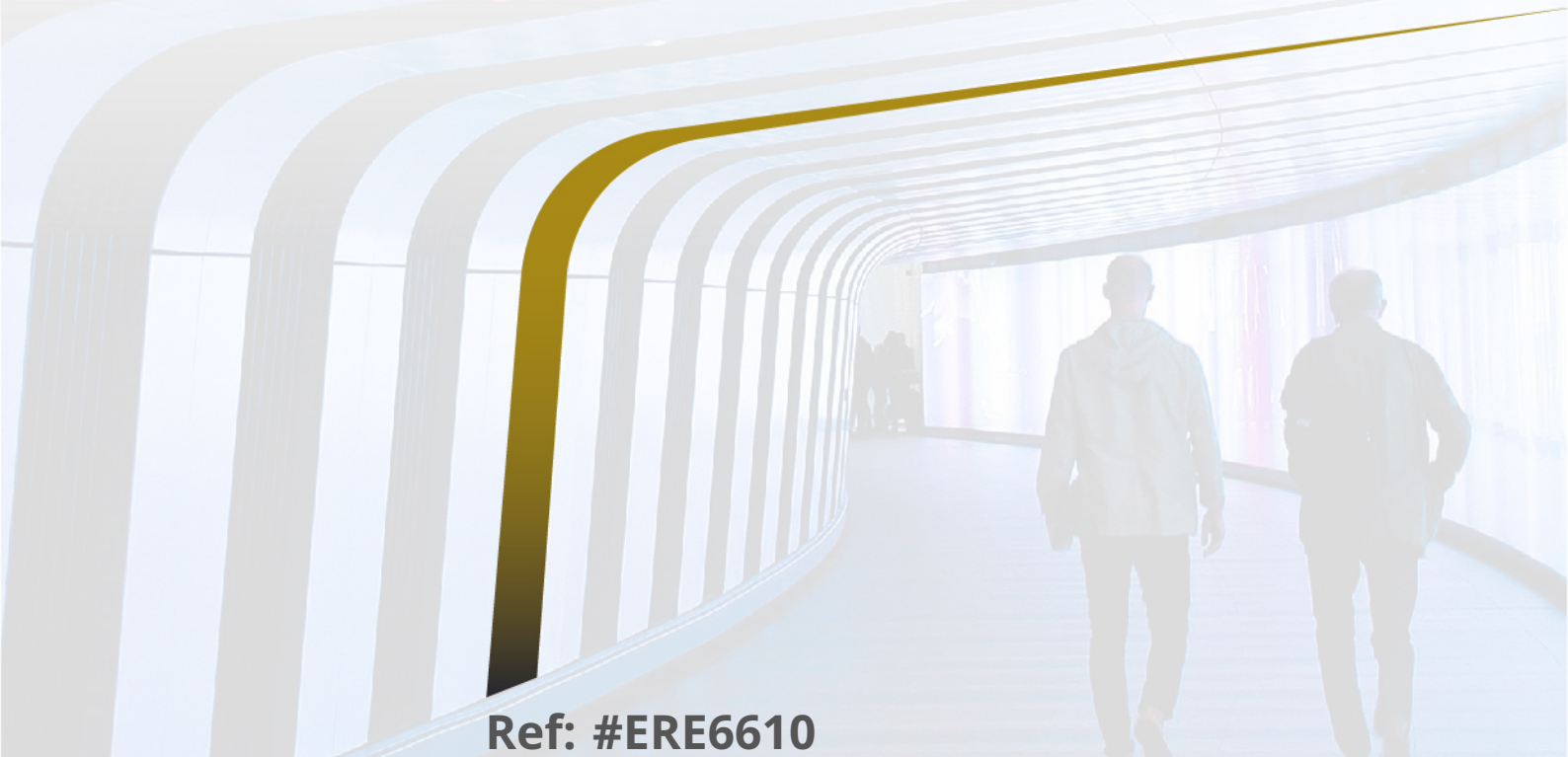
الدورة التدريبية: أمن أنظمة التحكم الصناعي (ICS Security)

للمنشآت الحيوية



Ref: #ERE6610

مقدمة الدورة التدريبية / لمحة عامة:

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

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

والتهديدات الوحدة الأولى: أساسيات أنظمة التحكم الصناعي

- مقدمة إلى أنظمة التحكم الصناعي (ICS) وأنواعها (SCADA, DCS, PLC).
- تكنولوجيا التشغيل (OT): الفروقات بين أمن تكنولوجيا المعلومات (IT) وأمن 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 ٦٢٤٤٣).

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.

الأنظمة الوحدة الثالثة: دفاعات الشبكة الصناعية وتأمين

- تصميم شبكات ICS آمنة (التجزئة، المناطق الأمنية).
- جدران الحماية الصناعية (Industrial Firewalls).
- أنظمة كشف ومنع التسلل (IDS/IPS) لـ OT.
- 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.

الكوارث الوحدة الخامسة: الاستجابة للحوادث والتعافي من

- 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:

التسجيل في الدورة؟ ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل

لا توجد شروط مسبقة.

الإجمالي لساعات الدورة التدريبية؟ كم تستغرق مدة الجلسة اليومية، وما هو العدد

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية. راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

(ICS) مع تقنيات الهجوم، كيف يمكن للمنظمات الحفاظ على مستوى في ظل التزايد المستمر للتهديدات السيبرانية وتطور

المستمر؟ الأخذ في الاعتبار قيود الموارد ومتطلبات التشغيل عالٍ من أمن أنظمة التحكم الصناعي

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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