الأمن الوقائي المتقدم للشخصيات الهامة وتأمين البصمة الرقمية

الإمارات العربية المتحدة - دبي

2026 / 04 /02 – 03/29

مقدمة:

في عالم 2026، لم تعد حماية الشخصيات الهامة تقتصر على المرافقة الجسدية فحسب، بل أصبحت حماية "البصمة الرقمية" هي الخط الدفاعي الأول والأساسي. إن أي ثغرة في الفضاء السيبراني للشخصية قد تتحول إلى تهديد فيزيائي ملموس. يهدف هذا البرنامج إلى تمكين القادة من هندسة منظومات حماية استباقية تصفّر البيروقراطية في إجراءات التأمين، وتوظف الذكاء الاصطناعي لضمان النزاهة والشفافية في إدارة الخصوصية، مما يعزز ريادة الدولة في تقديم نموذج أمني سيادي وشامل يحمي الرموز والقيادات الوطنية.

أهداف الدورة:

- استيعاب فلسفة "الحماية السيادية" وعلاقتها بالرشاقة المؤسسية وتصفير البيروقراطية في بروتوكولات الأمن.
- تطوير مهارات هندسة "البصمة الرقمية الآمنة" للشخصيات الهامة بنزاهة ووضوح تامة وفق المعايير العالمية.
- إتقان فن مواءمة "الاستخبارات مفتوحة المصدر (OSINT) "مع مستهدفات التميز والريادة الوطنية والسيادة.
- حوكمة البيانات الشخصية والحساسة لضمان حصانتها ضد التلاعب أو الابتزاز الرقمي والنزاهة والشفافية.
- اكتساب مهارات تصفير فجوات التهديد عبر تقنيات "الرصد اللحظي" ورصد نبض السمعة الرقمية والسيادة.
- تعزيز السيادة المعلوماتية من خلال تحصين قنوات التواصل الخاصة ومنع التبعية التقنية في أنظمة التشفير.
- تطبيق استراتيجيات "إدارة الظهور الاستراتيجي" لتعزيز كفاءة الحماية وتصفير مخاطر الهندسة الاجتماعية والتميز.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بخصوصية الشخصية مقابل متطلبات الأمن والنزاهة الوطنية.
- صياغة خارطة طريق شاملة لتحويل "الأمن الوقائي" إلى درع تقني وبشري محصن يدعم الريادة والتميز والسيادة.

محتويات الورشة:

اليوم الأول :

فلسفة الحماية السيادية والرشاقة في التخطيط الوقائي

هندسة الجاهزية الاستباقية وتصفير البيروقراطية في التحرك

- مفهوم الأمن الوقائي 2026 وأثره على السيادة الوطنية وجودة حياة الشخصيات والريادة العالمية.
- مواءمة استراتيجيات التأمين مع مبدأ تصفير البيروقراطية عبر أتمتة تصاريح التحرك والتنسيق اللحظي.
- تحليل العلاقة بين "الأمن غير المرئي" وبين بناء الثقة والمصداقية الدولية في النموذج الأمني للدولة.
- تمرين هندسة الاستباقية لتصميم دورة عمل تأمينية تصفّر زمن تقييم المسارات بنزاهة وشفافية مطلقة.

قيادة النزاهة في حوكمة دوائر الحماية والريادة الوطنية

- تعزيز السيادة على الأنظمة التقنية للحماية لضمان استقلاليتها وتوافقها مع القيم الوطنية والنمو.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في اختيار وتأهيل فرق الحماية الخاصة.
- بناء ثقافة "الأمان الممكن للازدهار" وعلاقتها بالولاء المؤسسي والأمن القومي السيادي الشامل.
- صياغة ميثاق أخلاقيات قائد فرق الحماية لدعم النزاهة والقدوة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة الأنظمة الذكية لتأمين المحيط

تصفير مخاطر الاختراق المادي عبر الدرونات والذكاء الاصطناعي

- توظيف الذكاء الاصطناعي والأنظمة المستقلة في رصد التهديدات المحيطة وتصفير فجوات المراقبة بنزاهة.
- حماية "البيانات اللحظية للتحركات" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنزاهة والتميز.
- تطبيق الهوية الرقمية في توثيق الدخول للمناطق الحساسة لتصفير الهدر البيروقراطي في إجراءات التدقيق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمحيط الشخصيات الهامة والمنشآت.

