الحوسبة السرية

(Confidential Computing) لحماية البيانات
قيد الاستخدام

الإمارات العربية المتحدة - دبي

14 – 18/ 06 / 2026

مقدمة:

في عام 2026، لم يعد تشفير البيانات "أثناء التخزين" أو "أثناء النقل" كافياً لحماية أسرار الدولة؛ فالثغرة الكبرى تكمن عندما يتم فك تشفير البيانات داخل المعالج لمعالجتها. إن الحوسبة السرية هي الحصن الأخير والسيادي الذي يحمي البيانات وهي "قيد الاستخدام". يهدف هذا البرنامج إلى تمكين القادة من أدوات عزل المعالجة داخل بيئات تنفيذ موثوقة (TEEs)، مما يصفّر البيروقراطية في التحقق من أمن السحب الهجينة، ويضمن النزاهة المطلقة للعمليات الرقمية الوطنية، مرسخاً مكانة الدولة كقوة تقنية عالمية لا يمكن اختراق عقلها الرقمي.

أهداف الدورة:

- استيعاب مفاهيم "الثقة القائمة على العتاد (Hardware-based Trust) "وعلاقتها بالسيادة الرقمية.
- تطوير مهارات هندسة "الجيوب الأمنية (Enclaves) "لعزل العمليات الحكومية الحساسة عن بيئة التشغيل.
- إتقان فن توظيف الحوسبة السرية لتصفير البيروقراطية في مشاركة البيانات بين الجهات دون كشفها.
- حوكمة ممارسات "الاستدلال السري" للذكاء الاصطناعي لضمان النزاهة والخصوصية المطلقة للنماذج.
- تعزيز السيادة المعلوماتية عبر بناء "سحب سيادية" تعتمد على تقنيات معالجة وطنية مستقلة.
- تطبيق استراتيجيات القيادة في إدارة "الأمان المتجذر في العتاد" وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة "المعالجة المحصنة" والرشاقة في إدارة السيادة الرقمية

هندسة الحصانة المطلقة وتصفير البيروقراطية في بناء الثقة

- مفهوم الحوسبة السرية 2026: الانتقال من حماية "الأوعية" إلى حماية "الأفكار والعمليات" والنمو.
- مواءمة استراتيجيات المعالجة مع مبدأ تصفير البيروقراطية عبر إلغاء الحاجة لتدقيق طبقات نظام التشغيل.
- تحليل العلاقة بين "الأمن المتجذر في المعالج" وبين بناء الثقة والمصداقية الدولية في الاقتصاد الرقمي.
- تمرين هندسة الاستباقية لتصميم دورة معالجة تصفّر زمن التحقق من أمان البيئة السحابية بنزاهة.

قيادة النزاهة في حوكمة "العتاد الموثوق" والريادة الوطنية الشاملة

- تعزيز السيادة على سلاسل توريد المعالجات لضمان خلوها من الأبواب الخلفية وتوافقها مع القيم.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في اختيار تقنيات الـ TEEs السيادية.
- بناء ثقافة "الأمان غير المشروط" وعلاقتها بجودة الحياة والولاء المؤسسي والأمن القومي الشامل.
- صياغة ميثاق أخلاقيات قائد الحوسبة السرية لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة بيئات التنفيذ الموثوقة(TEEs)

تصفير مخاطر الاختراق عبر "الجيوب الأمنية (Enclaves) "والذكاء الاصطناعي

- توظيف تقنيات Intel SGX و AMD SEVفي عزل البيانات الحكومية وتصفير احتمالات التجسس بنزاهة.
- حماية "نماذج الذكاء الاصطناعي السيادية" أثناء التدريب والاستدلال لضمان النزاهة الرقمية والتميز.
- تطبيق الهوية الرقمية للعمليات (Process Identity) لتصفير الهدر البيروقراطي في إجراءات الترخيص.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لصحة "المعالج الموثوق."

حوكمة الأنظمة الخوارزمية والنزاهة في "التصديق عن بُعد(Remote Attestation) "

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحقق الآلي من سلامة العتاد والبرمجيات.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأمان.
- ترسيخ مفهوم الأمانة في نتائج "التصديق الرقمي" لضمان المصداقية أمام صانع القرار والسيادة والنمو.
- ورشة عمل حول ضوابط استخدام الحوسبة السرية في تحسين جودة قرارات الأمن القومي بنزاهة تامة.

