MASTER THE CYB

Security Expert Training

Cyber Security and Technology

Master the Cyber Security Expert Training

Code: 259005

FUTURE CENTRE
مركز المستقبل

futurecentre.net

Course Introduction

Cyber threats are evolving in sophistication and scale, demanding a new caliber of security professionals who can anticipate, neutralize, and lead defense efforts against advanced attacks. **Master the Cyber: Security Expert Training** is an intensive, hands-on course designed for those ready to transcend foundational knowledge and achieve elite proficiency in cybersecurity. This program delves into advanced offensive and defensive tactics, cutting-edge tools, and strategic leadership skills required to protect organizations from modern threats like APTs, zero-day exploits, and large-scale ransomware campaigns. Through real-world simulations, threat-hunting exercises, and expert-led modules, participants will emerge as confident cybersecurity leaders capable of architecting unbreachable systems and guiding teams through the most complex cyber crises

Training Method

- Pre-assessment
- Live group instruction
- Use of real-world examples, case studies and exercises
- Interactive participation and discussion
- Power point presentation, LCD and flip chart
- Group activities and tests
- Each participant receives a binder containing a copy of the presentation
- slides and handouts
- Post-assessment

Course Objectives

Upon completion of this course, participants will be able to:

1. **Execute advanced penetration testing** and ethical hacking techniques to identify critical vulnerabilities.
2. **Design and implement zero-trust architectures** and defense-in-depth strategies.
3. **Lead cyber incident response** for sophisticated attacks (e.g., ransomware, APTs).
4. **Develop and automate security orchestration** (SOAR) and threat intelligence workflows.
5. **Manage cloud and hybrid environment security** (AWS, Azure, Kubernetes).
6. **Communicate cyber risk strategies** to executive leadership and stakeholders.

Who Should Attend?

This expert-level course is designed for:

- **Senior Cybersecurity Analysts and Engineers**
- **SOC Leads and Threat Hunters**
- **Penetration Testers and Red Team Members**
- **Security Architects and IT Risk Managers**
- **Aspiring CISOs and Security Directors**
- **Experienced IT Professionals** transitioning into cybersecurity leadership roles

Course Outline

Day 1: Advanced Threat Landscape and Offensive Security

- **Module 1:** The Modern Adversary: APTs, Cyber Warfare, and Criminal Ecosystems
- **Module 2:** Advanced Penetration Testing: OSINT, Social Engineering, and Physical Security Bypasses
- **Module 3:** Exploit Development: Buffer Overflows, Custom Payloads, and Evasion Techniques
- **Hands-On Lab:** Penetration Testing a Corporate Network (Kali Linux, Metasploit, C2 Frameworks)
- **Case Study:** Deconstructing a Nation-State Attack

Day 2: Defensive Mastery and Security Architecture

- **Module 4:** Zero-Trust Architecture: Micro-Segmentation and Identity-Centric Security
- **Module 5:** Advanced SIEM Use Cases: Query Writing, Correlation Rules, and Anomaly Detection
- **Module 6:** Deception Technologies and Threat Hunting Methodologies
- **Hands-On Lab:** Building a Zero-Trust Network and Writing Advanced SIEM Queries
- **Workshop:** Conducting a Threat Hunt in a Live Environment

Day 3: Cloud and DevOps Security

- **Module 7:** Securing Cloud Environments: AWS/Azure Security Hardening and CSPM
- **Module 8:** Container and Kubernetes Security: Pod Policies, Runtime Protection, and CI/CD Pipeline Security
- **Module 9:** DevSecOps: Integrating Security into SDLC and Automation
- **Hands-On Lab:** Auditing and Hardening a Cloud Environment; Implementing IaC Security Checks
- **Group Exercise:** Responding to a Cloud Supply Chain Attack

Course Outline

Day 4: Incident Response and Digital Forensics

- **Module 10:** Advanced Incident Response: Memory Forensics, Malware Analysis, and Lateral Movement Tracking
- **Module 11:** Digital Forensics: Disk, Network, and Log Analysis for Advanced Persistent Threats
- **Module 12:** Threat Intelligence: Leveraging IOCs, TTPs, and OSINT for Proactive Defense
- **Simulation:** Full-Scale Incident Response Drill (Ransomware and Data Exfiltration Scenario)
- **Lab:** Analyzing a Stolen Image and Memory Dump for Forensic Evidence

