



الصيد الاستباقي للتهديدات (Threat Hunting) باستخدام الذكاء الاصطناعي



الإمارات العربية المتحدة - دبي

2026 / 04 / 23 – 19



مقدمة:

في المشهد الأمني المتطور لعام 2026، لم يعد الانتظار خلف جدران الحماية كافياً؛ فالسيادة الرقمية تقتضي الانتقال من الدفاع السلبي إلى "الصيد النشط". يهدف هذا البرنامج إلى تمكين القادة من أدوات الصيد الاستباقي للتهديدات وتوظيف الذكاء الاصطناعي لتمشيط البيئات الرقمية بحثاً عن المخاطر الكامنة وتصفير البيروقراطية في عمليات الكشف والتحقيق، مع ضمان أعلى معايير النزاهة والمصداقية الوطنية، مما يعزز قيادة الدولة كحصن أمني ذكي ومنيع.

أهداف الدورة:

- استيعاب مفاهيم "الصيد الاستباقي (Threat Hunting)" وعلاقتها بالسيادة الرقمية الوطنية.
- تطوير مهارات هندسة "فرضيات الصيد" باستخدام التحليلات السلوكية المدعومة بالذكاء الاصطناعي.
- إتقان فن توظيف التعلم الآلي في اكتشاف الأنماط الإجرامية الخفية (Low and Slow) بنزاهة.
- حوكمة ممارسات الصيد لضمان التوازن بين الملاحقة الأمنية وبين حماية الخصوصية السيادية.
- تعزيز السيادة المعلوماتية عبر بناء "منصات صيد وطنية" تعتمد على خوارزميات سيادية مستقلة.
- تطبيق استراتيجيات القيادة في إدارة "نتائج الصيد" وضمان الشفافية والمصداقية أمام صانع القرار.



محتويات الورشة:

اليوم الأول :

فلسفة الصيد السيادي والرشاقة في مواجهة المجهول

هندسة الاستباقية وتصفير البيروقراطية في رصد التسلل

- مفهوم الصيد الاستباقي 2026 وأثره على السيادة الوطنية وجودة الحياة والريادة العالمية والنمو.
- موازنة استراتيجيات الصيد مع مبدأ تصفير البيروقراطية عبر أتمتة جمع البيانات من الأصول الرقمية.
- تحليل العلاقة بين "عقلية الصياد" وبين بناء الثقة والمصادقية الدولية في المنظومة الأمنية للدولة.
- تمرين هندسة الفرضيات لتصميم دورة عمل صيد تصفّر زمن العثور على المهاجمين بنزاهة وشفافية.

قيادة النزاهة في حوكمة رحلة الصيد والريادة الوطنية

- تعزيز السيادة على أدوات الصيد والتحليل لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في التعامل مع "الإنذارات الخاطئة".
- بناء ثقافة "الأمن النشط كمسؤولية قيادية" وعلاقتها بالولاء المؤسسي والنمو القومي الشامل.
- صياغة ميثاق أخلاقيات قائد فرق الصيد لدعم النزاهة والقُدوة والتميز في كافة المستويات.

اليوم الثاني :

السيادة التقنية وهندسة الصيد بالتحليل السلوكي والذكاء الاصطناعي

تصفير مخاطر التخفي عبر خوارزميات اكتشاف الشذوذ السلوكي

- توظيف الذكاء الاصطناعي في تمييز السلوكيات البشرية الطبيعية عن تحركات البرمجيات الخبيثة بنزاهة.
- حماية "بيانات الصيد السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية الاستدلالات والنزاهة الرقمية.
- تطبيق الهوية الرقمية في تتبع مسارات المستخدمين لتصفير الهدر البيروقراطي في إجراءات التحقق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لعمليات الصيد النشطة.



حوكمة الأنظمة الخوارزمية والنزاهة في استنباط التهديدات

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد "المؤشرات المشبوهة".
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من نقاط النهاية (Endpoints) لضمان المصادقية القانونية.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الصيد الأمني بنزاهة تامة.

