بناء القدرات الاستخباراتية في المصادر المفتوحة (OSINT) والويب العميق

الإمارات العربية المتحدة - دبي

2026 / 03 /12 – 08

مقدمة:

في عصر الانفجار المعلوماتي، لم تعد العبرة بامتلاك المعلومة، بل بالقدرة على استخلاص "الحقيقة الرقمية" من بين مليارات البيانات المتاحة. يهدف هذا البرنامج إلى تحويل الكوادر الاستخباراتية والبحثية إلى "محللين سياديين" قادرين على اختراق جدران المعلومات العامة والوصول إلى الويب العميق، مع توظيف الذكاء الاصطناعي لتصفير البيروقراطية في عمليات البحث، وضمان أعلى مستويات النزاهة والمصداقية في صناعة التقارير الأمنية والوقائية.

أهداف الدورة:

- استيعاب مفاهيم الاستخبارات الحديثة وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية المعلوماتية.
- تطوير مهارات البحث المتقدم في المصادر المفتوحة باستخدام تقنيات "البصمة الرقمية."
- إتقان فن الإبحار الآمن في الويب العميق (Deep Web) والويب المظلم (Dark Web) لغايات استخباراتية.
- توظيف الذكاء الاصطناعي في تحليل البيانات الضخمة (Big Data) وربط الإشارات الضعيفة.
- حوكمة العمليات الاستخباراتية لضمان النزاهة والامتثال للأطر القانونية والأخلاقية.
- تطبيق استراتيجيات الأمن العملياتي (OPSEC) لحماية الهوية والمهمة أثناء التقصي الرقمي.

محتويات الورشة:

اليوم الأول :

فلسفة الاستخبارات المفتوحة والسيادة الرقمية

هندسة الوعي المعلوماتي وتصفير البيروقراطية في الجمع

- مفهوم OSINT في عام 2026: من البحث التقليدي إلى الاستخبارات التنبؤية والسيادة الوطنية.
- مواءمة دورة حياة الاستخبارات مع مبدأ تصفير البيروقراطية عبر أتمتة جمع البيانات اللحظية.
- تحليل العلاقة بين "دقة المصدر المفتوح" وبين بناء الثقة والمصداقية في القرار القيادي.
- تمرين هندسة الاستباقية لتصميم دورة عمل استخباراتية تصفّر زمن التحقق من الإشاعات الرقمية.

قيادة النزاهة في حوكمة المصادر والريادة العالمية

- تعزيز السيادة على أدوات البحث الرقمي لضمان استقلاليتها عن الخوارزميات الخارجية والتحيز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في تقييم موثوقية المصادر.
- بناء ثقافة "الأمانة المعلوماتية" وعلاقتها بجودة الحياة والأمن القومي السيادي الشامل.
- صياغة ميثاق أخلاقيات المحلل الاستخباراتي الرقمي لدعم النزاهة والتميز في كافة المستويات.

اليوم الثاني :

تقنيات البحث المتقدم وهندسة البصمة الرقمية

تصفير الفجوات المعلوماتية عبر البحث الجغرافي والاجتماعي

- توظيف الذكاء الاصطناعي في الاستخبارات الجغرافية (GEOINT) من مصادر مفتوحة وتصفير احتمالات الخطأ.
- حماية "البيانات الاستخباراتية السيادية" عبر استخدام المتصفحات المعزولة وأنظمة التشفير الوطنية.
- تطبيق تقنيات "الربط المنطقي (Link Analysis) "لتصفير الهدر البيروقراطي في ملاحقة الشبكات الرقمية.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لتدفق المعلومات المفتوحة.

حوكمة الأنظمة الخوارزمية والنزاهة في تتبع الأثر الرقمي

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد "الأشخاص ذوي الأهمية."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأهداف.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من شبكات التواصل الاجتماعي لضمان المصداقية القانونية.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن الاستراتيجي بنزاهة.

اليوم الثالث :

الويب العميق والويب المظلم: السيادة في المناطق المجهولة

هندسة الوصول الآمن والشمولية الرقمية في استكشاف التهديدات

- فهم بنية الويب العميق (Deep Web) وتوظيفها في استرجاع الوثائق والبيانات غير المؤرشفة بنزاهة.
- الإبحار في الويب المظلم :(Dark Web) تكتيكات الرصد الاستباقي للأسواق السوداء والتهديدات الناشئة.
- تطبيق قاعدة الإرادة البشرية القيادية للتحقق من هوية المصادر في البيئات المجهولة وحماية السيادة.
- حساب معامل الثقة في المعلومات المستقاة من المصادر السرية الرقمية لتقليل احتمالات التضليل.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات المعلوماتية لضمان توافق عمليات الجمع مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد التهديدات السيبرانية في الويب المظلم لضمان النزاهة والعدالة في حماية المجتمع.
- بناء سجلات نزاهة رقمية لكل عملية اختراق معلوماتي (للغايات الأمنية) لضمان الشفافية والتميز.
- تمرين محاكاة لإدارة حوار أمني حول "الأخلاقيات في الويب المظلم" بأسلوب قيادي واثق وملهم.

