الدورة التدريبية: أمن التطبيقات وتطوير البرمجيات الآمنة المتقدم (Secure SDLC)



14 - 18 ديسمبر 2026
كوالالمبور
5200 € (للشخص الواحد)
Ref: #SM4278_340809

مقدمة الدورة التدريبية / لمحة عامة:

في عالم يعتمد بشكل متزايد على التطبيقات والبرمجيات، أصبح أمن التطبيقات وتطوير البرمجيات الآمنة (Secure SDLC) المتقدم ضرورة قصوى لحماية الشركات من الثغرات والهجمات السيبرانية. تتطلب عمليات تطوير البرمجيات الحديثة دمج الأمن في كل مرحلة من مراحل دورة حياة التطوير، بدءًا من التصميم وحتى النشر والصيانة. هذه الدورة التدريبية الشاملة مصممة لتزويد المطورين، مهندسي الأمن، ومديري المشاريع بالمعرفة والمهارات المتقدمة اللازمة لتصميم، تطوير، واختبار تطبيقات آمنة. سنتعمق في تحليل التهديدات، كتابة تعليمات برمجية آمنة، اختبار الاختراق للتطبيقات، وإدارة الثغرات الأمنية خلال دورة حياة تطوير البرمجيات الآمنة. تستند الدورة إلى أعمال خبراء أكاديميين بارزين في مجال أمن التطبيقات وهندسة البرمجيات، مثل البروفيسور Gary McGraw Gary McGraw، الذي يُعد رائدًا في مجال بناء البرمجيات الآمنة. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين المهنيين من تطوير تطبيقات قوية ومحمية، وتقليل المخاطر الأمنية، وضمان جودة البرمجيات. سيركز التدريب على الجوانب التطبيقية والعملية، مع تقديم دراسات حالة واقعية وتمارين محاكاة، لمساعدة المشاركين على تطبيق المفاهيم النظرية في بيئات عملهم الحقيقية، وتعزيز قدراتهم على بناء حلول برمجية آمنة بفعالية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مطورون البرمجيات.
- مهندسو أمن التطبيقات.
- مهندسو DevOps/Descopes.
- مديرو المشاريع التقنية.
- مدققو الأمن.
- مهندسو ضمان الجودة (QA).
- مختبرو الاختراق (Penetration Testers).

القطاعات والصناعات المستهدفة:

- شركات تطوير البرمجيات.
- شركات تقنية المعلومات.
- القطاع المصرفي والمالي.
- القطاع الحكومي.
- شركات التجارة الإلكترونية.
- شركات الاتصالات.
- أي مؤسسة تقوم بتطوير أو استخدام تطبيقات برمجية.

الأقسام المؤسسية المستهدفة:

- قسم تطوير البرمجيات.
- إدارة أمن المعلومات.
- قسم العمليات (Operations).
- إدارة الجودة.
- قسم التدقيق الداخلي.
- إدارة المخاطر.
- الاستراتيجية التقنية.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم مبادئ دورة حياة تطوير البرمجيات الآمنة (Secure SDLC).
- تحديد وتحليل التهديدات الأمنية في مراحل التطوير المختلفة.
- تطبيق أفضل الممارسات لكتابة تعليمات برمجية آمنة (Secure Coding).
- إجراء اختبارات أمن التطبيقات (SAST, DAST, IAST).
- إدارة الثغرات الأمنية ومعالجتها بفعالية.
- دمج أدوات وأتمتة الأمن في مسار التطوير (CI/CD).
- فهم معايير أمن التطبيقات (مثل OWASP Top 10).
- بناء ثقافة أمنية قوية داخل فرق التطوير.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وعملية مكثفة، تهدف إلى بناء قدرات احترافية في مجال أمن التطبيقات وتطوير البرمجيات الآمنة (Secure SDLC) المتقدم. تبدأ المنهجية بمحاضرات متعمقة يقدمها خبراء متخصصون في أمن التطبيقات وهندسة البرمجيات، يليها جلسات نقاش حيوية لتبادل الخبرات والتحديات في دمج الأمن ضمن دورة حياة التطوير. تركز الدورة بشكل كبير على دراسات الحالة الواقعية، حيث يقوم المشاركون بتحليل ثغرات أمنية في تطبيقات حقيقية، وتصميم حلول دفاعية، وتطوير استراتيجيات للتشفير والتحقق. تتضمن المنهجية ورش عمل تطبيقية ومختبرات افتراضية، تتيح للمتدربين كتابة تعليمات برمجية آمنة، وإجراء اختبارات اختراق للتطبيقات، واستخدام أدوات تحليل الشفرة المصدرية. يشجع BIG BEN Training Center العمل الجماعي والتعاون بين المتدربين لتعزيز التفكير النقدي وقدرات حل المشكلات الأمنية المعقدة في بيئة تطوير. يتم تقديم تغذية راجعة فردية ومستمرة لضمان تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مسلحون بالمعرفة والأدوات والخبرة العملية اللازمة لبناء وتأمين التطبيقات، مما يعزز مرونة المؤسسات وقدرتها على تقديم منتجات برمجية آمنة وموثوقة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة في دورة حياة تطوير البرمجيات الآمنة (Secure SDLC)

