تأمين أنظمة التحكم الصناعي (ICS) والتقنيات التشغيلية (OT)

الإمارات العربية المتحدة - دبي

12 – 16/ 04 / 2026

مقدمة:

في قلب النهضة الصناعية لعام 2026، تمثل أنظمة التحكم الصناعي (ICS) والتقنيات التشغيلية (OT) الأعصاب الحيوية التي تحرك محطات الطاقة، شبكات المياه، والمصانع الذكية. إن تأمين هذه الأنظمة لم يعد مجرد خيار تقني، بل هو جوهر السيادة الوطنية وحماية استمرارية جودة الحياة. يهدف هذا البرنامج إلى تمكين القادة من أدوات حماية البنية التحتية الحيوية وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في رصد التهديدات السيبرانية-الفيزيائية، مع ضمان أعلى معايير النزاهة والريادة العالمية.

أهداف الدورة:

- استيعاب الفوارق الجوهرية بين أمن المعلومات (IT) وأمن التقنيات التشغيلية (OT) من منظور سيادي.
- تطوير مهارات هندسة "الصمود الصناعي" لمواجهة الهجمات التي تستهدف أنظمة التحكم والسكادا.(SCADA)
- إتقان فن توظيف التوائم الرقمية (Digital Twins) في محاكاة التهديدات واختبار جاهزية المنشآت بنزاهة.
- حوكمة ممارسات الأمن الصناعي لضمان التوازن بين كفاءة الإنتاج ومتطلبات الحماية الوطنية.
- تعزيز السيادة المعلوماتية عبر بناء منظومات رصد وطنية مستقلة تعتمد على تقنيات سيادية.
- تطبيق استراتيجيات القيادة في إدارة الأزمات الصناعية الكبرى وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة الأمن الصناعي والرشاقة في إدارة السيادة التشغيلية

هندسة الحماية الاستباقية وتصفير البيروقراطية في البلاغات

- مفهوم الأمن الصناعي 2026 وأثره على السيادة الوطنية وجودة الحياة والريادة العالمية والنمو.
- مواءمة استراتيجيات التأمين مع مبدأ تصفير البيروقراطية عبر أتمتة رصد الانحرافات التشغيلية.
- تحليل العلاقة بين "سلامة الأصول الصناعية" وبين بناء الثقة والمصداقية الدولية في الاقتصاد الوطني.
- تمرين هندسة الاستباقية لتصميم دورة عمل أمنية تصفّر زمن الاستجابة للحوادث الصناعية بنزاهة وشفافية.

قيادة النزاهة في حوكمة المنشآت الحيوية والريادة الوطنية

- تعزيز السيادة على بروتوكولات التحكم الصناعي لضمان استقلاليتها وتوافقها مع القيم والهوية الوطنية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في إدارة مخاطر "التوقف غير المخطط له."
- بناء ثقافة "الأمان الصناعي كمسؤولية وطنية" وعلاقتها بجودة الحياة والولاء المؤسسي والنمو الشامل.
- صياغة ميثاق أخلاقيات قائد أنظمة OT لدعم النزاهة والقدوة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة رصد التهديدات بالذكاء الاصطناعي

تصفير مخاطر التعطل عبر التحليل السلوكي للآلات والتوائم الرقمية

- توظيف الذكاء الاصطناعي في رصد التغيرات الدقيقة في أداء المحركات والمستشعرات وتصفير احتمالات التخريب.
- حماية "البيانات التشغيلية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنزاهة الرقمية.
- تطبيق الهوية الرقمية للأصول والأنظمة لتصفير الهدر البيروقراطي في إجراءات التدقيق والوصول للشبكات.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحالة أنظمة ICSالوطنية.

حوكمة الأنظمة الخوارزمية والنزاهة في الاستجابة الآلية

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في إصدار "أوامر الإغلاق الطارئ."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الذكاء الاصطناعي لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن الصناعي بنزاهة تامة.

