استخدام الذكاء الاصطناعي والتعلم الآلي في عمليات الدفاع السيبراني الاستباقي

الإمارات العربية المتحدة - دبي

05 – 09/ 04 / 2026

مقدمة:

في المشهد السيبراني لعام 2026، لم يعد العنصر البشري وحده كافياً لمواجهة الهجمات التي تتم بسرعة البرمجيات. إن الذكاء الاصطناعي (AI) والتعلم الآلي (ML) هما "الدرع العصبي" الذي يمنح الدولة القدرة على التنبؤ والاعتراض والتعافي اللحظي. يهدف هذا البرنامج إلى تمكين القادة من أدوات الدفاع الذكي وتوظيف الخوارزميات السيادية لتصفير البيروقراطية في مراكز العمليات الأمنية (SOC)، مما يضمن النزاهة المطلقة والريادة العالمية في بناء "الحصانة الرقمية الذكية".

أهداف الدورة:

- استيعاب مفاهيم "الدفاع السيبراني المعزز بالذكاء الاصطناعي" وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة "نماذج التعلم الآلي" لاكتشاف التهديدات غير المعروفة.(Zero-day)
- إتقان فن توظيف النماذج اللغوية الكبيرة (LLMs) في أتمتة تحليل الحوادث وصياغة تقارير الاستجابة.
- حوكمة ممارسات الذكاء الاصطناعي الدفاعي لضمان الشفافية والنزاهة وتجنب الانحيازات الخوارزمية.
- تعزيز السيادة المعلوماتية عبر بناء "محركات دفاع وطنية" تعتمد على نماذج ذكاء اصطناعي مستقلة.
- تطبيق استراتيجيات القيادة في إدارة "الأمن الذاتي (Autonomous Security) "وضمان المصداقية الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة الدفاع الذكي والرشاقة في مواجهة "الهجمات بسرعة الضوء"

هندسة الحصانة الخوارزمية وتصفير البيروقراطية في مراكزSOC

- مفهوم الدفاع السيبراني الذكي 2026: الانتقال من القواعد الجامدة إلى "الوعي السلوكي" والريادة والنمو.
- مواءمة استراتيجيات الدفاع مع مبدأ تصفير البيروقراطية عبر أتمتة دورة حياة التنبيهات (Alert Lifecycle).
- تحليل العلاقة بين "سرعة الذكاء الاصطناعي" وبين بناء الثقة والمصداقية الدولية في المنظومة الرقمية.
- تمرين هندسة الاستباقية لتصميم منظومة دفاعية تصفّر زمن "الاكتشاف حتى الاحتواء" بنزاهة وشفافية.

قيادة النزاهة في حوكمة "القرار الآلي" والريادة الوطنية الشاملة

- تعزيز السيادة على نماذج الذكاء الاصطناعي الدفاعية لضمان استقلاليتها وتوافقها مع القيم والهوية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في التدخل البشري-(Human-in-the-loop).
- بناء ثقافة "الأمان المعتمد على الخوارزمية" وعلاقتها بجودة الحياة والولاء المؤسسي والنمو والتميز.
- صياغة ميثاق أخلاقيات قائد الدفاع السيبراني الذكي لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة اكتشاف الشذوذ السلوكي(ML-based Detection)

تصفير مخاطر التهديدات المتقدمة (APT) عبر نماذج التعلم العميق

- توظيف الشبكات العصبية العميقة (Deep Learning) في تحليل التزييف والأنماط المشبوهة وتصفير احتمالات الخطأ.
- حماية "البيانات التدريبية السيادية" عبر تقنيات التعلم الاتحادي (Federated Learning) لضمان النزاهة الرقمية.
- تطبيق الهوية الرقمية للنماذج (Model Identity) لتصفير الهدر البيروقراطي في إجراءات التدقيق والتحقق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لنتائج التحليل التنبؤي للمخاطر.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط مستويات الخطر

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

اليوم الثالث :

