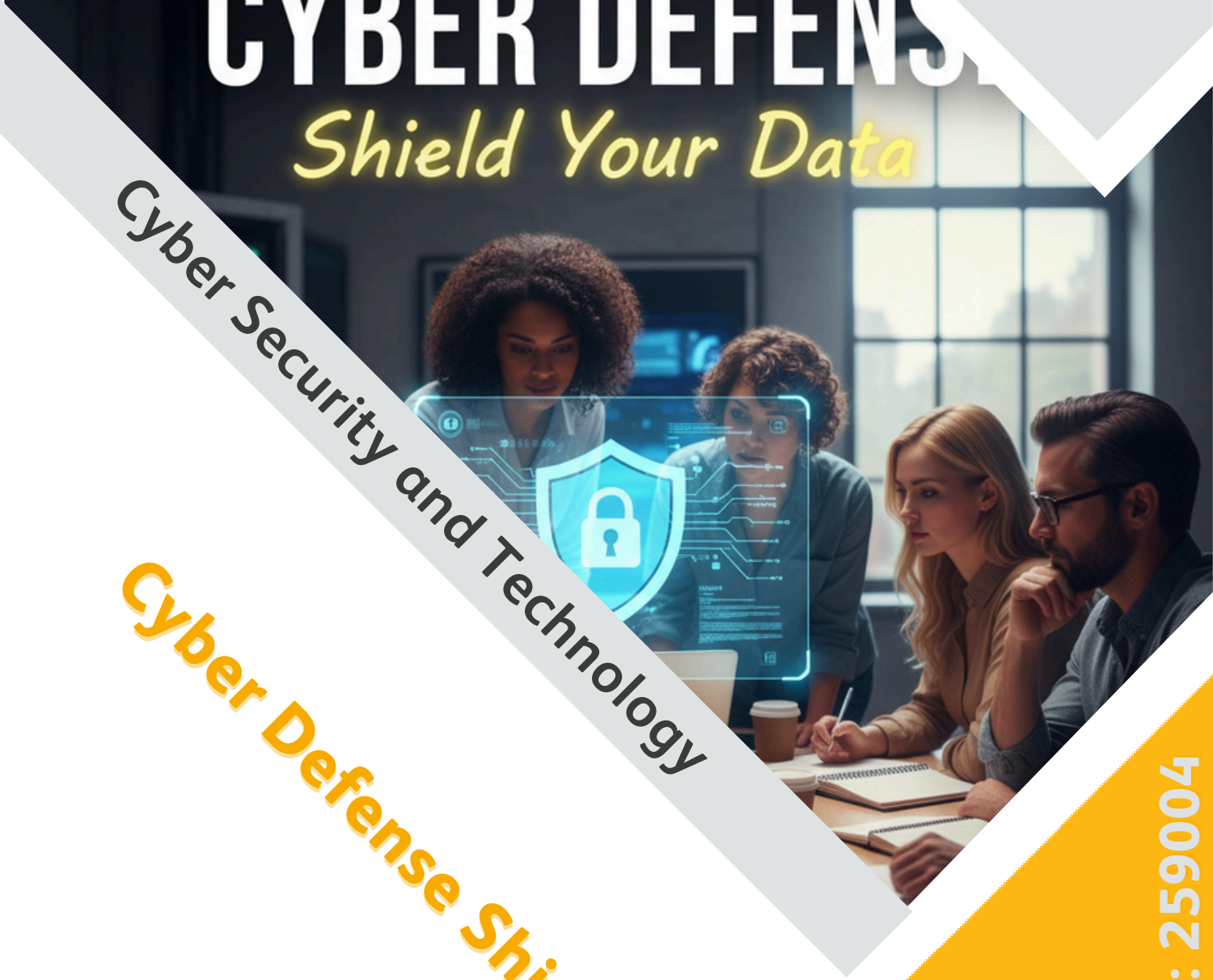

Cyber Security and Technology

Cyber Defense Shield Your Data

Code: 259004

FUTURE CENTRE
مركز المستقبل

futurecentre.net

Course Introduction

In the digital age, data is the lifeblood of organizations and the prime target for cyber adversaries. A single breach can lead to devastating financial losses, reputational damage, and regulatory penalties. Protecting this critical asset requires more than just generic security measures; it demands a focused, strategic, and robust defense-in-depth approach specifically designed around data. **Cyber Defense Shield: Your Data** is a specialized course that moves beyond perimeter security to focus on the core of what needs protection: your information.

