تأمين شبكات الجيل الخامس الحكومية ومخاطر تقنية تقطيع الشبكة (Slicing)

الإمارات العربية المتحدة - دبي

24 – 28/ 05 / 2026

مقدمة:

في فضاء عام 2026، يمثل الجيل الخامس (G5) "العمود الفقري" للدولة الذكية، حيث يربط بين الذكاء الاصطناعي، وإنترنت الأشياء، والخدمات الحكومية فائقة السرعة. إن تقنية "تقطيع الشبكة" (Network Slicing) هي الابتكار الذي يسمح بتخصيص مسارات رقمية سيادية مستقلة لكل قطاع، لكنها تحمل في طياتها مخاطر أمنية تتطلب "حصانة استباقية". يهدف هذا البرنامج إلى تمكين القادة من أدوات حماية هذه الشبكات، وتصفير البيروقراطية في إدارة الموارد الترددية، مع ضمان النزاهة والسيادة المطلقة على تدفق البيانات الوطنية.

أهداف الدورة:

- استيعاب مفاهيم "السيادة الترددية" وعلاقتها بالأمن القومي وتصفير البيروقراطية.
- تطوير مهارات هندسة "الشرائح الشبكية (Slices) "لضمان العزل التام للبيانات الحكومية الحساسة.
- إتقان فن رصد ومعالجة مخاطر "التداخل بين الشرائح (Cross-Slice Threats) "بنزاهة وشفافية.
- حوكمة ممارسات الوصول لشبكة الـ G 5لضمان التوازن بين سرعة التحول وبين متطلبات الحماية السيادية.
- تعزيز السيادة المعلوماتية عبر بناء "نواة شبكة وطنية (Sovereign Core) "مستقلة تماماً.
- تطبيق استراتيجيات القيادة في إدارة "الأزمات الاتصالية" وضمان المصداقية والسمعة الدولية الشاملة.

محتويات الورشة:

اليوم الأول :

فلسفة السيادة الرقمية والرشاقة في هندسة G5

هندسة الحصانة الترددية وتصفير البيروقراطية في إدارة الطيف

- مفهوم السيادة على شبكات G 5لعام 2026 وأثرها على جودة الحياة والنمو والتميز العالمي.
- مواءمة استراتيجيات الشبكة مع مبدأ تصفير البيروقراطية عبر أتمتة "تخصيص الشرائح " (Slice Provisioning).
- تحليل العلاقة بين "المنعة اللاسلكية" وبين بناء الثقة والمصداقية الدولية في النموذج الوطني.
- تمرين هندسة الاستباقية لتصميم دورة حياة للشبكة تصفّر زمن الاستجابة للأعطال بنزاهة وشفافية.

قيادة النزاهة في حوكمة "النسيج الرقمي" والريادة الوطنية الشاملة

- تعزيز السيادة على بروتوكولات G 5الوطنية لضمان استقلاليتها وتوافقها مع القيم والهوية.
- دور القائد في حماية صورة الدولة عبر ممارسات النزاهة في إدارة عقود مشغلي الاتصالات.
- بناء ثقافة "الاتصال كحق سيادي محصن" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والنمو.
- صياغة ميثاق أخلاقيات قائد شبكات المستقبل لدعم النزاهة والقدوة والتميز في كافة المستويات.

اليوم الثاني :

السيادة التقنية وهندسة تقطيع الشبكة (Slicing) والمخاطر

تصفير مخاطر الاختراق عبر "العزل الافتراضي" والذكاء الاصطناعي

- تحليل مخاطر "هروب البيانات من الشريحة (Slice Escape) "وتصفير احتمالات التداخل بنزاهة والتميز.
- حماية "الشرائح السيادية" عبر أنظمة تشفير وطنية تضمن موثوقية الاتصالات والنزاهة الرقمية والريادة.
- تطبيق الهوية الرقمية للشرائح (Slice ID) لتصفير الهدر البيروقراطي في إجراءات التحقق والولوج.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لصحة وأمن الشرائح الحكومية.

حوكمة الأنظمة الخوارزمية والنزاهة في إدارة موارد الشبكة

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي في "توجيه حركة البيانات " (Traffic Orchestration).
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير جودة الخدمة.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من رصد الشبكة لضمان المصداقية أمام صانع القرار والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات 5 Gبنزاهة تامة والتميز.

اليوم الثالث :

هندسة "انعدام الثقة (Zero Trust) "في بيئة 5 Gوالشمولية

تصفير البيروقراطية في "التحقق من الأطراف" والشمولية الرقمية

- تطبيق نموذج Zero Trust على مستوى الشبكة لتصفير مخاطر "الأجهزة المتصلة المعادية" بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات إدارة الشبكة لضمان حياد النظم الرقمية والتميز والنمو الشامل.
- تطبيق تقنيات "تجزئة الشبكة الدقيقة" لتصفير فجوات المراقبة بين البيئات الحكومية والخاصة والسيادة.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني للشبكة لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي الأجهزة (Vendors) لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي والاقتصادي لسرعات 5 Gلضمان النزاهة والعدالة والتميز والنمو.
- بناء سجلات نزاهة رقمية لكل تحديث في "نواة الشبكة (Core Network) "لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "5 Gوالسيادة الوطنية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في حوادث الشبكة

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل في حالات "انقطاع الخدمة أو الاختراق" 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 نجاحات التأمين لتصفير فرص انتشار الشائعات والنزاهة والشفافية.
- التدقيق الأخلاقي على سلاسل توريد مكونات G 5لضمان خلوها من الممارسات الضارة والسيادة والريادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الوطني والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "برمجة الشريحة" 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 الرصد ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "5 G Leader"القدوة: من تقطيع الشبكة إلى هندسة السيادة الرقمية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في بيئة الجيل الخامس

- مصفوفة "النبض اللحظي" لعزل الشرائح: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل بيانات تدفق المعلومات داخل "الشرائح الشبكية" إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن رصد "هروب البيانات (Slice Escape)" وضمان عزل القطاعات الحكومية الحساسة بنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" في توجيه البيانات :(Orchestration) هندسة مسار قرار "صفري الإجراءات" يسمح لنواة الشبكة (Core Network) بتوسيع أو تقليص موارد الشريحة آلياً فور رصد نبضة استراتيجية تطلب زيادة الأداء (مثل حالات الطوارئ). يضمن هذا البروتوكول استمرارية الخدمات فائقة السرعة دون قيود بيروقراطية أو انتظار للاعتمادات اليدوية التي تعيق سيولة العمليات الرقمية.
- حوكمة "النسيج الرقمي" والنزاهة الترددية: وضع ضوابط أخلاقية تضمن حياد الخوارزميات في إدارة "جودة الخدمة (QoS) "لكل شريحة، وتفعيل ميثاق "النزاهة في تخصيص الموارد" لضمان استقلال القرار التقني الوطني والوضوح التام أمام صانع القرار بشأن حصانة القنوات الاتصالية.
- مختبر "هندسة الصمود ضد التداخل الشبكي": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة اتصالية" ناتجة عن تداخل بين شريحة تجارية وشريحة سيادية، وكيفية تفعيل "بروتوكول العزل الذكي" لحماية تدفق المعلومات والسيادة الوطنية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة اتصالية تضمن نزاهة التعامل مع الشرائح 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 الاستراتيجي للشبكات يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء تقنية المعلومات، والاتصالات، والأمن السيبراني في الجهات السيادية والحكومية.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي في قطاع البنية التحتية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة الاتصالات الوطنية والسيادة.
- مهندسو الشبكات الاستراتيجية ومحللو مخاطر الجيل الخامس 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)