تحليل سلوك الكيانات والمستخدمين (UEBA)
للكشف عن التهديدات الداخلية

الإمارات العربية المتحدة - دبي

2026 / 05 /14 – 10

مقدمة:

في المشهد الأمني لعام 2026، لم تعد التهديدات تقتصر على الهجمات الخارجية، بل بات "الخطر الداخلي" يمثل التحدي الأكبر للسيادة المعلوماتية. إن تقنية UEBA ليست مجرد أداة مراقبة، بل هي "عقل اصطناعي" يفهم الأنماط البشرية والآلية ليحمي المؤسسة من الداخل دون المساس بجودة الحياة المهنية. يهدف هذا البرنامج إلى تمكين القادة من هندسة منظومات رصد سلوكي ذكية تصفّر البيروقراطية في التحقيقات الداخلية، وتضمن النزاهة والشفافية في حماية الأصول السيادية، مما يعزز ريادة الدولة كبيئة عمل فائقة الأمان والموثوقية.

أهداف الدورة:

- استيعاب مفاهيم "التحليل السلوكي (Behavioral Analytics) "وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة "خطوط الأساس السلوكية (Baselining) "لكل مستخدم وكيان في الشبكة الوطنية.
- إتقان فن توظيف التعلم الآلي في اكتشاف التهديدات الداخلية (المتعمدة وغير المتعمدة) بنزاهة وشفافية.
- حوكمة ممارسات الرقابة السلوكية لضمان التوازن بين الأمن المطلق وحماية خصوصية الكوادر البشرية.
- تعزيز السيادة المعلوماتية عبر بناء "محركات تحليل وطنية" تعتمد على خوارزميات سيادية مستقلة.
- تطبيق استراتيجيات القيادة في إدارة "حوادث الثقة" وضمان المصداقية والسمعة المؤسسية والتميز.

محتويات الورشة:

اليوم الأول :

فلسفة الأمن السلوكي والرشاقة في إدارة الثقة المؤسسية

هندسة الحصانة الداخلية وتصفير البيروقراطية في الرقابة

- مفهوم التهديد الداخلي 2026 وأثره على السيادة الوطنية وجودة الحياة والريادة العالمية والنمو.
- مواءمة استراتيجيات UEBA مع مبدأ تصفير البيروقراطية عبر أتمتة اكتشاف الأنماط المشبوهة لحظياً.
- تحليل العلاقة بين "الأمن القائم على السلوك" وبين بناء الثقة والمصداقية الدولية في المنظومة الإدارية.
- تمرين هندسة الاستباقية لتصميم دورة عمل رصد تصفّر زمن الكشف عن تسريب البيانات بنزاهة وشفافية.

قيادة النزاهة في حوكمة السلوك البشري والريادة الوطنية

- تعزيز السيادة على قواعد البيانات السلوكية لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في التعامل مع "تنبيهات السلوك" الحساسة.
- بناء ثقافة "الأمان القائم على النزاهة" وعلاقتها بجودة الحياة والولاء المؤسسي والأمن القومي الشامل.
- صياغة ميثاق أخلاقيات قائد التحليل السلوكي لدعم النزاهة والقدوة في كافة المستويات القيادية والوطنية.

اليوم الثاني :

السيادة التقنية وهندسة النمذجة السلوكية بالذكاء الاصطناعي

تصفير مخاطر التسلل عبر خوارزميات اكتشاف الشذوذ السلوكي

- توظيف الذكاء الاصطناعي في تمييز السلوكيات المهنية الطبيعية عن التحركات المريبة بنزاهة.(Anomaly Detection)
- حماية "البيانات السلوكية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية النتائج والنزاهة الرقمية.
- تطبيق الهوية الرقمية في تتبع مسارات الكيانات (الخوادم، التطبيقات) لتصفير الهدر البيروقراطي في التحقق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لدرجات المخاطر السلوكية.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط التهديدات

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد "الموظفين ذوي الخطورة."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأفعال.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من أنظمة الـ UEBA لضمان المصداقية والعدالة في الإجراءات.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن الداخلي بنزاهة تامة والتميز.