This course provides a comprehensive blueprint for building an unbreachable data security program. Participants will learn to classify sensitive data, implement cutting-edge encryption and access controls, monitor for exfiltration attempts, and respond effectively to data-centric incidents. This is not just a theoretical overview; it is a practical, hands-on training program designed to equip you with the skills to create a resilient shield around your most valuable asset.

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:

- **Classify and Discover Sensitive Data:** Identify, categorize, and locate critical data across on-premises and cloud environments.
- **Design a Data-Centric Security Architecture:** Implement a layered defense strategy using encryption, tokenization, and data masking.
- **Enforce Strict Access Governance:** Apply the principles of Least Privilege and Zero Trust to control who can access data, when, and from where.
- **Deploy Data Loss Prevention (DLP) Solutions:** Configure and manage DLP tools to monitor, detect, and prevent unauthorized data transfer and exfiltration.
- **Respond to Data Breaches:** Execute a targeted incident response plan specifically for data compromise scenarios.
- **Ensure Compliance with Data Regulations:** Navigate the requirements of GDPR, HIPAA, CCPA, and other data protection laws.

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: The Data Security Foundation

Morning:

- **Module 1: The Value of Data & The Threat Landscape:** Understanding why data is targeted. Overview of common data breach vectors (insider threats, phishing, misconfigurations).
- **Module 2: Data Security Principles:** Core concepts of Confidentiality, Integrity, and Availability (CIA) as they apply specifically to data.

Afternoon:

- **Module 3: Data Discovery and Classification:** Techniques and tools for finding and categorizing sensitive data (PII, PHI, IP, financial data) across the enterprise.
- **Hands-On Lab 1: Using a Discovery Tool:** Participants use tools to scan a simulated network environment to locate and classify sensitive data.
- **Day 1 Recap: Knowing what you have and where it lives.**

Day 2: Building the Shield – Encryption & Access Control

Morning:

- **Module 4: Cryptography Fundamentals:** Symmetric vs. Asymmetric encryption, hashing, and digital signatures.
- **Module 5: Implementing Encryption:** Data-at-Rest (Disk, Database) and Data-in-Transit (SSL/TLS, VPN) encryption strategies.

Afternoon:

- **Module 6: Advanced Data Protection:** Tokenization and Data Masking techniques for development and testing environments.
- **Hands-On Lab 2: Encrypting a Database & Configuring TLS:** Practical exercises in applying encryption to protect data.
- **Day 2 Recap: Rendering data useless to thieves.**

Day 3: Monitoring & Preventing Data Loss

Morning:

- **Module 7: Data Loss Prevention (DLP) Deep Dive:** Understanding DLP architectures (Network, Endpoint, Cloud).
- **Module 8: Designing DLP Policies:** Creating effective rules to block, quarantine, or alert on sensitive data movement.

Afternoon:

- **Module 9: Access Governance & Zero Trust for Data:** Implementing strict access controls, Multi-Factor Authentication (MFA), and Just-In-Time access.
- **Hands-On Lab 3: Configuring a DLP Policy:** Participants create and test DLP rules in a simulated corporate environment to prevent data exfiltration via email and USB.
- **Day 3 Recap: Watching the gates and controlling the keys.**

Course Outline

Day 4: Responding to a Data Incident

Morning:

- **Module 10: Data-Centric Incident Response:** Specialized procedures for containing and investigating a suspected data breach.
- **Module 11: Digital Forensics for Data Theft:** Techniques for identifying what data was taken, when, and by whom.

Afternoon:

- **Module 12: Breach Notification and Compliance:** Understanding legal requirements for disclosing breaches to regulators and affected individuals.
- **Tabletop Exercise: The Data Breach Simulation:** Teams work through a scenario involving a massive data leak, making critical decisions on containment, communication, and eradication.
- **Day 4 Recap: Having a plan for when things go wrong.**

Day 5: Strategy, Compliance, and Capstone

Morning:

- **Module 13: Building a Data Security Program:** Developing policies, standards, and procedures. Aligning with frameworks like NIST Privacy Framework and ISO 27001.
- **Module 14: Navigating Global Data Regulations:** GDPR, CCPA, HIPAA – key requirements and how technical controls help achieve compliance.

Afternoon:

- **Capstone Project: The Data Security Audit:**
  i. Participants are given a scenario of a company with poor data controls.
  ii. They must perform a mock audit: discover data, assess risks, and design a complete “Data Defense Shield” blueprint including policies, technical controls, and monitoring.
- **Presentation & Review:** Teams present their blueprints and receive feedback.
- **Course Conclusion:** Final Q&A, resources, and awarding of certificates.

