Unbreakable: Cyber Security Training

Cyber Security and Technology

Unbreakable Cyber Security Training

Code: 259002

FUTURE CENTRE
مركز المستقبل

futurecentre.net

Course Introduction

In today's digital-first world, cyber threats are evolving at an unprecedented pace, targeting organizations of all sizes and across all sectors. The ability to defend against these threats is no longer optional—it is a critical business imperative. **Unbreakable Cyber Security Training** is designed to equip professionals with the advanced knowledge and hands-on skills needed to build, manage, and defend resilient IT infrastructures. This course goes beyond theory, offering practical, real-world scenarios that simulate modern cyber attacks and defenses. Whether you're protecting sensitive data, ensuring regulatory compliance, or safeguarding organizational reputation, this training provides the tools to create an unbreakable security posture.

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. **Identify and mitigate common and emerging cyber threats**, including malware, phishing, ransomware, and APTs (Advanced Persistent Threats).
2. **Implement robust security frameworks** and best practices aligned with standards such as NIST, ISO 27001, and CIS Controls.
3. **Conduct vulnerability assessments and penetration testing** to proactively identify weaknesses.
4. **Design and enforce effective security policies** for networks, cloud environments, and endpoints.
5. **Respond to and recover from security incidents** using structured incident response methodologies.
6. **Promote a culture of security awareness** within their organization to reduce human-related risks.

Who Should Attend?

This course is ideal for:

- **IT and Network Administrators**
- **Cyber Security Analysts and SOC Team Members**
- **Risk and Compliance Officers**
- **System Architects and DevOps Engineers**
- **IT Managers and CISO Aspirants**
- **Anyone responsible for safeguarding digital assets**

Course Outline

Day 1: Fundamentals of Cyber Threats and Defense Strategies

- **Module 1:** Introduction to the Cyber Threat Landscape
- **Module 2:** Core Principles of Confidentiality, Integrity, and Availability (CIA Triad)
- **Module 3:** Overview of Security Frameworks (NIST, ISO 27001)
- **Hands-On Lab:** Setting Up a Secure Lab Environment
- **Case Study:** Anatomy of a Real-World Data Breach

Day 2: Network Security and Infrastructure Hardening

- **Module 4:** Secure Network Architecture Design
- **Module 5:** Firewalls, IDS/IPS, and VPNs
- **Module 6:** Endpoint Protection and Mobile Device Management
- **Hands-On Lab:** Configuring Firewalls and Intrusion Detection Systems
- **Group Exercise:** Designing a Secure Network for a Fictional Organization

Day 3: Vulnerability Management and Penetration Testing

- **Module 7:** Vulnerability Scanning and Risk Assessment
- **Module 8:** Ethical Hacking Techniques and Tools
- **Module 9:** Secure Coding and Application Security
- **Hands-On Lab:** Conducting a Penetration Test Using Kali Linux
- **Workshop:** Analyzing and Patching Vulnerabilities

Course Outline

Day 4: Incident Response and Recovery

- **Module 10:** Incident Response Lifecycle (Preparation to Recovery)
- **Module 11:** Digital Forensics and Evidence Handling
- **Module 12:** Disaster Recovery and Business Continuity Planning
- **Simulation Exercise:** Responding to a Ransomware Attack
- **Tabletop Exercise:** Incident Response Role-Play

Day 5: Security Governance and Future-Proofing

- **Module 13:** Cyber Security Policies and Employee Training
- **Module 14:** Cloud Security and IoT Threats
- **Module 15:** Emerging Trends (AI in Security, Quantum Computing Risks)
- **Capstone Project:** Developing a Comprehensive Security Plan
- **Course Wrap-Up:** Certification, Q&A, and Next Steps

المقدمة

في عالمنا الرقمي اليوم، تتطور التهديدات السيبرانية بوتيرة غير مسبوقة، مستهدفةً المؤسسات بجميع أحجامها وقطاعاتها. لم تعد القدرة على الدفاع ضد هذه التهديدات خيارًا، بل أصبحت ضرورةً أساسيةً للأعمال. صُممت **دورة "الأمن السيبراني غير القابل للاختراق"** لتزويد المحترفين بالمعرفة المتقدمة والمهارات العملية اللازمة لبناء وإدارة وحماية بنى تحتية مرنة لتكنولوجيا المعلومات. تتجاوز هذه الدورة النظرية، حيث تقدم سيناريوهات عملية واقعية تُحاكي الهجمات والدفاعات السيبرانية الحديثة. سواءً كنتَ تحمي بياناتك الحساسة، أو تضمن الامتثال للوائح التنظيمية، أو تحمي سمعة مؤسستك، فإن هذا التدريب يوفر لك الأدوات اللازمة لبناء بيئة أمنية حصينة.

