تأمين منظومات إنترنت الأشياء الحكومية من الحافة إلى السحابة

الإمارات العربية المتحدة - دبي

22 – 26/ 02 / 2026

مقدمة:

في قلب التحول الوطني الشامل لعام 2026، تمثل منظومات إنترنت الأشياء (IoT) "الجهاز الحسي" للدولة الرقمية؛ فهي التي تربط المدن الذكية، والمرافق الحيوية، والخدمات الحكومية بالواقع الميداني. إن حماية هذه المليارات من الأجهزة والمستشعرات تتطلب فكراً قيادياً ينتقل من الحماية المركزية إلى "الأمن الموزع" الذي يبدأ من الحافة (Edge) وينتهي بالسحابة السيادية. يهدف هذا البرنامج إلى تمكين القادة من هندسة منظومات متصلة تصفّر البيروقراطية في إدارة الأصول، وتضمن النزاهة المطلقة في تدفق البيانات، مما يعزز ريادة الدولة كأذكى وأأمن بيئة رقمية عالمية.

أهداف الدورة:

- استيعاب مفاهيم "إنترنت الأشياء السيادي" وعلاقتها بالأمن القومي وتصفير البيروقراطية.
- تطوير مهارات هندسة "أمن الحافة (Edge Security) "لضمان المعالجة الآمنة في المصدر.
- إتقان فن توظيف الذكاء الاصطناعي في رصد التهديدات الهجينة الموجهة للأجهزة المتصلة.
- حوكمة ممارسات "الربط المنظومي" لضمان الشفافية والنزاهة في إدارة البيانات الضخمة.
- تعزيز السيادة المعلوماتية عبر بناء سلاسل توريد تقنية "موثوقة سيادياً" ومستقلة.
- تطبيق استراتيجيات القيادة في إدارة الأزمات الناتجة عن تعطل الأنظمة المتصلة والريادة العالمية.

محتويات الورشة:

اليوم الأول :

فلسفة IoT السيادي والرشاقة في إدارة الأصول المتصلة

هندسة الحصانة الحسية وتصفير البيروقراطية في نشر المنظومات

- مفهوم إنترنت الأشياء الحكومي 2026 وأثره على السيادة الوطنية وجودة الحياة والنمو والتميز.
- مواءمة استراتيجيات IoT مع مبدأ تصفير البيروقراطية عبر أتمتة تسجيل وتأمين الأجهزة (ZTP).
- تحليل العلاقة بين "دقة المستشعرات" وبين بناء الثقة والمصداقية الدولية في المنظومة الذكية.
- تمرين هندسة الاستباقية لتصميم دورة حياة للأجهزة تصفّر زمن الكشف عن الأعطال بنزاهة وشفافية.

قيادة النزاهة في حوكمة "المجتمع المتصل" والريادة الوطنية الشاملة

- تعزيز السيادة على بروتوكولات الاتصال (5G/6G) لضمان استقلاليتها وتوافقها مع القيم والهوية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في إدارة الخصوصية داخل المدن الذكية.
- بناء ثقافة "الأمان كقاعدة للابتكار الحضري" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل.
- صياغة ميثاق أخلاقيات قائد منظومة IoT لدعم النزاهة والقدوة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة "أمن الحافة(Edge Security) "

تصفير مخاطر الاختراق عبر المعالجة الموزعة والذكاء الاصطناعي

- توظيف "حوسبة الحافة" لتصفير الهدر البيروقراطي في نقل البيانات الحساسة للسحابة والنمو.
- حماية "البيانات الحسية السيادية" عبر أنظمة تشفير وطنية تبدأ من المستشعر لضمان النزاهة الرقمية.
- تطبيق الهوية الرقمية للأشياء (IDoT) لتصفير زمن التحقق من سلامة الأجهزة المتصلة والريادة.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لصحة المنظومات الميدانية.

حوكمة الأنظمة الخوارزمية والنزاهة في اتخاذ القرار عند الحافة

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي في إصدار "قرارات الاستجابة الآلية."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الأجهزة القابلة للارتداء لضمان المصداقية والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات IoT بنزاهة تامة والتميز.

اليوم الثالث :

حوكمة السحابة والحياد في إدارة تدفق البيانات والشمولية

تصفير البيروقراطية في "الربط بين الحافة والسحابة" والشمولية الرقمية

- هندسة القنوات السحابية التي تصفّر زمن التزامن مع ضمان أعلى معايير السيادة والنزاهة والتميز.
- تفعيل الرقابة الأخلاقية على منصات IoT السحابية لضمان حياد النظم الرقمية في النتائج والنمو.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق تاريخ الأجهزة 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 الاجتماعي والبيئي لمنظومات IoT لضمان النزاهة والعدالة والتميز والريادة.
- بناء سجلات نزاهة رقمية لكل عملية تحديث برمجي كبرى (OTA) لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار أمني حول "المدن الذكية والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في العصر المتصل

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل في حالات "فقدان السيطرة على الأنظمة" والموازنة بين الإبهار والوقار السيادي والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة والفرق الميدانية لتعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن نجاحات التأمين لتصفير فرص انتشار الشائعات والنزاهة والشفافية.
- 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 أعطال في "أنظمة التحكم" لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والنزاهة والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج الرصد ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "المتصل" القدوة: من تأمين الحافة إلى هندسة السيادة الحسية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في منظومات IoT

- مصفوفة "النبض اللحظي" للأصول المتصلة: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل تدفقات البيانات من الحافة (Edge) إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن رصد "الانحرافات السلوكية" للأجهزة وضمان اكتشاف محاولات الاختراق أو التلاعب بالبيانات الميدانية في مهدها بنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للاستجابة الموزعة: هندسة مسار قرار "صفري الإجراءات" يسمح للمنظومة بتنفيذ عمليات "العزل التلقائي" للأجهزة المصابة فور رصد النبضة الاستراتيجية للتهديد. يضمن هذا البروتوكول استمرارية عمل المرافق الحيوية والخدمات الذكية دون قيود بيروقراطية أو انتظار للاعتمادات البشرية في الأزمات المتسارعة.
- حوكمة "الصدق الحسي" والنزاهة الرقمية: وضع ضوابط أخلاقية تضمن مطابقة "الهوية الرقمية للأشياء (IDoT) "للواقع الفيزيائي، وتفعيل ميثاق "النزاهة في البيانات الضخمة" لضمان استقلال القرار الوطني والوضوح التام أمام صانع القرار بشأن سلامة البنية التحتية المتصلة.
- مختبر "هندسة الحصانة ضد اختراقات المدن الذكية": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة" ناتجة عن تعطل منظومة استشعار كبرى، وكيفية تفعيل بروتوكول "التعافي الذاتي" لحماية جودة الحياة والسيادة المعلوماتية.

المخرجات الرئيسية للدورة:

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

الفئة المستهدفة:

- القيادات العليا ومدراء مشاريع المدن الذكية، والتحول الرقمي، والأمن السيبراني الحكومي.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية في قطاعات البلديات، الطاقة، والنقل.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة الأنظمة المتصلة والسيادة.
- رؤساء فرق المهام الخاصة ومحللو بيانات إنترنت الأشياء 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)