الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1570

(2011/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تعرف الهوية والاكتشاف

آليات الاكتشاف في إطار تبادل معلومات الأمن السيبراني

التوصيـــة ITU-T X.1570

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
الدليـــل	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 على 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

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

التوصيـــة ITU-T X.1570

آليات الاكتشاف في إطار تبادل معلومات الأمن السيبراني

ملخص

تقدم التوصية ITU-T X.1570 إطاراً لاكتشاف معلومات الأمن السيبراني والآلية التي تسمح بتحقيق ذلك. ويمكن اعتبار الاكتشاف مرحلة من مراحل دورة الحياة المتعلقة بمعلومات الأمن السيبراني القريبة من نشر المعلومات وحيازتها، وهي مراحل متكاملة وضرورية من أجل الاكتشاف. ومن ثم، فإن هذا الإطار يتناول كيفية نشر معلومات الأمن السيبراني، والحصول على قائمة المرشحين والحصول على المعلومات اللازمة. ويمكن تطبيق نظام الاكتشاف بواسطة آليات عشوائية شريطة توافقها مع الإطار، وتشمل هذه الآليات الاكتشاف على أساس معرّف هوية الكائن (OID) والاكتشاف على أساس إطار وصف الموارد (RDF) التي تعالجها هذه التوصية أيضاً.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1570	2011-09-02	17

العبارات الأساسية

معلومات الأمن السيبراني، اكتشاف المصدر، اكتشاف المعلومات.

تمهيـــد

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).

ملاحظـــة

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 2012

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 المصطلحات والتعاريف 1

1.3 مصطلحات معرّفة في وثائق أخرى 1

2.3 مصطلحات معرّفة في هذه التوصية 1

4 المختصرات 2

5 الاصطلاحات 3

6 إطار التعرُّف على مصدر معلومات الأمن السيبراني وتحديد موقعه 3

7 أنماط معلومات الأمن السيبراني المكتشفة ومستوى تفاصيلها 3

8 معرّف معلومات الأمن السيبراني 4

9 أنماط آليات الاكتشاف 5

1.9 آليات الاكتشاف القائم على معرّف الكائن (OID) في تبادل معلومات الأمن السيبراني 5

2.9 آليات الاكتشاف القائم على إطار وصف الموارد (RDF) في تبادل معلومات الأمن السيبراني 6

10 الأساليب المتاحة للنفاذ إلى المعلومات المكتشفة 7

التذييل I أنطولوجيا معلومات الأمن السيبراني التشغيلية 8

1.I ميادين تشغيل الأمن السيبراني 8

2.I الأدوار 8

3.I معلومات الأمن السيبراني 9

التذييل II مواصفات شرح قواعد البيانات وقواعد المعارف 12

التذييل III تنفيذ توضيحي للاكتشاف القائم على إطار وصف الموارد (RDF) 13

1.III مثال تنفيذ للاكتشاف القائم على إطار وصف الموارد (RDF) 13

2.III تراتبية أصناف معلومات الأمن السيبراني 13

ببليوغرافيا 15

مقدمة

يحظى تبادل معلومات الأمن السيبراني بأهمية أكثر من أي وقت مضى. وثمة معيار دولي لتبادل معلومات الأمن السيبراني يدعى "CYBEX" ويسترعي انتباهاً كبيراً بوجه خاص. ومن بين مواصفات CYBEX التقنية المختلفة، مواصفة اكتشاف CYBEX التي توفر خطة للعثور على مصدر معلومات الأمن السيبراني. وتشرح هذه التوصية إطار هذه المواصفة وتقنياتها.

التوصيـــة ITU-T X.1570

آليات الاكتشاف في إطار تبادل معلومات الأمن السيبراني

1 مجال التطبيق

تقدم هذه التوصية إطاراً لاكتشاف معلومات الأمن السيبراني والآلية التي تسمح بتحقيق ذلك. ويمكن اعتبار الاكتشاف مرحلة من مراحل دورة الحياة المتعلقة بمعلومات الأمن السيبراني القريبة من نشر المعلومات وحيازتها، وهي مراحل متكاملة وضرورية من أجل الاكتشاف. ومن ثم، فإن هذا الإطار يتناول كيفية نشر معلومات الأمن السيبراني، والحصول على قائمة المرشحين والحصول على المعلومات اللازمة. ويمكن تطبيق نظام الاكتشاف بواسطة آليات عشوائية شريطة توافقها مع الإطار. وتشمل هذه الآليات الاكتشاف على أساس معرّف هوية الكائن (OID) والاكتشاف على أساس إطار وصف الموارد (RDF) التي تعالجها هذه التوصية أيضاً.

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.

[ITU-T X.660] التوصية ITU-T X.660 (2011) | ISO/IEC 9834-1: 2012، *تكنولوجيا المعلومات – إجراءات عمل سلطات تسجيل معرف الكائن: الإجراءات العامة والفروع العليا لشجرة معرف الكائن العالمية*.

[W3C RDF] W3C Recommendation (2004), *Resource Description F ramework (RDF): Concepts and Abstract Syntax.* <http://www.w3.org/TR/rdf-concepts/>

3 المصطلحات والتعاريف

1.3 مصطلحات معرّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 معرّف (هوية) الكائن (object identifier) [ITU-T X660]: قائمة مرتّبة أو منظمة بالقيم الصحيحة الأولية تبدأ من جذر شجرة معرّف (هوية) الكائن الدولية وحتى العقدة، وهي تعرّف تلك العقدة بشكل واضح لا يشوبه الغموض.

2.1.3 الأنطولوجيا (ontology) [b-Gruber]: توصيف صريح لمفهوم.

2.3 مصطلحات معرّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 معلومات الأمن السيبراني: معلومات أو معارف منظمة تتعلق بما يلي:

1) "حالة" المعدات أو البرمجيات أو الأنظمة الشبكية المتعلقة بالأمن السيبراني، خاصة مواطن التعرض؛

2) الأدلة القضائية المتعلقة بالحوادث العارضة أو الأحداث؛

3) وسائل الاستدلال بالتجربة والاتجاهات المكتسبة من الأحداث السابقة؛

4) الأطراف التي تنفذ قدرات تبادل معلومات الأمن السيبراني ضمن نطاق هذا الإطار؛

5) مواصفات تبادل معلومات الأمن السيبراني، بما في ذلك الوحدات النمطية والمخططات والشروط والمقتضيات والأرقام المخصصة؛

6) نعوت الهويات والضمانات الخاصة بكافة معلومات الأمن السيبراني؛

7) المتطلبات والمبادئ التوجيهية والممارسات الخاصة بالتنفيذ.

ملاحظة – يستند هذا التعريف إلى وصف معلومات الأمن السيبراني الوارد في التوصية [b-ITU-T X.1500].

2.2.3 تبادل معلومات الأمن السيبراني: نقل معلومات الأمن السيبراني بين جهتي أمن سيبراني أو أكثر. وقد يكون النقل هذا أحادي الاتجاه أو ثنائي الاتجاه أو متعدد الاتجاهات، أي من العديد إلى العديد.

