

معتود من هايكروسوفت: مساعد محلل العمليات الأمنية

UK Traininig

PARTNER



معتهد من هايكروسوفت: مساعد محلل العمليات الأمنية

مقدمة

تم تصميم دورة الشهادة المعتمدة من هايكروسوفت: محلل عمليات الأمن لمتخصصي تكنولوجيا المعلومات الذين يسعون لتعزيز مهاراتهم في إدارة وتأمين بنية الأمن السيبراني في المؤسسة. ك محلل عمليات الأمن المعتمد، ستلعب دوراً محورياً في حماية البيانات الحساسة، وتحديد تهديدات الأمن، وضمان الحفاظ على الأمن التشغيلي داخل مؤسستك. توفر هذه الدورة الشاملة التي تستغرق 5 أيام المعرفة الأساسية وتجارب عملية ضرورية لتحقيق الشهادة المعتمدة من هايكروسوفت لمحلل عمليات الأمن.

أهداف الدورة

- فهم أساسيات تحليل عمليات الأمن وأهميته الحاسمة في حماية النصول التنظيمية، وما يعالج أسئلة مثل "ما هو الأمن التشغيلي؟" وتقدير تعريف واضح للأمن التشغيلي.
- إظهار الكفاءة في تكوين واستخدام Sentinel Microsoft لاكتشاف الحوادث الأمنية والتحقق فيها والاستجابة لها، وهي مهارة أساسية لأي محلل عمليات الأمن المعتمد.
- اكتساب الخبرة في استخبارات التهديدات وصيد التهديدات، مما يمكن من التعرف الاستباقي على تهديدات الأمن ضمن مشهد الأمن السيبراني.
- إتقان Defender Azure لحماية عبء العمل والموارد السحابية، مما يضمن تعزيز التكنولوجيا التشغيلية للأمن السيبراني في مؤسستك ضد التهديدات.
- تعلم كيفية إنشاء وإدارة التنبيهات الأمنية، وإجراء تحقيقات شاملة، وتطوير خطط استجابة فعالة للحوادث، مع التأكيد على أفضل الممارسات في عمليات الأمن.
- اكتساب المهارات اللازمة لتحليل بيانات الأمن، وإجراء التقييمات الأمنية، وتنفيذ تقنيات أساسية في إدارة الأمن التشغيلي.
- التحضير بشكل شامل لامتحان الشهادة المعتمدة من هايكروسوفت: محلل عمليات الأمن، مما يضمن جاهزيتك للتفوق في مجال الأمن السيبراني.

محاور الدورة

اليوم الأول: أساسيات عمليات الأمن

- مقدمة في تحليل عمليات الأمن وأهميتها في الأمن العالمي للعمليات.
- دور ومسؤوليات محلل عمليات الأمن.
- فهم التهديدات والمخاطر المختلفة وأيضاً أنواع مراكز عمليات الأمن المرتبطة بها.
- أساسيات معالجة الحوادث الأمنية والاستجابة لها.
- نظرة عامة على Sentinel Microsoft وقدراته في إدارة الحوادث الأمنية.

اليوم الثاني: Sentinel Microsoft وكشف التهديدات

- تكوين واستخدام Sentinel Microsoft بفعالية.
- تقنيات جمع وتحليل السجلات لاكتشاف الحوادث الأمنية.
- التحقق والاستجابة للتنبيهات، مما يعزز عمليات الأمن السيبراني لديك.
- عمليات إدارة الحالة وتتبع الحوادث.

اليوم الثالث: استخبارات التهديدات وصيد التهديدات

- أهمية استخبارات التهديدات في عمليات الأمن.
- تقنيات صيد التهديدات الاستباقية للبقاء في مقدمة التهديدات المحتملة.
- استخدام استخبارات التهديدات لتعزيز عمليات الأمن، بما في ذلك أساليب الكشف المتقدمة في Sentinel Microsoft.

PARTNER



اليوم الرابع: Defender Azure لأمن السحاب

- مقدمة عن Defender Azure وميزاته الأمنية.
- تأمين عبء العمل والموارد السحابية ضد التهديدات الناشئة.
- تقنيات مراقبة وحماية بيانات Azure.

اليوم الخامس: التقييم الأمني واستجابة الحوادث

- إنشاء وإدارة التنبهات الأمنية لإدارة الحوادث بشكل فعال.
- تحليل بيانات الأمن للحصول على رؤى هامة وتقييمات.
- إجراء التقييمات الأمنية وإدارة الثغرات.
- تطوير وتنفيذ خطط استجابة الحوادث، مما يجعلك جاهزاً للتطبيقات الواقعية.

من خلال إكمال هذه الدورة، ستكتسب فهماً شاملاً للأمن التشغيلي، مصمماً خصيصاً لتحديات الأمن السبراني اليوم. سواء كنت تستكشف دورة عمليات الأمن البحري أو تركز على أمن أنظمة التشغيل، فإن هذا البرنامج مصمم لتعليمك بالمهارات والمعرفة اللازمة للتفوق في بيئة مركز عمليات الأمن SOC.

ابدأ رحلتك نحو أن تصبح محلل عمليات الأمن المعتمد واتخذ الخطوة الأولى نحو حماية النصول الرقمية

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

