# تطبيق استراتيجيات "انعدام الثقة" (Zero Trust)
# في البيئات السحابية الحكومية

الإمارات العربية المتحدة - دبي

2026 / 02 /12 – 08

## مقدمة:

في فضاء السحابة الحكومية لعام 2026، سقطت "أسوار القلاع" التقليدية؛ فلم يعد هناك فرق بين داخل الشبكة وخارجها. إن استراتيجية "انعدام الثقة" (Zero Trust) هي المنهج السيادي الذي يتبنى مبدأ "لا تثق أبداً، تحقق دائماً". يهدف هذا البرنامج إلى تمكين القادة من إعادة هندسة الأمن السحابي ليكون مرناً وذكياً، يصفّر البيروقراطية في إجراءات التحقق، ويضمن النزاهة المطلقة في الوصول إلى الأصول الوطنية الحساسة، محققاً بذلك أعلى معايير الريادة في العصر الرقمي.

## أهداف الدورة:

- استيعاب الركائز الخمس لنموذج انعدام الثقة (الهوية، الأجهزة، الشبكة، التطبيقات، والبيانات).
- تطوير مهارات هندسة "الهوية الرقمية السيادية" كخط دفاع أول في السحابة الحكومية.
- إتقان فن "تجزئة الشبكة الدقيقة (Micro-segmentation) "لتصفير مخاطر الانتشار الجانبي للتهديدات.
- حوكمة ممارسات الوصول السحابي لضمان الشفافية والنزاهة في إدارة صلاحيات الكوادر الوطنية.
- تعزيز السيادة المعلوماتية عبر بناء بيئات سحابية "ممنوعة من الاختراق بناءً على التصميم."
- تطبيق استراتيجيات القيادة في التحول من "الأمن المحيطي" إلى "الأمن المرتكز على البيانات."

## محتويات الورشة:

**اليوم الأول :**

**فلسفة "انعدام الثقة" والرشاقة في السيادة السحابية**

**هندسة الحصانة الرقمية وتصفير البيروقراطية الأمنية**

- مفهوم :Zero Trust 2026 الانتقال من الثقة الافتراضية إلى التحقق المستمر والسيادة المطلقة والنمو.
- مواءمة استراتيجية السحابة مع مبدأ تصفير البيروقراطية عبر أتمتة سياسات الوصول (Policy as Code).
- تحليل العلاقة بين "الأمن المعتمد على الهوية" وبين بناء الثقة والمصداقية في الخدمات الحكومية الذكية.
- تمرين هندسة الاستباقية لتصميم بنية "انعدام الثقة" تصفّر زمن منح الوصول الآمن بنزاهة وشفافية.

**قيادة النزاهة في حوكمة الثقة والريادة الوطنية الشاملة**

- تعزيز السيادة على محركات الهوية الوطنية لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في تطبيق مبدأ "الحد الأدنى من الصلاحيات."
- بناء ثقافة "الأمان كداعم للابتكار السحابي" وعلاقتها بجودة الحياة والولاء المؤسسي والنمو الشامل.
- صياغة ميثاق أخلاقيات قائد الأمن السحابي لدعم النزاهة والقدوة والتميز في كافة المستويات.

**اليوم الثاني :**

**السيادة التقنية وهندسة الهوية كالمحيط الأمني الجديد**

**تصفير مخاطر انتحال الشخصية عبر التحقق متعدد العوامل (MFA) والبيومترية**

- توظيف الذكاء الاصطناعي في تحليل سلوك المستخدمين (UEBA) وتصفير احتمالات الدخول غير المصرح به.
- حماية "سجلات الهوية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنزاهة الرقمية.
- تطبيق الهوية الرقمية الموحدة (SSO) لتصفير الهدر البيروقراطي في إجراءات تسجيل الدخول المتعددة.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحالات التحقق والوصول السحابي.

**حوكمة الأنظمة الخوارزمية والنزاهة في إدارة الصلاحيات اللحظية**

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في إصدار "قرارات منح الوصول."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار والنمو.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الذكاء الاصطناعي لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات أمن السحابة بنزاهة تامة والتميز.

