CORE CONCEPT

دورة الأمن السيبراني للتقنيات التشغيلية وأنظمة التحكم الصناعي وفق IEC 62443

دورة الأمن السيبراني للتقنيات التشغيلية وأنظمة التحكم الصناعي وفق IEC 62443

مقدمة:

دورة الأمن السيبراني للتقنيات التشغيلية وأنظمة التحكم الصناعي دورة تمتد أسبوع في المناطق والقنوات وفق IEC 62443 وتقييم المخاطر والاستجابة لحوادث أنظمة التحكم، موجهة إلى مهندسي أنظمة التحكم والأتمتة وموظفي أمن التقنيات التشغيلية وأمن المعلومات في منشآت الطاقة والمرافق والتصنيع والعمليات، وتنتهي بإعداد خطة تحسين أمن التقنيات التشغيلية. فكثير من المصانع تربط أنظمة التحكم بشبكات الأعمال وبالموردين عن بعد دون تقسيم أو رؤية للأصول أو خطة استجابة مختبرة، فيبقى الإنتاج والسلامة معرضين للحوادث السيبرانية. ويتولى المشاركون أصلا صيانة أنظمة التحكم أو تأمين الشبكات، ويتدربون عبر دراسات حالة على معماريات مصانع وسيناريوهات حوادث. وتقدم كور كونسبت هذه الدورة.

أهداف الدورة:

- مطابقة معمارية أنظمة التحكم الصناعي مع نموذج Purdue المرجعي وتحديد أصولها الحرجة وتدفقات بياناتها
- تقسيم المنشأة إلى مناطق وقنوات وتحديد مستويات الأمن المستهدفة باستخدام سلسلة ISA/IEC 62443
- إجراء تقييم لمخاطر الأمن السيبراني للتقنيات التشغيلية يوازن بين عواقب السلامة والإنتاج والبيئة
- تصميم تقسيم الشبكات والمنطقة العازلة بين تقنية المعلومات والتقنيات التشغيلية والوصول الآمن عن بعد للموردين والمهندسين
- تخطيط حصر الأصول والمراقبة السلبية والتحديثات وإدارة الثغرات بما يحافظ على توافر المصنع
- إعداد دليل الاستجابة لحوادث أنظمة التحكم وخطة تحسين أمن التقنيات التشغيلية بما يتوافق مع SP 800-82 Rev. 3 NIST

الفئة المستهدفة:

- مهندسو أنظمة التحكم المسؤولون عن تصميم أنظمة التحكم الموزع والمحكمات المنطقية SCADAg وصيانتها
- فنيو الأتمتة المسؤولون عن الأجهزة الميدانية والمتحكمات ومحطات العمل الهندسية
- موظفو أمن التقنيات التشغيلية المسؤولون عن حماية الشبكات الصناعية ومراقبتها
- موظفو أمن المعلومات المسؤولون عن توسيع عمليات الأمن إلى شبكات المصانع
- قادة التشغيل والصيانة المسؤولون عن استمرارية الإنتاج وتغييرات الأنظمة
- مهندسو المشاريع والتكامل المسؤولون عن مخرجات الموردين ومكاملي الأنظمة

محاور الدورة:

اليوم 1: أنظمة التحكم الصناعي ومشهد تهديدات التقنيات التشغيلية

- مستويات نموذج Purdue المرجعي وتدفقات بيانات التقنيات التشغيلية
- مراجعة معمارية أنظمة DCS وPLCs وSCADA وأنظمة السلامة
- الفروق بين أولويات أمن المعلومات والتقنيات التشغيلية وقيودها
- سوابق الحوادث السيبرانية الصناعية والدروس المستفادة منها
- خط الأساس لمعمارية المصنع الحالية وحرجية الأصول

اليوم 2: معايير الأمن والمناطق ونماذج المخاطر

- بنية سلسلة ISA/IEC 62443 وأدوار الأطراف المعنية
- تقسيم المنشأة الصناعية إلى مناطق وقنوات
- تحديد مستويات الأمن والمتطلبات الأساسية
- تقييم مخاطر الأمن السيبراني للتقنيات التشغيلية بترتيب العواقب
- طبقات التقنيات التشغيلية وضوابطها في NIST SP 800-82 Rev. 3

اليوم 3: تأمين الشبكات الصناعية والعمليات

- تقسيم الشبكات وتصميم قواعد الجدران النارية الصناعية
- معمارية المنطقة العازلة لنظم الأرشفة التشغيلية ونقل البيانات
- الوصول الآمن عن بعد للموردين والمهندسين
- حصر أصول التقنيات التشغيلية والمراقبة السلبية للشبكات
- إدارة التحديثات والثغرات ضمن قيود توافر المصنع

