الأمن السيبراني الاستباقي للبنى التحتية للطاقة الوطنية

الإمارات العربية المتحدة - دبي

15 – 19/ 03 / 2026

مقدمة:

في ظل الرؤية السيادية الرامية إلى حماية الشرايين الحيوية للدولة وتطبيق مبدأ تصفير البيروقراطية في أنظمة الحماية، لم يعد الأمن السيبراني مجرد جدار حماية تقليدي، بل أصبح "درعاً استباقياً" قادراً على صيد التهديدات قبل وصولها. إن حماية البنى التحتية للطاقة تتطلب "نبضاً استراتيجياً" يدمج بين تكنولوجيا العمليات (OT) وتقنية المعلومات (IT) بنزاهة واحترافية مطلقة. يهدف هذا البرنامج إلى تمكين القادة والمهندسين من أدوات "الدفاع النشط"، وحوكمة مرونة الأنظمة الطاقوية، لضمان استمرارية الأعمال ومعصوميتها من الاختراق، مما يرسخ ريادة المؤسسة كبيئة عمل استراتيجية ومنضبطة تدعم التميز والسيادة المعلوماتية والنمو المستدام.

أهداف الدورة:

- استيعاب فلسفة "الحصانة الرقمية السيادية" وعلاقتها بالرشاقة المؤسسية وتصفير البيروقراطية في إدارة الأزمات.
- تطوير مهارات "صيد التهديدات (Threat Hunting) "في أنظمة التحكم الصناعي بنزاهة ووضوح تامة.
- إتقان فن مواءمة معايير "الثقة الصفرية (Zero Trust) "مع مستهدفات السيادة الوطنية والريادة التقنية.
- حوكمة البيانات الضخمة الناتجة عن رصد الشبكة لضمان حصانتها ضد التلاعب أو التجسس والنزاهة والوضوح.
- اكتساب مهارات تصفير فجوات الاستجابة عبر تقنيات "الأتمتة الدفاعية" ورصد نبض الاختراق اللحظي والسيادة.
- تعزيز السيادة الرقمية من خلال تحصين برمجيات الحماية الوطنية ومنع التبعية التقنية للموردين الخارجيين.
- تطبيق استراتيجيات "المرونة السيبرانية" لتعزيز كفاءة الإنفاق وتصفير الهدر المالي والزمني والتميز الشامل.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بالشفافية عند وقوع الاختراق وتأثيرها على السمعة والسيادة.
- صياغة خارطة طريق شاملة لتحويل "قطاع الأمن السيبراني" إلى درع تقني محصن يدعم الريادة والتميز والسيادة.

محتويات الورشة:

اليوم الأول:

فلسفة الدفاع الاستباقي وتصفير البيروقراطية في الأمن السيبراني

من "رد الفعل" إلى "الصيد الاستراتيجي والرشاقة السيادية"

- مفهوم الأمن الاستباقي كقوة سيادية: لماذا نحتاج لبنية تحتية "منيعة" لضمان نمو الدولة والتميز الوطني والريادة؟
- مواءمة رحلة الرصد السيبراني مع استراتيجية تصفير البيروقراطية: إلغاء عوائق الاستجابة اليدوية عبر "الدفاع المؤتمت."
- تحليل العلاقة بين "المرونة الرقمية" وبين بناء الثقة والمصداقية الوطنية في استقرار قطاع الطاقة والنمو المستدام.
- تمرين هندسة النبض الدفاعي: تحديد الثغرات المحتملة في أنظمة الطاقة وتصميم مسارات "صيد" بنزاهة ووضوح تامة.

النزاهة والسيادة في بناء "المنظومات الرقمية الموثوقة والحصينة"

- مفهوم السيادة على "شيفرات المصدر": حماية برمجيات الحماية الوطنية من التلاعب أو الأبواب الخلفية والتميز.
- دور القائد في حماية سلامة البيانات عبر ممارسات النزاهة في برمجة معايير التحقق والشفافية والسيادة الوطنية.
- سيكولوجية اليقين الرقمي: بناء المصداقية عبر الشفافية في توضيح آليات الكشف عن التسلل والنزاهة والريادة.
- صياغة ميثاق أخلاقيات "الأمن السيادي" لضمان توافق سلوك النظم مع القيم الوطنية والنمو المستدام والريادة.

