استخبارات التهديدات السيبرانية والتحليل التنبؤي للمخاطر الأمنية

الإمارات العربية المتحدة - دبي

15 – 19/ 02 / 2026

مقدمة:

في المشهد الأمني لعام 2026، لم تعد المعلومات مجرد بيانات، بل أصبحت "استخبارات التهديدات" (CTI) هي المحرك الاستراتيجي الذي يضمن السيادة الرقمية للدولة. إن القدرة على التنبؤ بالهجوم قبل وقوعه هي الفارق بين المؤسسات الرشيقة والمؤسسات التقليدية. يهدف هذا البرنامج إلى تمكين القادة من أدوات التحليل التنبؤي وتوظيف الذكاء الاصطناعي السيادي لتصفير البيروقراطية في تدفق المعلومات الأمنية، مع ضمان أعلى معايير النزاهة والشفافية في حماية الأصول الوطنية الكبرى.

أهداف الدورة:

- استيعاب مفاهيم استخبارات التهديدات السيبرانية وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة "دورة حياة الاستخبارات (Intelligence Lifecycle) "باستخدام التقنيات المؤتمتة.
- إتقان فن توظيف الخوارزميات التنبؤية في رصد التهديدات الهجينة واكتشاف الأنماط الخفية بنزاهة.
- حوكمة ممارسات تبادل المعلومات الأمنية لضمان التوازن بين السرعة التشغيلية وحماية الخصوصية السيادية.
- تعزيز السيادة المعلوماتية عبر بناء "منصات استخبارات وطنية" تعتمد على سحابات أمنية مستقلة.
- تطبيق استراتيجيات القيادة في إدارة "الوعي الميداني الرقمي" وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة الاستخبارات السيادية وتصفير البيروقراطية المعلوماتية

هندسة الوعي الميداني وتصفير البيروقراطية في تدفق البيانات

- مفهوم استخبارات التهديدات (CTI) كدرع لحماية السيادة الوطنية وضمان جودة الحياة الرقمية والريادة.
- مواءمة دورة حياة الاستخبارات مع مبدأ تصفير البيروقراطية عبر أتمتة جمع البيانات من المصادر المتعددة.
- تحليل العلاقة بين "دقة المعلومة الاستخباراتية" وبين بناء الثقة والمصداقية الدولية في المنظومة الأمنية.
- تمرين هندسة الاستباقية لتصميم دورة عمل استخباراتية تصفّر زمن معالجة التهديدات بنزاهة وشفافية مطلقة.

قيادة النزاهة في حوكمة مصادر المعلومات والريادة العالمية

- تعزيز السيادة على أدوات الجمع والتحليل لضمان استقلاليتها وتوافقها مع القيم الوطنية والنمو والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في تقييم مصداقية المصادر (Source Integrity).
- بناء ثقافة "الأمان القائم على المعرفة" وعلاقتها بالولاء المؤسسي والأمن القومي السيادي الشامل والريادة.
- صياغة ميثاق أخلاقيات محلل الاستخبارات السيادي لدعم النزاهة والقدوة في كافة المستويات القيادية والوطنية.

اليوم الثاني :

السيادة التقنية وهندسة التحليل التنبؤي للمخاطر

تصفير مخاطر الاختراق عبر الذكاء الاصطناعي والنمذجة التنبؤية

- توظيف الذكاء الاصطناعي في بناء نماذج تنبؤية تصفّر احتمالات المفاجأة الاستراتيجية والريادة والتميز.
- حماية "بيانات التهديدات السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنزاهة الرقمية.
- تطبيق الهوية الرقمية في توثيق تدفق الاستخبارات لتصفير الهدر البيروقراطي في إجراءات التحقق والاعتماد.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمؤشرات التهديد الوطنية.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط التهديدات

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد مستويات الخطر القومي.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأثر الاستراتيجي.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الـ "ويب المظلم (Dark Web) "لضمان المصداقية والتميز.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الاستخبارات بنزاهة تامة والريادة.

اليوم الثالث :

الحياد والعدالة في إدارة المعلومات والشمولية الرقمية

هندسة الحماية الشاملة والشمولية الرقمية في توزيع المعلومات

- استخدام التحليلات الذكية لضمان عدالة وصول التنبيهات الأمنية لجميع القطاعات بنزاهة وشفافية والريادة.
- تفعيل الرقابة الأخلاقية على منصات تبادل المعلومات لضمان الشفافية وحياد النظم الرقمية في النتائج.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات التحليل التي قد تغفل البعد الإنساني أو السيادي.
- حساب معامل الثقة في مؤشرات الإنجاز الاستخباراتي لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات المعلوماتية مع الجهات الدولية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي للتهديدات السيبرانية لضمان النزاهة والعدالة في حماية الأفراد والنمو.
- بناء سجلات نزاهة رقمية لكل عملية تحليل استخباراتي كبرى لضمان الشفافية المطلقة والوضوح والتميز.
- تمرين محاكاة لإدارة حوار تقني حول "الاستخبارات 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 الحكومي والوطني.
- الرقابة على البصمة الرقمية للالتزام الاستخباراتي وأثرها في تعزيز مصداقية القرار السيادي عالميًا والريادة.
- بناء أنظمة الإفصاح الاستباقي عن التهديدات المجهضة لضمان الشفافية وتصفير الشائعات الرقمية المضللة.
- التدقيق الأخلاقي على سلاسل توريد المعلومات الأمنية لضمان خلوها من الممارسات الضارة والنزاهة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالبيانات

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الاستخباراتي والسيادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في تقدير التهديد لضمان استعادة الثقة ببيانات صادقة ونزيهة.
- 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.

اليوم الخامس :

مختبر الابتكار المهني وصناعة نموذج "الذكاء التنبؤي" الريادي

التطبيق العملي وتصفير البيروقراطية في أنظمة الاستخبارات والتميز المؤسسي

- تطوير خارطة الطريق التنفيذية لدمج أدوات استخبارات التهديدات (CTI) في الممارسات اليومية بمرونة ورشاقة تضمن سيادة القرار والتميز والنمو المستدام.
- تصميم بروتوكولات الحوكمة الذكية الخاصة بـ دورة حياة الاستخبارات لتصفير المسارات البيروقراطية وضمان النزاهة والشفافية والوضوح في التعامل مع التهديدات اللحظية.
- منهجية صياغة ملفات التميز للمنافسة في الجوائز الوطنية (مثل جوائز الأمن السيبراني والريادة الرقمية) مع التركيز على الابتكار في "التحليل التنبؤي" والرشاقة والوضوح.
- تمرين مختبر المحاكاة لإدارة المعضلات الاستخباراتية المعقدة (مثل التهديدات الهجينة المجهولة) وصياغة الحلول الاستباقية الناجحة والتميز في الأداء والسيادة الرقمية.

المخرجات الرئيسية للدورة:

- متلاك استراتيجية حصانة استخباراتية تضمن نزاهة التعامل مع التهديدات والبيانات 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 الاستراتيجي للتهديدات يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء مراكز العمليات الأمنية (SOC) وفرق استخبارات التهديدات.(CTI)
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة المعلومات الأمنية.
- رؤساء فرق الاستجابة للطوارئ ومحللو المخاطر في الجهات الحكومية والسيادية.

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)