

# هندسة أمن الشبكات القائمة على مبدأ انعدام الثقة

8 - 12 فبراير 2027

برشلونة (إسبانيا)

UK Traininig

# PARTNER



## هندسة أمن الشبكات القائمة على مبدأ انعدام الثقة

المرجع: 336958\_3255273 التاريخ: 8 - 12 فبراير 2027 المكان: برشلونة (إسبانيا) الرسوم: GBP 5900

### مقدمة

في ظل ازدياد التهديدات السيبرانية وتطور أساليب الهجمات الرقمية، لم تعد الأنظمة الأمنية التقليدية القائمة على الثقة داخل الشبكات كافية لحماية البنى التحتية للمؤسسات. هنا يظهر مفهوم هندسة أمن الشبكات المعمارية القائمة على مبدأ انعدام الثقة كأحد أكثر النماذج تطوراً وفعالية في إدارة الأمن السيبراني.

يرتكز هذا النموذج على مبدأ أساسي هو "عدم الثقة بأي كيان سواء داخل الشبكة أو خارجها"، حيث تُمنح الصلاحيات فقط بناءً على تحقق الهوية والتحكم الدقيق في الوصول. تسعى هذه الدورة إلى تزويد المشاركين بفهم شامل لمفاهيم هندسة انعدام الثقة، وآليات تنفيذها، وأفضل الممارسات لتطبيقها في بيئات العمل الحديثة.

تهدف الدورة إلى تطوير القدرات التحليلية والعملية لدى المهنيين في مجال الأمن السيبراني، من خلال منهج تطبيقي يربط بين المفاهيم النظرية وحلول الحماية الفعلية في المؤسسات.

### أهداف الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- فهم الأسس النظرية لمبدأ انعدام الثقة في الأمن السيبراني.
- تحليل نقاط الضعف في الأنظمة التقليدية ومقارنتها بهندسة انعدام الثقة.
- تصميم بنية أمنية متكاملة تعتمد على التحقق المستمر والحد الأدنى من الصلاحيات.
- تطبيق تقنيات المصادقة متعددة العوامل وإدارة الهوية والوصول.
- تنفيذ سياسات التحكم في حركة البيانات داخل الشبكات السحابية والهجينة.
- استخدام أدوات المراقبة والتحليل للكشف عن التهديدات في الوقت الفعلي.
- تطوير خطة انتقال تدريجية لتبني نموذج انعدام الثقة ضمن المؤسسة.

UK Traininig

**PARTNER**



## مهاور الءورة

### اليوم الأول: مءءل إلى ھنءسة انءءام الثقة

- المفهوم العام لانءءام الثقة وأسباب ظهوره في الأمن السيبراني.
- مقارنة بين أمن الشبكات التقليءي ونموء انءءام الثقة.
- المبادئ الأساسية: التحقق المستمر، التحكم في الوصول، التقسيم الءقيق للشبكة.
- البنية التحتية التقنية الءاعمة للنموء.
- آءءيات التطبيق في المؤسسات ذات الأنظمة القءيمة.

### اليوم الثاني: إءارة الهوية والتحقق من المستخدمين

- ءور الهوية الرقمية في تطبيق انءءام الثقة.
- المصادقة متعددة العوامل وأهميتها في الحماية.
- إءارة الوصول القائمة على الءور والسياسات الءيناميكية.
- التحكم في الأجهزة المصرء لها بالءءول إلى الشبكة.
- بناء بيئة مصادقة موءءة في الأنظمة السحابية والهئية.

### اليوم الثالث: التقسيم الشبكي والتحكم في حركة البيانات

- تصميم الشبكات الءقيقة Micro-Segmentation وتقليل مخاطر الاختراق.
- مراقبة حركة البيانات والتحقق من الأنشطة المشبوءة.
- تطبيق سياسات "الأقل صلاحية" في بيئة العمل.
- حماية البيانات أثناء النقل والتخزين باستخدام التشفير.
- آليات الاستجابة الفورية عند اكتشاف محاولات غير مصرء بها.

### اليوم الرابع: الرؤية والتحليل الأمني المتقدم

- استخدام أءوات التحليل للكشف المبكر عن التهءءات.
- ءور الءكاء الاصطناعي في ءعم قرارات الأمن السيبراني.
- ءمء أنظمة المراقبة والسياسات الأمنية في منصة واءءة.
- إءارة التنبيهات وتءءء أولويات الاستجابة.
- التحليل الجنائي للءواءء وتوثيقها لتحسين البنية الأمنية.

UK Traininig

**PARTNER**



## اليوم الخامس: التنفيذ العملي والاستراتيجية المؤسسية

- تطوير خارطة طريق لتطبيق نموذج انعدام الثقة.
- مراحل الانتقال من الأنظمة التقليدية إلى الأنظمة الحديثة.
- دمج النموذج مع سياسات الحوكمة المؤسسية وإدارة المخاطر.
- اختبار الأداء الأمني وتقييم كفاءة النظام الجديد.
- إعداد خطط استمرارية الأعمال واستعادة الأنظمة بعد الهجمات.

## لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب معرفة معمقة بمفهوم انعدام الثقة وأحدث تقنيات الأمان السبراني.
- تطوير القدرة على تصميم وتنفيذ بنى أمنية متقدمة للمؤسسات.
- تعلم كيفية اكتشاف التهديدات مبكراً وتقليل فرص الاختراق.
- تعزيز مهارات إدارة الهوية والتحكم في الصلاحيات الرقمية.
- فهم كيفية حماية البيانات في البيئات السحابية والهجينة.
- تطبيق أدوات التحليل الأمني والاستجابة الفورية للحوادث.
- تحسين كفاءة أنظمة الأمن وتقليل التكاليف التشغيلية طويلة الأمد.
- بناء ثقافة مؤسسية قائمة على الثقة الصفرة لحماية الأصول الرقمية.

## الخاتمة

تعد هندسة أمن الشبكات القائمة على مبدأ انعدام الثقة تحولاً جذرياً في منهجية إدارة الأمن السبراني، فهي لا تركز فقط على الحماية من الخارج، بل تعيد تعريف مفهوم الأمان داخل المؤسسات ذاتها. من خلال تطبيق هذا النموذج، يمكن بناء بيئة رقمية آمنة ومرنة قادرة على التصدي للتحديات المعقدة التي تفرضها الهجمات الإلكترونية الحديثة.

تزود هذه الدورة المشاركين بفهم متكامل لكيفية تصميم وتطبيق هذا النموذج بفعالية، مما يضمن للمؤسسات تحقيق توازن بين الأمان، الأداء، والمرونة التشغيلية. ومع تزايد الاعتماد على الأنظمة الرقمية والسحابة، يصبح تبني مبدأ انعدام الثقة ضرورة استراتيجية وليست خياراً تقنياً فقط.

UK Training

**PARTNER**