اليوم الثاني:

الهندسة التقنية والسيادة السيبرانية لأنظمة الـOT/IT

الأمان الرقمي والربط البيني لأنظمة "التحكم الصناعي والذكاء الاصطناعي"

- هندسة "الأمن المدمج" في الشبكات الذكية وكيفية حوكمة مسارات البيانات لضمان السيادة المعلوماتية والوضوح.
- الأمان الرقمي كركيزة للسيادة: حماية "أعصاب الطاقة" من هجمات الفدية والتخريب الرقمي العابر للحدود والنزاهة.
- إدارة الهوية الرقمية للأنظمة والأفراد وأثرها على موثوقية الولوج والنزاهة الإجرائية والنمو والريادة الوطنية.
- تمرين تقني: تصميم بروتوكول تصفير الاختراق لأنظمة (SCADA) بنزاهة وشفافية تامة والتميز والوضوح والريادة.

أخلاقيات التفاعل مع أنظمة "الذكاء الاصطناعي في الكشف عن الشذوذ الرقمي"

- حدود استخدام الذكاء الاصطناعي في "تحليل سلوك الشبكة" دون انتهاك السرية السيادية للبيانات والتميز والنمو.
- حوكمة مخرجات أنظمة "العزل التلقائي للتهديدات": الضمان الأخلاقي للعدالة في حماية المرافق الحيوية والسيادة.
- مفهوم الأمانة في الأتمتة: تجنب الاعتماد الكلي على "الخوارزميات" دون وجود حكمة قيادية بشرية والنزاهة والتميز.
- ورشة عمل: وضع ضوابط أخلاقية لاستخدام البيانات الضخمة في تطوير كفاءة الأمن السيبراني والريادة والنمو.

اليوم الثالث:

الحياد والعدالة في بيئة العمل المعززة بأنظمة الدفاع الذكي

النزاهة الرقمية ومكافحة الانحياز في "تحديد المسؤوليات والتحقيق الجنائي"

- أخلاقيات العدالة المهنية الرقمية: ضمان نزاهة تقييم أداء فرق الدفاع بناءً على تحليل الواقع الفعلي والنمو.
- الرقابة الأخلاقية على أنظمة "التحقيق الآلي في الحوادث": كيف نضمن الشفافية والنزاهة في رصد مسببات الاختراق؟
- تطبيق قاعدة الإرادة البشرية القيادية: التدخل لتجاوز قرار آلي قد يضر بمبدأ السيادة أو الروح المعنوية والريادة.
- حساب معامل الثقة في نماذج المحاكاة لتقليل احتمالات الخطأ الناتج عن الهلوسة الرقمية للبيانات والنمو الشامل.

حوكمة المسؤولية عن مخرجات "القرارات الدفاعية المؤتمتة"

- المسؤولية المهنية للقائد عند حدوث "عزل خاطئ" لمرفق طاقة أدى لتأخر مهمة سيادية والنزاهة والتميز والنمو.
- إدارة العلاقة مع مزودي تكنولوجيا الأمن العالمية: ضمان السيادة والشفافية في الملكية الفكرية والنمو والريادة.
- بناء أنظمة التحقق المزدوج لضمان عدم غياب الحكمة البشرية في العمليات السيادية الحساسة والتميز والوضوح.
- تمرين محاكاة: إدارة أزمة تواصل ناتجة عن خلل في سجلات "النبض الدفاعي" وكيفية علاجه بنزاهة استراتيجية.

