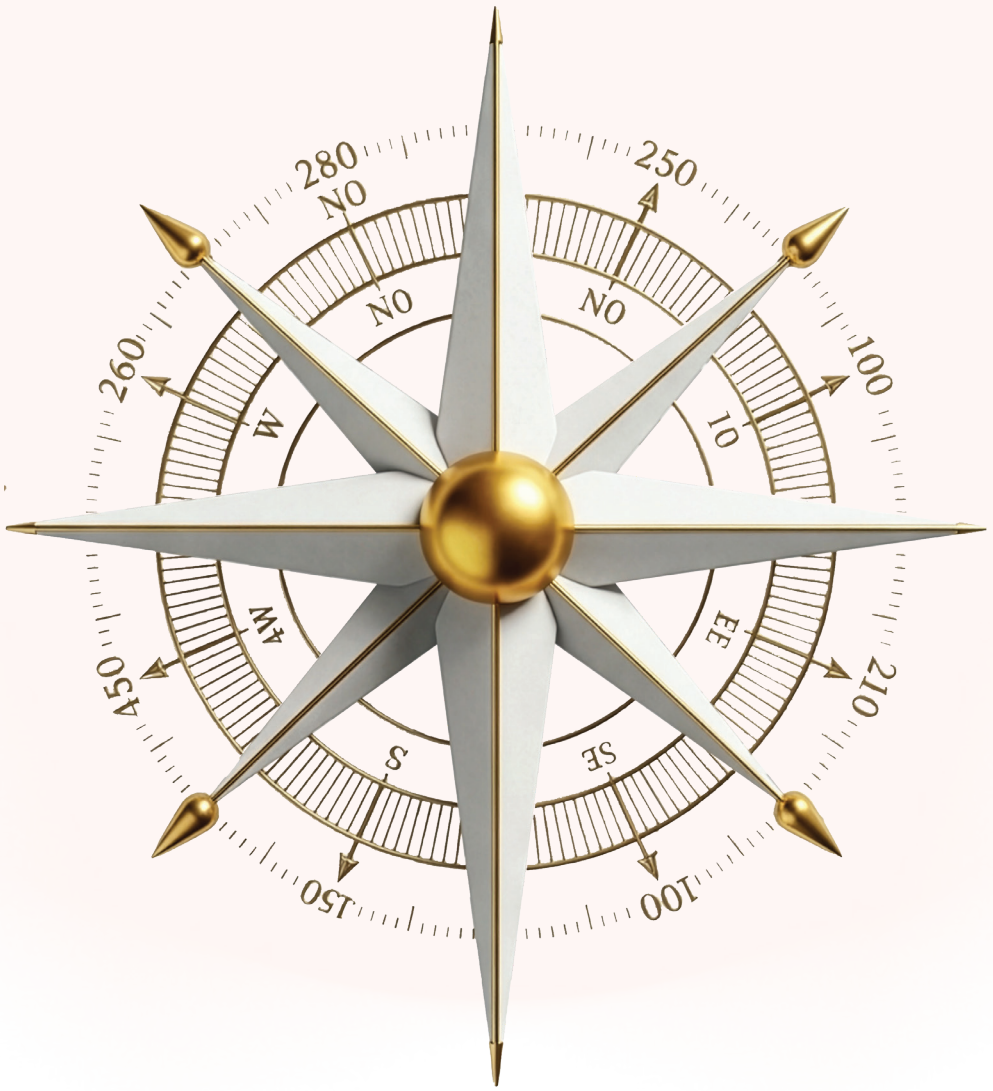
CONCEPT

ضوابط الأمن السيبراني للأنظمة التشغيلية OTCC في السعودية: حماية أنظمة التحكم الصناعي OT/ICS



ضوابط الأمن السيبراني للأنظمة التشغيلية OTCC في السعودية: حماية أنظمة التحكم الصناعي OT/ICS