Day 5: Leadership, Strategy, and Capstone Challenge

- **Module 13:** Cybersecurity Leadership: Building and Managing a High-Performance Security Team
- **Module 14:** Risk Management and Compliance: NIST, ISO 27001, and GDPR Deep Dive
- **Module 15:** Executive Communication: Presenting Cyber Risk to the Board
- **Capstone Challenge:** Red vs. Blue Team Exercise in a Simulated Enterprise Environment
- **Course Wrap-Up:** Certifications, Career Pathways, and Final Review

المقدمة

تتطور التهديدات السيبرانية من حيث التعقيد والنطاق، مما يتطلب كفاءات جديدة من خبراء الأمن القادرين على توقع الهجمات المتطورة وتحييدها وقيادة جهود الدفاع ضدها. **"إتقان الأمن السيبراني: تدريب خبراء الأمن"** هو دورة مكثفة وعملية مصممة للمستعدين لتجاوز المعرفة الأساسية وتحقيق كفاءة عالية في الأمن السيبراني. يتعمق هذا البرنامج في التكتيكات الهجومية والدفاعية المتقدمة، والأدوات المتطورة، ومهارات القيادة الاستراتيجية اللازمة لحماية المؤسسات من التهديدات الحديثة مثل التهديدات المتقدمة المستمرة (APTs)، وثغرات يوم الصفر (Zero-day Explorations)، وحملات برامج الفدية واسعة النطاق. من خلال عمليات محاكاة واقعية، وتمارين لرصد التهديدات، ووحدات تدريبية بقيادة خبراء، سيُصبح المشاركون قادة أمن سيبراني واثقين قادرين على تصميم أنظمة حصينة وتوجيه الفرق خلال أكثر الأزمات السيبرانية تعقيدًا.

طريقة التدريب

- التقييم المسبق
- تدريب جماعي مباشر
- استخدام أمثلة واقعية ودراسات حالة وتمارين
- مشاركة ونقاش تفاعلي
- عرض تقديمي باستخدام باور بوينت، وشاشة LCD، ولوح ورقي
- أنشطة واختبارات جماعية
- يحصل كل مشارك على ملف يحتوي على نسخة من العرض التقديمي
- شرائح ومطبوعات
- التقييم اللاحق

أهداف الدورة

عند الانتهاء من هذه الدورة، سيكون المشاركون قادرين على:

1. **تنفيذ اختبارات الاختراق المتقدمة** وتقنيات القرصنة الأخلاقية لتحديد نقاط الضعف الحرجة.
2. **تصميم وتنفيذ بنيات الثقة الصفرية** واستراتيجيات الدفاع المتعمق.
3. **قيادة الاستجابة للحوادث السيبرانية** للهجمات المعقدة (على سبيل المثال، برامج الفدية، والهجمات المستمرة المتقدمة).
4. **تطوير وتشغيل** سير عمل تنسيق الأمن (SOAR) ومعلومات التهديدات.
5. **إدارة أمان البيئة السحابية والهجينة** (AWS Azureg Kubernetesg).
6. **توصيل استراتيجيات المخاطر السيبرانية** إلى القيادة التنفيذية وأصحاب المصلحة

من ينبغي أن يهتم؟

تم تصميم هذه الدورة التدريبية على مستوى الخبراء من أجل:

- **كبار المحللين والمهندسين في مجال الأمن السيبراني**
- **قادة مركز العمليات الأمنية وصائدو التهديدات**
- **مختبرو الاختراق وأعضاء الفريق الأحمر**
- **مهندسو الأمن ومديرو مخاطر تكنولوجيا المعلومات**
- **طموحات مسؤولي أمن المعلومات ومديري الأمن**
- **محترفو تكنولوجيا المعلومات ذوو الخبرة** ينتقلون إلى أدوار قيادية في مجال الأمن السيبراني

محتويات الكورس

اليوم الأول مشهد التهديدات المتقدمة والأمن الهجومي

- **الوحدة 1:** العدو الحديث: التهديدات المتطورة المستمرة، والحرب السيبرانية، والأنظمة الإجرامية
- **الوحدة 2:** اختبار الاختراق المتقدم: OSINT والهندسة الاجتماعية وتجاوزات الأمن المادي
- **الوحدة 3:** تطوير الاستغلال: تجاوزات المخزن المؤقت، والحمولات المخصصة، وتقنيات التهرب
- **ورشة عمل عملية:** اختبار اختراق شبكة الشركة (كالي لينكس، ميتاسبلويت، أطر عمل C2)
- **دراسة حالة:** تفكيك هجوم دولة قومية