3.2.3 الاكتشاف: فعل أو عملية اكتشاف الهدف، أي الحصول على معرفة الهدف للمرة الأولى.

4.2.3 المستخرِج: كيان يستخرج معلومات الأمن السيبراني.

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

CCE تعداد التشكيلات الشائعة (*Common Configuration Enumeration*)

CERT فريق الاستجابة للطوارئ الحاسوبية (*Computer Emergency Response Teams*)

CIRT فريق الاستجابة للحوادث الحاسوبية (*Computer Incident Response Team*)

CPE تعداد المنصات الشائعة (*Common Platform Enumeration*)

CVE مَواطن الضعف والتعرض الشائعة (*Common Vulnerabilities and Exposures*)

CVSS نظام تقييم مواطن التعرض الشائعة (*Common Vulnerability Scoring System*)

CWE تعداد مواطن الضعف الشائعة (*Common Weakness Enumeration*)

CWSS نظام تقييم مواطن الضعف الشائعة (*Common Weakness Scoring System*)

CYBEX تبادل معلومات الأمن السيبراني (*CYBersecurity information EXchange*)

HTTP بروتوكول نقل النص التشعبي (*Hypertext Transfer Protocol*)

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

MAEC تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها (*Malware Attribute Enumeration and Characterization*)

OID معرف هوية الكائن (*Object IDentifier*)

OVAL لغة التعرض والتقييم المفتوحة (*Open Vulnerability and Assessment Language*)

RDF إطار وصف الموارد (*Resource Description Framework*)

SCAP بروتوكول أتمتة المحتوى الأمني (*Security Content Automation Protocol*)

SNMP بروتوكول إدارة الشبكات البسيطة (*Simple Network Management Protocol*)

XCCDF نسق وصف القائمة المرجعية القابل للتوسع في التشكيلة (*eXensible Configuration Checklist Description Format*)

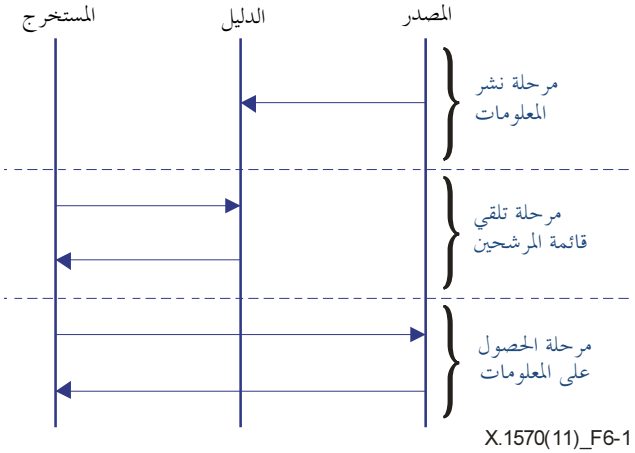
5 الاصطلاحات

لا توجد.

6 إطار التعرُّف على مصدر معلومات الأمن السيبراني وتحديد موقعه

تنفذ منظمات أمن سيبراني مختلفة بروتوكولات أمن سيبراني مشتركة كي تلتقط في التطبيقات التشغيلية، وتتبادل، معلومات حالة النظام والثغرات الأمنية والأدلة القضائية ومعلومات الاستدلال بالتجربة بصدد الحوادث الأمنية. وإذ تصبح هذه المعلومات متاحة من مصادر مختلفة وكثيرة، ينبغي للمنفذين مواءمة كيفية التعرف على منظمات الأمن السيبراني وسياسات الثقة وتبادل المعلومات، ومواءمة المعلومات نفسها التي يتم تبادلها أو توزيعها. ولمعالجة هذه المسألة، يقدم هذا القسم إطاراً لتحديد هوية ومكان ومصدر معلومات الأمن السيبراني – إطار اكتشاف معلومات الأمن السيبراني.

وينطوي العثور على معلومات الأمن السيبراني على ثلاث جهات: المستخرِج والمصدر والدليل. فيستخرج المستخرج المعلومات عن طريق إرسال طلب، ويوفر المصدر المعلومات المطلوبة، ويسجل الدليل البيانات الوصفية لمعلومات المصدر ويساعد المتلقي في العثور على المصدر الصحيح.

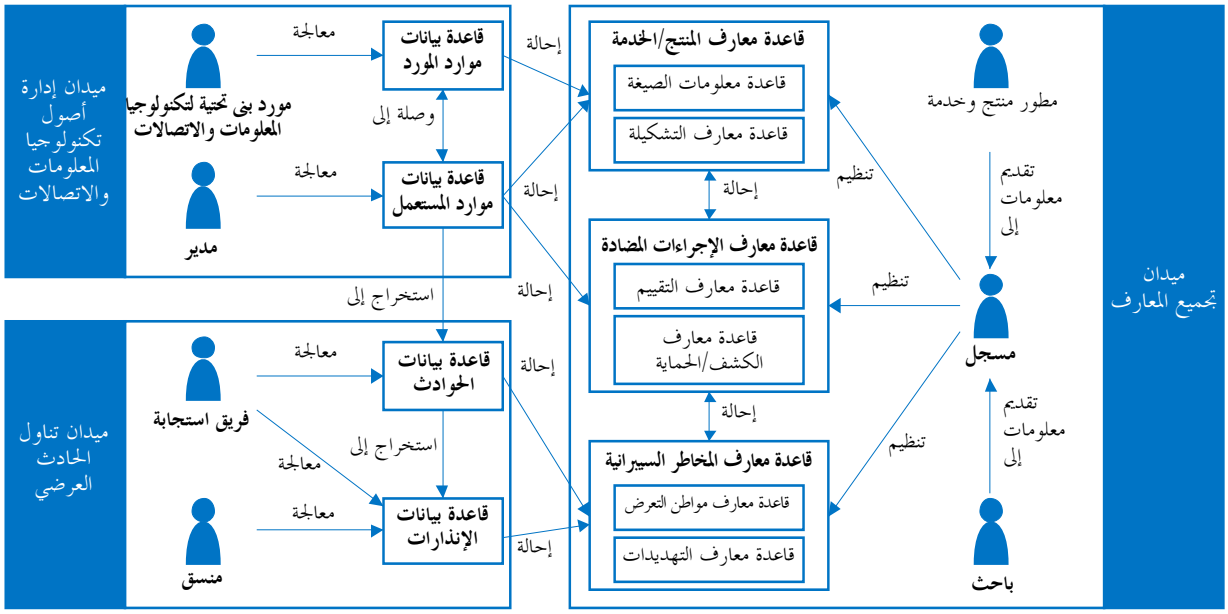


الشكل 6-1 – مراحل الاكتشاف الثلاث

عملية الاكتشاف هي عملية تواصل الجهات الثلاث، كما يرد رسمها في الشكل 6-1. وهي على ثلاث مراحل: نشر المعلومات وتلقي قائمة المرشحين والحصول على المعلومات. فينشر المصدر معلوماته من أجل المجتمع السيبراني بتسجيلها لدى الدليل في مرحلة نشر المعلومات. ويستعلم المستخرج من دليل السجل بشأن قائمة المصادر المرشحة في مرحلة تلقي القائمة المرشحة. ثم يختار المستخرج من القائمة المصدر الذي يبدو الأنسب، ويتلقى معلومات المصدر في مرحلة اختيار المصدر.

