الدورة التدريبية: أمن المعلومات السيبراني في أنظمة الاتصالات والشبكات المتقدمة للتهديدات الحديثة

26 - 30 اكتوبر 2026
لندن
5900 € (للشخص الواحد)
Ref: #TEL1272_357983

مقدمة الدورة التدريبية / لمحة عامة:

في عصر تتزايد فيه التهديدات السيبرانية وتتطور باستمرار، أصبح أمن المعلومات في أنظمة الاتصالات والشبكات ضرورة قصوى وليست مجرد رفاهية. مع التوسع الهائل في البنية التحتية الرقمية، من شبكات الجيل الخامس (5G) إلى إنترنت الأشياء (IoT)، تتزايد نقاط الضعف المحتملة التي يمكن استغلالها من قبل المهاجمين. هذه الدورة التدريبية الشاملة من BIG BEN Training Center صُممت لتزويد المشاركين بالمعرفة والمهارات المتقدمة اللازمة لحماية البيانات والأنظمة الحيوية من الهجمات السيبرانية. سيتعلم المتدربون كيفية تحديد التهديدات، وتقييم المخاطر، وتنفيذ حلول أمنية قوية تشمل التشفير، وأمن الشبكات، وإدارة الهوية، والاستجابة للحوادث. سيتم التركيز على أحدث التقنيات وأفضل الممارسات في مجال الأمن السيبراني المطبقة على أنظمة الاتصالات الحديثة. تُستلهم هذه الدورة من أعمال أكاديميين ورواد في مجال الأمن السيبراني مثل Bruce Schneier، مؤلف كتاب "Applied Cryptography"، الذي يُعد مرجعًا أساسيًا في مجال التشفير وأمن البيانات. يلتزم BIG BEN Training Center بتقديم تدريب يجمع بين المفاهيم النظرية المتعمقة والتطبيقات العملية الموجهة نحو سيناريوهات التهديدات الحالية والمستقبلية، مما يضمن أن يكون المشاركون مجهزين لمواجهة التحديات الأمنية المعقدة في بيئة الاتصالات الرقمية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- متخصصو الأمن السيبراني.
- مهندسو الشبكات والاتصالات.
- مدراء أمن المعلومات.
- مسؤولو الامتثال والمخاطر.
- محللو الأمن ومستشارو الأمن السيبراني.
- مدراء تكنولوجيا المعلومات.
- المهندسون الذين يعملون على تصميم وتطوير أنظمة الاتصالات.
- أي شخص معني بحماية الأصول الرقمية في بيئة الشبكات.

القطاعات والصناعات المستهدفة:

- شركات الاتصالات ومزودو خدمات الإنترنت.
- البنوك والمؤسسات المالية.
- القطاع الحكومي والدفاعي.
- شركات الأمن السيبراني والاستشارات الأمنية.
- قطاع الطاقة والمرافق الحيوية.
- شركات تطوير البرمجيات والمنصات الرقمية.
- قطاع الرعاية الصحية لحماية بيانات المرضى.
- شركات التصنيع التي تعتمد على الشبكات الذكية.

الأقسام المؤسسية المستهدفة:

- أقسام أمن المعلومات والسيبراني.
- إدارات تكنولوجيا المعلومات والشبكات.
- أقسام الامتثال والمراجعة الداخلية.
- أقسام إدارة المخاطر.
- فرق الاستجابة للحوادث الأمنية.
- أقسام الهندسة والتطوير.
- إدارات البنية التحتية.

أهداف الدورة التدريبية:

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

- فهم التهديدات السيبرانية المتقدمة ونقاط الضعف في أنظمة الاتصالات.
- تطبيق مبادئ التشفير وأمن البيانات لحماية المعلومات الحساسة.
- تصميم وتنفيذ استراتيجيات أمنية قوية للشبكات اللاسلكية والسلكية.
- إدارة الهوية والوصول بشكل فعال في بيئات الشبكات المعقدة.
- التعرف على هجمات الهندسة الاجتماعية وكيفية التخفيف منها.
- تنفيذ أنظمة كشف ومنع التسلل المتقدمة (IDS/IPS).
- تطوير خطط الاستجابة للحوادث الأمنية والتعافي من الكوارث.
- الامتثال للمعايير واللوائح الأمنية الدولية والمحلية (مثل ISO 27001).
- إجراء تقييمات المخاطر الأمنية واختبارات الاختراق.
- تأمين البنية التحتية السحابية والشبكات المعرفة بالبرمجيات (SDN).

