الدورة التدريبية: الأمن السيبراني لشبكات الجيل الخامس (5G) وتقنيات الاتصالات)

#CYB5360

) وتقنيات الاتصالاتGالدورة التدريبية: الأمن السيبراني لشبكات الجيل الخامس (5

مقدمة الدورة التدريبية / لمحة عامة:

تُمثل شبكات الجيل الخامس (G5) تحولًا جذريًا في عالم الاتصالات، مقدمة سرعات فائقة، زمن انتقال منخفضًا، وقدرة على ربط عدد هائل من الأجهزة. هذا التوسع الهائل يفتح آفاقًا جديدة للمدن الذكية، السيارات ذاتية القيادة، وإنترنت الأشياء (IoT)، ولكنه في الوقت نفسه يخلق بيئة جديدة من التهديدات السيبرانية المعقدة. إن أي اختراق أمني في بنية G5 التحتية يمكن أن يهدد الأمن القومي، ويعطل الخدمات الحيوية، ويهدد خصوصية الأفراد. تقدم هذه الدورة التدريبية المتخصصة لمهندسي الاتصالات، متخصصي الأمن السيبراني، ومطوري الشبكات، المعرفة والمهارات اللازمة لـتأمين شبكات G5 من الهجمات الرقمية. سنتناول في هذه الدورة مفاهيم أمن G5، التهديدات المتقدمة، والضوابط الأمنية اللازمة. سيكتسب المشاركون القدرة على تحديد نقاط الضعف، تطبيق حلول أمنية قوية، ووضع استراتيجيات متكاملة لـأمن الاتصالات اللاسلكية. تهدف الدورة إلى بناء كوادر متخصصة قادرة على تأمين مستقبل الاتصالات. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات الدولية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور روبرت فيشر (Robert Fisher)، المعروف بأعماله في أمن الشبكات اللاسلكية. يقدم BIG BEN Training Center هذه الدورة لتمكين قادة التكنولوجيا من بناء بنية تحتية آمنة ومرنة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو الشبكات والاتصالات.
- متخصصو الأمن السيبراني في قطاع الاتصالات.
- مطورو الشبكات اللاسلكية.
- مديرو البنية التحتية لـ G5.
- القيادات التقنية في شركات الاتصالات.
- المستشارون في الأمن السيبراني.

القطاعات والصناعات المستهدفة:

- شركات الاتصالات ومزودو الخدمة.
- صناع معدات الشبكات.
- الجهات الحكومية وما في حكمها المسؤولة عن الاتصالات.
- شركات الأمن السيبراني.
- قطاع النقل والمدن الذكية.

الأقسام المؤسسية المستهدفة:

- إدارة الشبكات.
- إدارة الأمن السيبراني.
- إدارة البحث والتطوير.
- إدارة العمليات والتشغيل.
- إدارة المخاطر.

أهداف الدورة التدريبية:

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

- فهم بنية شبكات G5 وتحدياتها الأمنية الفريدة.
- القدرة على تحديد التهديدات التي تستهدف أنظمة G5.
- تأمين مكونات شبكة G5 الأساسية (Core Network).
- حماية البيانات وخصوصية المستخدمين في شبكات الجيل الخامس.
- تطبيق ضوابط أمنية على أجهزة إنترنت الأشياء (IoT) المتصلة بـ G5.
- وضع استراتيجيات للاستجابة للحوادث في بيئة G5.
- الامتثال للمعايير الدولية لأمن الاتصالات.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية متقدمة وعملية، مصممة لتمكين المشاركين من فهم وتطبيق إجراءات الأمن السيبراني لشبكات G5. سيتمكن المتدربون من خلال دراسات الحالة الواقعية لهجمات سيبرانية على شبكات الاتصالات، وورش العمل التفاعلية، من اكتساب خبرة مباشرة في تأمين البنية التحتية لـ G5. تتضمن المنهجية مناقشات متعمقة حول الفرق بين أمن G4 وG5، والتحديات الأمنية لتقنية Network Slicing. سيتم التركيز على تحليل المخاطر وبناء دفاعات قوية ضد التهديدات المتقدمة. يقدم BIG BEN Training Center هذه الدورة لتعزيز الخبرة الأمنية لدى العاملين في قطاع الاتصالات وضمان مستقبل رقمي آمن.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات شبكات 5G وتحديات الأمن