- مفاهيم أمن التطبيقات وأهميته.
- المراحل الأساسية لدورة حياة تطوير البرمجيات (SDLC).
- دمج الأمن في كل مرحلة من مراحل SDLC.
- تحليل التهديدات ونمذجة المخاطر (Threat Modeling).
- أهمية المتطلبات الأمنية في مرحلة التصميم.
- المعايير وأفضل الممارسات (OWASP Top 10، CWE/SANS Top 25).
- الفرق بين أمن البنية التحتية وأمن التطبيقات.

الوحدة الثانية: التصميم الآمن وكتابة التعليمات البرمجية الآمنة

- مبادئ التصميم الآمن للتطبيقات.
- معماريات الأمن (Security Architectures).
- ممارسات كتابة التعليمات البرمجية الآمنة (Secure Coding Practices).
- التعامل مع الإدخالات (Input Validation) ومنع الحقن (Injection Attacks).
- إدارة الأخطاء والاستثناءات (Error and Exception Handling).
- تأمين التشفير وإدارة المفاتيح.
- التعامل الآمن مع الجلسات (Session Management).

الوحدة الثالثة: اختبار أمن التطبيقات واكتشاف الثغرات

- أنواع اختبار أمن التطبيقات (SAST, DAST, IAST).
- تحليل الشفرة المصدرية الثابت (Static Application Security Testing).
- اختبار أمن التطبيقات الديناميكي (Dynamic Application Security Testing).
- اختبار الاختراق اليدوي والآلي للتطبيقات.
- التعامل مع الثغرات الشائعة (مثل XSS، CSRF).
- أدوات فحص الثغرات الأمنية في التطبيقات.
- أتمتة اختبار الأمن في مسارات CI/CD.

الوحدة الرابعة: إدارة الثغرات الأمنية والاستجابة للحوادث

- تصنيف الثغرات الأمنية وتحديد أولوياتها.
- عمليات التصحيح وإدارة الثغرات.
- الاستجابة لحوادث أمن التطبيقات.
- تحليل الأسباب الجذرية للثغرات.
- مراقبة أداء الأمن بعد التصحيح.
- بناء فريق استجابة لحوادث أمن التطبيقات.
- أهمية التغذية الراجعة المستمرة من الاختبارات.

الوحدة الخامسة: حوكمة أمن التطبيقات والتوجهات المستقبلية

- وضع سياسات ومعايير أمن التطبيقات.
- التوعية والتدريب الأمني للمطورين.
- مراجعة الكود (Code Review) من منظور أمني.
- أتمتة الأمن في دورة حياة التطوير (Descopes).
- أمن التطبيقات في السحابة والحاويات.
- تأمين واجهات برمجة التطبيقات (APIs).
- التوجهات المستقبلية في أمن التطبيقات (AI، ML).

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في ظل سرعة التغيير في التقنيات وتزايد تعقيد التطبيقات، كيف يمكن لفرق تطوير البرمجيات أن تدمج الأمن بشكل فعال في كل مرحلة من مراحل دورة الحياة، لضمان إنتاج برمجيات آمنة وموثوقة دون إعاقة وتيرة الابتكار؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتقدم والعملي على أمن التطبيقات وتطوير البرمجيات الآمنة (Secure SDLC) المتقدم، مما يميزها عن الدورات التي تقدم لمحة عامة فقط. نحن لا نكتفي بتقديم المفاهيم النظرية، بل نغوص في التطبيقات العملية من خلال ورش عمل مكثفة وتمارين مختبرية تحاكي سيناريوهات تطوير حقيقية، مما يمنح المشاركين خبرة مباشرة لا تقدر بثمن في بناء واختبار تطبيقات آمنة. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على اطلاع بأحدث التهديدات والحلول الأمنية وأفضل الممارسات في هذا المجال الحيوي. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا خبراء قادرين على دمج الأمن في كل مرحلة من مراحل تطوير البرمجيات، مما يعزز مرونة المؤسسات وقدرتها على تقديم منتجات برمجية عالية الجودة وآمنة.