تأمين التقنيات التشغيلية (OT) والبنى التحتية الحيوية الوطنية

الإمارات العربية المتحدة - دبي

18 – 22/ 01 / 2026

مقدمة:

تمثل التقنيات التشغيلية (OT) القلب النابض للبنى التحتية الحيوية من محطات طاقة ومياه وشبكات نقل، وحمايتها هي جوهر السيادة الوطنية. يهدف هذا البرنامج إلى تمكين القادة من أدوات حماية الأنظمة الصناعية والتحكم (ICS/SCADA) وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في مراقبة الأصول المادية، مع ضمان النزاهة والشفافية في إدارة المخاطر السيادية، مما يضمن ريادة الدولة واستقرار جودة الحياة تحت كافة الظروف.

أهداف الدورة:

- استيعاب الفوارق الجوهرية بين أمن تقنية المعلومات (IT) وأمن التقنيات التشغيلية (OT) من منظور سيادي.
- تطوير مهارات هندسة الصمود للبنى التحتية الحيوية باستخدام منهجيات الثقة الصفرية (Zero Trust).
- إتقان فن توظيف التوائم الرقمية والذكاء الاصطناعي في التنبؤ بالأعطال والتهديدات الفيزيائية-السيبرانية.
- حوكمة سلاسل التوريد للتقنيات الصناعية لضمان حماية السيادة المعلوماتية والأصول الوطنية.
- تعزيز السيادة الرقمية عبر بناء بروتوكولات أمنية وطنية خاصة بالأنظمة التشغيلية المحلية.
- تطبيق استراتيجيات القيادة في إدارة الأزمات الكبرى التي تمس الخدمات الأساسية للجمهور بنزاهة.

محتويات الورشة:

اليوم الأول :

فلسفة أمن الـ OT والسيادة على الأصول المادية

هندسة الحماية الفيزيائية الرقمية وتصفير البيروقراطية الرقابية

- مفهوم الأمن القومي المرتبط بالتقنيات التشغيلية والسيادة على أنظمة التحكم الصناعي.
- مواءمة أمن الـ OT مع استراتيجية تصفير البيروقراطية عبر أتمتة الرقابة اللحظية للأصول الميدانية.
- تحليل الفجوة بين أنظمة IT و OTوتصميم بنية تحتية هجينة تضمن النزاهة والريادة العالمية.
- تمرين هندسة الجاهزية لتحديد الأصول الحيوية وتصميم دورات استجابة رشيقة تصفّر زمن التوقف.

قيادة النزاهة في حوكمة أنظمة التحكم(SCADA/ICS)

- تعزيز السيادة على بروتوكولات الاتصال الصناعية لضمان استقلالية الأنظمة الوطنية عن التدخلات الخارجية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في صيانة الأصول وتأمين وصول البيانات.
- بناء ثقافة "الأمان أولاً" وعلاقتها بجودة الحياة والثقة المجتمعية في استدامة الخدمات الأساسية.
- صياغة ميثاق أخلاقيات حارس البنية التحتية السيادي لدعم التميز في كافة المستويات القيادية والميدانية.

اليوم الثاني :

السيادة التقنية وهندسة الرصد التنبؤي للأصول

تصفير مخاطر التخريب عبر التوائم الرقمية والذكاء الاصطناعي

- توظيف الذكاء الاصطناعي في بناء توائم رقمية للمحطات والشبكات تصفّر زمن اكتشاف الاختراقات "الصامتة."
- حماية "البيانات التشغيلية السيادية" عبر تقنيات التشفير الصناعي لضمان موثوقية الأداء والنزاهة.
- تطبيق الهوية الرقمية للأجهزة (Device Identity) لتصفير الهدر البيروقراطي في عمليات التدقيق الميداني.
- تطوير لوحات تحكم سيادية للرصد الأمني والتشغيلي المتكامل بعيداً عن التقارير الورقية التقليدية.

