الصيد الاستباقي للتهديدات والاستجابة المتقدمة للحوادث السيبرانية (DFIR)

الإمارات العربية المتحدة - دبي

15 – 19/ 03 / 2026

مقدمة:

في الفضاء السيبراني لعام 2026، لم يعد الانتظار خلف جدران الحماية خياراً استراتيجياً؛ فالسيادة الرقمية تقتضي الانتقال من الدفاع الساكن إلى "الصيد النشط". يجمع هذا البرنامج بين فن الصيد الاستباقي (Threat Hunting) وعلوم التحقيق الجنائي الرقمي والاستجابة للحوادث (DFIR). يهدف البرنامج إلى تمكين القادة من أدوات الكشف المبكر وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في التحقيقات السيبرانية، مع ضمان أعلى معايير النزاهة والشفافية في حماية مفاصل الدولة، مما يعزز ريادة المنظومة الأمنية عالمياً.

أهداف الدورة:

- استيعاب مفاهيم "المنعة السيادية" وعلاقتها بالصيد الاستباقي وتصفير البيروقراطية.
- تطوير مهارات هندسة "فرضيات الصيد" باستخدام التحليلات السلوكية والذكاء الاصطناعي.
- إتقان فن التحقيق الجنائي الرقمي (Digital Forensics) وضمان سلامة الأدلة السيادية.
- بناء خطط استجابة رشيقة (Agile Incident Response) تصفّر زمن احتواء التهديدات.
- حوكمة ممارسات DFIR لضمان النزاهة والشفافية أمام الجهات الرقابية والقضائية.
- تطبيق استراتيجيات القيادة في إدارة الأزمات الرقمية الكبرى وضمان السمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة "الصيد السيادي" والرشاقة في الكشف المبكر

هندسة الاستباقية وتصفير البيروقراطية في رصد التسلل

- مفهوم الصيد الاستباقي 2026: الانتقال من الاستجابة للإنذارات إلى "البحث عن الأثر" والريادة والنمو.
- مواءمة استراتيجيات الصيد مع مبدأ تصفير البيروقراطية عبر أتمتة جمع البيانات من كافة الأصول الرقمية.
- تحليل العلاقة بين "عقلية الصياد" وبين بناء الثقة والمصداقية 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 الشاملة

- تعزيز السيادة على أدوات الصيد والتحليل لضمان استقلاليتها وتوافقها مع القيم والهوية الوطنية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في التعامل مع "النتائج الإيجابية الخاطئة."
- بناء ثقافة "الأمن النشط كمسؤولية قيادية" وعلاقتها بجودة الحياة والولاء المؤسسي والنمو والريادة.
- صياغة ميثاق أخلاقيات قائد فرق الصيد السيادي لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة الصيد بالذكاء الاصطناعي(AI Hunting)

تصفير مخاطر التخفي عبر خوارزميات اكتشاف الشذوذ السلوكي

- توظيف الذكاء الاصطناعي في تمييز الأنماط الإجرامية الخفية (Low and Slow) وتصفير احتمالات الخطأ.
- حماية "بيانات الصيد السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية الاستدلالات والنزاهة الرقمية والتميز.
- تطبيق الهوية الرقمية في تتبع مسارات المهاجمين لتصفير الهدر البيروقراطي في إجراءات التحقق والتحري.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لعمليات الصيد النشطة والنمو.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط التهديدات المتقدمة

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد "مؤشرات الاختراق.(IOCs) "
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار والنمو.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الـ "ويب المظلم" لضمان المصداقية أمام صانع القرار والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الصيد بنزاهة تامة والتميز.

