الدورة التدريبية: أمن الحوسبة الطرفية (Edge Computing Security) للشركات الصناعية

مايو ٢٠٢٦ ٠٨ - ٠٤

كوالالمبور

(للشخص الواحد) € ٥٢٠٠

Ref: #CYB3696_273658

مقدمة الدورة التدريبية / لمحة عامة:

الصناعية الذكية الطرفية أو ما يعرف بـEdge Computing، حجر مع التوسع الهائل في التحول الرقمي، أصبحت الحوسبة التقنية معالجة البيانات بالقرب من مصدرها، مما وإنترنت الأشياء الصناعي (.(IIoTتتيح هذه الزاوية في تمكين العمليات ومُعقدة، مما يجعل ومع ذلك، فإن هذا التوزيع الواسع للأجهزة والنقاط يقلل من زمن الانتقال ويزيد من كفاءة العمليات. الطرفية يمكن أن يعطل خطوط حماية هذه الأنظمة تحديًا بالغ الأهمية. إن أي هجوم الطرفية يفتح ثغرات أمنية جديدة تقدم هذه الدورة التدريبية المتخصصة لمهندسي الإنتاج، ويهدد السلامة العامة، ويسبب خسائر مالية سيبراني على الحوسبة في هذه الدورة العمليات، المعرفة والمهارات اللازمة لـتأمين الأنظمة الصناعية، متخصصي الأمن السيبراني، ومديري ضخمة. سيكتسب المشاركون القدرة على مفاهيم أمنEdge Computing ، التهديدات الشائعة، البنية التحتية الطرفية. سنتناول خطط استباقية لحماية البيانات الصناعية. تهدف تحديد نقاط الضعف، تطبيق ضوابط أمنية قوية، ووضع واستراتيجيات الحماية. إلى أحدث المعايير مما يضمن أن المؤسسات الصناعية تكون دائمًا في الدورة إلى بناء كوادر متخصصة في الأمن الصناعي، بارزين مثل البروفيسور ديفيد إتش. وأفضل الممارسات الدولية، مع الاستفادة من إسهامات طليعة الدفاع. يستند المحتوى أمن أنظمة التحكم الصناعي. يقدمBIG BEN Training كولسن (David H. Coulson)، المعروف بأعماله في خبراء أكاديميين آمنة وموثوقة. الصناعة من بناء هذه الدورة لتمكين قادة Center

بيئة تشغيلية

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

مهندسو الأنظمة الصناعية.

- مديرو الأمن السيبراني.
- مهندسو الشبكات التشغيلية (OT).
- مهندسو إنترنت الأشياء الصناعي (IIoT).
- المتخصصون في أمن المعلومات.
- مديرو العمليات والإنتاج.

القطاعات والصناعات المستهدفة:

- قطاع الصناعات التحويلية.
- قطاع الطاقة والنفط والغاز.
- قطاع الرعاية الصحية.
- الجهات الحكومية وما في حكمها.
- قطاع الاتصالات.
- قطاع النقل والخدمات اللوجستية.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- إدارة العمليات التشغيلية (OT).
- إدارة تقنية المعلومات.
- إدارة الإنتاج.
- إدارة المخاطر.

أهداف الدورة التدريبية:

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

- فهم مفهوم الحوسبة الطرفية ومخاطرها الأمنية.
- القدرة على تحديد التهديدات التي تستهدف أنظمة Edge.
- تأمين الأجهزة الطرفية والاتصالات.
- تطبيق ضوابط أمنية على إنترنت الأشياء الصناعي (IIoT).
- وضع سياسات أمنية متكاملة لبيئات OT وIT.
- الاستجابة للحوادث الأمنية في الأنظمة الصناعية.
- الامتثال للمعايير الأمنية الخاصة بالقطاع.

