إدارة الثغرات والاختبار الاختراقي للشبكات
(Network Pentesting)

الإمارات العربية المتحدة - دبي

2026 / 08 /20 – 16

مقدمة:

في المشهد الرقمي لعام 2026، لم يعد اختبار الاختراق مجرد "تدقيق تقني"، بل أصبح أداة استراتيجية لقياس صلابة السيادة الوطنية. إن اكتشاف الثغرة قبل الخصم هو قمة الرشاقة الأمنية.

يهدف هذا البرنامج إلى تمكين القادة من أدوات "الهجوم الاستباقي" وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في رحلة اكتشاف ومعالجة الفجوات الأمنية، مع ضمان أعلى معايير النزاهة والمصداقية في حماية الأعصاب الرقمية للدولة، مما يعزز ريادة المنظومة الدفاعية عالمياً.

أهداف الدورة:

- استيعاب مفاهيم "الحصانة الشبكية" وعلاقتها بالأمن القومي وتصفير البيروقراطية.
- تطوير مهارات هندسة "اختبارات الاختراق الهادفة (Goal-Oriented Pentesting) " للأنظمة الحيوية.
- إتقان فن إدارة "دورة حياة الثغرات (Vulnerability Lifecycle) "بنهج الاستباقية والنزاهة.
- حوكمة ممارسات الاختبار لضمان التوازن بين كشف المخاطر وبين استقرار الخدمات الحكومية.
- تعزيز السيادة المعلوماتية عبر بناء "مختبرات اختبار وطنية" مستقلة ومحمية سيادياً.
- تطبيق استراتيجيات القيادة في إدارة "نتائج الاختراق" وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة "الدفاع بالهجوم" والرشاقة في إدارة المخاطر

هندسة الحصانة الاستباقية وتصفير البيروقراطية في تقارير الثغرات

- مفهوم اختبار الاختراق 2026 وأثره على السيادة الوطنية وجودة الحياة والنمو والتميز العالمي.
- مواءمة استراتيجيات الاختبار مع مبدأ تصفير البيروقراطية عبر أتمتة "إدارة الأصول " (Asset Discovery).
- تحليل العلاقة بين "الشفافية التقنية" وبين بناء الثقة والمصداقية الدولية في النموذج الأمني.
- تمرين هندسة الاستباقية لتصميم دورة اختبار تصفّر زمن "الاكتشاف حتى الإغلاق" بنزاهة وشفافية.

قيادة النزاهة في حوكمة "الفريق الأحمر" والريادة الوطنية الشاملة

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

اليوم الثاني :

السيادة التقنية وهندسة الاختبار بالذكاء الاصطناعي(AI Pentesting)

تصفير مخاطر الاختراق عبر المسح الذكي والتحليلات التنبؤية للثغرات

- توظيف الذكاء الاصطناعي في محاكاة أساليب المهاجمين وتصفير فجوات الرصد الميداني بنزاهة والتميز.
- حماية "بيانات الاختبار السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية النتائج والنزاهة الرقمية.
- تطبيق الهوية الرقمية للفرق المختبرة لتصفير الهدر البيروقراطي في إجراءات الترخيص والولوج والسيادة.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لنتائج "اختبارات الاختراق المستمرة."

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط مستويات الخطر الشبكي

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد "أولويات المعالجة."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من رصد الثغرات لضمان المصداقية أمام صانع القرار والنمو.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الاختبار بنزاهة تامة والسيادة.

اليوم الثالث :

هندسة "الفريق الأرجواني" والحياد في إدارة الموارد والشمولية

تصفير البيروقراطية في "التعاون الدفاعي-الهجومي" والشمولية الرقمية

- هندسة نموذج Purple Teaming الذي يصفّر زمن نقل المعرفة بين الهجوم والدفاع بنزاهة والتميز.
- تفعيل الرقابة الأخلاقية على منصات التنسيق الأمني لضمان حياد النظم الرقمية والريادة والنمو الشامل.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق خطوات الاختبار 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 للثغرات المكتشفة لضمان النزاهة والعدالة والتميز والنمو.
- بناء سجلات نزاهة رقمية لكل عملية اختبار كبرى لضمان الشفافية المطلقة والوضوح والريادة والسيادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "نتائج الاختبار والجدارة المؤسسية" بأسلوب واثق وملهم.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في "نتائج الاختراق"

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند الكشف عن "ثغرات سيادية" والموازنة بين الإبهار والوقار السيادي والنزاهة والتميز.
- الرقابة على البصمة الرقمية للأنظمة المختبرة لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الدفاعات المحصنة" لتصفير فرص انتشار الشائعات والنزاهة التامة.
- التدقيق الأخلاقي على سلاسل توريد برمجيات الاختبار 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 الاختبار والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "محاكاة الهجوم" 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 الرصد ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "المحصن" القدوة: من اكتشاف الثغرات إلى هندسة السيادة الشبكية

هندسة "النبض الاستراتيجي" والرشاقة السيادية في إدارة الثغرات

- مصفوفة "النبض اللحظي" للثغرات السيادية: تصميم نظام رصد رقمي يعتمد على الذكاء الاصطناعي لتحويل بيانات المسح الاختراقي المستمر إلى "نبضات استراتيجية" تظهر للقائد فوراً، مما يصفّر زمن "الاكتشاف حتى الإغلاق" ويضمن معالجة الفجوات الأمنية في مرحلة التكون وبنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للتعافي الفوري: هندسة مسار قرار "صفري الإجراءات" يسمح للفريق الأرجواني بتفعيل ضوابط الحماية التلقائية فور رصد محاولة اختراق ناجحة، مما يضمن استمرارية الخدمات الحكومية الحيوية دون قيود بيروقراطية أو تأخير في طلب الأذونات الإدارية.
- حوكمة "الصدق التقني" والنزاهة الرقمية: وضع ضوابط أخلاقية تضمن أن تكون نتائج "الفريق الأحمر" نابعة من محاكاة واقعية ومحمية سيادياً، مما يمنع الانحيازات الرقمية التي قد تخفي نقاط الضعف الحرجة، ويحقق ريادة وطنية قائمة على الشفافية المطلقة والوضوح التام أمام صانع القرار.
- مختبر "هندسة الحصانة الهجومية": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة سيبرانية" ناتجة عن ثغرة صفرية (Zero-day)، وكيفية توجيه الموارد التقنية والاتصالية لحماية السمعة الوطنية والسيادة المعلوماتية.

المخرجات الرئيسية للدورة:

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

الفئة المستهدفة:

- القيادات العليا ومدراء أمن المعلومات(CISOs) ، ومدراء تقنية المعلومات، والتميز المؤسسي.
- فرق تصفير البيروقراطية والتحول الرقمي المعنيون بضبط جودة البنية التحتية الرقمية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بتقييم مخاطر الشبكات السيادية.
- رؤساء فرق الاختبار (Red Teams) ومحللو الثغرات 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)