غرفة تجارة عمّان
AMMAN CHAMBER OF COMMERCE

نموذج المحتوى التدريبي		
نموذج جودة ومخاطر	رقم الإصدار: 2/2	الصفحة: 4/1

العنوان باللغة العربية:	الأمن السيبراني : حماية الأنظمة والمعلومات من التهديدات الرقمية	العنوان باللغة الإنجليزية:	**Cybersecurity: Protecting Systems and Information from Digital Threats**
عدد الساعات التدريبية:	(60) ساعة تدريبية		
أيام البرنامج التدريبي:	السبت والاحد والثلاثاء والاربعاء من الساعة 5:00 عصرا ولغاية 00: 8 مساءًا		
تاريخ البرنامج التدريبي:	2025/11/29 ولغاية 2025/12/30		
قاعة / مختبر:	قاعات أكاديمية غرفة تجارة عمان للتدريب – الشميساني		
الرسوم المقررة:	لأعضاء الغرفة: (300) دينار.	لغير الأعضاء: (325) دينار.	
خصم المجموعات:	• خصم بنسبة 10% على رسوم المشارك الواحد إبتداءً من المشارك الثاني في حال قامت المنشأة بإنتداب إثنين من موظفيها وبحدٍ أقصى أربعة موظفين. • خصم بنسبة 15% على رسوم المشارك الواحد إبتداءً من المشارك الثاني في حال قامت المنشأة بإنتداب أكثر من أربعة من موظفيها. 🔗 ميثاق رضا مُتلقي خدمات أكاديمية غرفة تجارة عمان للتدريب تجربة تدريبية متميزة: برامجنا يقدمها نخبة من المدربين الخبراء لضمان تجربة تعليمية رائدة. الالتزام بالمواعيد: تنفيذ البرامج التدريبية في المواعيد المعلنة دون تأخير. رضاك هو أولويتنا: إذا لم يحقق تابرنامج توقعاتك, يمكنك الانسحاب بعد الجلسة الأولى و استرداد الرسوم كاملة. https://ammanchamber.org.jo/wsimages/808080.pdf		
الأهداف:	• تزويد المشاركين بالمعرفة الأساسية والمتقدمة في مجال الأمن السيبراني. • تطوير مهارات تحليل التهديدات واكتشاف الثغرات الأمنية. • إعداد المشاركين لتطبيق إجراءات وقائية واستباقية ضد الهجمات الإلكترونية. • التدريب على أدوات وتطبيقات احترافية تُستخدم في مجال الاختراق الأخلاقي والحماية. • تعزيز مهارات إعداد خطط الاستجابة للطوارئ الرقمية واسترجاع الأنظمة.		

غرفة تجارة عمّان
AMMAN CHAMBER OF COMMERCE

نموذج المحتوى التدريبي		
نموذج جودة ومخاطر	رقم الإصدار: 2/2	الصفحة: 4/2

المحتويات:	**المحور الأول: مقدمة في الأمن السيبراني (4 ساعات)** • **المحتوى النظري:** ○ **تعريف الأمن السيبراني وأهميته.** ○ **أنواع التهديدات والهجمات السيبرانية.** ○ **الفرق بين الأمن السيبراني وأمن المعلومات.** ○ **الإطار القانوني والأخلاقي للأمن الرقمي.** • **التطبيق العملي:** ○ **مناقشة حالات واقعية لهجمات سيبرانية.** ○ **تحليل خبر صحفي/تقني لهجوم حديث وأثره.** **المحور الثاني: مكونات البنية التحتية للأمن السيبراني (6 ساعات)** • **المحتوى النظري:** ○ **طبقات الحماية في الشبكات وأنظمة التشغيل.** ○ **أنواع الجدران النارية.(Firewalls)** ○ **أنظمة كشف التسلل (IDS) ومنع التسلل.(IPS)** ○ **أمن الأجهزة والهواتف المحمولة.** • **التطبيق العملي:** ○ **إعداد جدار ناري بسيط وتجربة قواعد الحماية.** ○ **استخدام أداة IDS لمراقبة نشاط الشبكة.** ○ **تمرين على حماية جهاز محمول بإعدادات أمان.** **المحور الثالث: أنواع الهجمات وأساليبها (10 ساعات)** • **المحتوى النظري:** ○ **البرمجيات الخبيثة :(Malware) فيروسات، Trojans، .(Ransomware** ○ **هجمات التصيد الاحتيالي.(Phishing Attacks)** ○ **هجمات حجب الخدمة.(DDoS)** ○ **الهندسة الاجتماعية.(Social Engineering)** ○ **اختراق كلمات المرور وطرق الحماية منها.** • **التطبيق العملي:** ○ **تجربة محاكاة لهجوم تصيد احتيالي وتحليل رسائل البريد المزيفة.** ○ **تنفيذ هجوم DDoS وهمي على بيئة افتراضية.** ○ **تمرين على كسر كلمة مرور ضعيفة ومقارنتها بكلمة مرور قوية.** **المحور الرابع: إدارة الهوية والتحكم بالوصول (6 ساعات)** • **المحتوى النظري:** ○ **أنظمة إدارة الهوية.(IAM)** ○ **المصادقة متعددة العوامل.(MFA)** ○ **صلاحيات المستخدمين والتسجيل الآمن.**

