الدورة التدريبية: أمن أنظمة التحكم الصناعية (ICS/SCADA) للمنشآت الحيوية



13 - 17 ديسمبر 2026
عمان
3800 € (للشخص الواحد)
Ref: #CYB1940_397372

مقدمة الدورة التدريبية / لمحة عامة:

تُعد أنظمة التحكم الصناعية (ICS/SCADA) عصب المنشآت الحيوية مثل محطات الطاقة، شبكات المياه، وخطوط النفط والغاز. تتعرض هذه الأنظمة لتهديدات سيبرانية متزايدة، مما يجعل تأمينها أولوية قصوى لضمان استمرارية الخدمات الأساسية وحماية البنية التحتية الوطنية. تقدم هذه الدورة التدريبية المتخصصة للمهندسين والفنيين والمديرين العاملين في القطاعات الصناعية والحيوية المعرفة والمهارات اللازمة لفهم تحديات أمن ICS/SCADA، وتطبيق أفضل الممارسات الأمنية، والوقاية من الهجمات السيبرانية التي تستهدف هذه الأنظمة الحساسة. سنتناول في هذه الدورة الهندسة المعمارية لأنظمة ICS/SCADA، نقاط الضعف الشائعة، واستراتيجيات الدفاع المتقدمة. سيكتسب المشاركون القدرة على تقييم المخاطر الأمنية، تنفيذ ضوابط الحماية، والاستجابة للحوادث التي قد تؤثر على العمليات الصناعية. تهدف الدورة إلى بناء كوادر متخصصة في أمن التشغيل (OT Security). يستند المحتوى إلى أحدث المعايير الصناعية وأطر العمل الأمنية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور ستيف كيرني (Steve Kuni)، المعروف بأعماله في أمن الأنظمة الصناعية والتحكم الآلي. يقدم BIG BEN Training Center هذه الدورة لتعزيز مرونة المنشآت الحيوية ضد التهديدات السيبرانية المعقدة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو التحكم الآلي وأنظمة SCADA.
- متخصصو الأمن السيبراني في القطاع الصناعي.
- مديرو العمليات في المنشآت الحيوية.
- مديرو تكنولوجيا المعلومات والتشغيل (IT/OT).
- فنيو الصيانة والتشغيل في الصناعات التحويلية.
- مدققو الأنظمة الصناعية.

القطاعات والصناعات المستهدفة:

- قطاع الطاقة (كهرباء، نفط، غاز).
- قطاع المياه والصرف الصحي.
- الصناعات التحويلية (بما في ذلك التصنيع الذكي).
- قطاع النقل (سكك حديد، مطارات).
- الصناعات الكيميائية والبتروكيماوية.
- الهيئات الحكومية وما في حكمها، خاصة تلك المشرفة على البنية التحتية الحرجة.

الأقسام المؤسسية المستهدفة:

- إدارة التشغيل والصيانة (OT).
- إدارة تقنية المعلومات (IT).
- إدارة الأمن السيبراني.
- إدارة المخاطر والسلامة.
- إدارة المشاريع (لمشاريع الأنظمة الصناعية).

أهداف الدورة التدريبية:

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

- فهم مفاهيم أنظمة التحكم الصناعية (ICS/SCADA) وأهمية تأمينها.
- تحديد نقاط الضعف والتهديدات الشائعة التي تستهدف أنظمة التشغيل.
- تطبيق مبادئ الأمن السيبراني على بيئة التحكم الصناعي.
- القدرة على تصميم وتنفيذ حلول أمنية لـ ICS/SCADA.
- إدارة المخاطر الأمنية وتقييم الثغرات في الأنظمة الصناعية.
- الاستجابة الفعالة للحوادث السيبرانية التي تؤثر على العمليات الصناعية.
- الامتثال للمعايير واللوائح الأمنية الخاصة بالمنشآت الحيوية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية وتطبيقية، مصممة خصيصًا لتلبية احتياجات تأمين أنظمة التحكم الصناعية (ICS/SCADA). سيتمكن المتدربون من خلال ورش العمل العملية ودراسات الحالة الواقعية لهجمات على أنظمة صناعية، من فهم كيفية تطبيق إجراءات الأمن السيبراني في بيئات التشغيل الحساسة. تتضمن المنهجية مناقشات تفاعلية حول التحديات الفريدة لأمن OT، والفروق بين أمن IT وأمن OT. سيتم التركيز على التحليل العميق للهجمات الصناعية مثل Stuxnet، وكيفية بناء دفاعات متعددة الطبقات. يقدم BIG BEN Training Center هذه الدورة لتزويد المشاركين بالمهارات اللازمة لحماية المنشآت الحيوية وضمان استمرارية العمليات الصناعية بأمان وفعالية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة إلى أنظمة التحكم الصناعية وأمنها

