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

يونيو ٢٠٢٦ ٠٥ - ٠١

برشلونة - *

(للشخص الواحد) ٧٠٠ €

Ref: #SM4278_331431

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ 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

- 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 ١٠).
- 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 المصدرية. 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):

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 ١٠، CWE/SANS Top ٢٥).
- 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).
- الحقن (Injection Attacks) والتعامل مع الإدخالات (Input Validation) ومنع الثغرات.
- إدارة الأخطاء والاستثناءات (Error and Exception Handling).
- تأمين التشفير وإدارة المفاتيح.
- التعامل الآمن مع الجلسات (Session Management).

الوحدة الثالثة: اختبار أمن التطبيقات واكتشاف

- 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.

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 (AI، ML).

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 لمحة التطبيقات وتطوير البرمجيات الآمنة (Secure SDLC) تتميز هذه الدورة بتركيزها المتقدم والعملي 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 علىCenter الأكاديمي المتقدم، المقدم منBIG 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