الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

# ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

# X.1541

(2017/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تبادل الأحداث/الحوادث العارضة/المعلومات الحدسية

---

# الإصدار 2 لنسق تبادل وصف الشيء المتعلق بالحادث

التوصية ITU-T X.1541

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 (1) | |
| 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 (1) | 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 (2) | |
| اتصالات الطوارئ | X.1309-X.1300 |
| أمن شبكات المحاسيس واسعة الانتشار | X.1319-X.1310 |
| أمن شبكة الكهرباء الذكية | X.1339-X.1330 |
| البريد المعتمد | X.1349-X.1340 |
| أمن إنترنت الأشياء (IoT) | X.1369-X.1360 |
| أمن أنظمة النقل الذكية (ITS) | X.1389-X.1370 |
| أمن سجل الحسابات الموزع | X.1429-X.1400 |
| البروتوكول الأمني (2) | X.1459-X.1450 |
| 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 |
| أمن أشكال أخرى للحوسبة السحابية | X.1699-X.1680 |

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

**التوصية ITU-T X.1541**

# الإصدار 2 لنسق تبادل وصف الشيء المتعلق بالحادث


## ملخص

تصف التوصية ITU-T X.1541 نموذج معلومات للإصدار 2 لنسق تبادل وصف الشيء المتعلق بالحادث (IODEF) وتقدم نموذج بيانات ذي صلة محدد بمخطط اللغة XML. ويوصف الإصدار 2 للنسق IODEF تمثيلاً لنموذج بيانات لتبادل المعلومات التي يشيع تبادلها عن أمن الحاسوب أو غيرها من الحوادث. ويتم ذلك بسرد الفقرات ذات الصلة من المعيار IETF RFC 7970 مع تبيان ما إذا كانت معيارية أم إعلامية.


## التسلسل التاريخي

| الطبعة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1541 | 2012-09-07 | 17 | 11.1002/1000/11375 |
| 2.0 | ITU-T X.1541 | 2017-09-06 | 17 | 11.1002/1000/13264 |

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. 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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد 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 البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2018

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

# جدول المحتويات

**الصفحة**


1 مجال التطبيق ..... 1
2 المراجع ..... 1
3 التعاريف ..... 1
1.3 مصطلحات معرَّفة في وثائق أخرى ..... 1
2.3 مصطلحات معرفة في هذه التوصية ..... 1
4 المختصرات والأسماء المختصرة ..... 1
5 الاصطلاحات ..... 2
6 نسق تبادل وصف الشيء المتعلق بالحادث ..... 2
1.6 مقدمة ..... 2
2.6 أنماط بيانات النسق IODEF ..... 2
3.6 نموذج معلومات النسق IODEF ..... 3
4.6 اعتبارات المعالجة ..... 5
5.6 تمديد النسق IODEF ..... 6
6.6 قضايا التدويل ..... 6
7.6 أمثلة ..... 6
8.6 نموذج بيانات النسق IODEF (مخطط اللغة XML) ..... 6
9.6 الاعتبارات الأمنية ..... 6
10.6 اعتبارات هيئة تخصيص أرقام الإنترنت ..... 6
11.6 المراجع ..... 7
بيبليوغرافيا ..... 8

**مقدمة**

توفر التوصية ITU-T X.1500، "نظرة عامة على تبادل معلومات الأمن السيبراني"، توجيهات بشأن تبادل معلومات الأمن السيبراني، بما في ذلك معلومات عن الحوادث العارضة والمؤشرات كما تقدمها هذه التوصية. ونسق تبادل وصف الشيء المتعلق بالحادث (IODEF) هو نموذج بيانات يمثل المعلومات التي يشيع تبادلها بشأن أمن الحاسوب. وهو يصف تمثيلاً لنموذج بيانات بلغة XML لنقل معلومات الحادث بين الكيانات التي تتولى المسؤولية التشغيلية من أجل إنشاء دفاعات استباقية أو القيام بأنشطة لتدارك الخلل أو المراقبة والإنذار ضمن دائرة مستخدمين محددة. ويوفر نموذج البيانات طريقة لتشفير المعلومات عن الجهات المضيفة والشبكات والخدمات التي تعمل على هذه الأنظمة وعن منهجية الاستغلال والبيانات المصاحبة وعن تأثير الحادث وعن النُّهج المحدودة لتوثيق سير العمل.

