILLER LES SECRETS DE LA CYBERSÉCURITÉ :

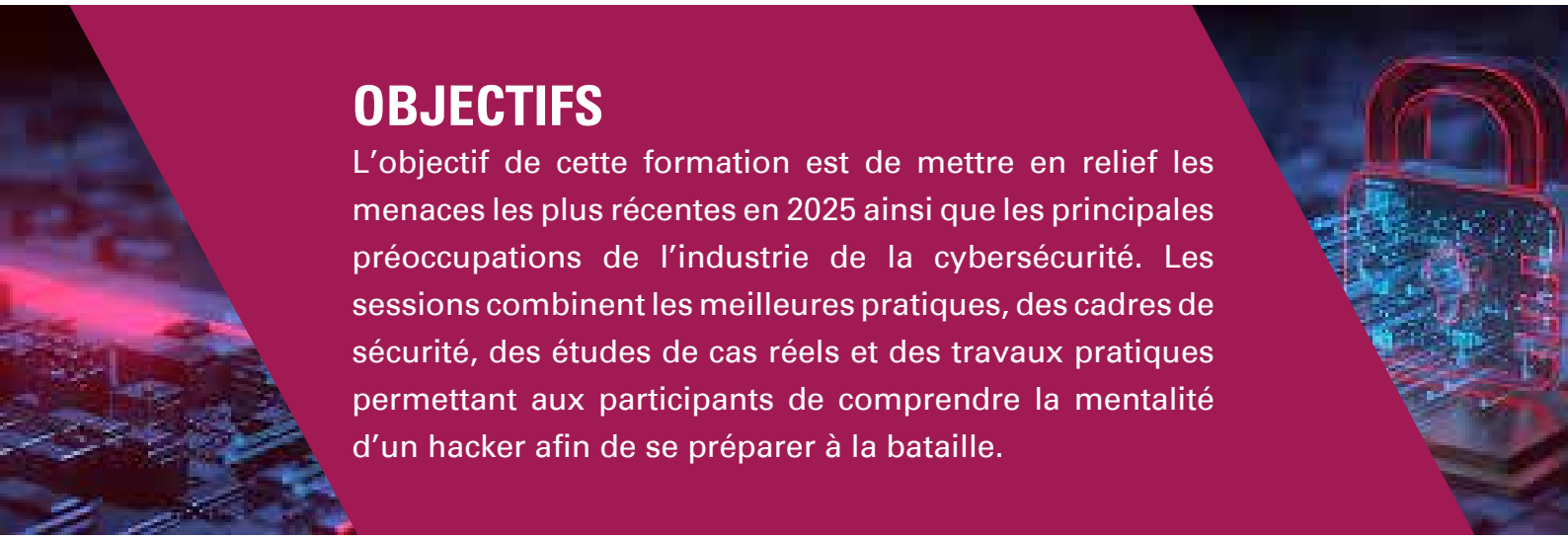
OUTILS ET TECHNIQUES AVANCÉS POUR LES PROFESSIONNELS DE LA CYBERSÉCURITÉ

23 – 25 JUIN 2025

CASABLANCA – ROYAUME DU MAROC

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 relief 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.

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

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

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

JOUR 3

1. Sécurité de l'infrastructure
2. Réaliser un test de préparation face aux rançongiciels
3. Attaques physiques et remédiation – « Rubber Ducky » et câbles O.MG
4. Durcissement des systèmes : outils et démonstrations
5. Enrichissement des logs avec SYSMON
6. 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
7. Mise en œuvre, configuration et usage optimal de MISP (Malware Information Sharing Platform)
8. Solutions SIEM open source – WAZUH
9. IA appliquée à BURP et WAZUH
10. Clôture et recommandations

L'INTERVENANT
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 œuvre 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.