7 أنماط معلومات الأمن السيبراني المكتشفة ومستوى تفاصيلها

تستطيع آليات الاكتشاف أن تكتشف معلومات الأمن السيبراني. وتسعى هذه الآلية لاكتشاف الأنماط السبعة التالية من المعلومات: قاعدة بيانات موارد المستخدم، وقاعدة بيانات موارد المورّد، وقاعدة بيانات الحوادث، وقاعدة بيانات الإنذارات، وقاعدة معارف المنتج والخدمة، وقاعدة معارف المخاطر السيبرانية، وقاعدة معارف الإجراءات المضادة. ويقدم الشكل 7-1 نموذج الأنطولوجيا المستخدم في هذه التوصية ويُظهر العلاقة بين أنماط المعلومات المستخدمة في هذا النموذج.



الشكل 7-1 – أنطولوجيا معلومات الأمن السيبراني التشغيلية

هذه الأنطولوجيا هي نموذج لوصف الحصول على معارف معلومات الأمن السيبراني وتجميعها واستخدامها، وتتألف هذه المعارف من مجموعة من ميادين العمليات والأدوار وأنماط المعلومات. وتبين الخطوط المتصلة العلاقة بين أنماط المعلومات في حين تشير الأسهم إلى إدخال المعلومات من جهة إلى قاعدة معارف/قاعدة بيانات. وتتسم الوظائف المعروضة في الجانب الأيمن بعموميتها، ويمكن لجهات مثل أفرقة الاستجابة للحوادث الحاسوبية (CIRT) أن تشمل واحدة أو أكثر من هذه الوظائف. ويستخدم هذا النموذج لتحديد ميادين عمليات الأمن السيبراني، وبعدئذ للتعرف على جهات الأمن السيبراني المطلوبة لدعم العمليات في كل ميدان. ويرد شرح تفاصيل الأنطولوجيا في التذييل I.

ويظهر الجدول II-1 مواصفات الأمن السيبراني المتسقة مع سبعة أنماط من المعلومات الموصوفة في نموذج الأنطولوجيا هذا. وسيواكب مستوى تفاصيل المعلومات السيبرانية المكتشفة مستوى تفاصيل المعايير. وباستخدام هذا النهج، يكون مستوى التفاصيل مرناً بما فيه الكفاية يتيح استخدام معايير متنوعة يمكن أن تُنشأ لأغراض محددة.

8 معرّف معلومات الأمن السيبراني

تدعو الحاجة لإفراد معرّف ليتعرف على معلومات الأمن السيبراني. وأي معرّف فريد عالمياً يُستخدم لتبادل معلومات الأمن السيبراني عالمياً يتعين أن يمتلك الخصائص التالية:

- البساطة وسهولة الاستخدام والمرونة وقابلية التوسع، والتدرّجية وإمكانية النشر
- الإدارة الموزعة لمختلف خطط المعرّف
- الموثوقية طويلة الأجل لأصحاب سجلات المعرف وتيسر الأدوات عالية الأداء لاكتشاف المعلومات المرتبطة بأي معرّف.

وهناك معرفان مرشحان يفيان بالمتطلبات المذكورة أعلاه: وهما إطار معرّف الكائن (OID) وإطار وصف الموارد (RDF)، ويمثلان النموذجين الأولين للخدمات المشتركة واكتشاف المعلومات، على النحو الذي يرد بحثه في الفقرة 9.

9 أنماط آليات الاكتشاف

يمكن تنفيذ خطط الاكتشاف بآليات عشوائية طالما التزمت الإطار. وتصنف في نمطين – مركزية ولا مركزية – من منطلق كيف تسجل سجلات معلومات الأمن السيبراني وتديرها.

وفي حالة الآلية المركزية، تدير الدلائل واحد أو أكثر من السجلات "المركزية"، مما يسهل تحديد مواقع المعلومات المستهدفة ويسرع من اكتشافها (وفي بعض الحالات، يمكن حذف قائمة المرشحين في مرحلة التلقي). بيد أن الطرف الباحث يحتاج أولاً لأن يعلم بوجود تسجيل معين قبل أن يتمكن من استخدامه. كما أن ما ينطوي عليه الحفاظ على مستودع مركزي من موارد متنوعة وتكاليف مستحقة يمكن أن يبعده عن متناول ذوي الموارد المحدودة. والآلية المعتادة هنا هي الاكتشاف القائم على معرّف الكائن (OID).

وفي حالة الآلية اللامركزية، تدير الدلائل سجلات "موزعة" متعددة. وتتميز هذه الحالة بحد أدنى من موارد وتكاليف ترتبط بإتاحة المعلومات، ولا حاجة لمن يقدم المعلومات ومن يطلبها لأن يعرف كل منهما بوجود الآخر مسبقاً. غير أن البحث عن المعلومات دون أي معرفة بها سيضطر الباحث فعلياً للسعي زحفاً في كل أرجاء الإنترنت. والآلية المعتادة هنا هي الاكتشاف القائم على إطار وصف الموارد (RDF).

1.9 آليات الاكتشاف القائم على معرّف الكائن (OID) في تبادل معلومات الأمن السيبراني

تتعرف آلية الاكتشاف القائم على معرّف الكائن (OID) على مصادر معلومات الأمن السيبراني وتحدد مواقعها باستخدام معرّف الكائن، وذلك ضمن هيكل شجرة تراتبية تعرّف أوراقها هوية الكائنات. وتنشئ معرفات الكائنات تسمية تراتبية، أي سلسلة قيم أقواس تبدأ من جذر الشجرة وصولاً إلى إحدى أوراقها. ويمكن الوصول إلى أي معلومة أمن سيبراني مسجلة بالسير في مسالك شجرة معرّف الكائن من جذرها إلى إحدى أوراقها؛ علماً بأن معلومات الأمن السيبراني تُسجل في إطار فرع معرف كائن تبادل معلومات الأمن السيبراني [b-ITU-T X.1500.1] {joint-iso-itu-t(2) cybersecurity(48)}.

وترد في الفقرات 1.1.9-3.1.9، تفاصيل مراحل الاكتشاف التي عُرضت مقدمة عنها في الفقرة 6.

