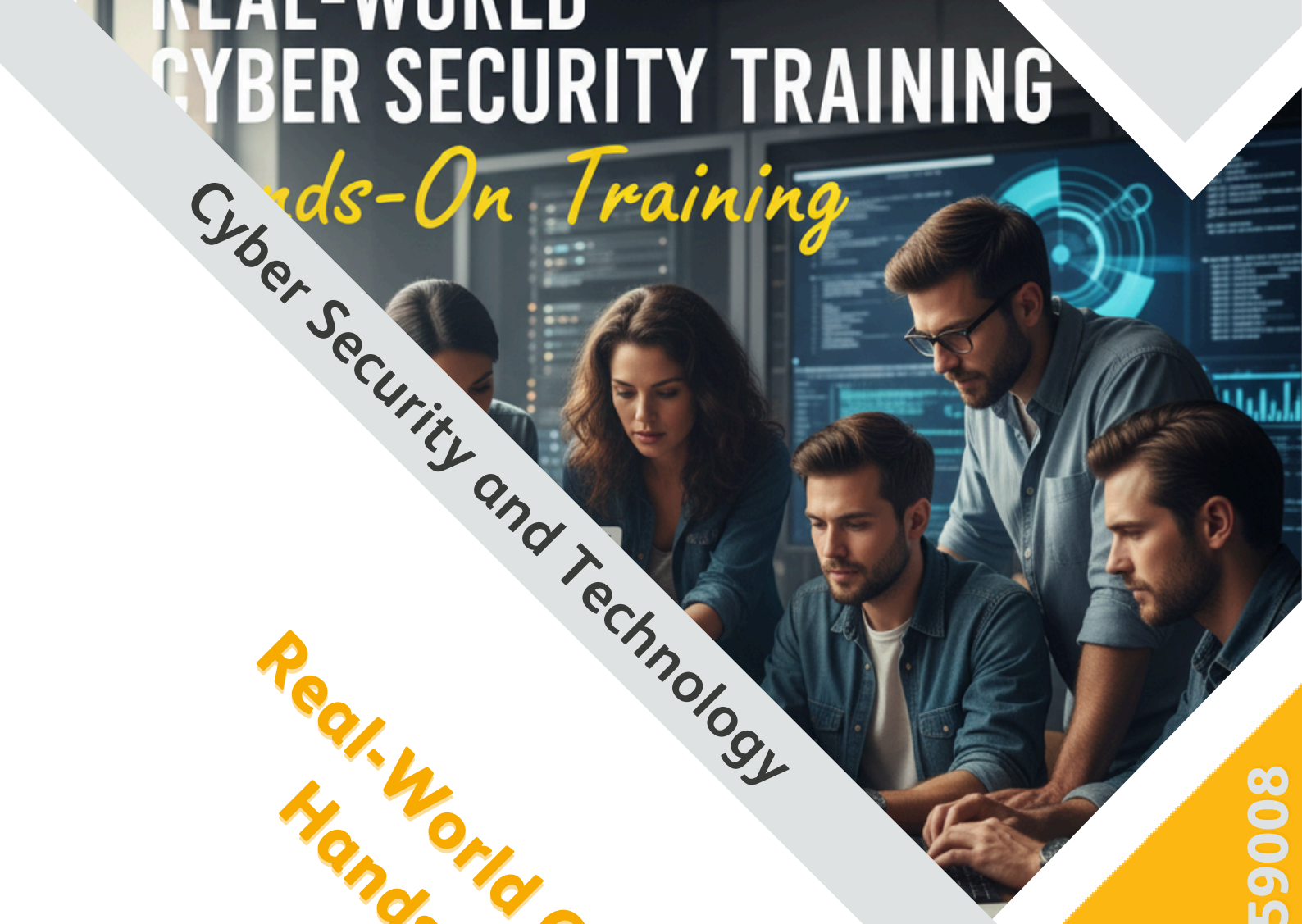

Cyber Security and Technology

Real-World Cyber Security Hands-On Training

Code: 259008

FUTURE CENTRE
مركز المستقبل

futurecentre.net

Course Introduction

Theory alone is not enough to defend against modern cyber threats. Security professionals need practical, hands-on experience with the tools and techniques used by both attackers and defenders in the field. This intensive, five-day course is built entirely around a immersive, lab-driven curriculum.

