

# € TRAINING

الاهن السببرانى

8 - 19 ديسمبر 2024  
القاهرة (مصر)



## الامن السيبراني

رمز الدورة: 1132 | تاريخ الإنعقاد: 8 - 19 ديسمبر 2024 | دولة الإنعقاد: القاهرة (هـصـر) - التكلفة: 6965 يورو

### مقدمة عن البرنامج التدريبي:

هذا البرنامج التدريبي يتناول أهمية الامن السيبراني حيث سيتم فيه تسليط الضوء على اهم المحاور للامن السيبراني و الاليات الدولية المستخدمة في حماية الامن السيبراني و تحليل الهجمات السيبرانية والتعامل معها.

### أهداف البرنامج التدريبي:

في نهاية البرنامج سيكون المشاركون قادرين على:

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

### 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 حماية المؤسسات.
- التهديدات السيبرانية وتأثيرها على الأمن القومي.

#### الوحدة الثانية:

#### قواعد الأمن السيبراني في المؤسسات:

- الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات.
- مهندات الأمن السيبراني في المؤسسات الصناعية والحيوية.
- الحروب السيبرانية والهجمات الموجهة لنظم المعلومات.
- قواعد الاستخدام الأمن لنظم المعلومات في المؤسسات.
- أهمية التوعية والتدريب في تعزيز الأمن السيبراني.

## الوحدة الثالثة:

### دراسة تحليلية لأشهر الهجمات السيبرانية:

- دراسة تحليلية لهجمات أرامكو السيبرانية.
- دراسة تحليلية لهجمات أستونيا السيبرانية والآثار المترتبة عليها.
- دراسة تحليلية لهجمات مختلفة في مختلف أنحاء العالم.
- تحليل لأهم المواقع الإحصائية للهجمات السيبرانية.
- الدروس المستفادة من الهجمات السيبرانية الكبرى.

## 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 الفدية.

## الوحدة الخامسة:

### 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 الإنتربول في حماية الأمن السيبراني.
- التعاون الدولي في مواجهة التهديدات السيبرانية.

## الوحدة السادسة:

### تقييم الجاهزية السيبرانية:

- أدوات تقييم الجاهزية السيبرانية.
- تحليل نتائج تقييم الجاهزية السيبرانية.
- دور التقييم الدوري في تعزيز الأمن السيبراني.
- كيفية تحسين جاهزية المؤسسات لمواجهة التهديدات السيبرانية.
- أهمية الاستجابة السريعة للحوادث السيبرانية.

## الوحدة السابعة:

### الحماية المتقدمة للشبكات:

- تقنيات الحماية المتقدمة للشبكات.
- إدارة الوصول والسيطرة على المعلومات.
- حماية البيانات أثناء النقل.
- أهمية التشفير في حماية المعلومات.
- تطوير استراتيجيات الحماية للشبكات الداخلية.

## الوحدة الثامنة:

### تطوير سياسات وإجراءات الأمن السيبراني:

- كيفية تطوير سياسات الأمن السيبراني.
- إجراءات التعامل مع الحوادث السيبرانية.
- آليات المراجعة والتحديث المستمر للسياسات.
- دور السياسات والإجراءات في تعزيز ثقافة الأمن السيبراني.
- تحديات تنفيذ سياسات الأمن السيبراني في المؤسسات.

## الوحدة التاسعة:

### التعامل مع الحوادث السيبرانية:

- أنواع الحوادث السيبرانية.
- الخطوات المتبعة في التحقيق في الحوادث.
- استعادة النظام بعد الحوادث.
- توثيق الحوادث والإبلاغ عنها.
- تطوير خطط الطوارئ والاستجابة للحوادث السيبرانية.

## الوحدة العاشرة:

### إدارة المخاطر السيبرانية:

- مفهوم إدارة المخاطر السيبرانية.
- تحليل وتقييم المخاطر السيبرانية.
- استراتيجيات التخفيف من المخاطر.
- دور إدارة المخاطر في تحسين الأمن السيبراني.
- أمثلة على إدارة المخاطر السيبرانية في المؤسسات.