تطبيق بنية "انعدام الثقة" (Zero Trust) لتأمين الشبكات الحكومية

الإمارات العربية المتحدة - دبي

05 – 09/ 07 / 2026

مقدمة:

في عصر لم تعد فيه الأسوار التقليدية كافية لحماية البيانات السيادية، تبرز بنية "انعدام الثقة" (Zero Trust) كفلسفة أمنية تقضي بأن "الثقة خطر". يهدف هذا البرنامج إلى تمكين القادة من إعادة هندسة الشبكات الحكومية لتكون حصوناً رقمية لا تعترف بالثقة الافتراضية، بل بالتحقق المستمر. سنعمل على توظيف الذكاء الاصطناعي لتصفير البيروقراطية في إجراءات الوصول، مع ضمان أعلى مستويات النزاهة والشفافية في حماية الأصول المعلوماتية، مما يعزز ريادة الدولة كبيئة تقنية فائقة الأمان والسيادة في عام 2026.

أهداف الدورة:

- استيعاب المبادئ الأساسية لبنية Zero Trust وعلاقتها بالسيادة الرقمية الوطنية.
- تطوير مهارات هندسة "إدارة الهوية والوصول (IAM) "لتصفير البيروقراطية في رحلة المستخدم.
- إتقان فن توظيف "التجزئة الدقيقة (Micro-segmentation) "لحماية البيانات الحساسة بنزاهة.
- حوكمة ممارسات التحقق المستمر لضمان التوازن بين الأمن المطلق وبين انسيابية العمل الحكومي.
- تعزيز السيادة المعلوماتية عبر بناء "بوابات وصول سيادية" تعتمد على معايير وطنية مستقلة.
- تطبيق استراتيجيات القيادة في إدارة "بيئة الثقة الصفرية" وضمان المصداقية في تقارير الامتثال.

محتويات الورشة:

اليوم الأول :

فلسفة انعدام الثقة والرشاقة في الوصول السيادي

هندسة الحصانة الرقمية وتصفير البيروقراطية في التحقق

- مفهوم "الثقة الصفرية" كدرع لحماية السيادة الوطنية من التهديدات الداخلية والخارجية المتطورة.
- مواءمة استراتيجيات الأمن مع مبدأ تصفير البيروقراطية عبر أتمتة إجراءات التحقق "خلف الكواليس."
- تحليل العلاقة بين "الأمن غير المرئي" وبين بناء الثقة والمصداقية الدولية في المنظومة الرقمية للدولة.
- تمرين هندسة الوصول لتصميم دورة عمل تصفّر زمن الدخول للأنظمة بنزاهة وشفافية رقمية كاملة.

قيادة النزاهة في حوكمة الهوية والريادة العالمية

- تعزيز السيادة على قواعد بيانات الهوية الرقمية لضمان استقلاليتها وتوافقها مع القيم الوطنية والنمو.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في منح وصلاحية الوصول للبيانات.
- بناء ثقافة "التحقق كقيمة" وعلاقتها بجودة الحياة والولاء المؤسسي والأمن القومي الشامل.
- صياغة ميثاق أخلاقيات قائد بيئة "انعدام الثقة" لدعم النزاهة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة التحقق المستمر بالذكاء الاصطناعي

تصفير مخاطر الاختراق عبر التحليل السلوكي والتوائم الرقمية

- توظيف الذكاء الاصطناعي في مراقبة الأنماط السلوكية للمستخدمين وتصفير احتمالات انتحال الشخصية بنزاهة.
- حماية "بيانات الوصول السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية الهوية والنتائج الرقمية.
- تطبيق "التوثيق متعدد العوامل (MFA) "الذكي لتصفير الهدر البيروقراطي في إجراءات الدخول المتعددة.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحالة الثقة في الشبكة.

حوكمة الأنظمة الخوارزمية والنزاهة في منح الصلاحيات

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في إصدار "قرارات الوصول."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقييم المستخدمين.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من أنظمة الرصد لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن السيادي بنزاهة تامة.

