Protect Your Digital Fortress

Cyber Security and Technology

Advanced Cyber Security Protect Your Digital Fortress

Code: 259007

FUTURE CENTRE
مركز المستقبل

futurecentre.net

Course Introduction

In today's hyper-connected world, organizations face an ever-evolving barrage of sophisticated cyber threats. Traditional security measures are no longer sufficient to protect critical digital assets. This advanced course moves beyond the basics to equip you with the strategic knowledge and tactical skills needed to build, defend, and manage a resilient "digital fortress."

This intensive, five-day program delves into the mindset of adversaries, explores cutting-edge attack vectors, and teaches advanced defensive techniques. Through a combination of expert instruction, hands-on labs, and real-world case studies, participants will learn to architect robust security postures, proactively hunt for threats, and respond effectively to incidents, ensuring their organization can operate securely in a hostile digital landscape.

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

- **Analyze** and **deconstruct** advanced persistent threat (APT) methodologies and modern malware.
- **Design** and **implement** a defense-in-depth strategy incorporating zero-trust principles.
- **Conduct** proactive threat hunting to identify indicators of compromise (IOCs) and advanced attacks lurking within networks.
- **Master** advanced techniques in penetration testing to identify critical vulnerabilities before attackers do.
- **Develop** and **execute** a comprehensive incident response plan to contain, eradicate, and recover from security breaches.
- **Evaluate** and **harden** cloud security postures across major platforms (AWS, Azure, GCP).
- **Implement** robust security controls for critical assets, including data encryption, access management, and network segmentation.

Who Should Attend?

This advanced course is designed for IT and security professionals with foundational cybersecurity knowledge who are responsible for protecting organizational infrastructure and data.

- **Security Architects** & **Network Security Engineers**
- **SOC Analysts (Tier 2/3)** & **Threat Hunters**
- **Penetration Testers** & **Vulnerability Assessors**
- **Incident Responders** & **CSIRT Team Members**
- **Senior System Administrators** & **Network Administrators**
- **IT Managers** & **Security Consultants** overseeing security strategy
- **Cloud Security Specialists**

Prerequisites: A solid understanding of networking fundamentals (TCP/IP, DNS, HTTP/S) and basic cybersecurity concepts (firewalls, viruses, phishing). Experience in a technical IT role is highly recommended.

Course Outline

Day 1: Foundations of the Modern Digital Fortress

- **Module 1: The Evolving Threat Landscape**
- **Advanced Persistent Threats (APTs), Nation-State Actors, and Cybercrime Ecosystems**
- **The Cyber Kill Chain & MITRE ATT&CK Framework**
- **Module 2: Architecting for Security: Zero Trust & Defense-in-Depth**
- **Principles of Zero Trust Architecture (ZTA)**
- **Designing a layered defensive strategy**
- **Hands-On Lab: Mapping a real-world APT campaign to the MITRE ATT&CK framework.**

Day 2: Advanced Threat Analysis and Vulnerability Management

- **Module 3: Deconstructing Advanced Malware**
  - Static and Dynamic Analysis of sophisticated malware
  - Reverse engineering fundamentals for threat intelligence
- **Module 4: Proactive Defense: Vulnerability Management & Penetration Testing**
  - Prioritizing risk with threat-led vulnerability management
  - Advanced penetration testing methodologies (OWASP Top 10, network pivoting)
- **Hands-On Lab:** Conducting a dynamic malware analysis in a controlled sandbox environment.

Day 3: Securing the Perimeterless Network: Cloud & Data

- **Module 5: Cloud Security Posture Management (CSPM)**
  - Common misconfigurations in AWS, Azure, and GCP
  - Implementing identity and access management (IAM) best practices in the cloud
- **Module 6: Protecting the Crown Jewels: Data Security**
  - Advanced Data Loss Prevention (DLP) strategies
  - Implementing encryption (at-rest, in-transit, in-use) and tokenization
- **Hands-On Lab:** Identifying and remediating critical misconfigurations in a simulated cloud environment.

