Global Horizon
TRAINING CENTER

دورة:

تصميم معمارية الأمن السيبراني

16 - 20 يونيو 2025

باكو

تصميم معمارية الأمن السيبراني

رمز الدورة: IT12831 تاريخ الإنعقاد: 16 - 20 يونيو 2025 دولة الإنعقاد: باكو - رسوم الإشتراك: 5500 Euro

مقدمة

مع ازدياد اعتماد العالم على التكنولوجيا، يزداد أيضًا خطر الهجمات الإلكترونية لذلك يُعدّ تصميم معمارية الأمن السيبراني الفعال أمرًا بالغ الأهمية لحماية المؤسسات من هذه الهجمات و تهدف هذه الدورة إلى تزويد المشاركين بالمهارات والمعرفة اللازمة لتصميم وتنفيذ معمارية الأمن السيبرانيه

أهداف البرنامج

- فهم مبادئ التصميم في معمارية الأمن السيبراني
- القدرة على تحليل المخاطر وتقييمها
- القدرة على تصميم عناصر التحكم في الوصول
- القدرة على تصميم شبكات آمنة
- القدرة على تصميم أنظمة الكشف عن التسلل ومنعها
- القدرة على تصميم أنظمة الاستجابة للحوادث
- القدرة على تصميم أنظمة إدارة الهوية والوصول
- القدرة على تصميم أنظمة إدارة التشفير
- القدرة على تطبيق أفضل الممارسات في تصميم معمارية الأمن السيبراني
- القدرة على مواكبة أحدث الاتجاهات في تصميم معمارية الأمن السيبراني

الفئات المستهدفة

- مهندسو الأمن السيبراني
- مهندسو الشبكات
- مسؤولي أنظمة المعلومات
- مديرو تكنولوجيا المعلومات
- أي شخص مهتم بتصميم وتنفيذ معمارية الأمن السيبراني

ما الذي ستتعلمه؟

- ستتعلم مبادئ التصميم الأساسية لعمارة الأمن السيبراني.

- ستتعلم كيفية تحليل المخاطر وتقييمها.
- ستتعلم كيفية تصميم عناصر التحكم في الوصول.
- ستتعلم كيفية تصميم شبكات آمنة.
- ستتعلم كيفية تصميم أنظمة الكشف عن التسلل ومنعها.
- ستتعلم كيفية تصميم أنظمة الاستجابة للحوادث.
- ستتعلم كيفية تصميم أنظمة إدارة الهوية والوصول.
- ستتعلم كيفية تصميم أنظمة إدارة التشفير.
- ستتعلم كيفية تطبيق أفضل الممارسات في تصميم معمارية الأمن السيبراني.
- ستتعلم كيفية مواكبة أحدث الاتجاهات في تصميم معمارية الأمن السيبراني.

كيف ستستفيد من هذه الدورة؟

- ستتمكن من تصميم وتنفيذ معمارية الأمن السيبراني الفعالة.
- ستتمكن من حماية المؤسسات من الهجمات الإلكترونية.
- ستتمكن من تحسين مهاراتك في مجال الأمن السيبراني.
- ستتمكن من الحصول على شهادة معتمدة في تصميم معمارية الأمن السيبراني.

المحاور العامه

اليوم الأول:

- مقدمة في الأمن السيبراني
- مبادئ التصميم في معمارية الأمن السيبراني
- النماذج الشائعة لعمارة الأمن السيبراني
- تحليل المخاطر وتقييمها

اليوم الثاني:

- تصميم عناصر التحكم في الوصول
- تصميم شبكات آمنة
- تصميم أنظمة الكشف عن التسلل ومنعها
- تصميم أنظمة الاستجابة للحوادث

اليوم الثالث:

- تصميم أنظمة إدارة الهوية والوصول
- تصميم أنظمة إدارة التشفير
- تصميم أنظمة الأمن السيبراني للمؤسسات
- أفضل الممارسات في تصميم معمارية الأمن السيبراني

اليوم الرابع:

- دراسة حالات حقيقية لتصميم معمارية الأمن السيبراني
- أحدث الاتجاهات في تصميم معمارية الأمن السيبراني
- ورشة عمل تطبيقية لتصميم معمارية الأمن السيبراني

اليوم الخامس:

- اختبارات تقييمية
- مراجعة الدورة
- توزيع الشهادات