Participants will be immersed in a simulated enterprise environment where they will learn by doing. You will exploit vulnerabilities, analyze malware, respond to live incidents, and configure security tools just as you would on the job. This course provides the critical, real-world experience needed to build confidence and proficiency in core cybersecurity disciplines, from penetration testing to incident response.

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:

- **Execute** a structured penetration test, from reconnaissance and exploitation to post-exploitation and reporting.
- **Identify, analyze, and contain** live security incidents within a corporate network.
- **Apply** digital forensics techniques to acquire evidence and perform analysis on disk images and memory dumps.
- **Configure** and **utilize** essential security tools including SIEM, EDR, and firewalls for active defense.
- **Analyze** real-world malware samples to understand their functionality and extract indicators of compromise (IOCs).
- **Develop** and **practice** incident response procedures through a full-scale simulation.

Who Should Attend?

This course is designed for individuals who need to develop practical, technical skills in cybersecurity operations.

- **Aspiring Security Analysts** (SOC Tier 1)
- **System Administrators** and **Network Administrators** looking to transition into security roles
- **IT Professionals** wanting to gain hands-on cybersecurity skills
- **Junior Penetration Testers**
- **Computer Science/IT Students** with a focus on security
- **IT Managers** who want to understand the technical challenges their teams face

Prerequisites: Basic understanding of networking (IP addresses, TCP/UDP, ports) and Windows/Linux operating systems. No prior security experience is required, but a strong technical curiosity is essential.

Course Outline

Day 1: The Attacker's Playbook – Hands-On Penetration Testing

- **Module 1: Passive & Active Reconnaissance**
  - Hands-On: Using tools like whois, nslookup, and nmap to scout a target network.
- **Module 2: Exploitation Fundamentals**
  - Hands-On: Exploiting common vulnerabilities (e.g., in web apps, network services) to gain initial access.
- **Module 3: Post-Exploitation & Pivoting**
  - Hands-On: Maintaining access, escalating privileges, and moving laterally through the network.
- **Lab 1:** Capture-the-flag style exercise to compromise a target server.

Day 2: Defensive Operations – Monitoring and Detection

- **Module 4: Introduction to SIEM & Log Analysis**
  - Hands-On: Ingesting logs into a SIEM (e.g., Splunk, Elastic Stack) and writing basic correlation rules.
- **Module 5: Endpoint Detection and Response (EDR)**
  - Hands-On: Using an EDR tool to monitor processes, network connections, and detect malicious activity.
- **Module 6: Network Security Monitoring**
  - Hands-On: Analyzing PCAP files with Wireshark to identify malicious traffic and data exfiltration.
- **Lab 2:** Hunt for malicious activity based on SIEM alerts and PCAP analysis.

Day 3: Digital Forensics Fundamentals

- **Module 7: Disk Forensics**
  - Hands-On: Acquiring a disk image and analyzing it with Autopsy/FTK to find hidden files, timelining, and artifact recovery.
- **Module 8: Memory Forensics**
  - Hands-On: Using Volatility to analyze a memory dump for evidence of running malware, rootkits, and network connections.
- **Module 9: Live System Triage**
  - Hands-On: Using trusted tools to analyze a live, compromised system without altering evidence.
- **Lab 3:** Solve a forensic mystery by finding how a system was compromised and what data was stolen.

Course Outline

Day 4: Malware Analysis and Incident Response

- **Module 10: Malware Analysis in a Sandbox**
  - Hands-On: Safely executing malware samples in a contained environment and analyzing behavioral reports.
- **Module 11: Static Analysis**
  - Hands-On: Extracting strings, examining imports, and identifying basic packers without running the code.
- **Module 12: The Incident Response Cycle**
  - Lecture & Discussion: Walkthrough of NIST SP 800-61 (Preparation, Detection, Containment, Eradication, Recovery).
- **Lab 4:** Analyze a provided malware sample and produce a IOC report.