حوكمة الأنظمة الخوارزمية والنزاهة في الصيانة التنبؤية

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في اتخاذ قرارات الإغلاق أو التحويل.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير أعطال الشبكات.
- ترسيخ مفهوم الأمانة في البيانات الميدانية لضمان المصداقية أمام المجتمع والجهات الرقابية العليا.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن الصناعي بنزاهة تامة.

اليوم الثالث :

الحياد والعدالة في استمرارية الخدمات الحيوية

هندسة الحماية الشاملة والشمولية الرقمية في توزيع الموارد

- استخدام التحليلات الذكية لضمان عدالة استمرارية الخدمات (ماء/كهرباء) لجميع فئات المجتمع بنزاهة.
- تفعيل الرقابة الأخلاقية على منصات إدارة الأزمات لضمان الشفافية وحياد البيانات الرقمية في النتائج.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الأمن التشغيلي التي قد تغفل البعد الإنساني.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني للمنشآت لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع مزودي التقنيات العالمية لضمان توافق الأنظمة مع معايير جودة الحياة والسيادة.
- تطوير آليات رصد الأثر الاجتماعي للسياسات الأمنية الصناعية لضمان النزاهة والعدالة في تقديم الخدمة.
- بناء سجلات نزاهة رقمية لكل عملية صيانة أو تحديث أمني لضمان الشفافية المطلقة والوضوح التام.
- تمرين محاكاة لإدارة حوار أمني حول استدامة الخدمات بأسلوب قيادي واثق وملهم للجمهور الواعي.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة في الأزمات الصناعية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات الفيزيائية-السيبرانية والموازنة بين الإبهار التقني وبين الوقار السيادي.
- الرقابة على البصمة الرقمية للالتزام الأمني وأثرها في تعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن الحوادث التقنية لضمان الشفافية وتصفير فرص انتشار الشائعات.
- التدقيق الأخلاقي على سلاسل توريد قطع الغيار والبرمجيات لضمان خلوها من الممارسات غير العادلة.

حصانة البنية التحتية ضد الانتهاكات المعلوماتية والتضليل

- المسؤولية القيادية في التبليغ عن الثغرات التي قد تهدد أمن الشبكات الوطنية الكبرى والسيادة.
- مهارات التواصل الأخلاقي عند حدوث عطل تشغيلي لضمان استعادة الثقة ببيانات صادقة ونزيهة وشفافة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والمهني.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالبيانات.

اليوم الخامس :

هندسة الاستجابة السيادية وتصفير البيروقراطية في تأمين التقنيات التشغيلية (OT) والبنى التحتية الوطنية

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 تحلية مياه أو شبكة طاقة وطنية، واختبار قدرة "التوائم الرقمية" على عزل الجزء المصاب لحظياً وتفعيل بروتوكول "الحصانة التشغيلية" بنزاهة ووضوح تام لضمان استمرارية تدفق الخدمات الأساسية للمجتمع.
- 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 كوارث مادية، مع الحفاظ على الحصانة الرقمية والسيادة الوطنية الكاملة.
- 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، وتطوير حلول هندسية استباقية لغرس "السيادة التقنية" في المكونات المحلية، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار حماية البنية التحتية الموحد".

المخرجات الرئيسية للدورة:

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

الفئة المستهدفة:

- استيعاب الفوارق الجوهرية بين أمن تقنية المعلومات (IT) وأمن التقنيات التشغيلية (OT) من منظور سيادي.
- تطوير مهارات هندسة الصمود للبنى التحتية الحيوية باستخدام منهجيات الثقة الصفرية (Zero Trust).
- إتقان فن توظيف التوائم الرقمية والذكاء الاصطناعي في التنبؤ بالأعطال والتهديدات الفيزيائية-السيبرانية.
- حوكمة سلاسل التوريد للتقنيات الصناعية لضمان حماية السيادة المعلوماتية والأصول الوطنية.
- تعزيز السيادة الرقمية عبر بناء بروتوكولات أمنية وطنية خاصة بالأنظمة التشغيلية المحلية.
- تطبيق استراتيجيات القيادة في إدارة الأزمات الكبرى التي تمس الخدمات الأساسية للجمهور بنزاهة.

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)