- إدارة كلمات المرور والتوثيق.
- التطبيق العملي:
  - تفعيل خاصية المصادقة الثنائية (2FA) على حساب تجريبي.
  - إنشاء حسابات بمستويات صلاحيات مختلفة.
  - تجربة أداة إدارة كلمات المرور.

المحور الخامس: أمن الشبكات والبروتوكولات (8 ساعات)

- المحتوى النظري:
  - حماية الشبكات اللاسلكية.(Wi-Fi Security)
  - تشفير البيانات ونقلها بأمان.(VPN, SSL/TLS)
  - أساسيات تحليل حزم البيانات.
  - إعدادات الشبكة الآمنة.
- التطبيق العملي:
  - تجربة إعداد VPN على شبكة محلية.
  - استخدام Wireshark لتحليل حركة مرور البيانات.
  - اختبار إعدادات الأمان لشبكة لاسلكية.

المحور السادس: اختبار الاختراق الأخلاقي (Ethical Hacking) (8 ساعات)

- المحتوى النظري:
  - مقدمة في اختبار الاختراق الأخلاقي.
  - مراحل الاختراق.Reconnaissance, Scanning, Gaining Access :
  - الأدوات الشهيرة مثل Kali Linux و.Metasploit
- التطبيق العملي:
  - محاكاة اختبار اختراق على نظام افتراضي.
  - استخدام Metasploit لاختبار ثغرة محددة.
  - تجربة عملية لهجوم ودفاع في بيئة تدريبية.

المحور السابع: الاستجابة للحوادث والتعافي (4 ساعات)

- المحتوى النظري:
  - خطة الاستجابة للحوادث.
  - تحليل آثار الهجمات.
  - آليات استرجاع الأنظمة والبيانات.
  - دور الفرق الأمنية.
- التطبيق العملي:
  - إعداد خطة استجابة وهمية لهجوم سيبراني.
  - تمرين على استرجاع ملفات مشفرة) محاكاة.(Ransomware
  - لعب أدوار بين فريق الهجوم والدفاع.

	المحور الثامن: المشروع التطبيقي والاختبار النهائي (4 ساعات) • **المحتوى النظري:** ○ **عرض متطلبات المشروع النهائي.** ○ **شرح منهجية تقييم شاملة للبرنامج.** • **التطبيق العملي:** ○ **تنفيذ مشروع لحماية شبكة أو مؤسسة افتراضية.** ○ **تحليل الثغرات الأمنية وتقديم توصيات للتحسين.** ○ **اختبار نهائي لتقييم المعارف والمهارات المكتسبة.**
المشاركون:	• مسؤولو أمن المعلومات في المؤسسات • مدراء الأنظمة والشبكات • طلبة وخريجو تكنولوجيا المعلومات والحاسوب • المهتمون بالعمل في مجال الأمن السيبراني • رواد الأعمال الراغبون بحماية بيانات مشاريعهم
لغة التدريب:	امكانية عقد البرنامج باللغة العربية و/أو اللغة الانجليزية
عدد المتدربين:	غير محدد