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة منهجية تدريبية متعمقة وعملية، تجمع بين المعرفة النظرية المتطورة والتطبيقات العملية المكثفة. تبدأ الدورة بمراجعة شاملة للمفاهيم الأساسية لأمن المعلومات والتهديدات السيبرانية، ثم تنتقل إلى تحليل متقدم لدراسات الحالة الواقعية التي تُبرز الهجمات السيبرانية الحديثة على أنظمة الاتصالات والشبكات. سيُشارك المتدربون في ورش عمل عملية باستخدام أدوات ومحاكيات أمنية متقدمة، حيث سيقومون بتنفيذ سيناريوهات اختراق ودفاع، وتكوين حلول أمنية، وتحليل السجلات الأمنية. سيتم التركيز على الجانب العملي من خلال تمارين محاكاة الاختراق، والتحقيق الجنائي الرقمي، وتخطيط الاستجابة للحوادث. تشمل المنهجية مناقشات جماعية مكثفة لتعزيز التفكير النقدي وتبادل الخبرات بين المشاركين. يتم تقديم تغذية راجعة بناءة وفردية لضمان فهم عميق للمفاهيم وتنمية المهارات التطبيقية. يهدف BIG BEN Training Center إلى تمكين المشاركين من اكتساب الخبرة العملية اللازمة لحماية البنى التحتية للاتصالات والشبكات من أشد التهديدات السيبرانية تطورًا، مما يجعلهم خبراء مؤهلين في هذا المجال الحيوي.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن المعلومات السيبراني.

- مقدمة في الأمن السيبراني ومفاهيمه الأساسية.
- مبادئ حماية البيانات والخصوصية.
- التهديدات السيبرانية الشائعة وأنواع الهجمات.
- مفاهيم التشفير وأمن المعلومات.
- إدارة المخاطر والضعف.
- الأطر والمعايير الأمنية (مثل NIST, ISO 27001).
- أهمية الأمن السيبراني في أنظمة الاتصالات.

الوحدة الثانية: أمن الشبكات والاتصالات.

- تأمين البنية التحتية للشبكات (Wired/Wireless).
- بروتوكولات أمن الشبكات (IPSec, SSL/TLS).
- جدران الحماية وأنظمة كشف/منع التسلل (IDS/IPS).
- أمن الشبكات اللاسلكية (Wi-Fi, 5G).
- أمن إنترنت الأشياء (IoT) والتحكم الصناعي (ICS).
- الشبكات المعرفة بالبرمجيات (SDN) والأمن السحابي.
- أمن الاتصالات الصوتية والمرئية.

الوحدة الثالثة: إدارة الهوية والوصول والتشفير المتقدم.

- مفاهيم إدارة الهوية والوصول (IAM).
- المصادقة متعددة العوامل (MFA).
- أنظمة التحكم في الوصول (ACLs).
- التشفير المتماثل وغير المتماثل.
- البنية التحتية للمفاتيح العامة (PKI).
- التوقيعات الرقمية والشهادات.
- تشفير البيانات أثناء النقل والتخزين.

الوحدة الرابعة: تحليل البرمجيات الخبيثة والاستجابة للحوادث.

- أنواع البرمجيات الخبيثة (الفيروسات، الفدية، الديدان).
- أساليب تحليل البرمجيات الخبيثة.
- مفاهيم الاستجابة للحوادث الأمنية.
- خطوات الاستجابة للحوادث (الاكتشاف، الاحتواء، الاستئصال، التعافي).
- التحقيق الجنائي الرقمي وجمع الأدلة.
- أهمية التخطيط لاستمرارية الأعمال.
- محاكاة الهجمات واختبار الاختراق.

الوحدة الخامسة: التحديات المتقدمة والتوجهات المستقبلية.

- أمن الذكاء الاصطناعي وتعلم الآلة في الأمن السيبراني.
- أمن سلسلة الكتل (Blockchain) في الاتصالات.
- مفاهيم الأمن الكمومي.
- التهديدات السيبرانية الناشئة (Zero-day exploits).
- أمن الحوسبة السحابية المتقدمة.
- الوعي الأمني والتدريب البشري.
- التعاون الدولي في مكافحة الجرائم السيبرانية.

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:

مع التوسع الهائل في الرقمنة والترابط بين الأنظمة، كيف يمكن للمؤسسات تحقيق توازن فعال بين الانفتاح التكنولوجي الضروري للابتكار وبين الحفاظ على أقصى درجات الأمن السيبراني ضد التهديدات المتزايدة والمعقدة باستمرار؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الشامل والعميق على أمن المعلومات السيبراني المخصص لأنظمة الاتصالات والشبكات، مما يجعلها مختلفة عن الدورات العامة في الأمن السيبراني. نحن لا نكتفي بتقديم المفاهيم النظرية، بل نغوص في تفاصيل التطبيقات العملية والأمثلة الواقعية من قطاع الاتصالات، مثل تأمين شبكات الجيل الخامس (5G) وتطبيقات إنترنت الأشياء (IoT) الحرجة. نركز على استراتيجيات الدفاع في العمق، وإدارة المخاطر المتقدمة، وأساليب الاستجابة للحوادث المصممة خصيصًا لبيئات الاتصالات المعقدة. تتضمن الدورة ورش عمل مكثفة وتمارين محاكاة تحاكي سيناريوهات الهجمات الحقيقية على البنية التحتية للاتصالات، مما يمنح المشاركين خبرة عملية لا تقدر بثمن في اكتشاف التهديدات والتصدي لها. نحن نهدف إلى إعداد متخصصين قادرين على قيادة جهود الأمن السيبراني في مؤسساتهم، وحماية الأصول الرقمية الأكثر حساسية في عالم الاتصالات المتطور.