أمن إنترنت الأشياء الصناعي (IIoT)

الإمارات العربية المتحدة - دبي

2026 / 11 /12 – 08

مقدمة:

في قلب النهضة الصناعية لعام 2026، يمثل إنترنت الأشياء الصناعي (IIoT) "الجهاز العصبي" للمصانع الذكية والمرافق الحيوية. إن حماية هذه المليارات من المستشعرات والآلات المتصلة لم تعد مجرد مهمة تقنية، بل هي جوهر السيادة الصناعية وضمان استمرارية النمو الوطني. يهدف هذا البرنامج إلى تمكين القادة من أدوات حماية الأنظمة السيبرانية-الفيزيائية، وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في رصد الانحرافات التشغيلية، مع ضمان أعلى معايير النزاهة والريادة العالمية في بناء "صناعة محصنة" ومستدامة.

أهداف الدورة:

- استيعاب مفاهيم "الصناعة السيادية" وعلاقتها بأمن IIoT وتصفير البيروقراطية الإجرائية.
- تطوير مهارات هندسة "أمن الحافة (Edge Security) "لضمان حماية البيانات في مصدر الإنتاج.
- إتقان فن توظيف التوائم الرقمية (Digital Twins) في محاكاة التهديدات واختبار الصمود الصناعي.
- حوكمة ممارسات الربط بين أنظمة الـ IT والـ OT لضمان النزاهة والشفافية في تدفق البيانات.
- تعزيز السيادة المعلوماتية عبر بناء "منصات IIoT وطنية" مستقلة ومحمية سيادياً.
- تطبيق استراتيجيات القيادة في إدارة "الأزمات الصناعية الذكية" وضمان المصداقية الدولية والنمو.

محتويات الورشة:

اليوم الأول :

فلسفة الصناعة الذكية والرشاقة في إدارة السيادة التشغيلية

هندسة الحصانة الصناعية وتصفير البيروقراطية في إدارة الأصول

- مفهوم IIoT لعام 2026 وأثره على السيادة الوطنية وجودة الحياة والنمو والتميز العالمي.
- مواءمة استراتيجيات التأمين مع مبدأ تصفير البيروقراطية عبر أتمتة جرد وتأمين المستشعرات (ZTP).
- تحليل العلاقة بين "كفاءة الإنتاج" وبين بناء الثقة والمصداقية الدولية في المنتج الوطني.
- تمرين هندسة الاستباقية لتصميم دورة عمل أمنية تصفّر زمن "رصد العطل" بنزاهة وشفافية مطلقة.

قيادة النزاهة في حوكمة "المصنع المتصل" والريادة الوطنية الشاملة

- تعزيز السيادة على بروتوكولات الاتصال الصناعي) مثل MQTT و OPC UA)لضمان استقلاليتها.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في إدارة سلاسل التوريد التقنية.
- بناء ثقافة "الأمان كدافع للإنتاجية" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والنمو.
- صياغة ميثاق أخلاقيات قائد أنظمة IIoT لدعم النزاهة والقدوة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة رصد التهديدات بالذكاء الاصطناعي(AIoT)

تصفير مخاطر التعطل عبر التحليل السلوكي للآلات والتوائم الرقمية

- توظيف الذكاء الاصطناعي في رصد التغيرات الدقيقة في أداء المحركات وتصفير احتمالات التخريب بنزاهة.
- حماية "البيانات الصناعية السيادية" عبر أنظمة تشفير وطنية تضمن موثوقية المعلومات والنزاهة الرقمية.
- تطبيق الهوية الرقمية للأشياء (IDoT) لتصفير الهدر البيروقراطي في إجراءات التدقيق والوصول للشبكة.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لصحة المنظومات الميدانية والنمو.

حوكمة الأنظمة الخوارزمية والنزاهة في الاستجابة الآلية والتحكم

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي 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 الحافة (Edge) لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات IIoT بنزاهة تامة والتميز.

اليوم الثالث :

هندسة الصمود والحياد في إدارة الموارد والشمولية

تصفير البيروقراطية في "الربط بين الحافة والسحابة" والشمولية الصناعية

- هندسة القنوات السحابية التي تصفّر زمن التزامن مع ضمان أعلى معايير السيادة والنزاهة والتميز.
- تفعيل الرقابة الأخلاقية على منصات IIoT لضمان حياد النظم الرقمية في توزيع الموارد والنمو.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق تاريخ الصيانة وتصفير احتمالات التلاعب بنزاهة.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي الأجهزة لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والنمو.
- تطوير آليات رصد الأثر البيئي والاجتماعي للحوادث الصناعية لضمان النزاهة والعدالة والتميز.
- بناء سجلات نزاهة رقمية لكل عملية تحديث برمجي للأجهزة (OTA) لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار أمني حول "التطور الصناعي والخصوصية" بأسلوب قيادي واثق وملهم.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في الأزمات الصناعية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل في حالات "تعطل خطوط الإنتاج" والموازنة بين الإبهار والوقار السيادي والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة والفرق الفنية لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الحصانة الصناعية" لتصفير فرص انتشار الشائعات والنزاهة.
- التدقيق الأخلاقي على سلاسل توريد المكونات الإلكترونية لضمان خلوها من الممارسات الضارة والسيادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الميداني والسيادة.
- مهارات التواصل الأخلاقي عند حدوث عطل في "أنظمة التحكم" لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والنزاهة.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج الرصد 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 أمنIIoT

- مصفوفة "النبض اللحظي" للأنظمة السيبرانية-الفيزيائية: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل بيانات المستشعرات في خطوط الإنتاج إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن رصد "الانحرافات التشغيلية" وضمان اكتشاف محاولات التخريب الرقمي في مهدها بنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للاستجابة الصناعية المؤتمتة: هندسة مسار قرار "صفري الإجراءات" يسمح للأنظمة بتنفيذ عمليات "الإغلاق الآمن" أو تحويل المسارات الإنتاجية فور رصد النبضة الاستراتيجية للتهديد. يضمن هذا البروتوكول استمرارية عمل المرافق الحيوية (مثل المياه والكهرباء) دون قيود بيروقراطية أو انتظار للاعتمادات البشرية في اللحظات الحرجة.
- حوكمة "التوأم الرقمي السيادي" والنزاهة: وضع ضوابط أخلاقية تضمن مطابقة المحاكاة الافتراضية للواقع الميداني تماماً، وتفعيل ميثاق "النزاهة في بيانات الحافة" لضمان استقلال القرار الصناعي الوطني والوضوح التام أمام صانع القرار بشأن سلامة الأصول.
- 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 العزل الذكي" لحماية خطوط الإنتاج والسيادة الوطنية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة منظومية تضمن نزاهة التعامل مع الأجهزة والبيانات الوطنية بنسبة 100%.
- القدرة على هندسة منظومات رصد واستجابة رشيقة وسيادية تتوافق مع معايير 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 الميداني المتصل يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء القطاعات الصناعية، والطاقة، والمياه، والنقل الذكي، والتصنيع المتقدم.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي في المصانع الكبرى.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بسلامة البنية التحتية الصناعية والسيادة.
- رؤساء فرق الصيانة الاستراتيجية ومحللو مخاطر IIoT 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)