الدورة التدريبية: أمن أنظمة التحكم الصناعي (ICS Security) للمنشآت الحيوية



26 - 30 اكتوبر 2026
كاليفورنيا
7900 € (للشخص الواحد)
Ref: #ERE6610_364976

مقدمة الدورة التدريبية / لمحة عامة:

أصبح أمن أنظمة التحكم الصناعي (ICS Security) في المنشآت الحيوية تحديًا بالغ الأهمية في ظل تزايد التهديدات السيبرانية وتأثيرها المحتمل على البنية التحتية الحيوية مثل محطات الطاقة، شبكات المياه، وخطوط النفط والغاز. إن ضمان حماية أنظمة ICS من الهجمات السيبرانية ليس فقط مسألة تقنية، بل هو ضرورة وطنية وأمنية لضمان استمرارية الخدمات الأساسية وسلامة الأرواح والممتلكات. تُقدم هذه الدورة التدريبية المتخصصة من BIG BEN Training Center منهجًا شاملاً يغطي أساسيات أمن ICS، من فهم نقاط الضعف الفريدة في هذه الأنظمة إلى تطوير وتنفيذ استراتيجيات دفاعية قوية. سيتعلم المشاركون كيفية تحديد المخاطر، تطبيق أفضل الممارسات الأمنية، والاستجابة للحوادث السيبرانية بفعالية. يشدد الأكاديمي المعروف Ronald Krutz في كتابه "Securing SCADA Systems" على الفروقات الجوهرية بين أمن تكنولوجيا المعلومات (IT Security) وأمن أنظمة التحكم الصناعي (OT Security)، مؤكدًا على الحاجة إلى نهج متخصص لحماية هذه الأنظمة. يلتزم BIG BEN Training Center بتزويد المشاركين بالمعرفة والمهارات اللازمة لتأمين أنظمة التحكم الصناعي، وتمكينهم من حماية الأصول الحيوية من التهديدات المتطورة، وبالتالي المساهمة في بناء بنية تحتية رقمية أكثر مرونة وأمانًا.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو أمن المعلومات.
- مهندسو أنظمة التحكم الصناعي (ICS).
- مديرو تكنولوجيا المعلومات والتشغيل (IT/OT).
- مهندسو الشبكات الصناعية.
- محللو الأمن السيبراني.
- مسؤولو الامتثال والتدقيق.
- المديرون الفنيون في المنشآت الحيوية.
- المختصون في إدارة المخاطر.

القطاعات والصناعات المستهدفة:

- قطاع الطاقة (كهرباء، نفط، غاز).
- قطاع المياه والصرف الصحي.
- الصناعات التحويلية الثقيلة.
- النقل واللوجستيات.
- الاتصالات السلكية واللاسلكية.
- البنية التحتية الحيوية.
- القطاع الحكومي والدفاع.
- الهيئات الحكومية وما في حكمها.

الأقسام المؤسسية المستهدفة:

- إدارة أمن المعلومات.
- قسم تكنولوجيا التشغيل (OT).
- إدارة المخاطر والامتثال.
- قسم الهندسة والتحكم.
- إدارة العمليات.
- قسم البنية التحتية.
- إدارة السلامة والصحة المهنية.

أهداف الدورة التدريبية:

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

- فهم المبادئ الأساسية لأمن أنظمة التحكم الصناعي (ICS Security).
- تحديد الفروقات بين أمن تكنولوجيا المعلومات (IT) وأمن تكنولوجيا التشغيل (OT).
- تحليل التهديدات ونقاط الضعف الفريدة في أنظمة ICS.
- تطبيق إطار عمل أمني شامل لحماية أنظمة التحكم الصناعي.
- تنفيذ أفضل الممارسات في أمن الشبكات الصناعية.
- تأمين مكونات أنظمة ICS (PLC, RTU, HMI, SCADA).
- تطوير خطط الاستجابة للحوادث السيبرانية في بيئة ICS.
- استخدام أدوات وتقنيات الرصد الأمني لأنظمة التحكم.
- الامتثال للمعايير واللوائح الدولية لأمن ICS.
- بناء ثقافة الوعي الأمني داخل المنشأة.

منهجية الدورة التدريبية:

يُقدم BIG BEN Training Center هذه الدورة بمنهجية تدريبية متعمقة وعملية، تركز على تزويد المشاركين بالخبرة المباشرة في أمن أنظمة التحكم الصناعي. تجمع المنهجية بين المحاضرات النظرية التي تغطي مفاهيم أمن ICS، وورش العمل التطبيقية التي تتيح للمشاركين محاكاة هجمات سيبرانية على بيئات ICS افتراضية، وتطبيق استراتيجيات الدفاع. سيتمكن المشاركون من تحليل سجلات الأحداث، واستخدام أدوات الكشف عن التهديدات، وتكوين جدران الحماية الصناعية، وتنفيذ سياسات التحكم في الوصول. تُقدم دراسات حالة واقعية لأحدث الهجمات السيبرانية على المنشآت الحيوية وكيفية الاستجابة لها، مما يعزز فهم المشاركين للتحديات الفعلية. يتم تشجيع النقاشات الجماعية وتبادل الخبرات بين المشاركين، مما يثري الفهم ويسهم في بناء رؤى جديدة حول حماية البنية التحتية الحيوية. يقدم المدربون، وهم خبراء في مجال الأمن السيبراني الصناعي، توجيهات فردية وتغذية راجعة مستمرة لضمان اكتساب المشاركين للمهارات اللازمة لتأمين أنظمة التحكم الصناعي بفعالية. يهدف هذا النهج إلى تأهيل المشاركين ليكونوا قادة في مجال أمن ICS، قادرين على حماية الأصول الأكثر أهمية للمجتمعات.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أنظمة التحكم الصناعي والتهديدات

