

€ TRAINING

الأمن السيبراني



4 - 8 أغسطس 2024
اسطنبول (تركيا)
Sheraton Istanbul Levent

الأمن السيبراني

رمز الدورة: Q782 تاريخ الإنعقاد: 4 - 8 أغسطس 2024 دولة الإنعقاد: اسطنبول (تركيا) - Levent Istanbul Sheraton التكلفة: 5850 يورو

مقدمة عن البرنامج التدريبي:

يعد الأمن السيبراني جزءًا مهمًا من الأمن في البلدان اليوم، وهو يقوم على حماية البنية التحتية المعلوماتية لدولة ما، والتي تشمل مرافق مهمة وأنظمة مهمة تدير مؤسسات الدولة المهمة، مثل الحكومة. يمكن أن تشكل تهديدات الأمن السيبراني تهديدًا للأمن القومي لأي بلد، لذلك أعدت العديد من الدول هيئات للتخصص في الأمن السيبراني. تم تسخير جميع القدرات للأمن السيبراني، وهو أحد المعايير المستخدمة لقياس مستوى الجاهزية السيبرانية لدولة ما. الاتحاد الدولي للاتصالات ITU لديها مؤشر يقيس مدى استعداد الدولة للتعامل مع التهديدات السيبرانية.

أهداف البرنامج التدريبي:

في نهاية البرنامج سيكون المشاركون قادرين على:

- فهم هجمات فيروسات الفدية وكيفية التعامل معها
- فهم الآليات الدولية والوطنية لحماية الأمن السيبراني
- فهم محاور الأمن السيبراني والتهديدات التي تكتنفه وكيفية التعامل معها
- فهم الهجمات السيبرانية وكيفية القيام بها ونقاط الضعف والقوة في نظم المعلومات

الفئات المستهدفة:

- ضباط الشرطة العاملين في مجال البحث الجنائي وتحليل المعلومات
- أعضاء النيابة العامة والقضاة
- موظفي القطاع الحكومي والخاص
- ضباط أمن المعلومات في القطاع الشرطي والعسكري
- المحامين
- مسؤولي الأمن في المؤسسات والشركات

محاور البرنامج التدريبي:

الوحدة الاولى:

التعريف بالأمن السيبراني ومحاوره والحماية القانونية له

- مفهوم الأمن السيبراني
- العناصر الأساسية للأمن السيبراني
- الجوانب القانونية لحماية الأمن السيبراني

الوحدة الثانية:

دراسة تحليلية لأشهر الهجمات السيبرانية

- دراسة تحليلية لهجمات مختلفة في مختلف أنحاء العالم
- تحليل لأهم المواقع الإحصائية للهجمات السيبرانية
- دراسة تحليلية لهجمات أرامكو السيبرانية
- دراسة تحليلية لهجمات أستونيا السيبرانية والآثار المترتبة عليها

الوحدة الثالثة:

الجهود الدولية و الوطنية لحماية الأمن السيبراني

- الحماية الدولية للأمن السيبراني و تنظيم قواعد الحروب السيبرانية لجنة تالين للأمن السيبراني
- دور الاتحاد الدولي للاتصالات في تقييم الجاهزية السيبرانية للتعامل مع الهجمات السيبرانية
- جهود الإنتربول في حماية الأمن السيبراني
- الأمن السيبراني في دولة الإمارات العربية المتحدة

الوحدة الرابعة:

هجمات فيروسات الفدية و كيفية عملها و إستراتيجية التعامل معها

- التعرف بفيروسات الفدية
- آلية عمل فيروسات الفدية و الهدف من الهجمات المرتكبة بها
- أشهر هجمات فيروسات الفدية و الآثار المترتبة عليها
- كيفية التعامل مع الهجمات و الوقاية منها

الوحدة الخامسة:

قواعد الأمن السيبراني في المؤسسات

- الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات
- مهددات الأمن السيبراني في المؤسسات الصناعية و الحيوية
- الحروب السيبرانية و الهجمات الموجهة لنظم المعلومات
- قواعد الاستخدام الآمن لنظم المعلومات في المؤسسات