الاتحاد الدولي للاتصالات

ITU-T X.1208

(2014/01)

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

مؤشر المخاطرة في مجال الأمن السيبراني لتعزيز الثقة والأمن في استخدام الاتصالات/ تكنولوجيا المعلومات والاتصالات

التوصية ITU-T X.1208

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	**X.1229–X.1200**
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أشكال أخرى لأمن الحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1208

مؤشر المخاطرة في مجال الأمن السيبراني لتعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات

ملخص

تصف التوصية ITU-T X.1208 منهجية تستخدم وفقها المنظمات مؤشرات الأمن السيبراني عند حساب مقياس مخاطرة وهي تقدم قائمة بمؤشرات الأمن السيبراني المحتملة.

والغرض من التوصية ITU-T X.1208 هو مساعدة المنظمات التي تقوم بتنفيذ أو تشغيل جزء من البنية التحتية العالمية لتكنولوجيات المعلومات والاتصالات بغرض تقييم إمكانيات الأمن السيبراني لهذه المنظمات وما تتعرض له من المخاطر. وتتضمن التوصية مبادئ توجيهية الهدف منها تيسير عملية اتخاذ القرار داخل المنظمات فيما يتعلق بكيفية تحسين الأمن السيبراني وكيفية الحد من المخاطر وتحديد المواضع التي يمكن/ينبغي فيها لتلك المنظمات استثمار الموارد من أجل تحسين قدراتها في مجال الأمن السيبراني.

ولا تقترح التوصية ITU-T X.1208 استخدام دليل أو مؤشر واحد للتعبير عن قدرات منظمة ما في مجال الأمن السيبراني.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات	الرقم المميز*
1.0	ITU-T X.1208	2014-01-24	17	11.1002/1000/11950

عبارات أساسية

مؤشر الأمن السيبراني، مؤشر المخاطرة في مجال الأمن السيبراني

* للنفاذ إلى هذه التوصية، اطبع الرابط الإلكتروني http://handle.itu.int/ في مجال العنوان لمتصفح الإنترنت لديك، متبوعاً بالرقم المميز للهوية. ومثال ذلك http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2014

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

المحتويات

الصفحة

التوصية ITU-T X.1208

مؤشر المخاطرة في مجال الأمن السيبراني لتعزيز الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات

1 مجال التطبيق

توفر هذه التوصية مبدأ توجيهياً لمساعدة المنظمات في وضع واختيار وتحديد البيانات التي يتعين جمعها (على أساس مؤشرات مختارة، وتبين كيف يمكن أن تُستخدم هذه المعلومات لحساب مؤشر المخاطرة في مجال الأمن السيبراني (CSIR)؛ علماً بأن منظمة ما يمكن أن تضع مؤشر مخاطرة في مجال الأمن السيبراني قياساً بمجموعة محددة من مؤشرات الأمن السيبراني (CSI). بينما يمكن للإدارات داخل منظمة ما أن تضع أيضاً مؤشر مخاطرة في مجال الأمن السيبراني فيما يتعلق بمجموعة محددة من مؤشرات الأمن السيبراني (CSI). والغرض من مؤشر الأمن السيبراني هو السماح بتقييم مستوى اقتدار الأمن السيبراني في نقطة معينة من الزمن لدى المنظمة، وعندما تتكرر هذه العملية في نقاط أخرى من الزمن، فهو يسمح بالوقوف على حالة التقدم الذي يحرزه برنامج الأمن السيبراني في منظمة على مر الزمن.

وتقدم هذه التوصية قائمة من المؤشرات المحتملة وتصف المنهجية التي يتعين استخدامها في حساب مؤشر المخاطرة في مجال الأمن السيبراني عند استخدام مؤشرات الأمن السيبراني هذه.

والقصد من هذه التوصية هو أن تعين المنظمات التي تقوم بتنفيذ أو تشغيل جزء من البنية التحتية العالمية لتكنولوجيا المعلومات والاتصالات في تقييم قدراتها الخاصة بالأمن السيبراني وحساب مؤشر المخاطرة لديها في مجال الأمن السيبراني. والهدف من هذه المبادئ التوجيهية هو تيسير عملية اتخاذ القرار داخل المنظمات فيما يتعلق بكيفية تحسين الأمن السيبراني وكيفية الحد من المخاطر في مجال الأمن السيبراني والمواضع التي يمكن/ينبغي فيها لتلك المنظمات استثمار الموارد من أجل تحسين الأمن السيبراني.

ويتعين ألا تُستخدم هذه التوصية لوضع مؤشر المخاطرة في مجال الأمن السيبراني من المخاطر على أساس المستوى القطري. علاوة على ذلك، ولا تقترح هذه التوصية استخدام دليل أو مؤشر واحد للتعبير عن قدرات منظمة ما في مجال الأمن السيبراني (انظر الفقرة 1.6).

الملاحظة 1 – ينبغي عدم إجراء مقارنات بين المنظمات لمؤشر المخاطرة المحسوب في مجال الأمن السيبراني. لأن كل منظمة أو جماعة محلية يُفترض أن تختار ما تراه مناسباً كمجموعة من مؤشرات الأمن السيبراني لمنظمتها. علاوة على ذلك، يُنتظر منها أن تطور ما يخصها من منهجية ومعايير القياس للتصدي للمخاطر والشواغل التي تعترضها. وفي بعض الحالات يمكن أن تُستخدم معلومات شخصانية، بدلاً من بيانات موضوعية. وبالتالي، يوصى بألا يقارَن البتة مؤشر المخاطرة في مجال الأمن السيبراني لدى إحدى المنظمات مع ذلك المعتمد لدى منظمة أخرى، لأن الأمر يعتمد على السياق إلى حد كبير.

الملاحظة 2 – قد لا تتوافق المؤشرات الموضحة في هذه التوصية مع تلك التي وضعتها القطاعات الصناعية الأخرى جراء اختلاف مقاصد تلك الصناعات.

2 المراجع

لا توجد.

3 التعاريف

1.3 الشروط المحددة في مكان آخر

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 تدقيق أمني [b-ITU-T X.800]: استعراض مستقل وفحص لسجلات النظام وأنشطته بغية اختبار مدى كفاية ضوابط النظام، ولضمان الامتثال للسياسات والإجراءات التشغيلية المعمول بها، ولكشف الخروقات الأمنية، وللتوصية بأي تغييرات ضرورية في الضوابط والسياسات والإجراءات.

2.1.3 برمجية روبوتية [b-ITU-T X-Sup.8]: برنامج حاسوبي مؤتمت يُستخدم لتنفيذ مهام محددة مصممة لأغراض ضارة. وهذا المصطلح مرادف لمصطلح روبوت.

3.1.3 الأمن السيبراني [التوصية b-ITU-T X.1205]: مجموع الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب والممارسات الفضلى وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية. ويسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة والمستعملين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتضم الأهداف العامة للأمن ما يلي:

- التيسر
- السلامة التي قد تضم الاستيقان وعدم الرفض
- السرية.

4.1.3 قياس [b-ENISA]: الفعل أو عملية القياس، حيث تحدَد قيمة متغير كمي بالمقارنة مع وحدة قياس (معيارية).

5.1.3 مبيِّن [b-ENISA]: نظام قياسات متصلة يمكِّن التحديد الكمي لخاصية ما لنظام أو مكون أو عملية. ويتكون المبيِّن من مقياسين أو أكثر.

6.1.3 برمجية تصحيحية [b-ITU-T X.1206]: ترميم منشور على نطاق واسع لسد ثغرة أمنية في منتج محدد. وهو أسلوب لتحديث ملف يحل محل أجزاء منه يجري تغييرها بدلاً من الملف بأكمله.

7.1.3 المعلومات المحددة لهوية شخص (PII) [b-ITU-T X.1252]: أي معلومات أ) تعرف أو يمكن استعمالها في التعرف على الشخص الذي تخصه هذه المعلومات أو الاتصال به أو تحديد موقعه؛ ب) أو يمكن من خلالها الحصول على معلومات التعرف على شخص أو بيانات اتصاله؛ أو ج) تكون مرتبطة أو يمكن ربطها بشخص طبيعي بطريقة مباشرة أو غير مباشرة.

8.1.3 مخاطر [b-ISO/IEC 27000]: تأثير حالة عدم اليقين على الأهداف.

9.1.3 إدارة المخاطر [b-ISO/IEC 27000]: أنشطة منسقة لتوجيه منظمة وضبطها فيما يتعلق بالمخاطر.

10.1.3 شهادة الأمن [b-ITU-T X.810]: مجموعة بيانات متعلقة بالأمن تصدرها سلطة أمنية أو طرف ثالث موثوق به مع معلومات أمن تستخدم لتوفير سلامة البيانات وخدمات الاستيقان من أصل البيانات.

11.1.3 ضوابط الأمن [b-NIST FIPS 199]: الضوابط الإدارية والتشغيلية والتقنية (أي الضمانات أو التدابير المضادة) المنصوص عليها كي يحمي نظام المعلومات كتمان وسلامة وتيسر النظام ومعلوماته.

12.1.3 حادث أمني [b-ITU-T E.409]: حادث أمني هو أي حدث سلبي يمكن أن تُهدَد فيه بعض جوانب الأمن.

13.1.3 الرسائل الطفيلية [b-ITU-T X.1242]: معلومات إلكترونية تقدَّم من المرسِلين إلى المستقبلين بواسطة مطاريف، مثل الحواسيب والهواتف المتنقلة والهواتف الثابتة وغير ذلك، وهي عادة معلومات غير مطلوبة وغير مرغوبة وتعود بالضرر على المستقبلين.

14.1.3 التهديد [b-ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب فيه قد يتسبب في ضرر لنظام أو منظمة.

15.1.3 ثغرة أمنية [b-ITU-T X.1500]: أي نقطة يمكن استغلالها لانتهاك نظام ما أو المعلومات التي يحتوي عليها. (تواؤماً مع الملحق ألف بالتوصية [b-ITU-T X.800].)

16.1.3 نقطة ضعف [b-ITU-T X.1500]: قصور أو نقص لا يُعتبر ثغرة أمنية بحد ذاته، ويمكن، في مرحلة ما أن يصبح ثغرة أمنية، أو يمكن أن يساهم في فتح ثغرات أمنية أخرى.

