الهندسية الدورة التدريبية: تطوير البرمجيات الآمنة: أفضل الممارسات للمبرمجين والفرق

مايو ٢٠٢٦ ٠٨ - ٠٤

الدار البيضاء

(للشخص الواحد) € ٤١٠٠

Ref: #CYB4024_564650

مقدمة الدورة التدريبية / لمحة عامة:

المخاطر الأمنية التي أنظمة رقمية موثوقة ومقاومة للتهديدات. فمع تزايد يمثل تطوير البرمجيات الآمنة حجر الزاوية في بناء لتضمين الأمن في كل مرحلة من تستهدف نقاط الضعف في الأكواد المصدرية، مما يستدعي تعقيد التطبيقات، تتصاعد لبناء المتخصصة للمبرمجين، مهندسي البرمجيات، ومديري دورة حياة التطوير. تقدم هذه الدورة التدريبية نهجًا استباقيًا المعماري للبرمجيات، أفضل برمجيات حصينة من البداية. سنتناول في هذه الدورة المشاريع، المعرفة والمهارات اللازمة سيكتسب المشاركون القدرة على تحديد الثغرات ممارسات الكود الآمن، وتقنيات اختبار الاختراق. مفاهيم الأمن في التصميم الدورة إلى بناء كوادر هندسية الفعالة للحوادث الأمنية التي قد تحدث في الأمنية، تطبيق ضوابط أمنية في الكود، والاستجابة والمخاطر الأمنية على المدى الطويل. يستند المحتوى قادرة على كتابة كود آمن، مما يقلل من التكاليف التطبيقات. تهدف البروفيسور غاري ماكغرو أمن التطبيقات، مع الاستفادة من إسهامات خبراء إلى أحدث المعايير الصناعية وأفضل الممارسات في هندسة الأمن واختبار أمن التطبيقات. يقدم BIG BEN ، المعروف بأعماله الرائدة في (Gary McGraw) أكاديميين بارزين مثل الهندسية من بناء منتجات برمجية آمنة وموثوقة. الدورة لتمكين الفرق هذه Training Center

لـ:↰ الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- المبرمجون ومطورو البرمجيات.↰
- مهندسو الأمن.↰
- مديرو المشاريع التقنية.↰
- مهندسو البنية التحتية والأنظمة.↰
- فريق ضمان الجودة.↰
- الفرق الهندسية في الشركات الناشئة والتقنية.↰

القطاعات والصناعات المستهدفة:↰

- شركات تطوير البرمجيات.↰
- القطاع المالي والتكنولوجي.↰
- شركات التجارة الإلكترونية.↰
- القطاع الحكومي والجهات الأمنية.↰
- شركات الاتصالات.↰
- المؤسسات التي تعتمد على تطبيقات داخلية.↰

الأقسام المؤسسية المستهدفة:↰

- إدارة تطوير البرمجيات.↰
- إدارة الأمن السيبراني.↰
- أقسام ضمان الجودة.↰
- إدارة المنتجات.↰
- إدارة البنية التحتية.↰

أهداف الدورة التدريبية:

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

- التطوير الآمن (SDLC). فهم مبادئ تطوير البرمجيات الآمنة ودورة حياة
- الكود. القدرة على تحديد الثغرات الأمنية الشائعة في
- تطبيق أفضل الممارسات لكتابة كود آمن وموثوق.
- (SAST/DAST). استخدام أدوات تحليل الكود الثابت والديناميكي
- (Top ١٠). تأمين التطبيقات ضد هجمات الويب الشائعة (OWASP
- إجراء اختبارات اختراق بسيطة على التطبيقات.
- والإنتاج. الاستجابة للحوادث الأمنية في مرحلة التطوير

منهجية الدورة التدريبية:

من خلال ورش مصممة لدمج مفاهيم الأمن السيبراني في عمل تعتمد هذه الدورة التدريبية منهجية عملية وتشاركية، ومحاكاة هجمات الاختراق، من العمل العملية، التي تتضمن تحليل كود ضعيف وإعادة المبرمجين اليومي. سيتمكن المتدربون مناقشات متعمقة حول هجمات سيبرانية حقيقية اكتساب خبرة مباشرة في تطوير برمجيات آمنة. تتضمن كتابته بشكل آمن، BIG التركيز على الجانب التطبيقي لأمن التطبيقات، من وكيف كان يمكن تجنبها من خلال التصميم الآمن. سيتم المنهجية مما يعزز الثقة في هذه الدورة لتمكين الفرق الهندسية من بناء Center التشفير إلى إدارة الجلسات. يقدم BEN Training العلامة التجارية. منتجات رقمية آمنة وموثوقة،