اليوم الثالث :

التحقيق الجنائي الرقمي (DF) والحياد في حماية الأدلة

تصفير البيروقراطية في "سلسلة الحيازة الرقمية" والشمولية

- هندسة عمليات التحقيق الجنائي التي تصفّر زمن استخراج الأدلة مع ضمان أعلى معايير النزاهة القانونية.
- تفعيل الرقابة الأخلاقية على منصات الفحص الجنائي لضمان حياد النظم الرقمية في النتائج والتميز والريادة.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق الأدلة السيادية وتصفير احتمالات التلاعب بنزاهة وشفافية.
- حساب معامل الثقة في مؤشرات الإنجاز الجنائي لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والنمو.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع المختبرات الدولية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والنمو.
- تطوير آليات رصد الأثر القانوني والاجتماعي للتحقيقات الرقمية لضمان النزاهة والعدالة والتميز والريادة.
- بناء سجلات نزاهة رقمية لكل عملية فحص جنائي كبرى لضمان الشفافية والوضوح والريادة العالمية الشاملة.
- تمرين محاكاة لإدارة حوار قانوني حول "مشروعية الدليل الرقمي" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

الاستجابة المتقدمة للحوادث (IR) وإدارة السمعة

القيادة الاتصالية وحماية السمعة الرقمية أثناء الاستجابة للأزمات

- أخلاقيات التواصل في الأزمات السيبرانية المتسارعة والموازنة بين الإبهار والوقار السيادي والنزاهة والتميز.
- الرقابة على البصمة الرقمية لفرق الاستجابة لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو الشامل.
- بناء أنظمة الإفصاح الاستباقي عن نجاحات الاحتواء لتصفير فرص انتشار الشائعات والنزاهة والشفافية التامة.
- التدقيق الأخلاقي على سلاسل توريد برمجيات الاستجابة لضمان خلوها من الممارسات الضارة والسيادة والريادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

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

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "المحصن" القدوة: من مطاردة الأثر إلى هندسة السيادة الدفاعية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في الصيد والاستجابة

- مصفوفة "النبض اللحظي" لصيد التهديدات: تصميم نظام رصد سيادي يعتمد على التحليلات السلوكية لتحويل "الإشارات الضعيفة" في الشبكات إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن "البقاء داخل الشبكة (Dwell Time) "للمهاجمين، وضمان اكتشاف التسلل في مرحلة التكون وبنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للاحتواء الفوري: هندسة مسار قرار "صفري الإجراءات" يسمح لفرق الاستجابة المتقدمة بتنفيذ عمليات "العزل الذكي" للأصول المستهدفة فور رصد النبضة الاستراتيجية للحادث. يضمن هذا البروتوكول استمرارية الخدمات الحكومية الحيوية دون قيود بيروقراطية أو تأخير في طلب الاعتمادات الإدارية أثناء الأزمات المتسارعة.
- حوكمة "الحقيقة الرقمية" والنزاهة في DFIR: وضع ضوابط أخلاقية تضمن سلامة "سلسلة الحيازة الرقمية (Chain of Custody) "للأدلة السيادية، وتفعيل ميثاق "النزاهة في التحقيق الجنائي" لضمان خلو التقارير من الانحيازات الرقمية والوضوح التام أمام صانع القرار والجهات القضائية.
- مختبر "هندسة الحصانة ضد الأزمات الرقمية": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة حادث سيبري كبرى"، وكيفية توجيه الموارد التقنية والاتصالية لاستعادة العمليات وحماية السمعة الوطنية والسيادة المعلوماتية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة سيبرانية تضمن نزاهة التعامل مع الحوادث والبيانات 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 والنمو.
- بناء سجل ممارسات فضلى في إدارة الذكاء الاستراتيجي للحوادث يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات والمدراء في إدارات الأمن السيبراني، ومراكز العمليات الأمنية(SOC) ، والاستجابة للطوارئ.(CERT)
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية في القطاعات السيادية.
- خبراء التحقيق الجنائي الرقمي والحوكمة والنزاهة المعنيون بضبط جودة الأدلة الرقمية.
- رؤساء فرق صيد التهديدات ومحللو التهديدات المتقدمة (APT) 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)