اليوم الثالث :

التعاون السري والحياد في إدارة البيانات الضخمة والشمولية

تصفير البيروقراطية في "التحليلات متعددة الأطراف" والشمولية الرقمية

- هندسة منصات التعاون التي تصفّر زمن التنسيق الأمني عبر معالجة البيانات وهي مشفرة بنزاهة والتميز.
- تفعيل الرقابة الأخلاقية على منصات "مشاركة البيانات السرية" لضمان حياد النظم الرقمية والنمو الشامل.
- تطبيق تقنيات "التشفير المتماثل (FHE) "بجانب الحوسبة السرية لتصفير فجوات الخصوصية السيادية.
- حساب معامل الثقة في مؤشرات الإنجاز الرقمي لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي السحب العالمية لضمان تطبيق معايير "عدم الوصول للبيانات " (Zero Access).
- تطوير آليات رصد الأثر الاجتماعي للخصوصية المطلقة لضمان النزاهة والعدالة في نتائج المعالجة والتميز.
- بناء سجلات نزاهة رقمية لكل عملية معالجة بيانات حساسة لضمان الشفافية والوضوح والريادة العالمية.
- تمرين محاكاة لإدارة حوار استراتيجي حول "السيادة على المعالجات" بأسلوب قيادي واثق وملهم.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في حوادث العتاد

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند اكتشاف ثغرات في العتاد) مثل (Spectre/Meltdown والموازنة بين الإبهار والوقار.
- الرقابة على البصمة الرقمية للأنظمة السيادية لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن قوة "الدرع المادي" لتصفير فرص انتشار الشائعات والنزاهة والشفافية.
- التدقيق الأخلاقي على سلاسل توريد السيليكون 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 معلومات المعالجة والسيادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "بيئة التنفيذ" لضمان استعادة الثقة ببيانات صادقة.
- 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.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "Confidential-Native" القدوة: من حماية التخزين إلى هندسة السيادة على المعالجة الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في الحوسبة السرية

- مصفوفة "النبض اللحظي" لسلامة العتاد: تصميم نظام رصد سيادي يعتمد على تقنيات "التصديق عن بُعد (Remote Attestation) "لتحويل الحالة الأمنية للمعالجات إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن التحقق من أمان الجيوب الأمنية (Enclaves) وضمان أن المعالجة تتم في بيئة محصنة تماماً بنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للمعالجة المستقلة: هندسة مسار قرار "صفري الإجراءات" يسمح للأنظمة الحكومية بنقل العمليات الحساسة آلياً بين السحب الهجينة فور رصد النبضة الاستراتيجية التي تؤكد صحة العتاد .(Hardware Integrity) يضمن هذا البروتوكول استمرارية معالجة البيانات الضخمة دون قيود بيروقراطية أو انتظار للاعتمادات الأمنية اليدوية التي تعطل سرعة القرار.
- حوكمة "الخصوصية المطلقة" والنزاهة الرقمية: وضع ضوابط أخلاقية تضمن "عدم الوصول للبيانات (Zero Access) "حتى من قبل مسؤولي النظام، وتفعيل ميثاق "النزاهة في الاستدلال الذكي" لضمان استقلال خوارزميات الذكاء الاصطناعي الوطنية وحمايتها من التلاعب أثناء الاستخدام.
- مختبر "هندسة الحصانة ضد اختراقات المعالج": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة" ناتجة عن ثغرة في العتاد المادي، وكيفية تفعيل بروتوكول العزل الفوري لحماية الأصول المعلوماتية والسيادة الوطنية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة عتادية تضمن نزاهة التعامل مع البيانات والبيئات الوطنية بنسبة %.100
- القدرة على هندسة منظومات معالجة 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 للعتاد يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء مراكز البيانات، والأمن السيبراني، والتحول الرقمي في القطاعات السيادية.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية المعنيون بأمن البنى التحتية السحابية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المشرفون على حماية البيانات فائقة السرية.
- رؤساء فرق تطوير البرمجيات السيادية ومحللو أمن العتاد 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)