العمق التقني: ممارس · **أسلوب التطبيق:** جولة تفتيش ميدانية

مقدمة

تشغل المصافي ومحطات الكهرباء ومرافق المياه والمصانع في المملكة العربية السعودية أنظمة تحكم صممت لضمان الاستمرارية لا لمواجهة تهديدات الشبكات المتصلة، وتلزمها الهيئة الوطنية للأمن السيبراني اليوم بضوابط الأمن السيبراني للأنظمة التشغيلية OTCC-1:2022. وتواجه منشآت كثيرة صعوبة في تحويل هذه الضوابط إلى مناطق وقواعد وصول عن بعد وأدلة امتثال دون تعطيل الإنتاج. تطبق هذه الدورة من كور كونسبت ضوابط OTCC إلى جانب IEC 62443 وNIST SP 800-82 على بنى مصانع فعلية. ويخرج المشاركون بتقييم فجوات الامتثال لضوابط OTCC وخطة المعالجة لمنشآتهم.

أهداف الدورة

- تصنيف أصول التقنية التشغيلية في المنشأة وتحديد مستوى حساسيتها وفق OTCC والضوابط المنطبقة عليها
- مواءمة مجالات OTCC مع متطلبات IEC 62443 وإرشادات NIST SP 800-82 الإصدار الثالث لبناء مجموعة ضوابط موحدة
- تطبيق حصر الأصول وتقسيم الشبكات والوصول الآمن عن بعد ومراقبة الأنظمة التشغيلية بالمستوى الذي تتطلبه OTCC
- تقييم المخاطر السيبرانية التشغيلية وجاهزية النسخ الاحتياطي والاستجابة وأمن الموردين، واختيار ضابط مناسب لكل فجوة
- فحص بنية المنشأة مقابل معايير OTCC وتوثيق الملاحظات مع الأدلة الداعمة
- إعداد تقييم فجوات الامتثال لضوابط OTCC وخطة المعالجة بصيغة جاهزة لاعتماد الإدارة والاستعداد لتقييم الهيئة

الفئة المستهدفة

- مهندسو أنظمة التحكم والأتمتة المسؤولون عن بيئات PLC وDCS وSCADA
- أخصائيو الأمن السيبراني للأنظمة التشغيلية المسؤولون عن تطبيق ضوابط OTCC وECC في المنشآت الصناعية
- مهندسو الشبكات الصناعية والبنية التحتية المسؤولون عن شبكات المصانع والوصول عن بعد
- أخصائيو حوكمة الأمن السيبراني والامتثال الذين يعدون أدلة OTCC والتقييم الذاتي
- موظفو الصيانة والاعتمادية وتقنية المعلومات في المواقع الذين يديرون التغييرات والنسخ الاحتياطي ووصول الموردين

محاور الدورة

اليوم الأول: بيئة الأنظمة التشغيلية وضوابط OTCC في المملكة العربية السعودية

- أولويات تقنية المعلومات مقابل الأنظمة التشغيلية ومستويات النموذج المرجعي Purdue
- مكونات أنظمة التحكم الصناعي: PLC وDCS وSCADA وHMI وأنظمة السلامة الآلية SIS
- مشهد تهديدات الأنظمة التشغيلية وفق مصفوفة MITRE ATT&CK for ICS
- نطاق ضوابط OTCC-1:2022 وقابلية تطبيقها وارتباطها بالضوابط الأساسية للأمن السيبراني ECC الصادرة عن الهيئة الوطنية للأمن السيبراني
- مستويات حساسية المنشآت من 1 إلى 3 في OTCC ومصفوفة انطباق الضوابط

اليوم الثاني: مجالات OTCC والمعايير الدولية للأنظمة التشغيلية

- هيكل مجالات OTCC: الحوكمة والتعزيز والصمود والأطراف الخارجية
- عناصر برنامج الأمن لمالكي الأصول وفق IEC 62443-2-1:2024
- المناطق والقنوات ومستويات الأمن المستهدفة وفق IEC 62443-3-2
- متطلبات أمن الأنظمة ومستويات الأمن وفق IEC 62443-3-3
- ضمانات NIST SP 800-82 الإصدار الثالث ومواءمتها مع ضوابط OTCC