1.1.9 مرحلة نشر المعلومات

عند تسجيل المعلومات، يوفر مصدر أنماط متعددة من المعلومات الوصفية، من بينها فئات رئيسية هي: البلد/المنطقة ومعرف المنظمة ونمط المعلومات ونسق وصف المعلومات. فيحدد البلد/المنطقة بلد المنظمة أو منطقة المنظمة إذا كان المصدر منظمة عابرة للحدود الوطنية مثل الاتحاد الدولي للاتصالات. ويحدد المعرّف المنظمة ويمكن وصفها مثلاً باستخدام رقم غصن أقل كثافة أو اسم تجاري تنفرد به. ويحدد نمط المعلومات نوع المعلومات المذكورة في الفقرة 7. ويحدد نسق وصف المعلومات النسق، كأن يكون نسقاً متوافقاً مع مواطن الضعف والتعرض الشائعة (CVE) [b-ITU-T X.1520] أو مع نسق الإجابة التلقائية (ARF) [b-ARF].

وعند تلقي طلب التسجيل من المصدر، يسجل الدليل المعلومات ويخزنها على أساس البيانات الوصفية ويبني أشجاراً فرعية من معرفات الكائنات. ورغم أن هذه التوصية لا توصّف أي هيكل معياري للشجرة، يرد وصف بعض الهياكل المرشحة في التذييلين I وII.

2.1.9 مرحلة تلقي قائمة المرشحين

لا يرسل المستخرج بالضرورة استعلاماً إلى الدليل الذي يحتوي على السجل الثابت الوحيد لشجرة معرف الكائن. إذ يمكن أن يعرف هيكل الشجرة مسبقاً، وبالسير في مسالكها، يمكنه التعرف على المعلومات المطلوبة دون إرسال الاستعلام.

ويمكن أن يقبل الدليل استعلاماً عشوائياً (بما في ذلك استعلام البحث النصي) وأن يجيب بقائمة مرشحين.

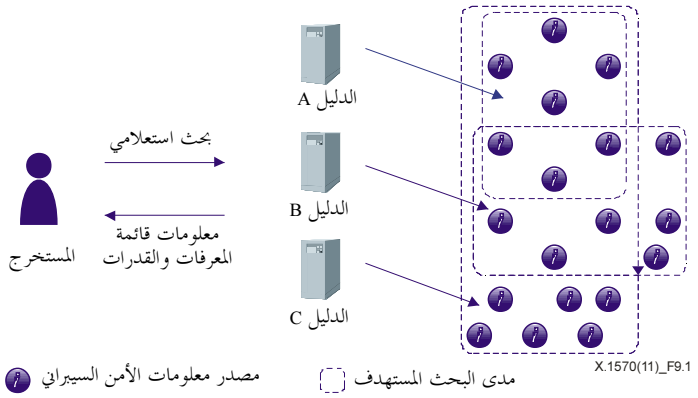
3.1.9 مرحلة الحصول على المعلومات

يختار المستخرج مصدراً للمعلومات استناداً إلى قائمة المرشحين أو بالسير في مسالك الشجرة من الجذر إلى ورقة، ثم يرسل طلباً إلى المصدر الذي يرد بتقديم معلومات الأمن السيبراني.

وفي الاكتشاف القائم على معرّف الكائن (OID)، يمكن اعتبار مرحلتي تلقي قائمة المرشحين والحصول على المعلومات متلازمتين لأن حصر المرشح بالسير في مسالك الشجرة يؤدي إلى اختيار مصدر واحد.

2.9 آليات الاكتشاف القائم على إطار وصف الموارد (RDF) في تبادل معلومات الأمن السيبراني

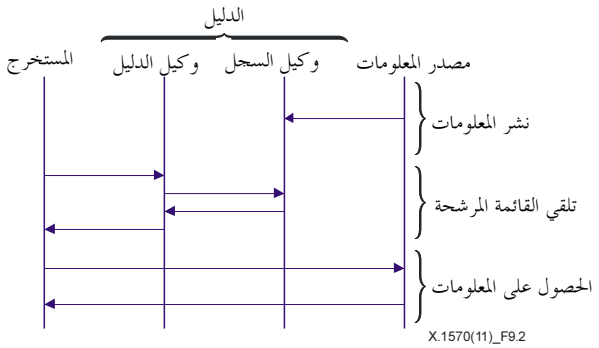
تتعرف آلية الاكتشاف القائم على إطار وصف الموارد (RDF) مصادر معلومات الأمن السيبراني وتحدد مواقعها على أساس إطار وصف الموارد. ويرد وصف مفهوم هذه الآلية في الشكل 9-1. فيمكن للمصدر أن يسجل نفسه في دليل واحد أو أكثر (يحوي سجلات) مما يسهل على المتلقين استخراج المعلومات. ويتم تبادل المعلومات عن هويات وقدرات جهات الأمن السيبراني بين هذه الجهات خلال عملية الاكتشاف. وترسل جهات الأمن السيبراني طلبات اكتشاف إلى دليل، ولكل منها مصادر مختلفة تصبح المدى الذي يتعين على محرك البحث أن يفتش فيه.



الشكل 9-1 – مفهوم اكتشاف إطار وصف الموارد

بخلاف الاكتشاف القائم على معرّف الكائن (OID)، توجد في الاكتشاف القائم على إطار وصف الموارد (RDF) دلائل تتألف من جهات متعددة، انظر الشكل 9-2. ومن وجهة نظر وظيفية، يتألف الدليل من وكيل اكتشاف ووكيل سجل. فيتواصل وكيل الاكتشاف مع المستخرِج (سطح بيني للمتلقي) فيما يتواصل وكيل السجل مع مصدر المعلومات (سطح بيني للمصدر). وقد يقع وكيل الاكتشاف ووكيل السجل في بعض الحالات ضمن حاسوب واحد. ويتم تبادل المعلومات عن القدرات والمعرفات بين الجهات الأربع.

ويرد عرض تفاصيل مراحل الاكتشاف، التي سُردت مقدمة عنها في الفقرة 6، في الفقرات من 1.2.9 حتى 3.2.9.



الشكل 9-2 – المخطط التتابعي للاكتشاف القائم على إطار وصف الموارد

1.2.9 مرحلة نشر المعلومات

يسجل مصدر معلوماته لدى وكيل التسجيل الذي يولد ويرتب بيانات وصفية مناسبة للبيانات في مرحلة نشر المعلومات. وكما في الاكتشاف القائم على معرّف الكائن (OID)، يوفر المصدر أنماطاً متعددة من المعلومات الوصفية عند تسجيل معلومات الأمن السيبراني، من بينها فئات رئيسية هي: البلد/المنطقة ومعرف المنظمة ونمط المعلومات ونسق وصف المعلومات. فيحدد البلد/المنطقة بلد المنظمة أو منطقة المنظمة إذا كان المصدر منظمة عابرة للحدود الوطنية مثل الاتحاد الدولي للاتصالات. ويحدد المعرّف المنظمة ويمكن وصفها مثلاً باستخدام رقم غصن أكثر كثافة أو اسم تجاري تنفرد به. ويحدد نمط المعلومات نوع المعلومات المذكورة في الفقرة 7. ويحدد نسق وصف المعلومات النسق، كأن يكون نسقاً متوافقاً مع مواطن الضعف والتعرض الشائعة (CVE) أو مع نسق الإجابة التلقائية (ARF).

