أمن الشبكات الكهربائية وحمايتها من الهجمات السيبرانية.

الإمارات العربية المتحدة - دبي

06 – 10/ 09 / 2026

مقدمة:

في ظل الرؤية السيادية الرامية إلى حماية البنية التحتية الحيوية للدولة وتحقيق "تصفير البيروقراطية" في بروتوكولات الأمان، لم يعد الأمن السيبراني للشبكات الكهربائية مجرد خيار تقني، بل أصبح "الدرع الواقي" للسيادة الوطنية الشاملة. إن حماية تدفق الطاقة تعني حماية النبض الاستراتيجي للدولة ضد التهديدات العابرة للحدود. يهدف هذا البرنامج إلى تمكين القادة والمهندسين من أدوات "الحصانة الرقمية"، وحوكمة أنظمة التحكم الصناعي (ICS/SCADA)، لضمان بناء شبكة طاقوية معصومة من الاختراق والتعطل، مما يرسخ ريادة المؤسسة كبيئة عمل استراتيجية ومنضبطة تدعم التميز والسيادة المعلوماتية والنمو المستدام.

أهداف الدورة:

- استيعاب فلسفة "الحصانة السيادية" وعلاقتها بالرشاقة المؤسسية وتصفير البيروقراطية في إدارة الأزمات الرقمية.
- تطوير مهارات تأمين أنظمة التحكم الإشرافي وجمع البيانات (SCADA) باحترافية تضمن السيادة والنزاهة والوضوح.
- إتقان فن مواءمة "بنية الثقة الصفرية (Zero Trust) "مع مستهدفات التميز والريادة الوطنية والنمو الشامل.
- حوكمة البيانات الضخمة الناتجة عن رصد التهديدات لضمان حصانتها ضد التلاعب أو التجسس الرقمي والنزاهة.
- اكتساب مهارات تصفير فجوات الاستجابة للحوادث عبر تقنيات "الدفاع الاستباقي" ورصد نبض الشبكة السيبراني.
- تعزيز السيادة الرقمية من خلال تحصين برمجيات الحماية ومنع التبعية التقنية في المشاريع القومية الكبرى.
- تطبيق استراتيجيات "المرونة السيبرانية" لتعزيز كفاءة الإنفاق وتصفير الهدر المالي والزمني والتميز الشامل.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بالشفافية والمسؤولية عند وقوع الهجمات والسيادة الوطنية.
- صياغة خارطة طريق شاملة لتحويل "أمن الطاقة" إلى درع تقني محصن يدعم الريادة والتميز والنزاهة والوضوح.

محتويات الورشة:

اليوم الأول:

فلسفة الدفاع السيادي وتصفير البيروقراطية في الأمن الكهربائي

من "رد الفعل" إلى "الحصانة الاستباقية والرشاقة الاستراتيجية"

- مفهوم الأمن السيبراني كقوة سيادية: لماذا نحتاج لبنية تحتية "منيعة" لضمان نمو الدولة والتميز الوطني؟
- مواءمة رحلة الدفاع الرقمي مع استراتيجية تصفير البيروقراطية: إلغاء عوائق الاستجابة اليدوية عبر "الأتمتة الدفاعية."
- تحليل العلاقة بين "الاستقرار الطاقوي" وبين بناء الثقة والمصداقية الوطنية في أمن الدولة والنمو الشامل.
- تمرين هندسة النبض الدفاعي: تحديد الثغرات الحرجة في الشبكة وتصميم مسارات حماية ذكية بنزاهة ووضوح تامة.

النزاهة والسيادة في بناء "المنظومات الرقمية الموثوقة والحصينة"

- مفهوم السيادة على "شيفرات التحكم": حماية سجلات الشبكة الوطنية من التلاعب أو الاختراق والتميز الرقمي.
- دور القائد في حماية سلامة المخرجات عبر ممارسات النزاهة في برمجة معايير الأمان والشفافية والسيادة الوطنية.
- سيكولوجية اليقين الرقمي: بناء المصداقية عبر الشفافية في توضيح آليات الكشف عن التهديدات والنزاهة والريادة.
- صياغة ميثاق أخلاقيات "الأمن السيبراني السيادي" لضمان توافق سلوك النظم مع القيم الوطنية والنمو المستدام.

اليوم الثاني:

الهندسة التقنية والسيادة السيبرانية لأنظمة الـ OT والـIT

الأمان الرقمي والربط البيني لأنظمة "التحكم الصناعي والشبكات المعلوماتية"

- هندسة "تقارب الـ OT/IT" وكيفية حوكمة مسارات البيانات لضمان السيادة المعلوماتية والوضوح والتميز والنمو.
- الأمان الرقمي كركيزة للسيادة: حماية "أعصاب الدولة" من هجمات الفدية والتخريب الرقمي والنزاهة والشفافية.
- إدارة الهوية الرقمية للأنظمة والأفراد وأثرها على موثوقية العمليات والنزاهة الإجرائية والريادة الوطنية الشاملة.
- 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 لبيانات المنشآت والتميز.
- حوكمة مخرجات أنظمة "العزل التلقائي للتهديدات": الضمان الأخلاقي للعدالة في حماية المرافق والسيادة والنمو.
- مفهوم الأمانة في الأتمتة: تجنب الاعتماد الكلي على "الخوارزميات" دون وجود حكمة هندسية قيادية بشرية والنزاهة.
- 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 والسيادة.
- 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 "الشبكات الاستباقية"

القيادة الاتصالية وحماية السمعة في البيئات الرقمية والريادة

- أخلاقيات إدارة السمعة عبر الابتكار في الحماية: الموازنة بين فخر التكنولوجيا ووقار السيادة والتميز والنمو والنزاهة.
- 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 والبرمجيات) 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 الشامل.
- 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 الشامل.

اليوم الخامس:

مختبر الابتكار المهني وصناعة نموذج "الدرع 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 عن التسلل.
- تمرين مختبر المحاكاة لإدارة المعضلات التقنية والأخلاقية (مثل هجوم متطور على محطة طاقة) وصياغة الحلول الناجحة.

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 الوطنية.
- إتقان أدوات الرقابة الأخلاقية على أنظمة الأتمتة لضمان الشفافية وتصفير مخاطر الانحياز الرقمي والتميز والنمو والوضوح.
- بناء سجل ممارسات فضلى في إدارة بيانات الأمن السيبراني يدعم اتخاذ القرار القيادي الآمن والمستدام والنزاهة والشفافية.
- تحقيق جاهزية كاملة للمؤسسة والمسؤول للمنافسة في فئات التميز والريادة في الابتكار والسيادة والنزاهة والوضوح والنمو.

الفئة المستهدفة:

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

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)