

# € TRAINING

الذهن السبيراني



4 - 8 أغسطس 2024  
اسطنبول (تركيا)

## الأمن السيبراني

رمز الدورة: 11146 تاريخ الإنعقاد: 4 - 8 أغسطس 2024 دولة الإنعقاد: اسطنبول (تركيا) - التكلفة: 5850 يورو

### مقدمة عن البرنامج التدريبي:

يسعى هذا البرنامج التدريبي لتقديم فهم شامل لمبادئ الأمن السيبراني وأفضل الممارسات المتبعة لمواجهته. حيث أن للأمن السيبراني دورًا حيويًا في حماية البيانات والمعلومات الحيوية في العصر الرقمي.

### أهداف البرنامج التدريبي:

#### في نهاية البرنامج سيكون المشاركون قادرين على:

- فهم هجمات فيروسات الفدية و كيفية التعامل معها
- فهم الآليات الدولية و الوطنية لحماية الأمن السيبراني
- فهم محاور الأمن السيبراني و التهديدات التي تكتنفه و كيفية التعامل معها
- فهم الهجمات السيبرانية و كيفية القيام بها و نقاط الضعف و القوة في نظم المعلومات

### الفئات المستهدفة:

- ضباط الشرطة العاملين في مجال البحث الجنائي و تحليل المعلومات
- أعضاء النيابة العامة و القضاة.
- موظفو القطاع الحكومي و الخاص.
- ضباط أمن المعلومات في القطاع الشرطي و العسكري.
- المحامون.
- مسؤولو الأمن في المؤسسات و الشركات.

### محاور البرنامج التدريبي:

#### الوحدة الأولى:

#### التعريف بالأمن السيبراني ومحاوره والحماية القانونية له:

- مفهوم الأمن السيبراني.
- العناصر الأساسية للأمن السيبراني.
- الجوانب القانونية لحماية الأمن السيبراني.
- أهمية الأمن السيبراني في العصر الحديث.
- التهديدات والتحديات التي تواجه الأمن السيبراني.
- الاستراتيجيات المتبعة لتعزيز 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.
- أسباب وتداعيات الهجمات السيبرانية.

- الدروس المستفادة من الهجمات السيبرانية.

### الوحدة الثالثة:

#### الجهود الدولية والوطنية لحماية الأمن السيبراني:

- الحماية الدولية للأمن السيبراني وتنظيم قواعد الحروب السيبرانية لجنة تالين للأمن السيبراني.
- دور الاتحاد الدولي للاتصالات في تقييم الجاهزية السيبرانية للتعامل مع الهجمات السيبرانية.
- جهود الإنترنت في حماية الأمن السيبراني.
- الأمن السيبراني في دولة الإمارات العربية المتحدة.
- السياسات الوطنية لحماية الأمن السيبراني.
- التعاون الدولي في مجال الأمن السيبراني.

### الوحدة الرابعة:

#### هجمات فيروسات الفدية وكيفية عملها واستراتيجية التعامل معها:

- التعريف بفيروسات الفدية.
- آلية عمل فيروسات الفدية والهدف من الهجمات المرتكبة بها.
- أشهر هجمات فيروسات الفدية والآثار المترتبة عليها.
- كيفية التعامل مع الهجمات والوقاية منها.
- استراتيجيات استجابة المؤسسات لهجمات فيروسات الفدية.
- التدابير الوقائية ضد فيروسات الفدية.

### الوحدة الخامسة:

#### قواعد الأمن السيبراني في المؤسسات:

- الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات.
- مهددات الأمن السيبراني في المؤسسات الصناعية والحيوية.
- الحروب السيبرانية والهجمات الموجهة لنظم المعلومات.
- قواعد الاستخدام الآمن لنظم المعلومات في المؤسسات.
- تطوير سياسات وإجراءات الأمن السيبراني في المؤسسات.
- تدريب الموظفين على الأمن السيبراني والتوعية بالمخاطر.