

CYBER STRONG

Your Security Blueprint

Cyber Security and Technology

Cyber Strong Your Security
Blueprint

Code: 259003



FUTURE CENTRE
مركز المستقبل




futurecentre.net



Course Introduction

In an era of escalating cyber threats, organizations must move beyond reactive measures and build proactive, resilient security infrastructures. **Cyber Strong: Your Security Blueprint** is a comprehensive course designed to equip professionals with the strategic and technical expertise needed to develop, implement, and manage an end-to-end cybersecurity framework. This training combines theoretical foundations with hands-on labs, real-world case studies, and blueprint-style planning to help participants create tailored security strategies aligned with organizational goals. Whether defending against ransomware, securing cloud environments, or ensuring regulatory compliance, this course provides the actionable insights to build an unbreakable defense.

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. **Analyze emerging cyber threats** and adapt defenses to evolving attack vectors.
2. **Design and implement a layered security architecture** using industry-standard frameworks (NIST, ISO 27001, CIS Controls).
3. **Conduct risk assessments** and prioritize mitigations based on impact and likelihood.
4. **Deploy and manage security tools** for networks, endpoints, cloud, and data protection.
5. **Lead incident response efforts** to contain, eradicate, and recover from breaches.
6. **Develop and enforce security policies** that promote a culture of cyber resilience.

Who Should Attend?

This course is ideal for:

- **IT and Cybersecurity Professionals** (Analysts, Administrators, Engineers)
- **Risk and Compliance Officers**
- **System and Network Architects**
- **IT Managers and Aspiring CISOs**
- **DevSecOps Practitioners**
- **Anyone responsible for organizational security**

Course Outline

Day 1: Building the Foundation – Threats and Frameworks

- **Module 1:** The Modern Cyber Threat Landscape (APTs, Ransomware, Insider Threats)
- **Module 2:** Core Security Principles: CIA Triad, Zero Trust, and Defense-in-Depth
- **Module 3:** Industry Frameworks: NIST CSF, ISO 27001, and CIS Controls
- **Hands-On Lab:** Risk Identification and Assessment Workshop
- **Case Study:** Dissecting a Major Data Breach

Day 2: Network and Infrastructure Security

- **Module 4:** Secure Network Design: Segmentation, VLANs, and NAC
- **Module 5:** Firewalls, IDS/IPS, and VPN Configuration
- **Module 6:** Wireless and IoT Security Best Practices
- **Hands-On Lab:** Configuring Firewall Rules and Intrusion Detection
- **Group Exercise:** Designing a Secure Network Architecture

Day 3: Endpoint, Cloud, and Data Protection

- **Module 7:** Endpoint Security: EDR, Anti-Malware, and Hardening
- **Module 8:** Cloud Security (AWS/Azure): IAM, Encryption, and CASB
- **Module 9:** Data Loss Prevention (DLP) and Encryption Strategies
- **Hands-On Lab:** Securing a Cloud Environment and Implementing DLP
- **Workshop:** Responding to a Simulated Endpoint Compromise

Course Outline

Day 4: Incident Response and Recovery

- **Module 10:** Incident Response Lifecycle: Preparation, Detection, and Containment
- **Module 11:** Digital Forensics: Evidence Collection and Analysis
- **Module 12:** Disaster Recovery and Business Continuity Planning
- **Simulation Exercise:** Tabletop Incident Response Drill
- **Lab:** Forensic Analysis of a Breach Scenario

Day 5: Governance and Future-Proofing


- **Module 13:** Security Policies, Awareness Training, and Compliance (GDPR, HIPAA)
- **Module 14:** Emerging Trends: AI in Security, Quantum Risks, and Supply Chain Threats
- **Module 15:** Creating Your Security Blueprint: Strategy and Roadmap Development
- **Capstone Project:** Building a Customized Security Blueprint
- **Course Wrap-Up:** Certification and Action Planning



المقدمة

في عصر تتصاعد فيه التهديدات السيبرانية، يتعين على المؤسسات تجاوز الإجراءات التفاعلية وبناء بنى تحتية أمنية استباقية ومرنة. "القوة السيبرانية: مخططك الأمني" دورة شاملة مصممة لتزويد المحترفين بالخبرة الاستراتيجية والتقنية اللازمة لتطوير وتنفيذ وإدارة إطار عمل متكامل للأمن السيبراني. يجمع هذا التدريب بين الأسس النظرية والمختبرات العملية ودراسات الحالة الواقعية والتخطيط بأسلوب المخططات، لمساعدة المشاركين على وضع استراتيجيات أمنية مصممة خصيصًا بما يتماشى مع أهداف المؤسسة. سواءً كان الهدف هو الدفاع ضد برامج الفدية، أو تأمين بيانات السحابة، أو ضمان الامتثال للوائح التنظيمية، توفر هذه الدورة رؤى عملية لبناء دفاع قوي.