2.3 المصطلحات المعرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 مؤشر الأمن السيبراني: أي من مجموعة المؤشرات التي تُستخدم لحساب أو قياس حالة المخاطر المهددة لقدرات أو كفاءة الأمن السيبراني لمنظمة أو مجتمع.

ملاحظة – مؤشرات الأمن السيبراني المختارة هي المؤشرات التي اختيرت لأنها هي المعنية، أي أنها ترتبط بطريقة أو بأخرى بتخوفات من مخاطر معينة.

2.2.3 مؤشر المخاطرة في مجال الأمن السيبراني: محصلة تنفيذ منهجية تحسب مؤشر المخاطرة في مجال الأمن السيبراني.

3.2.3 طاقم مؤشرات المخاطرة في مجال الأمن السيبراني: مجموعة مختارة من مؤشرات المخاطرة في مجال الأمن السيبراني التي ستُستخدم لحساب مؤشر المخاطرة في مجال الأمن السيبراني.

ملاحظة – لا يوجد طاقم واحد متفرد من مؤشرات المخاطرة في مجال الأمن السيبراني.

4.2.3 مؤشر: هذا المصطلح مرادف لمصطلح مبيِّن في الفقرة 5.1.3.

5.2.3 نظام إدارة أمن معلومات: جزء من نظام الإدارة العامة، قائم على أساس نهج مخاطر الأعمال، لإرساء أمن المعلومات وتنفيذه وتشغيله ومراقبته واستعراضه وصيانته وتحسينه، انظر الفقرة 1.2.3 من المرجع [b-ISO/IEC 27000].

ملاحظة – يتضمن نظام الإدارة الهيكل التنظيمي والسياسات وأنشطة التخطيط والمسؤوليات والممارسات والإجراءات والعمليات والموارد.

6.2.3 برنامج: سلسلة من الأنشطة المنسقة التي تهدف إلى تحقيق هدف أعمال واضح.

7.2.3 برنامج: مجموعة من التعليمات المشفرة التي تمكن آلة، وخاصة حاسوب، من إجراء التتابع المرغوب من العمليات.

8.2.3 مصدر التهديد: هو إما نية وطريقة الاستفادة من استغلال متعمد لثغرة أمنية، أو الحالة والطريقة التي قد تؤدي عرضاً إلى فتح ثغرة أمنية.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

AS نظام مستقل ذاتياً *(Autonomous system)*

BSA تحالف برمجيات الأعمال *(Business Software Alliance)*

C&A موثَّق ومعتمد *(Certified and Accredited)*

CIS مركز أمن الإنترنت *(Center for Internet Security)*

CSI مؤشر الأمن السيبراني *(Cybersecurity Indicator)*

CSIR مؤشر المخاطرة في مجال الأمن السيبراني *(Cybersecurity Indicator of Risk)*

CVE ثغرات أمنية ومواطن تعرُّض شائعة *(Common Vulnerabilities and Exposures)*

CYBEX إطار تبادل معلومات الأمن السيبراني *(Cybersecurity information Exchange)*

DB قاعدة بيانات *(Database)*

DDoS حرمان من الخدمة موزَّع *(Distributed Denial-of-Service)*

DHCP بروتوكول تشكيلة المضيف الدينامية *(Dynamic Host Configuration Protocol)*

DoS حرمان من الخدمة *(Denial-of-Service)*

DNS نظام اسم دينامي *(Domain Name System)*

GDP الناتج المحلي الإجمالي *(Gross Domestic Product)*

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*

ID معرف *(Identifier)*

IDS نظام كشف التسلل *(Intrusion Detection System)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPS نظام منع التسلل *(Intrusion Prevention System)*

ISMS نظام إدارة أمن المعلومات *(Information Security Management System)*

IT تكنولوجيا المعلومات *(Information Technology)*

PCA تحليل مكونات رئيسية *(Principal Components Analysis)*

PII المعلومات المحددة لهوية شخص *(Personally Identifiable Information)*

SSL طبقة مقبس آمن *(Secure Socket Layer)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TTP طرف ثالث موثوق *(Trusted Third Party)*

5 الاصطلاحات

يراد في هذه التوصية أن يفسَّر مصطلح منظمة بالمعنى الواسع. فيُفهم أن مجتمعاً ينبغي اعتباره مدرجاً ضمن مصطلح منظمة. بيد أن المنظمة ينبغي ألا تُعتبر أبداً مكافئة لبلد.

6 مؤشر الأمن السيبراني

1.6 مقدمة

بذلت جهود عديدة لقياس أداء تكنولوجيا المعلومات والاتصالات (ICT)، وتتبع التقدم الذي تحرزه، وتقييم أثر استخدام تكنولوجيا المعلومات والاتصالات على الحكومات والمشغلين والباحثين والصناعات. ومن أمثلة هذه المؤشرات ذات الخصوصية القطاعية، ما نشره مركز أمن الإنترنت [b-CIS] من سجل النتائج العالمي للحوسبة السحابية [b-BSA] ومبيّنات الأمن. وتركز المؤشرات الواردة في هذه التوصية على بعض جوانب الأمن السيبراني.

ويتألف مؤشر المخاطرة في مجال الأمن السيبراني الذي يرد وصفه في هذه التوصية من مؤشرات أمن سيبراني متعددة تجتمع في مؤشر مخاطرة واحد وتصف وضع المخاطر الحالي المهدد لقدرات الأمن السيبراني وفعاليته وكذلك لكفاءة تنفيذ الضوابط الأمنية لمنظمة أو مجتمع.

وهناك ظرفان منفصلان يمكن في ظلهما حساب مقياس مؤشر المخاطرة في مجال الأمن السيبراني: بالتقييم الذاتي لقدرات الأمن السيبراني، أو بجمع المؤشرات المحسوبة لدى بعض المنظمات الخارجية التي تشكل طرفاً ثالثاً. والقصد في هذه التوصية هو أن تستخدمها المنظمات للتقييم الذاتي.

ويمكن اختيار المؤشرات في هذه التوصية مع مراعاة المعايير الدولية لنظام إدارة أمن المعلومات [b-ISO/IEC 27001] و[b-ISO/IEC 27002] و[b-ISO/IEC 27003]، وأمن الشبكات [b-ISO/IEC 27033-1] و[b-ISO/IEC 27033-2] و[b-ISO/IEC 27033-4]، وغيرها من المواصفات [b-NIST SP 800-27] و[b-NIST SP 800-30] و[b-NIST SP 800-53]. وتسمح المعايير الدولية المتعلقة بالإدارة للمنظمات بتصميم وتنفيذ وصيانة مجموعة متماسكة من السياسات والعمليات والأنظمة لإدارة المخاطر المهددة لأصول المعلومات الخاصة بها، وبالتالي ضمان مستويات مقبولة من المخاطر المهددة لأمن المعلومات. والمعايير الدولية ذات الصلة بأمن الشبكات تعرِّف المفاهيم المرتبطة بهذا الشأن وتصفها، وتقدم توجيهات لإدارة أمن الشبكات. وتوفر المواصفات الأخرى المفهوم الأساسي للضوابط المعتمدة للتخفيف من المخاطر المحدقة بأصول المعلومات ولكيفية إدارة المخاطر في بيئة تكنولوجيا المعلومات والاتصالات لدى المنظمات.

ويمكن تجميع المؤشرات وفقاً لوظائف الأعمال: إدارة الحوادث، وإدارة الثغرة الأمنية، وإدارة البرمجيات التصحيحية، وأمن التطبيق، وإدارة التشكيلة، والفئة المالية.

ولا تقترح هذه التوصية استخدام دليل أو مؤشر واحد للتعبير عن قدرات الأمن السيبراني لمنظمة. وذلك لأن أمن منظمة هو كأمن أضعف حلقاتها، ليس إلا، واستخدام دليل للتعبير عن قدرات الأمن السيبراني في المنظمة لا يحدد على الوجه الصحيح الآثار المحتملة الناجمة عن الحلقة الأضعف. فإذا عُرض مؤشر المخاطرة في مجال الأمن السيبراني كرقم واحد، فإن ذلك يمكن أن يضلل أولئك الذين يُتوقع أن يستخدموا ذلك الرقم، ويمكن أيضاً أن يبعث على توقعات كاذبة لدى أولئك الذين يُتوقع أن يستخدموا هذا الرقم في عمليات صنع القرار. وبعبارة أدق، عند تجميع عدد من المؤشرات وتقييسها في رقم واحد (أي في دليل)، لا يعود واضحاً وجود نقاط ضعف الأمن السيبراني ومدى جسامتها في المنظمة. وبالتالي سيكون من غير المناسب استخدام هذا الدليل لبيان حسن قدرات الأمن السيبراني في منظمة ما، أو التفكير في استخدامه لمقارنة قدرات الأمن السيبراني بين المنظمات المختلفة.

2.6 المبادئ العامة لمؤشرات الأمن السيبراني

توضح هذه الفقرة المبادئ العامة التي ينبغي مراعاتها عند إعداد مؤشرات المخاطرة في مجال الأمن السيبراني.

- ينبغي تفضيل استخدام مجموعة مؤشرات متفق عليها على الصعيد العالمي عند حساب الأمن السيبراني.
- ينبغي اختيار مؤشرات الأمن السيبراني التي يمكن استخدامها لقياس الوضع الحالي لاقتدار الأمن السيبراني في التصدي لتهديدات أو قياس التقدم المحرز في برنامج أمن المعلومات لمنظمة أو مجتمع محلي.
- ينبغي اختيار مؤشرات الأمن السيبراني التي تتيح دقة وكتمان البيانات الخام المزمع جمعها كأساس لحساب مؤشر المخاطرة في مجال الأمن السيبراني.
- لا بد أن تحفظ عمليات جمع البيانات سلامة البيانات الخام المزمع استخدامها كأساس لحساب مؤشر المخاطرة في مجال الأمن السيبراني.
- ينبغي تفضيل استخدام المؤشرات التي قد تساعد صانعي السياسات على قياس أداء تنفيذ سياسة أمن المعلومات وتتبع التقدم المحرز في برنامج الأمن السيبراني.
- ينبغي وضع مؤشرات إضافية جديدة أو تحديث القائم منها في ضوء سرعة تغير خدمات تكنولوجيا المعلومات والاتصالات وتقنياتها.

