مستقبلنا المتصل الدورة التدريبية: تأمين إنترنت الأشياء والمدن الذكية: استراتيجيات حماية

يوليو ٢٠٢٦ ١٠ - ٠٦

شرم الشيخ

(للشخص الواحد) € ٤١٠٠

Ref: #SM9395_577821

مقدمة الدورة التدريبية / لمحة عامة:

غير مسبوقة. مع تزايد عدد نقلة نوعية في طريقة عيشنا وعملنا، لكنه يحمل في يمثل عصر إنترنت الأشياء (IoT) والمدن الذكية هذه البيئات الرقمية أمرًا بالغ الأهمية لحماية الأجهزة المتصلة وتشابك الأنظمة الذكية، يصبح تأمين طياته تحديات أمنية BIG BEN Training الأفراد. تقدم هذه الدورة التدريبية المتقدمة من البيانات الحساسة والبنية التحتية الحيوية وخصوصية وتزود المشاركين بالاستراتيجيات والأدوات اللازمة الأمنية المرتبطة بإنترنت الأشياء والمدن الذكية، فهمًا عميقًا للمخاطر Center المتعلقة بخصوصية المحتملة، بدءًا من الهجمات السيبرانية على الأجهزة لتأمين هذه الأنظمة المتطورة. سنتناول التهديدات والمعايير الدولية مسترشدة برؤى البيانات في المدن الذكية. تستمد هذه الدورة أسسها المتصلة وصولا إلى التحديات Shadbolt سبيل المثال لا الحصر، البروفيسور Sir Nigel خبراء الأمن السيبراني والمدن الذكية، ومنهم على من أحدث الأبحاث للتحديات الأمنية في الأنظمة المتصلة. الكمبيوتر والبيانات المفتوحة، الذي أسهمت أعماله (السير نايجل شادبولت)، رائد علوم آمنة وموثوقة، تعزز الابتكار مع الحفاظ على حماية تهدف الدورة إلى تمكين المهنيين من بناء بيئات ذكية في فهم أعمق الأصول الرقمية والمادية.

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مدراء أمن المعلومات والأمن السيبراني.
- مهندسو شبكات إنترنت الأشياء ومطورو الحلول الذكية.
- مخططو المدن الذكية ومسؤولو البنية التحتية.
- متخصصو حماية البيانات والخصوصية.
- مدراء المشاريع التقنية.
- مسؤولو الامتثال والمخاطر.
- المهندسون المعماريون للحلول الذكية.
- بالمدن الذكية. صناع القرار في القطاعات الحكومية والخاصة المعنية

القطاعات والصناعات المستهدفة:

- الذكية. الجهات الحكومية والبلديات المسؤولة عن تطوير المدن
- شركات تكنولوجيا المعلومات والاتصالات.
- شركات تطوير أجهزة إنترنت الأشياء.
- قطاع البنية التحتية والنقل الذكي.
- مرافق الطاقة والمياه (الشبكات الذكية).
- شركات الأمن السيبراني والاستشارات التقنية.
- قطاع الرعاية الصحية (الأجهزة الطبية المتصلة).
- صناعة السيارات المتصلة.

الأقسام المؤسسية المستهدفة:

- قسم الأمن السيبراني.
- قسم تكنولوجيا المعلومات والاتصالات.
- قسم تطوير المنتجات والحلول الذكية.
- قسم التخطيط العمراني والمدن الذكية.
- قسم إدارة المشاريع.
- القسم القانوني والامتثال.
- قسم البحث والتطوير.
- العمليات والتشغيل للبنى التحتية الذكية.

أهداف الدورة التدريبية:

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

- الأشياء والمدن الذكية. فهم التهديدات الأمنية الفريدة لأنظمة إنترنت
- والشبكات. تطبيق أفضل الممارسات لتأمين أجهزة إنترنت الأشياء
- الذكية. تطوير استراتيجيات حماية البيانات في بيئات المدن
- الذكية. تقييم المخاطر الأمنية المتعلقة بالبنية التحتية
- تصميم حلول أمنية قوية للأنظمة المتصلة.
- الأشياء. التعامل مع حوادث الأمن السيبراني في أنظمة إنترنت
- ضمان الامتثال للوائح والمعايير الأمنية ذات الصلة.
- بناء ثقافة أمنية شاملة في بيئات المدن الذكية.
- حماية خصوصية المستخدمين في سياق البيانات الضخمة.
- تعزيز مرونة البنية التحتية الذكية ضد الهجمات.

