التدريبية: الأمن السيبراني لإنترنت الأشياء
والأجهزة الذكية (IoT) الدورة

مايو ٢٠٢٦ ٠٨ - ٠٤

طوكيو

٦٥٠٠ € (للشخص الواحد)

Ref: #CYB5786_269290

مقدمة الدورة التدريبية / لمحة عامة:

آفاقًا جديدة للابتكار، ولكنه الذكية، من المنازل والمباني الذكية إلى المدن يمثل إنترنت الأشياء (IoT) ثورة في ربط الأجهزة الشخصية الأجهزة المتصلة، تتصاعد المخاطر السيبرانية التي يقدم أيضًا تحديات أمنية هائلة. مع تزايد عدد الصناعية، مما يفتح للمهندسين، المطورين، مديري والبنية التحتية الحرجة للخطر. تقدم هذه الدورة تستهدف هذه الأجهزة، مما يعرض البيانات والمهارات اللازمة لـتأمين أنظمة إنترنت الأشياء المنتجات، والمتخصصين في الأمن السيبراني، المعرفة التدريبية المتخصصة واستراتيجيات الدفاع مفاهيم أمن IoT الأساسية، نقاط الضعف الشائعة في وحماية الأجهزة الذكية. سنتناول في هذه الدورة المشاركون القدرة على تقييم المخاطر الأمنية لأجهزة المتقدمة في بيئات الشبكات الذكية. سيكتسب أجهزة إنترنت الأشياء، الأشياء والأجهزة التي قد تؤثر على الأنظمة المتصلة. تهدف الدورة إلى تطبيق ضوابط الحماية، والاستجابة للحوادث IoT، في أمن IoT ، مع الاستفادة من المتصلة. يستند المحتوى إلى أحدث المعايير وأفضل بناء كوادر متخصصة في أمن إنترنت آرتشي كول (Arun Kumar Rai)، المعروف بأعماله في إسهامات خبراء أكاديميين بارزين مثل البروفيسور الممارسات الصناعية لـمنظومات إنترنت الأشياء. هذه الدورة لتعزيز المرونة BIG BEN Training Center الابتكار الرقمي وأمن الأجهزة الذكية. يقدم السيبرانية

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- مهندسو تطوير أجهزة إنترنت الأشياء.
- متخصصو الأمن السيبراني.
- مديرو المنتجات للأجهزة الذكية.
- مهندسو الشبكات والأنظمة.
- المطورون العاملون على تطبيقات IoT
- على IoT المسؤولون عن إدارة المخاطر في الشركات التي تعتمد

القطاعات والصناعات المستهدفة:

- صناعة التكنولوجيا والأجهزة الذكية.
- قطاع الاتصالات.
- المدن الذكية والبنية التحتية.
- قطاع الرعاية الصحية (الأجهزة الطبية المتصلة).
- القطاع الصناعي (Industrial IoT).
- أمن IoT الهيئات الحكومية وما في حكمها، المعنية بتنظيم

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- أقسام البحث والتطوير.
- إدارة المنتجات.
- إدارة تقنية المعلومات.
- إدارة العمليات (لأنظمة IoT الصناعية).

أهداف الدورة التدريبية:

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

- الفريدة. فهم مفاهيم أمن إنترنت الأشياء (IoT) وتحدياته
- IoT تحديد نقاط الضعف والتهديدات الشائعة في أجهزة
- الطبقات. القدرة على تطبيق أفضل ممارسات أمن IoT على مختلف
- بها. تأمين الأجهزة الذكية والمنصات السحابية المرتبطة
- إدارة المخاطر الأمنية في بيئات إنترنت الأشياء.
- الاستجابة الفعالة للحوادث الأمنية في أنظمة IoT
- IoT الامتثال للمعايير واللوائح الأمنية الخاصة بـ

منهجية الدورة التدريبية:

الأشياء والأجهزة مصممة لتمكين المشاركين من فهم وتطبيق إجراءات تعتمد هذه الدورة التدريبية منهجية عملية ومبتكرة، التي تتضمن محاكاة اختراق أجهزة IoT ، الذكية. سيتمكن المتدربون من خلال ورش العمل الأمن السيبراني في عالم إنترنت تحديات أمن من اكتساب خبرة مباشرة في تأمين الأجهزة المتصلة. IoT، ودراسات الحالة الواقعية لهجمات على أنظمة العملية الأمنية. سيتم التركيز على أمن الطبقات البيانات في IoT ، والخصوصية، والتعامل مع تتضمن المنهجية مناقشات متعمقة حول هذه الدورة لتزويد إلى الاتصالات والمنصات السحابية. (Firmware) المختلفة لـ IoT ، من العتاد والبرمجيات الثابتة التحديثات آمنة وموثوقة. المشاركين بالمهارات اللازمة لبناء منظومات IoT يقدم BIG BEN Training Center

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الأمن الوحدة الأولى: أساسيات إنترنت الأشياء وتحديات

- مقدمة إلى مفهوم إنترنت الأشياء (IoT).
- هندسة أنظمة IoT ومكوناتها.
- نقاط الضعف والتهديدات الشائعة في أجهزة IoT.
- أهمية أمن IoT في مختلف الصناعات.
- الخصوصية في إنترنت الأشياء وحماية البيانات.
- أمثلة على حوادث اختراق أجهزة IoT.
- تحديات قابلية التوسع في أمن IoT.

