اتحاد مصارف الكويت
Kuwait Banking Association

IN COLLABORATION with

اتحاد المصارف العربية
Union of Arab Banks

UNLOCKING CYBERSECURITY SECRETS:
ADVANCED TOOLS & TECHNIQUES FOR SECURITY PROFESSIONALS

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

10 – 12 FEBRUARY 2025

MILLENNIUM HOTEL AND CONVENTION CENTRE SALMIYAH

KUWAIT

UNLOCKING CYBERSECURITY SECRETS:

ADVANCED TOOLS & TECHNIQUES FOR SECURITY PROFESSIONALS

BACKGROUND

The likelihood and impact of exploiting companies s assets are rising due to the usage of artificial intelligence, the availability of public tools, and the ongoing emergence of new vulnerabilities. Continuous Cyber security training is essential to addressing this growing risk trend and reducing the growing disparity between attackers and security professionals.

OBJECTIVES:

The purpose of this training is to shed the light on the latest threats in 2024 and the top concerns in the cybersecurity industry. Subsequently, the sessions combine best practices, security frameworks, real case studies and hand on labs in which attendees will understand the mindset of a hacker and get ready for the battle.

TARGETTED PARTICIPANTS:

- Chief Information Security Officers (CISO)
- IT auditors
- IT Risk officers
- Operational Risk officers
- System Administrators
- Information Technology support officers

PREREQUISITES:

Attendees should bring their laptops with minimum specs:

- Windows 10 or 11
- Memory: 16 GB RAM
- Available storage 200 GB
- Internet access required for some labs

UNLOCKING CYBERSECURITY SECRETS:

ADVANCED TOOLS & TECHNIQUES FOR SECURITY PROFESSIONALS

TRAINING AGENDA:

DAY 1:

1. Major Cyber security incidents in 2024
2. The threat Landscape - State of Cybersecurity in the Arab countries
3. Threat Models: MITRE ATT&CK and D3FEND
4. Cyber security top controls-SANS V8
5. Open source GRC tools
6. CISA assessment tools
7. Static analysis of PDF and Office files
8. Pattern Analysis and YARA rules use cases
9. Real cases discussion:
    a. OS platform attacks
    b. Web based attacks
    c. Email attacks
    d. Social engineering attacks
    e. Wireless attacks
    f. Web shell Attacks
    g. APIs and Facebook leaks
10. Hands on LAB: Attack simulation on DVWA

DAY 2:

1. Data disposal and data recovery techniques and Demos
2. Cryptography and Digital Signatures
3. BitLocker vulnerability and bypass techniques
4. The attack life cycle
5. APT Preventive controls and techniques
6. Sandboxing tools & techniques and evasion
7. OWASP Zap advanced techniques
8. Penetration testing framework- demos
9. Hands-on Lab: Use open-source tools to scan Web application and dynamic analysis of a web or mobile application.

DAY 3:

1. Secure your Infrastructure
2. Perform a Ransomware Readiness Test
3. Physical Security attacks and remediation- Rubber Ducky and O.MG cables
4. Security Hardening Checklists, tools, & demos
5. Logs enrichment with SYSMON
6. AI in Cybersecurity
    a. Chat GPT integration with KALI
    b. Chat GPT prompts for reconnaissance and scanning
    c. Chat GPT for Social engineering
    d. Perform web security attacks with Chat GPT
    e. AI use cases for OSINT
7. Implementation, configuration, and optimal use of a Malware Information Sharing Platform (MISP)
8. Open Source SIEM Solutions-WAZUH
9. Wrap-up and recommendations

UNLOCKING CYBERSECURITY SECRETS:

ADVANCED TOOLS & TECHNIQUES FOR SECURITY PROFESSIONALS

SPEAKER

JEAN-MICHEL KAWKABANI, CISA

ARCSHIELDS, DIRECTOR

Jean-Michel is the former Head of Information Security Department at Byblos Bank Group.

He is a Certified Information Systems Auditor (CISA) from ISACA, a lecturer at University Saint Joseph-ESIB and Ecole Nationale D' Administration (ENA) Lebanon and a cyber security trainer and technical committee member in the Union of Arab Banks.

Jean Michel was respectively the Head of IT Audit, the Head of MIS and the Head of Information Security department at Byblos Bank Group. He was recently appointed as Director of ArcShields Cybersecurity company.

He graduated from the French engineering school Ecole Nationale de la Statistique et de L'Analyse de L 'Information (ENSAI) and holds a degree in Economics from Saint Joseph University.

Jean Michel has been an Information Systems professional for more than 20 years including 19 years of Information Security and IT Audit in the financial industry.

He is a certified vulnerability scanner, an expert in implementing an Enterprise Security Architecture, conducting risk assessment, CSIRT, Digital forensics, IT Auditing and Penetration testing and has been teaching and lecturing security standards and best practices in reputable universities and governmental agencies.

كشف أسرار الأمن السيبراني:

أدوات وتقنيات متقدمة للمتخصصين في الأمن السيبراني

الخلفيـــــة

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 2024 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.

المشاركون المستهدفون

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

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

كشف أسرار الأمن السيبراني:

أدوات وتقنيات متقدمة للمتخصصين في الأمن السيبراني

جدول التدريب

اليوم الأول

1. الحوادث الكبرى في الأمن السيبراني لعام 2024
2. مشهد التهديدات - حالة الأمن السيبراني في الدول العربية
3. نماذج التهديدات MITRE ATT&CKو D3FEND
4. الضوابط الأمنية الأساسية - SANS V8
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. مختبر عملي: محاكاة هجوم على DVWA

اليوم الثاني

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. مختبر عملي: استخدام أدوات مفتوحة المصدر لفحص تطبيقات الويب والتحليل الديناميكي لتطبيق ويب أو تطبيق موبايل

اليوم الثالث

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 واستخدام منصة MISP لمشاركة معلومات البرمجيات الخبيثة
8. حلول SIEM مفتوحة المصدرWAZUH
9. 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 جبيل. 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 20 عامًا من الخبرة المهنية في نظم المعلومات، بما في ذلك 19 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)، والطب الشرعي الرقمي، وتدقيق تكنولوجيا المعلومات، واختبار الاختراق، وقد قام بالتدريس والمحاضرة حول معايير الأمن وأفضل الممارسات في جامعات مرموقة والوكالات الحكومية.

PARTICIPTION FESS:

- **UAB Members: 1200$**
- **Non Members: 1500$**

MEANS OF PAYMENT

Arab Bank – Amman – Jordan
Shmeisani Branch
Account no : 0118/010272-510
Iban no: JO76 ARAB 1180 0000 0011 8010 2725 10
Swift code : ARABJOAX118
Beneficiary name : Union of Arab Banks

For more information kindly send an email to
training@uabonline.org

www.uabonline.org