اليوم الثالث :

هندسة الصمود والحياد في إدارة الموارد والشمولية

تصفير البيروقراطية في إدارة سلاسل التوريد التقنية والشمولية

- تحليل مخاطر سلاسل التوريد لأجهزة الـ PLC والمستشعرات وتصفير زمن التحقق من سلامة المكونات.
- تفعيل الرقابة الأخلاقية على عقود الصيانة والتشغيل لضمان الشفافية وحياد النظم الرقمية في النتائج.
- تطبيق تقنيات "العزل الشبكي الذكي (Segmenting) "لتصفير زمن احتواء التهديدات بنزاهة وشفافية.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والتميز.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع مزودي التكنولوجيا لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والنمو.
- تطوير آليات رصد الأثر البيئي والاجتماعي للحوادث السيبرانية الصناعية لضمان النزاهة والعدالة في النتائج.
- بناء سجلات نزاهة رقمية لكل عملية تحديث للأنظمة الحيوية لضمان الشفافية المطلقة والوضوح والريادة.
- تمرين محاكاة لإدارة حوار أمني حول "التطور الصناعي والأمن" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في الأزمات الصناعية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات الصناعية المتسارعة والموازنة بين الإبهار والوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للأنظمة والفرق الفنية لتعزيز مصداقية القرار السيادي عالمياً والريادة والتميز.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة التشغيل لتصفير فرص انتشار الشائعات الرقمية والنزاهة.
- التدقيق الأخلاقي على سلاسل توريد التقنيات التشغيلية لضمان خلوها من الممارسات الضارة والنزاهة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالإنتاج

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الصناعي والسيادة.
- مهارات التواصل الأخلاقي عند حدوث عطل في أنظمة التحكم لضمان استعادة الثقة ببيانات صادقة ونزيهة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والنزاهة والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالبيانات والواقع.

اليوم الخامس :

هندسة الاستجابة السيادية وتصفير البيروقراطية في تأمين أنظمة التحكم الصناعي والتقنيات التشغيلية(OT)

مختبر "النبض السيادي" وإدارة صمود الأنظمة الصناعية تحت التهديد الهجين

- محاكاة "الاختراق الفيزيائي-السيبراني" والسيادة على الأصول: وضع القادة في سيناريو يحاكي هجوماً يستهدف محطة طاقة أو شبكة مياه وطنية، واختبار قدرة "التوائم الرقمية" على عزل الجزء المصاب لحظياً وتفعيل بروتوكول "الحصانة التشغيلية" بنزاهة ووضوح تام لضمان استمرارية الخدمات الأساسية دون توقف.
- تصفير البيروقراطية في "الاستجابة اللحظية للأعطال": تطبيق مسار قرار صفري الإجراءات لتحويل أحمال الطاقة أو تدفقات الموارد بناءً على تحليلات الذكاء الاصطناعي التنبؤية، لضمان حماية المرفق الحيوي في الزمن الحقيقي دون انتظار الاعتمادات الإدارية الورقية التي قد تؤدي إلى أضرار مادية جسيمة.
- هندسة "النزاهة الميدانية" والتحقق البشري السيادي: اختبار مهارة القائد في الموازنة بين مخرجات أنظمة التحليل الآلي للشبكات وبين "الحكمة الهندسية البشرية" لضمان عدم حدوث إغلاقات قسرية غير ضرورية للمرافق، وضمان استقرار جودة الحياة والمصداقية الدولية في ملف أمن الطاقة والخدمات بنزاهة وشفافية مطلقة.
- ورشة "تفكيك صوامع سلاسل التوريد الصناعية": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات السلوكية لتحديد الثغرات في قطع الغيار والبرمجيات الخارجية (مثل PLC)، وتطوير حلول هندسية استباقية لغرس "السيادة التقنية" في المكونات المحلية، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة صناعية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة %.100
- القدرة على هندسة منظومات رصد استباقية رشيقة وسيادية تتوافق مع متطلبات الريادة والتميز العالمية.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي في النتائج.
- بناء سجل ممارسات فضلى في إدارة الذكاء الأمني التشغيلي يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء القطاعات الحيوية (الطاقة، المياه، النفط والغاز، والنقل).
- مسؤولو الأمن السيبراني والتميز المؤسسي وفرق تصفير البيروقراطية في المنشآت الصناعية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بسلامة البنية التحتية الوطنية.
- رؤساء فرق الصيانة الاستراتيجية ومحللو مخاطر التقنيات التشغيلية في الهيئات الاتحادية.

أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أوالخاص.(Expert Panels)
- المختبرات التقنية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)