استراتيجيات مكافحة الجرائم المستحدثة في الفضاء السيبراني والميتافيرس

الإمارات العربية المتحدة - دبي

2026 / 10 /01 – 09/27

مقدمة:

مع دخولنا عام 2026، انتقل مسرح الجريمة من الواقع المادي إلى عوالم افتراضية معقدة "الميتافيرس"، حيث لم تعد الأساليب التقليدية كافية لمواجهة جرائم تزييف الهوية الافتراضية وسرقة الأصول الرقمية. يهدف هذا البرنامج إلى تمكين القادة من أدوات "الأمن الافتراضي الاستباقي" وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في ملاحقة الجناة عبر الحدود الرقمية، مع ضمان أعلى معايير النزاهة والشفافية في حماية السيادة الوطنية في فضاءات "ويب 3.0"، مما يعزز ريادة الدولة كأكثر البيئات الرقمية أماناً واستدامة.

أهداف الدورة:

- استيعاب أنماط الجرائم المستحدثة في الميتافيرس (تزييف الشخصيات، غسل الأموال الرقمي) وعلاقتها بالسيادة الوطنية.
- تطوير مهارات هندسة "الأمن الغامر (Immersive Security) "لتصفير البيروقراطية في رصد الانحرافات السلوكية الافتراضية.
- إتقان فن توظيف تقنيات "بلوكشين" والذكاء الاصطناعي في توثيق الجرائم السيبرانية بنزاهة وشفافية.
- حوكمة ممارسات التحقيق في العوالم الافتراضية لضمان القبول القانوني للأدلة الرقمية المستحدثة.
- تعزيز السيادة المعلوماتية عبر بناء "منصات أمنية افتراضية سيادية" تحمي الأصول الوطنية في الميتافيرس.
- تطبيق استراتيجيات القيادة في إدارة "الأزمات الرقمية العابرة للعوالم" وضمان المصداقية والريادة العالمية.

محتويات الورشة:

اليوم الأول :

فلسفة السيادة في الفضاء الغامر والرشاقة الأمنية

هندسة الحصانة الرقمية وتصفير البيروقراطية في العوالم الافتراضية

- مفهوم الجريمة في الميتافيرس وأثرها على السيادة الرقمية والنسيج الاجتماعي الوطني.
- مواءمة استراتيجيات المكافحة مع مبدأ تصفير البيروقراطية عبر أتمتة رصد المحتوى المخالف في الميتافيرس.
- تحليل العلاقة بين "الأمن الافتراضي" وبين بناء الثقة والمصداقية الدولية في ريادة الدولة وجذب الاستثمار.
- تمرين هندسة الاستجابة الاستباقية لتصميم دورة عمل تصفّر زمن حماية الهوية الرقمية بنزاهة وشفافية.

قيادة النزاهة في حوكمة الهويات الافتراضية والريادة

- تعزيز السيادة على بروتوكولات التحقق من الهوية (Avatars) لضمان استقلاليتها وتوافقها مع القيم الوطنية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في التعامل مع الخصوصية في العوالم الغامرة.
- بناء ثقافة "الأمان الافتراضي الشامل" وعلاقتها بجودة الحياة والنمو الاقتصادي السيادي والوطني.
- صياغة ميثاق أخلاقيات قائد الميتافيرس الأمني لدعم النزاهة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة التحقيق في الأصول الرقمية

تصفير مخاطر الاحتيال عبر بلوكشين والتحليلات الذكية

- توظيف الذكاء الاصطناعي في تتبع تدفقات العملات المشفرة والأصول الرقمية (NFTs) وتصفير مخاطر الغسل المالي.
- حماية "البيانات الافتراضية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية السجلات والنزاهة.
- تطبيق الهوية الرقمية الموحدة (Decentralized ID) لتصفير الهدر البيروقراطي في إجراءات التحقق والتحري.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي للجرائم في منصات الميتافيرس.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط التهديدات الافتراضية

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد الجناة الافتراضيين.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير السلوكيات.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من العوالم الغامرة لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن السيبراني بنزاهة تامة.

