

تقييم وإدارة مخاطر الأمن السيبراني

UK Traininig

PARTNER



تقييم وإدارة مخاطر الأمن السيبراني

مقدمة

ستعلمك دورة تقييم وإدارة مخاطر الأمن السيبراني كيفية إجراء تقييم المخاطر الأمنية لحماية مؤسستك. سوف تتعرف على القوانين واللوائح التي تفرض متطلبات صارمة للأمن السيبراني على جميع المنظمات، وستكتسب المهارات اللازمة لتطوير خطة تقييم الامتثال واستخدام عملية إدارة المخاطر القائمة على المعايير مع الحفاظ على وضع أمني مرضٍ يجب أن يكون لدى الحضور معرفة أساسية بالعمليات التجارية ومفاهيم التكنولوجيا. لا يتم افتراض المعرفة التقنية المتخصصة

أهداف الدورة

- تطبيق منهجيات قائمة على المعايير ومثبتة لتقييم وإدارة المخاطر التي تتعرض لها البنية التحتية لمعلومات مؤسستك
- تحديد وتنفيذ ضوابط الأمان التي تضمن الامتثال للقوانين واللوائح والسياسات والتوجيهات المعمول بها
- تهديد الحماية الأمنية لأنظمة التحكم الصناعية ICS والسحابة

معايير الدورة

اليوم الأول : مقدمة في تقييم وإدارة المخاطر

- ضمان الامتثال للقوى التنظيمية المعمول بها
- حماية المنظمة من الخسائر غير المقبولة
- وصف إطار عمل إدارة المخاطر RMF
- تطبيق عمليات إدارة المخاطر ISO / NIST
- توصيف متطلبات أمن النظام

تحديد النظام

- تحديد حدود أمان النظام
- تحديد الترابط بين النظام
- دمج الخصائص الفريدة لأنظمة التحكم الصناعية ICS والأنظمة القائمة على السحابة

تحديد مكونات المخاطر الأمنية

- تقدير تأثير التنازلات على السرية والنزاهة والتوافر
- اعتماد النهج المناسب لتصنيف مخاطر النظام

تهيئة الطريق للإدارة ناجحة للمخاطر

- توثيق تقييم المخاطر الحرجة وقرارات الإدارة في خطة أمان النظام SSP
- تعيين الأفراد المؤهلين لدوار حوكمة المخاطر

اليوم الثاني: اختيار الضوابط الأمنية المناسبة و تعيين خط أساس للتحكم الأمني

- التحقيق في عائلات الضبط الأمني
- تحديد خط الأساس من مخاطر أمن النظام

PARTNER



تكيف خط الأساس ليناسب النظام

- فحص هيكل الضوابط والتحسينات والمعايير المهنية
- تراكبات التحكم الملزمة إلى الأساس المحدد
- قياس الحاجة إلى التأكيد المعزز
- التمييز بين الضوابط الخاصة بالنظام والضوابط التعويضية وغير القابلة للتطبيق

اليوم الثالث : تقليل المخاطر من خلال تنفيذ الرقابة الفعالة و تحديد نهج التنفيذ

- تعظيم الفعالية المهنية من خلال البناء في الزمن
- تقليل المخاطر المتبقية في النظرة القديمة من خلال عناصر الزمان "المثبتة"

تطوير خطة التقييم

- تحديد أولويات عهق تقييم التحكم
- تحسين التحقق من خلال التسلسل والدمج
- التحقق من الامتثال من خلال الاختبارات والمقابلات والامتحانات

صياغة توصية التفويض

- تقييم مخاطر أمن النظام الشاملة
- التخفيف من المخاطر المتبقية
- نشر خطة العول والمعالم M & POA وتقييم المخاطر والتوصية

اليوم الرابع: تفويض تشغيل النظام و التوفيق بين السلطة والمسؤولية

- قياس تحول المخاطر التنظيمية
- رفع قرارات التفويض في سيناريوهات عالية المخاطر

تشكيل قرار قائم على المخاطر

- تقييم النثر التشغيلي للنظام
- موازنة المخاطر المتبقية مقابل المرافق التشغيلية
- إصدار السلطة للتشغيل ATO

اليوم الخامس : الحفاظ على الامتثال المستمر و تبرير إعادة التفويض المستمر

- قياس تأثير التغييرات على وضع أمن النظام
- تنفيذ إدارة التكوين الفعالة
- إجراء إعادة تقييم دورية للمراقبة

الحفاظ على وضعية أمنية مقبولة

- تقديم تدريب متابعة أولي وروتيني للتوعية المهنية
- جمع مقاييس الزمان الجارية
- تنفيذ عمليات إدارة الثغرات المهنية والاستجابة للحوادث واستمرارية الأعمال

UK Training
PARTNER



Blackbird Training Clients



UK Training
PARTNER



البرامج التدريبية

إدارة المشافي
القطاع العام
ورشات عمل خاصة
النفط والغاز
هندسة الاتصالات
تكنولوجيا المعلومات
الصحة والسلامة
القانون وإدارة العقود
الجهازك و السلامة
الطيران والصلاح الجوية
الإدارة العليا

البرامج التقنية/البرامج الإدارية

المهارات الاحترافية
الهالية والمحاسبة والهيرانية
الإعلام والعلاقات العامة
إدارة المشاريع
الهوراد البشرية
تدقيق الحسابات وضمان الجودة
التسويق والمبيعات وخدمة العملاء
السكرتارية وإدارة المكاتب
سلسلة التوريد والخدمات اللوجستية
الإدارة والقيادة
الرشاقة والارتقاء



BLACKBIRD
FOR TRAINING



International House 185 Tower Bridge
Road London SE1 2UF United Kingdom



+44 7401 1773 35
+44 7480 775526



Sales@blackbird-training.com



www.blackbird-training.com

UK Training

PARTNER