- مقدمة إلى أنظمة التحكم الصناعي (ICS) وأنواعها (SCADA, DCS, PLC).
- الفروقات بين أمن تكنولوجيا المعلومات (IT) وأمن تكنولوجيا التشغيل (OT).
- الهيكل المعماري لأنظمة ICS ونقاط الضعف.
- التهديدات السيبرانية الشائعة التي تستهدف ICS.
- دوافع المهاجمين وأساليبهم.
- تأثير الهجمات السيبرانية على المنشآت الحيوية.
- المعايير واللوائح الدولية لأمن ICS (NIST, IEC 62443).

الوحدة الثانية: تقييم المخاطر ونقاط الضعف في ICS

- منهجيات تقييم المخاطر لأنظمة ICS.
- تحديد الأصول الحيوية ونقاط الضعف.
- تحليل الثغرات الأمنية في البروتوكولات الصناعية.
- اختبار الاختراق (Penetration Testing) لبيئات ICS.
- تقنيات اكتشاف التهديدات المتقدمة.
- التعامل مع نقاط الضعف المتعلقة بالبشر.
- أدوات تقييم المخاطر وتحليل الثغرات.

الوحدة الثالثة: دفاعات الشبكة الصناعية وتأمين الأنظمة

- تصميم شبكات ICS آمنة (التجزئة، المناطق الأمنية).
- جدران الحماية الصناعية (Industrial Firewalls).
- أنظمة كشف ومنع التسلل (IDS/IPS) لOT.
- تأمين بروتوكولات الاتصال الصناعية.
- إدارة الوصول والتحكم في الهوية.
- تأمين الأجهزة الطرفية (Endpoints) في ICS.
- تشفير البيانات في بيئات ICS.

الوحدة الرابعة: حماية مكونات ICS وتطبيقاتها

- تأمين وحدات التحكم المنطقية القابلة للبرمجة (PLC).
- حماية وحدات التحكم عن بعد (RTU).
- تأمين واجهات المشغل البشري (HMI).
- إدارة التصحيحات والتحديثات في أنظمة ICS.
- أمن التطبيقات والبرمجيات في بيئة ICS.
- التكوينات الآمنة للأنظمة الصناعية.
- التعامل مع الثغرات الأمنية الخاصة بالموردين.

الوحدة الخامسة: الاستجابة للحوادث والتعافي من الكوارث

- خطوات الاستجابة للحوادث السيبرانية في ICS.
- فرق الاستجابة للحوادث (CSIRT) الصناعية.
- جمع الأدلة الجنائية الرقمية في بيئات OT.
- خطط التعافي من الكوارث واستمرارية الأعمال.
- التدريبات والمحاكاة لسيناريوهات الهجوم.
- بناء الوعي الأمني للمشغلين.
- التنسيق مع الجهات الحكومية والخاصة.

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 التزايد المستمر للتهديدات السيبرانية وتطور تقنيات الهجوم، كيف يمكن للمنظمات الحفاظ على مستوى عالٍ من أمن أنظمة التحكم الصناعي (ICS) مع الأخذ في الاعتبار قيود الموارد ومتطلبات التشغيل المستمر؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتقديمها منهجًا شاملاً وعمليًا في أمن أنظمة التحكم الصناعي (ICS Security)، وهو ما يميزها عن الدورات التي قد تركز على جوانب نظرية أو تقنية محدودة. نحن نُقدم تدريبًا مكثفًا يغطي ليس فقط الأدوات والتقنيات، بل أيضًا الفروقات الجوهرية بين أمن IT وأمن OT، وتقييم المخاطر، والاستجابة للحوادث، وهي جوانب حاسمة لحماية المنشآت الحيوية. ما يجعل دورتنا فريدة هو التركيز على الجانب العملي من خلال ورش العمل والمحاكاة التي تضع المشاركين في سيناريوهات هجوم ودفاع واقعية، مما يضمن اكتسابهم لمهارات قابلة للتطبيق مباشرة في بيئات ICS. كما تُقدم الدورة دراسات حالة لأحدث التهديدات وأفضل الممارسات العالمية، مع التركيز على الامتثال للوائح وبناء ثقافة أمنية. إن هذا المزيج من المحتوى التقني المتعمق، والتدريب العملي المكثف، والالتزام بمعايير الأمن العالمية، يجعل هذه الدورة ضرورية لكل من يسعى للتميز في تأمين أنظمة التحكم الصناعي وحماية البنية التحتية الحيوية للمستقبل.