Global Horizon
TRAINING CENTER

دورة:

إدارة الثغرات السيبرانية و معالجتها

10 - 14 مارس 2025

بوسطن (الولايات المتحدة الأمريكية)

إدارة الثغرات السيبرانية و معالجتها

رمز الدورة: IT12819 تاريخ الإنعقاد: 10 - 14 مارس 2025 دولة الإنعقاد: بوسطن (الولايات المتحدة الأمريكية) - رسوم الإشتراك: 6200 Euro

مقدمة

في عالم تزداد فيه التهديدات السيبرانية تعقيدًا وتكرارًا، تصبح إدارة الثغرات السيبرانية ومعالجتها جزءًا حيويًا من استراتيجية الأمن السيبراني لأي مؤسسة. هذه الدورة التدريبية المكثفة لمدة 5 أيام مصممة لتزويد المشاركين بالمعرفة والمهارات اللازمة لتحديد، تقييم، ومعالجة الثغرات السيبرانية بفعالية. من خلال مزيج من الدروس النظرية والتطبيقات العملية، سيكتسب المشاركون فهمًا عميقًا لأساسيات الثغرات السيبرانية، استراتيجيات التخفيف، وأفضل الممارسات لضمان أمان المعلومات ضمن منظماتهم.

أهداف البرنامج

- فهم الثغرات السيبرانية: تعريف المشاركين على مفاهيم الثغرات السيبرانية، أنواعها، وأساليب اكتشافها.
- تقييم وتحليل الثغرات: تزويد المشاركين بالأدوات والتقنيات لتقييم وتحليل الثغرات، وتعلم كيفية تحديد أولوياتها بناءً على درجة الخطورة.
- معالجة الثغرات: تعلم استراتيجيات وأساليب فعالة لمعالجة وتصحيح الثغرات، بالإضافة إلى إدارة الحوادث الأمنية.
- تطبيق المعرفة: تطبيق المعرفة المكتسبة من خلال تمارين عملية وسيناريوهات واقعية لتعزيز الفهم والمهارات.
- بناء ثقافة الأمان: تشجيع المشاركين على بناء ثقافة الأمان داخل منظماتهم وتبني أفضل الممارسات للحفاظ على بيئة عمل آمنة.

الجمهور المستهدف

هذه الدورة موجهة لمجموعة واسعة من المهنيين في مجال تكنولوجيا المعلومات والأمن السيبراني، بما في ذلك:

- مدراء الأمن السيبراني والمختصين: الذين يرغبون في تعزيز معرفتهم ومهاراتهم في إدارة الثغرات.
- محللو الأمن: الباحثون عن تعميق فهمهم لتحليل ومعالجة الثغرات الأمنية.
- مهندسو الشبكات ونظم المعلومات: الراغبين في تطوير قدراتهم في حماية البنى التحتية السيبرانية.
- المطورون والمبرمجون: الذين يسعون لفهم أفضل لأمن التطبيقات وكيفية تطوير برمجيات آمنة من الثغرات.
- طلاب تكنولوجيا المعلومات والأمن السيبراني: الباحثون عن توسيع معارفهم وتحسين فرصهم الوظيفية في مجال الأمن السيبراني.

المحاور العامه

اليوم الاول: المبادئ الأساسية وفهم الثغرات السيبرانية

- مقدمة عن الأمن السيبراني وأهميته.

- تعريف الثغرات السيبرانية، أنواعها، وأمثلة على ثغرات شائعة.
- كيفية اكتشاف الثغرات: أدوات وتقنيات الفحص.

اليوم الثاني: تقييم وتحليل الثغرات

- أساليب تقييم الثغرات وتصنيفها حسب الخطورة.
- تحليل الثغرات لفهم تأثيرها وكيفية استغلالها.
- استخدام أدوات التحليل والمحاكاة لفهم الثغرات بشكل أعمق.

اليوم الثالث: استراتيجيات معالجة الثغرات

- أساليب وأفضل الممارسات في معالجة الثغرات.
- التصحيح والتخفيف: كيفية اختيار الحل المناسب.
- إعداد خطط الاستجابة للحوادث وإدارة المخاطر.

اليوم الرابع: الأمن العملي والتدريبات

- تدريب عملي على أدوات فحص وتحليل الثغرات.
- تمارين على سيناريوهات واقعية لمعالجة الثغرات.
- تطبيق مبادئ التشفير والأمان لحماية البيانات.

اليوم الخامس: الاتجاهات المستقبلية وأفضل الممارسات

- نقاش حول الاتجاهات الحديثة في إدارة الثغرات السيبرانية.
- أفضل الممارسات والاستراتيجيات للحفاظ على بيئة عمل آمنة.
- كيفية بناء ثقافة الأمان في المؤسسات.