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

٢٩ يونيو - ٠٣ يوليو ٢٠٢٦

القاهرة - *

٤١٠٠ € (للشخص الواحد)

Ref: #CYB5360_565094

مقدمة الدورة التدريبية / لمحة عامة:

هائل من الأجهزة. هذا عالم الاتصالات، مقدمة سرعات فائقة، زمن انتقال تُمثل شبكات الجيل الخامس (G٥) تحولا جذريًا في
السيارات ذاتية القيادة، وإنترنت الأشياء (IoT)، التوسع الهائل يفتح آفاقًا جديدة للمدن الذكية، منخفضًا، وقدرة على ربط عدد
الأمن القومي، ٥G السيبرانية المعقدة. إن أي اختراق أمني في بنية ولكنه في الوقت نفسه يخلق بيئة جديدة من التهديدات
المتخصصة لمهندسي الاتصالات، الخدمات الحيوية، ويهدد خصوصية الأفراد. تقدم هذه ويعطل التحتية يمكن أن يهدد
والمهارات اللازمة لـتأمين شبكات ٥ G من الهجمات متخصصي الأمن السيبراني، ومطوري الشبكات، المعرفة الدورة التدريبية
على تحديد نقاط الضعف، التهديدات المتقدمة، والضوابط الأمنية اللازمة. الرقمية. سنتناول في هذه الدورة مفاهيم أمن G٥،
الاتصالات اللاسلكية. تهدف الدورة إلى بناء تطبيق حلول أمنية قوية، ووضع استراتيجيات متكاملة سيكتسب المشاركون القدرة
أكاديميين يستند المحتوى إلى أحدث المعايير وأفضل الممارسات كوادر متخصصة قادرة على تأمين مستقبل الاتصالات. لـأمن
بأعماله في أمن الشبكات(Fisher بارزين مثل البروفيسور روبرت فيشر (Robert الدولية، مع الاستفادة من إسهامات خبراء
آمنة ومرنة. الدورة لتمكين قادة التكنولوجيا من بناء بنية تحتية اللاسلكية. يقدم BIG BEN Training Center هذه ، المعروف

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مهندسو الشبكات والاتصالات.
- متخصصو الأمن السيبراني في قطاع الاتصالات.
- مطورو الشبكات اللاسلكية.
- مديرو البنية التحتية لـ ٥.G
- القيادات التقنية في شركات الاتصالات.
- المستشارون في الأمن السيبراني.

القطاعات والصناعات المستهدفة:

- شركات الاتصالات ومزودو الخدمة.
- صناع معدات الشبكات.
- الاتصالات. الجهات الحكومية وما في حكمها المسؤولة عن
- 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:

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

- فهم بنية شبكات ٥G وتحدياتها الأمنية الفريدة.
- ٥G. القدرة على تحديد التهديدات التي تستهدف أنظمة
- تأمين مكونات شبكة ٥G الأساسية (Core Network).
- الخامس. حماية البيانات وخصوصية المستخدمين في شبكات الجيل
- G. المتصلة بـ ٥ (IoT) تطبيق ضوابط أمنية على أجهزة إنترنت الأشياء
- وضع استراتيجيات للاستجابة للحوادث في بيئة ٥G.
- الامتثال للمعايير الدولية لأمن الاتصالات.

منهجية الدورة التدريبية:

المتدربون مصممة لتمكين المشاركين من فهم وتطبيق إجراءات تعتمد هذه الدورة التدريبية منهجية متقدمة وعملية، وورش العمل التفاعلية، من من خلال دراسات الحالة الواقعية لـهجمات سيبرانية الأمن السيبراني لشبكات ٥G. سيتمكن المنهجية مناقشات متعمقة حول الفرق بين ٥G. اكتساب خبرة مباشرة في تأمين البنية التحتية لـ على شبكات الاتصالات، يقدم BIG BEN سيتم التركيز على تحليل المخاطر وبناء Slicing. أمن ٤G و٥G، والتحديات الأمنية لتقنية Network تتضمن الاتصالات وضمان مستقبل رقمي هذه الدورة لتعزيز الخبرة الأمنية Training Center دفاعات قوية ضد التهديدات المتقدمة. آمن. لدى العاملين في قطاع

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات شبكات ٥G وتحديات الأمن

- مقدمة إلى بنية ٥G ومكوناتها.
- الخامس. التهديدات السيبرانية التي تستهدف شبكات الجيل
- نقاط الضعف في تقنيات (Slicing, Edge Computing).
- الفرق بين أمن ٥G والجيل السابق.
- أهمية تأمين ٥G للخدمات الحيوية.
- الوعي بالتهديدات من الخصوم المتقدمين (APTs).
- الأمن كجزء من تصميم ٥G.

الوحدة الثانية: تأمين شبكة ٥G الأساسية (Core Network)

- بنية شبكة ٥G الأساسية المبنية على السحابة (Cloud-native).
- تأمين واجهات البرمجة (APIs).
- المصادقة والترخيص في شبكة ٥G.
- 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 ٥G.
- حماية خصوصية المستخدمين في ٥G.
- تشفير البيانات أثناء النقل.
- الامتثال للوائح حماية البيانات (GDPR).
- إدارة الهوية في بيئة ٥G.
- أمن بيانات إنترنت الأشياء (IoT).
- التعامل مع المراقبة القانونية للبيانات.

والتهديدات الوحدة الرابعة: الاستجابة للحوادث الأمنية

- بناء خطة للاستجابة للحوادث في بيئة ٥G.
- 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 ٥G.
- أمن شبكات ٦G 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:

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 ٢٠-٢٥ 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:

استراتيجيات أمنية لا تقتصر البنية التحتية الحيوية، كيف يمكن للمهندسين في ظل الاعتماد المتزايد على شبكات 5G التشغيل مرنًا، وتضمن الخصوصية، وتُمكّن الشبكة من الصمود على الحماية التقنية فحسب، بل تُنشئ نظامًا بيئيًا والمخططين أن يبتكرون المستمر؟ أمام التهديدات المستقبلية مع الحفاظ على الابتكار

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

لمواجهة التحديات الأمن السيبراني لشبكات الجيل الخامس (5G)، مما تتميز هذه الدورة بتركيزها المتخصص والعميق على السيبراني بشكل عام، نغوص في التطبيق العملي الأمنية الفريدة في هذا المجال. بدلاً من تناول يوفر محتوى مصممًا خصيصًا لهجمات سيبرانية على شبكات وتأمين أجهزة إنترنت الأشياء (IoT). تقدم الدورة التحتية، وحماية البيانات، لتأمين بنية 5G الأمن مما دفاعات قوية. نركز على الترابط بين مكونات الشبكة الاتصالات، مع تحليل مفصل لنتائجها وكيفية بناء دراسات حالة واقعية مجرد دورة نظرية، بل هي برنامج يضمن أن المشاركين سيخرجون بخبرة عملية قابلة المختلفة والاستراتيجيات المتكاملة للأمن، السيبراني قادرين على حماية مستقبل الاتصالات. تدريبي مكثف يهدف إلى بناء متخصصين في الأمن للتطبيق. إنها ليست