# استراتيجيات بناء الصمود السيبراني للبنى التحتية الحيوية

الإمارات العربية المتحدة - دبي

18 – 22/ 01 / 2026

## مقدمة:

في عالم 2026، لم يعد الأمن السيبراني مجرد خط دفاع، بل أصبح الركيزة الأساسية لضمان استمرارية السيادة الوطنية وجودة الحياة. إن الصمود السيبراني (Cyber Resilience) يتجاوز مفهوم الحماية ليصل إلى قدرة المنشآت الحيوية على "الاستمرار تحت النار" والتعافي اللحظي بذكاء. يهدف هذا البرنامج إلى تمكين القادة من هندسة بنى تحتية صامدة تصفّر البيروقراطية في مواجهة الأزمات، وتوظف الذكاء الاصطناعي السيادي لضمان النزاهة والشفافية في حماية مفاصل الدولة الاستراتيجية.

## أهداف الدورة:

- استيعاب مفاهيم الصمود السيبراني السيادي وعلاقتها بتصفير البيروقراطية في الخدمات الحيوية.
- تطوير مهارات هندسة "البنية التحتية المرنة (Resilient Infrastructure) "ضد التهديدات الهجينة.
- إتقان فن توظيف التوائم الرقمية (Digital Twins) في محاكاة الهجمات واختبار الجاهزية بنزاهة.
- حوكمة ممارسات استمرارية الأعمال الرقمية لضمان حماية الأصول المعلوماتية والريادة الوطنية.
- تعزيز السيادة المعلوماتية عبر بناء منظومات حماية وطنية مستقلة تعتمد على سحابات سيادية آمنة.
- تطبيق استراتيجيات القيادة في إدارة "التعافي الذكي" وضمان المصداقية والسمعة الدولية للدولة.

## محتويات الورشة:

**اليوم الأول :**

### فلسفة الصمود السيادي وتصفير البيروقراطية الأمنية

**هندسة الجاهزية الوطنية والرشاقة في مواجهة التهديدات**

- مفهوم الصمود السيبراني كدرع لحماية السيادة الوطنية وضمان تدفق الخدمات الحيوية دون انقطاع والريادة.
- مواءمة استراتيجيات الصمود مع مبدأ تصفير البيروقراطية عبر أتمتة بروتوكولات الدفاع اللحظي.
- تحليل العلاقة بين "سرعة التعافي" وبين بناء الثقة والمصداقية الدولية في المنظومة التقنية للدولة.
- تمرين هندسة الاستباقية لتصميم دورة عمل تصفّر زمن رصد الاختراقات بنزاهة وشفافية مطلقة والتميز.

**قيادة النزاهة في حوكمة الأصول الحيوية والريادة العالمية**

- تعزيز السيادة على الأنظمة التقنية للبنية التحتية لضمان استقلاليتها وتوافقها مع القيم الوطنية والنمو.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في الإفصاح عن المخاطر وإدارة الأزمات.
- بناء ثقافة "الصمود كمسؤولية مشتركة" وعلاقتها بجودة الحياة والأمن القومي السيادي الشامل والريادة.
- صياغة ميثاق أخلاقيات قائد الصمود السيبراني لدعم النزاهة والقدوة في كافة المستويات القيادية والوطنية.

**اليوم الثاني :**

### السيادة التقنية وهندسة التوائم الرقمية للحماية

**تصفير مخاطر التعطل عبر الذكاء الاصطناعي والمحاكاة التنبؤية**

- توظيف الذكاء الاصطناعي في بناء توائم رقمية للمنشآت تصفّر زمن رصد التهديدات "تحت الرادار."
- حماية "بيانات التشغيل السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية القرارات والنزاهة الرقمية.
- تطبيق الهوية الرقمية للأصول لتصفير الهدر البيروقراطي في إجراءات التحقق والوصول للأنظمة الحساسة.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمؤشرات صمود البنية التحتية.

**حوكمة الأنظمة الخوارزمية والنزاهة في استنباط مخاطر الـOT**

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد أولويات الحماية الفنية.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأثر المناخي أو السيبراني.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من أنظمة التحكم الصناعي (SCADA) لضمان المصداقية.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الصمود بنزاهة تامة والتميز.

