التدريبية: الأمن السيبراني للمدن الذكية والبنية التحتية الحضرية الدورة

يونيو - ٠٣ يوليو ٢٠٢٦ ٢٩

باكو - *

(للشخص الواحد) € ٥٠٠٠

Ref: #CYB8238_270657

مقدمة الدورة التدريبية / لمحة عامة:

الرقمي يخلق بيئة تتكامل التكنولوجيا لتعزيز كفاءة الخدمات وتحسين تُمثل المدن الذكية مستقبل التنمية الحضرية، حيث
الحيوية. إن أي اختراق أمني في جديدة من التهديدات السيبرانية التي تستهدف البنية جودة الحياة. ولكن هذا الترابط
المياه، قد يؤدي إلى فوضى عارمة وكوارث غير متوقعة. أنظمة التحكم المروري، أو شبكات الطاقة، أو إدارة التحتية الحضرية
اللازمة لحماية الأمن السيبراني، المخططين الحضريين، ومهندسي تقدم هذه الدورة التدريبية المتخصصة لمتخصصي
مفاهيم الأمن السيبراني للبنية التحتية المدن الذكية من الهجمات الرقمية. سنتناول في هذه الأنظمة، المعرفة والمهارات
ضوابط أمنية قوية، وحماية البيانات الحضرية. سيكتسب المشاركون القدرة الحيوية، تأمين أنظمة إنترنت الأشياء (IoT) الدورة
إلى بناء كوادر متخصصة قادرة ووضع استراتيجيات متكاملة للأمن السيبراني في المدن على تحديد نقاط الضعف، تطبيق
استدامتها. يستند المحتوى إلى أحدث المعايير وأفضل على تأمين البنية التحتية الحضرية وضمان الذكية. تهدف الدورة
المعروف بأعماله في أمن خبراء أكاديميين بارزين مثل البروفيسور روبرت الممارسات الدولية، مع الاستفادة من إسهامات
الدورة لتمكين قادة المدن من بناء مستقبل حضري المدن الذكية. يقدم BIG BEN Training Center ديازن (Robert Dea Zen)
آمن ومرن. هذه

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- متخصصو الأمن السيبراني.
- مهندسو الأنظمة والشبكات.
- مخططو المدن والمهندسون الحضريون.
- مديرو البنية التحتية الحيوية (الطاقة، المياه، النقل).
- صانعو القرار في الهيئات الحكومية المحلية.
- المطورون العقاريون للمدن الذكية.

القطاعات والصناعات المستهدفة:

- الجهات الحكومية المحلية والوطنية.
- شركات البنية التحتية الحيوية.
- شركات الاتصالات وتقنية المعلومات.
- شركات النقل العام.
- شركات الأمن السيبراني.
- المؤسسات الأكاديمية والبحثية.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة تقنية المعلومات.
- إدارة التخطيط الحضري.
- إدارة العمليات والتحكم.
- إدارة المخاطر.

أهداف الدورة التدريبية:

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

- فهم التحديات الأمنية الفريدة للمدن الذكية.
- البنية التحتية. القدرة على تأمين أجهزة إنترنت الأشياء (IoT) في
- الذكية. حماية شبكات الاتصالات والأنظمة المركزية للمدن
- التحتية الحيوية. تأمين أنظمة التحكم الصناعي (ICS) والبنية
- تقييم المخاطر الأمنية ووضع استراتيجيات دفاعية.
- تطوير خطط الاستجابة للحوادث في بيئة المدن الذكية.
- التحتية الحضرية. الامتثال للوائح والمعايير المتعلقة بأمن البنية

منهجية الدورة التدريبية:

الذكية. نحو التطبيق العملي، مصممة لتمكين المشاركين من فهم تعتمد هذه الدورة التدريبية منهجية متقدمة وموجهة على المدن، وورش العمل سيتمكن المتدربون من خلال دراسات الحالة الواقعية وتطبيق إجراءات الأمن السيبراني للمدن الضعف الأنظمة الحضرية. تتضمن المنهجية مناقشات متعمقة التفاعلية، من اكتساب خبرة مباشرة في تأمين لهجمات سيبرانية ضد التهديدات الموجهة. يقدم المترتبة على ذلك. سيتم التركيز على تحليل المخاطر حول الترابط بين الأنظمة المختلفة ونقاط آمن للمدن. الخبرة الأمنية لدى العاملين في مجال التنمية هذه الدورة لتعزيز BIG BEN Training Center وبناء دفاعات قوية الحضرية وضمان مستقبل

