تقسيم الشبكات المتقدم

(Micro-Segmentation) وجدران الحماية NGFW

الإمارات العربية المتحدة - دبي

06 – 10/ 09 / 2026

مقدمة:

في الفضاء الرقمي لعام 2026، لم تعد جدران الحماية التقليدية كافية لحماية الأعصاب السيادية للدولة؛ فالتهديدات اليوم تتحرك أفقياً داخل الشبكة بذكاء وسرعة. يمثل هذا البرنامج حجر الزاوية في بناء "المنعة الرقمية" عبر دمج تقنيات التقسيم الدقيق (Micro-segmentation) مع جدران الحماية من الجيل التالي (NGFW). يهدف البرنامج إلى تمكين القادة من هندسة بيئات شبكية تصفّر البيروقراطية في إدارة السياسات، وتضمن العزل التام للأصول الحيوية، مما يعزز ريادة الدولة كأكثر البنى التحتية أماناً واستجابة في العالم.

أهداف الدورة:

- استيعاب مفاهيم "العزل السيادي" وعلاقتها بالأمن القومي وتصفير البيروقراطية الإجرائية.
- تطوير مهارات هندسة "التقسيم الدقيق" لضمان عدم الانتشار العرضي للتهديدات (Lateral Movement).
- إتقان فن توظيف جدران الحماية NGFW كأجهزة استشعار ذكية قادرة على تحليل المحتوى بنزاهة.
- حوكمة ممارسات "الوصول الأدنى (Least Privilege) "عبر أتمتة السياسات الأمنية البرمجية.
- تعزيز السيادة المعلوماتية عبر بناء "أسوار رقمية وطنية" مستقلة ومحمية سيادياً.
- تطبيق استراتيجيات القيادة في إدارة "النسيج الشبكي المحصن" وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة "انعدام الثقة" والرشاقة في تقسيم الشبكات

هندسة الحصانة المجهرية وتصفير البيروقراطية في إدارة المرور

- مفهوم Micro-segmentation 2026 وأثره على السيادة الوطنية وجودة الحياة والنمو والتميز.
- مواءمة استراتيجيات التقسيم مع مبدأ تصفير البيروقراطية عبر "السياسة كرمز (Policy as Code)".
- تحليل العلاقة بين "العزل الرقمي" وبين بناء الثقة والمصداقية الدولية في المنظومة الحكومية.
- تمرين هندسة الاستباقية لتصميم دورة عمل تصفّر زمن "احتواء التهديد" بنزاهة وشفافية مطلقة.

قيادة النزاهة في حوكمة "النسيج الشبكي" والريادة الوطنية الشاملة

- تعزيز السيادة على بروتوكولات العزل لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في تطبيق سياسات الوصول الصارمة.
- بناء ثقافة "الأمان غير المرئي" وعلاقتها بجودة الحياة والولاء المؤسسي والأمن القومي الشامل.
- صياغة ميثاق أخلاقيات قائد الشبكات المحصنة لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة جدران الحماية NGFW الذكية

تصفير مخاطر الاختراق عبر تحليل التطبيقات (App-ID) والذكاء الاصطناعي

- توظيف قدرات NGFW في تمييز التطبيقات والمحتوى وتصفير فجوات الرصد التقليدي بنزاهة والتميز.
- حماية "القنوات السيادية" عبر فحص التشفير العميق (SSL Inspection) لضمان النزاهة الرقمية والريادة.
- تطبيق الهوية الرقمية للمستخدمين داخل الجدار الناري لتصفير الهدر البيروقراطي في إجراءات التوثيق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحركة البيانات بين المناطق الحساسة.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط قواعد الحماية

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

اليوم الثالث :

هندسة "حركة المرور الأفقية (East-West) "والشمولية الرقمية

تصفير البيروقراطية في إدارة تدفقات البيانات والشمولية

- هندسة حماية "حركة المرور الأفقية" داخل مراكز البيانات لتصفير زمن اكتشاف الاختراق بنزاهة والتميز.
- تفعيل الرقابة الأخلاقية على منصات إدارة النسيج (Fabric) لضمان حياد النظم الرقمية والنمو الشامل.
- تطبيق تقنيات "سلاسل الكتل (Blockchain) "لتوثيق تغييرات القواعد وتصفير احتمالات التلاعب بالسجلات.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني للشبكة لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي الحلول الأمنية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي والاقتصادي لاستدامة الخدمات الرقمية لضمان النزاهة والعدالة والنمو.
- بناء سجلات نزاهة رقمية لكل عملية "تغيير جوهري" في بنية الشبكة لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "التقسيم الشبكي والرشاقة" بأسلوب واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في الحوادث الشبكية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل في حالات "فشل العزل أو الاختراق" والموازنة بين الإبهار والوقار السيادي والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة والفرق الفنية لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الدفاعات الدقيقة" لتصفير فرص انتشار الشائعات والنزاهة التامة.
- التدقيق الأخلاقي على سلاسل توريد الأجهزة والبرمجيات 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 الشبكة والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "سياسة العزل" 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 تأمين المحيط إلى هندسة السيادة المجهرية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في التقسيم الدقيق(Micro-Segmentation)

- مصفوفة "النبض اللحظي" للنسيج الشبكي: تصميم نظام رصد سيادي يعتمد على جدران الحماية من الجيل التالي (NGFW) لتحويل حركة المرور الأفقية (East-West) إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن رصد "التحركات العرضية" للمهاجمين وضمان عزل العمليات (Workloads) الحساسة في مرحلة التكون وبنزاهة ومصداقية تامة.
- بروتوكول "الرشاقة السيادية" للعزل التلقائي: هندسة مسار قرار "صفري الإجراءات" يسمح للشبكة بتنفيذ عمليات العزل الفوري لأي عملية رقمية يظهر عليها سلوك مشبوه، فور رصد النبضة الاستراتيجية للتهديد. يضمن هذا البروتوكول استمرارية عمل الخدمات الحكومية دون قيود بيروقراطية أو انتظار للاعتمادات اليدوية التي تعطل سرعة الاحتواء الأمني.
- حوكمة "النزاهة الرقمية" في إدارة السياسات: وضع ضوابط أخلاقية تضمن شفافية "السياسة كرمز(Policy as Code) "، وتفعيل ميثاق "الصدق في التحليل العميق (Deep Packet Inspection)لضمان استقلال القرار التقني الوطني والوضوح التام أمام صانع القرار بشأن حصانة الأصول المعلوماتية.
- مختبر "هندسة الحصانة ضد الانتشار الجانبي": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة شبكية" ناتجة عن تسلل ناجح للمحيط، وكيفية تفعيل "بروتوكول التقسيم الدقيق" لحظياً لمنع الوصول إلى قاعدة البيانات السيادية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة شبكية تضمن نزاهة التعامل مع البيانات والبيئات الوطنية بنسبة 100%.
- القدرة على هندسة منظومات عزل 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 للشبكات يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء تقنية المعلومات، والأمن السيبراني، والبنية التحتية الرقمية.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي في القطاعات السيادية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بسلامة تدفق البيانات الوطنية.
- رؤساء فرق هندسة الشبكات ومحللو أمن السحاب 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)