BLACKBIRD FOR TRAINING

معتمد من مايكروسوفت: مساعد محلل العمليات الأمنية

November 2027 11 – 7

القاهرة (مصر)



معتمد من مايكروسوفت: مساعد محلل العمليات الأمنية

المرجع: 300482_321856 **التاريخ:** 7 – 11 November 2027 **المكان:** القاهرة (مصر) **الرسوم:** GBP 4900

مقدمة الدورة

تُعد دورة محلل عمليات الأمن المعتمد من مايكروسوفت من البرامج التدريبية المهمة للمتخصصين الراغبين في تعزيز قدراتهم في حماية البيئات الرقمية الحديثة، ومراقبة التهديدات الأمنية، والاستجابة للحوادث السيبرانية بكفاءة أعلى. وفي ظل التوسع المستمر في المخاطر الرقمية، أصبحت المؤسسات بحاجة إلى كوادر قادرة على دعم الأمن التشغيلي، وتحليل الأحداث الأمنية، واكتشاف الأنشطة المشبوهة، والتعامل مع الحوادث بصورة سريعة ومنظمة.

تقدم هذه الدورة المكثفة على مدى أسبوع فهمًا عمليًا ومنهجيًا لمجال عمليات الأمن السيبراني، حيث تجمع بين المفاهيم الأساسية والتطبيقات العملية التي يحتاجها المتخصص في هذا المجال. كما توضح دور محلل عمليات الأمن داخل بيئة العمل، وتجيب بصورة عملية عن سؤال ما هو الأمن التشغيلي، مع تقديم مفهوم الأمن التشغيلي ضمن سياق المراقبة والتحليل والاستجابة للحوادث. كذلك تتناول الدورة أهم الأدوات والممارسات المستخدمة في دورة مركز عمليات الأمن، مع تركيز خاص على تقنيات مايكروسوفت مثل مايكروسوفت سنتينل وأزور ديفندر.

وتركز الدورة أيضًا على تنمية المهارات المرتبطة باكتشاف التهديدات، والتحقيق في الحوادث، وإدارة تنبيهات عمليات الأمن، ومعالجة الثغرات، وتطبيق أساليب دفاع استباقية. ومع الاهتمام بـ أفضل ممارسات عمليات الأمن والتقنيات التشغيلية للأمن السيبراني، تمنح هذه الدورة المشاركين قاعدة قوية تساعدهم على التعامل مع التهديدات المتغيرة والاستعداد بشكل أفضل لاجتياز الاختبار المهني المرتبط بهذه الشهادة.

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:



- فهم أساسيات تحليل عمليات الأمن وأهمية الأمن التشغيلي في حماية أصول المؤسسة.
- توضيح ما هو الأمن التشغيلي وتطبيق مفهوم الأمن التشغيلي في الأنشطة اليومية المرتبطة بالأمن السيبراني.
- استخدام مايكروسوفت سنتينل بكفاءة في دعم عمليات الأمن السيبراني.
- اكتشاف الحوادث الأمنية والتحقيق فيها والاستجابة لها باستخدام أساليب المراقبة والتحليل الحديثة.
- تطبيق أساليب استخبارات التهديدات وصيد التهديدات للكشف المبكر عن المخاطر وتقليل آثارها.
- استخدام أزور ديفندر لحماية البيئات السحابية وتعزيز أمن التقنيات التشغيلية للأمن السيبراني.
- إنشاء وإدارة تنبيهات عمليات الأمن بصورة فعالة، مع دعم إجراءات التحقيق والاستجابة للحوادث.
- تنفيذ تقييمات أمنية وتحليل الثغرات والمساهمة في تحسين إدارة الأمن التشغيلي.
- تطوير خطط الاستجابة للحوادث وفقًا لـ أفضل ممارسات عمليات الأمن.
- الاستعداد بصورة أفضل لاجتياز اختبار محلل عمليات الأمن المعتمد من مايكروسوفت والنجاح في الأدوار المهنية المرتبطة بهذا المجال.

