QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1506

دورة الأمن السيبراني الصناعي وأمن تقنيات التشغيل

الأتمتة الصناعية والتقنيات الرقمية
الهندسة الصناعية والصيانة والعمليات

المدة
5 أيام

طريقة التقديم
حضوري

شركة كويست ترينينج

quest-training.com

نظرة عامة على الدورة

تقدم دورة الأمن السيبراني الصناعي وأمن تقنيات التشغيل إطاراً مهنياً متكاملاً لفهم وحماية البيئات الصناعية التي تعتمد على أنظمة التحكم والأتمتة وتقنيات التشغيل. وتركز الدورة على تطوير قدرة المشاركين على تحديد المخاطر السيبرانية التي تواجه المنشآت الصناعية والبنية التحتية الحيوية، وتحليل نقاط الضعف، وتصميم ضوابط أمنية مناسبة تحافظ على استمرارية العمليات وسلامتها وموثوقيتها.

تتناول الدورة الخصائص المختلفة لبيئات تقنيات التشغيل مقارنة ببيئات تقنية المعلومات، مع التركيز على أنظمة التحكم الصناعي، وأنظمة التحكم الإشرافي وتجميع البيانات، وأنظمة التحكم الموزعة، وأجهزة التحكم المنطقية القابلة للبرمجة، وأجهزة القياس والتحكم، وشبكات الاتصالات الصناعية. كما توضح كيفية إدارة الأمن السيبراني في البيئات التي تتطلب تحقيق التوازن بين الحماية السيبرانية ومتطلبات السلامة والتوافر واستمرارية التشغيل.

يركز البرنامج على منهجيات تقييم المخاطر الأمنية في البيئات الصناعية، وتصنيف الأصول، وتحليل التهديدات والثغرات، وتقسيم الشبكات، والتحكم في الوصول، والمراقبة الأمنية، وإدارة التحديثات والتغييرات، وتأمين الوصول عن بُعد، وإدارة الموردين والأطراف الثالثة. كما يتناول الاستجابة للحوادث السيبرانية والتحقيق فيها واستعادة العمليات بعد الحوادث بما يتناسب مع طبيعة المنشآت الصناعية.

ومن خلال التمارين التطبيقية ودراسات الحالة والسيناريوهات الصناعية، يطور المشاركون القدرة على بناء تصور متكامل للمخاطر السيبرانية ووضع ضوابط عملية لحماية بيئات تقنيات التشغيل. وتساعد دورة الأمن السيبراني الصناعي وأمن تقنيات التشغيل المؤسسات الصناعية والجهات الحكومية وشركات النفط والغاز والمرافق والبنية التحتية الحيوية على تعزيز المرونة السيبرانية وتقليل المخاطر التي قد تؤثر في السلامة والتوافر واستمرارية العمليات.

أهداف الدورة

- تحليل مكونات بيئات تقنيات التشغيل وأنظمة التحكم الصناعي وتحديد الأصول الحيوية والمخاطر الأمنية المرتبطة بها خلال اليوم الأول من الدورة.

- تقييم التهديدات والثغرات السيبرانية التي يمكن أن تؤثر في الأنظمة الصناعية وشبكات التشغيل باستخدام منهجية منظمة خلال البرنامج.
- تطوير إطار عملي لتصنيف أصول تقنيات التشغيل وتحديد مستويات المخاطر والأولويات الأمنية.
- تطبيق مبادئ تقسيم الشبكات الصناعية والتحكم في الوصول لتقليل احتمالات الانتشار غير المصرح به داخل البيئة التشغيلية.
- تصميم ضوابط أمنية مناسبة لأنظمة التحكم الصناعي مع مراعاة متطلبات السلامة والتوافر واستمرارية التشغيل.
- تقييم مخاطر الوصول عن بُعد والأطراف الثالثة والموردين وتحديد الضوابط المناسبة للحد من المخاطر.
- تطبيق أساليب عملية لمراقبة الأنشطة الأمنية واكتشاف المؤشرات غير الطبيعية داخل بيئات تقنيات التشغيل.
- تطوير إجراءات للاستجابة للحوادث السيبرانية الصناعية واحتواء الحوادث ودعم استعادة العمليات.
- تقييم ممارسات إدارة التحديثات والتغييرات والنسخ الاحتياطية وإدارة الأصول بهدف تحسين المرونة الأمنية.
- إعداد خطة عملية لتحسين الأمن السيبراني في بيئة صناعية وربط الأولويات الأمنية بأهداف التشغيل واستمرارية الأعمال خلال الورشة الختامية.

