



الدورة التدريبية: الأمن السيبراني التشغيلي والصناعي IEC 62443 OT

Ref: #CYB83105607



مقدمة الدورة التدريبية / لمحة عامة:

لم تعد المصانع ومحطات الطاقة ومرافق المياه وشبكات النفط والغاز معزولة عن العالم الرقمي كما كانت في الماضي، فقد أدى التقارب المتسارع بين تقنية المعلومات IT والتقنية التشغيلية OT إلى فتح أبواب جديدة أمام التهديدات السيبرانية التي يمكن أن توقف خطوط الإنتاج، وتعطل الخدمات الحيوية، وتعرض سلامة البشر والبيئة للخطر. ومن هنا تأتي هذه الدورة التدريبية لتقدم رحلة متكاملة من الألف إلى الياء في الأمن السيبراني التشغيلي وأمن الصناعة، انطلاقاً من فهم بنية أنظمة التحكم الصناعي مثل SCADA وDCS وPLC، وصولاً إلى تطبيق سلسلة معايير IEC 62443 بوصفها الإطار الدولي الأكثر اعتماداً لحماية أنظمة الأتمتة والتحكم الصناعي طوال دورة حياتها. ويستند المحتوى إلى أعمال مرجعية بارزة، من أهمها كتاب Industrial Network Security للمؤلفين Joel Thomas Langill وEric D. Knapp، الذي يشرح بعمق مفاهيم الدفاع المتعدد الطبقات، والمناطق والقنوات Zones and Conduits، ومستويات الأمان Security Levels. وسيتعلم المشاركون كيفية إجراء تقييم مخاطر الأمن السيبراني الصناعي وفق IEC 62443-3-2، وتحديد مستويات الأمان المستهدفة، وبناء نظام إدارة الأمن السيبراني وفق IEC 62443-2-1، وتقييم متطلبات الأنظمة والمكونات وفق IEC 62443-3-3 وIEC 62443-4-2. ويقدم BIG BEN Training Center هذه الدورة لمساعدة المؤسسات على سد الفجوة بين فرق الهندسة وفرق الأمن السيبراني، وتعزيز المرونة التشغيلية، وبناء برنامج مستدام لحماية البنية التحتية الحرجة يوازن بين متطلبات السلامة واستمرارية التشغيل وحماية الأصول الصناعية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو وأخصائيو أمن أنظمة التحكم الصناعي OT وICS.
- مهندسو التحكم والأتمتة والأجهزة الدقيقة.
- مسؤولو أنظمة SCADA وDCS وPLC.
- أخصائيو أمن المعلومات المنتقلون إلى بيئات التقنية التشغيلية.
- مدراء المصانع ومدراء العمليات والصيانة.
- مدراء أمن المعلومات CISO ومدراء الأمن السيبراني.
- أخصائيو المخاطر والامتثال والحوكمة في المؤسسات الصناعية.
- مهندسو السلامة الوظيفية وسلامة العمليات.
- مكاملو الأنظمة ومصممو حلول الأتمتة الصناعية.
- مهندسو الشبكات المسؤولون عن الشبكات الصناعية وشبكات المصانع.
- المدققون الداخليون والخارجيون لضوابط الأمن الصناعي.



القطاعات والصناعات المستهدفة:

- قطاع النفط والغاز بمراحله الاستكشافية والنقل والتكرير ذات متطلبات السلامة العالية.
- شركات توليد الكهرباء ونقلها وتوزيعها.
- مرافق معالجة المياه والصرف الصحي وتوزيعها.
- مصانع البتروكيماويات والكيماويات ومصافي التكرير.
- المصانع وخطوط الإنتاج التي تتبنى تقنيات الصناعة 4.0.
- مصانع الأدوية وعلوم الحياة الخاضعة لمتطلبات الجودة والامتثال الصارمة.
- قطاع النقل والموانئ والمطارات وأنظمة إشارات السكك الحديدية.
- قطاع التعدين والمعادن والصناعات الثقيلة.
- المباني الذكية ومراكز البيانات وأنظمة إدارة المرافق.
- الهيئات الحكومية والجهات التنظيمية وسلطات البنية التحتية الوطنية الحرجة وما في حكمها.

الأقسام المؤسسية المستهدفة:

- إدارات الأمن السيبراني الصناعي والتقنية التشغيلية.
- إدارات أمن المعلومات والدفاع السيبراني.
- إدارات الهندسة والأتمتة.
- إدارات العمليات والإنتاج.
- إدارات الصيانة والموثوقية.
- إدارات الصحة والسلامة والبيئة.
- إدارات المخاطر والامتثال.
- إدارات التدقيق الداخلي.
- إدارات المشتريات وسلاسل الإمداد المسؤولة عن الموردين الصناعيين.
- إدارات البنية التحتية لتقنية المعلومات والشبكات.