محاور الدورة

اليوم الأول: أساسيات عمليات الأمن

- مقدمة في تحليل عمليات الأمن وأهميته في البيئات التشغيلية الحديثة
- التعرف على دور محلل عمليات الأمن ومسؤولياته
- شرح الأمن التشغيلي وأثره في حماية الأنظمة والبيانات
- استعراض أنواع مركز عمليات الأمن والمخاطر المرتبطة بها
- مقدمة في إدارة الحوادث الأمنية وآليات التصعيد والاستجابة
- التعرف على دور مايكروسوفت سنتينل في مراقبة الحوادث الأمنية وإدارتها

اليوم الثاني: مايكروسوفت سنتينل واكتشاف التهديدات

- إعداد واستخدام مايكروسوفت سنتينل في دعم عمليات الأمن السيبراني
- أساليب جمع السجلات وتحليلها للكشف عن الحوادث الأمنية
- اكتشاف السلوكيات المشبوهة والتحقيق في الحوادث بشكل فوري
- إدارة الحوادث والتنبيهات ومسارات المتابعة داخل مايكروسوفت سنتينل
- تحسين الرؤية الأمنية ورفع كفاءة الاستجابة داخل البيئة التشغيلية



اليوم الثالث: استخبارات التهديدات وصيد التهديدات

- أهمية استخبارات التهديدات في دعم عمليات الأمن
- استخدام مصادر استخبارات التهديدات لفهم المخاطر الناشئة
- تطبيق أساليب صيد التهديدات للكشف عن الأنشطة الخفية قبل تطورها
- تعزيز إمكانات مايكروسوفت سنتينل باستخدام أساليب اكتشاف متقدمة
- دعم الاكتشاف المبكر والاستجابة الأسرع من خلال التحليل المبني على المعلومات

اليوم الرابع: أزور ديفندر وأمن البيئة السحابية

- مقدمة في أزور ديفندر وخصائصه الأمنية لحماية الأحمال السحابية
- حماية الموارد السحابية من التهديدات المتطورة والأنشطة غير المصرح بها
- أساليب مراقبة بيئات أزور وتعزيز جاهزيتها الأمنية
- دعم حماية الأصول السحابية والتقنيات التشغيلية للأمن السيبراني
- تعزيز أمن الاعتماد السحابي من خلال المتابعة المستمرة والسياسات والضوابط

اليوم الخامس: التقييم الأمني والاستجابة للحوادث

- إنشاء وإدارة تنبيهات عمليات الأمن لدعم التحقيق وتتبع الحوادث
- تحليل البيانات الأمنية لاستخلاص المؤشرات والتهديدات الحرجة
- تنفيذ التقييمات الأمنية وإدارة الثغرات بشكل منهجي
- تطوير وتنفيذ خطط الاستجابة للحوادث استنادًا إلى أفضل ممارسات عمليات الأمن
- تحسين إدارة الأمن التشغيلي من خلال التقييم والمراجعة والتطوير المستمر

لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات!

- اكتساب فهم عملي ومنظم لمجال تحليل عمليات الأمن ومبادئ الأمن التشغيلي.
- تنمية المهارات التطبيقية في استخدام مايكروسوفت سنتينل وأزور ديفندر داخل البيئات الأمنية الحديثة.
- تعلم كيفية اكتشاف التهديدات، والتحقيق في الحوادث، وإدارة تنبيهات عمليات الأمن بكفاءة أعلى.
- تعزيز القدرات في استخبارات التهديدات وصيد التهديدات وإدارة الثغرات والاستجابة للحوادث.

رفع الجاهزية للعمل ضمن مركز عمليات الأمن والاستعداد بشكل أفضل لاجتياز اختبار محلل عمليات الأمن المعتمد من مايكروسوفت.

- بناء معرفة أعمق تدعم اتخاذ القرار وتطبيق أفضل ممارسات عمليات الأمن في بيئة العمل.



الخاتمة

توفر دورة محلل عمليات الأمن المعتمد من مايكروسوفت مسارًا تدريبيًا متكاملاً للمتخصصين الذين يسعون إلى تطوير دورهم في بيئات الأمن السيبراني الحديثة. فهي تجمع بين المعرفة الأساسية، والتطبيق العملي، وأدوات المراقبة والتحليل والاستجابة، بما يساعد المشاركين على فهم ما هو الأمن التشغيلي وتطبيق مفهوم الأمن التشغيلي بشكل عملي داخل بيئة العمل.

وخلال هذه الدورة، يكتسب المشاركون مهارات مهمة في استخدام مايكروسوفت سنتينل وأزور ديفندر، والاستفادة من استخبارات التهديدات، وتطبيق صيد التهديدات، وإجراء التقييمات الأمنية، وإدارة الحوادث بصورة أكثر فاعلية. ومن خلال ربط هذه الجوانب بـ أفضل ممارسات عمليات الأمن، تسهم الدورة في رفع كفاءة المشاركين، وتعزيز إدارة الأمن التشغيلي، ودعم تقدمهم المهني نحو الشهادة والنجاح في مجال عمليات الأمن.

