BLACKBIRD FOR TRAINING

# تدريب البرمجة الآمنة: التطوير والقيادة التقنية

October 2027 14 – 10

دبي (الإمارات العربية المتحدة)



# تدريب البرمجة الآمنة: التطوير والقيادة التقنية

**المرجع:** 326125_3254928 **التاريخ:** 10 – 14 October 2027 **المكان:** دبي (الإمارات العربية المتحدة) **الرسوم:** GBP 4900

## مقدمة

في عالم يتزايد فيه الاعتماد على البرمجيات والتطبيقات الرقمية، أصبحت البرمجة الآمنة Secure Code Training ضرورية لحماية الأنظمة والبيانات الحساسة.

تواجه المؤسسات الحكومية والخاصة في منطقة الشرق الأوسط وشمال أفريقيا تحديات متنامية في الحفاظ على أمن برمجياتها، مما يتطلب من قادة الفرق والمديرين التنفيذيين والمتخصصين تطوير مهارات عملية تواكب أحدث الاتجاهات والممارسات.

يستهدف هذا البرنامج التدريبي جميع المستويات الوظيفية - من الموظفين المبتدئين الساعين لبناء قاعدة معرفية قوية، إلى المديرين التنفيذيين الذين يركزون على استراتيجيات حماية البيانات وأمن البرمجيات.

سيساعدك هذا المقال في التعرف على أهمية Secure Code Training، وفوائده العملية، إضافة إلى عرض شامل لأهداف الدورة، ومحاورها اليومية، والتحديات التي قد تواجهها المؤسسات عند تطبيق هذه الممارسات.

تابع القراءة لاكتشاف كيف يمكن لهذا البرنامج أن يعزز من قدراتك وكفاءاتك في بناء برمجيات آمنة تدعم الأداء المؤسسي والإنتاجية.

## أهداف الدورة

- فهم أساسيات البرمجة الآمنة وأهميتها في السياق المؤسسي.
- التعرف على أبرز التهديدات والثغرات الأمنية في البرمجيات.
- تعلم كيفية كتابة كود آمن باستخدام أفضل الممارسات الحديثة.
- تطبيق الأدوات والتقنيات الموثوقة لاكتشاف الثغرات وإصلاحها.
- تطوير السياسات والإجراءات اللازمة لحماية البرمجيات والأنظمة.
- تعزيز قدرات التحليل الأمني والتعامل مع حالات الاختراق.
- اكتساب مهارات القيادة التقنية لبناء ثقافة البرمجة الآمنة في المؤسسة.
- توظيف البرمجة الآمنة لتعزيز سمعة المؤسسة وضمان الامتثال للمعايير الدولية.



## محاور الدورة

**اليوم الأول: مقدمة في البرمجة الآمنة**

- التعريف بمفهوم البرمجة الآمنة وأهميتها في المؤسسات.
- مناقشة العلاقة بين أمن البرمجيات وإدارة المخاطر المؤسسية.
- عرض أمثلة لحوادث اختراقات شهيرة بسبب كود غير آمن.
- توضيح أهم المفاهيم والمصطلحات المتعلقة بالبرمجة الآمنة.
- مناقشة التوجهات العالمية في كتابة كود آمن ومستدام.
- شرح دور البرمجة الآمنة في الامتثال للتشريعات المحلية والدولية.

### اليوم الثاني: التهديدات والثغرات الأمنية الشائعة

- تحليل أبرز الثغرات الأمنية مثل SQL Injection, XSS.
- فهم كيفية استغلال الثغرات الأمنية في البرمجيات.
- مناقشة المخاطر المرتبطة بضعف الكود داخل المؤسسات.
- التعرف على تأثير الثغرات الأمنية على سمعة المؤسسة.
- دراسة حالات عملية توضح آثار الهجمات الإلكترونية.
- تقديم نصائح أولية للحد من هذه التهديدات.

### اليوم الثالث: مبادئ كتابة الكود الآمن

- استعراض أفضل الممارسات العالمية في كتابة الكود.
- تعلم كيفية التعامل مع مدخلات المستخدم بأمان.
- مناقشة أساليب التحقق من صحة البيانات وتطهيرها.
- كتابة تعليمات برمجية تتوافق مع معايير الأمان الحديثة.
- التركيز على تقنيات التحكم في الوصول والتصاريح.
- تدريب عملي على أمثلة لكتابة كود آمن وتدقيقه.



## اليوم الرابع: الأدوات والتقنيات المساعدة

- التعرف على أدوات كشف الثغرات وتحليل الكود مثل SAST, DAST.
- مناقشة برامج التدقيق الآلي للكود وتكاملها مع دورة التطوير.
- استعراض حلول التشفير وحماية البيانات المضمنة.
- التعرف على تقنيات التحقق المستمر للأمان أثناء التطوير.
- دراسة كيفية دمج الأدوات الأمنية في بيئة DevOps.
- عرض أمثلة عملية لاستخدام هذه الأدوات في مشاريع حقيقية.

## اليوم الخامس: التقييم والتطبيق العملي

- تلخيص مفاهيم وأهداف الدورة وتوضيح سياقها التطبيقي.
- مناقشة استراتيجيات تقييم أمان الكود داخل المؤسسات.
- تقديم اختبارات عملية لتقييم مدى فهم المتدربين.
- عرض نماذج لتقييم جاهزية المؤسسة لتبني البرمجة الآمنة.
- تقديم إرشادات لوضع خطة عمل لتحسين أمان البرمجيات.
- مناقشة خطط التحسين المستمر وتعزيز ثقافة البرمجة الآمنة.

## لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات

- اكتساب فهم شامل لمفاهيم البرمجة الآمنة.
- تطوير مهارات عملية قابلة للتطبيق الفوري في العمل.
- تعلم كيفية إدارة الثغرات الأمنية وتقليل المخاطر الرقمية.
- تعزيز فرصك المهنية من خلال شهادات معتمدة.
- دعم استراتيجية المؤسسة في الامتثال وحماية البيانات.
- بناء قدرات قيادية لتطوير ثقافة الأمان في فرق العمل.
- الاطلاع على أحدث الأدوات والتقنيات الموثوقة.
- تحسين الأداء المؤسسي من خلال برمجيات أكثر أمانًا.



## الخاتمة

تُعد البرمجة الآمنة Secure Code Training من الركائز الأساسية لحماية المؤسسات من المخاطر الرقمية وضمان استدامة الأداء المؤسسي.

من خلال هذه الدورة، ستتمكن من اكتساب معرفة شاملة ومهارات عملية لتطوير برمجيات أكثر أمانًا.

يساعدك هذا التدريب على تحويل الأفكار النظرية إلى تطبيقات عملية تحمي الأنظمة من التهديدات الأمنية.

كما يزودك بأحدث الأدوات والتقنيات التي تعزز قدرتك على التكيف مع متطلبات السوق والتشريعات التنظيمية.

لا تقتصر فائدة هذا البرنامج على الحماية التقنية، بل تشمل بناء قدرات قيادية تمكنك من ترسيخ ثقافة الأمان والامتثال داخل مؤسستك.

**ابدأ اليوم في بناء مستقبل مهني مستدام وقادر على مواجهة التحديات الرقمية بثقة وفعالية.**