وعند تلقي طلب التسجيل من المصدر، يسجل الدليل المعلومات ويخزنها على أساس البيانات الوصفية وتحديثات قاعدة بيانات إطار وصف الموارد (RDF). وبما أن وكلاء السجلات كثيراً ما يستخدمون سجلات موزعة تراتبياً، يحتاج وكيل السجل لتحديد السجل الذي يتعين خزن البيانات فيه.

ورغم أن هذه التوصية لا توصّف أي هيكل معياري لنسق البيانات الوصفية لإطار وصف الموارد (RDF)، يرد وصف بعض الهياكل المرشحة في التذييلين I وII.

2.2.9 مرحلة تلقي قائمة المرشحين

يرسل المستخرِج استعلامات لوكيل اكتشاف يسيّرها إلى واحد أو أكثر من وكلاء السجلات الأنسب فيقومون بالتفتيش في قواعد البيانات الوصفية لديهم ويجيبون بقائمة من المصادر المرشحة في مرحلة تلقي قائمة المرشحين. فيجمع وكيل الاكتشاف المعلومات الواردة من وكلاء السجلات المتعددين ويرسلها إلى المستخرِج.

3.2.9 مرحلة الحصول على المعلومات

يختار المستخرِج المصدر الأنسب من القائمة في مرحلة الحصول على المعلومات.

10 الأساليب المتاحة للنفاذ إلى المعلومات المكتشفة

يمكن استخدام بروتوكولات الاتصالات المختلفة لتبادل معلومات الأمن السيبراني بما في ذلك بروتوكول نقل النص التشعبي (HTTP) (الذي يستخدم RDF) وبروتوكول إدارة الشبكات البسيطة (الذي يستخدم OID).

وقد ترغب بعض الأطراف بحصر الأطراف الذين يمكنهم النفاذ إلى المعلومات المكتشفة بوضع سياسات للتحكم بالنفاذ. تشمل المعايير الرئيسية للسياسات عنوان بروتوكول الإنترنت، والميدان، وبروتوكول الاتصالات، والهوية وكلمة المرور، وشهادة تحديد الهوية.

وأي طرف يسعى إلى معلومات بشأن الأمن السيبراني يتبادل رسائل مختلفة، بما فيها رسائل الطلب. وستعرَّف هذه الأساليب في توصيات من سلسلة ITU-T X.1500.

التذييل I

أنطولوجيا معلومات الأمن السيبراني التشغيلية

(لا يمثل هذا التذييل جزءاً أساسياً من هذه التوصية)

ترد في الفقرة 7 من هذه التوصية أنطولوجيا معلومات الأمن السيبراني التشغيلية على النحو المبين في الشكل 7-1. ويورد هذا التذييل تفاصيل الأنطولوجيا.

فهي تتألف من ميادين عمليات الأمن السيبراني ومن الأدوار اللازمة لتشغيل العمليات في الميادين، ومعلومات الأمن السيبراني المرتبطة بالأدوار. ويرد عرضها أدناه.

1.I ميادين تشغيل الأمن السيبراني

يشمل مصطلح "تشغيل الأمن السيبراني" مجموعة من العمليات الأمنية في المجتمع السيبراني، ولكن هذه الأنطولوجيا تركز على عمليات الأمن السيبراني التي تحفظ أمن المعلومات في المجتمعات السيبرانية. وأمن المعلومات هو الحفاظ على سرية المعلومات وسلامتها وتوافرها، ويشمل أحياناً المساءلة التي تنطوي عليها المعلومات أيضاً وأصالتها وموثوقيتها.

ولوصف ميدان مثل هذه العمليات، توفر الأنطولوجيا ثلاثة ميادين عمل للأمن السيبراني: إدارة موجودات تكنولوجيا المعلومات، والتعامل مع الحوادث، واكتناز المعرفة.

إدارة موجودات تكنولوجيا المعلومات: يدير هذا الميدان عمليات الأمن السيبراني داخل منظمات المستخدمين، من قبيل تركيب موجودات تكنولوجيا المعلومات وتشكيلها وإدارتها، ويشمل عمليتي الوقاية من الحوادث واحتواء الأضرار كلتيهما. ولا تقتصر موجودات تكنولوجيا المعلومات على مقتنيات المستخدم من تكنولوجيا المعلومات بل تتضمن أيضاً توصيلية الشبكة، والخدمات السحابية وخدمات الهوية التي تقدمها جهات خارجية للمستخدم.

التعامل مع الحوادث: يكشف هذا الميدان الحوادث التي تقع في المجتمعات السيبرانية ويستجيب لمقتضياتها من خلال مراقبة الأحداث الحاسوبية والحوادث المكونة من أحداث حاسوبية متعددة والسلوكيات الهجومية التي تسببت في الحوادث. وبعبارة أدق، فهو يراقب الأحداث الحاسوبية، ويقدم تقريراً بحادث حالما يكتشف شذوذاً. واستناداً إلى هذا التقرير، يحقق في ملابسات الحادث حتى يتمكن من توضيح نمط الهجوم والتدابير المضادة له. واستناداً إلى تحليل الحادث، فإنه قد يوفر التنبيهات والتحذيرات، ومثالها الإنذار المبكر لمنظمات المستخدمين بشأن التهديدات المحتملة.

اكتناز المعرفة: يجمع هذا الميدان معلومات الأمن السيبراني ويولدها، ويستخلص المعرفة التي يمكن للمنظمات الأخرى إعادة استخدامها. ولتسهيل إعادة الاستخدام، فهو يوحد التسميات والتصنيفات التي ينظم من خلالها المعارف ويكتنزها. ويشكل هذا الميدان أساساً للتعاون العالمي خارج حدود المنظمة.

2.I الأدوار

بناءً على ميادين الأمن السيبراني المعرّفة أعلاه، تحدد هذه الفقرة الأدوار اللازمة لإدارة عمليات الأمن السيبراني في كل ميدان. ففي ميدان إدارة موجودات تكنولوجيا المعلومات توجد جهة إدارية وجهة تقدم البنية التحتية لتكنولوجيا المعلومات. وفي ميدان التعامل مع الحوادث هناك فريق استجابة ومنسق. وفي ميدان اكتناز المعرفة ثمة باحث، ومطور منتجات وخدمات، وأمين سجل لعملياتهما، على التوالي؛ علماً بأن الأدوار تعرَّف من منظور الوظائف، ومن ثم يمكن لجهة واحدة أن تتولى عدة أدوار حسب السياق.

