الأمن التشغيلي والتحكم بالوصول وتصاريح العمل في المواقع الحساسة

الإمارات العربية المتحدة - دبي

2026 / 10 /01 – 09/27

مقدمة:

في عام 2026، لم تعد حماية المواقع الحساسة تقتصر على الأسوار المادية، بل أصبحت تعتمد على "الأمن التشغيلي الذكي" الذي يوازن بين صرامة الحماية وسلاسة العمليات. يهدف هذا البرنامج إلى تمكين القادة من أدوات حوكمة الوصول وتصاريح العمل الرقمية لتصفير البيروقراطية الإجرائية، مع ضمان السيادة الكاملة على بيانات الدخول والتحقق، وترسيخ قيم النزاهة والشفافية في حماية مفاصل الدولة الاستراتيجية.

أهداف الدورة:

- استيعاب مفاهيم الأمن التشغيلي (OPSEC) الحديثة وعلاقتها بالسيادة الرقمية الوطنية.
- تطوير مهارات هندسة "أنظمة الوصول اللحظي" لتصفير البيروقراطية في المواقع الحساسة.
- إتقان فن إدارة "تصاريح العمل الرقمية (Digital PTW) "وتتبع المقاولين بنزاهة وشفافية.
- حوكمة ممارسات الأمن الميداني لضمان التوازن بين الإنتاجية وبين المتطلبات السيادية الصارمة.
- تعزيز السيادة المعلوماتية عبر بناء قواعد بيانات وصول وطنية مستقلة ومحمية سيادياً.
- تطبيق استراتيجيات القيادة في إدارة "الأخطاء البشرية" وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة الأمن التشغيلي (OPSEC) والرشاقة في إدارة المواقع

هندسة الحصانة التشغيلية وتصفير البيروقراطية في الإجراءات

- مفهوم OPSEC 2026 وأثره على السيادة الوطنية وجودة الحياة المهنية والريادة والنمو.
- مواءمة استراتيجيات الأمن مع مبدأ تصفير البيروقراطية عبر أتمتة سجلات الحراسة والمراقبة.
- تحليل العلاقة بين "الأمن الوقائي" وبين بناء الثقة والمصداقية الدولية في المنظومة الوطنية.
- تمرين هندسة الاستباقية لتصميم دورة حياة للمعلومات التشغيلية تصفّر زمن كشف الثغرات بنزاهة.

قيادة النزاهة في حوكمة الأصول السيادية والريادة العالمية

- تعزيز السيادة على الأنظمة التقنية للأمن لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في التعامل مع التسريبات المعلوماتية.
- بناء ثقافة "الأمان كداعم للإنتاجية" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والنمو.
- صياغة ميثاق أخلاقيات قائد الأمن التشغيلي لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة التحكم بالوصول الذكي

تصفير مخاطر التسلل عبر التحقق الحيوي والذكاء الاصطناعي

- توظيف الذكاء الاصطناعي في إدارة الهوية والوصول (IAM) وتصفير احتمالات انتحال الشخصية بنزاهة.
- حماية "بيانات الوصول السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية السجلات والنزاهة الرقمية.
- تطبيق الهوية الرقمية الموحدة للموظفين والمقاولين لتصفير الهدر البيروقراطي في إجراءات التدقيق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحركة الأفراد والأصول.

حوكمة الأنظمة الخوارزمية والنزاهة في منح الصلاحيات

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد "مستويات الوصول."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الذكاء الاصطناعي لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الوصول بنزاهة تامة والسيادة.

اليوم الثالث :

هندسة تصاريح العمل (PTW) والحياد في إدارة الشركاء

تصفير البيروقراطية في تصاريح العمل الرقمية والشمولية

- هندسة أنظمة تصاريح العمل (Permit to Work) التي تصفّر زمن الموافقة مع ضمان أعلى معايير السلامة.
- تفعيل الرقابة الأخلاقية على منصات تتبع المقاولين لضمان الشفافية وحياد النظم الرقمية في النتائج.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق التصاريح وتصفير احتمالات التلاعب بالسجلات بنزاهة.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع شركات الصيانة لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والتميز.
- تطوير آليات رصد الأثر البيئي والمهني لتصاريح العمل لضمان النزاهة والعدالة في النتائج والنمو.
- بناء سجلات نزاهة رقمية لكل عملية تشغيلية كبرى لضمان الشفافية المطلقة والوضوح والريادة.
- تمرين محاكاة لإدارة حوار أمني حول "التصاريح والسرعة" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في المواقع الحساسة

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند حدوث خروقات أمنية أو حوادث مهنية والموازنة بين الإبهار والوقار السيادي.
- الرقابة على البصمة الرقمية للأنظمة والفرق الميدانية لتعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن نجاحات التأمين لتصفير فرص انتشار الشائعات والنزاهة والشفافية.
- التدقيق الأخلاقي على سلاسل توريد أنظمة الوصول لضمان خلوها من الممارسات الضارة والنزاهة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

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

اليوم الخامس :

هندسة الاستجابة الفورية وتصفير البيروقراطية في مواجهة الاختراقات التشغيلية

مختبر "الضغط العالي" وإدارة خروقات الوصول الذكي

- محاكاة اختراق "تحت الرادار": وضع القادة في سيناريو معقد يتضمن محاولة دخول غير مصرح به باستخدام هوية رقمية مزيفة، واختبار قدرة الأنظمة والفرق على الرصد اللحظي وتفعيل "بروتوكول الإغلاق السيادي" بنزاهة ووضوح.
- تصفير البيروقراطية في الاستجابة للطوارئ: تطبيق مسار قرار "صفري الإجراءات" للتعامل مع الحوادث المهنية الكبرى داخل المواقع الحساسة، لضمان وصول فرق الإنقاذ أو الصيانة دون عوائق إدارية، مع الحفاظ على الحصانة الأمنية للأصول.
- هندسة "التحقق المزدوج" تحت الأزمة: اختبار قدرة القائد على الموازنة بين "الأتمتة الذكية" و"الإرادة البشرية" عند تعطل أنظمة الوصول الإلكترونية، وضمان استمرارية العمليات بنزاهة تامة دون المساس بأمن الموقع.
- ورشة "تفكيك سجلات الحوادث": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات التنبؤية، لتحديد الفجوات السلوكية أو التقنية وتطوير حلول استباقية تمنع تكرار الثغرات في الواقع الميداني.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة تشغيلية تضمن نزاهة التعامل مع الأصول والبيانات الوطنية بنسبة 100%.
- القدرة على هندسة منظومات وصول 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 التشغيلي الاستراتيجي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء الأمن، والتشغيل، والصيانة في المواقع الحيوية (طاقة، دفاع، اتصالات).
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي في القطاعات الاستراتيجية.
- خبراء الحوكمة والنزاهة والرقابة الداخلية المعنيون بسلامة الأفراد والأصول السيادية.
- رؤساء فرق التصاريح والمشرفون الميدانيون في الهيئات الاتحادية والمحلية والشركات الوطنية.

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)