BLACKBIRD FOR TRAINING

إدارة الجدار الناري وأمن الشبكات

9 – 13 August 2027

باريس (فرنسا)



إدارة الجدار الناري وأمن الشبكات

المرجع: 337940_3255319 **التاريخ:** 9 – 13 August 2027 **المكان:** باريس (فرنسا) **الرسوم:** GBP 5900

مقدمة

في العصر الرقمي الحالي، أصبحت حماية البنية التحتية للشبكات من التهديدات السيبرانية ضرورة أساسية لضمان نجاح المؤسسات واستمراريتها.

سواء كانت الشبكات تعمل في بيئة مؤسسية، أو سحابية، أو في مراكز البيانات، فإن الإدارة الفعالة للجدران النارية وتطبيق ممارسات أمن الشبكات تمثل حجر الأساس للحفاظ على سرية البيانات واستقرار العمليات واستمرارية الأعمال.

تركز هذه الدورة على تزويد المشاركين بالمعرفة الأساسية والمهارات العملية لإدارة الجدران النارية وتأمين الشبكات بفعالية.

تم تصميم التدريب ليجمع بين الجانب النظري والتطبيقي، مع تشجيع المتدربين على مناقشة التحديات الواقعية من بيئة عملهم وتطبيق الحلول المناسبة ضمن مختبرات محاكاة عملية.

أهداف الدورة

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

1. فهم مبادئ أمن الشبكات والتعرف على مفاهيم الأمن السيبراني ومصادر التهديد وأساليب الدفاع.
2. تكوين وإدارة الجدران النارية وضبط إعداداتها لحماية الشبكات من التهديدات الداخلية والخارجية.
3. تطبيق أنظمة كشف ومنع التسلل واستخدامها لرصد الهجمات والتحكم في الاستجابة لها.
4. تحليل حركة البيانات ومراقبة السجلات لتحديد الأنشطة المشبوهة.
5. تطوير سياسات أمنية فعالة والاستجابة للحوادث الأمنية وفق منهجية منظمة.
6. تنفيذ تطبيقات عملية في بيئات محاكاة تشمل إعداد الجدران النارية، وتحديد القواعد الأمنية، وتشغيل أدوات المراقبة.



محاور الدورة

اليوم الأول: أساسيات أمن الشبكات

- مقدمة في مفاهيم الأمن السيبراني وأركانه الأساسية السرية، السلامة، التوافر.
- التعرف على أنواع الجدران النارية وأدوارها في حماية الشبكات.
- تحليل مشهد التهديدات السيبرانية الشائعة مثل البرمجيات الخبيثة وهجمات التصيد.
- مبادئ تطوير السياسات الأمنية والتحكم في الوصول إلى الشبكات.
- تقييم المخاطر ووضع استراتيجيات الحد من التهديدات.
- تمرين عملي: إعداد أولي لجدار ناري بسيط لحماية شبكة داخلية.

اليوم الثاني: هندسة الجدران النارية ونشرها

- تصميم المناطق الشبكية الآمنة وتكوين مناطق العزل DMZ.
- إعداد فلاتر الحزم وتحديد القواعد بناءً على العناوين والبروتوكولات.
- تأمين الاتصال عن بعد باستخدام الشبكات الافتراضية الخاصة.
- مراقبة أداء الجدار الناري وتسجيل الأحداث الأمنية.
- استخدام أدوات المراقبة لتحليل الأنشطة غير المصرح بها.
- تمرين عملي: إعداد جدار ناري متعدد الطبقات وتأمين الاتصالات البعيدة.

اليوم الثالث: الإدارة المتقدمة للجدران النارية

- مقارنة بين الجدران النارية التقليدية والجدران الحديثة متعددة الوظائف.
- مفاهيم ترجمة العناوين وإدارة الاتصال الآمن بين الشبكات.
- تحسين أداء الجدار الناري والحفاظ على كفاءته التشغيلية.
- ضبط قواعد الحركة الشبكية لضمان الأداء الآمن والمتوازن.
- اكتشاف الأعطال وتحديد الثغرات الأمنية في الجدار الناري.
- تطبيق عملي: إنشاء قواعد حماية متقدمة واختبار فاعليتها.



اليوم الرابع: كشف التسلل ومنع التهديدات

- فهم مفهوم أنظمة كشف التسلل وأنظمة المنع ودورها في حماية الشبكات.
- تحليل الهجمات الإلكترونية وأساليب اكتشافها.
- إدارة التنبيهات الأمنية وربطها بأحداث النظام.
- تحليل البيانات والربط بين السجلات لرصد الأنشطة المشبوهة.
- استخدام أدوات كشف التهديدات في بيئة محاكاة عملية.
- تمرين تطبيقي: محاكاة هجوم سيبراني والاستجابة له من خلال الجدار الناري ونظام كشف التسلل.

اليوم الخامس: الاستجابة للحوادث وتطبيق السياسات الأمنية

- تطبيق أفضل الممارسات في أمن الشبكات وفق الأطر والمعايير المعتمدة.
- مراحل الاستجابة للحوادث: الاكتشاف، الاحتواء، المعالجة، والتوثيق.
- تطوير السياسات الأمنية وضمان الالتزام بها داخل المؤسسة.
- إدارة الامتثال ومتابعة الإجراءات التصحيحية.
- تطبيق عملي شامل: تصميم وتنفيذ نظام حماية متكامل للشبكة.
- مراجعة ختامية وتقييم الأداء واختبار المعرفة المكتسبة.

لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات!

- اكتساب معرفة متقدمة في أمن الشبكات وإدارة الجدران النارية بفعالية.
- تطبيق عملي لأدوات الأمن السيبراني في بيئات تدريب محاكاة واقعية.
- تعزيز الكفاءة المهنية لمتخصصي تقنية المعلومات ومسؤولي الأمن.
- تقليل احتمالات الاختراق وتحسين استقرار الشبكة المؤسسية.
- تطوير مهارات تحليل الحوادث والاستجابة للطوارئ التقنية.
- تحسين الامتثال للمعايير الدولية في أمن المعلومات.
- رفع موثوقية الأنظمة وزيادة جاهزيتها التشغيلية.
- تعزيز فرص النمو المهني في مجالات الأمن السيبراني وإدارة المخاطر.

الخاتمة

تزود دورة إدارة الجدار الناري وأمن الشبكات المتدربين بالمعرفة العملية والفنية اللازمة لحماية الشبكات الحديثة من التهديدات السيبرانية المتزايدة.من خلال الدمج بين التدريب العملي والنظري، يكتسب المشاركون القدرة على تصميم وتنفيذ أنظمة حماية فعالة تتماشى مع متطلبات الأمن المؤسسي.



تمثل هذه الدورة خطوة أساسية نحو بناء كفاءات أمنية متقدمة، وضمان استمرارية الأعمال وحماية البنية التحتية الرقمية بكفاءة عالية.

