لمعايير الصناعة الدورة التدريبية: أمن تطبيقات الويب المتقدم والامتثال

Ref: #IT4663

مقدمة الدورة التدريبية / لمحة عامة:

والشركاء. ومع تزايد المؤسسات في العصر الرقمي الحالي، حيث تُشكل واجهة تُعد تطبيقات الويب العصب الحيوي للعديد من تستهدفها، مما يستدعي فهمًا عميقًا الاعتماد على هذه التطبيقات، تتصاعد كذلك التهديدات تفاعل أساسية مع العملاء BIG BEN الصناعية. تقدم هذه الدورة التدريبية الشاملة من لمفاهيم أمن تطبيقات الويب ومعايير الامتثال الأمنية التي الأمنية الشائعة مثل حقن SQL الممارسات والتقنيات في تأمين تطبيقات الويب، بدءًا رؤى متعمقة حول أحدث Training Center تحليل آليات الحماية المتقدمة وتطبيق أفضل المعايير والبرمجة النصية عبر المواقع (XSS)، وصولا إلى من اكتشاف الثغرات فهم المتطلبات التنظيمية نقاط الضعف، وتطبيق التشفير الآمن، وإدارة الهوية الأمنية العالمية. سيتعلم المشاركون كيفية الأمن و .PCI DSS تركز الدورة على الجانب العملي OWASP Top ١٠ والامتثال لمعايير الصناعة مثل والوصول، بالإضافة إلى الذي يُعد رائدًا (J. Greenwood) السيبراني مثل البروفيسور دانييل جرينبيرغ (Daniel) والتطبيقي، مستلهمة من أفكار خبراء على معرفة شاملة ومتكاملة تمكنهم من بناء في مجال أمن المعلومات والقانون، مما يضمن حصول من جامعة هارفارد، المعاصرة إلى تزويد المشاركين بالأدوات والمهارات Center تطبيقات ويب آمنة وموثوقة. يهدف BIG BEN Training المتدربين بفعالية. اللازمة لمواجهة تحديات الأمن السيبراني

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو تطوير الويب ومبرمجو التطبيقات.
- متخصصو الأمن السيبراني ومديرو أمن المعلومات.
- مدققو الأنظمة والمخاطر.
- مسؤولو البنية التحتية لتكنولوجيا المعلومات.
- محللو ضمان الجودة واختبار الاختراق.
- مديرو المنتجات التقنية.
- مستشارو الامتثال التنظيمي.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- قطاع التكنولوجيا والاتصالات.
- القطاع الحكومي والهيئات التنظيمية.
- قطاع الرعاية الصحية.
- قطاع التجارة الإلكترونية والتجزئة.
- قطاع الطاقة والمرافق.
- شركات تطوير البرمجيات والاستشارات التقنية.

الأقسام المؤسسية المستهدفة:

- أقسام تطوير البرمجيات.
- أقسام الأمن السيبراني وامن المعلومات.
- أقسام الامتثال والمخاطر.
- أقسام تكنولوجيا المعلومات والبنية التحتية.
- أقسام التدقيق الداخلي والخارجي.
- أقسام إدارة المشاريع التقنية.

أهداف الدورة التدريبية:

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

- وكيفية استغلالها. فهم التهديدات الأمنية الشائعة لتطبيقات الويب
- لتطبيقات الويب. تطبيق أفضل الممارسات لتأمين الشيفرة المصدرية
- بفعالية. التعرف على آليات التشفير وإدارة المفاتيح وتطبيقها
- والتفويض الآمنة. إدارة الهوية والوصول وتكوين أنظمة المصادقة
- وتقنيات متقدمة. تحديد نقاط الضعف في تطبيقات الويب باستخدام أدوات
- والتعافي من الكوارث. تطوير استراتيجيات الاستجابة للحوادث الأمنية
- GDPR و PCI DSS و ٢٠١٠ الالتزام بمعايير الامتثال الدولية مثل OWASP Top
- المحتملة. تقييم أمان تطبيقات الويب وتحليل الثغرات الأمنية
- بناء تطبيقات ويب مرنة ومقاومة للهجمات السيبرانية.

منهجية الدورة التدريبية:

للمفاهيم تجمع بين الشرح النظري المتعمق والتطبيقات العملية تتبع هذه الدورة التدريبية منهجية تفاعلية وشاملة، في BIG BEN Training Center المعقدة وتحويلها إلى مهارات قابلة للتطبيق. يتميز المكثفة، لضمان استيعاب المتدربين فرصة لتحليل سيناريوهات حقيقية للهجمات الأمنية وكيفية بالتركيز على دراسات الحالة الواقعية، التي تُقدم أسلوب التدريب على التعاون وتبادل الأفكار، مما يعزز المشكلات واقتراح الحلول. تُشجع ورش العمل الجماعية معالجتها، مما يمنح المشاركين الأسئلة، مواجهة التحديات الأمنية. تُعد الجلسات التفاعلية الفهم الجماعي ويكشف عن وجهات نظر متعددة في المتدربين المدربين الخبراء. يتم استخدام أدوات والمناقشات المفتوحة، وتلقي التغذية الراجعة جزءًا أساسيًا من المنهجية، حيث تتيح طرح الشامل يُجهز المتدربين من ممارسة تقنيات الدفاع والهجوم بطريقة محاكاة بيئة الاختراق الأخلاقي، مما يمكن الفورية من الالتزام اللازمة لبناء وتأمين تطبيقات ويب قوية ضد المتدربين بالمعرفة النظرية والخبرة العملية آمنة ومتحكم بها. هذا النهج بمعايير الصناعة وأفضل الممارسات. التهديدات السيبرانية المتجددة، مع

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن تطبيقات الويب.

