

دورة شهادة مدير أمن سكادا المعتمد لتأمين أنظ
سكادا

12 – 16 يوليو 2027

فيينا

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة شهادة مدير أمن سكادا المعتمد لتأمين أنظمة سكادا

المرجع: 99107_103600301 **التاريخ:** 12 – 16 يوليو 2027 **المكان:** فيينا **الرسوم:** Euro 7500

نظرة عامة على الدورة:

صُممت دورة شهادة مدير أمن سكادا المعتمد – تأمين أنظمة سكادا لتزويد المشاركين بمعرفة متقدمة في أمن سكادا وممارسات قوية لأمن أنظمة التحكم الصناعي ICS. تعد أنظمة سكادا التحكم الإشرافي وتحصيل البيانات ضرورية لإدارة عمليات الأتمتة الصناعية، ويعد تأمينها ضد التهديدات السيبرانية أمراً بالغ الأهمية. سيتعمق المشاركون في إدارة الأمن السيبراني لأنظمة سكادا، لتعلم الأساليب الأساسية مثل إطار عمل تقييم نقاط الضعف في أنظمة سكادا، واستراتيجيات الدفاع السيبراني الفعالة، وتقنيات إدارة المخاطر المتقدمة.

تدمج هذه الدورة بشكل فريد أفضل الممارسات العملية لأمن سكادا مع الرؤى الاستراتيجية حول إدارة تهديدات الأمن السيبراني لأنظمة سكادا، مما يمكن مديري الأمن من تحسين أطر العمل الأمنية ضمن بيئات الأمن الصناعي. سيكتسب الحاضرون رؤى قابلة للتنفيذ لتحسين التحكم في الوصول، وإدارة المصادقة، وتطبيق المنهجيات القائمة على المعايير معايير الأمن لضمان عمليات آمنة ومرنة. يتوافق هذا البرنامج المنظم بشكل وثيق مع الاتجاهات الحالية في الأمن السيبراني ويلبي الطلب المتزايد على المهنيين المعتمدين القادرين على حماية البنية التحتية الحيوية وتطبيق تقنيات فعالة لتقليل المخاطر في أنظمة سكادا.

AGILE LEADERS
Training Center

الجمهور المستهدف:

- مديرو أمن سكادا
- مشغلو أنظمة التحكم الصناعي ICS
- محللو الأمن السيبراني
- متخصصو أمن الشبكات
- متخصصو أمن التكنولوجيا التشغيلية OT
- مهندسو الأتمتة
- مديرو المخاطر

الإدارات التنظيمية المستهدفة:

- الأمن السيبراني وأمن تكنولوجيا المعلومات
- التكنولوجيا التشغيلية OT
- إدارة المخاطر والامتثال
- الأتمتة والتحكم الصناعي
- الهندسة والصيانة

AGILE LEADERS
Training Center

القطاعات الصناعية المستهدفة:

- الطاقة والمرافق
- النفط والغاز
- التصنيع
- إدارة المياه والنفايات
- النقل
- الصناعات الكيميائية والدوائية

مخرجات الدورة:

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطوير وتنفيذ إطار عمل لتقييم نقاط الضعف في أنظمة سكادا
- إدارة وتحسين التحكم في الوصول في أنظمة سكادا
- تطبيق أفضل الممارسات لإدارة المصادقة
- الإدارة الاستراتيجية لآليات الدفاع السيبراني
- تنفيذ استراتيجيات فعالة للتخفيف من مخاطر أمن سكادا
- تحسين السلامة التشغيلية باستخدام تقنيات أمن الأتمتة الصناعية المتقدمة
- استخدام استراتيجيات حماية أنظمة سكادا لتأمين البنية التحتية الحيوية
- إجراء تقييمات شاملة للمخاطر في أنظمة سكادا

منهجية التدريب:

تجمع منهجية التدريب لدورة شهادة مدير أمن سكادا المعتمد – تأمين أنظمة سكادا بين النظرية والمشاركة العملية، وتعزز التعلم النشط من خلال الجلسات الجماعية التفاعلية، ودراسات الحالة التفصيلية، وجلسات التقييم الشاملة. سيستفيد المشاركون من سيناريوهات واقعية توضح التحديات الحاسمة في الأمن الصناعي والدفاع السيبراني، مما يعزز قدرتهم على تطبيق أفضل ممارسات أمن سكادا المكتسبة بفعالية. تتضمن كل وحدة مناقشات جماعية تركز على تطبيق أطر العمل الأمنية وورش عمل تفاعلية حول إدارة التهديدات وإجراء تقييمات مفصلة لنقاط الضعف في أنظمة سكادا. ستسهل الجلسات التي يقودها الخبراء إتقان المشاركين لإدارة المصادقة والتحكم في الوصول. تمكن حلقات التقييم المستمر والممارسات التأملية الحاضرين من تنفيذ عمليات قوية لإدارة المخاطر بثقة، مما يضمن فهماً عملياً عميقاً للمحتوى.