بالتعاون
مع

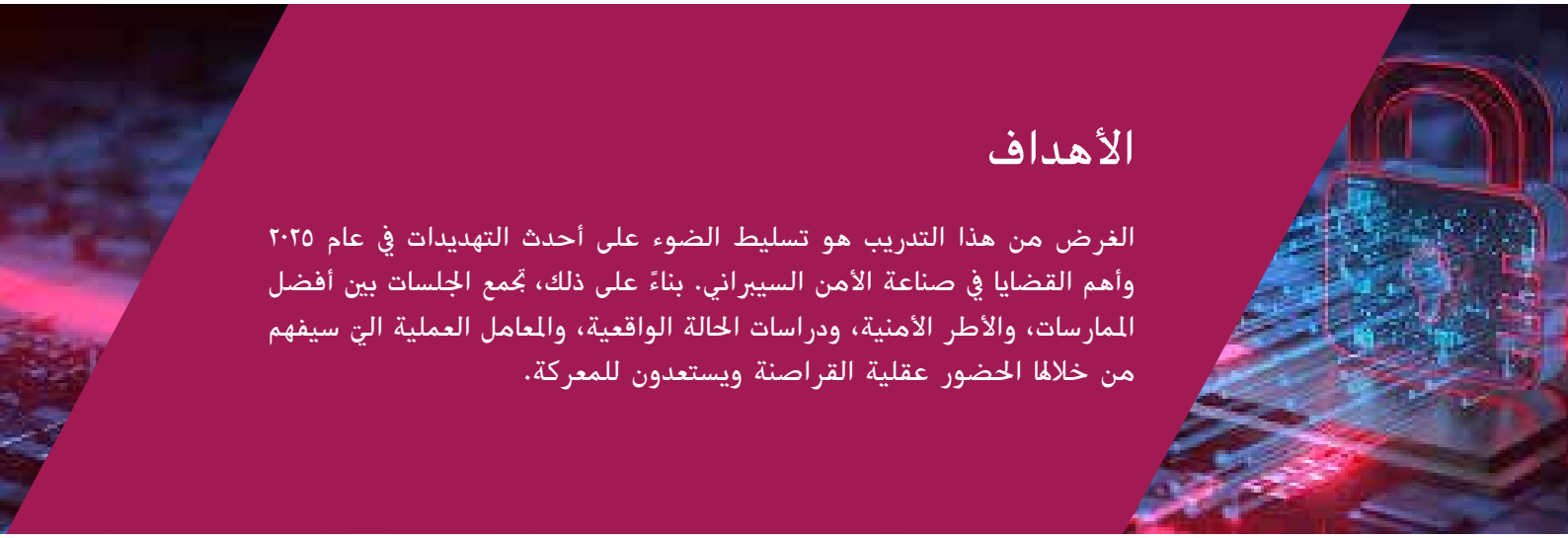
كشف أسرار الأمن السيبراني:
أدوات وتقنيات متقدمة للمتخصصين في الأمن السيبراني

٢٣ - ٢٥ حزيران / يونيو ٢٠٢٥
الدار البيضاء - المملكة المغربية

كشف أسرار الأمن السيبراني:
أدوات وتقنيات متقدمة للمتخصصين في الأمن السيبراني

الخلفيـــة

تزداد احتمالية وتأثير استغلال أصول الشركات بسبب استخدام الذكاء الاصطناعي، وتوفر الأدوات العامة، والظهور المستمر للثغرات الجديدة. يعد التدريب المستمر في مجال الأمن السيبراني أمرًا أساسيًا للتعامل مع هذا الاتجاه المتزايد في المخاطر وتقليص الفجوة المتنامية بين المهاجمين والمحترفين في مجال الأمن.



الأهداف

الغرض من هذا التدريب هو تسليط الضوء على أحدث التهديدات في عام ٢٠٢٥ وأهم القضايا في صناعة الأمن السيبراني. بناءً على ذلك، تجمع الجلسات بين أفضل الممارسات، والأطر الأمنية، ودراسات الحالة الواقعية، والمعامل العملية التي سيفهم من خلالها الحضور عقلية القراصنة ويستعدون للمعركة.

جدول التدريب

- من الساعة 9 صباحًا حتى 3 مساءً
- مدة الجلسات: 1 ساعة و 15 دقيقة
- فترات قهوة: 15 دقيقة
- الغداء الساعة 3 مساءً

المتطلبات الأساسية

يجب على الحضور إحضار أجهزة الكمبيوتر المحمولة الخاصة بهم بالمواصفات الدنيا التالية:

- Windows 10 أو 11
- الذاكرة: 16 جيجابايت رام
- المساحة المتاحة للتخزين: 200 جيجابايت
- الوصول إلى الإنترنت

المشاركون المستهدفون

- المسؤولون عن أمن المعلومات (CISO)
- مدققو تكنولوجيا المعلومات
- مسؤولو المخاطر في تكنولوجيا المعلومات
- مسؤولو المخاطر التشغيلية
- مسؤولو الأنظمة
- مسؤولو دعم تكنولوجيا المعلومات

كشف أسرار الأمن السيبراني:
أدوات وتقنيات متقدمة للمتخصصين في الأمن السيبراني

الخلفيـــة

اليـــوم الأول

1. الحوادث الكبرى في الأمن السيبراني لعام2025
2. مشهد التهديدات - حالة الأمن السيبراني في الدول العربية والمغرب
3. نماذج التهديدات MITRE ATT&CKو D3FEND
4. الضوابط الأمنية الأساسية - SANS V8 ٤٢ قاعدة للنظافة السيبرانية في أمن المعلومات(وفقًا لدليل الوكالة الوطنية لأمن نظم المعلومات – ANSSI)
5. أدوات الحوكمة والمخاطر والامتثال
6. أدوات تقييم CISA
7. التحليل الثابت لملفات PDF و Office
8. تحليل الأنماط وحالات استخدام قواعد YARA
9. مناقشة دراسات الحالة:
    - هجمات منصات التشغيل
    - الهجمات المستندة إلى الويب
    - هجمات البريد الإلكتروني
    - هجمات الهندسة الاجتماعية
    - الهجمات اللاسلكية
    - هجمات Web Shell
    - واجهات برمجة التطبيقات (APIs) وتسريبات فيسبوك
10. اختبار عملي: محاكاة هجوم على DVWA

