BLACKBIRD FOR TRAINING

إدارة مخاطر الأمن السيبراني والاستجابة للحوادث

17 – 21 يناير 2027

أون لاين

UK Traininig

PARTNER



www.blackbird-training.com

إدارة مخاطر الأمن السيبراني والاستجابة للحوادث

المرجع: 350093_3255743 **التاريخ:** 17 – 21 يناير 2027 **المكان:** أون لاين **الرسوم:** GBP 2700

مقدمة

تركز دورة إدارة مخاطر الأمن السيبراني والاستجابة للحوادث على إدارة المخاطر الرقمية والتعامل مع الحوادث الأمنية بطريقة منظمة وعملية. تواجه المؤسسات تهديدات متزايدة قد تؤثر على البيانات والأنظمة والعمليات والسمعة واستمرارية الخدمات، لذلك تحتاج إلى منهجية واضحة لتحديد المخاطر، وتقييم الضوابط، والاستعداد للحوادث، وتنسيق الاستجابة، والتحسين المستمر.

توضح الدورة كيفية تحديد مخاطر الأمن السيبراني، وتقييم أثرها، وترتيب أولويات الضوابط، وإعداد خطط الاستجابة للحوادث، وإدارة الحادث من مرحلة الاكتشاف حتى التعافي. كما تتناول التواصل أثناء الحوادث، وتوثيق الأدلة، واستخلاص الدروس المستفادة، وربط إدارة المخاطر بالامتثال والمرونة التشغيلية.

تمتد الدورة على أسبوع بتسلسل مترابط. تبدأ بأساسيات إدارة مخاطر الأمن السيبراني، ثم تنتقل إلى تقييم المخاطر وتخطيط الضوابط، ثم الاستعداد للاستجابة للحوادث، يلي ذلك التعامل مع الحوادث والتعافي، وتنتهي بمراجعة الأداء والتحسين المستمر.

أهداف الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- فهم مبادئ إدارة مخاطر الأمن السيبراني.
- تحديد التهديدات والثغرات والآثار المحتملة على الأعمال.
- تقييم مخاطر الأمن السيبراني وترتيب أولوياتها.
- ربط المخاطر السيبرانية بالتشغيل والامتثال والسمعة.
- تقييم الضوابط الحالية وتحديد الفجوات.
- إعداد إجراءات عملية لمعالجة مخاطر الأمن السيبراني.
- إعداد خطط منظمة للاستجابة للحوادث الأمنية.
- تحديد الأدوار والمسؤوليات ومسارات التصعيد أثناء الحوادث.
- إدارة مراحل الاكتشاف والاحتواء والمعالجة والتعافي.
- توثيق الحوادث وجمع الأدلة المطلوبة.
- التواصل بفعالية مع الأطراف المعنية أثناء الحوادث.
- مراجعة نتائج الحوادث وتحسين الجاهزية السيبرانية.



محاور الدورة

اليوم الأول: أساسيات إدارة مخاطر الأمن السيبراني.

- مفهوم مخاطر الأمن السيبراني وتأثيرها على الأعمال.
- التهديدات السيبرانية الشائعة التي تواجه المؤسسات.
- العلاقة بين الأصول والتهديدات والثغرات والضوابط.
- الفرق بين الوقاية والكشف والاستجابة والتعافي.
- أدوار ومسؤوليات الأمن السيبراني داخل الإدارات.
- التحديات الرئيسية في إدارة مخاطر الأمن السيبراني.

اليوم الثاني: تقييم المخاطر السيبرانية وتخطيط الضوابط.

- تحديد الأصول والأنظمة والمعلومات الحرجة.
- تقييم التهديدات والثغرات واحتمالية الحدوث والأثر.
- ترتيب المخاطر وفقًا لتأثيرها على الأعمال.
- مراجعة الضوابط الأمنية الحالية.
- تحديد الفجوات في الحماية والمراقبة وجاهزية الاستجابة.
- تطبيق عملي على إعداد سجل مخاطر سيبرانية.

