محاكاة الأزمات السيبرانية وتطوير خطط الاستجابة القطاعية

الإمارات العربية المتحدة - دبي

26 – 30/ 07 / 2026

مقدمة:

في المشهد الرقمي لعام 2026، لم تعد الأزمات السيبرانية مجرد احتمالات تقنية، بل أصبحت تحديات سيادية تتطلب "جاهزية تنبؤية". إن القدرة على محاكاة الأزمة قبل وقوعها هي الفارق بين التعافي الرشيق والشلل العملياتي. يهدف هذا البرنامج إلى تمكين القادة من أدوات المحاكاة المتقدمة وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في سلاسل اتخاذ القرار، مع ضمان أعلى معايير النزاهة والشفافية في حماية القطاعات الحيوية للدولة، مما يعزز صمود البنية التحتية والريادة العالمية.

أهداف الدورة:

- استيعاب مفاهيم "الصمود السيبراني القطاعي" وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة "سيناريوهات المحاكاة الواقعية" باستخدام التوائم الرقمية (Digital Twins).
- إتقان فن بناء خطط الاستجابة القطاعية الموحدة (Sectoral Playbooks) لضمان سرعة التحرك.
- حوكمة ممارسات المحاكاة لضمان النزاهة والشفافية في تقييم الفجوات الأمنية والتميز.
- تعزيز السيادة المعلوماتية عبر بناء "منصات محاكاة وطنية" محمية بتقنيات سيادية مستقلة.
- تطبيق استراتيجيات القيادة في إدارة "التعافي القطاعي الموحد" وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة المحاكاة السيادية والرشاقة في التخطيط للاستجابة

هندسة الجاهزية القطاعية وتصفير البيروقراطية التنسيقية

- مفهوم المحاكاة السيبرانية 2026: من التدريب التقليدي إلى المحاكاة الواقعية المستمرة والريادة.
- مواءمة استراتيجيات الاستجابة مع مبدأ تصفير البيروقراطية عبر أتمتة تدفق الأوامر القيادية.
- تحليل العلاقة بين "سرعة التنسيق القطاعي" وبين بناء الثقة والمصداقية الدولية في النموذج الوطني.
- تمرين هندسة الاستباقية لتصميم دورة عمل محاكاة تصفّر زمن تفعيل خطط الطوارئ بنزاهة وشفافية.

قيادة النزاهة في حوكمة سيناريوهات الأزمة والريادة الوطنية

- تعزيز السيادة على منصات المحاكاة لضمان استقلاليتها وتوافقها مع القيم والهوية والنمو والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في الكشف عن نقاط الضعف المكتشفة.
- بناء ثقافة "الشفافية في الفشل للنجاح في الواقع" وعلاقتها بجودة الحياة والأمن القومي الشامل.
- صياغة ميثاق أخلاقيات قائد المحاكاة السيبرانية لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة المحاكاة بالتوائم الرقمية والذكاء الاصطناعي

تصفير مفاجآت الأزمة عبر الذكاء الاصطناعي والمحاكاة الغامرة

- توظيف الذكاء الاصطناعي في بناء سيناريوهات أزمة "تتكيف تلقائياً" مع استجابة الفريق وتصفير التكرار.
- حماية "بيانات المحاكاة السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية النتائج والنزاهة الرقمية.
- تطبيق الهوية الرقمية للفرق المشاركة لتصفير الهدر البيروقراطي في إجراءات التقييم والاعتماد.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لنتائج المحاكاة الوطنية.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط سيناريوهات الهجوم

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في إصدار "تقارير الجاهزية."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأضرار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من المحاكاة لضمان المصداقية أمام صانع القرار والرقابة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الاستجابة بنزاهة تامة.