اليـــوم الثانـــي

1. تقنيات التخلص من البيانات واستردادها والعروض التوضيحية
2. التشفير والتوقيعات الرقمية
3. ثغرة BitLocker وتقنيات تجاوزها
4. دورة حياة الهجوم
5. الضوابط الوقائية لـ APT وتقنياتها
6. أدوات وتقنيات Sandboxing
7. تقنيات متقدمة لأداة OWASP Zap
8. إطار اختبار الاختراق - عروض حية
9. اختبار عملي: استخدام أدوات مفتوحة المصدر لفحص تطبيقات الويب والتحليل الديناميكي لتطبيق ويب أو تطبيق موبايل

اليـــوم الثالـــث

1. تأمين البنية التحتية الخاصة بك
2. إجراء اختبار استعداد ضد هجمات الفدية
3. هجمات الأمان المادي وطرق معالجتها - Rubber Ducky وكابلات O.MG
4. قوائم تدقيق للأمان، الأدوات، والعروض التوضيحية
5. تعزيز السجلات باستخدام SYSMON
6. الذكاء الاصطناعي في الأمن السيبراني
    - تكامل ChatGPT مع KALI
    - ChatGPT للاستطلاع والفحص
    - ChatGPT للهندسة الاجتماعية
    - تنفيذ هجمات الويب باستخدام ChatGPT
    - حالات استخدام الذكاء الاصطناعي في OSINT
7. تنفيذ وتكوين في استخدام منصة MISP لمشاركة معلومات البرمجيات الخبيثة
8. حلول SIEM مفتوحة المصدر BURP و WAZUH
9. الذكاء الاصطناعي فيWAZUH
10. الخاتمة والتوصيات

كشف أسرار الأمن السيبراني:
أدوات وتقنيات متقدمة للمتخصصين في الأمن السيبراني

المحاضر:
الأستاذ جان ميشال كوكباني
مدير ArcShields

شغل جان ميشال رئيس قسم أمن المعلومات في مجموعة بنك بيبلوس.
وهو مدقق معتمد في نظم المعلومات (CISA) من ISACA، ومحاضر في جامعة سان جوزيف - ESIB، ومدرسة الإدارة الوطنية (ENA) في لبنان، ومدرب في مجال الأمن السيبراني وعضو في اللجنة الفنية في اتحاد المصارف العربية.

شغل جان ميشال سابقًا مناصب رئيس تدقيق تكنولوجيا المعلومات، ورئيس نظم المعلومات الإدارية، ورئيس قسم أمن المعلومات في مجموعة بنك بيبلوس. وقد تم تعيينه مؤخرًا كمدير لشركة ArcShields للأمن السيبراني.

تخرج من المدرسة الفرنسية للهندسة Ecole Nationale de la Statistique et de L'Analyse de L'Information (ENSAI) ويحمل درجة في الاقتصاد من جامعة سان جوزيف.

يمتلك جان ميشال أكثر من ٢٠ عامًا من الخبرة المهنية في نظم المعلومات، بما في ذلك ١٩ عامًا في مجال أمن المعلومات وتدقيق تكنولوجيا المعلومات في الصناعة المالية.

وهو مدقق معتمد للثغرات، وخبير في تنفيذ بنية الأمان المؤسسية، وإجراء تقييمات المخاطر، ومركز استجابة الحوادث السيبرانية (CSIRT)، والتدقيق الرقمي، وتدقيق تكنولوجيا المعلومات، واختبار الاختراق، وقد قام بالتدريس والمحاضرة حول معايير الأمن وأفضل الممارسات في جامعات مرموقة والوكالات الحكومية.

FRAIS DE PARTICIPATION :

Membres de l'UBA: 900€
Non-membres de l'UBA: 1100€

Les frais comprennent la participation au séminaire, la réception du matériel, des rafraîchissements et un déjeuner quotidien

VIREMENT BANCAIRE:

Arab Bank – Amman – Jordan
Shmeisani Branch
Compte no : 536-010272/0118
Iban no: JO53 ARAB 36 2725 8010 0011 0000 1180
Swift code : ARABJOAX100
Nom du Bénéficiaire: Union of Arab Banks