



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

يونيو ٢٠٢٦ ٠٥ - ٠١

جينف

للشخص الواحد) € ٦٢٠٠

Ref: #SM4278_331444





لأ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

- (Secure SDLC) فهم مبادئ دورة حياة تطوير البرمجيات الآمنة
- المختلفة، تحديد وتحليل التهديدات الأمنية في مراحل التطوير
- (Secure Coding) تطبيق أفضل الممارسات لكتابة تعليمات برمجية آمنة
- (IAST) إجراء اختبارات أمن التطبيقات (SAST, DAST)
- 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:



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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):



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

- مفاهيم أمن التطبيقات وأهميته.
- ((SDLC)) المراحل الأساسية لدورة حياة تطوير البرمجيات
- دمج الأمن في كل مرحلة من مراحل ((SDLC))
- ((Modeling)) تحليل التهديدات ونمذجة المخاطر ((Threat))
- أهمية المتطلبات الأمنية في مرحلة التصميم.
- ((CWE/SANS Top ٢٥)) المعايير وأفضل الممارسات ((OWASP Top ١٠))
- الفرق بين أمن البنية التحتية وأمن التطبيقات.

البرمجية الآمنة الوحدة الثانية: التصميم الآمن وكتابة التعليمات

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

الثغرات الوحدة الثالثة: اختبار أمن التطبيقات واكتشاف



- أنواع اختبار أمن التطبيقات ((SAST, DAST, IAST))
- ((Security Testing) تحليل الشفرة المصدرية الثابت (Static Application))
- ((Application Security Testing) اختبار أمن التطبيقات الديناميكي (Dynamic))
- 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

للحوادث الوحدة الرابعة: إدارة الثغرات الأمنية والاستجابة

- 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.

المستقبلية الوحدة الخامسة: حوكمة أمن التطبيقات والتوجهات

- 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 ((ML/AI))



الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام، ساعة تدريبية، راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟



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