تصميم بنية شبكات مرنة وآمنة: من SD-WAN إلى SASE

الإمارات العربية المتحدة - دبي

13 – 17/ 12 / 2026

مقدمة:

في فضاء 2026، لم تعد الشبكات مجرد وسيلة لنقل البيانات، بل هي "الشرايين الرقمية" التي تضخ القوة في جسد الدولة الذكية. إن التحول من الشبكات التقليدية إلى تقنيات SD-WAN وصولاً إلى حافة الخدمة الأمنية الآمنة (SASE) يمثل قفزة نحو سيادة تقنية لا تعترف بالحدود الجغرافية بل بالمنعة الرقمية. يهدف هذا البرنامج إلى تمكين القادة من هندسة بنى تحتية تصفّر البيروقراطية في إدارة الاتصالات، وتضمن النزاهة المطلقة في تدفق المعلومات، مما يعزز ريادة الدولة كمركز عالمي للابتكار المتصل والآمن.

أهداف الدورة:

- استيعاب مفاهيم "السيادة الشبكية" وعلاقتها بالأمن القومي وتصفير البيروقراطية التشغيلية.
- تطوير مهارات الانتقال الاستراتيجي من الشبكات التقليدية إلى SD-WAN لتعزيز الرشاقة والنمو.
- إتقان فن دمج الأمن مع الشبكة عبر نموذج SASE لتحقيق "الحماية عند الحافة."
- حوكمة ممارسات "الوصول السحابي" لضمان الشفافية والنزاهة في إدارة الأصول الوطنية.
- تعزيز السيادة المعلوماتية عبر بناء شبكات وطنية مستقلة تعتمد على "نظام التشغيل السيادي."
- تطبيق استراتيجيات القيادة في إدارة "الشبكات الذاتية (Autonomous Networks) " وضمان المصداقية الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة "الشبكات المعرفة برمجياً (SD-WAN) "وتصفير البيروقراطية

هندسة الرشاقة الاتصالية وتصفير البيروقراطية في إدارة المسارات

- مفهوم SD-WAN 2026 وأثره على السيادة الوطنية وجودة الحياة والنمو والتميز العالمي.
- مواءمة استراتيجيات الشبكة مع مبدأ تصفير البيروقراطية عبر "الأتمتة المركزية " (Orchestration).
- تحليل العلاقة بين "مرونة الارتباط" وبين بناء الثقة والمصداقية الدولية في الخدمات الحكومية.
- تمرين هندسة الاستباقية لتصميم شبكة تصفّر زمن "إعادة التوجيه التلقائي" بنزاهة وشفافية.

قيادة النزاهة في حوكمة "التدفق المعلوماتي" والريادة الوطنية الشاملة

- تعزيز السيادة على أجهزة التوجيه الوطنية لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في توزيع أحمال الشبكة الحساسة.
- بناء ثقافة "الاتصال الموثوق" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والنمو والريادة.
- صياغة ميثاق أخلاقيات قائد الشبكات الذكية لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

التحول نحو :SASE دمج الشبكة والأمن عند الحافة

تصفير مخاطر التشتت الأمني عبر تقارب الشبكات والحماية السحابية

- مفهوم SASE (Secure Access Service Edge) كدرع سيادي يدمج SD-WAN مع الأمن السحابي.
- حماية "الوصول عن بُعد" عبر تقنيات ZTNA لتصفير البيروقراطية في منح الأذونات بنزاهة والتميز.
- تطبيق الهوية الرقمية للشبكة (Network Identity) لضمان النزاهة الرقمية والسيادة المعلوماتية.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحالة الأمن عند الحافة.

حوكمة الأنظمة الخوارزمية والنزاهة في إدارة بوابات الويب الآمنة(SWG)

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي في "فلترة المحتوى السيادي."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من رصد الحافة لضمان المصداقية والسيادة والنمو.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات SASE بنزاهة تامة.

اليوم الثالث :

هندسة "انعدام الثقة (Zero Trust) "والحياد في الوصول السحابي

تصفير البيروقراطية في "الوصول الخاص (ZTNA) "والشمولية الرقمية

- هندسة بروتوكولات الوصول التي تصفّر زمن التحقق مع ضمان أعلى معايير السيادة والنزاهة والتميز.
- تفعيل الرقابة الأخلاقية على منصات "وسيط أمن الوصول السحابي (CASB) "لضمان حياد النظم.
- تطبيق تقنيات "تجزئة الشبكة الدقيقة (Micro-segmentation) "لتصفير فجوات الاختراق الجانبي.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني للشبكة لتقليل احتمالات الخطأ والتميز والنمو.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي السحب العالمية لضمان توافق معايير SASE مع السيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي لسياسات الاتصال لضمان النزاهة والعدالة والتميز والنمو.
- بناء سجلات نزاهة رقمية لكل عملية "تغيير سياسة أمنية" لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "الشبكة كخدمة سيادية" بأسلوب قيادي واثق وملهم.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في الشبكات الذاتية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند حدوث "انقطاع في السحابة" والموازنة بين الإبهار والوقار السيادي والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة والفرق الفنية لتعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الشبكة ذاتية الإصلاح" لتصفير فرص انتشار الشائعات.
- التدقيق الأخلاقي على سلاسل توريد البرمجيات (SaaS) لضمان خلوها من الممارسات الضارة والسيادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التي قد تهدد أمن بنك معلومات الشبكة والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "أتمتة الشبكة" 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 الرقمي "SASE-Ready" القدوة: من إدارة الأجهزة إلى هندسة السيادة الشبكية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في بنيةSASE

- مصفوفة "النبض اللحظي" للتدفق الشبكي: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل بيانات حركة المرور عبر الحافة (Edge) إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن رصد "الانحرافات الاتصالية" وضمان اكتشاف محاولات التسلل عبر بوابات الويب في مهدها بنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للوصول السحابي الآمن: هندسة مسار قرار "صفري الإجراءات" يسمح للشبكة بتغيير مسارات البيانات وتفعيل بروتوكولات التحقق من الهوية (ZTNA)آلياً فور رصد النبضة الاستراتيجية للتهديد. يضمن هذا البروتوكول استمرارية عمل التطبيقات الحكومية الحساسة دون قيود بيروقراطية أو انتظار للاعتمادات اليدوية التي تعيق سرعة التحول الرقمي.
- حوكمة "الحقيقة الرقمية" في بوابات الويب: وضع ضوابط أخلاقية تضمن شفافية عمليات فلترة المحتوى وإدارة الوصول، وتفعيل ميثاق "النزاهة في الوساطة السحابية (CASB) "لضمان استقلال القرار التقني الوطني والوضوح التام أمام صانع القرار بشأن حصانة القنوات الاتصالية.
- مختبر "هندسة الصمود ضد انقطاع السحب": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة اتصالية" ناتجة عن تعطل مزود سحابي عالمي، وكيفية تفعيل بروتوكول "التحويل السيادي" للمسارات لحماية تدفق المعلومات والسيادة الوطنية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة اتصالية تضمن نزاهة التعامل مع البيانات والبيئات الوطنية بنسبة 100%.
- القدرة على هندسة منظومات ربط 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 الاستراتيجي للشبكات يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء تقنية المعلومات، والاتصالات، والأمن السيبراني، والتحول الرقمي.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية المعنيون بتطوير البنية التحتية الحكومية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المشرفون على سلامة تدفق البيانات السيادية.
- مهندسو الشبكات الاستراتيجية ومحللو أمن السحاب في الهيئات الاتحادية والمحلية والوطنية.

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)