إدارة الهوية والوصول (IAM/PAM) وربطها بأمن الشبكات

الإمارات العربية المتحدة - دبي

27 – 01/ 10 / 2026

مقدمة:

في عالم 2026، لم تعد الشبكة هي المحيط الأمني، بل أصبحت الهوية هي الجدار الجديد. إن إدارة الهوية والوصول (IAM) وإدارة الوصول المميز (PAM) تمثل القوة السيادية التي تمنح "الحق الرقمي" للأشخاص والآلات. يهدف هذا البرنامج إلى تمكين القادة من هندسة منظومات هوية تصفّر البيروقراطية في إجراءات التوثيق، وتضمن الربط اللحظي بين هوية المستخدم وأمن الشبكة، مما يرسخ النزاهة المطلقة ويحمي المفاصل الحيوية للدولة من الاختراقات الداخلية والخارجية.

أهداف الدورة:

- استيعاب مفهوم "الهوية كمحيط أمني" وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة أنظمة IAM لضمان الانسيابية المطلقة في رحلة المستخدم الرقمية.
- إتقان فن حوكمة "الوصول المميز (PAM) "لحماية الحسابات الإدارية فائقة الحساسية.
- ربط الهوية الرقمية ببروتوكولات أمن الشبكات (IDN) لتحقيق العزل الذكي للأصول.
- تعزيز السيادة المعلوماتية عبر بناء مخازن هوية وطنية مستقلة ومحمية سيادياً.
- تطبيق استراتيجيات القيادة في إدارة "أزمات الهوية" وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة "الهوية السيادية" والرشاقة في إدارة الوصول

هندسة الثقة المطلقة وتصفير البيروقراطية في إجراءات القيد(Onboarding)

- مفهوم الهوية الرقمية 2026 وأثره على السيادة الوطنية وجودة الحياة والنمو والتميز العالمي.
- مواءمة استراتيجيات IAM مع مبدأ تصفير البيروقراطية عبر "الهوية الموحدة (Single Source of Truth)".
- تحليل العلاقة بين "دقة التعريف" وبين بناء الثقة والمصداقية الدولية في المنظومة الرقمية.
- تمرين هندسة الاستباقية لتصميم دورة حياة للهوية تصفّر زمن "منح الصلاحيات" بنزاهة وشفافية.

قيادة النزاهة في حوكمة "الحق الرقمي" والريادة الوطنية الشاملة

- تعزيز السيادة على قواعد بيانات الهوية الوطنية لضمان استقلاليتها وتوافقها مع القيم والهوية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في مراجعة صلاحيات الوصول.
- بناء ثقافة "الهوية كمسؤولية وطنية" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والنمو.
- صياغة ميثاق أخلاقيات قائد أنظمة الهوية لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة التوثيق الذكي(Adaptive Auth)

تصفير مخاطر الانتحال عبر التحقق الحيوي والذكاء الاصطناعي

- توظيف "التوثيق التكيفي" لتصفير فجوات الأمن عبر تحليل السياق (الموقع، الجهاز، الوقت) بنزاهة.
- حماية "بيانات الهوية السيادية" عبر أنظمة تشفير وطنية تضمن موثوقية السجلات والنزاهة الرقمية.
- تطبيق تقنيات "الهوية اللامركزية (Self-Sovereign Identity)" لتصفير البيروقراطية في التحقق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمحاولات الوصول والتميز.

حوكمة الأنظمة الخوارزمية والنزاهة في "إدارة الدور(RBAC/ABAC) "

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي في تحديد "الصلاحيات التلقائية."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من رصد الهوية لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الوصول بنزاهة تامة.

