الدورة التدريبية: تأمين البنية التحتية الحيوية والتحكم الصناعي (OT/ICS Security) المتقدم



14 - 18 ديسمبر 2026
كوالالمبور
5200 € (للشخص الواحد)
Ref: #SM9645_340539

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التطور المتسارع لأنظمة التحكم الصناعي وتزايد الترابط بين التقنيات التشغيلية (OT) وتقنية المعلومات (IT)، أصبح تأمين البنية التحتية الحيوية والتحكم الصناعي (OT/ICS Security) المتقدم ضرورة قصوى لضمان استمرارية الخدمات الأساسية وحماية الأصول الوطنية. هذه الدورة التدريبية المتخصصة مصممة لتزويد المهندسين، الفنيين، ومديري الأمن بالمعرفة والمهارات المتقدمة اللازمة لتأمين أنظمة التحكم الصناعي والأنظمة التشغيلية ضد التهديدات السيبرانية المتزايدة والمعقدة. سنتعمق في فهم الثغرات الأمنية الفريدة لهذه الأنظمة، وكيفية تطبيق ضوابط أمنية فعالة، وتطوير خطط استجابة للحوادث المصممة خصيصًا لبيئات OT/ICS. تستند الدورة إلى أعمال خبراء أكاديميين بارزين في مجال أمن الأنظمة الصناعية، مثل البروفيسور Snorre H. Aunet، الذي يُعرف بأبحاثه في أمن أنظمة التحكم. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين المهنيين من حماية البنية التحتية الحيوية، وتقليل المخاطر التشغيلية، وضمان سلامة وأمان العمليات الصناعية المعقدة. سيركز التدريب على الجوانب العملية والتطبيقية، مع تقديم سيناريوهات واقعية ودراسات حالة وتمارين محاكاة، لمساعدة المشاركين على تطبيق المفاهيم النظرية في بيئات عملهم الحقيقية، وتعزيز قدراتهم على مواجهة التحديات الأمنية بفعالية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو أنظمة التحكم الصناعي (ICS).
- مهندسو التشغيل (OT).
- متخصصو الأمن السيبراني الصناعي.
- مديرو الأمن في قطاعات البنية التحتية الحيوية.
- مديرو تقنية المعلومات (IT) الذين يتعاملون مع أنظمة OT.
- مدققو الأمن الصناعي.
- المسؤولون عن الامتثال في القطاعات الصناعية.

القطاعات والصناعات المستهدفة:

- قطاع الطاقة (كهرباء، نفط وغاز).
- قطاع المياه والصرف الصحي.
- قطاع التصنيع الثقيل والعمليات الصناعية.
- قطاع النقل (سكك حديد، مطارات، موانئ).
- قطاع الاتصالات.
- الجهات الحكومية ذات الصلة بالبنية التحتية الحيوية.
- المؤسسات الدفاعية.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- قسم الهندسة والعمليات.
- إدارة تقنية المعلومات والتحكم الصناعي.
- إدارة المخاطر والامتثال.
- قسم السلامة.
- التدقيق الداخلي.
- الصيانة والتشغيل.

أهداف الدورة التدريبية:

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

- فهم الفروقات الأساسية بين أمن تقنية المعلومات وأمن التقنيات التشغيلية.
- تحديد وتقييم المخاطر الأمنية في أنظمة التحكم الصناعي.
- تطبيق أطر ومعايير الأمن الخاصة بأنظمة OT/ICS (مثل IEC 62443، NIST SP 800-82).
- تأمين مكونات شبكات التحكم الصناعي وأنظمة SCADA.
- اكتشاف الحوادث الأمنية في بيئات OT والاستجابة لها.
- تنفيذ حلول أمنية مخصصة لأنظمة التحكم الصناعي.
- تطوير خطط استمرارية الأعمال والتعافي من الكوارث في بيئات OT.
- تعزيز الوعي الأمني للموظفين العاملين على الأنظمة الصناعية.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية على منهجية تفاعلية وتطبيقية مكثفة، تهدف إلى تزويد المشاركين بفهم عميق ومهارات عملية في مجال تأمين البنية التحتية الحيوية والتحكم الصناعي (OT/ICS Security) المتقدم. تبدأ المنهجية بمحاضرات متخصصة يقدمها خبراء ذوو خبرة واسعة في أمن الأنظمة الصناعية، يليها جلسات نقاش حيوية لتبادل الخبرات والتحديات الفريدة لبيئات OT/ICS. تركز الدورة بشكل كبير على دراسات الحالة الواقعية، حيث يقوم المشاركون بتحليل سيناريوهات هجمات سيبرانية على أنظمة تحكم صناعي، وتقييم الثغرات، وتطوير استراتيجيات للحماية والاستجابة. تتضمن المنهجية ورش عمل تطبيقية ومختبرات افتراضية، تتيح للمتدربين تكوين ضوابط أمنية لأنظمة SCADA، وتنفيذ حلول أمنية في شبكات التحكم الصناعي، ومحاكاة الاستجابة للحوادث في بيئات OT. يشجع BIG BEN Training Center العمل الجماعي والتعاون بين المتدربين لتعزيز التفكير النقدي وقدرات حل المشكلات تحت الضغط. يتم تقديم تغذية راجعة فردية ومستمرة لضمان تحقيق أقصى استفادة من الدورة. تهدف هذه المنهجية إلى تمكين المشاركين من العودة إلى مؤسساتهم وهم مسلحون بالمعرفة والأدوات والخبرة العملية اللازمة لحماية البنية التحتية الحيوية وضمان استمرارية وسلامة العمليات الصناعية المعقدة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة في أمن أنظمة التحكم الصناعي والبنية التحتية الحيوية