اليوم الرابع:

المسؤولية المهنية وإدارة السمعة في عصر "الأمن الاستباقي"

القيادة الاتصالية وحماية السمعة في البيئات الرقمية والريادة

- أخلاقيات إدارة السمعة عبر الابتكار في الحماية: الموازنة بين فخر التكنولوجيا ووقار السيادة والتميز والنمو.
- الرقابة على البصمة الرقمية للأنظمة وأثرها على حيادية ومصداقية القرار السيادي والريادة والتميز والنمو الشامل.
- بناء نظام الإفصاح الاستباقي للجاهزية: ضمان الشفافية لتصفير فرص انتشار شائعات الاختراق أو الضعف الأمني.
- التدقيق الأخلاقي على سلاسل التوريد التقني (الخوادم، البرمجيات) لضمان خلوها من الممارسات المضللة والسيادة.

أخلاقيات الاستجابة للأزمات والانتهاكات في أنظمة بيانات الطاقة

- المسؤولية الأخلاقية في التبليغ عن الثغرات التقنية التي قد تهدد الأمن القومي والسيادة والتميز والنمو الشامل.
- فن التواصل الأخلاقي أثناء وقوع هجمات: حماية الثقة عبر بيانات صادقة ونزيهة دون تضليل والريادة والنمو.
- إدارة التعافي المؤسسي: إجراءات إعادة بناء الصورة بعد رصد انحراف في أداء خوارزميات الدفاع والسيادة والتميز.
- بناء خطة الحصانة الرقمية للمنظومة: تحصين الشبكة ضد الهجمات السيبرانية أو الإهمال المنهجي والتقني والنمو.

اليوم الخامس:

مختبر الابتكار المهني وصناعة نموذج "القائد السيبراني"

التطبيق العملي وتصفير البيروقراطية في أنظمة الأداء والتميز المؤسسي

- تطوير خارطة الطريق التنفيذية لدمج الأمن الاستباقي في العمليات اليومية بمرونة ورشاقة والنمو والتميز والسيادة.
- تصميم بروتوكولات الحوكمة الذكية الخاصة بـ "إدارة التغيير الأمني" لتصفير المسارات البيروقراطية والريادة والنمو.
- منهجية صياغة ملفات التميز للمنافسة في الجوائز الوطنية مع التركيز على الابتكار في تصفير زمن الكشف.
- تمرين مختبر المحاكاة لإدارة المعضلات التقنية والأخلاقية (مثل هجوم متطور على محطة طاقة) وصياغة الحلول.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة الأصول تضمن نزاهة التعامل مع تكنولوجيا الأمن بنسبة 100% والريادة والنمو والتميز.
- القدرة على هندسة بيئات عمل "استباقية وسيادية" بمرونة وتوافق مع متطلبات الريادة والتميز العالمي والسيادة.
- إتقان أدوات الرقابة الأخلاقية على أنظمة الأتمتة لضمان الشفافية وتصفير مخاطر الانحياز الرقمي والتميز والنمو.
- بناء سجل ممارسات فضلى في إدارة بيانات الأمن السيبراني يدعم اتخاذ القرار القيادي الآمن والمستدام والنزاهة.
- تحقيق جاهزية كاملة للمؤسسة والمسؤول للمنافسة في فئات التميز والريادة في الابتكار والسيادة والنزاهة والنمو.

الفئة المستهدفة:

- القيادات ومدراء إدارات الأمن السيبراني، تقنية المعلومات، العمليات، الاستراتيجية، والسيادة والتميز والنزاهة.
- مهندسو أنظمة التحكم(OT) ، مسؤولو أمن الشبكات، وخبراء الاستراتيجية في المنشآت الحكومية والاتحادية.
- مسؤولو التميز المؤسسي، مستشارو الحوكمة، وفرق تصفير البيروقراطية في قطاع الطاقة والتكنولوجيا والسيادة.
- رؤساء فرق مشاريع "الأمن القومي الرقمي" والكوادر المعنية بتطوير منظومات الأداء والريادة والنمو والتميز.
- الكوادر الطموحة الساعية لامتلاك جدارات قائد الأمن السيبراني في عصر الذكاء الاصطناعي والسيادة والنزاهة.

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)