- فهم تحديات الأمن السيبراني لتطبيقات الويب.
- نموذج OWASP Top 10 والمخاطر الشائعة.
- مفاهيم المصادقة والتفويض وإدارة الجلسات.
- مبادئ البرمجة الآمنة والتشفير.
- أدوات وتقنيات اختبار أمان الويب.
- مقدمة عن معايير الامتثال الصناعي.
- بناء بيئة عمل آمنة لتطوير التطبيقات.

الوحدة الثانية: هجمات الويب الشائعة وتقنيات الدفاع

- حقن SQL وهجمات قواعد البيانات.
- البرمجة النصية عبر المواقع (XSS) والحماية منها.
- التزوير عبر طلبات المواقع (CSRF) ووسائل المنع.
- هجمات الاختراق وكسر المصادقة.
- هجمات التحميل والتلاعب بالملفات.
- الحماية من هجمات DDoS ورفض الخدمة.
- أفضل الممارسات لتكوين الخوادم الآمنة.

الوحدة الثالثة: التشفير وإدارة المفاتيح وأمن البيانات

- مبادئ التشفير المتماثل وغير المتماثل.
- التوقيعات الرقمية والشهادات الرقمية.
- إدارة مفاتيح التشفير وتخزينها الآمن.
- تأمين البيانات في أثناء النقل والتخزين.
- التعامل مع البيانات الحساسة وحمايتها.
- مفاهيم أمن السحابة لتطبيقات الويب.
- تأمين واجهات برمجة التطبيقات (APIs).

الصناعية. الوحدة الرابعة: الامتثال التنظيمي والمعايير

- معيار أمان بيانات صناعة بطاقات الدفع (PCI DSS).
- اللائحة العامة لحماية البيانات (GDPR).
- قانون نقل التأمين الصحي والمساءلة (HIPAA).
- معايير أيزو ٢٧٠٠١ لنظم إدارة أمن المعلومات.
- إجراء عمليات التدقيق الأمني والامتثال.
- وضع سياسات وإجراءات أمن المعلومات.
- الاستجابة للحوادث الأمنية والتعافي.

ومستقبلها. الوحدة الخامسة: تقييم أمان تطبيقات الويب

- الويب. اختبار الاختراق (Penetration Testing) لأمان
- تحليل الثغرات الأمنية وأدوات الفحص الآلي.
- تقييم المخاطر الأمنية ووضع خطط التخفيف.
- أمن تطبيقات الويب في بيئات DevOps.
- الذكاء الاصطناعي وتعلم الآلة في أمن الويب.
- مستقبل أمن تطبيقات الويب والتهديدات الناشئة.
- بناء ثقافة أمنية قوية داخل المؤسسة.

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:

إعاقة عملية النشر؟ السريع في تطوير تطبيقات الويب، وضرورة تطبيق أعلى كيف يمكن للمنظمات تحقيق التوازن بين الابتكار

معايير الأمن والامتثال دون

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

على التطبيق العملي والعميق، حيث لا تقتصر على تقديم المفاهيم النظرية تتميز هذه الدورة التدريبية بمنهجها الشامل في مجال أمن تطبيقات الويب. يقدمBIG BEN والرؤى المستنيرة المستقاة من أفضل الممارسات فحسب، بل تُركز بشكل مكثف التغطية السطحية للمواضيع، ليغوص في تفاصيل الهجمات محتوى أكاديميًا متطورًا يتجاوز Training Center العالمية ربط المفاهيم النظرية تعتمد الدورة على أمثلة عملية من واقع الصناعة، مما السيبرانية المعقدة وأساليب الدفاع المتقدمة. مما يُمكّن العمل. بدلاً من مجرد سرد الأدوات، تُركز الدورة بالتحديات الحقيقية التي يواجهونها في بيئات يساعد المتدربين على يضمن هذا النهج حصول المشاركين من اتخاذ قرارات مستنيرة وتطوير حلول على فهم فلسفة الأمن وراء كل تقنية، مرنة وآمنة، مع القدرة على تلبية المتطلبات المتدربين على فهم معمق لكيفية بناء تطبيقات ويب أمنية مبتكرة ومستدامة. لمؤسساتهم. يجعلهم خبراء في مجال حماية الأصول الرقمية التنظيمية الصارمة ومعايير الامتثال الصناعي، مما