حوكمة الأنظمة الخوارزمية والنزاهة في رصد التهديدات

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد "الأشخاص ذوي الخطورة."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأهداف.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الكاميرات الذكية لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن الوقائي بنزاهة تامة.

اليوم الثالث :

تأمين البصمة الرقمية والحياد في إدارة الظهور الإلكتروني

هندسة الحماية المعرفية وتصفير البيروقراطية في تنظيف البيانات

- تحليل البصمة الرقمية (Digital Footprint) وكيفية تصفير الهدر المعلوماتي الذي قد يُستغل في الاستهداف.
- تفعيل الرقابة الأخلاقية على منصات التواصل التابعة للشخصية لضمان الشفافية وحياد النظم الرقمية والريادة.
- تطبيق تقنيات "إدارة الخصوصية الاستباقية" لتصفير زمن حذف البيانات الحساسة أو المسربة بنزاهة وشفافية.
- حساب معامل الثقة في مؤشرات الأمن الرقمي للشخصية لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الظهور الرقمي للشخصيات لضمان توافقه مع معايير جودة الحياة والسيادة الوطنية والنزاهة والتميز.
- تطوير آليات رصد التهديدات السيبرانية الموجهة للشخصية لضمان النزاهة والعدالة في حماية الخصوصية والنمو.
- بناء سجلات نزاهة رقمية لكل عملية تدقيق في الحسابات الشخصية لضمان الشفافية المطلقة والوضوح التام.
- تمرين محاكاة لإدارة حوار أمني حول "البصمة الرقمية والحرية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في المواقف الحرجة

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل عند وقوع حوادث أمنية أو تسريبات والموازنة بين الإبهار والوقار السيادي والنزاهة.
- الرقابة على البصمة الرقمية لفرق الحماية وأثرها في تعزيز مصداقية المؤسسة السيادية عالميًا والريادة.
- بناء أنظمة الإفصاح الاستباقي عن الحقائق لتصفير فرص انتشار الشائعات الرقمية المضللة والتميز والنمو.
- التدقيق الأخلاقي على سلاسل توريد الأجهزة الشخصية لضمان خلوها من الممارسات الضارة والنزاهة والشفافية.

حصانة المنظومة الوقائية ضد الانتهاكات المعلوماتية والتلاعب

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

اليوم الخامس :

هندسة الاستجابة الفورية وتصفير البيروقراطية في مواجهة التهديدات الهجينة للشخصيات

مختبر "الحصانة الرقمية" وإدارة خروقات الخصوصية السيادية

- محاكاة اختراق "البصمة الخفية": وضع القادة في سيناريو معقد يتضمن انتحال هوية رقمية للشخصية الهامة باستخدام تقنيات التزييف العميق، واختبار قدرة فرق الحماية على الرصد اللحظي وتفعيل "بروتوكول العزل السيادي" بنزاهة ووضوح تام.
- تصفير البيروقراطية في تأمين المسارات: تطبيق مسار قرار "صفري الإجراءات" لتغيير خطط التحرك الميداني بناءً على تهديد سيبراني رصده الذكاء الاصطناعي، لضمان أمن الشخصية دون عوائق إدارية أو تأخير في التنسيق بين الدوائر الأمنية المختصة.
- هندسة "اليقظة المزدوجة" تحت الضغط: اختبار قدرة القائد على الموازنة بين التحليلات الرقمية للمحيط وبين الحدس الأمني البشري عند تعرض أنظمة المراقبة الذكية للتشويش، وضمان استمرارية الحماية بنزاهة تامة دون المساس بخصوصية الشخصية الهامة.
- ورشة "تفكيك البصمة المسربة": مراجعة فورية لنتائج المحاكاة لتحديد الفجوات في السلوك الرقمي لفرق الحماية، وتطوير حلول استباقية تمنع استغلال البيانات المتاحة في الفضاء الإلكتروني لتنفيذ استهداف ميداني ملموس.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة وقائية 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 الوقائي الاستراتيجي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء إدارات حماية الشخصيات، والمراسم، والتشريفات في الجهات السيادية.
- مسؤولو الأمن الوقائي وفرق تصفير البيروقراطية والتحول الرقمي في المكاتب القيادية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بحماية أسرار وخصوصية الدولة.
- رؤساء فرق العمل الميدانية ومحللو الاستخبارات الوقائية 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)