3.6 مبادئ توجيهية لاختيار مؤشرات للمخاطر المهددة للأمن السيبراني

عند اختيار المؤشرات، قد يكون من الضروري لمنظمة أن تختار المؤشرات التي تسهل تحقيق أهداف وغايات المنظمة أو المجتمع. ويمكن للمنظمات أن تختار المؤشرات استناداً إلى وظائف الأعمال ذات الأولوية العالية.

وبالإضافة إلى ذلك، ينبغي للمؤشر أن:

- يقيس التأثير الكبير على نتائج الأداء؛
- يصنَّف في ثلاثة أنواع من المؤشرات: على مستوى النظام ومستوى البرامج وكلا المستويين؛
- يقيس التقدم المحرز في تنفيذ برنامج الأمن السيبراني، وضوابط أمنية محددة، وسياسات وإجراءات الأمن السيبراني المرتبطة بها؛
- يقيس جانبين من جوانب نتيجة تنفيذ التحكم الأمني ضمن برنامج أمني وهما الفعالية والكفاءة؛
- يقيس الأثر الإيجابي أو السلبي للأمن السيبراني على مهمة المنظمة أو المهمة المشتركة لمجتمع من المجتمعات؛
- يقيس قياس حالة نتائج أداء سياسة الأمن السيبراني المطبقة على مستوى النظام، أو على مستوى البرامج، أو على كلا المستويين؛
- يقيس الآثار الإيجابية والسلبية على مهمة منظمة ومجتمع وعلى الحياة اليومية للمستخدمين.

وعلاوة على ذلك، يجب أن تكون البيانات الخام دقيقة وموثوق بها ويمكن تحصيلها. وفي عملية القياس بأكملها، تدعو الحاجة لتوفير السلامة وحماية الخصوصية والتيسر للبيانات الخام.

4.6 تصنيف المؤشرات

هناك ثلاثة أنواع من المؤشرات وفقاً لطبيعة المؤشرات: من ناحية التنفيذ والفعالية/الكفاءة والتأثير. فتُستخدم مؤشرات التنفيذ للتدليل على التقدم المحرز في تنفيذ برنامج أمن المعلومات، والتدابير الأمنية المضادة المحددة، والسياسات والإجراءات الأمنية المرتبطة بها. ويمكن أن تصنَّف في نمطين فرعيين: مؤشرات التنفيذ على مستوى البرامج والمؤشرات على مستوى النظام. وتشمل الأمثلة على مؤشرات التنفيذ على مستوى النظام النسبة المئوية لموظفي أمن أنظمة المعلومات الذين تلقوا التدريب الأمني.

ويمكن أن تستخدم مؤشرات الفعالية/الكفاءة للتحقق من تنفيذ العمليات على مستوى البرنامج والضوابط الأمنية على مستوى النظام بشكل صحيح، وما إذا كانت تعمل على النحو المنشود، وما إذا كانت تفي بالأهداف والغايات المرجوة. وهي تتعامل مع جانبين من نتائج التنفيذ التحكم الأمني: فعالية النتيجة وكفاءتها، أي أن الفعالية تتناول المتانة فيما تتناول الكفاءة حسن التوقيت. ومن الأمثلة على مؤشر الفعالية، النسبة المئوية لحوادث أمن المعلومات الناجمة عن سوء تشكيلة التحكم في النفاذ؛ ومن الأمثلة على مؤشرات الكفاءة النسبة المئوية لمكونات النظام التي تخضع لصيانة في الموعد المحدد.

ويمكن أن تستخدم مؤشرات التأثير إلى تحديد أثر أمن المعلومات على مهمة منظمة أو مجتمع. فهي يمكن أن تكون تستخدم للقيام بالقياس الكمي للتوفير في التكاليف الذي ينتجه برنامج أمن المعلومات أو للتكاليف المتكبَدة في معالجة حادث يخل بأمن المعلومات، ولدرجة ثقة الجمهور التي حصل عليها برنامج أمن المعلومات، أو للآثار الأخرى لأمن المعلومات ذات الصلة بالمهمة. وتشمل الأمثلة على مؤشرات التأثير النسبة المئوية لنفقات المنظمة على أمن المعلومات من إجمالي الإنفاق في نظام المعلومات.

وبالإضافة إلى ذلك، يمكن تصنيف المؤشرات وفقاً لوظائف الأعمال: إدارة الحوادث، وإدارة الثغرة الأمنية، وإدارة البرمجيات التصحيحية، وأمن التطبيق، وإدارة التشكيلة، والمبينات المالية، وأمن البيانات والشبكة، وما إلى ذلك.

7 عملية إعداد مؤشر الأمن السيبراني

1.7 مقدمة

ينبغي أن ينظر إلى طاقم مؤشرات الأمن السيبراني باعتباره مجموعة أدوات رئيسية يمكن استخدامها لتقييم صلاحية إنفاذ سياسة أمن المعلومات ومعرفة الوضع الحالي لأمن المعلومات في منظمة.

2.7 منهجية لبناء طاقم مؤشرات الأمن السيبراني

إن إعداد طاقم مؤشرات الأمن السيبراني مهمة معقدة تحتاج لأن يضطلع بها مهنيون من ذوي المهارات العالية والمعرفة بعلوم الاقتصاد والأمن السيبراني والإحصاءات. ويتعين أن يقوم إعداد قائمة مؤشرات الأمن السيبراني على سياقات المنظمة، والجوانب المختلفة للمخاطر التي يتعين قياسها.

وينبغي لمعد مؤشرات الأمن السيبراني أن يأخذ في الاعتبار أن مؤشراً معيناً قد يتعرض لتقلبات كبيرة، على عكس المؤشرات ذات العينات الكبيرة، نظرا لشح العينات التي يجري قياسها، ومثال ذلك الحوادث، التي يمكن أن تُرصد في نطاق محدود. وبالتالي، ينبغي تطبيق التحليل العياني بعناية فائقة.

ويمكن استخدام الخطوات التالية لوضع طاقم مؤشرات للأمن السيبراني وجعل المعلومات جاهزة للاستخدام:

- تحديد المؤشرات الرئيسية التي يتعين اختيارها واستخدامها لحساب مؤشر المخاطرة في مجال الأمن السيبراني؛
- تحديد مصادر البيانات؛
- التعامل مع الرصدات الناقصة؛
- جعل المؤشرات قابلة للمقارنة مع بعضها البعض؛
- تحويل المؤشرات إلى قيم قياس المخاطرة؛
- استخراج مجموعة من قيم قياس المخاطرة.

1.2.7 اختيار مؤشرات لبناء مقياس مخاطرة

يعتمد اختيار المؤشرات لبناء مقياس مخاطرة على ما يجري قياسه فضلاً عن الجدوى العملية لجمع البيانات الخام.

ملاحظة – رغم أن إجراء القياس قد لا يكون عملياً في الوقت الراهن، يمكن التفكير ملياً في اختيار مؤشر ما. فيمكن أن تستخدم هذه العملية لتحديد نشاط عمل جديد يتيح جني البيانات بحيث يمكن تقييم المخاطر بشكل صحيح.

وقد يعتمد عدد المؤشرات على مهمة المنظمة وأهدافها، أو على نمط التكنولوجيات التي تستخدمها المنظمة. ويوصى باستخدام مجموعة واسعة من المؤشرات (من 10 إلى 30 مؤشراً مثلاً) لبناء مقياس مخاطرة ضمن مؤشر المخاطرة في مجال الأمن السيبراني. ويمكن لخلط مؤشرات شخصانية مع القياسات الموضوعية أن يؤثر على صلاحية حصيلة الحساب. لذلك، يوصى بتجنب استخدام مؤشرات شخصانية في بناء مؤشر المخاطرة في مجال الأمن السيبراني، ولكن قد تقتضي الضرورة مؤشراً شخصانياً في بعض مجالات إدارة المخاطر مما يجعل التحديد المنضبط لكيفية تعريف المؤشر الشخصاني أمراً حرجاً. وحالما تُختار المؤشرات، لعل من المستحسن أن تصنَّف في فئات مختلفة وفقاً لمهام أعمالها مثل إدارة الحوادث، وإدارة الثغرة الأمنية، وإدارة البرمجيات التصحيحية، وما إلى ذلك. وهذا يجعل من المؤشرات أكثر قابلية للإدارة، ويجعل المقارنة أكثر وضوحاً.

ويرد وصف إجراء الإعداد المفصل في الفقرة 3.7.

2.2.7 مصادر البيانات

يمكن أن يحدد مدى توفر البيانات لمؤشرات الأمن السيبراني عدد ونوعية المؤشرات اللازمة لحساب مؤشر المخاطرة في مجال الأمن السيبراني. فقد يؤدي الاعتماد المفرط على مصدر بيانات واحد إلى أخطاء وإغفالات. ولذلك، فمن الضروري التحقق من البيانات بالمقارنة مع مصادر مختلفة قبل تطبيقها على حساب مؤشر المخاطرة في مجال الأمن السيبراني.

3.2.7 التعامل مع البيانات المفقودة

عند جمع قياسات المخاطرة لمؤشر الأمن السيبراني، قد تُصادَف حالات تنقص فيها البيانات أو لا تتوفر. ويمكن في هذه الحالات إما أن تُترك البيانات فارغة – وعندئذ ستُسند المنظمة أي قيمة لذلك المؤشر أو أن يُستخدم الاستكمال الخارجي لتقدير البيانات المفقودة. ويمكن لترك البيانات فارغة أن يؤدي إلى استبعاد جوانب من مؤشر الأمن السيبراني. ويمكن للاستكمال الخارجي أن يضخم قيمة البيانات مؤدياً إلى المبالغة في النتائج الحسابية. فهناك مفاضلة بين الاستكمال الخارجي والإغفال؛ وينبغي لهذه المفاضلات أن تأخذ بعين الاعتبار قيمة البيانات أو أهمية المؤشرات. وربما ينبغي إجراء اختبار حساسية لتحديد مدى حساسية النتائج المحسوبة للتقلبات في القيمة المستكمَلة خارجياً أو للاستعاضة عن بيانات فارغة بالقيمة المقدرة.