اليوم الثالث :

الحياد والعدالة في إدارة الخصوصية والشمولية الرقمية

هندسة الحماية المعرفية وتصفير البيروقراطية في إدارة الهوية

- استخدام تقنيات "إخفاء الهوية (Anonymization) "أثناء التحليل لضمان النزاهة والشفافية وحماية الخصوصية.
- تفعيل الرقابة الأخلاقية على منصات التحليل السلوكي لضمان حياد النظم الرقمية في النتائج والتميز والريادة.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الأمن التي قد تغفل البعد الإنساني أو الهوية.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والنمو.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع مزودي التقنيات لضمان توافق الأنظمة مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر النفسي والاجتماعي لسياسات الرقابة السلوكية لضمان النزاهة والعدالة في النتائج.
- بناء سجلات نزاهة رقمية لكل عملية تدقيق سلوكي كبرى لضمان الشفافية المطلقة والوضوح والتميز.
- تمرين محاكاة لإدارة حوار أمني حول "التحليل السلوكي والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في التحقيقات الداخلية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل عند رصد تهديد داخلي والموازنة بين الإبهار والوقار السيادي الحكومي والوطني والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة السلوكية لتعزيز مصداقية القرار السيادي عالمياً والريادة والتميز.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة النزاهة المؤسسية لتصفير فرص انتشار الشائعات الرقمية والنمو.
- التدقيق الأخلاقي على سلاسل توريد برمجيات التحليل السلوكي لضمان خلوها من الممارسات الضارة والنزاهة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك معلومات السلوك والسيادة الوطنية.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "درجة مخاطر المستخدم" لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والنزاهة والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج التحليل ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

هندسة الاستجابة السلوكية وتصفير البيروقراطية في تحليل سلوك الكيانات والمستخدمين(UEBA)

مختبر "النبض السلوكي السيادي" وإدارة حوادث الثقة في البيئة الرقمية

- محاكاة "التسلل الصامت والسيادة المعلوماتية": وضع القادة في سيناريو يحاكي رصد "انحراف سلوكي" دقيق من قبل مستخدم ذي صلاحيات عالية (مثل محاولة الوصول لبيانات سيادية في توقيت غير معتاد)، واختبار قدرة أنظمة التحليل السلوكي على تفعيل بروتوكول "التنبيه الذكي" بنزاهة ووضوح تام لضمان حماية الأصول الوطنية قبل وقوع الضرر.
- تصفير البيروقراطية في "هندسة التحقيق الفوري": تطبيق مسار قرار صفري الإجراءات للتحقق من هوية المستخدم ودوافعه بناءً على "خط الأساس السلوكي" المعتمد، لضمان احتواء التهديد الداخلي في الزمن الحقيقي دون انتظار لجان التحقيق التقليدية التي قد تمنح المتسلل فرصة لمسح آثاره، مع الحفاظ على الحصانة القانونية والسيادة الرقمية الكاملة والريادة العالمية الشاملة.
- هندسة "النزاهة والخصوصية" والتحقق البشري السيادي: اختبار مهارة القائد في الموازنة بين مخرجات لوحات التحكم السلوكية التي تحدد "درجات المخاطر" وبين "الحكمة القيادية البشرية" لضمان عدم المساس بخصوصية الموظفين أو جودة حياتهم المهنية، ومنع أي انحيازات خوارزمية قد تظلم الكوادر الوطنية، مما يعزز ريادة الدولة كبيئة عمل عادلة وآمنة.
- ورشة "تفكيك صوامع البيانات السلوكية والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات السلوكية لتحديد الفجوات في "منظومة الثقة"، وتطوير حلول هندسية استباقية تمنع تضارب البيانات بين الأنظمة المختلفة، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار نزاهة مؤسسي معصوم".

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة سلوكية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة %.100
- القدرة على هندسة منظومات رصد استباقية 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 السلوكي الاستراتيجي يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء الموارد البشرية، وتقنية المعلومات، والأمن السيبراني في الجهات السيادية.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي في القطاع الحكومي والخاص.
- خبراء الحوكمة والنزاهة والرقابة الداخلية المعنيون بحماية الأسرار المؤسسية والوطنية.
- رؤساء فرق الاستجابة للحوادث ومحللو التهديدات الداخلية 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)