الجهة الإدارية: يدير هذا الدور نظام منظمته ويحافظ على خصائصه الوظيفية. ولهذا الغرض، يراقب هذا الدور استخدام النظام، ويشخصه عن طريق القيام بالتدقيق للتحقق من السلامة وتقصي مواطن الضعف وإجراء اختبارات اختراق، ثم تقييم

مستوى الأمان للنظام. ويمثل المسؤول عن إدارة النظام داخل كل منظمة مثالاً نمطياً على ذلك. كما يقوم مقدم خدمة الأمن المُدار (MSSP) بمقام جهة إدارية إذا ما أسندت منظمة ما بعض العمليات المذكورة أعلاه إلى جهة خارجية.

مزوّد البنية التحتية لتكنولوجيا المعلومات: يوفر هذا الدور البنية التحتية لتكنولوجيا المعلومات للمنظمة. وتشمل البنية التحتية وتوصيلية الشبكة والخدمات السحابية مثل البرمجيات كخدمة (SaaS) والمنصة كخدمة (PaaS) والبنية التحتية كخدمة (IaaS). ويمتلك مزود البنية التحتية لتكنولوجيا المعلومات معلومات عن الشبكات بين المنظمات، مثل معلومات طوبولوجيا الشبكة ومواصفات الخدمات السحابية. ومن الأمثلة النمطية على ذلك: مقدم خدمة الإنترنت (ISP)، ومقدم خدمة التطبيقات (ASP)، ومقدم الخدمة السحابية (CSP).

فريق الاستجابة: يراقب هذا الدور ويحلل حوادث متنوعة في المجتمعات السيبرانية، مثل النفاذ غير المصرح به وهجمات حجب الخدمة الموزعة (DDoS) والتصيد، وهو يكتنز المعلومات بشأن الحوادث. واستناداً إلى هذه المعلومات، يمكنه تنفيذ التدابير المضادة، من قبيل منع الحركة وتسجيل عناوين مواقع التصيد على القوائم السوداء. ومن الأمثلة النمطية على ذلك، فريق الاستجابة لمقتضيات الحوادث لدى مقدم خدمة الأمن المُدار (MSSP).

المنسق: يقوم هذا الدور بالتنسيق مع الأدوار الأخرى، ويتناول التهديدات المحتملة على أساس المعلومات المعروفة ذات الصلة بالحادث. فيوفر تحذيرات للمنظمات الأخرى ويقود في بعض الأحيان مسعىً تعاونياً لتخفيف الأضرار يتعامل مع هجمات مدمرة واسعة النطاق مثل هجمات حجب الخدمة الموزعة. ومن الأمثلة النمطية على ذلك، مركز تنسيق فريق الاستجابة للطوارئ الحاسوبية (CERT/CC)، سواء كان ذلك تجارياً أو غير تجاري.

الباحث: يبحث هذا الدور في قضايا الأمن السيبراني بما في ذلك نقاط الضعف والهجمات، ويستخلص المعارف من البحوث ويكتنزها. وهو ينشر العديد من المعلومات القابلة لإعادة الاستخدام عن طريق أمين السجل، بحيث تتمكن فرادى المؤسسات من تنفيذ التدابير المضادة اللازمة. ومن الأمثلة النمطية على ذلك: هيئة X-force ضمن شركة International Business Machines Corp (IBM)، ومعهد بحوث مخاطر الفضاء السيبراني (RRICS) في شركة the Little eArth Corporation Co., Ltd. (LAC)، ومختبر McAfee Lab. ضمن شركة McAfee Inc.

مطور المنتجات والخدمات: يطور هذا الدور المنتجات والخدمات ويكتنز المعلومات الخاصة بها، مثل ما يخصها من الإصدارات والتشكيلات ونقاط الضعف والترقيعات البرمجية. وشأنه شأن الباحث، فهو ينشر العديد من المعلومات القابلة لإعادة الاستخدام عن طريق أمين السجل، بحيث تتمكن فرادى المؤسسات من تنفيذ التدابير المضادة اللازمة. ومن الأمثلة النمطية على ذلك: منفذ بيع البرمجيات والفرد المبرمج للبرمجيات في القطاع الخاص.

أمين السجل: يصنف هذا الدور معارف الأمن السيبراني التي يقدمها الباحث ومطور المنتجات والخدمات، وينظمها ويكتنزها بحيث يمكن لمنظمات أخرى الاستفادة كذلك من هذه المعارف. ومن الأمثلة النمطية على ذلك: المعهد الوطني للمعايير والتكنولوجيا (NIST) ووكالة النهوض بتكنولوجيا المعلومات، في اليابان. وفي بعض الحالات يمكن للجهة العاملة بوصفها الباحث أو مطور المنتجات والخدمات أن تتولى أيضاً دور أمين السجل وتنشر المعلومات.

3.I معلومات الأمن السيبراني

تحدد هذه الفقرة المعلومات اللازمة لعمليات الأمن السيبراني، بناءً على ميادين العمليات وأدوارها. ومع مراعاة المعلومات التي ينطوي عليها كل من الأدوار، تعرّف هذه الأنطولوجيا أربع قواعد بيانات: موارد المستخدم، وموارد المقدم، والحادث، والإنذار. كما تعرِّف ثلاث قواعد معرفية: المنتجات والخدمات، والتدابير المضادة، والمخاطر السيبرانية.

1.3.I قاعدة بيانات موارد المستخدم

تقوم قاعدة بيانات موارد المستخدم باكتناز معلومات عن الموجودات داخل فرادى المنظمات وهي تحتوي على معلومات، مثل قوائم البرمجيات/العتاد، وتشكيلاتها، وحالة استخدام الموارد وسياسات الأمن بما فيها سياسات التحكم في النفاذ، ونتائج تقييم مستوى الأمن، وطوبولوجيا الشبكة الداخلية. كما أنها تحتوي على معلومات خارجية عن الموارد يمكن أن تستفيد منها

فرادى المنظمات المستخدِمة من قبيل قوائم الاشتراك للخدمات السحابية (على سبيل المثال، مراكز البيانات والبرمجيات كخدمة (SaaS)) وسجلات استخدامها. وتقوم الجهة الإدارية بمعالجة مثل هذه المعلومات. ويمكن الاستفادة من نسقي ARF وCRF لوصف نتائج تقييم الموجودات، في حين يمكن الاستفادة من علامات CVSS وCWSS لإسناد علامات إلى مستوى أمان موجودات تكنولوجيا المعلومات. وتستفيد الجهات الإدارية من هذه العلامات لتحديد أولويات عمليات الأمن من حيث الأهمية على موجودات تكنولوجيا المعلومات.