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. **تحديد وتخفيف التهديدات السيبرانية الشائعة والناشئة** ، بما في ذلك البرامج الضارة، والتصيد الاحتيالي، وبرامج الفدية، والتهديدات المستمرة المتقدمة.
2. **تنفيذ أطر عمل أمنية قوية** وأفضل الممارسات المتوافقة مع معايير مثل NIST وISO 27001 وضوابط CIS.
3. **إجراء تقييمات الثغرات واختبارات الاختراق** لتحديد نقاط الضعف بشكل استباقي.
4. **تصميم وتنفيذ سياسات أمنية فعالة** للشبكات وبيئات السحابة ونقاط النهاية.
5. **الاستجابة للحوادث الأمنية والتعافي منها** باستخدام منهجيات الاستجابة للحوادث المنظمة.
6. **تعزيز ثقافة الوعي الأمني** داخل مؤسستهم للحد من المخاطر المتعلقة بالإنسان

من ينبغي أن يهتم؟

هذه الدورة مثالية ل:

- **مسؤولي تكنولوجيا المعلومات والشبكات**
- **محللو الأمن السيبراني وأعضاء فريق مركز العمليات الأمنية**
- **مسؤولي المخاطر والامتثال**
- **مهندسو الأنظمة ومهندسو DevOps**
- **مديري تكنولوجيا المعلومات والمرشحين لمنصب CISO**
- **أي شخص مسؤول عن حماية الأصول الرقمية**

محتويات الكورس

اليوم الأول أساسيات التهديدات السيبرانية واستراتيجيات الدفاع

- **الوحدة 1:** مقدمة عن مشهد التهديدات السيبرانية
- **الوحدة 2:** المبادئ الأساسية للسرية والنزاهة والتوافر (ثالوث وكالة المخابرات المركزية)
- **الوحدة 3:** نظرة عامة على أطر الأمان (NIST، ISO 27001)
- **مختبر عملي:** إعداد بيئة مختبر آمنة
- **دراسة حالة:** تشريح خرق البيانات في العالم الحقيقي

اليوم الثاني أمن الشبكات وتعزيز البنية التحتية

- **الوحدة 4:** تصميم بنية الشبكة الآمنة
- **الوحدة 5:** جدران الحماية، وأنظمة كشف التسلل/منع التطفل، وشبكات VPN
- **الوحدة 6:** حماية نقطة النهاية وإدارة الأجهزة المحمولة
- **مختبر عملي:** تكوين جدران الحماية وأنظمة كشف التسلل
- **تمرين جماعي:** تصميم شبكة آمنة لمنظمة خيالية

اليوم الثالث إدارة الثغرات الأمنية واختبار الاختراق

- **الوحدة 7:** مسح الثغرات الأمنية وتقييم المخاطر
- **الوحدة 8:** تقنيات وأدوات الاختراق الأخلاقي
- **الوحدة 9:** الترميز الآمن وأمان التطبيقات
- **مختبر عملي:** إجراء اختبار اختراق باستخدام Kali Linux
- **ورشة عمل:** تحليل الثغرات الأمنية وتصحيحها

محتويات الكورس

اليوم الرابع الاستجابة للحوادث والتعافي منها

- **الوحدة 10:** دورة حياة الاستجابة للحوادث (التحضير للتعافي)
- **الوحدة 11:** الأدلة الجنائية الرقمية والتعامل مع الأدلة
- **الوحدة 12:** التعافي من الكوارث وتخطيط استمرارية الأعمال
- **تمرين محاكاة:** الاستجابة لهجوم برامج الفدية
- **تمرين الطاولة:** لعب الأدوار للاستجابة للحوادث

اليوم الخامس حوكمة الأمن والتحضير للمستقبل

- **الوحدة 13:** سياسات الأمن السيبراني وتدريب الموظفين
- **الوحدة 14:** أمن السحابة وتهديدات إنترنت الأشياء
- **الوحدة 15:** الاتجاهات الناشئة (الذكاء الاصطناعي في مجال الأمن، ومخاطر الحوسبة الكمومية)
- **مشروع التخرج:** تطوير خطة أمنية شاملة
- **ملخص الدورة:** الشهادة، والأسئلة والأجوبة، والخطوات التالية

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:

- 12/01/2026 - 16/01/2026 Click Now
- 01/06/2026 - 05/06/2026 Click Now
- 19/10/2026 - 23/10/2026 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