هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار أجهزة نقل البيانات في اتجاه واحد

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اختر التصنيف

الإصدار <1.0>

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <1.0>

قائمة المحتويات

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بأجهزة نقل البيانات في اتجاه واحد لدى <اسم الجهة> لتقليل المخاطر السيبرانية الناتجة من التهديدات الداخلية والخارجية. وأجهزة نقل البيانات في اتجاه واحد عبارة أدوات أو أجهزة شبكية تتيح نقل البيانات في اتجاه واحد محدد مسبقًا فقط.

تمت موائمة هذا المعيار مع الضوابط الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

ينطبق هذا المعيار على جميع أجهزة نقل البيانات في اتجاه واحد المثبتة على شبكة التقنية التشغيلية الخاصة ب<اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

1	المتطلبات العامة
الهدف	تحديد المتطلبات العامة لأجهزة نقل البيانات في اتجاه واحد وذلك للتأكد من حماية سرية وسلامة وتوافر البيانات وإدارتها بشكل آمن واستعمالها بصورة ملائمة عند الحاجة.
المخاطر المحتملة	قد يؤدي عدم استعمال أجهزة نقل البيانات في اتجاه واحد بشكل ملائم أو الخطأ في إعداداتها أو عدم إدارتها بما يتوافق مع المعايير الأمنية العامة إلى تعريض الجهة لتداعيات خطيرة تؤدي إلى اختراقات وتعطل الأعمال ووقوع حوادث مرتبطة بالسلامة أو خسائر مالية.
الإجراءات المطلوبة	
1-1	يجب تثبيت جميع أجهزة نقل البيانات في اتجاه واحد على معمارية <اسم الجهة> بما يتوافق مع سياسات الأمن السيبراني المعدَّة والمتطلبات اللازمة ووفقًا للأنظمة والتشريعات ذات العلاقة.
2-1	يجب تحديد جميع أجهزة نقل البيانات في اتجاه واحد وجردها وإداراتها وحمايتها، بما يتوافق مع معيار الأمن السيبراني لأصول أنظمة التحكم الصناعي.
3-1	يجب أن تكون أجهزة نقل البيانات في اتجاه واحد ممتثلة لمعايير الأمن السيبراني الصناعية حسب أفضل الممارسات (مثل معيار IEC 62443 ، ومعيار NIST SP 800-82).
4-1	يجب أن يسمح جهاز نقل البيانات في اتجاه واحد بتدفق البيانات من شبكة إلى أخرى مع تطبيق العزل المادي والمنطقي المناسب.

2	التحكم بالوصول
الهدف	تحديد المتطلبات الخاصة بعملية إعدادات الوصول إلى أجهزة نقل البيانات في اتجاه واحد، وذلك للتأكد من أن مسار العملية سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	قد يؤدي غياب التحديد المناسب والإدارة الملائمة للوصول إلى أجهزة نقل البيانات في اتجاه واحد وعدم إدارتها بما يتوافق مع المعايير الأمنية إلى تعريض الجهة لتداعيات خطيرة تؤدي إلى اختراق الأعمال وتهديد استمرارية التشغيل ووقوع خسائر مالية.
الإجراءات المطلوبة	
1-2	يجب أن يُخصص لجهاز نقل البيانات في اتجاه واحد واجهة إدارة شبكية منفصلة.
2-2	يجب أن يُخصص لجهاز نقل البيانات في اتجاه واحد واجهة مستخدم رسومية (GUI) أو واجهة سطر أوامر (CLI) مخصصة لإجراء إعدادات الأجهزة.
3-2	يجب تقييد صلاحيات الوصول إلى إعدادات أو صيانة أجهزة نقل البيانات في اتجاه واحد ومنحها لمسؤولي الأنظمة المصرح لهم فقط.
4-2	يجب حماية الوصول إلى إعدادات أجهزة نقل البيانات في اتجاه واحد باستعمال حسابات وكلمات مرور غير افتراضية.
5-2	يجب تقييد صلاحيات الوصول المادي إلى أجهزة نقل البيانات في اتجاه واحد ومنحها لمسؤولي الأنظمة المصرح لهم فقط وحمايتها بطبقات الأمن المادي.
3	إدارة الإعدادات
الهدف	تحديد متطلبات عملية إدارة الإعدادات الخاصة بأجهزة نقل البيانات في اتجاه واحد للتأكد من أن مسار العملية سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	قد يؤدي عدم تحديد الإعدادات الأساسية لأجهزة نقل البيانات في اتجاه واحد وعدم إدارة الإعدادات بما يتوافق مع المعايير الأمنية إلى تداعيات خطيرة تؤدي إلى اختراق العمليات وتهديد استمرارية التشغيل ووقوع خسائر مالية.
الإجراءات المطلوبة	
1-3	يجب تطوير وتوثيق الإعدادات الأمنية الأساسية لأجهزة نقل البيانات في اتجاه واحد، بما يشمل جوانب الاتصالات والتشغيل والتواصل بالأنظمة، ومراجعتها بشكل رسمي.
2-3	يجب أن توفر واجهة الإدارة/التشخيص إمكانية تسجيل الأحداث وإرسالها إلى أنظمة أمنية أخرى أو إلى خوادم السجلات.

