

أمن التطوير السحابي المتكامل وسلامة خطوط التكامل والتسليم المستمر

2027 مايو 17 – 21

دوسلدورف (ألمانيا)

UK Traininig

PARTNER



أمن التطوير السحابي المتكامل وسلامة خطوط التكامل والتسليم المستمر

المرجع: 201760_3255281 التاريخ: 17 - 21 مايو 2027 المكان: دوسلدورف (ألمانيا) الرسوم: GBP 5900

مقدمة

في عالم التكنولوجيا الحديث، لم يعد الأمن السيبراني مسؤولية فرق متخصصة فقط، بل أصبح جزءًا لا يتجزأ من دورة التطوير بأكملها. ومع الانتقال المتزايد إلى الحوسبة السحابية، برز مفهوم التطوير والأمن والتشغيل المتكامل الذي يجمع بين فرق البرمجة والأمن والبنية التحتية ضمن منظومة واحدة تهدف إلى بناء أنظمة أكثر أمانًا واستقرارًا.

تهدف هذه الدورة إلى تزويد المشاركين بفهم شامل لكيفية دمج ممارسات الأمان في كل مراحل التطوير والتشغيل السحابي، مع التركيز على حماية خطوط التكامل والتسليم المستمر من المخاطر والهجمات السيبرانية.

تمنح الدورة المتدربين القدرة على تصميم بيئات تطوير آمنة، وتطبيق استراتيجيات وقائية متقدمة، وضمان الامتثال للمعايير العالمية في الأمن السحابي.

أهداف الدورة

- التعرف على المفاهيم الأساسية للتطوير والأمن والتشغيل المتكامل في البيئات السحابية.
- فهم مكونات وأهمية خطوط التكامل والتسليم المستمر وأمنها.
- تطبيق أفضل الممارسات في دمج الأمان داخل دورة التطوير منذ المراحل الأولى.
- اكتساب مهارات تحليل المخاطر والثغرات في الأنظمة السحابية.
- تصميم استراتيجيات أمنية متكاملة لحماية البنية التحتية السحابية.
- استخدام أدوات وآليات الأتمتة لمراقبة الامتثال الأمني والتحقق من سلامة الكود البرمجي.
- تطوير خطط استجابة فعالة للحوادث الأمنية ضمن بيئة التطوير المستمر.
- تعزيز التعاون بين فرق البرمجة والأمن والتشغيل لضمان بيئة إنتاج آمنة ومستقرة.

UK Training

PARTNER



محاور الدورة

اليوم الأول: أساسيات الأمن في البيئات السحابية

- مقدمة حول مفاهيم الأمن السحابي وأهميته في العصر الرقمي.
- المبادئ الأساسية للتطوير والأمن والتشغيل المتكامل.
- الفرق بين الأساليب التقليدية والحديثة في إدارة الأمان.
- التعرف على التهديدات الشائعة في البيئات السحابية.
- فهم دورة حياة الكود الآمن من الإنشاء إلى النشر.
- دراسة حالات عملية توضح كيفية دمج الأمان في المشاريع السحابية.

اليوم الثاني: هندسة خطوط التكامل والتسليم المستمر

- التعريف بمفهوم خطوط التكامل والتسليم المستمر وأهميتها.
- مكونات البنية التحتية لخطوط التطوير الآمن.
- كيفية تحديد النقاط الحرجة التي تحتاج إلى حماية إضافية.
- أدوات إدارة الإصدارات والاختبار التلقائي ضمن الخطوط.
- تحليل التحديات الأمنية في مراحل الدمج والنشر.
- تطبيق نموذج أمان شامل يغطي دورة التطوير بأكملها.

اليوم الثالث: الأتمتة والأدوات الأمنية في بيئة التطوير

- مقدمة حول دور الأتمتة في تعزيز الأمن وتقليل الأخطاء البشرية.
- كيفية استخدام أدوات المسح الأمني الآلي للكشف عن الثغرات.
- بناء خطوط تحقق أمني تلقائي ضمن مراحل التطوير.
- دمج تقنيات المراقبة الذكية والتنبيه المبكر في بيئة العمل.
- إدارة مفاتيح الوصول والتوثيق المتقدم في الأنظمة السحابية.
- تدريب عملي على استخدام أدوات الأمان ضمن دورة التطوير المستمر.

UK Traininig

PARTNER



اليوم الرابع: حماية البنية التحتية والتطبيقات السحابية

- استراتيجيات متقدمة لتأمين البنية التحتية السحابية.
- التحكم في الصلاحيات وإدارة الهويات الرقمية.
- تأمين واجهات البرمجة وقواعد البيانات ضمن بيئة التطوير.
- تقنيات العزل بين البيئات المختلفة لمنع تسرب البيانات.
- التعامل مع نقاط الضعف في الحاويات والأنظمة الموزعة.
- وضع سياسات أمنية فعالة تتوافق مع المعايير العالمية.

اليوم الخامس: اختبار الأمان والاستجابة للحوادث

- منهجيات اختبار الأمان في خطوات التطوير السحابية.
- تقنيات التحقق من الامتثال الأمني للأنظمة والتطبيقات.
- تحليل نتائج الاختبارات واستخلاص الدروس التحسينية.
- بناء خطة متكاملة للاستجابة للحوادث الأمنية.
- توثيق الإجراءات والسياسات الأمنية بشكل منهجي.
- تقييم شامل للدورة وربط المفاهيم النظرية بالتطبيق العملي.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- اكتساب فهم عميق لآليات الأمان في بيئات التطوير السحابية.
- تعلم كيفية حماية خطوات التطوير من الهجمات السيبرانية.
- تطوير مهارات عملية في إدارة الأمان ضمن بيئة متكاملة.
- تحسين كفاءة فرق العمل من خلال تطبيق ممارسات الأتمتة الأمنية.
- ضمان الامتثال للمعايير والسياسات التنظيمية المعتمدة.
- تعزيز القدرات القيادية في اتخاذ قرارات أمنية استراتيجية.
- تقليل تكاليف المخاطر من خلال الوقاية المبكرة.
- الاستعداد للتعامل مع أي حادث أمني بسرعة وفعالية.

الخاتمة

يمثل دمج الأمان في دورة التطوير السحابي خطوة استراتيجية نحو بناء مؤسسات رقمية أكثر مرونة واستقرارًا. ومع التوسع في الاعتماد على الخدمات السحابية، أصبح ضمان سلامة خطوات التكامل والتسليم المستمر عنصرًا حاسمًا للحفاظ على موثوقية

الأنظمة وجودة الخدمات

UK Training

PARTNER



تقدم هذه الدورة للمشاركين المعرفة والأدوات التي يحتاجونها لتطبيق ممارسات الأمان المتكاملة بفعالية، مما يعزز من قدرتهم على إدارة المخاطر السيبرانية وتحقيق التميز التشغيلي.

إن الاستثمار في تطوير القدرات الأمنية ضمن بيئة التطوير الحديثة لم يعد خياراً، بل أصبح ضرورة لضمان استدامة الأعمال وحماية البيانات الحساسة من أي تهديدات محتملة.

UK Traininig

PARTNER

