الدورة التدريبية: الأمن السيبراني للمدن الذكية والبنية التحتية الحضرية

#CYB8238

الدورة التدريبية: الأمن السيبراني للمدن الذكية والبنية التحتية الحضرية

مقدمة الدورة التدريبية / لمحة عامة:

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

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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة في الأمن السيبراني للمدن الذكية

- مفهوم المدن الذكية ومكوناتها الأساسية.
- التهديدات السيبرانية التي تواجه البنية التحتية الحضرية.
- نقاط الضعف في أنظمة النقل، الطاقة، والمياه الذكية.
- الفرق بين أمن المدن الذكية وأمن المؤسسات التقليدية.
- 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.

الوحدة الثالثة: حماية البنية التحتية الحيوية الحضرية

- أمن أنظمة التحكم الصناعي (ICS) في المرافق الحضرية.
- 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.
- فصل الشبكات (Network Segmentation) لتأمين الأنظمة.

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.

الوحدة الخامسة: استراتيجيات الأمن السيبراني وبناء المرونة

- 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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على الأمن السيبراني للمدن الذكية والبنية التحتية الحضرية، مما يوفر محتوى مصممًا خصيصًا لمواجهة التحديات الأمنية الفريدة في هذا المجال. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لتأمين أنظمة إنترنت الأشياء(IoT) وحماية البنية التحتية الحيوية. تقدم الدورة دراسات حالة واقعية لهجمات سيبرانية على المدن، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز على الترابط بين الأنظمة 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 مدننا.