3-3	يجب أن يوفر جهاز نقل البيانات في اتجاه واحد وظائف النسخ الاحتياطي والاستعادة لتمكين المسؤولين من تصدير واستيراد الإعدادات الخاصة بأجهزة نقل البيانات في اتجاه واحد.
4-3	يجب أن يقوم جهاز نقل البيانات في اتجاه واحد بجمع وإرسال السجلات الخاصة بأي أحداث يمكن ان تدخل ضمن نطاق تفتيش التدقيق.
5-3	يجب تهيئة إعدادات أجهزة نقل البيانات في اتجاه واحد بحيث تقتصر على إرسال السجلات المحددة فقط إلى نظام السجلات المركزي باستخدام: بروتوكول SYSLOG وصيغ السجلات CEF أو LEEF أو RFC 5425.
4	الحماية البيئية والمادية
الهدف	تحديد متطلبات الحماية البيئية والمادية لأجهزة نقل البيانات في اتجاه واحد، وذلك للتأكد من أن مسار العملية سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	قد يؤدي قصور الحماية البيئية والمادية لأجهزة نقل البيانات في اتجاه واحد إلى تداعيات خطيرة تؤدي إلى اختراق بيئة العمل والعمليات، وهو ما قد يؤثر على استمرارية التشغيل ويتسبب في حوادث مرتبطة بالسلامة أو وقوع خسائر مالية.
الإجراءات المطلوبة	
1-4	عند الضرورة، يجب صناعة نسخة أكثر متانة وتحمل من جهاز نقل البيانات في اتجاه واحد، وذلك لكي يعمل الجهاز بشكل موثوق في البيئات وظروف الاستخدام القاسية، مثل الاهتزازات القوية ودرجات الحرارة الشديدة والظروف الرطبة أو الملبدة بالأتربة.
2-4	يجب تعديل جهاز نقل البيانات في اتجاه واحد بحيث يمكن تثبيته في البيئات الصناعية (داخل خزانات الأجهزة الإلكترونية أو على سكك تثبيت القواطع).
3-4	يجب أن يضمن عتاد جهاز نقل البيانات في اتجاه واحد ارتفاع مستويات التوافر (على سبيل المثال، استخدام مصدر طاقة إضافي).
5	حماية الاتصالات والأنظمة
الهدف	تحديد متطلبات حماية الأنظمة والاتصالات الخاصة بأجهزة نقل البيانات في اتجاه واحد، وذلك للتأكد من أن مسار العملية سليم وآمن وفقًا للقواعد الأمنية المحددة.
المخاطر المحتملة	قد يؤدي عدم تحديد إجراءات حماية الأنظمة والاتصالات الخاصة بأجهزة نقل البيانات في اتجاه واحد وعدم إدارتها بما يتوافق مع المعايير الأمنية إلى تداعيات خطيرة يمكن أن تؤدي إلى اختراقات أمنية لاتصالات الأنظمة، وهو ما قد يؤدي إلى تهديد استمرارية التشغيل ويتسبب في حوادث مرتبطة بالسلامة أو وقوع خسائر مالية.

الإجراءات المطلوبة	
1-5	يجب تثبيت جهاز نقل البيانات أعلى المنطقة المحايدة (DMZ) من جانب التقنية التشغيلية (OT) وعلى طبقة المنطقة المحايدة (DMZ)/(IT) تقنية المعلومات كنقطة اتصال وحيدة بين منطقة المصدر الصناعية المحمية وغيرها من مناطق/شبكات الأعمال غير الموثوقة.
2-5	يجب أن يقتصر جهاز نقل البيانات في اتجاه واحد على قبول البيانات الواردة من المصادر المسموحة المعروفة للبيانات، والتي يمكن حصرها في مزيج فريد من العناوين (IPs) والمنافذ وبرتوكولات الشبكة.
3-5	يجب ضبط معدل النقل لجهاز نقل البيانات في اتجاه واحد عند قيمة محددة بوحدة (Mbits/s)، ويتعين تحديد تلك القيمة بالاستناد إلى تقدير معدل نقل البيانات واختبار للمحاكاة.
4-5	يجب أن يدعم جهاز نقل البيانات في اتجاه واحد البروتوكولات الصناعية المستخدمة لتبادل البيانات بين منطقة المصدر الصناعية المحمية والمنطقة المحايدة (DMZ) ومناطق/شبكات الأعمال المستهدفة غير الموثوقة التي تستخدمها <اسم الجهة>.
5-5	يجب أن يدعم جهاز نقل البيانات في اتجاه واحد بروتوكولات الأتمتة المفتوحة والبروتوكولات السابقة، وأن يتمكن من استيعابها (على سبيل المثال، أي بروتوكول MODBUS، وبروتوكول OPC UA، وغيرهما).
6-5	يجب أن يدعم جهاز نقل البيانات في اتجاه واحد بروتوكولات الشبكية الإضافية المستخدمة للدعم التشغيلي أو نقل الملفات، وأن يتمكن من اكتشافها (مثل بروتوكول التحكم بالنقل (TCP) ، أو بروتوكول نقل الملفات (FTP)، أو بروتوكول نقل الملفات الآمن (SFTP)، أو بروتوكول نظام ملفات الإنترنت المشترك (CIFS)، أو بروتوكول وقت الشبكة (NTP)).
6	معايير أخرى
الهدف	يجب تهيئة الإعدادات الخاصة بأجهزة نقل البيانات في اتجاه واحد واستخدامها ومراقبتها بشكل آمن.
المخاطر المحتملة	قد يؤدي عدم التزام <اسم الجهة> بكافة المعايير والمتطلبات إلى تعريضها لمخاطر متزايدة مما قد يؤثر على استمرارية التشغيل ويتسبب في حوادث مرتبطة بالسلامة أو وقوع خسائر مالية.
الإجراءات المطلوبة	

اختر التصنيف

الإصدار <1.0>

1-6	يجب تطبيق المعايير التالية فيما يتعلق بأمن أصول أنظمة التحكم الصناعي: 1- معيار أمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)

الأدوار والمسؤوليات

1- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بأمن أجهزة وأنظمة التحكم الصناعي (OT/ICS)>.

4- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو في الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.