AGILE LEADERS
Training Center

مجموعة أدوات الدورة:

- دليل عمل رقمي شامل للدورة
- قوائم تحقق ونماذج لأمن سكادا
- أمثلة على أدوات تقييم نقاط الضعف في أنظمة سكادا
- الوصول إلى موارد إلكترونية لإدارة الأمن السيبراني لأنظمة سكادا
- ملفات PDF لدراسات الحالة ورؤى حول إدارة أمن سكادا

جدول أعمال الدورة:

اليوم الأول: مقدمة في أنظمة سكادا والأمن السيبراني

- الموضوع 1: فهم أنظمة سكادا، وتحصيل البيانات، وأمن الأتمتة
- الموضوع 2: أساسيات أمن سكادا
- الموضوع 3: مقدمة في أمن أنظمة التحكم الصناعي ICS ومعايير الأمن الصناعي
- الموضوع 4: أساسيات أمن الشبكات في أنظمة سكادا
- الموضوع 5: دور ومسؤوليات مدير أمن سكادا
- تأمل ومراجعة: مناقشة وتأمل في المفاهيم الأساسية مثل الدفاع السيبراني وأمن الأتمتة

اليوم الثاني: إدارة نقاط الضعف في أنظمة سكادا

- الموضوع 1: تطوير إطار عمل لتقييم نقاط الضعف في أنظمة سكادا
- الموضوع 2: تطبيق إطار عمل أمني لأنظمة سكادا
- الموضوع 3: تقنيات إدارة نقاط الضعف
- الموضوع 4: التطبيقات العملية لإدارة المخاطر
- الموضوع 5: وضع بروتوكولات فعالة للدفاع السيبراني
- تأمل ومراجعة: تلخيص النقاط الرئيسية المكتسبة حول تقنيات تقليل المخاطر في أمن سكادا

اليوم الثالث: تقنيات الأمن المتقدمة

- الموضوع 1: استراتيجيات أمن الأتمتة
- الموضوع 2: استراتيجيات حماية أنظمة سكادا
- الموضوع 3: أفضل الممارسات لتأمين البنى التحتية الحيوية
- الموضوع 4: تطبيق منهجيات أمن التكنولوجيا التشغيلية OT
- الموضوع 5: استكشاف دراسات حالة في الأمن السيبراني لأنظمة سكادا للمشغلين الصناعيين
- تأمل ومراجعة: ترسيخ الرؤى حول إدارة تهديدات الأمن السيبراني لأنظمة سكادا

اليوم الرابع: تطبيق أطر العمل الأمنية

- الموضوع 1: تطوير أطر عمل أمنية شاملة
- الموضوع 2: التدريب على تقييم المخاطر في أنظمة سكادا
- الموضوع 3: تقنيات متقدمة في أمن الأتمتة
- الموضوع 3: تحسين الوضع الأمني من خلال أمن أتمتة العمليات الصناعية
- الموضوع 4: استراتيجيات الاستجابة الفعالة للحوادث في أمن التكنولوجيا التشغيلية OT
- تأمل ومراجعة: تحليل التطبيقات العملية لاستراتيجيات حماية أنظمة سكادا

اليوم الخامس: تأمين البنية التحتية الحيوية

- الموضوع 1: التدريب على أمن البنية التحتية الحيوية
- الموضوع 2: ضمان الإدارة طويلة الأمد للأمن السيبراني لأنظمة سكادا
- الموضوع 3: أفضل الممارسات في الحفاظ على بنية تحتية آمنة لأنظمة سكادا
- الموضوع 4: تقنيات متقدمة في أمن الأتمتة
- الموضوع 5: الاتجاهات والابتكارات المستقبلية في أمن أتمتة العمليات الصناعية
- تأمل ومراجعة: مراجعة نهائية وجلسة استراتيجية باستخدام أفضل ممارسات أمن سكادا

AGILE LEADERS
Training Center

الأسئلة الشائعة:

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

يُفضل أن يكون لدى المشاركين معرفة أساسية بأنظمة سكادا، ومفاهيم الأمن السيبراني الأساسية، وخبرة سابقة في بيئات التكنولوجيا التشغيلية.

كم تبلغ مدة الجلسة اليومية، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تستمر كل جلسة يومية عادةً لمدة تتراوح بين 4 و5 ساعات، شاملة فترات الراحة والأنشطة التفاعلية. تمتد الدورة على مدى أسبوع، بإجمالي يتراوح بين 20 و25 ساعة تدريبية تقريباً.

هل إدارة أمن سكادا هي نفسها إدارة الأمن السيبراني لتكنولوجيا المعلومات؟

لا، فأمن سكادا يعالج بشكل خاص بيئات التكنولوجيا التشغيلية OT والأتمتة الصناعية، ويركز على التحديات الفريدة التي لا توجد عادةً في الأمن السيبراني التقليدي لتكنولوجيا المعلومات.

كيف تختلف هذه الدورة عن دورات أمن سكادا الأخرى:

تجمع دورة شهادة مدير أمن سكادا المعتمد – تأمين أنظمة سكادا بشكل فريد بين الأبعاد الاستراتيجية والتشغيلية لأمن سكادا. على عكس دورات الأمن السيبراني التقليدية، تركز هذه الدورة بشكل مكثف على التحديات المتخصصة في أمن أنظمة التحكم الصناعي ICS، والنهج العملية لأمن الأتمتة، والتطبيقات الواقعية. سيشارك المتدربون بعمق في إنشاء أطر عمل قابلة للتنفيذ مثل إطار عمل تقييم نقاط الضعف في أنظمة سكادا، وتطبيق منهجيات قابلة للتطبيق مباشرة في أدوارهم الوظيفية. تؤكد منهجية التدريب على الجلسات التفاعلية، ودراسات الحالة من مواقف صناعية حقيقية، والمناقشات الجماعية الشاملة، مما يضمن قدرة المشاركين على إدارة تهديدات الأمن السيبراني الصناعية المعقدة بفعالية. تركز هذه الدورة على الرؤى الاستراتيجية طويلة الأمد في استراتيجيات حماية أنظمة سكادا، مع دمجها بالمهارات التقنية للتطبيق الفوري، مما يميزها بشكل واضح عن خيارات التدريب الأخرى المتاحة.