اليوم الثالث :

التجزئة الدقيقة والحياد في إدارة الأمن الشبكي

هندسة الحماية الجزيئية والشمولية الرقمية في تغطية الأصول

- استخدام "التجزئة الدقيقة (Micro-segmentation) "لضمان عدالة حماية جميع البيانات بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على مسارات البيانات لضمان الشفافية وحياد النظم الرقمية في النتائج.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الأمن التي قد تغفل البعد الإنساني.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع مزودي السحب الرقمية لضمان توافقها مع معايير جودة الحياة والسيادة الوطنية والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي لسياسات الأمن الصارمة لضمان النزاهة والعدالة في تقديم الخدمة الرقمية.
- بناء سجلات نزاهة رقمية لكل عملية وصول حساسة لضمان الشفافية المطلقة والوضوح التام والتميز.
- تمرين محاكاة لإدارة حوار تقني حول "الأمن والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة في بيئة التهديدات المتطورة

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل عند اكتشاف محاولة اختراق والموازنة بين الإبهار التقني وبين الوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للالتزام الأمني وأثرها في تعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن الحوادث المجهضة لضمان الشفافية وتصفير الشائعات الرقمية.
- التدقيق الأخلاقي على سلاسل توريد البرمجيات الأمنية لضمان خلوها من الممارسات الضارة أو التجسسية.

حصانة الشبكة ضد الانتهاكات المعلوماتية والتلاعب بالهوية

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات السيادي والريادة الوطنية.
- مهارات التواصل الأخلاقي عند حدوث خطأ في أنظمة التحقق لضمان استعادة الثقة ببيانات صادقة ونزيهة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والمهني.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالحقائق والبيانات.

اليوم الخامس :

هندسة الاستجابة السيادية وتصفير البيروقراطية في تطبيق بنية "انعدام الثقة (Zero Trust) " والسيادة الرقمية الشاملة

مختبر "بوابة السيادة" وإدارة الثقة الصفرية في الشبكات الحكومية المعقدة

- محاكاة "الاختراق من الداخل" والسيادة على الهوية: وضع القادة في سيناريو يحاكي محاولة وصول غير مصرح به من داخل الشبكة باستخدام هوية منتحلة، واختبار قدرة أنظمة "التحقق المستمر" والذكاء الاصطناعي على تفعيل بروتوكول "التجزئة الدقيقة" بنزاهة ووضوح تام لعزل التهديد لحظياً ومنع انتشاره العرضي.
- تصفير البيروقراطية في "هندسة الوصول الذكي": تطبيق مسار قرار صفري الإجراءات لمنح صلاحيات الوصول بناءً على "السياق السلوكي" والموقع والجهاز، لضمان انسيابية العمل الحكومي في الزمن الحقيقي دون انتظار الاعتمادات اليدوية أو تكرار طلبات التحقق التقليدية التي تعيق الإنتاجية، مع الحفاظ على الحصانة الرقمية والريادة العالمية الشاملة.
- هندسة "النزاهة والخصوصية" والتحقق المزدوج: اختبار مهارة القائد في الموازنة بين سياسات "انعدام الثقة" الصارمة وبين "الحكمة البشرية السيادية" لضمان عدم عرقلة المهام القيادية الحساسة، ومنع أي انحيازات خوارزمية في تقييم موثوقية المستخدمين، مما يعزز ريادة الدولة كبيئة عمل تقنية فائقة الأمان والنزاهة والشفافية.
- ورشة "تفكيك صوامع البيانات والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام تحليلات "إدارة الهوية والوصول" لتحديد الفجوات في "منظومة الثقة"، وتطوير حلول هندسية استباقية تمنع تضارب الصلاحيات بين الجهات الحكومية، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار أمان شبكي موحد".

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة سيبرانية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة 100%.
- القدرة على هندسة بنية Zero Trust رشيقة وسيادية تتوافق مع متطلبات الريادة والتميز العالمية.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي في النتائج.
- بناء سجل ممارسات فضلى في إدارة الذكاء الأمني الشبكي يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء تقنية المعلومات والأمن السيبراني في الجهات السيادية والحكومية.
- مسؤولو البنية التحتية الرقمية وفرق التميز المؤسسي وتصفير البيروقراطية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بحماية الأصول المعلوماتية.
- رؤساء فرق الاستجابة للطوارئ الرقمية والمهندسون الاستراتيجيون في الشبكات الوطنية.

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)