2.3.I قاعدة بيانات موارد المقدِّم

تقوم قاعدة بيانات موارد المقدِّم باكتناز معلومات عن الموجودات خارج فرادى المنظمات. وللقيام بعمليات الأمن السيبراني بفعالية وكفاءة، تحتاج قاعدة بيانات لأن تكون موصولة بقاعدة بيانات موارد المستخدم لأن تمييز الحدود الفاصلة بين موجودات تكنولوجيا المعلومات الداخلية والخارجية يصبح أصعب فأصعب لا سيما في مجال الحوسبة السحابية. ويقوم مقدِّم البنية التحتية لتكنولوجيا المعلومات بمعالجة مثل هذه المعلومات. وتحتوي قاعدة البيانات أساساً على معلومات عن شبكات المقدِّم والخدمات السحابية. وتتناول معلومات شبكة المقدم الشبكات التي توصل بها كل منظمة مع المنظمات الأخرى، مثل الطوبولوجيا، ومعلومات التسيير، وسياسات التحكم في النفاذ، وحالة الحركة، ومستويات الأمان. وتشمل معلومات الخدمة السحابية مواصفات الخدمة، ومعلومات عن عبء العمل وعن سياسة الأمن لكل خدمة سحابية؛ علماً بأن المعلومات الخاصة بالمنظمات المستخدمة، مثل التشكيلة المحلية لكل خدمة سحابية، تخزَّن في قاعدة بيانات موارد المستخدم.

3.3.I قاعدة بيانات الحوادث

تحتوي قاعدة بيانات الحوادث على معلومات عن الحوادث تتولد على أساس تحليل المعلومات في قاعدة بيانات موارد المستخدم. ويعالج فريق الاستجابة تلك المعلومات. وتتضمن قاعدة البيانات هذه ثلاثة سجلات: سجل الأحداث، وسجل الحوادث، وسجل الهجمات.

ويحوي سجل الأحداث معلومات عن أحداث حاسوبية تشمل الرزم والملفات والمعاملات الخاصة بها. وتقدم الحواسيب عادة جل السجلات كسجلات حاسوبية، من قبيل سجلات أوقات تسجيل الدخول وتواريخه، وكذلك المعلومات التي تقدَّم عندما يسجل المستخدمون دخولهم إلى نظام ما. وهذه السجلات الحاسوبية هي أمثلة صنفية على هذا السجل. ويمكن استخدام لغة CEE لوصف السجل.

ويحتوي سجل الحوادث على معلومات عن الحوادث الأمنية، ويوفر معلومات من قبيل الحالة الراهنة لأنظمة المستخدم ومخاطر أخرى. وهو مستمد من تحاليل سجلات الأحداث وما يخمَّن بشأنها، وهي سجلات تُنشأ تلقائياً أو يدوياً. فعلى سبيل المثال، عند اكتشاف نفاذ مفرط إلى حاسوب ما، ينبغي تسجيل حالة الحاسوب (نفاذ مفرط إلى الحاسوب) ونتائجها المتوقعة (الحرمان من الخدمة) في سجل الحوادث. ويمكن الحكم على ضرر الحادث وكذلك الحاجة إلى تدابير مضادة بناءً على هذا السجل؛ علماً بأن سجل الحوادث قد يسجل تسجيل حوادث غير حقيقية، أي حوادث مرشَّحة لا تُعتبر حوادث بعد التحقيق. ويمكن استخدام نسق تبادل وصف الكائن المتعلق بالحادث (IODEF) لوصف السجل.

ويحتوي سجل الهجمات على معلومات عن الهجمات تُستمد من تحليل سجلات الحوادث. فهو يصف تسلسل الهجوم؛ مثل كيف بدأ الهجوم، وأي جزء من موجودات تكنولوجيا المعلومات استهدف، وكيف تم انتشار الضرر الناجم عن الهجوم؛ علماً بأن السجل يحتاج إلى أن يوصَل بسجل الحوادث.

4.3.I قاعدة بيانات التحذيرات

تحتوي قاعدة بيانات التحذيرات على معلومات عن تحذيرات بشأن الأمن السيبراني. وقد صُممت هذه المعلومات إما للعموم أو لمنظمة معينة. وعادةً ما تحتوي تلك المُعدَّة لعامة الناس على معلومات إحصائية وتنبيهات في حين أن تلك المُعدَّة لمنظمة معينة تحتوي على نصائح أمنية على مقاس المنظمة. وتتولد المعلومات على أساس المعلومات الواردة في قاعدة بيانات الحوادث وقاعدة المعارف بالمخاطر المحدقة بالأمن السيبراني. ويعالج المنسق وفريق الاستجابة هذه المعلومات. وبناءً على التحذيرات، يمكن للمنظمات المستخدمة أن تنفذ تدابير مضادة ضد المخاطر المحدقة بالأمن السيبراني.

5.3.I قاعدة معارف المخاطر السيبرانية

تكتنز قاعدة معارف المخاطر السيبرانية معلومات عن المخاطر المحدقة بالأمن السيبراني. وهي معلومات يقدمها الباحث ومطور المنتجات والخدمات، ثم يقوم أمين السجل بتنظيمها وتصنيفها. وتتضمن قاعدة المعارف قاعدتي معارف نقاط الضعف والتهديدات.

قاعدة معارف نقاط الضعف: تكتنز قاعدة المعارف هذه المعلومات المعروفة عن نقاط الضعف والتي تشمل التسمية، والتصنيف، وتعداد نقاط الضعف المعروفة في البرمجيات والنظام. وتتضمن أيضاً معلومات عن نقاط الضعف البشرية، وهي نقاط الضعف التي يعاني منها المستخدمون البشريون لتكنولوجيا المعلومات. ومن الأمثلة العملية لقاعدة البيانات هذه: قاعدة البيانات الوطنية لنقاط الضعف (NVD) وقاعدة البيانات عن نقاط الضعف في المصادر المفتوحة (OSVDB)، ويمكن استخدام نسقي CVE وCWE لوصف محتويات قاعدة المعارف.

قاعدة معارف التهديدات: تكتنز قاعدة المعارف هذه المعلومات المعروفة عن التهديدات المحدقة بالأمن السيبراني. وهي تشمل قاعدتي معارف الهجمات وإساءة الاستخدام. فتكتنز قاعدة معارف الهجمات معلومات عن الهجمات مثل أنماط الهجمات وأدواتها (البرمجيات الخبيثة على سبيل المثال) واتجاهاتها. وتتضمن معلومات الاتجاه، على سبيل المثال، اتجاهات الهجمات الماضية من حيث الجغرافيا وأهداف الهجمات ومعلومات إحصائية عن الهجمات الماضية. ويمكن استخدام نسقي CAPEC وMAEC لوصف محتويات قاعدة المعارف.

وتكتنز قاعدة معارف إساءة الاستخدام معلومات عن سوء استخدام تُعزى إلى الاستخدام غير المناسب من جانب المستخدمين، سواء كان ذلك حميداً أو خبيثاً. ويشمل الاستخدام الحميد أخطاء الطباعة، وضعف التمييز الناجم عن كفاف البصر غير المقصود، وسوء الفهم، والوقوع في شراك التصيد. فيما يشمل الاستخدام الخبيث حالات عدم الامتثال من قبيل استخدام خدمة على نحو غير مصرح به والنفاذ إلى مواد غير ملائمة. لاحظ أن قاعدتي معارف الهجمات وإساءة الاستخدام حُذفتا من الشكل 7-1 بداعي التبسيط.

