



التحول الرقمي

التحول الرقمي وأمان المعلومات

Course Introduction

يهدف هذا البرنامج التدريبي إلى تقديم فهما شامل حول كيفية تحقيق التحول الرقمي مع ضمان أمن المعلومات في كافة المراحل، وكيفية حماية البيانات والبنية التحتية الرقمية من الهجمات الإلكترونية.

Target Audience

- مدراء تكنولوجيا المعلومات.
- فرق التحول الرقمي.
- المختصون في تطوير واستراتيجيات التحول الرقمي.
- القادة وصناع القرار في المؤسسات الحكومية والخاصة.

Learning Objectives

عقب الانتهاء من هذا البرنامج التدريبي، سيتمكن المشاركون من

- التعرف على دور وأهمية التحول الرقمي وأثره على المؤسسات.
- فهم كيفية تأمين البيانات وحمايتها في ظل التحول الرقمي.
- التعرف على التحديات الأمنية التي تواجه المؤسسات أثناء تنفيذ التحول الرقمي.
- إتقان إدارة وتطبيق استراتيجيات أمن المعلومات في سياق التحول الرقمي.
- استكشاف الأدوات والتقنيات الحديثة المستخدمة في ضمان أمن المعلومات في البيئة الرقمية.
- تعزيز القدرة على إدارة المخاطر المرتبطة بالتحول الرقمي وأمن المعلومات.

Course Outline

• day one

مقدمة في التحول الرقمي وأمان المعلومات

- مفهوم التحول الرقمي وأهدافه.
- كيف يغير التحول الرقمي بيئة الأعمال والمجتمع.
- دور التكنولوجيا في تحسين الكفاءة والابتكار.
- مفهوم أمان المعلومات وأهدافه.
- مكونات أمان المعلومات: السرية، التكامل، والتوافر.
- التهديدات والتحديات الأمنية في العالم الرقمي.

استراتيجية التحول الرقمي

- تطوير رؤية التحول الرقمي.
- تحليل البيئة الداخلية والخارجية للمؤسسة.
- تحديد الأهداف الرئيسية للتحول الرقمي.
- مقاومة التغيير والتحديات الثقافية.
- إدارة الموارد والتكلفة.
- دمج التقنيات الحديثة في بيئة العمل الحالية.

• day two

مكونات التحول الرقمي في المؤسسات

- مفهوم السحابة وكيفية استخدامها في المؤسسات.
- استراتيجيات الانتقال إلى السحابة وتأثيرها على الأمن.
- وأنظمة الأعمال الأخرى، CRM، ERP، تطبيقات الهواتف المحمولة، أنظمة.
- أهمية تحليل البيانات وذكاء الأعمال في دعم التحول الرقمي.

أدوات وتقنيات أمان المعلومات في البيئة الرقمية

- أساليب التشفير وحماية البيانات من السرقة.
- تقنيات تشفير البيانات في السحابة، البريد الإلكتروني، والتطبيقات الأخرى.

- IDS و IPS: أدوات الكشف عن الهجمات.
 - كيف تحمي المؤسسات من الهجمات الموجهة والمتقدمة.
- day three

تهديدات الأمن السيبراني في التحول الرقمي

- أنواع الهجمات الإلكترونية الشائعة: الفيروسات، البرمجيات الخبيثة، هجمات DDoS.
- كيف تتعامل المؤسسات مع الهجمات الإلكترونية.
- التهديدات الأمنية في تطبيقات الويب.
- كيفية تأمين تطبيقات الهواتف المحمولة في بيئة العمل.

إدارة المخاطر الرقمية في التحول الرقمي

- كيفية تحديد وتحليل المخاطر الرقمية المرتبطة بالتحول الرقمي.
 - استراتيجيات لإدارة المخاطر الرقمية في المؤسسات.
 - استخدام أدوات التقييم والمراجعة الأمنية.
 - تحديد المخاطر المرتبطة بالشبكات، السحابة، والمعلومات الحساسة.
- day four

الحوكمة الرقمية وأمان المعلومات

- وضع استراتيجيات حوكمة المعلومات وأمانها.
- المسؤوليات القانونية والتنظيمية في الحوكمة الرقمية.
- مراجعة القوانين الدولية والمحلية لحماية البيانات.
- وكيفية تطبيقها في بيئة المؤسسات الرقمية CISO و GDPR قوانين مثل.

أتمتة أمان المعلومات في المؤسسات

- كيفية أتمتة آليات الحماية والرقابة في البيئة الرقمية.
 - أدوات وبرمجيات تساعد في أتمتة أمان المعلومات.
 - أدوات لرد الفعل السريع على الهجمات والتهديدات.
 - تطوير آليات لتسريع استجابة الحوادث الأمنية في الأنظمة الرقمية.
- day five

تطوير ثقافة الأمان في المؤسسات الرقمية

- أهمية الوعي الأمني في المؤسسات.
- كيفية بناء برامج تدريب فعالة للمؤسسات.
- استراتيجيات لتقليل الضرر من الهجمات الإلكترونية.
- كيفية رفع مستوى استعداد المؤسسة لمواجهة الهجمات المستقبلية.

ورشة عمل تطبيقية يتم فيها تطوير مهارات المشاركين على الحفاظ على أمان المعلومات أثناء تنفيذ مشروعات التحول الرقمي.

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
May 5, 2025	May 9, 2025	5 days	4950.00 \$	Turkey - Istanbul
Aug. 11, 2025	Aug. 15, 2025	5 days	4250.00 \$	UAE - Dubai
Nov. 9, 2025	Nov. 13, 2025	5 days	4250.00 \$	KSA - Riyadh