اليوم 4: الحوادث وسلسلة التوريد والحالات الإشكالية

- كشف حوادث أنظمة التحكم وفرزها ومسارات تصعيدها
- احتواء حوادث التقنيات التشغيلية دون إيقاف غير آمن للمصنع
- فحوص حماية أنظمة السلامة الآلية وفصلها
- متطلبات الأمن للموردين ومكاملي الأنظمة
- ضوابط الوسائط القابلة للإزالة وتحصين محطات العمل الهندسية

اليوم 5: دراسات الحالة وخطة تحسين أمن التقنيات التشغيلية

- دراسة حالة لمصنع معالجة غاز حول تصميم المناطق
- دراسة حالة لمرفق مياه حول مخاطر الوصول عن بعد
- دراسة حالة لمصنع تصنيع حول الاستجابة لبرمجيات الفدية
- صياغة دليل الاستجابة لحوادث أنظمة التحكم ومراجعته بتمرين مكتبي
- استكمال خطة تحسين أمن التقنيات التشغيلية وترتيب أولوياتها

المهارات التي ستكتسبها:

- تحليل معمارية التقنيات التشغيلية
- تصميم المناطق والقنوات
- تقييم المخاطر السيبرانية الصناعية
- تصميم تقسيم الشبكات
- تخطيط الوصول الآمن عن بعد
- إدارة ثغرات التقنيات التشغيلية
- الاستجابة لحوادث أنظمة التحكم
- متطلبات أمن الموردين

لماذا تحضر هذه الدورة:

- تسليم خطة تحسين أمن التقنيات التشغيلية بنموذج المناطق والقنوات وسجل المخاطر ودليل الاستجابة إلى مدير المصنع ورئيس أمن المعلومات
- تحديد المناطق والقنوات ومستويات الأمن التي تحتاجها المنشأة والضوابط التي تمول أولا
- تجنب توقف الإنتاج والإيقاف غير الآمن ووصول الموردين غير المضبوط الناتجة عن الشبكات غير المقسمة وخطط الاستجابة غير المختبرة
- إحاطة زملاء التشغيل والصيانة بإجراءات الوصول عن بعد والوسائط والحوادث التي جرى التدرب عليها في دراسات الحالة

الخاتمة:

بعد العودة إلى العمل يسلم المشارك خطة تحسين أمن التقنيات التشغيلية إلى مدير المصنع ورئيس أمن المعلومات وقادة الهندسة والصيانة. ويعتمدون عليها في الاتفاق على تغييرات تقسيم الشبكات وقواعد الوصول عن بعد وأدوار الاستجابة لحوادث أنظمة التحكم. وبعد أول دورة تحسين أو تمرين مكتبي تراجع المؤسسة تغطية الأصول والثغرات المفتوحة وأزمنة الاستجابة مقابل الخطة، وتعدل الأولويات حيث تبقى المخاطر مرتفعة.

الأسئلة الشائعة:

ما الذي يحتاجه المشارك قبل دورة الأمن السيبراني للتقنيات التشغيلية؟

يحتاج المشارك إلى فهم أنظمة التحكم الصناعي أو شبكات وأمن المعلومات، مع الاستعداد لتعلم الجانب الآخر. ويفيده إحضار مخطط شبكة مبسط أو قائمة أصول من منشأته لتطبيق دراسات الحالة على مصنعه.

بم تختلف دورة الأمن السيبراني للتقنيات التشغيلية عن دورات أمن المعلومات العامة؟

تحمي دورات أمن المعلومات البيانات وأنظمة المكاتب حيث تتقدم السرية. أما هذه الدورة فتحمي أنظمة التحكم حيث تتقدم السلامة والتوافر، باستخدام مناطق وقنوات ISA/IEC 62443 ومراقبة ملائمة للمصانع وحدود التحديث واستجابة تتجنب الإيقاف غير الآمن.

لماذا تعد المناطق والقنوات أساسية في الأمن السيبراني للتقنيات التشغيلية وفق IEC 62443؟

لأن المناطق تجمع الأصول ذات الاحتياجات الأمنية المتشابهة وتضبط القنوات الاتصال بينها، فتستطيع المنشأة تشديد حماية الأنظمة الحرجة والحد من انتشار الهجوم وتبرير الضوابط بالمخاطر لا بالمنتجات.

ماذا يعود به المشارك من دورة الأمن السيبراني للتقنيات التشغيلية؟

يعود المشارك بخطة تحسين أمن التقنيات التشغيلية تضم نموذج المناطق والقنوات وسجل المخاطر وتصاميم تقسيم الشبكات والوصول عن بعد ودليل الاستجابة لحوادث أنظمة التحكم في منشأته.