إسم البرنامج

الأمن السيبراني

☆☆☆☆☆ Cybersecurity

أهداف البرنامج :

- تعريف المتدربين بأهمية الامن السيبراني في العصر الحالي
- تحليل نقاط القوة و الضعف في نظام الامن في المنظمة و حمايتها من الهجمات الخارجية
- حماية البيانات الشخصية و بيانات المنظمة من المتسللين و الطرق المختلفة للنسخ الإحتياطية و جدران الحماية

محاور البرنامج :

الفصل الأول: الحاجة إلى الأمن السيبراني

- مقدمة في البيانات الشخصية
- مقدمة في البيانات التنظيمية
- أنواع البيانات التنظيمية
- السرية والنزاهة والتوافر
- تأثير ونتائج الخرق الأمني
- متخصصو الهجمات والأمن السيبراني
- لمحة عن مهاجم إلكتروني
- الحرب الإلكترونية
- نظرة عامة على الحرب الإلكترونية

الفصل الثاني: الهجمات والمفاهيم والأساليب

- تحليل الأمن السيبراني
- نقاط الضعف الأمنية والمآثر
- أنواع الثغرات الأمنية
- أنواع البرامج الضارة والأعراض
- طرق التسلل
- هندسة اجتماعية
- DoS و DDos و SEO
- تحليل الأمن السيبراني
- هجوم مختلط
- تقليل التأثير
- خصوصية البريد الإلكتروني ومتصفح الويب

الفصل الثالث : حماية بياناتك وخصوصيتك

- استخدم الشبكة اللاسلكية بأمان
- تشفير وصيانة بياناتك
- حماية خصوصيتك على الإنترنت
- مصادقة قوية
- توثيق ذو عاملين
- OAuth 2.0

الفصل الرابع: حماية المنظمة

- أنواع جدار الحماية
- أجهزة الأمن
- كشف الهجمات في الوقت الحقيقي
- الحماية والكشف ضد البرامج الضارة
- أفضل ممارسات الأمان
- نهج السلوك للأمن السيبراني
- سلسلة القتل الدفاعية الإلكترونية
- الأمن القائم على السلوك
- NetFlow و Cyberattack
- نهج Ciscco للأمن السيبراني
- CSIRT
- أدوات لمنع الحوادث واكتشافها
- IDS و IPS
- القضايا القانونية والأخلاقية المتعلقة بالأمن السيبراني والتعليم والمهن
- دليل الأمان

الفئة المستهدفة :

- موظفين أقسام أمن المعلومات و المتعلقة وظائفهم بحماية الشبكات و أصحاب المنشئات المتوسطة و الصغيرة
- الطلاب و خريجي أقسام أمن المعلومات و علوم الحاسب

أسلوب تنفيذ البرنامج :

- عروض تقديمية - محاضرات نقاشية - ورش عمل - دراسة حالات عملية - عرض بعض الرسوم والمخططات والفيديوهات
- البرنامج متوفر باللغة العربية / اللغة الإنجليزية
- البرنامج متوفر حضوري / أونلاين

الإستمرار في التدريب ... استمرار التطوير