Global Horizon
TRAINING CENTER

دورة:
أمن الشبكة والنظم

11 - 15 مايو 2025

الإسكندرية

أمن الشبكة والنظم

رمز الدورة: IT12818 تاريخ الإنعقاد: 11 - 15 مايو 2025 دولة الإنعقاد: الإسكندرية - رسوم الإشتراك: 4500 Euro

مقدمة

في عالم يتزايد فيه الاعتماد على التكنولوجيا والشبكات الرقمية، أصبح أمن الشبكات والنظم أمرًا حيويًا لحماية المعلومات الحساسة وضمان استمرارية الأعمال. تهدف هذه الدورة التدريبية المدتها 5 أيام إلى تزويد المشاركين بفهم شامل لأساسيات 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 البيئات التكنولوجية في مواجهة التهديدات المتطورة.

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 خصيصًا 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 العامه

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 التشفير 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 الأمن في البيئات 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.