Course Outline

Day 4: The Human Element: Threat Hunting & Access Control

- **Module 7: Proactive Threat Hunting**
  - Developing hypotheses, crafting queries (using SIEM, EDR)
  - Hunting for IOCs and anomalous behavior across endpoints and networks
- **Module 8: Advanced Identity and Access Management**
  - Privileged Access Management (PAM) solutions and strategies
  - Defending against credential-based attacks (e.g., Pass-the-Hash, Golden Ticket)
- **Hands-On Lab:** Using a SIEM to hunt for evidence of a lateral movement attack.

Day 5: Mastering Incident Response & Resilience

- **Module 9: Cyber Incident Response Mastery**
  - The SANS Incident Response Cycle: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned
  - Evidence collection and forensics fundamentals for responders
- **Module 10: Building a Resilient Future**
  - Developing and testing your incident response plan
  - Crisis communication and tabletop exercises
  - Course Recap and Building a Personal Action Plan
- **Capstone Exercise:** A simulated full-scale cyber incident where teams must respond, contain the threat, and present a lessons-learned report.

المقدمة

في عالمنا اليوم المترابط للغاية، تواجه المؤسسات وابلًا متطورًا من التهديدات السيبرانية المعقدة. لم تعد إجراءات الأمن التقليدية كافية لحماية الأصول الرقمية الحيوية. تتجاوز هذه الدورة المتقدمة الأساسيات لتزويدك بالمعرفة الاستراتيجية والمهارات التكتيكية اللازمة لبناء "حصن رقمي" متين والدفاع عنه وإدارته.
يتعمق هذا البرنامج المكثف، الذي يستمر خمسة أيام، في عقلية الخصوم، ويستكشف أحدث أساليب الهجوم، ويُدرِّس تقنيات دفاعية متقدمة. من خلال مزيج من التدريبات المتخصصة، والمختبرات العملية، ودراسات الحالة الواقعية، سيتعلم المشاركون كيفية بناء مواقف أمنية فعّالة، والتصدي للتهديدات بشكل استباقي، والاستجابة بفعالية للحوادث، مما يضمن قدرة مؤسساتهم على العمل بأمان في بيئة رقمية عدائية.

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 إكمال هذه الدورة بنجاح، سيكون المشاركون قادرين على:

- **تحليل** وتفكيك **منهجيات** التهديدات المستمرة المتقدمة (APT) والبرامج الضارة الحديثة.
- **تصميم** وتنفيذ استراتيجية الدفاع المتعمق التي تتضمن مبادئ الثقة الصفرية .
- **إجراء** بحث استباقي عن التهديدات لتحديد مؤشرات الاختراق والهجمات المتقدمة الكامنة داخل الشبكات.
- **إتقان** التقنيات المتقدمة في اختبار الاختراق لتحديد نقاط الضعف الحرجة قبل أن يفعلها المهاجمون.
- **تطوير** وتنفيذ خطة شاملة للاستجابة **للحوادث** لاحتواء خروقات الأمن والقضاء عليها والتعافي منها.
- **تقييم** وتعزيز مواقف أمان السحابة عبر المنصات الرئيسية (AWS و **Azure** وGCP).
- **تنفيذ** ضوابط أمنية قوية للأصول المهمة، بما في ذلك تشفير البيانات وإدارة الوصول وتقسيم الشبكة

من ينبغي أن يهتم؟

تم تصميم هذه الدورة المتقدمة لمحترفي تكنولوجيا المعلومات والأمن الذين لديهم معرفة أساسية بالأمن السيبراني والذين يتحملون مسؤولية حماية البنية التحتية والبيانات التنظيمية.

- **مهندسو الأمن** ومهندسو **أمن الشبكات**
- **محللو مركز العمليات الأمنية (المستوى 2/3)** وصائدو **التهديدات**
- **مختبرو الاختراق** ومقيّمو **الثغرات الأمنية**
- **المستجيبون للحوادث** وأعضاء **فريق الاستجابة للحوادث الأمنية الحاسوبية**
- **كبار مسؤولي النظام** ومسؤولي **الشبكة**
- **مديري تكنولوجيا المعلومات** ومستشاري **الأمن** الذين يشرفون على استراتيجية الأمن
- **متخصصون في أمن السحابة**

المتطلبات الأساسية: فهم متين لأساسيات الشبكات (TCP/IP، DNS، HTTP/S) ومفاهيم الأمن السيبراني الأساسية (جدران الحماية، الفيروسات، التصيد الاحتيالي). يُنصح بشدة بخبرة في مجال تقنية المعلومات