Day 5: Capstone Day – Full-Scale Incident Response Simulation

- **The Scenario:** A multi-stage attack is in progress. Participants are the emergency response team.
- **Phase 1: Detection & Triage:** Receive the initial alert and begin investigation using SIEM, EDR, and network tools.
- **Phase 2: Containment & Eradication:** Isolate affected systems, kill malicious processes, and remove attacker persistence.
- **Phase 3: Recovery & Lessons Learned:** Secure the environment, restore systems from clean backups, and write an incident report.
- **Final Debrief:** Teams present their findings, actions taken, and lessons learned from the simulation.

المقدمة

النظرية وحدها لا تكفي للدفاع ضد التهديدات السيبرانية الحديثة. يحتاج متخصصو الأمن إلى خبرة عملية ومباشرة في الأدوات والتقنيات التي يستخدمها كل من المهاجمين والمدافعين في الميدان. هذه الدورة المكثفة، التي تمتد لخمسة أيام، مبنية بالكامل على منهج دراسي شامل قائم على التجارب العملية.
سينخرط المشاركون في بيئة عمل افتراضية، حيث سيتعلمون بالممارسة. ستستغلون الثغرات الأمنية، وتحللون البرامج الضارة، وتستجيبون للحوادث المباشرة، وتُهيئون أدوات الأمن كما تفعلون في العمل. توفر هذه الدورة الخبرة العملية الحاسمة اللازمة لبناء الثقة والكفاءة في تخصصات الأمن السيبراني الأساسية، من اختبار الاختراق إلى الاستجابة للحوادث.

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:

- **تنفيذ** اختبار اختراق منظم، من الاستطلاع والاستغلال إلى مرحلة ما بعد الاستغلال وإعداد التقارير.
- **تحديد وتحليل واحتواء** الحوادث الأمنية المباشرة داخل شبكة الشركة.
- **تطبيق** تقنيات الطب الشرعي الرقمي لجمع الأدلة وإجراء التحليلات على صور الأقراص ومكبات الذاكرة.
- **قم بتكوين** واستخدام أدوات الأمان الأساسية بما في ذلك SIEM وEDR وجدران الحماية للدفاع النشط.
- **قم بتحليل** عينات البرامج الضارة في العالم الحقيقي لفهم وظائفها واستخراج مؤشرات الاختراق (IOCs).
- **تطوير** وممارسة إجراءات الاستجابة للحوادث من خلال محاكاة كاملة النطاق

من ينبغي أن يهتم؟

تم تصميم هذه الدورة للأفراد الذين يحتاجون إلى تطوير مهارات عملية وفنية في عمليات الأمن السيبراني.

- **محللو الأمن الطموحون** (SOC Tier 1)
- **مسؤولو النظام** ومسؤولو **الشبكة** الذين يتطلعون إلى الانتقال إلى أدوار أمنية
- **متخصصو تكنولوجيا المعلومات** الذين يرغبون في اكتساب مهارات عملية في مجال الأمن السيبراني
- **مختبرو الاختراق المبتدئون**
- **طلاب علوم الكمبيوتر/تكنولوجيا المعلومات** مع التركيز على الأمن
- **مديري تكنولوجيا المعلومات** الذين يريدون فهم التحديات الفنية التي تواجه فرقهم

المتطلبات الأساسية: فهم أساسي للشبكات (عناوين IP، TCP/UDP، المنافذ) وأنظمة تشغيل Windows/Linux. لا يشترط خبرة أمنية سابقة، ولكن الفضول التقني القوي ضروري

محتويات الكورس

اليوم الأول دليل المهاجم - اختبار الاختراق العملي

- **الوحدة 1: الاستطلاع السلبي والنشط**
  - التدريب العملي: استخدام أدوات مثل gwhois gnslookup nmap لاستكشاف شبكة مستهدفة.
- **الوحدة 2: أساسيات الاستغلال**
  - التدريب العملي: استغلال الثغرات الأمنية الشائعة (على سبيل المثال، في تطبيقات الويب وخدمات الشبكة) للحصول على الوصول الأولي.
- **الوحدة 3: ما بعد الاستغلال والتحول**
  - عملي: الحفاظ على إمكانية الوصول، وتصعيد الامتيازات، والتحرك أفقياً عبر الشبكة.
- **المختبر 1:** تمرين على نمط الاستيلاء على العلم لاختراق الخادم المستهدف.