- الفرق بين أمن تقنية المعلومات (IT) والتقنيات التشغيلية (OT).
- بنية أنظمة التحكم الصناعي (ICS) وأنواعها (SCADA، DCS، PLC).
- التهديدات والهجمات الفريدة على أنظمة OT/ICS.
- الأهمية الاستراتيجية لتأمين البنية التحتية الحيوية.
- المعايير والإرشادات الأمنية لأنظمة OT/ICS (مثل NIST SP 800-82).
- نموذج طبقات Purdue وأهميته في أمن OT.
- أمثلة تاريخية للهجمات على أنظمة التحكم الصناعي.

الوحدة الثانية: تقييم المخاطر وتحديد الثغرات في بيئات OT/ICS

- منهجيات تقييم المخاطر لأنظمة التحكم الصناعي.
- تحديد الثغرات الأمنية في مكونات OT/ICS.
- تقنيات فحص الثغرات (Vulnerability Scanning) واختبار الاختراق (Penetration Testing) في بيئات OT.
- إدارة التصحيحات (Patch Management) في أنظمة OT.
- تأمين الأجهزة والبرمجيات في الأنظمة الصناعية.
- أدوات وتقنيات تحليل المخاطر.
- التعامل مع الأجهزة القديمة (Legacy Systems).

الوحدة الثالثة: تصميم وتنفيذ حلول الأمن لأنظمة OT/ICS

- تقسيم الشبكات (Network Segmentation) في بيئات OT.
- تكوين جدران الحماية الصناعية (Industrial Firewalls).
- أنظمة كشف التسلل (IDS) ومنعه (IPS) لأنظمة OT.
- إدارة الهوية والوصول (IAM) في أنظمة التحكم الصناعي.
- تشفير البيانات في بيئات OT.
- تأمين الاتصالات والبروتوكولات الصناعية.
- أمن السحابة في سياق OT/ICS.

الوحدة الرابعة: الاستجابة للحوادث والتحقيق الجنائي في بيئات OT/ICS

- دورة حياة الاستجابة للحوادث في أنظمة التحكم الصناعي.
- اكتشاف الحوادث الأمنية في بيئات OT (anomaly detection).
- إجراءات الاحتواء والإزالة في الأنظمة الصناعية.
- جمع الأدلة الجنائية الرقمية من أنظمة OT/ICS.
- التحليل الجنائي للبرمجيات الخبيثة الصناعية.
- إعادة بناء الأنظمة بعد الحوادث.
- التواصل وإعداد التقارير بعد الحوادث الصناعية.

الوحدة الخامسة: الحوكمة، الامتثال، والتوجهات المستقبلية لأمن OT/ICS

- أطر الحوكمة والامتثال لأمن البنية التحتية الحيوية (مثل IEC 62443).
- تطوير سياسات وإجراءات أمن OT/ICS.
- التوعية والتدريب الأمني للموظفين في البيئات الصناعية.
- اختبار خطط استمرارية الأعمال والتعافي من الكوارث.
- الاتجاهات المستقبلية في أمن OT/ICS (مثل الذكاء الاصطناعي، إنترنت الأشياء الصناعي).
- التعاون الدولي في أمن البنية التحتية الحيوية.
- التحديات والفرص في حماية الأنظمة 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 التوسع المستمر للترابط الرقمي في الأنظمة الصناعية، كيف يمكن للمهندسين والمختصين في أمن OT/ICS أن يبتكرون حلولاً أمنية تحافظ على سلامة العمليات التشغيلية دون المساس بمرونة الإنتاج وكفاءته؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على تأمين البنية التحتية الحيوية والتحكم الصناعي (OT/ICS Security) المتقدم، وهو مجال يتطلب فهمًا فريدًا يختلف عن أمن تقنية المعلومات التقليدي. نحن نقدم رؤى متخصصة حول التحديات الأمنية المعقدة التي تواجه الأنظمة الصناعية، مع التركيز على أطر ومعايير الأمن المصممة خصيصًا لبيئات OT/ICS. تعتمد الدورة على منهجية تطبيقية مكثفة، تتضمن دراسات حالة واقعية وتمارين محاكاة لأنظمة تحكم صناعي، مما يمنح المشاركين خبرة عملية لا تقدر بثمن في بيئة تدريبية آمنة. يضمن المحتوى الأكاديمي المتقدم، المقدم من BIG BEN Training Center، أن يكون المشاركون على اطلاع بأحدث التهديدات والحلول الأمنية في هذا المجال الحيوي. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى بناء قدراتهم ليصبحوا خبراء قادرين على حماية البنية التحتية الحيوية، وضمان سلامة العمليات الصناعية، وتعزيز مرونة المؤسسات في مواجهة الهجمات السيبرانية المعقدة.