ويتمثل الهدف الأساسي لنسق IODEF في تعزيز القدرات التشغيلية وتحسين الوعي بالأوضاع. إذ يتيح الاعتماد الجماعي لنسق IODEF تحسين القدرة على تسوية الحوادث والتوعية بالأوضاع المستجدة في عالم التهديدات من خلال تبسيط التعاون والتشارك في المعلومات. وتتيح هيكلية نسق IODEF ما يلي:

- زيادة الأتمتة في معالجة معلومات الحادث، من خلال تبادل معلومات بناءة عن الحادث والاستغناء عن المحللين الأمنيين لتأويل الوثائق النصية ذات الشكل الحر؛
- انخفاض الجهد المبذول في الربط بين بيانات مماثلة، (حتى عندما تكون عالية التنظيم)، من مصادر مختلفة بما يعزز من الوعي بالأوضاع؛
- نسق مشترك لتوفير التشغيل البيني بين أدوات التعامل مع الحوادث وتحليلها، وتحديداً عندما تأتي المعلومات من كيانات متعددة.

وهناك العديد من الاعتبارات الإجرائية والقانونية واعتبارات الثقة والاعتبارات المتعلقة بالسياسات، التي قد تقيد أو تمنع تبادل المعلومات. ونسق IODEF ما هو إلا مواصفة فنية لا يحاول التصدي لهذه القضايا. ومع ذلك، فإن التطبيقات التشغيلية لنسق IODEF والأنساق والبروتوكولات المصاحبة ينبغي لها النظر في هذا السياق الأوسع عند إبرام اتفاقات تبادل المعلومات.

# الإصدار 2 لنسق تبادل وصف الشيء المتعلق بالحادث

## 1 مجال التطبيق

يوصف نسق تبادل وصف الشيء المتعلق بالحادث (IODEF) تمثيلاً لنموذج بيانات لتبادل المعلومات التي يشيع تبادلها عن حوادث أمن الحاسوب أو غيرها من الحوادث. وتصف هذه التوصية نموذج المعلومات الخاص بالنسق IODEF وتقدم نموذجاً للبيانات المصاحبة موصف بمخططات بلغة XML.

ويجب أن يوفر أي تمثيل أو إطار لنموذج بيانات يستخدم في التمكين من تبادل المعلومات عن حوادث أمن الحاسوب أو غيرها من الحوادث قدرات الامتثال لجميع القوانين واللوائح والسياسات الوطنية والإقليمية المعمول بها.

كما يتعين على مستعملي ومطبقي جميع توصيات قطاع تقييس الاتصالات، بما في ذلك هذه التوصية، الامتثال لجميع القوانين واللوائح والسياسات الوطنية والإقليمية المعمول بها.

## 2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[IETF RFC 7970] IETF RFC 7970 (2016), *The Incident Object Description Exchange Format Version 2*. <https://datatracker.ietf.org/doc/rfc7970/>

## 3 التعاريف

### 1.3 مصطلحات معرَّفة في وثائق أخرى

لا توجد.

### 2.3 مصطلحات معرفة في هذه التوصية

لا توجد.

## 4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

IANA هيئة تخصيص أرقام الإنترنت *(Internet Assigned Numbers Authority)*

IODEF نسق تبادل وصف الشيء المتعلق بالحادث *(Incident Object Description Exchange Format)*

## 5 الاصطلاحات

تعتبر المصطلحات التالية متكافئة:

- في استخدام الاتحاد الدولي للاتصالات، يتساوى فعل "يتعين" مع الصيغ الملزمة الأخرى مثل "يجب" وكذلك الأمر بالنسبة إلى الصيغ النافية لهذه الأفعال.
- في استخدام الاتحاد الدولي للاتصالات، يتساوى فعل "يتعين" وتصريفاته مع استخدام فريق مهام هندسة الإنترنت (IETF) لفعل "يجب" وتصريفاته.
- في استخدام الاتحاد الدولي للاتصالات، تتساوى عبارة "يتعين ألا" وتصريفاتها مع استخدام فريق مهام هندسة الإنترنت (IETF) لعبارة "يجب ألا" وتصريفاتها.