منهجية الدورة التدريبية:

من خلال مصممة لتمكين المشاركين من فهم وتطبيق استراتيجيات تعتمد هذه الدورة التدريبية منهجية تفاعلية وعملية، الصناعية، وورش العمل التطبيقية، دراسات الحالة الواقعية لـهجمات سيبرانية على أمن الحوسبة الطرفية. سيتمكن المتدربون IT تتضمن المنهجية مناقشات متعمقة حول الفرق بين أمن من ممارسة تأمين الأجهزة الطرفية وتحليل المخاطر. البنية التحتية على التفكير في كيفية بناء الصناعي. سيتم التركيز على الجانب الاستباقي للأمن، والتحديات الأمنية لإنترنت الأشياء، OTو هذه الدورة لتعزيز الخبرة الأمنية لدى العاملين في دفاعات قوية ومرنة. يقدم BIG BEN Training Center وتشجيع المشاركين القطاع الصناعي وضمان مستقبل رقمي آمن.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

والأمن الصناعي الوحدة الأولى: أساسيات الحوسبة الطرفية ((Edge

- مقدمة إلى الحوسبة الطرفية ومكوناتها.
- الفرق بين Edge و Cloud Computing.
- التهديدات السيبرانية على الأنظمة الصناعية.
- التحديات الأمنية الفريدة لـ Edge Computing.
- مفاهيم إنترنت الأشياء الصناعي (IIoT).
- أهمية تأمين Edge Computing للشركات.
- الوعي بالهجمات المتقدمة (APTs).

الوحدة الثانية: تأمين الأجهزة الطرفية والبيانات

- تأمين الأجهزة الطرفية (Endpoints).
- المصادقة والترخيص للأجهزة.
- تشفير البيانات على الأجهزة وفي الشبكة.
- إدارة الثغرات الأمنية للأجهزة.
- تأمين الاتصالات بين الأجهزة والشبكة.
- التحكم في الوصول إلى البيانات.
- مراقبة الأداء والتهديدات.

الوحدة الثالثة: استراتيجيات أمن الشبكة الطرفية

- أمن الشبكات في بيئة Edge.
- تجزئة الشبكات (Network Segmentation).
- أمن السحابة الطرفية (Edge Cloud Security).
- تأمين واجهات البرمجة (APIs).
- أنظمة كشف الاختراقات (IDS) والوقاية منها (IPS).
- تأمين البنية التحتية لشبكات 5G.
- بناء جدران حماية قوية.

الوحدة الرابعة: حوكمة الأمن والاستجابة للحوادث

- وضع سياسات أمنية متكاملة.
- إدارة المخاطر الأمنية في بيئة Edge.
- بناء خطة للاستجابة للحوادث الصناعية.
- التحقيق في الحوادث الأمنية في الأنظمة التشغيلية (OT).
- التعافي من الهجمات واستمرارية الأعمال.
- الامتثال للمعايير الدولية (ISA/IEC ٦٢٤٤٣).
- التدريب على الوعي الأمني.

الوحدة الخامسة: مستقبل الأمن في الحوسبة الطرفية

- دور الذكاء الاصطناعي في حماية Edge.
- أمن سلاسل التوريد الرقمية.
- استراتيجيات الأمن الاستباقي.
- دمج الأمن في تصميم الأنظمة (Security by Design).
- المرونة السيبرانية في البيئة الصناعية.
- التعاون مع مجتمع الأمن السيبراني.
- التطور المستقبلي لـ Edge Computing.

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:

بل تُنشئ الصناعي، كيف يمكن للمؤسسات أن تبتكر استراتيجيات في ظل التوسع السريع للحوسبة الطرفية في القطاع من التعافي بسرعة من الهجمات مع نظامًا بيئيًا آمنًا وشاملاً، وتضمن الخصوصية، أمنية لا تقتصر على حماية الأجهزة فحسب، الحفاظ على الابتكار المستمر في العمليات التشغيلية؟ وتُمكّن المؤسسة

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

الفريدة في الطرفية (Edge Computing)، مما يوفر محتوى مصممًا تتميز هذه الدورة بتركيزها المتخصص على أمن الحوسبة في التطبيق العملي لتأمين الأجهزة القطاع الصناعي. بدلاً من تناول الأمن السيبراني خصيصًا لمواجهة التحديات الأمنية على متكاملة لإنترنت الأشياء الصناعي (.(IIoT تقدم الطرفية، وحماية الاتصالات، ووضع استراتيجيات بشكل عام، نغوص قوية. نركز على الترابط بين البنية التحتية الصناعية، مع تحليل مفصل لنتائجها الدورة دراسات حالة واقعية لهجمات سيبرانية مما يضمن أن المشاركين سيخرجون بخبرة عملية قابلة أمن IT و OT والاستراتيجيات الاستباقية للأمن، وكيفية بناء دفاعات مستقبل الصناعة. تدريبي مكثف يهدف إلى بناء متخصصين في الأمن للتطبيق. إنها ليست مجرد دورة نظرية، بل هي برنامج السيبراني قادرين على حماية