أهداف الدورة التدريبية:

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

- شرح بنية أنظمة التحكم الصناعي والفروق الجوهرية بين أولويات أمن IT وأمن OT.
- تفسير هيكل سلسلة معايير IEC 62443 وأدوار أجزائها المختلفة.
- إجراء تقييم منهجي لمخاطر الأمن السيبراني التشغيلي وفق IEC 62443-3-2.
- تحديد المناطق والقنوات الأمنية ومستويات الأمان المستهدفة للبيئات الصناعية.
- تصميم بنية دفاع متعدد الطبقات للشبكات الصناعية باستخدام التقسيم والوصول الآمن عن بعد.
- تطبيق المتطلبات الأساسية ومتطلبات أمن الأنظمة الواردة في IEC 62443-3-3.
- بناء نظام إدارة للأمن السيبراني الصناعي والمحافظة عليه وفق IEC 62443-2-1.
- تقييم أمن الموردين والمكونات باستخدام IEC 62443-4-1 و IEC 62443-4-2.
- إعداد خطط لاكتشاف الحوادث الصناعية والاستجابة لها والتعافي منها بما يحمي السلامة واستمرارية التشغيل.
- وضع خارطة طريق عملية للامتثال لمعيار IEC 62443 والتحسين المستمر.

منهجية الدورة التدريبية:

تعتمد هذه الدورة على منهجية تطبيقية قائمة على السيناريوهات الواقعية، تمزج بين الشرح المنظم على يد خبراء متخصصين والتطبيق العملي المكثف، بحيث يغادر المشاركون وهم يمتلكون مهارات قابلة للنقل المباشر إلى بيئاتهم الصناعية. يبدأ كل يوم تدريبي بعروض مركزة تشرح مبادئ الأمن السيبراني التشغيلي والأجزاء ذات الصلة من معيار IEC 62443 بلغة واضحة وعملية، تليها نقاشات موجهة تربط كل مفهوم بالتحديات التشغيلية الفعلية التي يواجهها المشاركون في مؤسساتهم. وتتيح دراسات الحالة المفصلة لحوادث سيبرانية صناعية موثقة للمشاركين تحليل مسارات الهجوم وتحديد الضوابط الغائبة، واقتراح إجراءات تصحيحية مستندة إلى المعيار. ويحتل العمل الجماعي موقعاً محورياً في التجربة التدريبية، إذ يعمل المشاركون ضمن مجموعات صغيرة متعددة التخصصات تحاكي التعاون المطلوب بين فرق الهندسة والعمليات والأمن السيبراني، لتنفيذ تمارين مثل رسم المناطق والقنوات لمصنع افتراضي، وتحديد مستويات الأمان المستهدفة، وصياغة أجزاء من نظام إدارة الأمن السيبراني. وتشمل الجلسات التفاعلية محاكاة للاستجابة للحوادث على الطاولة، وورش عمل لتقييم المخاطر، ونقاشات منظمة حول الموازنة بين الأمن والسلامة واستمرارية التشغيل. وطوال البرنامج، يقدم مدبرو BIG BEN Training Center تغذية راجعة مستمرة وبناءة على مخرجات المجموعات والمساهمات الفردية، إلى جانب اختبارات معرفية قصيرة في نهاية كل وحدة لتثبيت النقاط الرئيسية. ويحرص BIG BEN Training Center على ربط كل نشاط بأهداف قابلة للقياس، ليتمكن المشاركون من تطبيق ممارسات IEC 62443 بثقة، والارتقاء بمستوى نضج الأمن السيبراني الصناعي في مؤسساتهم، وتحويل المعرفة المكتسبة إلى قرارات عملية تحمي الأصول والأفراد والعمليات.



خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن السيبراني التشغيلي وأنظمة التحكم الصناعي

- مفهوم التقنية التشغيلية ودورها في البنية التحتية الحرجة.
- مكونات أنظمة التحكم الصناعي مثل SCADA و DCS و PLC و RTU و HMI.
- نموذج Purdue Enterprise Reference Architecture وأهميته الأمنية.
- الفروق الجوهرية بين أولويات وقيود أمن IT وأمن OT.
- بروتوكولات الاتصال الصناعية مثل Modbus و DNP3 و OPC UA و PROFINET.
- تقارب IT و OT واتساع سطح الهجوم الصناعي.
- خريطة التهديدات التشغيلية بما فيها برمجيات الفدية والتهديدات الداخلية والجهات المدعومة من دول.
- الدروس المستفادة من أبرز الحوادث السيبرانية الصناعية.

الوحدة الثانية: فهم سلسلة معايير IEC 62443 وهيكلها

- هدف سلسلة IEC 62443 ونطاقها وتطورها.
- هيكل المعيار عبر الأجزاء العامة والسياسات والإجراءات والأنظمة والمكونات.
- أدوار مالكي الأصول ومكاملي الأنظمة وموردي المنتجات.
- المفاهيم الأساسية مثل المتطلبات الأساسية Foundational Requirements ومستويات الأمان.
- الدفاع المتعدد الطبقات Defense in Depth بوصفه مبدأً توجيهياً للمعيار.
- العلاقة بين IEC 62443 و ISO/IEC 27001 و NIST Cybersecurity Framework.
- ربط متطلبات IEC 62443 بدورة حياة الأتمتة الصناعية.
- المفاهيم الخاطئة الشائعة وتحديات تبني المعيار.