- مقدمة إلى أنظمة التحكم الصناعية (ICS/SCADA) وPLC.
- مكونات أنظمة ICS وهندستها المعمارية.
- أهمية أمن ICS/SCADA للمنشآت الحيوية.
- التهديدات السيبرانية الفريدة التي تواجه أنظمة التشغيل.
- الفروقات بين أمن تقنية المعلومات (IT) وأمن تقنية التشغيل (OT).
- المخاطر التشغيلية ومخاطر السلامة من الهجمات السيبرانية.
- أمثلة على حوادث أمن ICS/SCADA.

الوحدة الثانية: تقييم المخاطر وإدارة الضعف في ICS/SCADA

- مبادئ تقييم المخاطر الأمنية لأنظمة ICS.
- تحديد نقاط الضعف في مكونات ICS/SCADA.
- تحليل التهديدات ونقاط الضعف الخاصة بالبيئات الصناعية.
- وضع خطة إدارة المخاطر الأمنية لـ OT.
- تنفيذ اختبارات الاختراق وفحص الثغرات في أنظمة التحكم.
- أدوات وتقنيات تقييم المخاطر.
- تقارير تقييم المخاطر الأمنية.

الوحدة الثالثة: ضوابط الأمن السيبراني لأنظمة التحكم الصناعية

- تصميم شبكات آمنة لأنظمة ICS (Zones and Conduits).
- تأمين جدران الحماية (Firewalls) وأنظمة IDS/IPS في بيئات OT.
- إدارة الوصول والتحكم به في أنظمة ICS.
- تشفير الاتصالات في الشبكات الصناعية.
- أمن الأجهزة الطرفية والتحكم في الوسائط القابلة للإزالة.
- تأمين البروتوكولات الصناعية (Modbus, DNP3).
- إدارة التكوينات الآمنة لـ ICS.

الوحدة الرابعة: الاستجابة للحوادث وإدارة الأزمات في بيئات OT

- وضع خطة الاستجابة للحوادث الأمنية في أنظمة ICS.
- اكتشاف الحوادث السيبرانية في بيئات التشغيل.
- إجراءات الاحتواء والاستئصال والتعافي من الهجمات الصناعية.
- التحقيق الجنائي الرقمي في حوادث OT.
- التواصل الفعال أثناء الأزمات التي تؤثر على المنشآت الحيوية.
- استمرارية الأعمال والتعافي من الكوارث في القطاع الصناعي.
- التعامل مع التهديدات المتقدمة المستمرة (APTs).

الوحدة الخامسة: الامتثال والمعايير وتأمين المستقبل في ICS/SCADA

- المعايير واللوائح الأمنية الخاصة بـ ICS/SCADA (مثل NIST SP 800-82, ISA/IEC 62443).
- المتطلبات التنظيمية لأمن المنشآت الحيوية.
- التدقيق الأمني والامتثال في بيئات OT.
- بناء ثقافة أمنية للعاملين في المنشآت الصناعية.
- التحديات الناشئة في أمن ICS/SCADA (مثل IoT الصناعي).
- الذكاء الاصطناعي والتعلم الآلي في أمن OT.
- مستقبل أمن أنظمة التحكم الصناعية.

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 الترابط المتزايد بين أنظمة تقنية المعلومات (IT) وأنظمة تقنية التشغيل (OT)، وكيف يمكن للمؤسسات الصناعية أن تبني استراتيجية أمن سيبراني موحدة وفعالة، لا تقتصر على فصل الشبكات، بل تدمج أفضل الممارسات من كلا المجالين لإنشاء دفاع شامل ضد الهجمات المعقدة التي تستهدف المنشآت الحيوية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على أمن أنظمة التحكم الصناعية (ICS/SCADA)، مما يوفر محتوى مصممًا خصيصًا لحماية المنشآت الحيوية. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التحديات والحلول الأمنية الفريدة لبيئات التشغيل (OT). تقدم الدورة دراسات حالة واقعية لهجمات سيبرانية صناعية، مثل Stuxnet، مع تحليل مفصل لنتائجها وكيفية بناء دفاعات قوية ضدها. نركز على التقارب بين IT وOT، وتطبيق المعايير الصناعية مثل ISA/IEC 62443. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي عملي يهدف إلى بناء مهندسين وفنيين أمنيين قادرين على حماية البنية التحتية الحيوية من التهديدات السيبرانية المتطورة وضمان استمرارية العمليات الصناعية.