



دورة:
أمن الشبكة والنظم

2025 - 31 - 27
باكتو

أمن الشبكة والنظم

رمز الدورة: IT12818 | تاريخ الإنعقاد: 27 - 31 أكتوبر 2025 | دولة الإنعقاد: باكو | رسوم الإنعقاد: 5500 Euro

مقدمة

في عالم يتزايد فيه الاعتماد على التكنولوجيا والشبكات الرقمية، أصبح أمن الشبكات والنظم أمرًا حيوياً لحماية المعلومات الحساسة وضمان استمرارية الأعمال. تهدف هذه الدورة التدريبية المدتها 5 أيام إلى تزويذ المشاركين بفهم شامل لأساليب أمن الشبكات والنظم، التشفير، إدارة المفاتيح، تأمين البنية التحتية للشبكة، الأمن السحابي، وإدارة الحوادث والتعافي من الكوارث. من خلال دمج النظرية بالتطبيق العملي، ستمكن الدورة المشاركين من تطوير المهارات اللازمة لتأمين البيانات التكنولوجية في مواجهة التهديدات المتطرفة.

أهداف البرنامج

- فهم أساسيات أمن الشبكات والنظم: تقديم المفاهيم الأساسية والمصطلحات المتعلقة بأمن الشبكات والنظم.
- معرفة التشفير وإدارة المفاتيح: تعلم كيفية استخدام التشفير وإدارة المفاتيح لحماية البيانات.
- تأمين البنية التحتية للشبكة: تطبيق أفضل الممارسات لحماية البنية التحتية للشبكة والأجهزة المتصلة.
- الأمان في البيئات السحابية والشبكات اللاسلكية: فهم التحديات الأمنية الخاصة بالسحابة والشبكات اللاسلكية وكيفية معالجتها.
- إدارة الحوادث والتعافي من الكوارث: تطوير مهارات في إعداد خطط استجابة للحوادث وتنفيذ استراتيجيات التعافي من الكوارث.

الجمهور المستهدف

هذه الدورة مصممة خصيصاً للأفراد الذين يرغبون في تعزيز معرفتهم ومهاراتهم في مجال أمن الشبكات والنظم، بما في ذلك:

- المهنيين في مجال تكنولوجيا المعلومات: الذين يعملون في أدوار تتعلق بالشبكات، الأمن السيبراني، أو إدارة النظم.
- المدراء التنفيذيون لتكنولوجيا المعلومات: الذين يحتاجون إلى فهم شامل للمخاطر الأمنية وكيفية إدارتها.
- الطلاب والخريجون الجدد: الراغبون في دخول مجال الأمن السيبراني أو توسيع معرفتهم في هذا المجال.
- أي شخص لديه اهتمام بتعلم كيفية حماية الشبكات والنظم من التهديدات الأمنية.

المحاور العامة

اليوم الاول: أساسيات أمن الشبكات والنظم

- مقدمة عامة عن أمن الشبكات والنظم.
- فهم التهديدات، الضعف، والهجمات الأساسية.
- أهمية أمن الشبكات في الحماية ضد الهجمات الإلكترونية.

اليوم الثاني: التشفير وإدارة المفاتيح

- مبادئ التشفير والأنواع الرئيسية للتشفير الكلاسيكي والحديث.
- إدارة المفاتيح والشهادات الرقمية.
- بروتوكولات التشفير المستخدمة في تأمين الاتصالات.

اليوم الثالث: حماية البنية التحتية للشبكة

- جدران الحماية وأنظمة الكشف عن التسلل IDS وأنظمة الوقاية من التسلل IPS.
- تأمين البنية التحتية للشبكة والأجهزة الطرفية.
- استراتيجيات تأمين نقاط النهاية والسيرفرات.

اليوم الرابع: الأمن السحابي والشبكات اللاسلكية

- تحديات الأمان في البيانات السحابية وكيفية مواجهتها.
- تأمين الشبكات اللاسلكية وبروتوكولات التشفير المتقدمة.
- أفضل الممارسات لإدارة الأمان في الشبكات اللاسلكية والسحابية.

اليوم الخامس: إدارة الحوادث والتعافي من الكوارث

- إعداد خطط استجابة للحوادث وإدارة الحوادث الأمنية.
- استراتيجيات التعافي من الكوارث واستمرارية الأعمال.
- تمارين عملية على سيناريوهات واقعية وكيفية التعامل مع الحوادث الأمنية.