4.2.7 تحويل البيانات

تنطوي مرحلة التحويل على خطوتين: تحويل من القيمة المطلقة إلى القيمة النسبية وتحويل القيم النسبية للمؤشرات إلى مؤشر مخاطرة في مجال الأمن السيبراني. وتتحول القيم المطلقة عموماً إلى قيم قابلة للمقارنة بقسمة الناتج على العدد الإجمالي للبنود. ويمكن أن تزوَّد العديد من المؤشرات بالفعل في حالتها المتحولة، لذلك قد لا تكون هذه الخطوة ضرورية.

3.7 عملية وضع مؤشرات الأمن السيبراني

تنطوي عملية وضع مؤشرات الأمن السيبراني على اختيار المؤشرات المناسبة لمهمة وأهداف منظمة أو مجتمع. وتتكون هذه العملية من خمس خطوات هي: تحديد مصلحة أصحاب المصلحة، وتعريف الأهداف والغايات، وسياسات أمن المعلومات، والمبادئ التوجيهية، واستعراض الإجراءات، واستعراض تنفيذ أمن المعلومات، واختيار المؤشرات.

الخطوة 1، هي تحديد مصلحة أصحاب المصلحة: وينطوي ذلك على تحديد أصحاب المصلحة المعنيين ومصلحتهم. ومن أصحاب المصلحة الأساسيين، رئيس المنظمة، ورئيس قسم المعلومات، ورئيس قسم الأمن، ومسؤول أمن نظام المعلومات، ومدير البرنامج، ومدير الشبكة، ومهندسو الأمن، وموظفو دعم نظام المعلومات. وتشمل نتائج هذه الخطوة جميع المصالح في قياس أمن المعلومات. ويمكن لكل صاحب مصلحة أن يطلب مجموعة مختلفة من المؤشرات تمثل وجهة نظره داخل المنطقة الخاضعة لمسؤوليته.

الخطوة 2، هي تعريف الأهداف والغايات: وينطوي ذلك على تحديد الأهداف والغايات من أداء أمن المعلومات. ويمكن التعبير عنها في شكل السياسات والمتطلبات والقوانين واللوائح والمبادئ التوجيهية والإرشادات. ويمكن اشتقاق أهداف وغايات برنامج أمن المعلومات من الغايات والأهداف المحددة على مستوى عال لدعم مهمة المنظمة.

الخطوة 3، وهي سياسات أمن المعلومات، والمبادئ التوجيهية، واستعراض الإجراءات: وينطوي ذلك على وصف تفاصيل كيف ينبغي تنفيذ الضوابط الأمنية في السياسات والإجراءات الخاصة بالمنظمة.

الخطوة 4، وهي استعراض تنفيذ أمن المعلومات: وينطوي ذلك على استعراض المؤشرات القائمة ومستودعات البيانات ذات الصلة التي يمكن استخدامها لاشتقاق المؤشرات الجديدة.

الخطوة 5، وهي اختيار المؤشرات: وينطوي ذلك على اختيار ووضع ثلاثة أنواع من المؤشرات الموضحة في الفقرة 4.6. وتنطوي هذه الخطوة على اختيار طاقم مؤشرات تتبع تنفيذ العملية، وكفاءتها/فعاليتها، وتأثيرها على المهمة، وإذا لزم الأمر، وضع مؤشرات جديدة حسب الاقتضاء.

8 مؤشرات الأمن السيبراني المحتملة

تصف هذه الفقرة مختلف مؤشرات الأمن السيبراني المحتملة التي حُددت كمؤشرات رئيسية قابلة للتطبيق لبناء طاقم مؤشرات الأمن السيبراني في منظمة. ويمكن تصنيف المؤشرات ضمن ثلاث فئات: مؤشرات أساسية، ومؤشرات موصى بها، ومؤشرات اختيارية. وبالإضافة إلى ذلك، يمكن تصنيف المؤشرات ضمن ثلاث فئات حسب طبيعة المؤشر: مؤشرات تنفيذ، ومؤشرات فعالية/كفاءة، ومؤشرات تأثير. ولا تحدد هذه التوصية مستوى المتطلبات المرتبط بأي مؤشر. ويُتوقع أن تحدد المنظمات مستوى متطلبات كل مؤشر وفقاً لما تنوي اعتماده كسياسة أمن للمنظمة. ويمكن للمنظمات كذلك أن تضع مؤشرات إضافية تتناول خصوصية وضعها، وهي مدعوة لفعل ذلك.

وقد أُعدت مؤشرات هذه الفقرة، انظر الجداول 8-1 إلى 8-30، لتستخدمها منظمة ما، ومع ذلك، يمكن أن تكون قابلة للتطبيق على مجتمع محلي من خلال تجميع المؤشرات من المنظمات التي تعد من مكونات هذا المجتمع.

وهناك مؤشرات تُستحسن فيها في بعض الحالات القيمة الأكبر، أي الأكبر هو الأفضل، فيما تُستحسن القيمة الأصغر، أي الأصغر هو الأفضل، في بعض آخر من الحالات. وهناك حالات أخرى لا يُستدل فيها بالحدس ما إذا كان الأكبر أو الأصغر هو الأفضل.

الجدول 8-1 – المؤشر 1: إدارة ثغرة أمنية (على مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	النسبة المئوية للثغرات الأمنية ذات التأثير الكبير التي ضُيقت.
الهدف	ينبغي للمنظمة أن تعالج الثغرات الأمنية المعروفة في الوقت المحدد.
المؤشر	النسبة المئوية للثغرات الأمنية ذات التأثير الكبير التي ضُيقت بعد اكتشافها ضمن الإطار الزمني الذي تحدده المنظمة.
الصيغة	(إجمالي عدد الثغرات الأمنية ذات التأثير الكبير التي ضُيقت في الوقت المحدد/إجمالي عدد الثغرات الأمنية ذات التأثير الكبير التي جرى التعرف عليها) × 100.
البيانات الخام	• عدد الثغرات الأمنية التي جرى التعرف عليها خلال الفترة الزمنية التي تحددها المنظمة. (ملاحظة: يجب حساب عدد الثغرات الأمنية التي جرى التعرف عليها خلال الفترة الزمنية التي تحددها المنظمة من البيانات الخام.) • عدد الثغرات الأمنية ذات التأثير الكبير التي ضُيقت خلال تلك الفترة الزمنية.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	التوصية ITU-T X.1521، نظام تقييم الثغرة الأمنية، [b-ITU-T X.1521] والتوصية ITU-T X.1520، الثغرات الأمنية ومواطن التعرض الشائعة [b-ITU-T X.1520].

الجدول 8-2 – المؤشر 2: صيانة سجل التدقيق الأمني (على مستوى النظام، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	النسبة المئوية لأجهزة النقطة الطرفية التي يُحتفظ لها بسجل التدقيق الأمني.
الهدف	ينبغي للمنظمة أن تحتفظ بسجل تدقيق أمني لنظام كي تحقق في أنشطة غير أصولية للنقاط الطرفية.
المؤشر	النسبة المئوية لأجهزة النقطة الطرفية التي يُحتفظ لها بسجل التدقيق الأمني.
الصيغة	(إجمالي عدد أجهزة النقطة الطرفية ذات سجل تدقيق أمني/إجمالي عدد أجهزة النقطة الطرفية) × 100.
البيانات الخام	• عدد أجهزة النقطة الطرفية التي يحتفظ لها مخدم سجل مركزي أو جهاز النقطة الطرفية بسجل تدقيق أمني. • إجمالي عدد أجهزة النقطة الطرفية.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-3 – المؤشر 3: الاستجابة للحوادث (على مستوى النظام وعلى مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	الاستجابة للحوادث.
الهدف	ينبغي للمنظمة الإبلاغ عن الحوادث في الوقت المحدد لكل فئة حادث.
المؤشر	النسبة المئوية للحوادث المبلغ عنها ضمن الإطار الزمني المطلوب لكل فئة معمول بها.
الصيغة	(عدد الحوادث المبلغ عنها في الوقت المحدد/إجمالي عدد الحوادث المبلغ عنها) × 100، عن كل فئة.
البيانات الخام	• عدد الحوادث المبلغ عنها ضمن الإطار الزمني الذي تحدده المنظمة. • إجمالي عدد الحوادث المبلغ عنها.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	التوصية ITU-T X.1544، تعداد وتصنيف أنماط الهجمات الشائعة [b-ITU-T X.1544].

الجدول 8-4 – المؤشر 4: متوسط الوقت اللازم لتضييق الثغرات الأمنية (على مستوى النظام وعلى مستوى البرنامج، الأصغر هو الأفضل)

المجال	البيانات
هوية المؤشر	متوسط الوقت اللازم لتضييق الثغرات الأمنية.
الهدف	صُمم المؤشر للدلالة على أداء المنظمة في معالجة الثغرات الأمنية التي تم تحديدها. وكلما قل الوقت اللازم لتضييق الثغرات الأمنية، كانت المنظمة أقدر غالباً على الرد الفعّال للحد من مخاطر استغلال الثغرات الأمنية.
المؤشر	يحدد متوسط الوقت اللازم لتضييق الثغرات الأمنية القيمة الوسطية لطول الوقت المستغرق لتضييق الثغرات الأمنية المحددة في منظمة.
الصيغة	مجموع (تواريخ اكتمال تضييق الثغرات الأمنية – تواريخ اكتشافها) / عدد (الثغرات الأمنية التي تم تضييقها).
البيانات الخام	• تواريخ الكشف عن الثغرات الأمنية. • تواريخ تضييق الثغرات الأمنية. • العدد الكلي للثغرات الأمنية المكتشفة • إجمالي عدد الثغرات الأمنية التي تم تضييقها.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	التوصية ITU-T X.1521، نظام تقييم الثغرة الأمنية، [b-ITU-T X.1521] والتوصية ITU-T X.1520، الثغرات الأمنية ومواطن التعرض الشائعة [b-ITU-T X.1520].

