الشرح التفصيلي لكل برنامج:

اسم البرنامج	مدته	مستوى الدخول للتدرب على البرنامج
9 دورة الأمن السبراني والحماية من الجرائم المعلوماتية	18 يوم 30 ساعة تدريبية	شهادة المرحلة الابتدائية على الأقل

وصف البرنامج

تركّز دورة "الأمن السيبراني" على تأهيل المشاركين بالمعارف والمهارات اللازمة لفهم التهديدات الرقمية، وتأمين البيانات والأنظمة من الهجمات الإلكترونية المتزايدة. تُعد هذه الدورة مدخلًا أساسيًا لفهم مبادئ أمن المعلومات، حماية الشبكات، التشفير، الكشف عن التهديدات، وأساليب الدفاع الرقمي، مع التركيز على الممارسات العالمية والمعايير الأمنية المتبعة.
تُناسب الدورة الراغبين في دخول مجال أمن المعلومات أو تطوير مسيرتهم المهنية في هذا المجال المتنامي

الهدف العام للبرنامج:

- فهم مفهوم الأمن السيبراني وأهميته في العصر الرقمي ..
- . التعرف على أنواع الهجمات السيبرانية وطرق الحماية منها.
- تعلم المبادئ الأساسية لتأمين الشبكات والأنظمة..
- اكتساب مهارات التشفير وحماية البيانات الحساسة..
- التعرف على أدوات ومنصات الأمن السيبراني..
- في العصر الرقمي . الإلمام بالسياسات الأمنية.

الأهداف التفصيلية للبرنامج:

بنهاية الدورة تكون الخريجة قادرة وبكفاءة على معرفة:

- - -مقدمة في الأمن السيبراني:
- -المفاهيم الأساسية.
- -الفرق بين أمن المعلومات والأمن السيبراني.
- -أهمية الأمن السيبراني على مستوى الأفراد والمؤسسات والدول.
- -أنواع التهديدات السيبرانية:
- -الفيروسات، البرمجيات الخبيثة، التصيد، هجمات حجب الخدمة الهندسة الاجتماعية.
- -أمن الشبكات والبنية التحتية:
- الجدران النارية (Firewalls).
- -التشفير وإدارة المفاتيح:
- -التشفير المتماثل وغير المتماثل.
- -التوقيعات الرقمية وشهادات الأمان (SSL).
- -أدوات الأمن السيبراني:
- -مقدمة عن أدوات مثل Wireshark، Kali Linux، Nessus وغيرها.
- -الامتثال والسياسات:
- -إعداد سياسات أمنية داخل المؤسسات.
- -الاستجابة للحوادث وتحليل الاختراقات:
- -خطوات التصرف عند وقوع اختراق.
- -توثيق الحوادث والتعلم منها.

يحصل المتدرب بنهاية الدورة على :

- شهادة حضور معتمدة من المعهد التدريبي.
- معرفة شاملة بأساسيات حماية الأنظمة والمعلومات.
- القدرة على تحليل التهديدات السيبرانية والتعامل معها.