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

#CYB3696

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

مقدمة الدورة التدريبية / لمحة عامة:

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

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

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:

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

- 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:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الحوسبة الطرفية (Edge) والأمن الصناعي

- مقدمة إلى الحوسبة الطرفية ومكوناتها.
- الفرق بين Edge وCloud 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 G5.
- 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 62443).
- 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:

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

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص على أمن الحوسبة الطرفية (Edge Computing)، مما يوفر محتوى مصممًا خصيصًا لمواجهة التحديات الأمنية الفريدة في القطاع الصناعي. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لـتأمين الأجهزة الطرفية، وحماية الاتصالات، ووضع استراتيجيات متكاملة لـإنترنت الأشياء الصناعي (IIoT). تقدم الدورة دراسات حالة واقعية لـهجمات سيبرانية على البنية التحتية الصناعية، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية. نركز على الترابط بين أمن IT وOT والاستراتيجيات الاستباقية 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 الصناعة.