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الذكية الوحدة الأولى: مقدمة في الأمن السيبراني للمدن

- مفهوم المدن الذكية ومكوناتها الأساسية.
- الحضرية. التهديدات السيبرانية التي تواجه البنية التحتية
- الذكية. نقاط الضعف في أنظمة النقل، الطاقة، والمياه
- التقليدية. الفرق بين أمن المدن الذكية وأمن المؤسسات
- أمثلة على حوادث أمنية في المدن الذكية.
- إطار عمل الأمن السيبراني للمدن الذكية.
- أهمية حماية البيانات الشخصية في المدن الذكية.

الوحدة الثانية: تأمين أنظمة إنترنت الأشياء(IoT)

- مبادئ أمن أجهزة إنترنت الأشياء (IoT)
- نقاط الضعف الشائعة في أجهزة IoT
- المصادقة والترخيص في بيئات IoT
- تشفير الاتصالات بين أجهزة IoT والشبكات.
- إدارة الثغرات الأمنية في أجهزة IoT
- أمن تحديثات البرامج الثابتة (Firmware)
- تصميم بنية تحتية آمنة لـ IoT

الحضرية الوحدة الثالثة: حماية البنية التحتية الحيوية

- الحضرية. أمن أنظمة التحكم الصناعي (ICS) في المرافق
- تأمين شبكات الطاقة الذكية (Smart Grids)
- حماية أنظمة إدارة المياه.
- أمن شبكات النقل الذكية والتحكم المروري.
- التحكم في الوصول المادي والرقمي.
- مراقبة التهديدات في البنية التحتية الحيوية.
- الأنظمة. فصل الشبكات (Network Segmentation) لتأمين

الوحدة الرابعة: حماية البيانات الحضرية والخصوصية

- أنواع البيانات التي تجمعها المدن الذكية.
- أمن البيانات والخصوصية في المدينة الذكية.
- تشفير البيانات أثناء النقل والتخزين.
- الامتثال للوائح حماية البيانات (GDPR, CCPA)
- إدارة الهوية في بيئة المدن الذكية.
- التعامل مع بيانات الكاميرات والمستشعرات.
- أخلاقيات الأمن السيبراني في المدن الذكية.

المرونة الوحدة الخامسة: استراتيجيات الأمن السيبراني وبناء

- وضع استراتيجية أمن سيبراني متكاملة للمدينة.
- الاستجابة للحوادث الأمنية والتعافي منها.
- بناء فريق عمل متخصص في الأمن السيبراني.
- التعاون مع القطاع الخاص والخبراء.
- التوعية الأمنية لجميع المعنيين.
- التدقيق الأمني الدوري للبنية التحتية الحضرية.
- المرونة السيبرانية واستدامة الخدمات الحيوية.

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

إجمالي المدة إلى بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام، ساعة تدريبية. ٢٥-٢٠ راحة وأنشطة تفاعلية، ليصل

سؤال للتأمل:

استراتيجيات أمنية لا تقتصر البنية التحتية الحضرية، كيف يمكن للمسؤولين في ظل الاعتماد المتزايد على التكنولوجيا لربط وتضمن الخصوصية، وتُمكن المدينة من الصمود أمام على الحماية التقنية، بل تُنشئ بنية تحتية مرنة، والمخططين أن يبتكرون الخدمات الأساسية للمواطنين؟ التهديدات المستقبلية مع الحفاظ على استمرارية

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

مصممًا خصيصًا لمواجهة الأمن السيبراني للمدن الذكية والبنية التحتية تتميز هذه الدورة بتركيزها المتخصص والعميق على الأمن السيبراني بشكل عام، نغوص في التطبيق التحديات الأمنية الفريدة في هذا المجال. بدلاً من الحضرية، مما يوفر محتوى سيبرانية على المدن، مع وحماية البنية التحتية الحيوية. تقدم الدورة دراسات (IoT) العملي لتأمين أنظمة إنترنت الأشياء تناول على الترابط بين الأنظمة المختلفة والاستراتيجيات تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز حالة واقعية لهجمات مكثف يهدف إلى بناء بخبرة عملية قابلة للتطبيق. إنها ليست مجرد دورة المتكاملة للأمن، مما يضمن أن المشاركين سيخرجون مستقبل مدننا. متخصصين في الأمن السيبراني قادرين على حماية نظرية، بل هي برنامج تدريبي