الفئة المستهدفة

تستهدف دورة الأمن السيبراني الصناعي وأمن تقنيات التشغيل المتخصصين في الأمن السيبراني وتقنيات المعلومات وتقنيات التشغيل والهندسة والتحكم والأتمتة وإدارة الشبكات وإدارة الأنظمة الصناعية. كما تناسب مهندسي أنظمة التحكم الصناعي ومهندسي الأجهزة والتحكم ومهندسي الأتمتة والشبكات الصناعية ومتخصصي الأمن السيبراني ومديري أمن المعلومات ومتخصصي إدارة المخاطر واستمرارية الأعمال.

وتعد الدورة مناسبة أيضاً لمديري العمليات والصيانة والهندسة والأمن السيبراني وتقنية المعلومات، ومسؤولي أمن المنشآت الصناعية، ومتخصصي أنظمة التحكم، ومديري المشاريع الصناعية، ومسؤولي إدارة الموردين والأطراف الثالثة، والقيادات التنفيذية وصناع القرار في الجهات الحكومية والوزارات والمؤسسات العامة وشركات النفط والغاز والطاقة والمياه والمرافق والمنشآت الصناعية والبنية التحتية الحيوية التي تعتمد على أنظمة

التشغيل والأتمتة والتحكم الصناعي.

مخرجات التعلم

- شرح الفرق بين أمن تقنية المعلومات وأمن تقنيات التشغيل ومتطلبات الحماية الخاصة بالبيئات الصناعية.
- تحديد مكونات أنظمة التحكم الصناعي والأصول التشغيلية الحيوية وتقييم أهميتها الأمنية والتشغيلية.
- تحليل التهديدات والثغرات التي تستهدف أنظمة التحكم والشبكات والأجهزة الصناعية.
- تقييم المخاطر السيبرانية وربطها بتأثيراتها المحتملة على السلامة والتوافر واستمرارية العمليات.
- تصميم مبادئ مناسبة لتقسيم الشبكات الصناعية وعزل الأنظمة الحساسة.
- تطبيق ضوابط إدارة الهوية والوصول والوصول عن بُعد في بيئات تقنيات التشغيل.
- تقييم مخاطر الموردين والأطراف الثالثة وتطوير متطلبات أمنية مناسبة للتعامل معهم.
- تطوير إجراءات للمراقبة والكشف والاستجابة للحوادث السيبرانية في البيئات الصناعية.
- تقييم ممارسات إدارة الأصول والتحديثات والتغييرات والنسخ الاحتياطية من منظور الأمن السيبراني.
- إعداد خطة عملية لتحسين المرونة السيبرانية وأمن تقنيات التشغيل بما يتوافق مع متطلبات المؤسسة التشغيلية.
- المحاور التدريبية:

محاور الدورة

اليوم الأول

أساسيات الأمن السيبراني الصناعي وتقنيات التشغيل

- مفهوم الأمن السيبراني الصناعي وأمن تقنيات التشغيل
- الفروقات بين بيئات تقنية المعلومات وتقنيات التشغيل
- مكونات أنظمة التحكم الصناعي
- أنظمة التحكم الإشرافي وتجميع البيانات
- أنظمة التحكم الموزعة
- أجهزة التحكم المنطقية القابلة للبرمجة وأنظمة القياس والتحكم
- الشبكات والبروتوكولات الصناعية
- تحديد الأصول الصناعية الحيوية وتصنيفها
- المخاطر السيبرانية المرتبطة بالبيئات الصناعية
- التطبيق العملي: رسم خريطة للأصول والأنظمة في بيئة صناعية وتحديد أهم الأصول التي تحتاج إلى حماية

