التحليل التنبؤي للمخاطر الأمنية في المنشآت الحيوية

سوريا – دمشق

15 – 19/ 02 / 2026

مقدمة:

تمثل المنشآت الحيوية الأعمدة الفقرية لاستقرار الدولة، وفي عام 2026، لم يعد تأمينها يعتمد على الحراسة التقليدية، بل على "الذكاء الاستباقي" الذي يقرأ التهديد قبل تشكله. يهدف هذا البرنامج إلى تمكين القادة من أدوات التحليل التنبؤي وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في رصد المخاطر، مع ضمان أعلى معايير النزاهة والشفافية في حماية السيادة الرقمية والوطنية، مما يعزز ريادة الدولة كحصن أمني ذكي ومنيع.

أهداف الدورة:

- استيعاب مفاهيم التحليل التنبؤي (Predictive Analytics) وعلاقتها بالسيادة الرقمية الوطنية.
- تطوير مهارات هندسة "أنظمة الإنذار المبكر" لتصفير البيروقراطية في تبليغ المخاطر.
- إتقان فن توظيف التوائم الرقمية (Digital Twins) في محاكاة التهديدات واختبار صمود المنشأة.
- حوكمة ممارسات جمع وتحليل البيانات لضمان النزاهة والشفافية وحماية الخصوصية السيادية.
- تعزيز السيادة المعلوماتية عبر بناء "محركات تنبؤ وطنية" تعتمد على سحابة أمنية سيادية.
- تطبيق استراتيجيات القيادة في إدارة "النتائج التنبؤية" وضمان المصداقية في تقارير الجاهزية.

محتويات الورشة:

اليوم الأول :

فلسفة الأمن التنبؤي والرشاقة في إدارة المخاطر

هندسة الحصانة الاستباقية وتصفير البيروقراطية الرقابية

- مفهوم الأمن التنبؤي كدرع لحماية السيادة الوطنية وضمان جودة الحياة واستمرارية الخدمات.
- مواءمة استراتيجيات الرصد مع مبدأ تصفير البيروقراطية عبر أتمتة تدفق البيانات الأمنية اللحظية.
- تحليل العلاقة بين "دقة التنبؤ" وبين بناء الثقة والمصداقية الدولية في أمن المنشآت الوطنية.
- تمرين هندسة الجاهزية لتصميم دورة عمل تنبؤية تصفّر زمن الكشف عن الثغرات بنزاهة وشفافية.

قيادة النزاهة في حوكمة الأصول الحيوية والريادة العالمية

- تعزيز السيادة على الأنظمة التقنية للتنبؤ لضمان استقلاليتها وتوافقها مع القيم والهوية الوطنية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في عرض مستويات الخطر الفعلي والمتوقع.
- بناء ثقافة "الأمان المعتمد على البيانات" وعلاقتها بالنمو الاقتصادي السيادي والوطني الشامل.
- صياغة ميثاق أخلاقيات محلل المخاطر التنبؤي لدعم النزاهة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة التوائم الرقمية للمنشآت

تصفير مخاطر الاختراق عبر المحاكاة الذكية والتحليلات المتقدمة

- توظيف الذكاء الاصطناعي في بناء توائم رقمية للمنشآت تصفّر زمن اكتشاف التسلل أو العطل الفني.
- حماية "البيانات التنبؤية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنزاهة.
- تطبيق الهوية الرقمية للأصول والأنظمة لتصفير الهدر البيروقراطي في إجراءات التحقق والتحري.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد التنبؤي اللحظي لحالة المنشأة.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط المخاطر

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في إصدار "تنبيهات الخطر."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأثر.
- 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 تامة.

اليوم الثالث :

الحياد والعدالة في إدارة الأمن التنبؤي والشمولية

هندسة الحماية الشاملة والشمولية الرقمية في تغطية المنشآت

- استخدام التحليلات الذكية لضمان عدالة توزيع موارد الحماية على جميع المنشآت بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات رصد التهديدات لضمان الشفافية وحياد البيانات الرقمية والنتائج.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات التنبؤ 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 مزودي التقنيات لضمان توافق الأنظمة مع معايير جودة الحياة والسيادة الوطنية.
- تطوير آليات رصد الأثر الاجتماعي للسياسات الأمنية التنبؤية لضمان النزاهة والعدالة في النتائج.
- بناء سجلات نزاهة رقمية لكل عملية تحليل مخاطر كبرى لضمان الشفافية المطلقة والوضوح والتميز.
- تمرين محاكاة لإدارة حوار أمني حول "التنبؤ والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة في الأزمات التنبؤية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل عند رصد تهديد محتمل والموازنة بين الإبهار التقني وبين الوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للالتزام الأمني وأثرها في تعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن المخاطر المجهضة لضمان الشفافية وتصفير الشائعات الرقمية.
- التدقيق الأخلاقي على سلاسل توريد البيانات الأمنية لضمان خلوها من الممارسات الضارة أو المضللة.

حصانة المنظومة التنبؤية ضد الانتهاكات المعلوماتية والتلاعب

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الأمني والسيادة.
- مهارات التواصل الأخلاقي عند حدوث عطل في أنظمة المحاكاة لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والمهني.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالبيانات.

اليوم الخامس :

هندسة الاستجابة الاستباقية وتصفير البيروقراطية في حماية المنشآت الحيوية

مختبر "التوائم الرقمية" وإدارة التهديدات المتوقعة تحت الضغط

- محاكاة اختراق "النبض الرقمي": وضع القادة في سيناريو معقد يحاكي هجوماً هجيناً على منشأة طاقة حيوية، واختبار قدرة الأنظمة التنبؤية على رصد الأنماط غير الطبيعية وتفعيل بروتوكولات العزل التلقائي بنزاهة ووضوح تام.
- تصفير البيروقراطية في "غرف العمليات": تطبيق مسار قرار صفري الإجراءات لنشر فرق التدخل بناءً على "إنذار تنبؤي"، لضمان حماية المفاصل الحيوية للدولة دون انتظار الموافقات الإدارية التقليدية المعطلة، مع الحفاظ على السيادة المعلوماتية الكاملة.
- هندسة "اليقظة الخوارزمية" في الأزمات: اختبار قدرة القائد على التدخل البشري الحكيم لتصحيح مسارات الذكاء الاصطناعي في حال وجود "إنذارات كاذبة"، وضمان استمرارية تشغيل المنشأة بنزاهة تامة ودون الإضرار بجودة الحياة أو الأمن القومي.
- ورشة "تفكيك سيناريوهات الفشل": مراجعة فورية لمخرجات المحاكاة لتحديد الفجوات في بيانات الحساسات الميدانية، وتطوير نماذج تنبؤية أكثر رشاقة تمنع تشكل التهديد في الواقع الميداني وتحمي السمعة الوطنية والريادة العالمية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة تنبؤية 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 والمدراء في إدارات أمن المنشآت الحيوية (الطاقة، المياه، الاتصالات، الصحة).
- مسؤولو الاستراتيجية والتميز المؤسسي وفرق تصفير البيروقراطية في القطاعات الأمنية.
- خبراء التحول الرقمي والحوكمة والنزاهة المعنيون بتطوير أنظمة الرقابة الذكية.
- رؤساء فرق العمل الميدانية ومحللو المخاطر الاستراتيجية في المؤسسات 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)