الوحدة الثالثة: تقييم المخاطر والمناطق والقنوات ومستويات الأمان

- منهجية تقييم المخاطر وفق IEC 62443-3-2.
- تحديد النظام قيد الدراسة والأصول الصناعية الحرجة.
- تعريف المناطق والقنوات الأمنية للشبكات الصناعية.
- نمذجة التهديدات وتحليل الثغرات في بيئات OT.
- تقييم العواقب على السلامة والبيئة والإنتاج والسمعة.
- تحديد مستويات الأمان المستهدفة والممكنة والمحققة.
- دمج مخاطر الأمن السيبراني مع تحليل مخاطر العمليات والسلامة الوظيفية.
- توثيق مواصفات متطلبات الأمن السيبراني.

الوحدة الرابعة: بنية الشبكات الصناعية الآمنة والضوابط التقنية

- متطلبات أمن الأنظمة ومستويات الأمان وفق IEC 62443-3-3.
- تقسيم الشبكات والجدران النارية الصناعية والمناطق منزوعة السلاح DMZ.
- الوصول الآمن عن بعد للموردين وفرق الهندسة.
- التعريف والمصادقة والتحكم في الاستخدام للمستخدمين والأجهزة الصناعية.
- إدارة التحديثات ومعالجة الثغرات في البيئات التشغيلية.
- جرد الأصول وإدارة الإعدادات وتقوية الأنظمة.
- المراقبة المستمرة لشبكات OT واكتشاف السلوك غير الطبيعي.
- متطلبات أمن المكونات وفق IEC 62443-4-2 والتطوير الآمن وفق IEC 62443-4-1.

الوحدة الخامسة: إدارة الأمن السيبراني الصناعي والاستجابة للحوادث وخارطة الامتثال

- إنشاء نظام إدارة الأمن السيبراني وفق IEC 62443-2-1.
- الحوكمة والأدوار والمسؤوليات والسياسات الخاصة بأمن OT.
- التوعية الأمنية وتطوير كفاءات فرق الهندسة والعمليات.
- التخطيط للاستجابة للحوادث التشغيلية واكتشافها واحتوائها والتعافي منها.
- استمرارية الأعمال والتعافي من الكوارث في العمليات الصناعية.
- إدارة أمن الموردين وسلاسل الإمداد.
- قياس نضج الأمن السيبراني التشغيلي والاستعداد للتدقيق والتقييم.
- بناء خارطة طريق عملية لتطبيق IEC 62443 والتحسين المستمر.



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:

إذا حققت منشأة صناعية جميع مستويات الأمان التقنية التي يحددها معيار IEC 62443، بينما لا يزال المهندسون وفرق الأمن السيبراني يعترفون بالخطر بطرق مختلفة جذرياً، فهل يمكن لهذه المؤسسة أن تدعي حقاً أنها آمنة، أم أن المرونة التشغيلية الحقيقية تعتمد على الحكم المشترك أكثر من اعتمادها على الامتثال ذاته؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بأنها تتعامل مع الأمن السيبراني التشغيلي بوصفه تخصصاً هندسياً قائماً بذاته، لا مجرد امتداد لأمن تقنية المعلومات التقليدي. فكثير من البرامج التدريبية تركز على الأدوات أو على قوائم امثال مجردة، بينما تبني هذه الدورة فهماً عميقاً لأسباب حاجة البيئات الصناعية إلى طريقة تفكير مختلفة، حيث تحدد السلامة واستمرارية التشغيل والعواقب المادية كل قرار أمني. ولا يكفي المشاركون بالقراءة عن معيار IEC 62443، بل يطبقونه خطوة بخطوة، انتقالاً من تقييم المخاطر وتصميم المناطق والقنوات إلى اختيار مستويات الأمان وبناء نظام الإدارة وتقييم الموردين، وكل ذلك من خلال سيناريوهات صناعية واقعية. وتسد الدورة الفجوة القديمة بين مهندسي التحكم ومتخصصي الأمن السيبراني بوضع المنظورين معاً في التمارين نفسها، مما يشجع على لغة مشتركة وملكية مشتركة للمخاطر. وتوضح الأمثلة العملية المستمدة من قطاعات الطاقة والمياه والتصنيع والنفط والغاز كيف تتطور الهجمات داخل المصانع الحقيقية، وكيف كان يمكن للصواب المصممة جيداً أن تغير النتيجة. ويتوازن العمق الأكاديمي للمحتوى مع الصلة المباشرة ببيئة العمل، فيعود المشاركون بخارطة طريق واضحة يمكنهم عرضها على الإدارة العليا والبدء في تنفيذها فوراً. ويجمع BIG BEN Training Center بين التيسير الاحترافي والتعاون المنظم والتغذية الراجعة المستمرة، لتقديم تجربة تعليمية في الأمن السيبراني الصناعي تعزز الكفاءة الفردية والمرونة المؤسسية، وتؤهل المشاركين ليصبحوا قادة واثقين في تبني معيار IEC 62443 داخل مؤسساتهم.