اليوم الرابع :

الأمن العملياتي (OPSEC) وحصانة المحلل الرقمي

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الاستخباراتية

- أخلاقيات التخفي الرقمي والموازنة بين الإبهار التقني وبين الوقار السيادي والالتزام القانوني.
- الرقابة على البصمة الرقمية للمحللين لتعزيز مصداقية المؤسسة وحماية السيادة عالميًا والريادة.
- بناء أنظمة "الهويات المستعارة الآمنة" لضمان الشفافية المؤسسية وتصفير مخاطر كشف المهام.
- التدقيق الأخلاقي على أدوات التخفي والبرمجيات المستخدمة لضمان خلوها من الثغرات والنزاهة.

حصانة المنظومة السيادية ضد الانتهاكات والمعلومات المضللة

- المسؤولية القيادية في التبليغ عن الثغرات التي قد تهدد أمن بنك المعلومات الاستخباراتي والسيادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في تقدير المعلومة لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والمهني.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج التحليل ضد التلاعب الممنهج بالحقائق والواقع.

اليوم الخامس :

هندسة الاستجابة الاستخباراتية وتصفير البيروقراطية في استخلاص الحقيقة الرقمية والسيادة المعلوماتية

مختبر "الحقيقة الرقمية السيادية" وإدارة التقصي في بيئات الويب العميق والمظلم

- محاكاة "تتبع الأثر الرقمي العابر للحدود" والسيادة المعلوماتية: وضع القادة في سيناريو يحاكي رصد تهديد أمني ناشئ في الويب المظلم يستهدف الأصول الحيوية، واختبار القدرة على استخدام أدوات الربط المنطقي لكشف الهويات الرقمية وتفعيل بروتوكول "الحصانة المعلوماتية" بنزاهة ووضوح تام لضمان حماية الأمن القومي.
- تصفير البيروقراطية في "دورة حياة المعلومة الاستخباراتية": تطبيق مسار قرار صفري الإجراءات لتحويل البيانات الخام المستخرجة من المصادر المفتوحة إلى تقارير تنفيذية موجهة لصناع القرار، لضمان استباق التهديدات دون انتظار الدورات الإدارية التقليدية التي قد تسبب تقادم المعلومة، مع الحفاظ على الحصانة القانونية والسيادة الرقمية الكاملة والريادة العالمية الشاملة.
- هندسة "النزاهة المعلوماتية" والتحقق المزدوج: اختبار مهارة القائد في الموازنة بين نتائج التحليل الآلي للبيانات الضخمة وبين "الحكمة البشرية السيادية" لضمان عدم السقوط في فخ التضليل الرقمي، وضمان استقرار المصداقية الدولية والريادة في جودة التقارير الاستخباراتية بنزاهة وشفافية مطلقة عبر تطبيق معايير دقيقة لقياس موثوقية المصادر وقيمة التحقق الرقمي دون الاعتماد على معادلات جامدة.
- ورشة "تفكيك صوامع البيانات والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات السلوكية لتحديد الفجوات في "الأمن العملياتي"، وتطوير حلول هندسية استباقية تمنع كشف الهوية الرقمية للمحللين، مما يحقق التميز في الأداء الاستخباراتي والوضوح التام أمام الجهات العليا والشركاء الدوليين بأسلوب قيادي واثق وملهم.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة معلوماتية تضمن نزاهة التعامل مع التهديدات والبيانات 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 الاستخباراتي يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات والمدراء في إدارات التحليل الاستخباراتي، والأمن الوطني، ومكافحة الجرائم الإلكترونية.
- مسؤولو التخطيط الاستراتيجي وفرق استشراف المستقبل في الجهات السيادية والحكومية.
- خبراء التحول الرقمي والحوكمة والنزاهة المعنيون بضبط جودة ومصداقية المعلومات.
- محللو البيانات والباحثون في مراكز الدراسات الاستراتيجية وغرف العمليات الأمنية.

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)