اليوم الثالث: تطبيق الضوابط الأساسية للأنظمة التشغيلية

- حصر أصول الأنظمة التشغيلية بالمراقبة السلبية للشبكة
- تقسيم الشبكات والمنطقة المنزوعة السلاح الصناعية وتصميم البوابات أحادية الاتجاه
- الوصول الآمن عن بعد عبر خوادم العبور والتحقق متعدد العوامل
- إدارة التحديثات والثغرات في الأنظمة التشغيلية بالضوابط التعويضية
- سير عمل جمع سجلات الأحداث ومراقبة السلوك غير المعتاد

اليوم الرابع: مخاطر الأنظمة التشغيلية والصمود وأمن الموردين

- التحليل السيبراني لمخاطر العمليات بدمج HAZOP مع تقييم المخاطر وفق IEC 62443-3-2
- النسخ الاحتياطي والاستعادة وإدارة النسخ المرجعية للأنظمة التشغيلية
- دليل الاستجابة للحوادث في الأنظمة التشغيلية المتوافق مع مجال الصمود في OTCC
- متطلبات أمن المكاملين والموردين وفق IEC 62443-2-4
- سجل أدلة الامتثال لضوابط OTCC والاستعداد للتقييم الذاتي لدى الهيئة الوطنية للأمن السيبراني

اليوم الخامس: الجولة الميدانية وتقييم الفجوات

- جولة ميدانية في المنشأة: التحقق من مخطط المناطق والقنوات
- قائمة فحص غرفة التحكم ومحطات العمل الهندسية
- تقييم الفجوات ضابطا بضابط وفق OTCC لمنشأة من المستوى الثاني
- إعداد مسودة تقييم فجوات الامتثال لضوابط OTCC وخطة المعالجة
- لجنة مراجعة بين الزملاء والدفاع عن خطة المعالجة

المهارات المكتسبة

- تصنيف أصول الأنظمة التشغيلية
- تصميم المناطق والقنوات
- تقسيم الشبكات الصناعية
- ضبط الوصول عن بعد للأنظمة التشغيلية
- التحليل السيبراني لمخاطر العمليات
- الجاهزية للحوادث في الأنظمة التشغيلية
- إدارة أدلة الامتثال لضوابط OTCC
- ضمان أمن موردي الأنظمة التشغيلية

لماذا تحضر هذه الدورة

- تعود إلى عملك بتقييم فجوات الامتثال لضوابط OTCC وخطة المعالجة لمنشأتك، وقد راجعها الزملاء
- تشرح لإدارة المنشأة ضوابط OTCC المنطبقة على مستوى حساسية منشأتك وأسباب انطباقها
- تكتشف ضعف التقسيم ووصول الموردين غير المضبوط وغياب النسخ الاحتياطي خلال الجولة الميدانية قبل أن يكتشفها المقيم
- تقارن ممارسات أمن الأنظمة التشغيلية بمهندسين من قطاعات النفط والغاز والكهرباء والمياه والتصنيع

الخاتمة

لا تستطيع المنشآت الصناعية حماية ما لم تحصره وتقسمه وتوثق أدلته. تنتقل هذه الدورة من بنى الأنظمة التشغيلية ومتطلبات ضوابط OTCC الصادرة عن الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية، مرورا بمعايير IEC 62443 وSP 800-82 NIST، وصولا إلى الضوابط وأساليب تقييم المخاطر وإجراءات الصمود التي تحول المتطلبات إلى حماية فعلية. ويحول اليوم الأخير ذلك إلى تقييم فجوات وخطة معالجة يعود بهما المشارك إلى موقعه، فيمتلك مسارا مرتبا وقابلا للدفاع عنه نحو الامتثال وتشغيل أكثر أمانا.