اليوم الثالث :

التنسيق القطاعي والحياد في إدارة الموارد والشمولية

هندسة الاستجابة القطاعية الموحدة وتصفير البيروقراطية في الدعم التبادلي

- تطوير خطط استجابة (Playbooks) تصفّر زمن التنسيق بين قطاعات الطاقة، الصحة، والمالية بنزاهة.
- تفعيل الرقابة الأخلاقية على منصات التنسيق القطاعي لضمان حياد النظم الرقمية في توزيع الموارد.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات التعافي التي قد تغفل البعد الإنساني.
- حساب معامل الثقة في مؤشرات الإنجاز القطاعي لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات بين القطاعات لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والنمو.
- تطوير آليات رصد الأثر الاجتماعي للأزمات السيبرانية لضمان النزاهة والعدالة في حماية الخدمات.
- بناء سجلات نزاهة رقمية لكل تمرين محاكاة وطني لضمان الشفافية المطلقة والوضوح والتميز.
- تمرين محاكاة لإدارة حوار قطاعي حول "التعاون في الأزمات" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في الأزمات السيبرانية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات السيبرانية المتسارعة والموازنة بين الإبهار والوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للاستجابة الوطنية وأثرها في تعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن الحقائق لتصفير فرص انتشار الشائعات الرقمية المضللة والنزاهة.
- التدقيق الأخلاقي على سلاسل توريد برمجيات الاستجابة لضمان خلوها من الممارسات الضارة والنزاهة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالواقع

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك معلومات الأزمات والسيادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "محاكاة الأزمة" 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 المحاكاة ضد التلاعب الممنهج بالبيانات والواقع.

اليوم الخامس :

هندسة الاستجابة السيادية وتصفير البيروقراطية في محاكاة الأزمات السيبرانية والسيادة الرقمية الشاملة

مختبر "الجاهزية السيادية" وإدارة التعافي القطاعي تحت محاكاة التوائم الرقمية

- محاكاة "الشلل القطاعي" والسيادة على القرار: وضع القادة في سيناريو يحاكي هجوماً سيبرانياً شاملاً يستهدف قطاعات الطاقة والمالية في آن واحد، واختبار قدرتهم على تفعيل "منصات المحاكاة الوطنية"، وتفعيل بروتوكول "التعافي الرشيق" بنزاهة ووضوح تام لضمان صمود البنية التحتية دون انتظار المراسلات التقليدية.
- تصفير البيروقراطية في "هندسة الاستجابة الموحدة": تطبيق مسار قرار صفري الإجراءات لتفعيل خطط الاستجابة القطاعية (Sectoral Playbooks) بناءً على التنبؤات اللحظية للذكاء الاصطناعي، لضمان انتقال الأجهزة السيادية من مرحلة "رصد الهجوم" إلى "التعافي الشامل" دون عوائق إجرائية، مع الحفاظ على الحصانة الرقمية والريادة العالمية.
- هندسة "النزاهة والصدق" في تقييم الجاهزية: اختبار مهارة القائد في الموازنة بين مخرجات أنظمة "المحاكاة الغامرة" وبين "الحكمة البشرية السيادية" لضمان كشف الفجوات الأمنية بنزاهة، ومنع أي محاولات لتجميل نتائج التمارين، مما يعزز ريادة الدولة كبيئة تقنية فائقة الموثوقية والشفافية تضع الأمن القومي في قلب أهدافها.
- ورشة "تفكيك صوامع التنسيق والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام تحليلات "لوحات التحكم السيادية" لتحديد الثغرات في "منظومة الاستجابة الموحدة"، وتطوير حلول هندسية استباقية تمنع تضارب الأوامر بين القطاعات الحيوية، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار صمود وطني معصوم".

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة محاكاة تضمن نزاهة التعامل مع الأزمات والبيانات الوطنية بنسبة %.100
- القدرة على هندسة منظومات استجابة قطاعية رشيقة وسيادية تتوافق مع معايير 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 للأزمات يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء مراكز الاستجابة للطوارئ السيبرانية (CERT) في القطاعات الحيوية.
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية في الجهات الحكومية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة الجاهزية الوطنية.
- رؤساء فرق المهام الخاصة ومحللو الأزمات السيبرانية 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)