الدورة التدريبية: الأمن السيبراني لأنظمة التحكم الصناعي في النفط والغاز OT/ICS وتأمين البنية التحتية الحيوية



16 - 20 نوفمبر 2026
برلين
5800 € (للشخص الواحد)
Ref: #OG5527_329978

مقدمة الدورة التدريبية / لمحة عامة:

تُعد أنظمة التحكم الصناعي (ICS) والتكنولوجيا التشغيلية (OT) عصب العمليات الحيوية في قطاع النفط والغاز، حيث تضمن استمرارية الإنتاج وسلامة العاملين والأصول. في ظل التحديات المتزايدة للتهديدات السيبرانية، أصبح تأمين هذه الأنظمة أمرًا بالغ الأهمية لضمان استقرار الطاقة العالمية. تقدم هذه الدورة التدريبية الشاملة من BIG BEN Training Center رؤى متعمقة حول أحدث المفاهيم والاستراتيجيات في مجال الأمن السيبراني لأنظمة التحكم الصناعي في قطاع النفط والغاز. نهدف إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لحماية البنية التحتية الحيوية من الهجمات السيبرانية المعقدة. تتناول الدورة تحليل المخاطر، وتطبيق أفضل الممارسات الأمنية، والاستجابة للحوادث، مع التركيز على خصوصية بيئات OT/ICS. يتبنى هذا البرنامج نهجًا تعليميًا شاملاً يغطي الجوانب النظرية والعملية، مستلهمًا من أعمال خبراء رائدين في المجال مثل الدكتور جو أندرسون (Dr. Joe Anderson)، الذي أسهم بشكل كبير في فهم أمن الأنظمة الصناعية من خلال مؤلفاته مثل كتاب "Cybersecurity for Industrial Control Systems". سيتعلم المشاركون كيفية بناء دفاعات قوية ضد التهديدات المتطورة التي تستهدف أنظمة PLC، DCS، SCADA، وغيرها من مكونات OT الحيوية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مدراء أمن المعلومات والمخاطر.
- مهندسو أنظمة التحكم الصناعي.
- متخصصو تكنولوجيا المعلومات والتشغيل.
- مدراء العمليات والإنتاج في قطاع النفط والغاز.
- المسؤولون عن الامتثال واللوائح التنظيمية.
- فنيو الصيانة والتشغيل المسؤولون عن الأنظمة الحساسة.
- فرق الاستجابة للحوادث السيبرانية.

القطاعات والصناعات المستهدفة:

- صناعة النفط والغاز (استكشاف، إنتاج، تكرير، نقل).
- قطاع الطاقة والطاقة المتجددة.
- قطاع المياه والصرف الصحي.
- الصناعات التحويلية الثقيلة.
- البنية التحتية الحيوية.
- الهيئات الحكومية وما في حكمها.

الأقسام المؤسسية المستهدفة:

- إدارات أمن المعلومات والسيبرانية.
- إدارات الهندسة والعمليات.
- إدارات تكنولوجيا المعلومات والاتصالات.
- إدارات المخاطر والامتثال.
- إدارات الإنتاج والتشغيل.
- إدارات السلامة والصحة المهنية.

أهداف الدورة التدريبية:

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

- فهم التحديات الأمنية الفريدة لأنظمة التحكم الصناعي في قطاع النفط والغاز.
- تحديد وتقييم المخاطر السيبرانية المحتملة التي تستهدف بيئات OT/ICS.
- تطوير وتنفيذ استراتيجيات دفاعية فعالة لحماية البنية التحتية الحيوية.
- تطبيق أفضل الممارسات والمعايير الدولية لأمن أنظمة SCADA وDCS.
- إدارة حوادث الأمن السيبراني والاستجابة لها بفعالية لتقليل التأثير.
- فهم أهمية تقسيم الشبكات واستخدام الجدران النارية الصناعية.
- تطبيق سياسات الوصول الآمن ومصادقة المستخدمين في بيئات OT.
- تحليل الثغرات الأمنية في أجهزة وبرمجيات التحكم الصناعي.
- تصميم وتنفيذ حلول أمنية متكاملة لأنظمة ICS.
- مواكبة أحدث التهديدات والتقنيات في مجال الأمن السيبراني الصناعي.
- تقييم مستوى النضج الأمني لأنظمة التحكم.
- تطوير خطط التعافي من الكوارث واستمرارية الأعمال.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية من BIG BEN Training Center منهجية تعليمية تفاعلية وشاملة، مصممة لتمكين المشاركين من اكتساب فهم عميق ومهارات عملية في الأمن السيبراني لأنظمة التحكم الصناعي في قطاع النفط والغاز. تتضمن المنهجية مجموعة متنوعة من الأساليب التعليمية لضمان أقصى استفادة، بدءًا من المحاضرات التفاعلية التي تقدم المفاهيم الأساسية والنظريات المتقدمة، وصولاً إلى دراسات الحالة الواقعية التي تُحلل سيناريوهات الهجمات السيبرانية الحقيقية في بيئات OT/ICS وكيفية التصدي لها. يتم التركيز بشكل كبير على العمل الجماعي من خلال ورش العمل التطبيقية، حيث يُتاح للمشاركين فرصة لتطبيق المعرفة المكتسبة في تصميم وتنفيذ حلول أمنية، وإجراء تقييمات للمخاطر، وتطوير خطط الاستجابة للحوادث. كما تتضمن الدورة جلسات تفاعلية للنقاش المفتوح وتبادل الخبرات بين المشاركين والمدربين، مما يعزز الفهم ويشجع على التفكير النقدي. يتم تقديم تغذية راجعة مستمرة لضمان تحقيق أهداف التعلم وتطوير المهارات المطلوبة لحماية البنية التحتية الحيوية. هذه المنهجية المتكاملة تضمن أن يكتسب المشاركون فهمًا شاملاً وتطبيقًا عمليًا لأحدث استراتيجيات الأمن السيبراني الصناعي.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني لأنظمة التحكم الصناعي OT/ICS.