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. تحليل التهديدات السيبرانية الناشئة وتكييف الدفاعات مع متجهات الهجوم المتطورة.
 2. تصميم وتنفيذ بنية أمنية متعددة الطبقات باستخدام الأطر القياسية في الصناعة (NIST، ISO 27001، CIS Controls).
 3. إجراء تقييمات المخاطر وإعطاء الأولوية للتخفيف منها على أساس التأثير والاحتمالية.
 4. نشر وإدارة أدوات الأمان للشبكات ونقاط النهاية والسحابة وحماية البيانات.
 5. قيادة جهود الاستجابة للحوادث لاحتواء الخروقات والقضاء عليها والتعافي منها.
 6. تطوير وتنفيذ سياسات أمنية تعزز ثقافة المرونة السيبرانية

من ينبغي أن يهتم؟

- هذه الدورة مثالية ل:
- متخصصو تكنولوجيا المعلومات والأمن السيبراني (المطلون والمسؤولون والمهندسون)
 - مسؤولي المخاطر والامتثال
 - مهندسو النظم والشبكات
 - مديري تكنولوجيا المعلومات ومسؤولي أمن المعلومات الطموحين
 - ممارسو DevSecOps
 - أي شخص مسؤول عن الأمن التنظيمي

محتويات الكورس

اليوم الأول بناء الأساس - التهديدات والأطر

- الوحدة 1: مشهد التهديدات السيبرانية الحديثة (الهجمات المستمرة المتقدمة، وبرامج الفدية، والتهديدات الداخلية)
- الوحدة 2: مبادئ الأمن الأساسية: ثلوث وكالة المخابرات المركزية، والثقة الصفريّة، والدفاع المتعمق
- الوحدة 3: أطر الصناعة: معايير NIST CSF و ISO 27001 وضوابط CIS
- ورشة عمل عملية: ورشة عمل تحديد المخاطر وتقييمها
- دراسة حالة: تحليل خرق كبير للبيانات

اليوم الثاني أمن الشبكات والبنية التحتية

- الوحدة 4: تصميم الشبكة الآمنة: التجزئة، وشبكات VLAN، وNAC
- الوحدة 5: جدران الحماية، وأنظمة كشف التسلل/منع التطفل، وتكوين الشبكات الافتراضية الخاصة (VPN)
- الوحدة 6: أفضل ممارسات أمن الاتصالات اللاسلكية وإنترنت الأشياء
- مختبر عملي: تكوين قواعد جدار الحماية واكتشاف التطفل
- تمرين جماعي: تصميم بنية شبكة آمنة

اليوم الثالث نقطة النهاية والسحابة وحماية البيانات

- الوحدة 7: أمان نقطة النهاية: EDR، ومكافحة البرامج الضارة، والتحصين
- الوحدة 8: أمان السحابة (AWS/Azure): IAM والتشفير وCASB
- الوحدة 9: منع فقدان البيانات (DLP) واستراتيجيات التشفير
- مختبر عملي: تأمين بيئة سحابية وتنفيذ منع فقدان البيانات (DLP)
- ورشة عمل: الاستجابة لاختراق نقطة نهاية محاكاة

محتويات الكورس

اليوم الرابع الاستجابة للحوادث والتعافي منها

- الوحدة 10: دورة حياة الاستجابة للحوادث: التحضير والكشف والاحتواء
- الوحدة 11: الأدلة الجنائية الرقمية: جمع الأدلة وتحليلها
- الوحدة 12: التعافي من الكوارث وتخطيط استمرارية الأعمال
- تمرين محاكاة: تمرين الاستجابة للحوادث على الطاولة
- المختبر: التحليل الجنائي لسيناريو الاختراق

اليوم الخامس الحوكمة وتأمين المستقبل

- الوحدة 13: سياسات الأمان، والتدريب على التوعية، والامتثال (اللائحة العامة لحماية البيانات، وقانون التأمين الصحي المحمول والمساءلة)
- الوحدة 14: الاتجاهات الناشئة: الذكاء الاصطناعي في الأمن، ومخاطر الكم، وتهديدات سلسلة التوريد
- الوحدة 15: إنشاء مخططك الأمني: تطوير الاستراتيجية وخريطة الطريق
- مشروع التخرج: بناء مخطط أمني مخصص
- ملخص الدورة: الاعتماد وتخطيط العمل

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:



19/01/2026 - 23/01/2026

[Click Now](#)



08/06/2026 - 12/06/2026

[Click Now](#)



26/10/2026 - 30/10/2026

[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