اليوم الثالث :

إدارة الوصول المميز (PAM) وحماية "مفاتيح المملكة"

تصفير البيروقراطية في إدارة الحسابات الحساسة والشمولية الرقمية

- هندسة أنظمة PAM التي تصفّر زمن الوصول الطارئ للمهندسين مع ضمان الرقابة الصارمة بنزاهة.
- تفعيل الرقابة الأخلاقية على منصات "تسجيل الجلسات" لضمان الشفافية وحياد النظم الرقمية والنمو.
- تطبيق تقنية "الوصول في الوقت المناسب (Just-In-Time) "لتصفير مخاطر الحسابات الدائمة والسيادة.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني للحسابات المميزة لتقليل احتمالات الخطأ والتميز.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع شركات الصيانة الخارجية لضمان توافق وصولهم مع معايير السيادة والنزاهة.
- تطوير آليات رصد الأثر المهني لصلاحيات الوصول لضمان النزاهة والعدالة والتميز والنمو الشامل.
- بناء سجلات نزاهة رقمية لكل عملية "تغيير صلاحيات" كبرى لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "الوصول والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

الربط بأمن الشبكات وإدارة السمعة والنزاهة

هندسة "الشبكات المعرفة بالهوية (IDN) "وتصفير البيروقراطية التنسيقية

- ربط نظام IAM بجدران الحماية لتصفير فجوات العزل الشبكي بناءً على هوية المستخدم بنزاهة والتميز.
- الرقابة على البصمة الرقمية للوصول المميز لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن نجاحات "تصفير الاختراقات الداخلية" لتعزيز النزاهة والشفافية.
- التدقيق الأخلاقي على سلاسل توريد برمجيات الهوية لضمان خلوها من الممارسات الضارة والسيادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالهوية

- المسؤولية القيادية في التبليغ عن الثغرات التي قد تهدد أمن بنك معلومات الهوية والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "منح صلاحية" 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 "حارس الهوية" القدوة: من إدارة الحسابات إلى هندسة السيادة الرقمية

هندسة "النبض الاستراتيجي" والرشاقة السيادية في إدارة الهوية

- مصفوفة "النبض اللحظي" للهوية والوصول: تصميم نظام رصد رقمي يعتمد على الذكاء الاصطناعي لتحويل محاولات الوصول وسلوكيات المستخدمين إلى "نبضات استراتيجية" تظهر للقائد فوراً، مما يصفّر زمن "منح أو حجب الصلاحيات" ويضمن أن يكون الوصول مبنياً على السياق اللحظي وبنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للوصول في الوقت المناسب (JIT): هندسة مسار قرار "صفري الإجراءات" يسمح بمنح صلاحيات الوصول المميز (PAM) للعمليات الطارئة آلياً فور التحقق من الهوية الحيوية، مما يضمن استمرارية الأعمال الحساسة دون قيود بيروقراطية أو انتظار للاعتمادات اليدوية المجهدة.
- حوكمة "الهوية اللامركزية" والنزاهة الرقمية: وضع ضوابط أخلاقية تضمن ملكية المستخدم لبياناته (Self-Sovereign Identity) ومحمايتها سيادياً، مما يمنع الانحيازات الرقمية في تحديد "الأدوار"، ويحقق ريادة وطنية قائمة على الشفافية المطلقة والوضوح التام أمام صانع القرار
- مختبر "هندسة الحصانة ضد الانتحال": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة اختراق هوية" مميزة، وكيفية تفعيل العزل الشبكي التلقائي بناءً على الهوية (IDN) لحماية الأصول المعلوماتية والسيادة الوطنية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة للهوية تضمن نزاهة التعامل مع الصلاحيات 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 للهوية يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء تقنية المعلومات، والأمن السيبراني، وإدارة المخاطر والتميز المؤسسي.
- مسؤولو التحول الرقمي وفرق تصفير البيروقراطية المعنيون بتطوير تجربة المستخدم والسيادة.
- خبراء الحوكمة والنزاهة والرقابة التقنية المشرفون على صلاحيات الوصول في الجهات الحكومية.
- رؤساء فرق أمن الشبكات ومحللو الهوية الرقمية 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)