محاكاة الهجمات السيبرانية المتقدمة (APT) واختبار جاهزية الدفاعات

الإمارات العربية المتحدة - دبي

05 – 09/ 07 / 2026

مقدمة:

في المشهد الأمني لعام 2026، لم تعد الهجمات السيبرانية مجرد محاولات عشوائية، بل أصبحت "عمليات استراتيجية طويلة الأمد" تقودها دول أو منظمات احترافية تحت مسمى التهديدات المتقدمة المستمرة (APT). إن السيادة الرقمية تقتضي ألا ننتظر الهجوم، بل أن نحاكيه بأنفسنا لنكشف نقاط الضعف قبل الخصوم. يهدف هذا البرنامج إلى تمكين القادة من أدوات "الهجوم المخطط" وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في تقارير الثغرات، مع ضمان أعلى معايير النزاهة والشفافية في بناء حصون رقمية لا تخترق، مما يعزز ريادة الدولة كقوة سيبرانية مهابة الجانب.

أهداف الدورة:

- استيعاب فلسفة "الهجوم من أجل الدفاع" وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة "سيناريوهات APT" واقعية تحاكي أساليب الفاعلين الدوليين الأكثر تعقيداً.
- إتقان فن "الفريق الأرجواني (Purple Teaming)" لدمج قدرات الهجوم والدفاع بنزاهة وشفافية.
- حوكمة ممارسات اختبار الاختراق لضمان التوازن بين كشف الثغرات وبين استمرارية الأعمال الحيوية.
- تعزيز السيادة المعلوماتية عبر بناء "منصات محاكاة وطنية" مستقلة عن الحلول التجارية الخارجية.
- تطبيق استراتيجيات القيادة في إدارة "نتائج الاختبارات" وضمان المصداقية أمام القيادة العليا والنمو.

محتويات الورشة:

اليوم الأول :

فلسفة "التفكير بعقلية المهاجم" والرشاقة في كشف الفجوات

هندسة الجاهزية الهجومية وتصفير البيروقراطية في رصد الثغرات

- مفهوم محاكاة APT 2026 وأثرها على السيادة الوطنية وجودة الحياة والريادة العالمية والنمو.
- مواءمة استراتيجيات المحاكاة مع مبدأ تصفير البيروقراطية عبر أتمتة دورة "الاختبار-التقرير-المعالجة."
- تحليل العلاقة بين "الصدق في كشف الفجوات" وبين بناء الثقة والمصداقية الدولية في النموذج الأمني.
- تمرين هندسة الاستباقية لتصميم سيناريو هجوم يصفّر زمن اكتشاف مسارات التسلل بنزاهة وشفافية.

قيادة النزاهة في حوكمة "الفريق الأحمر" والريادة الوطنية الشاملة

- تعزيز السيادة على أدوات الاختبار لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في الإفصاح عن نتائج الاختبارات الحرجة.
- بناء ثقافة "المصارحة التقنية" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والنمو والريادة.
- صياغة ميثاق أخلاقيات قائد فرق المحاكاة لدعم النزاهة والقدوة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة المحاكاة بالذكاء الاصطناعي(AI Red Teaming)

تصفير مفاجآت الهجوم عبر الأتمتة الذكية والتحليلات التنبؤية

- توظيف الذكاء الاصطناعي في محاكاة أساليب "الهجوم المتكيف" وتصفير فجوات المراقبة الميدانية بنزاهة.
- حماية "سجلات الاختبار السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية النتائج والنزاهة الرقمية.
- تطبيق الهوية الرقمية للفرق المشاركة لتصفير الهدر البيروقراطي في إجراءات الترخيص والولوج الميداني.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لنتائج محاكاة الهجوم والنمو.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط سيناريوهات الاختراق

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في إصدار "قرارات الهجوم المحاكى."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأضرار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من إطار MITRE ATT&CK لضمان المصداقية والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات المحاكاة بنزاهة تامة والتميز.

اليوم الثالث :

هندسة "الفريق الأرجواني" والحياد في إدارة التحالفات الدفاعية

تصفير البيروقراطية في "التعاون بين الهجوم والدفاع" والشمولية الرقمية

- هندسة نموذج Purple Teaming الذي يصفّر زمن نقل المعرفة من المهاجم إلى المدافع بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات التنسيق الأمني لضمان حياد النظم الرقمية والتميز والنمو الشامل.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق خطوات المحاكاة وتصفير احتمالات التلاعب بالسجلات.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والسيادة.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع شركات الاختبار الدولية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي والاقتصادي لنجاح المحاكاة في حماية الخدمات والتميز والنمو.
- بناء سجلات نزاهة رقمية لكل عملية "هجوم مخطط" كبرى لضمان الشفافية والوضوح والريادة والسيادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "نتائج الاختبار والجدارة القيادية" بأسلوب واثق وملهم.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في "إدارة الثغرات"

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند الكشف عن "ثغرات من الدرجة الصفرية" والموازنة بين الإبهار والوقار والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة المختبرة لتعزيز مصداقية القرار السيادي عالمياً والريادة والتميز.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الدفاعات المحصنة" لتصفير فرص انتشار الشائعات والنزاهة.
- التدقيق الأخلاقي على سلاسل توريد برمجيات الاختبار 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 الاختبار والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "محاكاة الأزمة" لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج الرصد ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "المهاجم-المدافع" القدوة: من محاكاة الاختراق إلى هندسة الحصانة الوطنية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في محاكاةAPT

- مصفوفة "النبض اللحظي" للتهديدات المتقدمة: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل سيناريوهات المحاكاة إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن "اكتشاف مسار الهجوم (Attack Path Discovery) "وضمان فحص جاهزية الأنظمة الحيوية بنزاهة ومصداقية تامة ضد أساليب APT الدولية.
- بروتوكول "الرشاقة السيادية" للمعالجة الاستباقية: هندسة مسار قرار "صفري الإجراءات" يسمح لفرق الدفاع بتحديث القواعد الأمنية آلياً فور رصد النبضة الاستراتيجية التي تكشف ثغرة حرجة أثناء المحاكاة. يضمن هذا البروتوكول إغلاق الفجوات دون قيود بيروقراطية أو انتظار لتقارير ورقية مطولة تعطل سرعة التحصين الدفاعي.
- حوكمة "الصدق الهجومي" والنزاهة الرقمية: وضع ضوابط أخلاقية تضمن واقعية محاكاة "الفريق الأحمر(Red Teaming) "، وتفعيل ميثاق "النزاهة في الإفصاح" لضمان الوضوح التام أمام صانع القرار بشأن نقاط الضعف الحقيقية، بعيداً عن الانحيازات الرقمية أو محاولات تجميل النتائج.
- مختبر "هندسة الحصانة ضد الأزمات المصطنعة": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة سيبرانية كبرى" تم هندستها بعناية، وكيفية تفعيل بروتوكول "التعاون الأرجواني" (Purple Teaming) لحظياً لضمان السيادة المعلوماتية والتعافي السريع.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة هجومية تضمن نزاهة التعامل مع الثغرات والبيانات الوطنية بنسبة %.100
- القدرة على هندسة منظومات اختبار 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 للاختبار يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء مراكز العمليات الأمنية(SOC) ، وفرق الاستجابة(CERT) ، ومدراء أمن المعلومات.(CISOs)
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية في القطاعات السيادية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة الأنظمة الوطنية والتميز.
- رؤساء فرق الاختبار (Red Teams) ومحللو التهديدات المتقدمة 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)