الجدول 8-5 – المؤشر 5: استعمال برمجية الأمن التصحيحية (على مستوى النظام، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	برمجية الأمن التصحيحية.
الهدف	ينبغي لأجهزة النقطة الطرفية أن تستعمل برمجية الأمن التصحيحية لتضييق الثغرات الأمنية.
المؤشر	النسبة المئوية لأجهزة النقطة الطرفية التي تستعمل نظام إدارة البرمجية التصحيحية.
الصيغة	(إجمالي عدد أجهزة النقطة الطرفية التي تستخدم برمجية الأمن التصحيحية/إجمالي عدد أجهزة النقطة الطرفية) × 100.
البيانات الخام	• إجمالي عدد أجهزة النقطة الطرفية التي تستعمل برمجية الأمن التصحيحية. • عدد أجهزة النقطة الطرفية.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-6 – المؤشر 6: متوسط الوقت المستغرَق لتطبيق البرمجية التصحيحية (على مستوى النظام وعلى مستوى البرنامج، الأصغر هو الأفضل)

المجال	البيانات
هوية المؤشر	متوسط الوقت المستغرَق لتطبيق البرمجية التصحيحية.
الهدف	إن متوسط الوقت المستغرَق لتطبيق البرمجية التصحيحية يحدد متوسط طول الوقت اللازم لنشر برمجية تصحيحية في أنظمة المنظمة. وكلما أمكن الإسراع بنشر البرمجيات التصحيحية قل متوسط الوقت اللازم لتطبيقها وقل الوقت اللازم للمنظمة لنشرها في الأنظمة في حالة وجود ثغرة أمنية معروفة.
المؤشر	متوسط الوقت المستغرَق لنشر برمجية تصحيحية في أنظمة المنظمة.
الصيغة	مجموع (تواريخ التثبيت – تواريخ التيسر) / عدد (البرمجيات التصحيحية المكتملة).
البيانات الخام	• تواريخ التثبيت. • تواريخ التيسر. • إجمالي عدد البرمجيات التصحيحية المكتملة.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-7 – المؤشر 7: متوسط الوقت اللازم لإكمال تغيير التشكيلة
(على مستوى النظام وعلى مستوى البرنامج، الأصغر هو الأفضل)

المجال	البيانات
هوية المؤشر	متوسط الوقت اللازم لإكمال تغيير التشكيلة.
الهدف	إن متوسط الوقت اللازم لإكمال تغيير التشكيلة يحدد متوسط طول الوقت المستغرَق لإكمال تغيير التشكيلة في أنظمة المنظمة. وكلما أمكن الإسراع بنشر التغيير، قل متوسط الوقت اللازم لتطبيق البرمجية التصحيحية وقل الوقت اللازم للمنظمة لنشرها في الأنظمة في حالة عدم استقرار معروفة.
المؤشر	متوسط الوقت المستغرَق لإكمال تغيير التشكيلة في أنظمة المنظمة.
الصيغة	مجموع (تواريخ الإكمال – تواريخ التبليغ) / عدد (التغييرات المكتملة).
البيانات الخام	• تواريخ الإكمال. • تواريخ التبليغ. • إجمالي عدد التغييرات المكتملة.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-8 – المؤشر 8: تغطية تقييم المخاطر (على مستوى النظام وعلى مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	تغطية تقييم المخاطر.
الهدف	ينبغي للمنظمة أن تجري قدر الإمكان تقييماً للمخاطر التي قد تتعرض لها التطبيقات في أنظمة المنظمة.
المؤشر	النسبة المئوية لتطبيقات الأعمال التي أجري لها تقييم مخاطر في أي وقت.
الصيغة	عدد (التطبيقات التي أجري لها تقييم مخاطر) / عدد (التطبيقات) × 100.
البيانات الخام	• عدد التطبيقات التي أجري لها تقييم مخاطر. • عدد التطبيقات.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-9 – المؤشر 9: تغطية برنامج كشف البرمجيات الخبيثة ومعالجتها (على مستوى النظام، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	برنامج كشف البرمجيات الخبيثة ومعالجتها.
الهدف	ينبغي لأجهزة المستخدم النهائي أن تستعمل برنامج مكافحة الفيروسات للتخفيف من البرمجيات الخبيثة بما في ذلك الفيروسات الكامنة في هذه الأجهزة.
المؤشر	النسبة المئوية لأجهزة النقطة الطرفية التي تستعمل برنامج كشف البرمجيات الخبيثة ومعالجتها.
الصيغة	(إجمالي عدد أجهزة النقطة الطرفية التي تستعمل برنامج كشف البرمجيات الخبيثة ومعالجتها /إجمالي عدد أجهزة النقطة الطرفية) × 100.
البيانات الخام	• إجمالي عدد أجهزة النقطة الطرفية التي تستعمل برنامج مكافحة الفيروسات. • عدد أجهزة النقطة الطرفية.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-10 – المؤشر 10: تغطية التخطيط للطوارئ (على مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	اختبار خطة الطوارئ.
الهدف	ينبغي للمنظمة أن تختبر خطة الطوارئ لنظم المعلومات.
المؤشر	النسبة المئوية لأنظمة النقطة الطرفية التي اختُبرت لها خطة الطوارئ.
الصيغة	(عدد أنظمة النقطة الطرفية التي اختُبرت لها خطة الطوارئ/إجمالي عدد أنظمة النقطة الطرفية) × 100.
البيانات الخام	• عدد أنظمة المعلومات التي اختُبرت لها خطة الطوارئ. • عدد أنظمة النقطة الطرفية.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-11 – المؤشر 11: تقييم الأمن (على مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	النسبة المئوية لأنظمة المعلومات الحائزة موافقات التقييم الأمني.
الهدف	ينبغي لنظام النقطة الطرفية في المنظمة أن يكون حائزاً الشهادة ومعتمداً قبل نشره لضمان قيام بيئة من الأمن والمساءلة شاملة للموظفين والمرافق والمنتجات.
المؤشر	النسبة المئوية لأنظمة النقطة الطرفية الجديدة التي اكتمل نيلها للشهادة والاعتماد قبل نشرها.
الصيغة	(عدد أنظمة المعلومات التي اكتمل نيلها للشهادة والاعتماد/إجمالي عدد أنظمة المعلومات) × 100.
البيانات الخام	• عدد أنظمة النقطة الطرفية الجديدة التي اكتمل نيلها للشهادة والاعتماد. • عدد أنظمة النقطة الطرفية الجديدة.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-12 – المؤشر 12: التعهد الأمني (على مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	التعهد الأمني أو مدونة قواعد السلوك.
الهدف	ينبغي للموظفين المخولين بالنفاذ إلى أنظمة النقطة الطرفية أن يوقعوا تعهداً أمنياً قبل النفاذ إلى نظام معلومات منظمة.
المؤشر	النسبة المئوية لموظفي أمن نظام النقطة الطرفية الذين وقعوا على تعهد أمني.
الصيغة	(عدد الموظفين الذين يُسمح لهم بالنفاذ إلى النظام الموقعين على قواعد السلوك/إجمالي عدد الموظفين الذين يُسمح لهم بالنفاذ إلى نظام النقطة الطرفية) × 100.
البيانات الخام	• عدد الموظفين الذين يُسمح لهم بالنفاذ إلى النظام بعد التوقيع على تعهد أمني. • عدد الموظفين الذين يُسمح لهم بالنفاذ إلى النظام.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• تنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-13 – المؤشر 13: التحكم في النفاذ عن بُعد ببوابة الأمن (على مستوى النظام/البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	نقاط النفاذ عن بُعد المحمية.
الهدف	ينبغي للمنظمة أن تنشر بوابة أمن لتمكين النفاذ المحمي عن بُعد وحماية أصولها الداخلية.
المؤشر	النسبة المئوية لنقاط النفاذ عن بُعد المحمية.
الصيغة	(عدد نقاط النفاذ عن بُعد التي تستخدم بوابة أمن/إجمالي عدد نقاط النفاذ عن بُعد في منظمة) × 100.
البيانات الخام	• عدد نقاط النفاذ عن بُعد المحمية التي تستخدم بوابة أمن. • عدد نقاط النفاذ عن بُعد المحمية.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-14 – المؤشر 14: التحكم في النفاذ عن بُعد بوظيفة أمنية لمنع التسلل أو كشف التسلل (على مستوى النظام/البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	نقاط النفاذ عن بُعد المحمية.
الهدف	ينبغي للمنظمة أن تنفّذ وظيفة أمنية لمنع التسلل أو كشفه لحماية الأصول الداخلية للمنظمة.
المؤشر	النسبة المئوية لنقاط النفاذ عن بُعد المحمية.
الصيغة	(عدد نقاط النفاذ عن بُعد التي تنفذ وظيفة أمنية لمنع التسلل أو كشفه/إجمالي عدد نقاط النفاذ عن بُعد) × 100.
البيانات الخام	• عدد نقاط النفاذ عن بُعد المحمية التي تنفذ وظيفة أمنية لمنع التسلل أو كشفه. • عدد نقاط النفاذ عن بُعد.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	• فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-15 – المؤشر 15: التحكم في النفاذ اللاسلكي (على مستوى النظام/البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	نقاط النفاذ اللاسلكي المحمية.
الهدف	ينبغي للمنظمة أن توفر نقاط نفاذ لا سلكي محمية لحماية الشبكة الداخلية من النفاذ غير المصرح به.
المؤشر	النسبة المئوية لنقاط النفاذ اللاسلكي المحمية.
الصيغة	(عدد نقاط النفاذ اللاسلكي المحمية/إجمالي عدد نقاط النفاذ اللاسلكي) × 100.
البيانات الخام	• عدد نقاط النفاذ اللاسلكي المحمية. • عدد نقاط النفاذ اللاسلكي.
التواتر	أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-16 – المؤشر 16: أمن الموظفين (على مستوى النظام/مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	الفحص الأمني للموظفين.
الهدف	ينبغي للمنظمة أن تسمح للموظفين المخولين بالنفاذ إلى أنظمة النقطة الطرفية.
المؤشر	النسبة المئوية للأفراد المفحوصين قبل منحهم حق النفاذ إلى أنظمة النقطة الطرفية الخاصة بالمنظمة.
الصيغة	(عدد الأفراد المفحوصين/مجموع الأفراد المخولين بالنفاذ) × 100.
البيانات الخام	• عدد الأفراد المفحوصين. • عدد الأفراد.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-17 – المؤشر 17: حماية المعلومات المحددة لهوية شخص (PII)
(على مستوى النظام/البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	النسبة المئوية للمعلومات الحساسة المحمية المحددة لهوية شخص.
الهدف	ينبغي للمنظمة أن تحمي معلوماتها الحساسة المحددة لهويات أشخاص بطريقة مجفرة.
المؤشر	النسبة المئوية للمعلومات الحساسة المحمية المحددة لهوية شخص.
الصيغة	(عدد المعلومات الحساسة المجفرة المحددة لهويات أشخاص/إجمالي عدد المعلومات المحددة لهويات أشخاص) × 100.
البيانات الخام	• عدد المعلومات المحددة لهويات أشخاص. • إجمالي عدد المعلومات المحددة لهويات أشخاص.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة وتنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-18 – المؤشر 18: حماية البيانات الاحتياطية (على مستوى النظام/البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	معدل التفتيش على سلامة البيانات الاحتياطية.
الهدف	ينبغي للمنظمة أن توفر حماية سلامة البيانات الاحتياطية.
المؤشر	النسب المئوية للبيانات الاحتياطية المحمية من حيث السلامة.
الصيغة	(كمية البيانات الاحتياطية المحمية من حيث السلامة/إجمالي كمية البيانات احتياطية) × 100.
البيانات الخام	• كمية البيانات الاحتياطية المحمية من حيث السلامة. • الكمية الكلية للبيانات الاحتياطية.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة وتنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-19 – المؤشر 19: تغطية نظام معتمد لإدارة الأمن (مثل ISMS)
(على مستوى النظام/البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	تغطية نظام الإدارة.
الهدف	ينبغي للنقطة الطرفية في المنظمة أن تنال شهادة نظام إدارة الأمن (مثل ISMS).
المؤشر	النسبة المئوية لأنظمة النقطة الطرفية التي يشملها نظام إدارة الأمن المعتمد.
الصيغة	(عدد أنظمة النقطة الطرفية المشمولة بنظام إدارة الأمن المعتمد (مثل ISMS)/إجمالي عدد أنظمة النقطة الطرفية) × 100.
البيانات الخام	• عدد أنظمة النقطة الطرفية المشمولة بنظام معتمد لإدارة الأمن (مثل ISMS). • العدد الكلي لأنظمة النقطة الطرفية.
التواتر	أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة وتنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-20 – المؤشر 20: نشر المخدم الآمن (على مستوى النظام وعلى مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	نشر المخدم الآمن.
الهدف	ينبغي لخدمات الشبكة الخاصة بالمنظمة أن تتبادل المعلومات عن طريق استخدام نفق آمن للنفاذ عن بُعد.
المؤشر	النسبة المئوية لخدمات الشبكة التي تستخدم نفقاً آمناً، مثل TLS، أو SSL، أو قشرة آمنة.
الصيغة	(عدد خدمات الشبكة التي تستخدم نفقاً آمناً/إجمالي عدد خدمات الشبكة) × 100.
البيانات الخام	• عدد خدمات الشبكة التي تستخدم نفقاً آمناً. • إجمالي عدد خدمات الشبكة.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة وتنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	
ملاحظة – يمكن نشر المخدم الآمن بسبل عديدة ليوفر نفقاً آمناً بين النقاط الطرفية. ويشمل ذلك المخدمات المحمية بواسطة SSL/TLS وقشرة آمنة.	