اليوم الثالث: تخطيط الاستجابة للحوادث والاستعداد لها.

- هدف خطة الاستجابة للحوادث الأمنية.
- تحديد أنواع الحوادث ومستويات الخطورة وقواعد التصعيد.
- بناء هيكل فريق الاستجابة للحوادث.
- إعداد إجراءات التواصل والإبلاغ.
- التنسيق بين فرق تقنية المعلومات والشؤون القانونية والامتثال والإدارة.
- تطبيق عملي على إعداد مخطط أولي لخطة استجابة لحادث أمني.



اليوم الرابع: التعامل مع الحوادث والاحتواء والتعافي.

- اكتشاف الحوادث الأمنية والتحقق منها.
- احتواء الحوادث لتقليل أثرها التشغيلي.
- التحقيق في الأسباب الجذرية والأنظمة المتأثرة.
- إزالة التهديدات واستعادة الخدمات.
- توثيق الإجراءات والجداول الزمنية والقرارات والأدلة.
- تطبيق عملي على إدارة سيناريو حادث أمني سيبراني.

اليوم الخامس: الدروس المستفادة والتحسين المستمر.

- مراجعة أداء الاستجابة للحوادث.
- تحديد نقاط ضعف الضوابط وفجوات الاستجابة.
- إعداد تقارير الدروس المستفادة.
- تحديث سجلات المخاطر وخطط الاستجابة.
- قياس جاهزية الأمن السيبراني والمرونة التشغيلية.
- تطبيق متكامل يربط بين تقييم المخاطر والضوابط والاستجابة والتعافي والتحسين.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- تحسين القدرة على تحديد وإدارة مخاطر الأمن السيبراني.
- تعزيز الجاهزية للتعامل مع الحوادث الأمنية.
- بناء خطط استجابة منظمة للحوادث.
- تقليل الاضطراب التشغيلي أثناء الحوادث السيبرانية.
- تحسين التنسيق بين الفرق التقنية والإدارية.
- دعم سرعة الاحتواء والتعافي.
- تحسين توثيق الحوادث وجمع الأدلة.
- تعزيز الالتزام ومتطلبات التدقيق.
- تحديد فجوات الضوابط الأمنية.
- تحسين التواصل أثناء الحوادث.
- تعزيز المرونة السيبرانية من خلال الدروس المستفادة.
- بناء منهجية عملية للتحسين المستمر في إدارة المخاطر.



الخاتمة

تقدم دورة إدارة مخاطر الأمن السيبراني والاستجابة للحوادث إطارًا عمليًا لتحديد مخاطر الأمن السيبراني وتقييمها وإدارتها، مع تجهيز المؤسسة للتعامل الفعال مع الحوادث الأمنية. تغطي الدورة المراحل الرئيسية لإدارة المخاطر والحوادث، بدءًا من فهم التهديدات وآثارها على الأعمال، ثم تقييم المخاطر، وتخطيط الضوابط، وإعداد خطط الاستجابة، والتعامل مع الحوادث، وتحسين الجاهزية.

يتبع البرنامج تسلسلاً مترابطًا يساعد المشاركين على فهم العلاقة بين إدارة المخاطر والاستجابة للحوادث. فتقييم المخاطر يدعم اختيار الضوابط المناسبة، بينما تضمن خطط الاستجابة قدرة المؤسسة على التحرك بسرعة عندما تتحول التهديدات إلى أحداث فعلية.

بنهاية الدورة، سيكون لدى المشاركين فهم عملي لكيفية إدارة مخاطر الأمن السيبراني، وإعداد خطط الاستجابة، وتنسيق الإجراءات أثناء الحوادث، وتوثيق الأدلة، واستعادة الخدمات، وتحسين الجاهزية المستقبلية. وتساعد الدورة على تعزيز الحماية، وتوضيح مسؤوليات الاستجابة، وتقليل الاضطراب، ورفع مستوى المرونة السيبرانية داخل المؤسسة.