اليوم الثاني

تقييم المخاطر والتهديدات والثغرات في البيئات الصناعية

- منهجيات تقييم مخاطر الأمن السيبراني الصناعي
- تحديد مصادر التهديدات والجهات المهاجمة
- تحليل الثغرات في الأنظمة والأجهزة والشبكات الصناعية
- تقييم تأثير المخاطر على التشغيل والسلامة والإنتاج
- تصنيف الأصول حسب الأهمية والحساسية
- تحليل سيناريوهات الهجمات على أنظمة التحكم الصناعي

اليوم الثاني — تابع

- إدارة مخاطر الأنظمة القديمة وغير القابلة للتحديث
- تحديد الأولويات الأمنية بناءً على مستوى المخاطر
- تطوير سجل مخاطر خاص ببيئة تقنيات التشغيل
- التطبيق العملي: تنفيذ تقييم مخاطر لبيئة صناعية وتحليل السيناريوهات الأكثر تأثيراً

اليوم الثالث

حماية الشبكات والأنظمة الصناعية

- مبادئ تصميم الشبكات الصناعية الآمنة
- تقسيم الشبكات وعزل المناطق الأمنية
- التحكم في تدفق البيانات بين بيئات تقنية المعلومات وتقنيات التشغيل
- إدارة الهوية والصلاحيات والوصول إلى الأنظمة الصناعية
- تأمين الوصول عن بُعد
- حماية الأجهزة والأنظمة الصناعية
- إدارة التحديثات والتغييرات في بيئات التشغيل
- النسخ الاحتياطية واستعادة الأنظمة الحرجة
- أمن الموردين والأطراف الثالثة
- التطبيق العملي: تصميم نموذج حماية لشبكة صناعية وتحديد الضوابط المناسبة لكل منطقة تشغيلية

اليوم الرابع

المراقبة الأمنية والاستجابة للحوادث الصناعية

- مبادئ المراقبة الأمنية في بيئات تقنيات التشغيل
- تحديد السلوكيات والأنشطة غير الطبيعية

اليوم الرابع — تابع

- جمع وتحليل السجلات والأحداث الأمنية
- مؤشرات الاختراق والحوادث في البيئات الصناعية
- الاستجابة للحوادث السيبرانية الصناعية
- احتواء الحوادث وتقليل تأثيرها على العمليات
- التحقيق في الحوادث وتحليل أسبابها
- خطط استمرارية الأعمال والتعافي من الحوادث السيبرانية
- اختبارات الجاهزية والاستجابة للحوادث
- التطبيق العملي: محاكاة حادث سيبراني صناعي وتطوير إجراءات الاكتشاف والاحتواء والاستجابة والتعافي

اليوم الخامس

الحوكمة والمرونة السيبرانية وخطة التحسين

- حوكمة الأمن السيبراني في بيئات تقنيات التشغيل
- السياسات والإجراءات والمسؤوليات الأمنية
- إدارة المخاطر والامتثال والمتطلبات التنظيمية
- إدارة دورة حياة الأصول الصناعية
- قياس مستوى النضج الأمني والمرونة السيبرانية
- تطوير مؤشرات الأداء والمخاطر الأمنية
- إدارة مخاطر الموردين والأطراف الثالثة
- تحديد أولويات مشاريع التحسين الأمني
- تطوير خارطة طريق لتعزيز أمن تقنيات التشغيل
- ورشة ختامية: إعداد خطة متكاملة لتحسين الأمن السيبراني الصناعي والمرونة التشغيلية

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة: https://quest-training.com/courses/industrial-cybersecurity-ot-security-training-course

الموقع الإلكتروني: https://quest-training.com

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440