اليوم الثالث :

الحياد والعدالة في إدارة البيئة الافتراضية والشمولية

هندسة الحماية الشاملة والشمولية الرقمية في الميتافيرس الوطني

- استخدام التحليلات الذكية لضمان عدالة حماية جميع المستخدمين في البيئات الافتراضية بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات التفاعل الافتراضي لضمان الشفافية وحياد النظم الرقمية في النتائج.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الأمن التي قد تغفل البعد الإنساني أو الهوية.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني للميتافيرس لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع مزودي منصات الميتافيرس لضمان توافقها مع معايير جودة الحياة والسيادة الوطنية.
- تطوير آليات رصد الأثر الاجتماعي للجرائم الافتراضية لضمان النزاهة والعدالة في صون الحريات العامة.
- بناء سجلات نزاهة رقمية لكل عملية مكافحة كبرى في الميتافيرس لضمان الشفافية المطلقة والتميز.
- تمرين محاكاة لإدارة حوار أمني حول "الأمن والقيم في الميتافيرس" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة في بيئة "ويب 3.0"

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات الافتراضية المتسارعة والموازنة بين الإبهار وبين الوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للالتزام الأمني وأثرها في تعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن إحباط جرائم الميتافيرس لضمان الشفافية وتصفير الشائعات المضللة.
- التدقيق الأخلاقي على سلاسل توريد الأصول الرقمية لضمان خلوها من الممارسات غير العادلة أو التجسسية.

حصانة العوالم الافتراضية ضد الانتهاكات المعلوماتية والتلاعب

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات السيادي والريادة الوطنية.
- مهارات التواصل الأخلاقي عند حدوث اختراق لمنصة افتراضية لضمان استعادة الثقة ببيانات صادقة ونزيهة.
- 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 بالحقائق والبيانات.

اليوم الخامس :

مختبر الابتكار المهني وصناعة نموذج "الأمن الافتراضي" الريادي

التطبيق العملي وتصفير البيروقراطية في ملاحقة الجرائم المستحدثة والتميز المؤسسي

- تطوير خارطة الطريق التنفيذية لدمج أدوات الأمن الغامر (Immersive Security) في العمليات اليومية بمرونة ورشاقة تضمن سيادة القرار والتميز والنمو المستدام في عام 2026.
- تصميم بروتوكولات الحوكمة الذكية الخاصة بـ الاستجابة الأمنية في العوالم الافتراضية لتصفير المسارات البيروقراطية وضمان النزاهة والشفافية والوضوح في ملاحقة الجناة عبر الحدود الرقمية والريادة العالمية.
- منهجية صياغة ملفات التميز للمنافسة في الجوائز الوطنية (مثل جوائز الأمن السيبراني، والحوكمة الرقمية، والريادة الأمنية) مع التركيز على الابتكار في "تصفير الجريمة الافتراضية" والرشاقة والوضوح.
- تمرين مختبر المحاكاة لإدارة المعضلات الأمنية في الميتافيرس (مثل سرقة الهوية الرقمية أو غسل الأموال المشفر) وصياغة الحلول الاستباقية الناجحة والتميز في الأداء الحكومي والسيادة الرقمية الكاملة.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة رقمية غامرة تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة 100.%
- القدرة على هندسة منظومات مكافحة 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 الافتراضي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء إدارات مكافحة الجرائم الإلكترونية، والابتكار، والتحول الرقمي.
- مسؤولو الاستراتيجية والتميز المؤسسي وفرق تصفير البيروقراطية في قطاعات الأمن والقضاء.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بتنظيم الفضاءات الافتراضية.
- رؤساء فرق التحقيق الجنائي الرقمي ومحللو الأصول المشفرة في الجهات السيادية.

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)