المقدمة

في العصر الرقمي، تُعدّ البيانات شريان الحياة للمؤسسات والهدف الرئيسي للمهاجمين السيبرانيين. قد يؤدي أي اختراق واحد إلى خسائر مالية فادحة، وإضرار بالسمعة، وعقوبات تنظيمية. تتطلب حماية هذه الأصول الحيوية أكثر من مجرد تدابير أمنية عامة؛ بل تتطلب نهجًا دفاعيًا مُركّزًا واستراتيجيًا وقويًا ومُعمّقًا مُصمّمًا خصيصًا للبيانات. " **درع الدفاع السيبراني: بياناتك** " دورة تدريبية متخصصة تتجاوز أمن المحيط لتركز على جوهر ما يحتاج إلى حماية: معلوماتك.

تقدم هذه الدورة مخططًا شاملاً لبناء برنامج أمن بيانات محصن ضد الاختراق. سيتعلم المشاركون تصنيف البيانات الحساسة، وتطبيق أحدث تقنيات التشفير وضوابط الوصول، ومراقبة محاولات الاختراق، والاستجابة بفعالية للحوادث المتعلقة بالبيانات. هذه ليست مجرد نظرة عامة نظرية، بل هي برنامج تدريب عملي مصمم لتزويدك بالمهارات اللازمة لبناء درع قوي يحمي أغلى أصولك

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:

- **تصنيف البيانات الحساسة واكتشافها:** تحديد البيانات المهمة وتصنيفها وتحديد موقعها عبر البيئات المحلية والسحابية.
- **تصميم بنية أمان تركز على البيانات:** تنفيذ استراتيجية دفاعية متعددة الطبقات باستخدام التشفير وتجزئة البيانات وإخفاء البيانات.
- **فرض حوكمة صارمة للوصول:** تطبيق مبادئ الحد الأدنى من الامتياز والثقة الصفرية للتحكم في من يمكنه الوصول إلى البيانات، ومتى، ومن أين.
- **نشر حلول منع فقدان البيانات (DLP):** قم بتكوين أدوات منع فقدان البيانات (DLP) وإدارتها لمراقبة واكتشاف ومنع نقل البيانات غير المصرح بها وتسربها.
- **الاستجابة لانتهاكات البيانات:** تنفيذ خطة استجابة للحوادث مستهدفة خصيصًا لسيناريوهات اختراق البيانات.
- **ضمان الامتثال للوائح البيانات:** تصفح متطلبات GDPR وHIPAA وCCPA وقوانين حماية البيانات الأخرى

من ينبغي أن يهتم؟

تعد هذه الدورة ضرورية للمحترفين الذين تشمل مسؤولياتهم حماية البيانات الحساسة أو إدارتها أو حوكمتها.

- **محللون ومتخصصون في أمن البيانات**
- **مديري ومسؤولي أمن تكنولوجيا المعلومات**
- **مسؤولي الشبكة والنظام**
- **مسؤولي الامتثال والمخاطر**
- **مهندسو أمن السحابة**
- **مسؤولي قواعد البيانات (DBAs)**
- **أي شخص مشارك في تصميم أو تنفيذ استراتيجيات حماية البيانات**

محتويات الكورس

اليوم الأول مؤسسة أمن البيانات

صباح:

- **الوحدة ١: قيمة البيانات ومشهد التهديدات:** فهم أسباب استهداف البيانات. نظرة عامة على عوامل اختراق البيانات الشائعة (التهديدات الداخلية، والتصيد الاحتيالي، والتكوينات الخاطئة).
- **الوحدة 2: مبادئ أمن البيانات:** المفاهيم الأساسية للسرية والنزاهة والتوافر (CIA) كما تنطبق على البيانات على وجه التحديد.

بعد الظهر:

- **الوحدة 3: اكتشاف البيانات وتصنيفها:** تقنيات وأدوات للعثور على البيانات الحساسة وتصنيفها (معلومات التعريف الشخصية، والمعلومات الصحية الشخصية، والملكية الفكرية، والبيانات المالية) عبر المؤسسة.
- **المختبر العملي 1: استخدام أداة الاكتشاف:** يستخدم المشاركون أدوات لمسح بيئة شبكة محاكاة لتحديد البيانات الحساسة وتصنيفها.
- **ملخص اليوم الأول: معرفة ما لديك وأين يوجد.**

اليوم الثاني بناء الدرع - التشفير والتحكم في الوصول

صباح:

- **الوحدة 4: أساسيات التشفير:** التشفير المتماثل مقابل التشفير غير المتماثل، والتجزئة، والتوقيعات الرقمية.
- **الوحدة 5: تنفيذ التشفير:** استراتيجيات تشفير البيانات الساكنة (القرص، قاعدة البيانات) والبيانات أثناء النقل (SSL/TLS، VPN).