**ملاحظة** – لدى فريق مهام هندسة الإنترنت (IETF)، يُستخدم الفعلان "يتعين" و"يجب" (shall وmust على التوالي بالإنكليزية) بأحرفهما الصغيرة بالإنكليزية في سياق النصوص الإعلامية.

## 6 نسق تبادل وصف الشيء المتعلق بالحادث

تُعرِّف الفقرة 6 الإصدار 2 لنسق تبادل وصف الشيء المتعلق بالحادث (IODEF)، مع إحالات مباشرة إلى أقسام المعيار [IETF RFC 7970] بموازاة الفقرات مع ما يقابلها من أرقام أقسام. لذا، على سبيل المثال، فإن الفقرة x.6 تقابل القسم x في المعيار [IETF RFC 7970] مع عناوين مرادفة.

### 1.6 مقدمة

القسم 1 من المعيار [IETF RFC 7970] إعلامي.

#### 1.1.6 المصطلحات

القسم 1.1 من المعيار [IETF RFC 7970] إعلامي.

#### 2.1.6 الترميزات

القسم 2.1 من المعيار [IETF RFC 7970] إعلامي.

#### 3.1.6 بشأن نموذج بيانات IODEF

القسم 3.1 من المعيار [IETF RFC 7970] إعلامي.

#### 4.1.6 تغييرات عن المعيار RFC 5070

القسم 4.1 من المعيار [IETF RFC 7970] إعلامي.

### 2.6 أنماط بيانات النسق IODEF

القسم 2 من المعيار [IETF RFC 7970] إعلامي، لكن أقسامه الفرعية، أي 1.2 إلى 15.2 معيارية. وهي تعرف أنماط البيانات التالية:

- الأعداد الصحيحة (القسم 1.2 من المعيار [IETF RFC 7970] يعرفها)
- الأعداد الحقيقية (القسم 2.2 من المعيار [IETF RFC 7970] يعرفها)
- الأحرف والسلاسل (القسم 3.2 من المعيار [IETF RFC 7970] يعرفها)
- السلاسل متعددة اللغات (القسم 4.2 من المعيار [IETF RFC 7970] يعرفها)

- السلاسل الاثنينية (القسم 5.2 من المعيار [IETF RFC 7970] يعرفها)
  - البايتات ذات الأساس 64 (القسم 1.5.2 من المعيار [IETF RFC 7970] يعرفها)
  - البايتات الست عشرية (القسم 2.5.2 من المعيار [IETF RFC 7970] يعرفها)
- الأنماط المعددة (القسم 6.2 من المعيار [IETF RFC 7970] يعرفها)
- سلسلة التاريخ–الوقت (القسم 7.2 من المعيار [IETF RFC 7970] يعرفها)
- سلسلة النطاق الزمني (القسم 8.2 من المعيار [IETF RFC 7970] يعرفها)
- قوائم المنافذ (القسم 9.2 من المعيار [IETF RFC 7970] يعرفها)
- العنوان البريدي (القسم 10.2 من المعيار [IETF RFC 7970] يعرفه)
- رقم الهاتف (القسم 11.2 من المعيار [IETF RFC 7970] يعرفه)
- سلسلة البريد الإلكتروني (القسم 12.2 من المعيار [IETF RFC 7970] يعرفها)
- سلاسل موقع الموارد الموحد (القسم 13.2 من المعيار [IETF RFC 7970] يعرفها)
- المعرِّفات ومراجع المعرِّف (القسم 14.2 من المعيار [IETF RFC 7970] يعرفها)
- البرمجيات (القسم 15.2 من المعيار [IETF RFC 7970] يعرفها)
  - صنف SoftwareReference (القسم 1.15.2 من المعيار [IETF RFC 7970] يعرفه)
- التمديد (القسم 16.2 من المعيار [IETF RFC 7970] يعرفه)

### 3.6 نموذج معلومات النسق IODEF

القسم 3 من المعيار [IETF RFC 7970] إعلامي، لكن أقسامه الفرعية، أي الأقسام من 1.3 إلى 29.3 معيارية. وهي تعرف نماذج البيانات التالية:

- صنف وثيقة النسق IODEF (القسم 1.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف الحادثة (القسم 2.3 من المعيار [IETF RFC 7970] يعرفه)
- النعوت المشتركة (القسم 3.3 من المعيار [IETF RFC 7970] يعرفها)
  - نعت التقييد (القسم 1.3.3 من المعيار [IETF RFC 7970] يعرفه)
  - نعت معرف الهوية القابل للرصد (القسم 2.3.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف معرف هوية الحادثة (القسم 4.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف معرف الهوية البديل (القسم 5.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف النشاط ذي الصلة (القسم 6.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف الطرف القائم بالتهديد (القسم 7.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف الحملة (القسم 8.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف الاتصال (القسم 9.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف تداول السجل (القسم 1.9.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف العنوان البريدي (القسم 2.9.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف البريد الإلكتروني (القسم 3.9.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف الهاتف (القسم 4.9.3 من المعيار [IETF RFC 7970] يعرفه)

- صنف الاكتشاف (القسم 10.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف نمط الاكتشاف (القسم 1.10.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف الطريقة (القسم 11.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف المرجع (القسم 1.11.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف التقييم (القسم 12.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف أثر النظام (القسم 1.12.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف أثر الأعمال (القسم 2.12.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف أثر الوقت (القسم 3.12.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف أثر النقد (القسم 4.12.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف الثقة (القسم 5.12.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف التأريخ (القسم 13.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف بند التأريخ (القسم 1.13.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف EventData (القسم 14.3 من المعيار [IETF RFC 7970] يعرفه)
  - الربط بين صنفي الحادثة والحدث (القسم 1.14.3 من المعيار [IETF RFC 7970] يعرفه)
  - تعريف تكراري لصنف بيانات الحدث (القسم 2.14.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف التوقعات (القسم 15.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف التدفق (القسم 16.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف النظام (القسم 17.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف العقدة (القسم 18.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف العنوان (القسم 1.18.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف دور العقدة (القسم 2.18.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف العداد (القسم 3.18.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف بيانات الميدان (القسم 19.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف مخدمات الأسماء (القسم 1.19.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف جهات اتصال الميدان (القسم 2.19.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف الخدمة (القسم 20.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف اسم الخدمة (القسم 1.20.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف رأسية التطبيق (القسم 2.20.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف بيانات البريد الإلكتروني (القسم 21.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف السجل (القسم 22.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف بيانات السجل (القسم 1.22.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف نمط السجل (القسم 2.22.3 من المعيار [IETF RFC 7970] يعرفه)

- صنف مفاتيح سجل ويندوز المعدلة (القسم 23.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف المفتاح (القسم 1.23.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف بيانات الشهادة (القسم 24.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف الشهادة (القسم 1.24.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف بيانات الملف (القسم 25.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف الملف (القسم 1.25.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف بيانات التنميق (القسم 26.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف التنميق (القسم 1.26.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف التنميق التقريبي (القسم 2.26.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف بيانات التوقيع (القسم 27.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف بيانات المؤشر (القسم 28.3 من المعيار [IETF RFC 7970] يعرفه)
- صنف المؤشر (القسم 29.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف معرف هوية المؤشر (القسم 1.29.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف معرف هوية المؤشر البديل (القسم 2.29.3 من المعيار [IETF RFC 7970] يعرفه)
  - الصنف القابل للرصد (القسم 3.29.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف صيغة المؤشر (القسم 4.29.3 من المعيار [IETF RFC 7970] يعرفه)
  - الصيغ المعبر عنها بصيغة المؤشر (القسم 5.29.3 من المعيار [IETF RFC 7970] يعرفها)
  - صنف المرجع القابل للرصد (القسم 6.29.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف مرجع المؤشر (القسم 7.29.3 من المعيار [IETF RFC 7970] يعرفه)
  - صنف مرحلة الهجمة (القسم 8.29.3 من المعيار [IETF RFC 7970] يعرفه)

### 4.6 اعتبارات المعالجة

القسم 4 من المعيار [IETF RFC 7970] معياري، على الرغم من أن بعض أقسامه الفرعية إعلامية، كما يوضح في الأقسام الفرعية التالية:

#### 1.4.6 التشفير

القسم 1.4 من المعيار [IETF RFC 7970] معياري.