منهجية الدورة التدريبية:

بهدف تمكين منهجية تعليمية متطورة تجمع بين المعرفة النظرية يعتمد BIG BEN Training Center في هذه الدورة الذكية. سيتم تقديم المحتوى من المشاركين من مواجهة التحديات الأمنية لإنترنت المتعمقة والتطبيق العملي المكثف، حالة يقوم المشاركون بتطبيق المفاهيم المكتسبة على خلال محاضرات تفاعلية، تليها ورش عمل عملية حيث الأشياء والمدن معالجتها. سيتم تشجيع مفصلة لأحدث الهجمات الأمنية والثغرات في أنظمة سيناريوهات واقعية. تتضمن الدورة دراسات مما يثري الفهم ويفتح آفاقًا جديدة للحلول. كما النقاشات الجماعية وتبادل الخبرات بين المشاركين، إنترنت الأشياء، وكيفية تهدف هذه المنهجية إلى المتقدمة، مثل اختبار الاختراق لأجهزة إنترنت سيتم توفير فرص لممارسة أدوات وتقنيات التأمين وتنفيذ استراتيجيات أمنية فعالة لحماية البنية بناء قدرات عملية لدى المتدربين، تمكنهم من تصميم الأشياء وتحليل الثغرات. التحتية المتصلة للمدن الذكية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

والمدن الذكية الوحدة الأولى: مقدمة إلى أمن إنترنت الأشياء

- مفاهيم إنترنت الأشياء والمدن الذكية.
- الأشياء. المخاطر والتهديدات الأمنية في بيئات إنترنت
- التحديات الفريدة لأمن المدن الذكية.
- طبقات الأمن في أنظمة إنترنت الأشياء.
- أهمية الخصوصية في المدن الذكية.
- النماذج المعمارية لأنظمة إنترنت الأشياء.
- المتطلبات التنظيمية لأمن إنترنت الأشياء.

والاتصالات الوحدة الثانية: تأمين أجهزة إنترنت الأشياء

- نقاط الضعف الشائعة في أجهزة إنترنت الأشياء.
- الثابتة). استراتيجيات تأمين الأجهزة (الأجهزة والبرامج
- بروتوكولات الاتصال الآمنة لإنترنت الأشياء.
- تشفير البيانات في أجهزة إنترنت الأشياء.
- إدارة الهوية والوصول لأجهزة إنترنت الأشياء.
- تحديثات البرامج الثابتة الآمنة.
- مراقبة الأجهزة واكتشاف السلوكيات الشاذة.

الذكية الوحدة الثالثة: حماية البيانات والخصوصية في المدن

- تحديات خصوصية البيانات في المدن الذكية.
- إدارة البيانات الضخمة وأمنها.
- الامتثال للوائح حماية البيانات (GDPR، CCPA).
- أخلاقيات جمع واستخدام البيانات في المدن الذكية.
- تقنيات إخفاء الهوية والخصوصية المعززة.
- أمن السحابة في بيئات إنترنت الأشياء والمدن الذكية.
- التحليلات الأمنية لبيانات المدن الذكية.

الوحدة الرابعة: أمن البنية التحتية الحيوية والأنظمة الذكية

- تأمين شبكات الاتصالات (5G، LoRaWAN).
- أمن أنظمة التحكم الصناعية (ICS/SCADA) في المدن.
- حماية البنية التحتية للنقل الذكي.
- أمن شبكات الطاقة الذكية (Smart Grids).
- التعامل مع هجمات حجب الخدمة الموزعة (DDoS) على المدن الذكية.
- الاستجابة للحوادث الأمنية في البنية التحتية الذكية.
- التعافي من الكوارث في بيئات المدن الذكية.

الوحدة الخامسة: بناء استراتيجيات أمنية شاملة للمدن الذكية

- تقييم المخاطر الأمنية للمشاريع الذكية.
- وضع سياسات وإجراءات أمنية شاملة.
- بناء فرق عمل متخصصة في أمن المدن الذكية.
- التعاون مع الجهات الحكومية والخاصة لتأمين المدن.
- التوعية والتدريب على الأمن السيبراني للمواطنين.
- التحسين المستمر لبرامج أمن المدن الذكية.
- التحديات المستقبلية والابتكارات في أمن إنترنت الأشياء.

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 ٢٥٢٠- 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:

الذكية التي المدن الذكية، كيف يمكن للمجتمعات تحقيق التوازن في ظل التطور المتسارع لإنترنت الأشياء وتوسع مفهوم

وحماية خصوصية الأفراد في بيئة متصلة تعزز جودة الحياة، وبين ضمان الأمن السيبراني الأمثل بين الابتكار وتقديم الخدمات

ومعقدة بشكل متزايد؟ المطلق

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

الأمنية المعقدة للمدن الذكية، والفريد الذي يجمع بين التأمين الشامل لإنترنت تتميز هذه الدورة التدريبية بمنهجها المتكامل التطورات التقليدية. يقدم BIG BEN Training Center محتوى مما يقدم رؤية بانورامية لا توفرها الدورات الأشياء والتحديات إنترنت الأشياء المتشابكة. ما يميز هذه البحثية والمعايير العالمية في الأمن السيبراني أكاديميًا متقدمًا يستند إلى أحدث ومستنيرة لكيفية والتشغيلية، حيث لا تقتصر على سرد نقاط الضعف، بل الدورة هو تركيزها على الجوانب الاستراتيجية لبيئات فهمًا عميقًا لكيفية الموازنة بين تصميم وتنفيذ بنية تحتية آمنة للمدن الذكية. يكتسب تتعداها إلى تقديم حلول عملية وقابلاً للتطبيق الهجمات السيبرانية. الأمثلة الواقعية ودراسات الابتكار والأمن، وكيفية بناء أنظمة مرنة تتحمل المشاركون لمواجهة التحديات الأمنية المعقدة في المستقبل الفوري، مما يضمن أن يكون المتدربون مجهزين الحالة تجعل المحتوى حيويًا المتصل.