الوحدة الثانية: أمن عتاد وبرمجيات إنترنت الأشياء الثابتة (Firmware)

- تأمين العتاد (Hardware Security) في أجهزة IoT.
- أمن البرمجيات الثابتة (Firmware Security).
- التشفير المضمن (Embedded Encryption).
- التمهيد الآمن (Secure Boot) وتحديثات البرمجيات الثابتة الآمنة.
- حماية منافذ التصحيح (Debugging Ports).
- المصادقة الآمنة للأجهزة.
- تصميم أجهزة IoT مقاومة للاختراق.

الوحدة الثالثة: أمن الاتصالات وبروتوكولات IoT

- بروتوكولات الاتصالات الشائعة في IoT (MQTT, CoAP, Zigbee, Bluetooth).
- تأمين قنوات الاتصال (SSL/TLS, DTLS).
- إدارة المفاتيح والتشفير في شبكات IoT.
- حماية الشبكات اللاسلكية المستخدمة في IoT.
- أمن الاتصالات من الجهاز إلى السحابة (Device-to-Cloud Security).
- التعامل مع هجمات حجب الخدمة (DDoS) على أجهزة IoT.
- أمن البوابات (Gateways).

الوحدة الرابعة: أمن منصات IoT السحابية وإدارة البيانات

- Google Cloud IoT). تأمين منصات IoT السحابية (AWS IoT, Azure IoT,
- أمن البيانات في السحابة والتخزين الآمن.
- إدارة الهوية والوصول (IAM) لمنصات IoT.
- IoT أمن واجهات برمجة التطبيقات (API Security) لـ
- تحليلات الأمن السيبراني لبيانات IoT.
- السحابة. الامتثال للوائح حماية البيانات (GDPR) في
- مراقبة التهديدات في بيئات IoT السحابية.

في IoT ومستقبل الأمن الوحدة الخامسة: إدارة المخاطر والاستجابة للحوادث

- تقييم المخاطر الأمنية لنشر أنظمة IoT.
- وضع خطة الاستجابة للحوادث الأمنية في بيئات IoT.
- اكتشاف الاختراقات والاستجابة السريعة لها.
- التحقيق الجنائي الرقمي في حوادث IoT.
- التحديثات الأمنية وإدارة دورة حياة الجهاز الآمنة.
- المعايير واللوائح (مثل ETSI EN ٣٠٣ ٦٤٥).
- IoT Security). مستقبل أمن إنترنت الأشياء (AI, Blockchain في

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:

يبتكرون نماذج أمنية مستدامة لا والترابط المتزايد بينها، كيف يمكن للمطورين في ظل الانتشار الهائل لأجهزة إنترنت الأشياء البيانات التهديدات المستقبلية وتُنشئ منظومة IoT مرنة تقتصر على معالجة نقاط الضعف الحالية، بل تتوقع والمهندسين أن عبر الأجيال القادمة من الأجهزة الذكية؟ وآمنة تحافظ على الخصوصية وتضمن سلامة

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

مصممًا خصيصًا لمواجهة الأمن السيبراني لإنترنت الأشياء (IoT) والأجهزة تتميز هذه الدورة بتركيزها المتخصص والعميق على من تناول الأمن السيبراني بشكل عام، نغوص في التحديات الأمنية في هذا المجال سريع التطور. بدلاً الذكية، مما يوفر محتوى ودراسات حالة الاتصالات والمنصات السحابية. تقدم الدورة ورش عمل التطبيق العملي لـأمن عتاد وبرمجيات IoT، وتأمين نركز على التعامل مع الخصوصية واقعية لـهجمات على أنظمة IoT، مما يمنح المشاركين عملية تتضمن محاكاة الاختراقات لنجاح أي نظام IoT. إنها ليست مجرد دورة نظرية، وإدارة دورة حياة الجهاز الآمنة، وهي جوانب حاسمة خبرة عملية مباشرة. وموثوقة. IoT أمن إنترنت الأشياء قادرين على تصميم ونشر أنظمة بل هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في آمنة