- مقدمة إلى بنية G5 ومكوناتها.
- التهديدات السيبرانية التي تستهدف شبكات الجيل الخامس.
- نقاط الضعف في تقنيات (Slicing, Edge Computing).
- الفرق بين أمن G5 والجيل السابق.
- أهمية تأمين G5 للخدمات الحيوية.
- الوعي بالتهديدات من الخصوم المتقدمين (APTs).
- الأمن كجزء من تصميم G5.

الوحدة الثانية: تأمين شبكة 5G الأساسية (Core Network)

- بنية شبكة G5 الأساسية المبنية على السحابة (Cloud-native).
- تأمين واجهات البرمجة (APIs).
- المصادقة والترخيص في شبكة G5.
- تشفير الاتصالات داخل الشبكة.
- أمن خدمات الحوسبة المتطورة (MEC).
- التعامل مع الثغرات الأمنية في الشبكة الأساسية.
- فصل الشبكات المنطقية (Network Slicing).

الوحدة الثالثة: حماية البيانات وخصوصية المستخدم

- البيانات الشخصية التي تجمعها شبكات G5.
- حماية خصوصية المستخدمين في G5.
- تشفير البيانات أثناء النقل.
- الامتثال للوائح حماية البيانات (GDPR).
- إدارة الهوية في بيئة G5.
- أمن بيانات إنترنت الأشياء (IoT).
- التعامل مع المراقبة القانونية للبيانات.

الوحدة الرابعة: الاستجابة للحوادث الأمنية والتهديدات

- بناء خطة للاستجابة للحوادث في بيئة G5.
- أدوات اكتشاف الاختراقات في شبكات الجيل الخامس.
- التحقيق في الحوادث الأمنية.
- التعامل مع هجمات حجب الخدمة (DDoS).
- التصدي لهجمات التزييف (Spoofing).
- التعافي من الحوادث واستمرارية الأعمال.
- التعاون مع الجهات الأمنية.

الوحدة الخامسة: مستقبل الأمن في شبكات الاتصالات

- تأثير الذكاء الاصطناعي في أمن G5.
- أمن شبكات G6 المستقبلية.
- استراتيجيات الأمن الاستباقي (Proactive Security).
- التعاون بين شركات الاتصالات والجهات الحكومية.
- المرونة السيبرانية واستدامة الخدمات.
- التدريب المستمر على أحدث التهديدات.
- التحول نحو بنية شبكة Zero Trust.

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 الاعتماد المتزايد على شبكات G5 لتشغيل البنية التحتية الحيوية، كيف يمكن للمهندسين والمخططين أن يبتكرون استراتيجيات أمنية لا تقتصر على الحماية التقنية فحسب، بل تُنشئ نظامًا بيئيًا مرنًا، وتضمن الخصوصية، وتُمكّن الشبكة من الصمود أمام التهديدات المستقبلية مع الحفاظ على الابتكار المستمر؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على الأمن السيبراني لشبكات الجيل الخامس (G5)، مما يوفر محتوى مصممًا خصيصًا لمواجهة التحديات الأمنية الفريدة في هذا المجال. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لتأمين بنية G5 التحتية، وحماية البيانات، وتأمين أجهزة إنترنت الأشياء (IoT). تقدم الدورة دراسات حالة واقعية لهجمات سيبرانية على شبكات الاتصالات، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز على الترابط بين مكونات الشبكة المختلفة والاستراتيجيات المتكاملة للأمن، مما يضمن أن المشاركين سيخرجون بخبرة عملية قابلة للتطبيق. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في الأمن السيبراني قادرين على حماية مستقبل الاتصالات.