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

الإمارات العربية المتحدة - دبي

18 – 22/ 01 / 2026

مقدمة:

في قلب النهضة الحكومية الشاملة لعام 2026، تمثل أنظمة التحكم الصناعي (ICS) والتقنيات التشغيلية (OT) "الجهاز الحركي" للدولة؛ فهي التي تدير محطات الطاقة، شبكات المياه، وأنظمة النقل الذكية. إن حماية هذه الأصول لم تعد مجرد مهمة فنية، بل هي جوهر السيادة الوطنية وضمان 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 في استدامة الخدمات الأساسية.

أهداف الدورة:

- استيعاب الفوارق الجوهرية بين أمن المعلومات (IT) وأمن التقنيات التشغيلية (OT) من منظور سيادي وحكومي.
- تطوير مهارات هندسة "الصمود الصناعي" لمواجهة الهجمات التي تستهدف أنظمة السكادا (SCADA)والمستشعرات.
- إتقان فن توظيف التوائم الرقمية (Digital Twins) في محاكاة التهديدات واختبار جاهزية المرافق بنزاهة.
- حوكمة ممارسات الأمن الصناعي لضمان التوازن بين كفاءة الإنتاج وبين متطلبات الحماية الوطنية الصارمة.
- تعزيز السيادة المعلوماتية عبر بناء منظومات رصد وطنية مستقلة تعتمد على تقنيات تشفير 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 التقنية

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

قيادة النزاهة في حوكمة المنشآت الحيوية والريادة الوطنية الشاملة

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

اليوم الثاني :

السيادة التقنية وهندسة رصد التهديدات بالذكاء الاصطناعي

تصفير مخاطر التعطل عبر التحليل السلوكي للآلات والتوائم الرقمية السيادية

- 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 والتميز.
- تطبيق الهوية الرقمية للأصول والأنظمة لتصفير الهدر البيروقراطي في إجراءات التدقيق والوصول للشبكات.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحالة أنظمة ICSالحكومية والنمو.

حوكمة الأنظمة الخوارزمية والنزاهة في الاستجابة الآلية والتحكم

- 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 والنمو.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الذكاء الاصطناعي لضمان المصداقية أمام صانع القرار والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن الصناعي بنزاهة تامة والتميز.

اليوم الثالث :

هندسة الصمود والحياد في إدارة الموارد والشمولية

تصفير البيروقراطية في إدارة سلاسل التوريد التقنية والشمولية الصناعية

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

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي التكنولوجيا لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والتميز.
- 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 الدوليين.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في الأزمات الصناعية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل في الأزمات الصناعية المتسارعة والموازنة بين الإبهار والوقار السيادي الحكومي والنمو.
- 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 والشفافية.
- التدقيق الأخلاقي على سلاسل توريد التقنيات التشغيلية لضمان خلوها من الممارسات الضارة والنزاهة والسيادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالإنتاج

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الصناعي والسيادة والريادة.
- 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 الرقمي والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالبيانات والواقع.

اليوم الخامس :

خارطة الطريق وصناعة القائد الصناعي الرقمي القدوة: من تأمين المستشعرات إلى هندسة السيادة التشغيلية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في أمن التقنيات التشغيلية (OT)

- مصفوفة "النبض اللحظي" للأنظمة السيبرانية-الفيزيائية: تصميم نظام رصد سيادي يعتمد على التحليلات السلوكية لتحويل بيانات أجهزة الـ PLC وأنظمة السكادا إلى "نبضات استراتيجية" تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن رصد "الانحرافات التشغيلية" وضمان اكتشاف محاولات التلاعب بالترددات أو الضغوط الميدانية في مهدها بنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للاستجابة الصناعية المؤتمتة: هندسة مسار قرار "صفري الإجراءات" يسمح للأنظمة الحيوية بتنفيذ عمليات "العزل المنطقي" للمرافق المتضررة فور رصد النبضة الاستراتيجية للتهديد. يضمن هذا البروتوكول استمرارية عمل شبكات المياه والطاقة دون قيود بيروقراطية أو انتظار للاعتمادات البشرية في لحظات الخطر الوشيك.
- حوكمة "النزاهة التشغيلية" والسيادة على البيانات: وضع ضوابط أخلاقية تضمن مطابقة بيانات "التوأم الرقمي" للواقع الميداني، وتفعيل ميثاق "الصدق التقني" في البلاغات الصناعية لضمان استقلال القرار الوطني والوضوح التام أمام صانع القرار بشأن سلامة الأصول الاستراتيجية للدولة.
- مختبر "هندسة الحصانة ضد اختراقات OT/IT": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة صناعية" ناتجة عن تغلغل رقمي في أنظمة التحكم، وكيفية تفعيل "بروتوكول الدفاع المشترك" لحماية خطوط الإنتاج والسيادة الوطنية.

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.

الفئة المستهدفة:

- القيادات العليا ومدراء قطاعات المرافق الحيوية (الطاقة، المياه، النفط، الغاز، والنقل الذكي).
- مسؤولو الأمن السيبراني والتميز المؤسسي وفرق تصفير البيروقراطية في المنشآت الحكومية الكبرى.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بسلامة البنية التحتية الوطنية والسيادة المعلوماتية.
- رؤساء فرق المهام الخاصة ومحللو مخاطر التقنيات التشغيلية في الهيئات الاتحادية والمحلية.

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)