محتويات الكورس

اليوم الأول أسس الحصن الرقمي الحديث

- **الوحدة 1: مشهد التهديدات المتطور**
  - التهديدات المستمرة المتقدمة (APTs)، والجهات الفاعلة من الدول القومية، وأنظمة الجرائم الإلكترونية
  - سلسلة القتل السيبراني وإطار عمل MITRE ATT&CK
- **الوحدة 2: هندسة الأمن: الثقة الصفرية والدفاع المتعمق**
  - مبادئ هندسة الثقة الصفرية (ZTA)
  - تصميم استراتيجية دفاعية متعددة الطبقات
- **مختبر عملي:** رسم خريطة لحملة APT في العالم الحقيقي لإطار عمل MITRE ATT&CK.

اليوم الثاني تحليل التهديدات المتقدمة وإدارة الثغرات الأمنية

- **الوحدة 3: تفكيك البرامج الضارة المتقدمة**
  - التحليل الثابت والديناميكي للبرامج الضارة المتطورة
  - أساسيات الهندسة العكسية لاستخبارات التهديدات
- **الوحدة 4: الدفاع الاستباقي: إدارة الثغرات الأمنية واختبار الاختراق**
  - إعطاء الأولوية للمخاطر من خلال إدارة الثغرات القائمة على التهديدات
  - منهجيات اختبار الاختراق المتقدمة (أفضل 10 في OWASP، محور الشبكة)
- **مختبر عملي:** إجراء تحليل ديناميكي للبرامج الضارة في بيئة رملية خاضعة للرقابة

اليوم الثالث تأمين الشبكة بلا محيط: السحابة والبيانات

- **الوحدة 5: إدارة وضع أمن السحابة (CSPM)**
  - التكوينات الخاطئة الشائعة في AWS وAzure وGCP
  - تنفيذ أفضل ممارسات إدارة الهوية والوصول (IAM) في السحابة
- **الوحدة 6: حماية جواهر التاج: أمن البيانات**
  - استراتيجيات منع فقدان البيانات المتقدمة (DLP)
  - تنفيذ التشفير (في حالة السكون، أثناء النقل، أثناء الاستخدام) والترميز
- **مختبر عملي:** تحديد وإصلاح التكوينات الخاطئة الحرجة في بيئة سحابية محاكاة

محتويات الكورس

اليوم الرابع العنصر البشري: البحث عن التهديدات والتحكم في الوصول

- **الوحدة 7: البحث الاستباقي عن التهديدات**
  - تطوير الفرضيات، وصياغة الاستعلامات (باستخدام SIEM وEDR)
  - البحث عن مؤشرات الأداء الرئيسية والسلوك الشاذ عبر نقاط النهاية والشبكات
- **الوحدة 8: إدارة الهوية والوصول المتقدمة**
  - حلول واستراتيجيات إدارة الوصول المتميز (PAM)
  - الدفاع ضد الهجمات القائمة على بيانات الاعتماد (على سبيل المثال، Pass-the-Hash، Golden Ticket)
- **مختبر عملي:** استخدام SIEM للبحث عن أدلة على هجوم الحركة الجانبية

اليوم الخامس إتقان الاستجابة للحوادث والمرونة

- **الوحدة 9: إتقان الاستجابة للحوادث السيبرانية**
  - دورة الاستجابة للحوادث في SANS: التحضير، والتحديد، والاحتواء، والاستئصال، والتعافي، والدروس المستفادة
  - أساسيات جمع الأدلة والطب الشرعي للمستجيبين
- **الوحدة 10: بناء مستقبل مرن**
  - تطوير واختبار خطة الاستجابة للحوادث الخاصة بك
  - التواصل في حالات الأزمات وتمارين الطاولة
  - ملخص الدورة وبناء خطة عمل شخصية
- **تمرين التخرج:** محاكاة لحادثة سيبرانية كاملة النطاق حيث يتعين على الفرق الاستجابة واحتواء التهديد وتقديم تقرير الدروس المستفادة

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:

- 16/02/2026 - 20/02/2026 Click Now
- 06/07/2026 - 10/07/2026 Click Now
- 23/11/2026 - 27/11/2026 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