BLACKBIRD FOR TRAINING

تقييم وإدارة مخاطر الأمن السيبراني



تقييم وإدارة مخاطر الأمن السيبراني

مقدمة

تعد الدورة التدريبية في تقييم وإدارة مخاطر الأمن السيبراني خطوة أساسية لكل من يرغب في حماية منظمتهم من التهديدات الإلكترونية المتزايدة. من خلال تعلم كيفية إجراء تقييم مخاطر الأمن السيبراني، ستحصل على المهارات اللازمة لتحديد وتقييم التهديدات الأمنية، بالإضافة إلى تطوير خطة تقييم الامتثال واعتماد عملية إدارة المخاطر المبنية على المعايير. ستركز الدورة على تقديم الأساسيات حول تقييم مخاطر الأمن السيبراني وأهميته في بيئة الأعمال المعاصرة. سيتم تطبيق هذه المعرفة لتوفير حماية فعالة للبنية التحتية للمعلومات، مع ضمان الامتثال للأنظمة والقوانين ذات الصلة.

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تطبيق منهجيات تقييم وإدارة مخاطر الأمن السيبراني المبنية على المعايير لضمان حماية المعلومات.
- اختيار وتنفيذ الضوابط الأمنية التي تضمن الامتثال للقوانين، اللوائح، والسياسات المتعلقة بالأمن السيبراني.
- توسيع الحماية الأمنية لتشمل أنظمة التحكم الصناعي ICS وأنظمة الحوسبة السحابية.
- فهم أهمية إدارة المخاطر في الأمن السيبراني وكيفية تطبيقه بنجاح في بيئات العمل.
- معرفة الفرق بين إدارة المخاطر وتقييم المخاطر في الأمن السيبراني.

محاور الدورة

اليوم الأول: مقدمة في تقييم وإدارة المخاطر



- ضمان الامتثال للوائح والأنظمة التنظيمية السارية.
- حماية المنظمة من الخسائر غير المقبولة.
- التعريف بإطار عمل إدارة المخاطر RMF.
- تطبيق عمليات إدارة المخاطر باستخدام معايير NIST وISO.
- تحديد متطلبات أمان النظام:
  - تعريف النظام.
  - تحديد حدود الأمان للنظام.
  - تحليل التداخلات النظامية.
  - دمج خصائص أنظمة التحكم الصناعي ICS وأنظمة السحابة.

اليوم الثاني: اختيار الضوابط الأمنية المناسبة

- فحص عائلات الضوابط الأمنية.
- تحديد الأساس الأمني بناءً على تحليل مخاطر الأمن السيبراني.
- تخصيص الأساس ليناسب النظام.
- دراسة هيكل الضوابط الأمنية وكيفية تخصيصها لاحتياجات النظام.

اليوم الثالث: تقليل المخاطر من خلال تنفيذ الضوابط

- تعظيم فعالية الأمن من خلال تضمين الأمان في النظام.
- تقليل المخاطر المتبقية في الأنظمة القديمة باستخدام عناصر أمان مضافة.
- تطوير خطة تقييم:
  - تحديد أولويات عمق التقييم.
  - التحقق من الامتثال من خلال الاختبارات والمقابلات والفحوصات.
  - إصدار توصية التوثيق.

اليوم الرابع: تفويض تشغيل النظام

- تقييم مستوى تحمل المخاطر في المنظمة.
- اتخاذ قرارات تفويض في السيناريوهات عالية المخاطر.
- إصدار التفويض لتشغيل النظام ATO.
- تقييم تأثير النظام على العمليات التشغيلية.



اليوم الخامس: الحفاظ على الامتثال المستمر

- قياس تأثير التغييرات على وضع الأمان في النظام.
- تنفيذ إدارة التكوين الفعالة.
- إعادة تقييم الضوابط الأمنية بشكل دوري.
- تقديم التدريب الأولي والمتابعة المستمرة للتوعية بالأمن السيبراني.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- تدريب عملي في تقييم وإدارة المخاطر في الأمن السيبراني باستخدام منهجيات معتمدة.
- تعزيز فهمك حول إدارة المخاطر في الأمن السيبراني وكيفية تطبيقها في بيئات العمل المختلفة.
- معرفة كيفية إجراء تقييم مخاطر الأمن السيبراني وتحليل أمان النظام لضمان حماية المعلومات الحساسة.
- تطوير المهارات اللازمة لضمان الامتثال للمتطلبات القانونية والتنظيمية.
- تعلم كيفية التعامل مع أنظمة التحكم الصناعي ICS والأنظمة السحابية في إطار الأمن السيبراني.

الخاتمة

تُعد هذه الدورة خطوة حاسمة نحو تعزيز أمن المعلومات في المنظمة من خلال تطبيق أفضل الممارسات في تقييم وإدارة المخاطر السيبرانية. إذا كنت ترغب في اكتساب المهارات اللازمة لمواجهة التحديات الأمنية المتزايدة في عالم اليوم المتصل، فإن هذه الدورة هي خيارك المثالي.

انضم الآن إلى دورة تدريبية متخصصة في تقييم مخاطر الأمن السيبراني وابدأ في حماية بياناتك ونظمك بفعالية.