#### 2.4.6 حيز اسم النسق IODEF

القسم 2.4 من المعيار [IETF RFC 7970] معياري.

#### 3.4.6 التحقق

القسم 3.4 من المعيار [IETF RFC 7970] معياري.

### 4.4.6 أوجه عدم التوافق مع الإصدار 1

القسم 4.4 من المعيار [IETF RFC 7970] إعلامي.

### 5.6 تمديد النسق IODEF

القسم 5 من المعيار [IETF RFC 7970] إعلامي.

توفر التوصية [b-ITU-T X.1500]، "نظرة عامة على تبادل معلومات الأمن السيبراني"، توجيهات بشأن تبادل معلومات الأمن السيبراني، بما في ذلك معلومات عن الحوادث العارضة والمؤشرات كما تقدمها هذه التوصية (ITU-T X.1541). وتقدم هذه التوصية (ITU-T X.1541) النسق الأساسي لتبادل معلومات الحوادث غير أنها لا تغطي جميع حالات الاستعمال الواردة في التوصية [b-ITU-T X.1500]. وقد يتم تطوير تمديدات لتغطية حالات الاستعمال الضرورية.

### 1.5.6 تمديد القيم المعددة للنعوت

القسم 1.5 من المعيار [IETF RFC 7970] معياري، وكذلك أقسامه الفرعية.

### 2.5.6 أصناف التمديد

القسم 2.5 من المعيار [IETF RFC 7970] معياري، وكذلك أقسامه الفرعية.

### 6.6 قضايا التدويل

القسم 6 من المعيار [IETF RFC 7970] معياري.

### 7.6 أمثلة

القسم 7 من المعيار [IETF RFC 7970] إعلامي، وكذلك أقسامه الفرعية التي توضح أمثلة لوثائق النسق IODEF.

### 8.6 نموذج بيانات النسق IODEF (مخطط اللغة XML)

القسم 8 من المعيار [IETF RFC 5070] معياري.

### 9.6 الاعتبارات الأمنية

القسم 9 من المعيار [IETF RFC 7970] معياري، وكذلك أقسامه الفرعية.

في عمليات التنفيذ المطابقة لقطاع تقييس الاتصالات، يوفر نسق وبروتوكول تبادل الرسائل الأساسي المستعمل في تبادل رسائل النسق IODEF الضمانات المناسبة للسرية والسلامة والاستيقان.

**ملاحظة** – تستعمل كلمة "يجب" (في حالتها الأدنى) في فريق مهام هندسة الإنترنت من أجل النص الإعلامي.

### 10.6 اعتبارات هيئة تخصيص أرقام الإنترنت

القسم 10 من المعيار [IETF RFC 7970] معياري، وكذلك أقسامه الفرعية.

## 11.6 المراجع

### 1.11.6 المراجع المعيارية

القسم 1.11 من المعيار [IETF RFC 7970] إعلامي.

حددت هذه التوصية القسم 1.11 من المعيار [IETF RFC 7970] كنص إعلامي لأن قطاع تقييس الاتصالات لم يتخذ موقفاً بشأن أي من هذه المراجع إزاء هذه التوصية. غير أن من المسلم أن فريق مهام هندسة الإنترنت حدد مجموعة من المراجع المعيارية للمعيار [IETF RFC 7970].

### 2.11.6 المراجع الإعلامية

القسم 2.11 من المعيار [IETF RFC 5070] إعلامي.

# بيبليوغرافيا

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

## سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

| | |
|---|---|
| السلسلة A | تنظيم العمل في قطاع تقييس الاتصالات |
| السلسلة D | مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي |
| 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 | البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها |
| السلسلة M | إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات 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، والقياسات والاختبارات المرتبطة بهما |
| السلسلة R | الإرسال البرقي |
| السلسلة S | التجهيزات المطرافية للخدمات البرقية |
| السلسلة T | المطاريف الخاصة بالخدمات التليماتية |
| 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، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية |
| السلسلة Z | اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات |

طُبعت في سويسرا
جنيف، 2018