الدورة التدريبية: أمن الشبكات والبيانات المتقدم: استراتيجيات الحماية والتصدي للتهديدات



26 - 30 اكتوبر 2026

بوسطن

7500 € (للشخص الواحد)

Ref: #NO9224_353147

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التزايد المستمر للتهديدات السيبرانية، أصبح أمن الشبكات والبيانات ليس مجرد خيار، بل ضرورة قصوى للمؤسسات للحفاظ على استمراريتها وسلامة أصولها الرقمية. تقدم هذه الدورة التدريبية الشاملة منهجًا متعمقًا في أحدث استراتيجيات حماية الشبكات وتأمين البيانات، بدءًا من فهم أنواع الهجمات السيبرانية وصولًا إلى تطبيق آليات الدفاع المتقدمة. يركز التدريب على تزويد المشاركين بالمهارات العملية والنظرية اللازمة لبناء منظومات دفاعية قوية وفعالة. يستعرض BIG BEN Training Center هذه المفاهيم بعمق، مستنيرًا بأعمال رواد المجال مثل البروفيسور روس أندرسون (Ross Anderson)، المعروف بإسهاماته البارزة في هندسة أمن المعلومات، مما يضمن تقديم محتوى أكاديمي وعملي رفيع المستوى. ستُمكن الدورة المتدربين من فهم كيفية تحليل المخاطر، تطبيق أفضل ممارسات أمن الشبكات، والتعامل مع الحوادث الأمنية بفعالية. يتعمق البرنامج في تفاصيل التشفير، أمن التطبيقات، أمن السحابة، وإدارة الثغرات لضمان أن يكون المتدرب جاهزًا لمواجهة التحديات الأمنية المعاصرة والمعقدة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديري أمن المعلومات.
- مهندسي أمن الشبكات.
- محللي الأمن السيبراني.
- مسؤولي تكنولوجيا المعلومات.
- المتخصصين في الامتثال والمخاطر.
- المدققين الأمنيين.
- المطورين المسؤولين عن أمن التطبيقات.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- شركات الاتصالات وتقنية المعلومات.
- الحكومة والدفاع.
- الرعاية الصحية.
- النفط والغاز والطاقة.
- التصنيع.
- قطاع التجزئة والتجارة الإلكترونية.

الأقسام المؤسسية المستهدفة:

- إدارة أمن المعلومات.
- قسم تكنولوجيا المعلومات.
- الامتثال وإدارة المخاطر.
- قسم العمليات الأمنية (SOC).
- قسم تطوير البرمجيات.
- قسم البنية التحتية.
- التدقيق الداخلي.

أهداف الدورة التدريبية:

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

- تحليل وتقييم المخاطر الأمنية للشبكات والبيانات.
- تصميم وتنفيذ حلول أمن الشبكات المتقدمة.
- تطبيق تقنيات التشفير لحماية البيانات.
- التعرف على أنواع الهجمات السيبرانية وسبل الوقاية منها.
- إدارة جدران الحماية وأنظمة كشف التسلل.
- وضع خطط الاستجابة للحوادث الأمنية.
- تطبيق أفضل ممارسات أمن البيانات.
- فهم أمن الحوسبة السحابية والتحديات المرتبطة بها.
- الالتزام بالمعايير التنظيمية لأمن المعلومات.
- إجراء تدقيقات أمنية وتقييمات للضعف.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وتطبيقية مكثفة، مصممة لتمكين المشاركين من اكتساب خبرة عملية في أمن الشبكات والبيانات. تبدأ كل وحدة بمحاضرات نظرية متعمقة تغطي المفاهيم الأساسية، تليها جلسات ورش عمل عملية تُطبق فيها التقنيات الأمنية على سيناريوهات واقعية. يتم استخدام دراسات حالة مستوحاة من هجمات سيبرانية حقيقية لمساعدة المشاركين على فهم كيفية تحليل التهديدات وتطبيق الدفاعات. يشجع BIG BEN Training Center على العمل الجماعي والمناقشات المفتوحة لتعزيز تبادل المعرفة والخبرات. تُقدم جلسات تغذية راجعة فردية وجماعية لضمان فهم عميق للمفاهيم وتطوير المهارات. تهدف المنهجية إلى تزويد المتدربين بالقدرة على تأمين البنية التحتية للشبكات، حماية البيانات الحساسة، والتعامل مع التهديدات السيبرانية بفعالية وثقة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن المعلومات ومفاهيم الشبكات

