(IoT و 5Gالدورة التدريبية: تصميم وتأمين شبكات الاتصالات اللاسلكية المتقدمة (5

#TEL8727

الدورة التدريبية: تصميم وتأمين شبكات الاتصالات اللاسلكية المتقدمة (5G و IoT)

مقدمة الدورة التدريبية / لمحة عامة:

يشهد العالم ثورة في مجال الاتصالات اللاسلكية مع الانتشار المتزايد لشبكات الجيل الخامس (5G) وتطبيقات إنترنت الأشياء (IoT)، مما يفتح آفاقًا غير مسبوقة للابتكار والتواصل. ومع هذه التطورات تأتي تحديات كبيرة في تصميم وتأمين هذه الشبكات الحيوية، خاصة في سياق البنية التحتية الحرجة. هذه الدورة التدريبية من BIG BEN Training Center صُممت لتزويد المشاركين بالمعرفة والمهارات اللازمة لتصميم بنى تحتية لشبكات لاسلكية آمنة وفعالة، قادرة على دعم متطلبات 5G وIoT. ستغطي الدورة مفاهيم متقدمة في أمن الشبكات اللاسلكية، بدءًا من التشفير والمصادقة، مرورًا بحماية البيانات والخصوصية، وصولًا إلى استراتيجيات الاستجابة للحوادث السيبرانية. سيتعلم المتدربون كيفية تقييم المخاطر، وتنفيذ حلول أمنية قوية، وضمان الامتثال للمعايير الدولية. تُستلهم هذه الدورة من أعمال أكاديميين بارزين في مجال أمن الشبكات اللاسلكية، مثل William Stallings، مؤلف كتاب "Cryptography and Network Security: Principles and Practice"، الذي يعد مرجعًا أساسيًا في هذا المجال. يلتزم BIG BEN Training Center بتقديم تجربة تعليمية فريدة تجمع بين المفاهيم النظرية العميقة والتطبيقات العملية الموجهة نحو سيناريوهات العالم الحقيقي. سيتأهل المشاركون لتصميم وتأمين شبكات لاسلكية متطورة تلبي أعلى معايير الأداء والأمان في العصر الرقمي.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الشبكات والاتصالات.
- متخصصو الأمن السيبراني.
- مهندسو الحلول والمعماريون التقنيون.
- مديرو البنية التحتية لتكنولوجيا المعلومات.
- المطورون العاملون على تطبيقات IoT.
- الاستشاريون في مجال الاتصالات والأمن.
- التقنيون والفنيون المسؤولون عن نشر وصيانة الشبكات.
- صناع القرار في الشركات التي تعتمد على الشبكات اللاسلكية المتقدمة.

القطاعات والصناعات المستهدفة:

- قطاع الاتصالات ومزودو خدمات الجيل الخامس.
- شركات الأمن السيبراني.
- قطاع الطاقة والمرافق الذكية.
- شركات التصنيع الصناعي والتحول الرقمي.
- القطاع الحكومي والدفاعي.
- شركات النقل واللوجستيات التي تستخدم IoT.
- قطاع الرعاية الصحية لتطبيقات الرعاية عن بعد.
- البنوك والمؤسسات المالية لأمن البيانات.

الأقسام المؤسسية المستهدفة:

- أقسام أمن المعلومات.
- إدارات الشبكات والبنية التحتية.
- أقسام البحث والتطوير.
- فرق التشغيل والصيانة.
- أقسام تطوير المنتجات والخدمات.
- أقسام المخاطر والامتثال.
- إدارات التحول الرقمي.

أهداف الدورة التدريبية:

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

- تصميم بنية تحتية لشبكات 5G وIoT آمنة وفعالة.
- تحديد التهديدات ونقاط الضعف في الشبكات اللاسلكية المتقدمة.
- تطبيق بروتوكولات التشفير والمصادقة المتقدمة لحماية البيانات.
- فهم آليات تأمين أجهزة وحساسات إنترنت الأشياء.
- إدارة مخاطر الأمن السيبراني في بيئات الشبكات اللاسلكية.
- تنفيذ استراتيجيات الدفاع في العمق لحماية البنية التحتية.
- الاستجابة للحوادث الأمنية في شبكات 5G وIoT.
- الامتثال للمعايير واللوائح الأمنية الدولية والمحلية.
- تقييم أداء الشبكات اللاسلكية من منظور أمني.
- تطوير خطط استمرارية الأعمال للشبكات الحيوية.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة منهجية تدريبية متقدمة تركز على التطبيق العملي والتحليل العميق لتحديات تصميم وتأمين شبكات الاتصالات اللاسلكية المتقدمة. تبدأ الدورة بمراجعة للمفاهيم النظرية الأساسية لشبكات 5G وIoT، ثم تنتقل إلى دراسات حالة واقعية تُظهر التحديات الأمنية الشائعة وكيفية التعامل معها. سيشارك المتدربون في ورش عمل عملية مكثفة، تتضمن استخدام أدوات المحاكاة والمنصات الافتراضية لتصميم وتكوين شبكات آمنة، واختبار نقاط الضعف، وتنفيذ الدفاعات اللازمة. سيتم تحليل أمثلة من هجمات سيبرانية حقيقية على شبكات لاسلكية، مع التركيز على استراتيجيات الاكتشاف والاستجابة والتعافي. تشمل المنهجية مناقشات جماعية لتعزيز التفكير النقدي وتبادل الخبرات بين المشاركين. يتم تقديم تغذية راجعة فردية لضمان فهم عميق للمفاهيم وتنمية المهارات التطبيقية. يهدف BIG BEN Training Center إلى تمكين المشاركين من اكتساب خبرة عملية في تأمين البنى التحتية الحرجة لشبكات الجيل الخامس وإنترنت الأشياء، مما يؤهلهم لمواجهة التحديات الأمنية المعقدة في هذا المجال الحيوي.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات 5G وIoT وتحدياتها الأمنية.