الجدول 8-21 – المؤشر 21: نسبة استلام الرسائل الطفيلية (البرنامج، الأصغر هو الأفضل)

المجال	البيانات
هوية المؤشر	نسبة استلام الرسائل الطفيلية.
الهدف	ينبغي للمنظمة أن تستخدم مرشاح الرسائل الطفيلية لمنع رسائل البريد الإلكتروني الطفيلية من الوصول إلى الموظفين.
المؤشر	النسبة المئوية للموظفين الذين تلقوا أكثر من العدد الذي تحدده المنظمة لرسائل البريد الإلكتروني الطفيلية خلال إطار زمني محدد.
الصيغة	(عدد الموظفين الذين تلقوا كمية معينة من رسائل البريد الإلكتروني الطفيلية/إجمالي عدد الموظفين) × 100.
البيانات الخام	• عدد الموظفين الذين تلقوا رسائل بريد إلكتروني طفيلية بما يتجاوز أرقاماً تحددها المنظمة خلال إطار زمني محدد. • عدد الموظفين.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة وتنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-22 – المؤشر 22: برنامج التوعية لدى المنظمة (الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	برنامج التوعية لدى المنظمة.
الهدف	ينبغي أن يكون هناك برنامج توعية للموظفين.
المؤشر	النسبة المئوية للموظفين الذين يشاركون في برنامج التوعية.
الصيغة	(عدد الموظفين الذين شاركوا في برنامج التوعية/إجمالي عدد الموظفين) × 100.
البيانات الخام	• عدد الموظفين الذين شاركوا في برنامج التوعية. • عدد الموظفين.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة وتنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-23 – المؤشر 23: التدريب والتثقيف الأمني (على مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	التدريب والتثقيف الأمني.
الهدف	ينبغي لموظفي المنظمة أن يتموا التدريب والتثقيف الأمني للاستجابة للحوادث الأمنية على نحو كافٍ.
المؤشر	النسبة المئوية للموظفين الذين أتموا التدريب والتثقيف الأمني ضمن الإطار الزمني الذي تحدده المنظمة.
الصيغة	(عدد الموظفين الذين أتموا التدريب والتثقيف الأمني/إجمالي عدد الموظفين) × 100.
البيانات الخام	• عدد الموظفين الذين أتموا التدريب والتثقيف. • عدد الموظفين.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تأثير/تنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-24 – المؤشر 24: دور ومسؤولية الأمن السيبراني (على مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	الدور والمسؤولية.
الهدف	ينبغي للمنظمة أن توظف وتنظم فريق استجابة للأمن السيبراني.
المؤشر	النسبة المئوية للموظفين المرتبطين بأمن المعلومات.
الصيغة	(عدد الموظفين المشاركين في مهمة الأمن السيبراني/إجمالي عدد موظفي تكنولوجيا المعلومات) × 100.
البيانات الخام	• عدد الموظفين المرتبطين بأنشطة الأمن السيبراني. • عدد الموظفين العاملين في مجال تكنولوجيا المعلومات.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تأثير/تنفيذ.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-25 – المؤشر 25: الإصابة بالبرمجيات الضارة
(على مستوى البرنامج وعلى مستوى النظام، الأصغر هو الأفضل)

المجال	البيانات
هوية المؤشر	أجهزة النقطة الطرفية المصابة بالبرمجيات الضارة.
الهدف	ينبغي حماية أجهزة النقطة الطرفية المخصصة للموظفين من البرمجيات الضارة المختلفة.
المؤشر	النسبة المئوية لحواسيب الموظفين المصابة بفيروس أو برمجيات ضارة أو مخترقة من مهاجمين يستخدمون تكنولوجيات التسلل الإلكتروني.
الصيغة	(إجمالي عدد أجهزة النقطة الطرفية المصابة بالبرمجيات الضارة/إجمالي عدد أجهزة النقطة الطرفية) × 100.
البيانات الخام	• عدد أجهزة النقطة الطرفية المصابة بفيروس أو برمجيات ضارة أو مخترقة من مهاجمين يستخدمون تكنولوجيات التسلل الإلكتروني. • إجمالي عدد أجهزة النقطة الطرفية في منظمة.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تأثير وفعالية.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-26 – المؤشر 26: تسرب معلومات محددة لهوية شخص (على مستوى البرنامج)

المجال	البيانات
هوية المؤشر	تسرب معلومات محددة لهوية شخص.
الهدف	ينبغي للمنظمة حماية المعلومات المحددة لهوية الأشخاص من التسرب إلى منظمات خارجية.
المؤشر	النسبة المئوية للمعلومات المحددة لهوية أشخاص التي تسربت خلال إطار زمني محدد في حادثة بُلِّغ عنها بشأن معلومات محددة لهوية أشخاص. **ملاحظة** – ينبغي لمعدي هذا المؤشر أن يحددوا وحدة القياس التي تخصهم فيما يتعلق بمعلومات محددة لهوية شخص.
الصيغة	(عدد المعلومات المحددة لهوية الأشخاص التي تسربت خلال الإطار الزمني الذي تحدده المنظمة في حادثة بُلِّغ عنها بشأن معلومات محددة لهوية أشخاص/إجمالي عدد المعلومات المحددة لهوية الأشخاص) × 100.
البيانات الخام	• عدد المعلومات المحددة لهوية الأشخاص التي تسربت خلال الإطار الزمني الذي تحدده المنظمة في حادثة بُلِّغ عنها بشأن معلومات محددة لهوية أشخاص. • إجمالي عدد المعلومات المحددة لهوية الأشخاص.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تأثير.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-27 – المؤشر 27: ميزانية الأمن كنسبة مئوية من ميزانية تكنولوجيا المعلومات والاتصالات (على مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	ميزانية الأمن كنسبة مئوية من ميزانية تكنولوجيا المعلومات والاتصالات.
الهدف	ينبغي للمنظمة أن تخصص ميزانية للأمن السيبراني.
المؤشر	النسبة المئوية لميزانية الأمن السيبراني إلى ميزانية تكنولوجيا المعلومات والاتصالات في المنظمة؛ على افتراض أن ميزانية الأمن مضمنَّة في ميزانية تكنولوجيا المعلومات.
الصيغة	(ميزانية الأمن السيبراني/مجموع ميزانية تكنولوجيا المعلومات والاتصالات) × 100.
البيانات الخام	• مبلغ ميزانية الأمن السيبراني. • مبلغ الميزانية الإجمالية لتكنولوجيا المعلومات والاتصالات.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تأثير.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-28 – المؤشر 28: نسبة الأجهزة المخوَّلة (الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	نسبة الأجهزة المخوَّلة إلى جميع الأجهزة لدى المنظمة.
الهدف	ينبغي للمنظمة أن تقتفي أثر نفاذ الأجهزة (حواسيب، مكونات الشبكة، طابعات، أي شيء مزود بعناوين بروتوكول الإنترنت) إلى الشبكة وتضبطه/تحجبه/تصححه على أساس جرد أصول الأجهزة المسموح بتوصيلها إلى الشبكة.
المؤشر	نسبة الأجهزة المخوَّلة إلى جميع الأجهزة لدى المنظمة.
الصيغة	(عدد الأجهزة المخوَّلة/عدد الأجهزة) × 100.
البيانات الخام	• عدد الأجهزة المخوَّلة. • عدد الأجهزة.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تأثير.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول 8-29 – المؤشر 29: نسبة البرمجيات المخوَّلة (الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	نسبة أصول البرمجيات المخوَّلة إلى جميع أصول البرمجيات لدى المنظمة.
الهدف	ينبغي للمنظمة أن تقتفي أثر تركيب وتنفيذ البرمجيات في الحواسيب وتضبطهما/تحجبهما/تصححهما على أساس جرد أصول البرمجيات المعتمدة.
المؤشر	نسبة أصول البرمجيات المخوَّلة إلى جميع أصول البرمجيات لدى المنظمة.
الصيغة	(عدد أصول البرمجيات المخوَّلة/إجمالي عدد أصول البرمجيات) × 100.
البيانات الخام	• عدد أصول البرمجيات المخوَّلة. • إجمالي عدد أصول البرمجيات.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تأثير.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	التوصية ITU-T X.1528، تعداد المنصة الشائعة، [b-ITU-T X.1528] و[ISO/IEC 19770-2]، تكنولوجيا المعلومات – إدارة أصول البرمجيات – الجزء 2: وسم تحديد هوية البرمجيات [b-ISO/IEC 19770-2].