اليوم الثالث :

هندسة البيانات والحياد في إدارة مصادر الصيد والشمولية

تصنيف البيروقراطية في هندسة البيانات الأمنية والشمولية

- تحليل البيانات الضخمة المستخرجة من السجلات (Logs) وتصنيف زمن الربط المنطقي بين الأحداث المشبوهة.
- تفعيل الرقابة الأخلاقية على منصات الصيد لضمان الشفافية وحياد النظم الرقمية في النتائج والتميز.
- تطبيق تقنيات "الصيد في السحابة السيادية" لتصنيف زمن احتواء التهديدات العابرة للحدود بنزاهة وشفافية.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع مزودي المعلومات الأمنية لضمان توافرها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي للعمليات الأمنية الاستباقية لضمان النزاهة والعدالة في النتائج والتميز.
- بناء سجلات نزاهة رقمية لكل عملية صيد كبرى لضمان الشفافية المطلقة والوضوح والريادة العالمية.
- تمرين محاكاة لإدارة حوار أمني حول "الصيد الاستباقي والخصوصية" بأسلوب قيادي واثق وملهم.



اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في البلاغات الأمنية

القيادة الاتصالية وحماية السمعة الرقمية للجهازية الوطنية

- أخلاقيات التواصل عند الكشف عن تهديدات كامنة مجهزة والموازنة بين الإبهار والوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للأنظمة والفرق الفنية لتعزيز مصداقية القرار السيادي عالمياً والريادة والتميز.
- بناء أنظمة الإفصاح الاستباقي عن نجاحات الصيد لتصفير فرص انتشار الشائعات الرقمية والنزاهة التامة.
- التدقيق الأخلاقي على سلاسل توريد برمجيات الصيد لضمان خلوها من الممارسات الضارة والنزاهة والشفافية.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك معلومات الصيد والسيادة الوطنية.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "فرضية الصيد" لضمان استعادة الثقة ببيانات صادقة ونزيهة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والنزاهة والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحسين نتائج الصيد ضد التلاعب الممنهج بالبيانات والواقع الرقمي.



اليوم الخامس :

هندسة الاستجابة الفورية وتصفير البيروقراطية في مواجهة التهديدات السيبرانية الكامنة

مختبر "الصيد السيادي" وإدارة فرضيات الاختراق تحت الضغط

- محاكاة اختراق "العدو الصامت" والسيادة الرقمية: وضع القادة في سيناريو معقد يحاكي تسلاً خفياً طويل الأمد (APT) داخل شبكة سيادية وطنية، واختبار قدرة الخوارزميات والفرق على صيد التهديد قبل تنفيذ هجومه النهائي، وتفعيل "بروتوكول العزل اللحظي" بنزاهة ووضوح تام لضمان حماية الموارد الحساسة.
- تصفير البيروقراطية في "الاستجابة للاكتشاف": تطبيق مسار قرار "صفري الإجراءات" للانتقال الفوري من مرحلة "الاشتباه السلوكي" إلى مرحلة "الاحتواء الرقمي" الموجه، لضمان حماية الأصول السيادية دون انتظار الموافقات الإدارية التقليدية التي قد تمنح المهاجم فرصة للهروب، مع الحفاظ على الحصانة القانونية للأدلة والريادة العالمية الشاملة.
- هندسة "الحدس الرقمي" تحت الأزمات: اختبار قدرة القائد على الموازنة بين مخرجات أنظمة "الاكتشاف الشذوذ السلوكي" وبين الحكمة البشرية القيادية عند تعارض البيانات، لضمان استمرارية الخدمات بنزاهة تامة ودون المساس بالسيادة المعلوماتية أو التسبب في "إنذارات كاذبة" تضر بجودة الحياة المهنية والمصادقية الدولية والنمو.
- ورشة "تشريح مسارات التسلل": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات السلوكية لتحديد "الفجوات الدفاعية" الكامنة، وتطوير حلول هندسية استباقية تمنع تكرار التسلل في الواقع الميداني، مما يحقق التميز في الأداء الأمني والوضوح التام أمام صانع القرار والريادة العالمية

المخرجات الرئيسية للدورة:

- امتلاك استراتيجيات حصانة استباقية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة 100%.
- القدرة على هندسة منظومات صيد رشيفة 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 للصيد يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.



الفئة المستهدفة:

- القيادات العليا ومدراء مراكز العمليات الأمنية (SOC) وفرق الاستجابة للحوادث (IR).
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية في القطاعات السيادية.
- خبراء التحول الرقمي والحوكمة والنزاهة المعنيون بضبط جودة العمليات الاستخباراتية السيبرانية.
- رؤساء فرق صيد التهديدات ومحللو البيانات الأمنية 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 أو الخاص. (Expert Panels)
- المختبرات التكنولوجية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)