اليوم الثاني العمليات الدفاعية - المراقبة والكشف

- **الوحدة 4: مقدمة إلى SIEM وتحليل السجلات**
  - التدريب العملي: إدخال السجلات إلى SIEM (على سبيل المثال، Elastic، Splunk Stack) وكتابة قواعد الارتباط الأساسية.
- **الوحدة 5: اكتشاف نقطة النهاية والاستجابة لها (EDR)**
  - التدريب العملي: استخدام أداة EDR لمراقبة العمليات واتصالات الشبكة واكتشاف الأنشطة الضارة.
- **الوحدة 6: مراقبة أمن الشبكة**
  - التدريب العملي: تحليل ملفات PCAP باستخدام Wireshark لتحديد حركة المرور الضارة واستخراج البيانات.
- **المختبر 2:** البحث عن الأنشطة الضارة استنادًا إلى تنبيهات SIEM وتحليل PCAP.

اليوم الثالث أساسيات الطب الشرعي الرقمي

- **الوحدة 7: تحليلات القرص**
  - التدريب العملي: الحصول على صورة قرص وتحليلها باستخدام Autopsy/FTK للعثور على الملفات المخفية والجدول الزمني واستعادة القطع الأثرية.
- **الوحدة 8: تحليلات الذاكرة**
  - تطبيق عملي: استخدام Volatility لتحليل تفريغ الذاكرة بحثًا عن أدلة على تشغيل البرامج الضارة، وبرامج الجذر، واتصالات الشبكة.
- **الوحدة 9: فرز النظام المباشر**
  - التدريب العملي: استخدام أدوات موثوقة لتحليل نظام حي ومخترق دون تغيير الأدلة.
- **المختبر 3:** حل لغز الطب الشرعي من خلال معرفة كيفية اختراق النظام وما هي البيانات التي تمت سرقتها.

محتويات الكورس

اليوم الرابع تحليل البرامج الضارة والاستجابة للحوادث

- **الوحدة 10: تحليل البرامج الضارة في بيئة اختبار**
  - التدريب العملي: تنفيذ عينات البرامج الضارة بشكل آمن في بيئة محددة وتحليل التقارير السلوكية.
- **الوحدة 11: التحليل الثابت**
  - التدريب العملي: استخراج السلاسل، وفحص الواردات، وتحديد الحزم الأساسية دون تشغيل الكود.
- **الوحدة 12: دورة الاستجابة للحوادث**
  - محاضرة ومناقشة: شرح مفصل لمعيار NIST SP 800-61 (التحضير، الكشف، الاحتواء، الاستئصال، الاسترداد).
- **المختبر 4:** تحليل عينة من البرامج الضارة المقدمة وإنتاج تقرير IOC

اليوم الخامس يوم المشروع الختامي - محاكاة الاستجابة للحوادث على نطاق واسع

- **السيناريو:** هجوم متعدد المراحل قيد التنفيذ. المشاركون هم فريق الاستجابة للطوارئ.
- **المرحلة 1: الكشف والفرز:** تلقي التنبيه الأولي وبدء التحقيق باستخدام SIEM وEDR وأدوات الشبكة.
- **المرحلة الثانية: الاحتواء والاستئصال:** عزل الأنظمة المتأثرة، وقتل العمليات الضارة، وإزالة استمرار المهاجم.
- **المرحلة 3: الاسترداد والدروس المستفادة:** تأمين البيئة، واستعادة الأنظمة من النسخ الاحتياطية النظيفة، وكتابة تقرير عن الحادث.
- **الإحاطة النهائية:** تقدم الفرق نتائجها، والإجراءات التي اتخذتها، والدروس المستفادة من المحاكاة.

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:

- 23/02/2026 - 27/02/2026 Click Now
- 13/07/2026 - 17/07/2026 Click Now
- 30/11/2026 - 04/12/2026 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