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

البرمجيات (SDLC) الوحدة الأولى: أساسيات الأمن في دورة حياة تطوير

- مقدمة إلى دورة حياة تطوير البرمجيات الآمنة (SDLC).
- التصميم الأمني والنمذجة الأمنية للتهديدات (Threat Modeling).
- مفاهيم الأمن الأساسية (OWASP Top ١٠).
- أهمية الأمن الاستباقي بدلاً من التفاعلي.
- الفرق بين أمن التطبيقات وأمن البنية التحتية.
- التوعية الأمنية للمطورين.
- الامتثال للوائح الأمنية في التطوير.

الوحدة الثانية: كتابة الكود الآمن (Secure Coding)

- أفضل الممارسات في كتابة كود آمن.
- التحقق من صحة المدخلات (Input Validation).
- التعامل الآمن مع الأخطاء والاستثناءات.
- أمن المصادقة والجلسات.
- التعامل مع البيانات الحساسة (التشفير والتجزئة).
- الحماية من هجمات الحقن (SQL, Command Injection).
- منع هجمات XSS وCSRF.

الشائعة الوحدة الثالثة: تأمين التطبيقات ضد هجمات الويب

- هجمات الحقن (Injection Attacks).
- هجمات البرمجة عبر المواقع (Cross-Site Scripting - XSS).
- هجمات تزوير الطلبات عبر المواقع (Cross-Site Request Forgery - CSRF).
- الثغرات في المصادقة وإدارة الجلسات.
- التحكم في الوصول المعطل (Broken Access Control).
- تأمين خوادم التطبيقات والويب.
- الحماية من الثغرات في التكوين.

الوحدة الرابعة: اختبار أمن التطبيقات (Application Security Testing)

- أنواع اختبار أمن التطبيقات.
- تحليل الكود الثابت (Static Analysis Security Testing - SAST).
- تحليل الكود الديناميكي (Dynamic Analysis Security Testing - DAST).
- اختبار الاختراق اليدوي.
- أتمتة اختبارات الأمان في خطوط التطوير (CI/CD).
- إدارة الثغرات الأمنية المكتشفة.
- التحليل الأمني للمكتبات والتبعيات (Dependencies).

الأمن الوحدة الخامسة: الاستجابة للحوادث وبناء ثقافة

- التطبيق.وضع خطة للاستجابة للحوادث الأمنية على مستوى
- اكتشاف الاختراقات والاستجابة السريعة لها.
- التحقيق الجنائي الرقمي في حوادث التطبيقات.
- بناء ثقافة أمنية قوية ضمن الفريق الهندسي.
- الأمن.التواصل مع الفرق الأخرى (Ops, Legal) بشأن
- مراجعة الكود الأمنية الجماعية.
- مستقبل تطوير البرمجيات الآمنة.

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 ٢٠-٢٥ 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:

تقتصر على معالجة كيف يمكن للمبرمجين والفرق الهندسية أن يبتكرون في ظل التطور المتسارع لـلغات البرمجة وأطر العمل، كود مرنة ومحصنة تضمن سلامة وأمان الثغرات المعروفة، بل تتوقع نقاط الضعف المستقبلية منهجيات تطوير برمجيات آمنة لا التطبيقات على المدى الطويل؟ وتُنشئ بنية

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

بدلاً من تناول تطوير البرمجيات الآمنة، مما يوفر محتوى مصمماً تتميز هذه الدورة بتركيزها المتخصص والعميق على تصميم الكود وحتى اختباره. الأمن السيبراني بشكل عام، نغوص في التطبيق العملي خصيصًا للمبرمجين والفرق الهندسية. وكتابة كود آمن، مما يمنح المشاركين خبرة عملية تقدم الدورة ورش عمل عملية تتضمن تحليل كود ضعيف لـأمن التطبيقات، من العملية الهندسية. إنها الأمن ودورة حياة التطوير (SDLC)، مما يضمن أن مباشرة في حماية منتجاتهم. نركز على الدمج بين يهدف إلى بناء مطورين قادرين على بناء برمجيات ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف الأمن جزء لا يتجزأ من آمنة، مما يقلل من المخاطر ويحمي سمعة المؤسسة.