Global Horizon
TRAINING CENTER

دورة:

# حوكمة السياسات و الإجراءات الامن السيبراني

13 - 17 يوليو 2026

كوالالمبور (ماليزيا)

# حوكمة السياسات و الإجراءات  الامن السيبراني

رمز الدورة: IT12830 تاريخ الإنعقاد: 13 - 17 يوليو 2026 دولة الإنعقاد: كوالالمبور (ماليزيا) - رسوم الإشتراك: 5775 Euro 

## مقدمة البرنامج

مع تزايد الاعتماد العالمي على التكنولوجيا، يزداد أيضًا خطر الهجمات الإلكترونية، مما يجعل تصميم معمارية أمن سيبراني فعّالة أمرًا بالغ الأهمية لحماية المؤسسات وبياناتها الحيوية.

تهدف هذه الدورة إلى تزويد المشاركين بالمعرفة والمهارات العملية اللازمة لتصميم وتنفيذ معمارية الأمن السيبراني بطريقة منهجية، تمكّنهم من مواجهة التهديدات الإلكترونية بفاعلية وتحقيق أعلى مستويات الحماية.

## أهداف البرنامج

بنهاية الدورة، سيكون المشاركون قادرين على:

1. فهم**مبادئ التصميم الأساسية**لمعمارية الأمن السيبراني.
2. تحليل**المخاطر الأمنية**وتقييمها بشكل منهجي.
3. تصميم**عناصر التحكم في الوصول**وحمايتها.
4. إنشاء**شبكات آمنة**وفق أفضل الممارسات.
5. تصميم**أنظمة الكشف عن التسلل ومنعها**.
6. تصميم**أنظمة الاستجابة للحوادث**بكفاءة.
7. تصميم**أنظمة إدارة الهوية والوصول**.
8. تصميم**أنظمة إدارة التشفير**وتأمين البيانات.
9. تطبيق**أفضل الممارسات العالمية**في معمارية الأمن السيبراني.
10. مواكبة**أحدث الاتجاهات والتقنيات**في تصميم المعمارية الأمنية.

## الفئات المستهدفة

- مهندسو الأمن السيبراني.
- مهندسو الشبكات.
- مسؤولو أنظمة المعلومات.
- مدراء تكنولوجيا المعلومات.
- أي محترف يسعى لتصميم وتنفيذ معمارية أمن سيبراني فعّالة.

## الكفاءات المكتسبة

بعد إتمام الدورة، سيتمكن المشاركون من:

- تصميم وتنفيذ معمارية الأمن السيبراني المتكاملة.
- حماية المؤسسات من التهديدات والهجمات الإلكترونية.
- تحسين مهاراتهم في مجال الأمن السيبراني العملي.
- الحصول على شهادة معتمدة في تصميم معمارية الأمن السيبراني.

## محاور البرنامج

### اليوم الأول: أساسيات الأمن السيبراني

- مقدمة شاملة في الأمن السيبراني.
- مبادئ التصميم في معمارية الأمن السيبراني.
- النماذج الشائعة لمعمارية الأمن السيبراني.
- تحليل المخاطر وتقييمها.

### اليوم الثاني: التحكم في الوصول والأمان الشبكي

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

### اليوم الثالث: إدارة الهوية والتشفير

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

### اليوم الرابع: التطبيقات العملية ودراسة الحالات

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

### اليوم الخامس: التقييم والختام

- اختبارات تقييمية للمهارات المكتسبة.
- مراجعة شاملة لمحتوى الدورة.
- توزيع الشهادات المعتمدة.