- مقدمة إلى أنظمة التحكم الصناعي (ICS) والتكنولوجيا التشغيلية (OT)
- الفروقات الرئيسية بين أمن تكنولوجيا المعلومات (IT) وأمن تكنولوجيا التشغيل (OT)
- مكونات وأنواع أنظمة ICS (SCADA, DCS, PLC) في قطاع النفط والغاز
- لمحة تاريخية عن الهجمات السيبرانية الكبرى على البنية التحتية الحيوية
- أهمية تأمين أنظمة OT/ICS في صناعة النفط والغاز
- التهديدات السيبرانية الشائعة التي تواجه أنظمة التحكم الصناعي
- مفهوم "التقارب IT/OT" وتحدياته الأمنية

الوحدة الثانية: تحليل المخاطر وإدارة الثغرات في بيئات OT/ICS.

- مفاهيم تحليل المخاطر الخاصة بأنظمة التحكم الصناعي
- تحديد الأصول الحيوية وتقييمها في قطاع النفط والغاز
- منهجيات تقييم المخاطر (مثل NIST CSF, ISA/IEC 62443)
- إدارة الثغرات الأمنية واكتشافها في مكونات OT/ICS
- التعامل مع الثغرات المعروفة وغير المعروفة (Zero-day exploits)
- تقييم تأثير الهجمات السيبرانية المحتملة على العمليات التشغيلية
- تطوير سجل المخاطر وخطط التخفيف

الوحدة الثالثة: استراتيجيات الدفاع السيبراني وتأمين الشبكات الصناعية.

- تأمين الشبكات الصناعية وتقسيمها (Segmentation)
- جدران الحماية الصناعية (Industrial Firewalls) وأنظمة كشف التسلل (IDS)
- التحكم في الوصول (Access Control) وإدارة الهوية في بيئات OT
- تشفير الاتصالات والبروتوكولات الصناعية
- تأمين الأجهزة الطرفية والمحطات العاملة
- تطبيق مبادئ "الدفاع في العمق" (Defense in Depth)
- الحماية من البرمجيات الخبيثة الموجهة لأنظمة ICS

الوحدة الرابعة: الاستجابة للحوادث والتعافي من الكوارث في OT/ICS.

- تطوير خطة الاستجابة للحوادث السيبرانية في بيئات OT/ICS
- التعرف على الحوادث وجمع الأدلة الرقمية
- تحليل الحوادث والاستجابة الأولية
- احتواء الاختراقات وتخفيف الأضرار
- إعادة الأنظمة إلى وضعها الطبيعي والتعافي من الكوارث
- التواصل وإعداد التقارير بعد الحادث
- الدروس المستفادة والتحسين المستمر لخطط الاستجابة

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

- المعايير واللوائح الدولية لأمن أنظمة التحكم الصناعي (ISA/IEC 62443, NIST SP 800-82)
- أهمية الامتثال في قطاع النفط والغاز
- الحوكمة الأمنية وإدارة المخاطر على مستوى المؤسسة
- التدريب والتوعية بأمن OT/ICS للعاملين
- التهديدات الناشئة والتوجهات المستقبلية في الأمن السيبراني الصناعي (مثل IoT, AI/ML)
- تحديات أمن سلسلة التوريد (Supply Chain Security) في OT
- بناء ثقافة أمنية قوية داخل المؤسسة

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:

كيف يمكن للمؤسسات تحقيق توازن فعال بين متطلبات الإنتاجية والسلامة التشغيلية ومتطلبات الأمن السيبراني الصارمة في بيئات أنظمة التحكم الصناعي؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتركيزها العميق والمتخصص على الأمن السيبراني في أنظمة التحكم الصناعي (OT/ICS) ضمن سياق قطاع النفط والغاز، وهو ما يميزها عن الدورات العامة. يقدم BIG BEN Training Center محتوى أكاديميًا وعمليًا يغطي أحدث التحديات والحلول في هذا المجال شديد الحساسية. نبرز الجوانب العملية من خلال تحليل دراسات حالة واقعية لهجمات سيبرانية مؤثرة على البنية التحتية الحيوية، مما يوفر للمشاركين رؤى حقيقية حول التهديدات وكيفية التصدي لها. بدلاً من مجرد سرد الأدوات، نركز على استراتيجيات الدفاع المتكاملة وتطوير خطط الاستجابة للحوادث، مما يمكن المتدربين من بناء قدرات دفاعية مستدامة. تعتمد الدورة على أحدث المعايير واللوائح العالمية، مما يضمن حصول المشاركين على معرفة قابلة للتطبيق مباشرة في بيئات عملهم المعقدة. هذا المزيج من التخصص، والواقعية، والمنهجية الأكاديمية التطبيقية يجعل هذه الدورة متميزة في إعداد الخبراء لمواجهة تحديات الأمن السيبراني الصناعي بكفاءة وفعالية.