- مقدمة إلى أمن المعلومات والتهديدات السيبرانية.
- مبادئ أمن الشبكات الأساسية.
- مكونات الشبكة وتأثيرها على الأمن.
- نموذج OSI ومناطق الهجوم.
- مفاهيم التشفير وأمن البيانات.
- تحليل المخاطر الأمنية.
- القوانين واللوائح المتعلقة بأمن المعلومات.

الوحدة الثانية: تقنيات حماية الشبكات المتقدمة

- جدران الحماية (Firewalls) المتقدمة وتكوينها.
- أنظمة كشف ومنع التسلل (IDS/IPS).
- الشبكات الخاصة الافتراضية (VPN) وتأمين الاتصالات.
- إدارة نقاط الضعف وتصحيح الثغرات الأمنية.
- فحص المنافذ واكتشاف نقاط الضعف.
- بروتوكولات التوجيه الآمنة.
- مقدمة إلى أمن الشبكات اللاسلكية.

الوحدة الثالثة: أمن البيانات والتشفير

- مبادئ أمن البيانات.
- أنواع التشفير (Symmetric, Asymmetric, Hashing).
- إدارة المفاتيح والتصديقات الرقمية.
- أمن قواعد البيانات.
- أمن تخزين البيانات.
- التعافي من الكوارث والنسخ الاحتياطي للبيانات.
- حماية البيانات أثناء النقل (Data in Transit).

الوحدة الرابعة: أمن التطبيقات والحوسبة السحابية

- مقدمة إلى أمن التطبيقات.
- ثغرات الويب الشائعة (OWASP Top 10).
- أمن البرمجيات والتطوير الآمن.
- أمن الحوسبة السحابية (Cloud Security).
- نماذج أمن السحابة (IaaS, PaaS, SaaS).
- تحديات أمن البيانات في السحابة.
- أمن الحاويات والخدمات المصغرة.

الوحدة الخامسة: الاستجابة للحوادث الأمنية والتحقيق الجنائي الرقمي

- مراحل الاستجابة للحوادث الأمنية.
- أدوات تحليل الحوادث.
- التحقيق الجنائي الرقمي في الشبكات.
- جمع الأدلة الرقمية والحفاظ عليها.
- إدارة السجلات والتدقيق الأمني.
- التخطيط للتعافي من الكوارث.
- التحليل بعد الحادثة والدروس المستفادة.

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:

كيف يمكن للمؤسسات تحقيق التوازن الفعال بين تطبيق أقصى درجات أمن الشبكات والبيانات وضمان سهولة الوصول والمرونة التشغيلية دون إعاقة الابتكار أو تجربة المستخدم؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل على أمن الشبكات والبيانات من منظور متقدم وعملي، مما يجعلها مختلفة عن الدورات التي تقتصر على المفاهيم النظرية. يقدم BIG BEN Training Center منهجًا يجمع بين الأكاديمية التطبيقية والخبرة العملية، مع التركيز على التهديدات السيبرانية الحالية والناشئة. ما يميز هذه الدورة هو التركيز على كيفية بناء دفاعات قوية، إدارة الثغرات الأمنية، والتعامل مع الحوادث الأمنية بفعالية. يتم تزويد المشاركين بأدوات تحليل الأمن وأفضل الممارسات الصناعية، مما يمكنهم من تطبيق المعرفة المكتسبة فورًا في بيئات عملهم. الدورة ليست مجرد شرح للمفاهيم، بل هي تدريب عملي مكثف يهدف إلى بناء خبراء قادرين على تأمين البنية التحتية الرقمية بكفاءة ومرونة، وضمان استمرارية الأعمال في مواجهة التحديات السيبرانية المتزايدة.