**اليوم الثالث :**

## هندسة الشبكة الدقيقة والحياد في إدارة التطبيقات والشمولية

### تصفير البيروقراطية في "تجزئة الشبكة (Micro-segmentation) "والشمولية الرقمية

- هندسة الشبكات السحابية التي تصفّر زمن احتواء التهديدات عبر العزل اللحظي للتطبيقات بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات إدارة التطبيقات السحابية لضمان حياد النظم الرقمية والتميز والنمو.
- تطبيق تقنيات "الوصول الخاص بالذكاء الاصطناعي" لتصفير فجوات المراقبة بين البيئات السحابية المختلفة.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والسيادة.

### المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي السحب العالمية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والنمو.
- تطوير آليات رصد الأثر الاجتماعي لسياسات الأمن السحابي لضمان النزاهة والعدالة في نتائج الوصول والتميز.
- بناء سجلات نزاهة رقمية لكل عملية وصول حساسة للسحابة الحكومية لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار أمني حول "انعدام الثقة والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

**اليوم الرابع :**

## المسؤولية المهنية وإدارة السمعة والنزاهة في الأمن السحابي

### القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند حدوث "محاولات اختراق مجهضة" والموازنة بين الإبهار والوقار السيادي والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة السحابية لتعزيز مصداقية القرار السيادي عالمياً والريادة والتميز.
- بناء أنظمة الإفصاح الاستباقي عن قوة المنظومة السحابية لتصفير فرص انتشار الشائعات والنزاهة والشفافية.
- التدقيق الأخلاقي على سلاسل توريد البرمجيات السحابية لضمان 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 السحابي والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث عطل في "محرك الثقة" 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 "المحقق" القدوة: من أمن المحيط إلى هندسة السيادة السحابية الشاملة**

**هندسة "النبض الاستراتيجي" والرشاقة السيادية في بيئة انعدام الثقة(Zero Trust)**

- مصفوفة "النبض اللحظي" للتحقق المستمر: تصميم نظام رصد سيادي يعتمد على التحليلات السلوكية (UEBA) لتحويل كل "طلب وصول" إلى نبضة استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن رصد "الانحرافات السلوكية" وضمان أن كل عملية دخول تتم بناءً على سياق حي وآمن وبنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للوصول الديناميكي: هندسة مسار قرار "صفري الإجراءات" يسمح للأنظمة السحابية بمنح أو حجب الصلاحيات آلياً فور رصد النبضة الاستراتيجية التي تشير إلى تغير في "معامل الثقة" للجهاز أو المستخدم. يضمن هذا البروتوكول استمرارية العمل الحكومي دون قيود بيروقراطية أو انتظار للاعتمادات اليدوية التي تعيق سرعة التحول السحابي.
- حوكمة "النزاهة الرقمية" في محركات الهوية: وضع ضوابط أخلاقية تضمن استقلالية "محركات الثقة" عن المؤثرات الخارجية، وتفعيل ميثاق "النزاهة في إدارة الصلاحيات" لضمان خلو النظام من الانحيازات الرقمية والوضوح التام أمام صانع القرار بشأن حصانة الأصول الوطنية السحابية.
- مختبر "هندسة الحصانة ضد التسلل الجانبي": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة" ناتجة عن محاولة تحرك جانبي داخل السحابة، وكيفية تفعيل بروتوكول "التجزئة الدقيقة" (Micro-segmentation) لحظياً لحماية التطبيقات والسيادة الوطنية.

## المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة سحابية تضمن نزاهة التعامل مع الأصول والبيانات الوطنية بنسبة 100%.
- القدرة على هندسة منظومات وصول 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 للسحابة يدعم اتخاذ القرار القيادي الآمن والمستدام.

## الفئة المستهدفة:

- القيادات العليا ومدراء مراكز البيانات السحابية، وأمن المعلومات، والتحول الرقمي.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية في القطاعات الحكومية والسيادية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة الوصول للبيانات الحساسة.
- مهندسو البنية التحتية السحابية ومحللو الأمن السيبراني 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)