**البرنامج المتقدم في أمن المعلومات الإلكترونية**

**المقدمة**

مع التوسع المتسارع في استخدام التقنيات الرقمية والاعتماد المتنامي على الأنظمة الإلكترونية في مختلف مجالات الحياة، أصبحت حماية المعلومات الرقمية أمراً جوهرياً لضمان استمرارية وأمان المؤسسات والأفراد.
يتطلب تأمين البيانات الرقمية مستوى عالٍ من الكفاءة الفنية والمعرفة المتخصصة، لمواجهة التحديات المستجدة والتهديدات السيبرانية المتطورة التي تستهدف سرية البيانات وسلامتها وتوافرها.

**الفئات المستهدفة**

يُوجه هذا البرنامج المتقدم إلى الفئات التالية:
- مدراء تكنولوجيا المعلومات والمسؤولين عن أمن الشبكات في الشركات والمؤسسات
- محللو أمن المعلومات والمتخصصون في الأمن السيبراني
- مهندسو البرمجيات ومطورو الأنظمة الراغبون في تعزيز معارفهم في أمن المعلومات
- محترفو تكنولوجيا المعلومات الساعون إلى ترقية مهاراتهم ضمن مجال أمن البيانات الرقمية

**الكفاءات المستهدفة**

- الإلمام بمفاهيم ومبادئ أمن المعلومات الأساسية
- القدرة على تحليل وتقدير المخاطر الأمنية وتطبيق التدابير الوقائية المناسبة
- تصميم وتنفيذ سياسات واستراتيجيات الأمان الرقمي ضمن البنى التحتية لتقنية المعلومات
- فهم آليات الكشف عن التسلل والاستجابة الفورية للحوادث
- إدارة التهديدات الإلكترونية وسبل الوقاية منها
- إعداد وتنفيذ سياسات الحماية والتوعية للمستخدمين
- تحليل الهجمات الرقمية وتوثيق نتائجها عبر تقارير احترافية وتوصيات عملية

**محتوى الدورة**

**الوحدة الأولى: المفاهيم الأساسية في أمن المعلومات**

- تعريف أمن المعلومات وأهميته في البيئة الرقمية
- تصنيفات التهديدات الإلكترونية وأنماط الهجمات السيبرانية
- المبادئ الأساسية في تصميم أنظمة الأمان واستخدام تقنيات التشفير
- أنواع الهجمات السيبرانية الشائعة
- آليات وتقنيات الحماية من التسللات الأمنية

**الوحدة الثانية: تحليل وتقييم التهديدات**

- تقنيات تحليل المخاطر وتقييم الأصول وتحديد نقاط الضعف
- أساليب التصدي للثغرات ونقاط الانكشاف الأمني
- استراتيجيات الاستجابة للحوادث وخطط التعافي
- مراجعة أمان البرمجيات وتقييم الثغرات التقنية

**الوحدة الثالثة: حماية الشبكات وأنظمة الاتصال**

- تصميم الشبكات الآمنة ومعايير حمايتها
- أنظمة كشف التسلل وأدوات الحماية الاستباقية
- حماية قنوات الاتصال وتشفير البيانات المنقولة
- إدارة الهويات الرقمية وأدوات المصادقة والتحكم في الوصول

**الوحدة الرابعة: أمن المعلومات في بيئة الحوسبة السحابية**

- حماية البيانات الشخصية والمؤسسية في خدمات السحابة
- أدوات وتقنيات الأمن السحابي وضمان استمرارية الخدمة
- مراقبة أنشطة المستخدمين وإدارة الأذونات في البيئة السحابية

**الوحدة الخامسة: إدارة منظومة أمن المعلومات**

- تطبيق استراتيجيات تخطيط وإدارة المخاطر المعلوماتية
- تطوير وتطبيق سياسات الأمان الرقمي والإجراءات التشغيلية
- تدقيق الضوابط الأمنية ومتابعة الامتثال
- التعامل مع حوادث أمن المعلومات وإجراء التحقيقات الرقمية

**الوحدة السادسة: اختبارات الأمان والتقييم الفني**

- تنفيذ اختبارات الاختراق وتحليل الثغرات
- تقييم شدة التهديدات ونقاط الضعف الفنية
- التصدي للهجمات السيبرانية المتقدمة والناشئة باستخدام أدوات متطورة

**الوحدة السابعة: الاعتبارات القانونية والأخلاقية**

- الإطار التشريعي والتنظيمي المرتبط بأمن المعلومات
- المبادئ الأخلاقية والمهنية في ممارسات الأمن السيبراني
- كيفية التعامل مع حالات التزوير والجرائم الإلكترونية والانتهاكات القانونية