

## ورشة عمل أمن المعلومات والأمن السيبراني

UK Traininig

# PARTNER



## ورشة عمل أمن المعلومات والأمن السيبراني

### مقدمة

في عصرنا الرقمي الحالي، حيث تتزايد تهديدات الأمن السيبراني تعقيدًا وتواترًا، أصبح إدارة أمن المعلومات جزءًا أساسيًا من نجاح المؤسسات وحمايتها. تم تصميم هذه الورشة لتزويد المشاركين بالأدوات والمعرفة اللازمة لحماية الأصول، البيانات، والأنظمة التنظيمية من المخاطر الإلكترونية.

من خلال تطبيقات عملية ورؤى نظرية، سيتعرف المشاركون على ما هو أمن المعلومات، فهم تعريف أمن المعلومات وأهميته، واكتساب أساسيات الأمن السيبراني. تغطي هذه الورشة مفاهيم مثل سياسات أمن المعلومات، تقنيات الحد من المخاطر، الاستجابة للحوادث، وتنفيذ برامج فعالة لإدارة أمن المعلومات بما يتماشى مع معايير الصناعة.

### أهداف الورشة

بنهاية هذه الورشة، سيكون المشاركون قادرين على:

- فهم لماذا يعتبر أمن المعلومات مهمًا ودوره في حماية بيانات المؤسسات.
- تعلم أساسيات إدارة أمن المعلومات وكيفية تنفيذها بشكل فعال.
- اكتساب فهم واضح لمسؤوليات محل أمن المعلومات واستراتيجيات تحديد الثغرات.
- تطوير خطة عملية لـ أمن المعلومات للتعامل مع التهديدات والثغرات الأمنية.
- استكشاف الأدوات والأطر لإجراء تدقيق أمن المعلومات وضمان الامتثال.
- التعرف على سياسات أمن المعلومات التي تحمي المؤسسات من التهديدات الداخلية والخارجية.
- دمج الضوابط الأمنية المادية والرقمية لتحقيق برنامج شامل لـ أمن المعلومات.
- البقاء على اطلاع على اتجاهات الأمن السيبراني، التهديدات الناشئة، وخدمات أمن المعلومات الحديثة.

UK Training

**PARTNER**



## محاور الورشة

### اليوم الأول: الوعي بالأمن السيبراني

- ما هو أمن المعلومات؟ تعريفه ومبادئه وأهميته في المؤسسات الحديثة.
- المبادئ الأساسية: السرية، التكامل، والتوافر.
- لمحة عامة عن تهديدات الأمن السيبراني وتأثيراتها على المؤسسات.
- أساسيات الخطوة في البيانات المتحركة مقابل البيانات الثابتة.
- جلسة عملية: اكتشاف الشبكات وتحديد الثغرات من خلال الفحص والتخطيط.

### اليوم الثاني: هندسة الأمن

- مقدمة عن هندسة أمن تكنولوجيا المعلومات وأهميتها في الحماية التنظيمية.
- استكشاف تقنيات تقسيم الشبكات، ترجمة العناوين، والتحكم في الوصول.
- دور التشفير والصلاحيات في تأمين البيانات.
- تدريب عملي: بناء هيكل أمني قوي للشبكات لتعزيز الحماية.

### اليوم الثالث: إدارة الهوية وتعزيز أمان الشبكات

- أساسيات إدارة الهوية ودورها في برامج أمن المعلومات.
- استكشاف آليات المصادقة، سياسات كلمات المرور، والأنظمة الموحدة للهوية.
- تقنيات تعزيز أمان الشبكات، بما في ذلك حماية الوصول الإداري وتأمين الأجهزة.
- أفضل الممارسات لتصفية حركة المرور وتأمين أجهزة الشبكات.

### اليوم الرابع: أمان البرمجيات والأمان المادي

- تحديد ومعالجة ثغرات البرمجيات من خلال ممارسات البرمجة الآمنة.
- أهمية المراقبة البيئية وتسجيل الدخول في اكتشاف الثغرات.
- مراجعة شاملة للضوابط الأمنية المادية ودمجها مع الأنظمة الرقمية.
- دراسة سياسات أمن المعلومات لضمان حماية الموارد البشرية والأجهزة.

UK Training

**PARTNER**



## اليوم الخامس: الاستجابة للحوادث واتجاهات الأمن السيبراني

- تطوير خطة فعالة للاستجابة للحوادث الأمنية.
- فهم استمرارية الأعمال وخطط التعافي من الكوارث.
- الاطلاع على اتجاهات الأمن السيبراني الناشئة، معايير شهادة أمن المعلومات، والتهديدات المستقبلية.
- أهمية تدريب أمن المعلومات لمواكبة التهديدات والثغرات المحتملة.

## لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- فهم شامل للأمن السيبراني: اكتساب معرفة متعمقة بـ ما هو أمن المعلومات وكيفية تنفيذه بشكل فعال.
- تطبيق عملي: تعلم كيفية تطوير خطة أمنية عملية وإجراء تدقيق أمن المعلومات.
- مواكبة التطورات: البقاء على اطلاع بأحدث التهديدات واتجاهات إدارة أمن المعلومات.
- الحصول على شهادة مهنية: التحضير للحصول على شهادة أمن المعلومات لتعزيز مستقبلك المهني.
- قيادة الأمان التنظيمي: تطوير المهارات اللازمة لقيادة برامج أمن المعلومات التي تتماشى مع أفضل الممارسات الصناعية

## الخاتمة

تقدم ورشة الأمن السيبراني وإدارة أمن المعلومات منهجًا شاملًا لتطوير مهارات المشاركين في إدارة أمن المعلومات وحماية أنظمة المؤسسات من التهديدات الإلكترونية. من خلال تعلم كيفية إجراء تدقيق أمن المعلومات، تطوير سياسات أمن المعلومات، والاستجابة للحوادث، سيكون المشاركون مستعدين للتعامل مع تحديات الأمن السيبراني بفعالية.

سواء كنت محلل أمن معلومات، محترفًا يسعى للحصول على شهادة أمن المعلومات، أو قائدًا يهدف إلى تنفيذ برامج أمان قوية، ستوفر لك هذه الورشة الأدوات والإطار اللازمين لضمان نجاحك ونجاح مؤسستك في هذا المجال الحاسم.

## الأسئلة الشائعة

### ما هو أمن المعلومات، ولماذا يُعد مهمًا للمؤسسات؟

يوضح البرنامج مفهوم أمن المعلومات ويجب عن سؤال ما هو أمن المعلومات؟، مع شرح تعريف أمن المعلومات وأهميته طبيقه في حماية البيانات والأنظمة والأصول الرقمية. كما يتناول إدارة أمن المعلومات ودورها في الحفاظ على سرية المعلومات وسلامتها وتوافرها، والحد من المخاطر والتهديدات السيبرانية.

UK Training

**PARTNER**



## كيف يساعد البرنامج في تطوير نظام متكامل لإدارة أمن المعلومات؟

يركز البرنامج على إدارة أمن المعلومات من خلال إعداد برنامج أمن المعلومات، ووضع سياسات أمن المعلومات، وإعداد خطة أمن المعلومات، وتطبيق أفضل الممارسات في أمن تقنية المعلومات. كما يتعلم المشاركون كيفية بناء بيئة أمنية متكاملة تتوافق مع المعايير الدولية ومتطلبات الامتثال.

## هل يغطي البرنامج تقييم المخاطر والتدقيق والخدمات الأمنية؟

نعم، يتناول البرنامج تدقيق أمن المعلومات، وإجراء تقييم مخاطر الأمن السيبراني، وتحليل الثغرات الأمنية، والاستجابة للحوادث، بالإضافة إلى استعراض أحدث خدمات أمن المعلومات، وطول الأمن السيبراني، وخدمات الأمن السيبراني التي تساعد المؤسسات على تعزيز مستوى الحماية وتقليل المخاطر.

## لمن يناسب هذا البرنامج، وما المهارات التي يكتسبها المشاركون؟

طعم البرنامج لمحلي أمن المعلومات، ومتخصصي الأمن السيبراني، ومديري أمن المعلومات، ومدققي الأنظمة، ومسؤولي الامتثال، والعاملين في تقنية المعلومات، وجميع المهنيين الراغبين في تطوير خبراتهم في هذا المجال. كما يكتسب المشاركون مهارات إعداد السياسات الأمنية، وإدارة المخاطر، وتطبيق الضوابط الأمنية، والاستجابة للحوادث، وإدارة برامج أمن المعلومات بكفاءة.

## هل يساعد البرنامج في الحصول على شهادات مهنية والتقدم الوظيفي؟

بالتأكيد، يعد البرنامج خيارًا مناسبًا للراغبين في الحصول على شهادة في أمن المعلومات أو شهادة في الأمن السيبراني، كما يدعم الاستعداد للالتحاق ببرامج ودورات الأمن السيبراني المتقدمة. ويساعد المشاركين على تطوير مهاراتهم المهنية، وتعزيز فرصهم في العمل كمحلي أمن معلومات، أو متخصصي أمن سيبراني، أو شغل المناصب المتقدمة في مجال أمن المعلومات وإدارة الأمن السيبراني.

UK Training

**PARTNER**

