€TRAINING

الأمن السيبراني

1 - 5 يونيو 2025
Online

الأمن السيبراني

رمز الدورة: Q782 تاريخ الإنعقاد: 1 - 5 يونيو 2025 دولة الإنعقاد: Online - التكلفة: 2200 يورو

مقدمة عن البرنامج التدريبي:

يشير الأمن السيبراني إلى الإطار المؤسسي الذي يُعنى بتنظيم حماية الأنظمة الرقمية والبنى التحتية المعلوماتية من التهديدات الإلكترونية التي قد تؤثر على استقرار العمليات المؤسسية وسلامة البيانات. يعتمد هذا المجال على منظومات فنية وهيكلية تضمن السيطرة على الوصول ورصد الأنشطة وضبط المعايير التقنية والتنظيمية وفق سياسات وطنية ودولية. يركّز هذا البرنامج على عرض البنى التنظيمية للأمن السيبراني والعناصر التقنية المصاحبة لها والضوابط المؤسسية المرتبطة بالامتثال والجاهزية التشغيلية.

أهداف البرنامج التدريبي:

في نهاية هذا البرنامج، سيكون المشاركون قادرين على:

- التعرف على المفاهيم المؤسسية المرتبطة بالأمن السيبراني وأنظمته التنظيمية.
- تصنيف عناصر البنية التقنية المعتمدة في حماية البيئة الرقمية.
- تحليل مصادر التهديد الإلكتروني وآليات تنظيم الاستجابة المؤسسية.
- تحديد الهياكل التنظيمية المرتبطة بالامتثال السيبراني.
- تعزيز مهارات صياغة التوجهات المؤسسية لدعم استمرارية أمن المعلومات.

الفئات المستهدفة:

- المسؤولون عن إدارة نظم المعلومات والبنية التحتية الرقمية.
- الكوادر التقنية العاملة في أقسام أمن المعلومات.
- الموظفون المختصون في حوكمة الأمن السيبراني والامتثال.
- الجهات الرقابية المعنية بتنظيم الأمن الرقمي.
- مديرو الإدارات التقنية في المؤسسات العامة والخاصة.

محاور البرنامج التدريبي:

الوحدة الأولى:

الإطار العام للأمن السيبراني:

- مفاهيم الأمن السيبراني في السياق المؤسسي.
- التمييز بين أمن المعلومات والأمن السيبراني.
- أنواع التهديدات الرقمية وخصائصها التنظيمية.
- العلاقة بين البنية المؤسسية ومستوى الجاهزية السيبرانية.
- المرجعيات الوطنية والدولية في الأمن السيبراني.

الوحدة الثانية:

البنية التقنية في بيئات الحماية الرقمية:

- عناصر نظم الحماية التقنية في المؤسسات.
- طرق هيكلة أنظمة الشبكات وضوابط التحكم بالوصول.
- أساليب ضبط إعدادات الأجهزة ونقاط النهاية ضمن البيئة المؤسسية.

- كيفية ترتيب البيانات وفق أولويات الحماية.
- الأدوات التقنية المستخدمة في الرصد والتأمين.

الوحدة الثالثة:

عملية تنظيم الاستجابة للتهديدات السيبرانية:

- آليات تصنيف الحوادث الرقمية في البيئات التشغيلية.
- الهياكل الإدارية المسؤولة عن تنسيق الاستجابة.
- إجراءات ضبط الحدث من لحظة الاكتشاف إلى المعالجة المؤسسية.
- أدوار الفرق الفنية والتنظيمية في التعامل مع الحوادث.
- أنظمة التحليل المؤسسي للثغرات وأسبابها.

الوحدة الرابعة:

الامتثال والمعايير في الأمن السيبراني:

- الضوابط المؤسسية المرتبطة بالتشريعات الوطنية.
- الأطر المعيارية ISO 27001 وNIST.
- نظام التوثيق الداخلي في بيئات الامتثال.
- متطلبات التدقيق الفني والتنظيمي في الأمن السيبراني.
- العلاقة بين الامتثال وكفاءة العمليات الرقمية.

الوحدة الخامسة:

استمرارية الأمن السيبراني وتطوير الجاهزية:

- العوامل المؤسسية المؤثرة في استمرارية الحماية.
- نظم التخطيط التشغيلي في مواجهة المخاطر السيبرانية.
- أدوات قياس الجاهزية الرقمية على المستوى المؤسسي.
- الهياكل الداعمة للتطوير المستمر في الأمن السيبراني.
- توجهات دعم ثقافة الأمن الرقمي داخل المؤسسة.