بعد الظهر:

- **الوحدة 6: حماية البيانات المتقدمة:** تقنيات التجزئة وإخفاء البيانات لبيئات التطوير والاختبار.
- **المختبر العملي 2: تشفير قاعدة البيانات وتكوين TLS:** تمارين عملية في تطبيق التشفير لحماية البيانات.
- **ملخص اليوم الثاني: جعل البيانات عديمة الفائدة للصوص.**

اليوم الثالث مراقبة ومنع فقدان البيانات

صباح:

- **الوحدة 7: الغوص العميق في منع فقدان البيانات (DLP):** فهم هياكل منع فقدان البيانات (الشبكة، نقطة النهاية، السحابة).
- **الوحدة 8: تصميم سياسات منع فقدان البيانات:** إنشاء قواعد فعالة لمنع أو حجر أو تنبيه حركة البيانات الحساسة.

بعد الظهر:

- **الوحدة 9: حوكمة الوصول والثقة الصفرية للبيانات:** تنفيذ ضوابط وصول صارمة، والمصادقة متعددة العوامل (MFA)، والوصول في الوقت المناسب.
- **المختبر العملي 3: تكوين سياسة منع فقدان البيانات (DLP):** يقوم المشاركون بإنشاء قواعد منع فقدان البيانات واختبارها في بيئة مؤسسية محاكاة لمنع تسرب البيانات عبر البريد الإلكتروني وUSB.
- ملخص اليوم الثالث: مراقبة البوابات والتحكم بالمفاتيح.

محتويات الكورس

اليوم الرابع الاستجابة لحادثة البيانات

صباح:

- **الوحدة 10: الاستجابة للحوادث المتعلقة بالبيانات:** إجراءات متخصصة لاحتواء خرق البيانات المشتبه به والتحقيق فيه.
- **الوحدة 11: التحليلات الرقمية لسرقة البيانات:** تقنيات لتحديد البيانات التي تم أخذها، ومتى، ومن قبل من.

بعد الظهر:

- **الوحدة 12: إخطار الخروقات والامتثال لها:** فهم المتطلبات القانونية للإفصاح عن الخروقات للجهات التنظيمية والأفراد المتضررين.
- **تمرين على الطاولة: محاكاة خرق البيانات:** تعمل الفرق من خلال سيناريو يتضمن تسربًا هائلاً للبيانات، واتخاذ قرارات حاسمة بشأن الاحتواء والاتصال والقضاء.
- **ملخص اليوم الرابع: وضع خطة للتعامل مع الأمور عندما تسوء.**

اليوم الخامس الاستراتيجية والامتثال والمشروع النهائي

صباح:

- **الوحدة ١٣: بناء برنامج لأمن البيانات:** تطوير السياسات والمعايير والإجراءات. التوافق مع أطر عمل مثل إطار عمل الخصوصية للمعهد الوطني للمعايير والتكنولوجيا (NIST) ومعيار ISO ٢٧٠٠١.
- **الوحدة 14: التنقل بين لوائح البيانات العالمية:** اللائحة العامة لحماية البيانات ، وقانون خصوصية المستهلك في كاليفورنيا، وقانون التأمين الصحي المحمول والمساءلة (HIPAA) - المتطلبات الرئيسية وكيف تساعد الضوابط الفنية في تحقيق الامتثال.

بعد الظهر:

- **مشروع التخرج: تدقيق أمن البيانات:**
  i. يتم منح المشاركين سيناريو لشركة ذات ضوابط بيانات ضعيفة.
  ii. يتعين عليهم إجراء تدقيق تجريبي: اكتشاف البيانات، وتقييم المخاطر، وتصميم مخطط "درع الدفاع عن البيانات" الكامل بما في ذلك السياسات، والضوابط الفنية، والمراقبة.
- **العرض والمراجعة:** تقدم الفرق مخططاتها وتتلقى التعليقات.
- **اختتام الدورة:** الأسئلة والأجوبة النهائية، والموارد، ومنح الشهادات

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:

- 26/01/2026 - 30/01/2026 Click Now
- 15/06/2026 - 19/06/2026 Click Now
- 02/11/2026 - 06/11/2026 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