الجدول 8-30 – المؤشر 30: أمن برمجيات التطبيقات (الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	نسبة برمجيات التطبيقات المحمية من الهجمات البرمجية الكبرى على مستوى التطبيقات (مثل CWE top 25) إلى جميع أصول برمجيات التطبيقات لدى المنظمة.
الهدف	ينبغي للمنظمة أن تكشف وتمنع الهجمات البرمجية الكبرى على مستوى التطبيقات، وأن تصدر تنبيهاً أو ترسل بريداً إلكترونياً بهذا الشأن إلى الموظف الإداري في المؤسسة خلال 24 ساعة من الكشف والمنع.
المؤشر	نسبة برمجيات التطبيقات المحمية من الهجمات البرمجية الكبرى على مستوى التطبيقات إلى جميع أصول برمجيات التطبيقات لدى المنظمة.
الصيغة	(عدد برمجيات التطبيقات المحمية من الهجمات البرمجية الكبرى على مستوى التطبيقات/عدد جميع أصول برمجيات التطبيقات) × 100.
البيانات الخام	• عدد برمجيات التطبيقات المحمية من الهجمات البرمجية الكبرى على مستوى التطبيقات. • عدد جميع أصول برمجيات التطبيقات.
التواتر	• أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	تأثير.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	التوصية ITU-T X.1524، تعداد نقاط الضعف الشائعة، [b-ITU-T X.1524] والتوصية ITU-T X.1544، تعداد وتصنيف أنماط الهجوم الشائعة [b-ITU-T X.1544].

التذييل I

أمثلة على مؤشرات مقاييس ومبينات المخاطر المهددة لأمن المعلومات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يعطي هذا الملحق مثالين عن مجموعات مؤشرات مقاييس ومبينات المخاطر المهددة لأمن المعلومات، يمكن استخدامها لحساب مؤشر الأمن السيبراني.

ويوفر معيار المعهد الوطني للمعايير والتكنولوجيا [b-NIST SP 800-55] تسعة عشر مرشحاً محتملاً من قياسات المخاطر على مستوى النظام وعلى مستوى البرنامج ويمكن تصنيفها على النحو التالي:

- قياسات المخاطر على مستوى النظام:
  - التحكم في النفاذ؛
  - التدقيق والمساءلة؛
  - تحديد الهوية والاستيقان؛
  - الصيانة؛
  - تقييم المخاطر.
- قياسات المخاطر على مستوى البرنامج:
  - نفقات الأمن، وإدارة الثغرة الأمنية؛
  - التوعية والتدريب؛
  - إصدار الشهادات والاعتماد والتقييمات الأمنية؛
  - إدارة التشكيلة؛
  - التخطيط للطوارئ؛
  - البيئة المادية.
- قياسات المخاطر على مستوى البرنامج وعلى مستوى النظام:
  - الاستجابة للحوادث؛
  - حماية الوسائط؛
  - التخطيط؛
  - الأمن الشخصي؛
  - تحصيل النظام والاتصالات؛
  - سلامة النظام والمعلومات.

وبالإضافة إلى ذلك، يوفر الدليل [b-NRI] الخاص بالمنتدى الاقتصادي العالمي (WEF) العديد من المؤشرات بينما يستخدم المنتدى [b-WEF] شهادة طبقة المقابس الآمنة (SSL) أو شهادة أمن طبقة النقل (TLS) التي تختلف على اختلاف منافذ البيع.

التذييل II

تصنيف المؤشرات وفق طبيعتها

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

توخياً للحصول على قبول أوسع لهذه التوصية في مختلف المنظمات، سيكون من المفيد تحديد الحد الأدنى من القياسات التي يمكن للبلدان النامية الحصول عليها واستخدامها دون تكبد تكاليف ذات شأن.

فعلى سبيل المثال، يمكن تنفيذ المؤشر 24 (دور ومسؤولية الأمن السيبراني) في الفقرة 8 بسهولة في البداية، لأن قياسه ينطوي فقط على عد الرؤوس. فيما تحتاج بعض المؤشرات الأخرى إلى استحداث مزيد من الأدوات و/أو قواعد البيانات الأخرى من أجل جعل تلك مؤشرات قابلة للقياس. فعلى سبيل المثال، يتطلب المؤشر 1 (إدارة الثغرة الأمنية) الوجود الفعلي للأدوات وقواعد البيانات المرتبطة بإدارة الثغرة الأمنية. وبالتالي، يجب على المنظمات التي ترغب في استخدام هذا المؤشر النظر في فائدة القيام باستثمار لجعل هذه المعلومات متاحة مقابل تكلفة للقيام بذلك. وبالمثل، يتطلب المؤشر 2 كون وظيفة إدارة أصول تكنولوجيا المعلومات والاتصالات معمولاً بها بالفعل في منظمة أو مجتمع ما. وتتطلب فئة أخرى من المؤشرات قدرات معينة داخل منظمة من أجل جعلها قابلة للقياس. فعلى سبيل المثال، يتطلب المؤشر 4 (متوسط الوقت اللازم لتضييق الثغرات الأمنية) معرفة تاريخ وقوع الحادث، وهو صعب من دون قدرات التدقيق والتحليل.

ويصف هذا التذييل تصنيف المؤشرات وفق طبيعتها: أي تلك التي يمكن قياسها بسهولة وتلك القابلة للقياس باستخدام أدوات و/أو قواعد بيانات موجودة في المنظمات عادةً، وتلك القابلة للقياس إذا قررت المنظمة تنفيذ قدرات قياس معززة.

الجدول II-1 – تصنيف المؤشرات وفق طبيعتها

طبيعة المؤشرات	رقم المؤشر	هوية المؤشر
مؤشرات قابلة للقياس بسهولة	المؤشر 12: التعهد الأمني	التعهد الأمني أو مدونة قواعد السلوك
	المؤشر 16: أمن الموظفين	الفحص الأمني للموظفين
	المؤشر 24: دور ومسؤولية الأمن السيبراني	دور ومسؤولية الأمن السيبراني
	المؤشر 27: ميزانية الأمن كنسبة مئوية من ميزانية تكنولوجيا المعلومات والاتصالات	ميزانية الأمن كنسبة مئوية من ميزانية تكنولوجيا المعلومات والاتصالات
مؤشرات يمكن قياسها باستخدام أدوات و/أو قواعد بيانات القياس الموجودة في المنظمات عادةً	المؤشر 1: إدارة ثغرة أمنية	النسبة المئوية للثغرات الأمنية الكبيرة التي ضُيقت
	المؤشر 2: صيانة سجل التدقيق الأمني	النسبة المئوية لأجهزة النقطة الطرفية التي يُحتفظ لها بسجل تدقيق أمني
	المؤشر 3: الاستجابة للحوادث	الاستجابة للحوادث
	المؤشر 8: تغطية تقييم المخاطر	تغطية تقييم المخاطر
	المؤشر 9: تغطية برنامج كشف البرمجيات الخبيثة ومعالجتها	تغطية برنامج كشف البرمجيات الخبيثة ومعالجتها
	المؤشر 21: نسبة استلام الرسائل الطفيلية	نسبة استلام الرسائل الطفيلية
	المؤشر 22: برنامج التوعية لدى المنظمة	برنامج التوعية لدى المنظمة
	المؤشر 23: التدريب والتثقيف الأمني	التدريب والتثقيف الأمني

الجدول II-1 – تصنيف المؤشرات وفق طبيعتها

طبيعة المؤشرات	رقم المؤشر	هوية المؤشر
	المؤشر 28: نسبة الأجهزة المخوَّلة	نسبة الأجهزة المخوَّلة إلى جميع الأجهزة لدى المنظمة
	المؤشر 29: نسبة البرمجيات ا.لمخوَّلة	نسبة أصول البرمجيات المخولة إلى جميع أصول البرمجيات لدى المنظمة
	المؤشر 30: أمن برمجيات التطبيقات	نسبة برمجيات التطبيقات المحمية من الهجمات البرمجية الكبرى على مستوى التطبيقات (مثل CWE top 25) إلى جميع أصول برمجيات التطبيقات لدى المنظمة.
مؤشرات يحتمل أن تستلزم تطوير قدرات قياس إضافية ضمن منظمة	المؤشر 4: متوسط الوقت اللازم لتضييق الثغرات الأمنية	متوسط الوقت اللازم لتضييق الثغرات الأمنية
	المؤشر 5: استعمال برمجية الأمن التصحيحية	برمجية الأمن التصحيحية
	المؤشر 6: متوسط الوقت المستغرَق لتطبيق البرمجية التصحيحية	متوسط الوقت المستغرَق لتطبيق البرمجية التصحيحية
	المؤشر 7: متوسط الوقت اللازم لإكمال تغيير التشكيلة	متوسط الوقت اللازم لإكمال تغيير التشكيلة
	المؤشر 10: تغطية التخطيط للطوارئ	اختبار خطة الطوارئ
	المؤشر 11: تقييم الأمن	النسبة المئوية لأنظمة المعلومات الحائزة موافقات التقييم الأمني
	المؤشر 13: التحكم في النفاذ عن بُعد ببوابة الأمن	نقاط النفاذ عن بُعد المحمية
	المؤشر 14: التحكم في النفاذ عن بُعد بوظيفة أمنية لمنع التسلل أو كشف التسلل	نقاط النفاذ اللاسلكي المحمية
	المؤشر 17: حماية المعلومات المحددة لهوية شخص (PII)	النسبة المئوية للمعلومات الحساسة المحمية المحددة لهوية شخص
	المؤشر 18: حماية البيانات الاحتياطية	معدل التفتيش على سلامة البيانات الاحتياطية
	المؤشر 19: تغطية نظام معتمد لإدارة الأمن	تغطية نظام الإدارة
	المؤشر 20: النشر المخدم الآمن	النشر الآمن لمخدم
	المؤشر 25: الإصابة بالبرمجيات الضارة	أجهزة النقطة الطرفية المصابة بالبرمجيات الضارة
	المؤشر 26: تسرب معلومات محددة لهوية شخص	تسرب معلومات محددة لهوية شخص

التذييل III

مؤشرات تجريبية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يصف هذا التذييل عدداً من المؤشرات التجريبية (انظر الجداول III-1 إلى III-6) التي قد يصح استخدامها في المنظمات.