**اليوم الثالث :**

**الحياد والعدالة في إدارة استمرارية الخدمات والشمولية**

**هندسة الحماية الشاملة والشمولية الرقمية في إدارة الأثر المجتمعي**

- استخدام التحليلات الذكية لضمان عدالة حماية الخدمات لجميع المناطق بنزاهة وشفافية والريادة والنمو.
- تفعيل الرقابة الأخلاقية على منصات استمرارية الأعمال لضمان الشفافية وحياد النظم الرقمية في النتائج.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات التعافي التي قد تغفل البعد الإنساني أو السيادي.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والتميز.

**المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية**

- حوكمة الشراكات مع مزودي التقنيات العالمية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي لسياسات الصمود لضمان النزاهة والعدالة في حماية الموارد الوطنية.
- بناء سجلات نزاهة رقمية لكل عملية تعافي كبرى لضمان الشفافية المطلقة والوضوح التام والريادة.
- تمرين محاكاة لإدارة حوار تقني حول "الصمود والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

**اليوم الرابع :**

## المسؤولية المهنية وإدارة السمعة والنزاهة في التعافي

### القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات السيبرانية المتسارعة والموازنة بين الإبهار وبين الوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للالتزام بالمعايير وأثرها في تعزيز مصداقية القرار السيادي عالميًا والريادة.
- بناء أنظمة الإفصاح الاستباقي عن محاولات الاختراق المجهضة لضمان الشفافية وتصفير الشائعات المضللة.
- التدقيق الأخلاقي على سلاسل توريد البرمجيات 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 الوطني والسيادة.
- مهارات التواصل الأخلاقي عند حدوث "توقف مؤقت" للخدمة 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 العمل الأمني ضد التلاعب الممنهج بالبيانات والواقع.

**اليوم الخامس :**

## مختبر الابتكار المهني وصناعة نموذج "الصمود السيادي" الريادي

### التطبيق العملي وتصفير البيروقراطية في أنظمة الحماية واستمرارية الأعمال والتميز

- تطوير خارطة الطريق التنفيذية لدمج أدوات الصمود السيبراني في الممارسات اليومية بمرونة ورشاقة تضمن سيادة القرار والتميز والنمو المستدام في عام 2026.
- تصميم بروتوكولات الحوكمة الذكية الخاصة بـ التعافي التلقائي (Self-Healing) لتصفير المسارات البيروقراطية وضمان النزاهة والشفافية والوضوح في إدارة البنى التحتية والريادة العالمية.
- منهجية صياغة ملفات التميز للمنافسة في الجوائز الوطنية (مثل جوائز الأمن السيبراني والحوكمة الرقمية) مع التركيز على الابتكار في "الصمود تحت الضغط" والرشاقة والوضوح والنمو.
- تمرين مختبر المحاكاة لإدارة الأزمات السيبرانية الهجينة وصياغة الحلول الاستباقية الناجحة والتميز في الأداء الحكومي الشامل والسيادة الرقمية المستقلة.

## المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة سيبرانية تضمن نزاهة التعامل مع الأزمات والبيانات الوطنية بنسبة 100%.
- القدرة على هندسة منظومات صمود رشيقة وسيادية تتوافق مع متطلبات الريادة والتميز العالمية الشاملة.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي في النتائج.
- بناء سجل ممارسات فضلى في إدارة الذكاء الاستراتيجي للصمود يدعم اتخاذ القرار القيادي الآمن والمستدام.

## الفئة المستهدفة:

- القيادات العليا ومدراء إدارات تقنية المعلومات والأمن السيبراني في قطاعات الطاقة، المياه، النقل، والصحة.
- مسؤولو الاستراتيجية والتميز المؤسسي وفرق تصفير البيروقراطية في الجهات السيادية والحكومية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بحماية البنية التحتية الوطنية الحيوية.
- رؤساء فرق العمل الميدانية ومحللو المخاطر السيبرانية في المؤسسات الاستراتيجية الكبرى.

## 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)