الذكاء الاصطناعي التوليدي (GenAI) والحياد في أتمتة الاستجابة

تصفير البيروقراطية في تحليل الحوادث والشمولية الرقمية

- استخدام النماذج اللغوية الكبيرة (LLMs) في شرح التهديدات المعقدة وتصفير زمن كتابة التقارير الفنية.
- تفعيل الرقابة الأخلاقية على منصات "مساعدي الأمن الذكي" لضمان حياد النظم الرقمية والتميز والنمو.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق مخرجات الذكاء الاصطناعي وتصفير احتمالات التلاعب بنزاهة.
- حساب معامل الثقة في مؤشرات الإنجاز الدفاعي لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والسيادة.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي تقنيات الذكاء الاصطناعي لضمان توافقها مع معايير السيادة والنزاهة والنمو.
- تطوير آليات رصد الأثر الاجتماعي للقرارات المؤتمتة لضمان النزاهة والعدالة في حماية الخدمات والتميز.
- بناء سجلات نزاهة رقمية لكل خوارزمية دفاعية سيادية لضمان الشفافية المطلقة والوضوح والريادة.
- تمرين محاكاة لإدارة حوار أمني حول "الذكاء الاصطناعي والخصوصية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في العصر الذكي

القيادة الاتصالية وحماية السمعة الرقمية ضد الهجمات المعاكسة(Adversarial AI)

- أخلاقيات التواصل عند وقوع هجمات تستهدف "تسميم نماذج الذكاء الاصطناعي" والموازنة بين الإبهار والوقار.
- الرقابة على البصمة الرقمية للنماذج السيادية لتعزيز مصداقية القرار السيادي عالمياً والريادة والتميز.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الحصانة الخوارزمية" لتصفير فرص انتشار الشائعات والنزاهة والشفافية.
- التدقيق الأخلاقي على سلاسل توريد البيانات والبرمجيات لضمان خلوها من الممارسات الضارة والسيادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك معلومات الذكاء الاصطناعي والريادة.
- مهارات التواصل الأخلاقي عند حدوث "هلوسة خوارزمية" 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 الدفاع ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "Native AI" القدوة: من الدفاع الآلي إلى السيادة الخوارزمية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في الدفاع الذكي

- مصفوفة "النبض اللحظي" للتهديدات الخوارزمية: تصميم نظام رصد سيادي يعتمد على التعلم العميق لتحويل أنماط "الشذوذ السلوكي" في الشبكات إلى نبضات استراتيجية تظهر للقائد فوراً، مما يصفّر زمن "الاكتشاف حتى الاحتواء" ويضمن استباق الهجمات التي تستهدف تسميم النماذج (Model Poisoning) بنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للاستجابة المستقلة (Autonomous Response): هندسة مسار قرار "صفري الإجراءات" يسمح لمنظومة الذكاء الاصطناعي بتنفيذ عمليات "العزل التلقائي" للأصول المصابة فور رصد النبضة الاستراتيجية للهجوم، مما يضمن استمرارية الخدمات الحكومية الحيوية دون قيود بيروقراطية أو انتظار للاعتمادات البشرية في الأزمات فائقة السرعة.
- حوكمة "الحقيقة الرقمية" والنزاهة الخوارزمية: وضع ضوابط أخلاقية تضمن خلو نماذج الدفاع من "الانحيازات الرقمية"، وتفعيل ميثاق "النزاهة في البيانات التدريبية" لضمان استقلالية القرار الأمني الوطني والوضوح التام أمام صانع القرار.
- مختبر "هندسة الحصانة ضد الهجمات المعاكسة": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة" ناتجة عن هجوم يستهدف خوارزميات الدفاع نفسها، وكيفية تفعيل بروتوكول "التدخل البشري الحكيم" لحماية السيادة المعلوماتية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة خوارزمية تضمن نزاهة التعامل مع البيانات والبيئات الوطنية بنسبة 100%.
- القدرة على هندسة منظومات رصد واستجابة رشيقة وسيادية تتوافق مع معايير 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 للدفاع يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء الأمن السيبراني، والتحول الرقمي، ومختبرات الابتكار التقني.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي في القطاعات السيادية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بسلامة وصحة الأنظمة الذكية.
- رؤساء فرق المهام السيبرانية وعلماء بيانات الأمن 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)