تحليل التهديدات وتقييم المخاطر الأمنية وبناء خطط الاستجابة

الإمارات العربية المتحدة - دبي

2026 / 12 /03 – 11/29

مقدمة:

في المشهد الأمني المتسارع لعام 2026، لم يعد تحليل التهديدات مجرد إجراء روتيني، بل أصبح المحرك الذكي لضمان السيادة الوطنية وحماية الأصول السيادية. يهدف هذا البرنامج إلى نقل القادة من عقلية "رد الفعل" إلى "الاستباقية الرقمية" عبر توظيف الذكاء الاصطناعي لتصفير البيروقراطية في تقييم المخاطر، مع ضمان أعلى معايير النزاهة والشفافية في بناء خطط استجابة مرنة تعزز جودة الحياة وتدعم ريادة الدولة العالمية.

أهداف الدورة:

- استيعاب مفاهيم "استخبارات التهديدات (Threat Intelligence) "وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة "خرائط المخاطر الديناميكية" باستخدام التحليلات التنبؤية المتقدمة.
- إتقان فن بناء خطط استجابة آلية (Automated Playbooks) تضمن سرعة التحرك ونزاهة التنفيذ.
- حوكمة ممارسات جمع البيانات الأمنية لضمان التوازن بين الأمن المطلق وحماية الخصوصية السيادية.
- تعزيز السيادة المعلوماتية عبر بناء منظومات رصد وطنية مستقلة تحمي الأصول المؤسسية الكبرى.
- تطبيق استراتيجيات القيادة في إدارة الأزمات الأمنية وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة تحليل التهديدات والسيادة في عصر الرشاقة

هندسة الاستخبارات الأمنية وتصفير البيروقراطية المعلوماتية

- مفهوم التهديد السيادي وأثره على الأمن القومي وجودة الحياة المؤسسية في عام 2026.
- مواءمة دورة حياة التهديد مع مبدأ تصفير البيروقراطية عبر أتمتة تدفق المعلومات الأمنية.
- تحليل العلاقة بين "الوعي الميداني الرقمي" وبين بناء الثقة والمصداقية الدولية في النموذج الوطني.
- تمرين هندسة الاستباقية لتصميم دورة عمل تصفّر زمن الكشف عن التهديدات الناشئة بنزاهة.

قيادة النزاهة في حوكمة مصادر المعلومات والريادة

- تعزيز السيادة على أدوات الجمع والتحليل لضمان استقلالية القرار الأمني الوطني والنمو.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في تصنيف وتقييم التهديدات.
- بناء ثقافة "الأمان القائم على المعرفة" وعلاقتها بجودة الحياة والتميز المؤسسي الشامل.
- صياغة ميثاق أخلاقيات محلل التهديدات السيادي لدعم النزاهة والقدوة في كافة المستويات.

اليوم الثاني :

السيادة التقنية وهندسة التقييم التنبؤي للمخاطر

تصفير مخاطر الاختراق عبر الذكاء الاصطناعي والتحليلات المتقدمة

- توظيف الذكاء الاصطناعي في بناء نماذج تنبؤية للمخاطر تصفّر احتمالات المفاجأة الاستراتيجية.
- حماية "بيانات المخاطر السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية النتائج والنزاهة.
- تطبيق الهوية الرقمية للأصول لتصفير الهدر البيروقراطي في إجراءات التدقيق والتحقق الميداني.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمصفوفة المخاطر الوطنية.

حوكمة الأنظمة الخوارزمية والنزاهة في تقدير الأثر

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في إصدار "قرارات الحماية."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في النتائج.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الحساسات الذكية لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن القومي بنزاهة.

اليوم الثالث :

هندسة الاستجابة والحياد في إدارة الأزمات والشمولية

بناء خطط الاستجابة الرشيقة وتصفير البيروقراطية التنفيذية

- هندسة خطط الاستجابة (Incident Response Plans) التي تضمن تصفير زمن التعافي بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات إدارة الأزمات لضمان حياد النظم الرقمية في توزيع المهام.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الاستجابة 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 القطاع الخاص لضمان توافق خطط الاستجابة مع معايير جودة الحياة والسيادة.
- تطوير آليات رصد الأثر الاجتماعي للسياسات الأمنية لضمان النزاهة والعدالة في النتائج والتميز.
- بناء سجلات نزاهة رقمية لكل عملية استجابة كبرى لضمان الشفافية المطلقة والوضوح والريادة.
- تمرين محاكاة لإدارة حوار أمني حول "الاستجابة والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في البلاغات

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل عند الكشف عن التهديدات والمخاطر والموازنة بين الإبهار والوقار السيادي.
- الرقابة على البصمة الرقمية للالتزام الأمني وأثرها في تعزيز مصداقية القرار السيادي عالميًا.
- بناء أنظمة الإفصاح الاستباقي عن المخاطر المجهضة لضمان الشفافية وتصفير الشائعات الرقمية.
- التدقيق الأخلاقي على سلاسل توريد البيانات الأمنية لضمان خلوها من الممارسات الضارة والنزاهة.

حصانة الأنظمة السيادية ضد الانتهاكات المعلوماتية والتلاعب

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات والسيادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في تقدير المخاطر 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 التخطيط ضد التلاعب الممنهج بالبيانات.

اليوم الخامس :

هندسة الاستجابة الاستباقية وتصفير البيروقراطية في تحليل التهديدات والسيادة الأمنية

مختبر "النبض السيادي" وإدارة الاستجابة المرنة تحت ضغط التهديدات المتطورة

- محاكاة "الحصار الرقمي" والسيادة المعلوماتية: وضع القادة في سيناريو يحاكي تهديداً أمنياً هجيناً يستهدف الأصول المؤسسية الكبرى، واختبار قدرتهم على استخدام "استخبارات التهديدات" لتفعيل بروتوكول "الاستجابة التلقائية" بنزاهة ووضوح تام لضمان حماية السيادة المعلوماتية للدولة دون انقطاع في الخدمات.
- تصفير البيروقراطية في "هندسة خطط الاستجابة": تطبيق مسار قرار صفري الإجراءات لتنفيذ خطط الاستجابة الآلية المبرمجة مسبقاً، لضمان تحييد المخاطر في الزمن الحقيقي دون انتظار الموافقات الإدارية التقليدية التي قد تمنح التهديد فرصة للتغلغل، مع الحفاظ على الحصانة القانونية والسيادة الرقمية والريادة العالمية الشاملة.
- هندسة "النزاهة الأمنية" والتحقق المزدوج: اختبار مهارة القائد في الموازنة بين مخرجات لوحات التحكم السيادية التي تقيم خطورة التهديد وبين "الحكمة البشرية السيادية" لضمان عدالة قرارات الحماية، ومنع أي انحيازات رقمية قد تمس الخصوصية أو جودة الحياة، مما يعزز ريادة الدولة كحصن أمن ذكي ومنيع يتسم بالشفافية المطلقة.
- ورشة "تفكيك صوامع البيانات والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات السلوكية لتحديد الفجوات في مصفوفة المخاطر، وتطوير حلول هندسية استباقية تمنع تضارب المعلومات بين الفرق الأمنية المختلفة، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار حماية أمني معصوم".

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة أمنية 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 الأمني الاستراتيجي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء إدارات الأمن، والمخاطر، والجاهزية في الجهات السيادية والحكومية.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي الأمني.
- خبراء الحوكمة والنزاهة والرقابة الداخلية المعنيون بضبط جودة الخطط الأمنية.
- رؤساء غرف العمليات ومحللو الاستخبارات الأمنية 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)