اليوم الثاني إتقان الدفاع والهندسة الأمنية

- **الوحدة 4:** هندسة الثقة الصفرية: التجزئة الدقيقة والأمان المرتكز على الهوية
- **الوحدة 5:** حالات استخدام SIEM المتقدمة: كتابة الاستعلامات وقواعد الارتباط واكتشاف الشذوذ
- **الوحدة 6:** تقنيات الخداع ومنهجيات البحث عن التهديدات
- **مختبر عملي:** بناء شبكة ثقة صفرية وكتابة استعلامات SIEM متقدمة
- **ورشة عمل:** إجراء عملية بحث عن التهديدات في بيئة حية

اليوم الثالث أمن السحابة DevOpsg

- **الوحدة 7:** تأمين بيئات السحابة: تعزيز أمان AWS/Azure وCSPMg
- **الوحدة 8:** أمان الحاويات Kubernetesg: سياسات Pod، وحماية وقت التشغيل، وأمان خط أنابيب CI/CD
- **الوحدة 9:** DevSecOps: دمج الأمان في SDLC والأتمتة
- **مختبر عملي:** تدقيق وتعزيز بيئة السحابة؛ تنفيذ فحوصات أمان IaC
- **تمرين جماعي:** الاستجابة لهجوم سلسلة التوريد السحابية

محتويات الكورس

اليوم الرابع الاستجابة للحوادث والتحليلات الجنائية الرقمية

- **الوحدة 10:** الاستجابة المتقدمة للحوادث: تحليلات الذاكرة وتحليل البرامج الضارة وتتبع الحركة الجانبية
- **الوحدة 11:** الطب الشرعي الرقمي: تحليل القرص والشبكة والسجل للتهديدات المستمرة المتقدمة
- **الوحدة 12:** استخبارات التهديدات: الاستفادة من IOCs وTTPs وOSINT للدفاع الاستباقي
- **محاكاة:** تدريب شامل على الاستجابة للحوادث (سيناريو برامج الفدية وسرقة البيانات)
- **المختبر:** تحليل صورة مسروقة وملف تفريغ ذاكرة للحصول على أدلة جنائية

اليوم الخامس القيادة والاستراتيجية وتحدي المشروع النهائي

- **الوحدة 13:** قيادة الأمن السيبراني: بناء وإدارة فريق أمني عالي الأداء
- **الوحدة 14:** إدارة المخاطر والامتثال: نظرة متعمقة على معايير NIST وISO 27001 وGDPR
- **الوحدة 15:** الاتصال التنفيذي: عرض المخاطر السيبرانية على مجلس الإدارة
- **تحدي المشروع النهائي:** تمرين الفريق الأحمر مقابل الفريق الأزرق في بيئة مؤسسية محاكاة
- **ملخص الدورة:** الشهادات، والمسارات المهنية، والمراجعة النهائية

Terms & Conditions

Complete & Mail to future centre or email

Info@futurecentre.com

Cancellation and Refund Policy

Delegates have 14 days from the date of booking to cancel and receive a full refund or transfer to another date free of charge. If less than 14 days' notice is given, then we will be unable to refund or cancel the booking unless on medical grounds. For more details about the Cancellation and Refund policy, please visit
https://futurecentre.net/

Registration & Payment

Please complete the registration form on the course page & return it to us indicating your preferred mode of payment. For further information, please get in touch with us

Course Materials

The course material, prepared by the future centre, will be digital and delivered to candidates by email

Certificates

Accredited Certificate of Completion will be issued to those who attend & successfully complete the programme.

Travel and Transport

We are committed to picking up and dropping off the participants from the airport to the hotel and back.

Registration & Payment

Complete & Mail to future centre or email

Info@futurecentre.com

Registration Form

- Full Name (Mr / Ms / Dr / Eng) .....
- Position .....
- Telephone / Mobile .....
- Personal E-Mail .....
- Official E-Mail .....
- Company Name .....
- Address .....
- City / Country .....

Payment Options

- ☐ Please invoice me
- ☐ Please invoice my company

Course Calander:

- 02/02/2026 - 06/02/2026 Click Now
- 22/06/2026 - 26/06/2026 Click Now
- 09/11/2026 - 13/11/2026 Click Now

VENUES

- LONDON
- BARCELONA
- KUALA LUMPER
- AMSTERDAM
- DAMASCUS
- ISTANBUL
- SINGAPORE
- PARIS
- DUBAI

OUR PARTNERS

THANK YOU

CONTACT US

+963 112226969

+963 953865520

Info@futurecentre.com

Damascus - Victoria - behind Royal Semiramis hotel

FUTURE CENTRE
مركز المستقبل

futurecentre.net