الجدول III-1 – المؤشر III-1: متوسط الوقت المستغرَق لاكتشاف الحادث (على مستوى النظام وعلى مستوى البرنامج، الأصغر هو الأفضل)

المجال	البيانات
هوية المؤشر	متوسط الوقت المستغرَق لاكتشاف الحادث.
الهدف	ينبغي للمنظمة أن تكتشف الحوادث فور وقوعها وأن تقيس متوسط الوقت المستغرَق لاكتشاف الحادث لإثبات فعالية المنظمة في الكشف عن الحوادث الأمنية. وبشكل عام، كلما أسرعت منظمة في الكشف عن حادث، قلت الأضرار التي يرجح أن تتكبدها.
المؤشر	متوسط المدة الزمنية، بالساعات، التي انقضت بين وقت وقوع مجموعة معينة من الحوادث ووقت اكتشافها.
الصيغة	مجموع (أوقات اكتشاف الحوادث – أوقات وقوعها) / عدد (الحوادث).
البيانات الخام	الوقت المستغرَق لاكتشاف الحوادث، لكل حادث. إجمالي عدد الحوادث المبلغ عنها.
التواتر	أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول III-2 – المؤشر III-2: تزويد الوصلة بوصلة رديفة (النظام، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	نسبة وصلات الشبكة المزودة بوصلة رديفة.
الهدف	ينبغي للمنظمة أن تمد وصلات رديفة ضمن الشبكة الرئيسية لضمان تيسر واستمرار خدمات المنظمة.
المؤشر	نسبة وصلات الشبكة المزودة بوصلة رديفة.
الصيغة	(عدد الوصلات المزودة بوصلة رديفة /إجمالي عدد وصلات الشبكة) × 100.
البيانات الخام	عدد الوصلات الرديفة للمسيّرات أو نظام اسم الميدان (DNS) أو بروتوكول تشكيلة المضيف الدينامية (DHCP) أو جدار الحماية، أو قاعدة البيانات (DB). عدد الوصلات غير المزودة بوصلة رديفة.
التواتر	أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول III-3 – المؤشر III-3: الإصابة ببرمجيات روبوتية (على مستوى النظام، الأصغر هو الأفضل)

المجال	البيانات
هوية المؤشر	النسبة المئوية لأجهزة النقطة الطرفية المصابة ببرمجيات روبوتية.
الهدف	ينبغي للمنظمة أن تخفف من وجود البرمجيات الروبوتية في شبكتها.
المؤشر	النسبة المئوية لأجهزة النقطة الطرفية المصابة ببرمجيات روبوتية معروفة في منظمة. ويفترض أن المنظمة تستخدم نظاماً لكشف الإصابة ببرمجيات روبوتية.
الصيغة	(إجمالي عدد أجهزة النقطة الطرفية المصابة ببرمجيات روبوتية معروفة/إجمالي عدد أجهزة النقطة الطرفية) × 100.
البيانات الخام	عدد أجهزة النقطة الطرفية المصابة ببرمجيات روبوتية.
التواتر	أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول III-4 – المؤشر III-4: تدابير الحرمان من الخدمة الموزع (DDoS) (على مستوى النظام، الأصغر هو الأفضل)

المجال	البيانات
هوية المؤشر	تدابير الحرمان من الخدمة الموزع.
الهدف	ينبغي للمنظمة حماية أنظمة النقطة الطرفية ضد هجمات الحرمان من الخدمة الموزع (أو الحرمان من الخدمة (DoS)) ضمن الإطار الزمني الذي تحدده المنظمة.
المؤشر	النسبة المئوية لأنظمة المنظمة غير المتوفرة لمدة زمنية محددة بسبب هجمات الحرمان من الخدمة (DoS).
الصيغة	(عدد أنظمة المنظمة التي لا تتوفر لمدة زمنية محددة بسبب هجمات الحرمان من الخدمة خلال الفترة التي تحددها المنظمة/إجمالي عدد المواقع الإلكترونية العائدة لمنظمة) × 100.
البيانات الخام	عدد المواقع الإلكترونية التي لا تتوفر لمدة زمنية محددة بسبب هجمات الحرمان من الخدمة ضمن الإطار الزمني الذي تحدده المنظمة. عدد المواقع الإلكترونية الكلي.
التواتر	أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول III-5 – المؤشر III-5: أداء سجل التدقيق الأمني (على مستوى النظام وعلى مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	النسبة المئوية لحوادث الأمن الحاسوبية التي التقط لها سجل التدقيق الأمني آثاراً يمكن رصدها.
الهدف	ينبغي للمنظمة أن تقيّم فعالية سجلات التدقيق الأمني.
المؤشر	النسبة المئوية لحوادث الأمن الحاسوبية التي التقط لها سجل التدقيق الأمني آثاراً يمكن رصدها.
الصيغة	(الحوادث المبلَّغ عنها التي خلفت آثاراً يمكن رصدها في السجلات/إجمالي عدد الحوادث المبلَّغ عنها) × 100.
البيانات الخام	عدد الحوادث المبلَّغ عنها التي وُجد لها آثار يمكن رصدها في سجلات التدقيق الأمني. (إما سجل مركزي أو سجلات مجمعة من النقاط الطرفية) إجمالي عدد الحوادث المبلَّغ عنها.
التواتر	أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

الجدول III-6 – المؤشر III-6: أداء التخفيف من الحوادث (على مستوى النظام وعلى مستوى البرنامج، الأكبر هو الأفضل)

المجال	البيانات
هوية المؤشر	النسبة المئوية لحوادث الأمن الحاسوبية الواقعة ضمن الأنظمة الموثَّقة والمعتمدة (نقاط طرفية أو مجموعات من النقاط الطرفية).
الهدف	ينبغي للمنظمة أن تقيّم فعالية إجراءات التوثيق والاعتماد.
المؤشر	النسبة المئوية لحوادث الأمن الحاسوبية الواقعة ضمن الأنظمة الموثَّقة والمعتمدة.
الصيغة	(الحوادث المبلَّغ عنها الواقعة ضمن الأنظمة الموثَّقة والمعتمدة/إجمالي عدد الحوادث المبلَّغ عنها) × 100.
البيانات الخام	عدد الحوادث المبلَّغ عنها الواقعة ضمن الأنظمة الموثَّقة والمعتمدة إجمالي عدد الحوادث المبلَّغ عنها.
التواتر	أسبوعياً، شهرياً، ربع سنوياً، سنوياً.
النمط	فعالية/كفاءة.
مستوى المتطلبات	
يسري على	المنظمات، (مجتمع من خلال تجميع المنظمات).
مرجع من تقنيات CYBEX	

بيبليوغرافيا

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991) | ISO/IEC 7498-2 (1989), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity.*

[b-ITU-T X.1206] Recommendation ITU-T X.1206 (2008), *A vendor-neutral framework for automatic notification of security related information and dissemination of updates*.

[b-ITU-T X.1242] Recommendation ITU-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures*.

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration*.

[b-ITU-T X.1528] Recommendation ITU-T X.1528 (2012), *Common platform enumeration*.

[b-ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification*.

[b-ITU-T X-Sup.8] ITU-T X-series Recommendations − Supplement 8 (2010), *ITU-T X.1205 − Supplement on best practices against botnet threats*.

[b-ISO/IEC 19770-2] ISO/IEC 19770-2:2009, *Information technology – Software asset management – Part 2: Software identification tag*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27003] ISO/IEC 27003:2010, *Information technology – Security techniques – Information security management system implementation guidance*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27033-2] ISO/IEC 27033-2:2012, *Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security*.

[b-ISO/IEC 27033-4] ISO/IEC 27033-4: 2014, *Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways*.

[b-NIST SP 800-27] NIST SP 800-27 Revision A (2004), *Engineering Principles for IT Security (A Baseline for Achieving Security), Revision A*.

[b-NIST SP 800-30] NIST SP 800-30 Revision 1 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST SP 800-53] NIST SP 800-53 Revision 4 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-NIST SP 800-55] NIST SP 800-55 Revision 1 (2008), *Performance Measurement Guide for Information Security*.

[b-NIST FIPS 199] NIST FIPS PUB 199 (2004), *Standards for Security Categorization of Federal Information and Information Systems*.

[b-ENISA] ENISA (V6_2, 2011), *Measurement Frameworks and Metrics for Resilient Networks and Services: technical report*.

[b-NRI] World Economic Forum (2013), *Networked Readiness Index*.

[b-WEF] World Economic Forum (2013), *Secure Internet servers*. (Sources: The World Bank, World Development Indicators Online; national sources).

[b-CIS] Center for Internet Security (2010), *The CIS security metrics*.

[b-Nelson] Nelson, C. E. (2010), *Security metrics: An overview,* ISSA Journal, Vol.8, No. 8.

[b-BSA] BSA (2013), *BSA Global Cloud Computing Scorecard*. http://cloudscorecard.bsa.org/2013/

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2014