- مقدمة في بنية شبكات 5G ومكوناتها.
- مفاهيم إنترنت الأشياء (IoT) وتطبيقاتها.
- نقاط الضعف الأمنية الشائعة في 5G وIoT.
- التهديدات والهجمات المحتملة على الشبكات اللاسلكية.
- أهمية أمن الشبكات في البنية التحتية الحرجة.
- مبادئ حماية البيانات والخصوصية في IoT.
- التشريعات والمعايير الأمنية ذات الصلة.

الوحدة الثانية: تصميم أمني لشبكات 5G.

- هندسة الأمن في شبكات 5G.
- بروتوكولات التشفير والمصادقة في 5G.
- تأمين واجهات شبكة 5G.
- حماية شرائح الشبكة (Network Slicing).
- أمن الحوسبة الطرفية (Edge Computing).
- إدارة الهوية والوصول في 5G.
- تأمين شبكات النفاذ اللاسلكية (RAN).

الوحدة الثالثة: تأمين أجهزة ومنصات IoT.

- مبادئ أمن أجهزة إنترنت الأشياء.
- تأمين بروتوكولات الاتصال لـ IoT.
- حماية البيانات في سحابة IoT.
- إدارة دورة حياة أمن أجهزة IoT.
- التشفير خفيف الوزن لـ IoT.
- المصادقة والتفويض لأجهزة IoT.
- تأمين التحديثات البرمجية لأجهزة IoT.

الوحدة الرابعة: الدفاع في العمق والاستجابة للحوادث.

- مفاهيم الدفاع في العمق للشبكات اللاسلكية.
- أنظمة كشف ومنع التسلل (IDS/IPS).
- جدران الحماية المتقدمة للشبكات اللاسلكية.
- تحليل السجلات الأمنية ومراقبة الشبكة.
- التخطيط والاستجابة للحوادث الأمنية.
- التحقيق الجنائي الرقمي في حوادث الشبكات.
- إدارة الثغرات الأمنية والتصحيحات.

الوحدة الخامسة: أمن الشبكات المتقدم والتوجهات المستقبلية.

- أمن الشبكات المعرفة بالبرمجيات (SDN) والشبكات الافتراضية.
- تأمين الذكاء الاصطناعي وتعلم الآلة في الشبكات.
- البلوك تشين في أمن الاتصالات.
- تأمين الاتصالات الكمومية.
- التهديدات الناشئة والاتجاهات المستقبلية في الأمن السيبراني.
- الامتثال للمعايير الأمنية (مثل NIST, ISO 27001).
- بناء ثقافة أمنية قوية في المؤسسات.

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:

في ظل التطور المتسارع لتقنيات الجيل الخامس وإنترنت الأشياء، كيف يمكن للمهندسين والمتخصصين الموازنة بين الحاجة إلى الابتكار والسرعة في النشر، وبين ضمان أعلى مستويات الأمن والخصوصية لملايين الأجهزة والبيانات التي ستتصل بهذه الشبكات؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على دمج مفاهيم التصميم والأمن لشبكات الاتصالات اللاسلكية المتقدمة، وتحديدًا 5G وIoT، مع إيلاء اهتمام خاص لمتطلبات البنية التحتية الحرجة. بدلاً من تقديم نظرة عامة، تتعمق الدورة في الجوانب التقنية والأمنية، وتقدم رؤى عملية حول كيفية بناء شبكات قوية ومحصنة ضد التهديدات السيبرانية المتزايدة. على سبيل المثال، نتعمق في تفاصيل تأمين شرائح الشبكة في 5G وتأمين أجهزة إنترنت الأشياء ذات الموارد المحدودة، وهي تحديات حرجة في العالم الواقعي. نركز على دراسات الحالة الفعلية والتمارين التطبيقية التي تحاكي سيناريوهات الهجمات السيبرانية والاستجابة لها، مما يمنح المشاركين خبرة عملية لا تقدر بثمن. الدورة مصممة لتزويد المتدربين ليس فقط بالمعرفة النظرية، بل بالمهارات العملية اللازمة لتصميم وتنفيذ وصيانة شبكات لاسلكية آمنة وموثوقة، مما يجعلهم خبراء مطلوبين في سوق العمل المتطور.