

مراقبة أمن الشبكات وتنفيذ نظم إدارة المعلومات
والأحداث الأمنية

UK Traininig

PARTNER



مراقبة أمن الشبكات وتنفيذ نظم إدارة المعلومات والأحداث الأمنية

مقدمة

في ظل التهديدات الإلكترونية المتزايدة وتنوع أساليب الهجمات الرقمية، أصبحت مراقبة أمن الشبكات وتنفيذ نظم إدارة المعلومات والأحداث الأمنية من أهم الركائز لحماية البنية التحتية الرقمية للمؤسسات.

تهدف هذه الدورة إلى تمكين المشاركين من فهم عميق لأساليب المراقبة الفعالة، وآليات تحليل البيانات الأمنية، وتطبيق أنظمة الإدارة الذكية التي تساهم في كشف التهديدات والاستجابة لها في الوقت المناسب.

تركز الدورة على الدمج بين الجوانب النظرية والعملية، من خلال التعرف على المكونات الأساسية لأنظمة المراقبة، وآلية عمل نظم الإدارة الأمنية، وكيفية تحليل السجلات واكتشاف الأنماط غير الطبيعية.

كما تمنح المشاركين القدرة على بناء بيئة مراقبة متكاملة تعتمد على التحليل الآلي والمستمر للبيانات لضمان أعلى مستويات الأمان والاستجابة.

أهداف الدورة

بنهاية هذه الدورة سيتمكن المشاركون من:

- فهم المفاهيم الأساسية لمراقبة أمن الشبكات ومكوناتها الرئيسية.
- تطبيق أنظمة إدارة المعلومات والأحداث الأمنية بشكل فعال.
- تحليل السجلات الأمنية واستخراج المؤشرات الدالة على المخاطر.
- اكتشاف الأنشطة المشبوهة في الوقت الحقيقي والتعامل معها.
- بناء مركز عمليات أمنية يعتمد على التحليل الآلي للبيانات.
- تطبيق آليات الاستجابة السريعة للحوادث الإلكترونية.
- دمج المراقبة الأمنية ضمن سياسات المؤسسة التقنية.
- تعزيز مستوى الحماية ضد الهجمات المتقدمة والمستمرة.

UK Training

PARTNER



محاور الدورة

اليوم الأول: أساسيات مراقبة أمن الشبكات

- المفاهيم العامة لمراقبة الشبكات وأهميتها في المؤسسات الحديثة.
- أنواع التهديدات التي تستهدف البنى التحتية الرقمية.
- مكونات نظام المراقبة الأمني وأدواته الرئيسية.
- طرق جمع وتحليل البيانات من الأجهزة والشبكات.
- التعرف على الأنماط غير الطبيعية في حركة البيانات.
- تمرين عملي لتطبيق تحليل أولي لحركة الشبكة.

اليوم الثاني: المفاهيم الأساسية لأنظمة الإدارة الأمنية

- تعريف نظم إدارة المعلومات والأحداث الأمنية ووظائفها.
- كيفية تجميع البيانات من مصادر متعددة داخل المؤسسة.
- مراحل تحليل البيانات داخل النظام الأمني.
- التعرف على مؤشرات الاختراق والهجمات الرقمية.
- إعداد السياسات الأمنية وربطها بنظام المراقبة.
- تمرين تطبيقي حول إدارة الأحداث الأمنية في الوقت الحقيقي.

اليوم الثالث: تصميم وتنفيذ بيئة المراقبة الأمنية

- متطلبات بناء مركز مراقبة أمني متكامل.
- إعداد خريطة تدفق البيانات بين الأنظمة المختلفة.
- تحديد نقاط المراقبة الحرجة داخل الشبكة.
- اختيار أدوات التحليل المناسبة لاحتياجات المؤسسة.
- إعداد تقارير دورية لقياس فعالية المراقبة.
- ورشة عمل لتصميم نموذج لمركز عمليات أمنية.

UK Training

PARTNER



اليوم الرابع: الاستجابة للحوادث والتحليل المتقدم

- منهجيات التعامل مع الحوادث الأمنية واكتشافها المبكر.
- تحليل السجلات التفصيلية بعد وقوع الاختراقات.
- تحديد مصدر الهجوم ومسار الاختراق.
- تطبيق أساليب التحليل السلوكي للمستخدمين والأنظمة.
- وضع خطة استجابة متكاملة للحوادث الأمنية.
- تمرين عملي لمحاكاة استجابة لحادث أمني فعلي.

اليوم الخامس: التكامل، التقييم، والتحسين المستمر

- دمج أنظمة الإدارة الأمنية مع حلول الحماية الأخرى.
- تطوير مؤشرات أداء لمتابعة كفاءة النظام الأمني.
- تحليل الثغرات وتحسين خطط الاستجابة المستقبلية.
- استخدام التحليل التلي في كشف الأنماط المتكررة للهجمات.
- مناقشة أفضل الممارسات في تنفيذ نظم المراقبة الأمنية.
- تقييم نهائي للمشاركين ومراجعة أهم المفاهيم المكتسبة.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب فهم متكامل لأحدث تقنيات مراقبة الشبكات وإدارة الأمن.
- تطوير مهارات تحليل البيانات الأمنية والاستجابة للحوادث.
- بناء قدرات مؤسسية فعالة للكشف المبكر عن التهديدات.
- تحسين كفاءة نظم الحماية وتقليل زمن التعافي من الهجمات.
- تعلم كيفية إدارة الأحداث الأمنية في بيئة معقدة.
- تعزيز الجاهزية التقنية للتعامل مع الهجمات المتقدمة.
- ربط المراقبة الأمنية بالحوكمة المؤسسية وسياسات الامتثال.
- تطبيق ممارسات عملية قابلة للتنفيذ مباشرة داخل المؤسسة.

الخاتمة

تعد مراقبة أمن الشبكات وتنفيذ نظم إدارة المعلومات والأحداث الأمنية من الركائز الأساسية لحماية المؤسسات في العصر الرقمي.

UK Training

PARTNER



فهي لا تقتصر على كشف الهجمات فحسب، بل تمتد إلى تحليل السلوك، التنبؤ بالتهديدات، وتعزيز قدرة المؤسسات على اتخاذ قرارات استباقية.

من خلال هذه الدورة، يتمكن المشاركون من بناء أنظمة مراقبة متطورة تعتمد على التحليل الذكي للبيانات وتطبيق أفضل الممارسات في إدارة الأمن المؤسسي، بما يضمن استمرارية العمل وسلامة البنية التحتية التقنية.

UK Traininig

PARTNER