6.3.I قاعدة معارف التدابير المضادة

تكتنز قاعدة معارف التدابير المضادة معلومات عن التدابير المضادة لمخاطر الأمن السيبراني. وهي معلومات يقدمها الباحث ومطور المنتجات والخدمات، ثم يقوم أمين السجل بتنظيمها وتصنيفها. وتتضمن قاعدة المعارف قاعدتي معارف التقييم والكشف/الحماية.

قاعدة معارف التقييم: تكتنز قاعدة المعارف هذه القواعد والمعايير المعروفة لتقييم مستوى الأمن في موجودات تكنولوجيا المعلومات وقوائم مراجعة التشكيلات، والبرمجيات الاستدلالية، بما في ذلك الممارسات الفضلى. وتُعد صيغتا CVSS/CWSS من فضلى الممارسات في تقييم مستويات الأمن وتُكتنز في قاعدة المعارف هذه. وفيما عدا ذلك، يمكن استخدام نسقي XCCDF وOVAL لوصف القواعد وتقديم القوائم المرجعية.

قاعدة معارف التقييم والكشف/الحماية: تكتنز قاعدة المعارف هذه القواعد والمعايير المعروفة بشأن اكتشاف التهديدات الأمنية والحماية منها. كما تكتنز البرمجيات الاستدلالية، بما فيها الممارسات الفضلى.

7.3.I قاعدة معارف المنتجات والخدمات

تكتنز قاعدة معارف المنتجات والخدمات معلومات عن المنتجات والخدمات. وهي معلومات يقدمها الباحث ومطور المنتجات والخدمات، ثم يقوم أمين السجل بتنظيمها وتصنيفها. وتتضمن قاعدة المعارف هذه قاعدتي معارف الإصدارات والتشكيلات.

قاعدة معارف الإصدارات: تكتنز قاعدة المعارف هذه معلومات الإصدار على المنتجات والخدمات، والتي تشمل التسمية وتعداد الإصدارات الخاصة بها. وفيما يتعلق بالمنتج، ترد هنا أيضاً ترقيعات أمنية. ويمكن استخدام نسق CPE لتعداد المنصات المشتركة.

قاعدة معارف التشكيلات: تكتنز قاعدة المعارف هذه معلومات تشكيلة المنتجات والخدمات. وتتضمن تسمية التشكيلات المعروفة للمنتجات والخدمات وتصنيفها وتعدادها. وفيما يتعلق بتشكيلة الخدمة، فهي تتضمن أيضاً مبادئ توجيهية بشأن استخدامات الخدمة. ويمكن استخدام نسق CCE لتعداد التشكيلات الشائعة للمنتجات.

وترد معلومات أوفى عن هذه الأنطولوجيا في [b-Ontology] وفي التذييل II للتوصية [b-ITU-T X.1500].

التذييل II

مواصفات شرح قواعد البيانات وقواعد المعارف

(لا يمثل هذا التذييل جزءاً أساسياً من هذه التوصية)

تُشرح الأنماط السبعة من المعلومات التي تطرقت إليها الفقرة 7 بمجموعة من مواصفات الأمن السيبراني بما في ذلك المواصفات المتوافقة مع التوصية ITU-T X.1500 (مثل CVE وIODEF)، كما يتضح في الجدول I.1. وسيواكب مستوى تفاصيل المعلومات الأمن السيبراني المكتشفة مستوى تفاصيل المواصفات. وباستخدام هذا النهج، يكون مستوى التفاصيل مرناً بما يتيح إنشاء مواصفات متنوعة لأغراض محددة.

الجدول II.1 – المواصفات الداعمة للأنطولوجيا

الميادين	قواعد المعارف/قواعد البيانات		المواصفات
إدارة موجودات تكنولوجيا المعلومات	قاعدة بيانات موارد المستخدم		علامات ARF، AI، CVSS/CWSS
	قاعدة بيانات موارد المقدِّم		---
التعامل مع الحوادث	قاعدة بيانات الحوادث		CEE، IODEF
	قاعدة بيانات التحذيرات		IODEF
اكتناز المعرفة	قاعدة معارف المخاطر السيبرانية	قاعدة معارف نقاط الضعف	CVE، CWE، CVRF
		قاعدة معارف التهديدات	CAPEC، MAEC
	قاعدة معارف التدابير المضادة	قاعدة معارف التقييم	صيغة CVSS/CWSS
		قاعدة معارف الكشف/الحماية	OVAL، XCCDF
	قاعدة معارف المنتجات والخدمات	قاعدة معارف الإصدارات	CPE
		قاعدة معارف التشكيلات	CCE

التذييل III

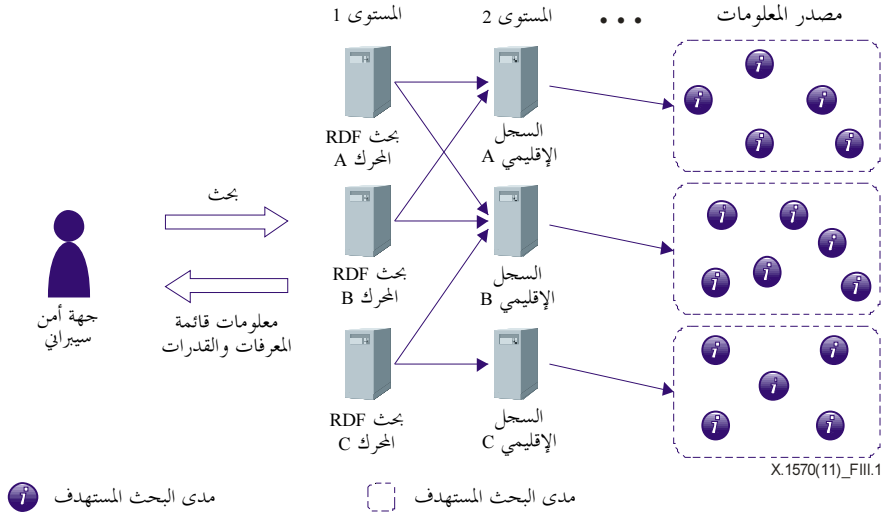
تنفيذ توضيحي للاكتشاف القائم على إطار وصف الموارد (RDF)

(لا يمثل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.III مثال تنفيذ للاكتشاف القائم على إطار وصف الموارد (RDF)

يصور الشكل 9-1 مفهوماً يمكن تنفيذه بجمع وكلاء الاكتشاف وكلاء السجل معاً ضمن محركات بحث إطار وصف الموارد. فترسل جهات الأمن السيبراني طلب اكتشاف إلى محرك بحث إطار وصف الموارد (RDF) الذي يجيب بقائمة الهويات وقدراتها؛ علماً أن لكل محرك بحث مصادر مختلفة تشكل المدى الذي يبحث فيه.

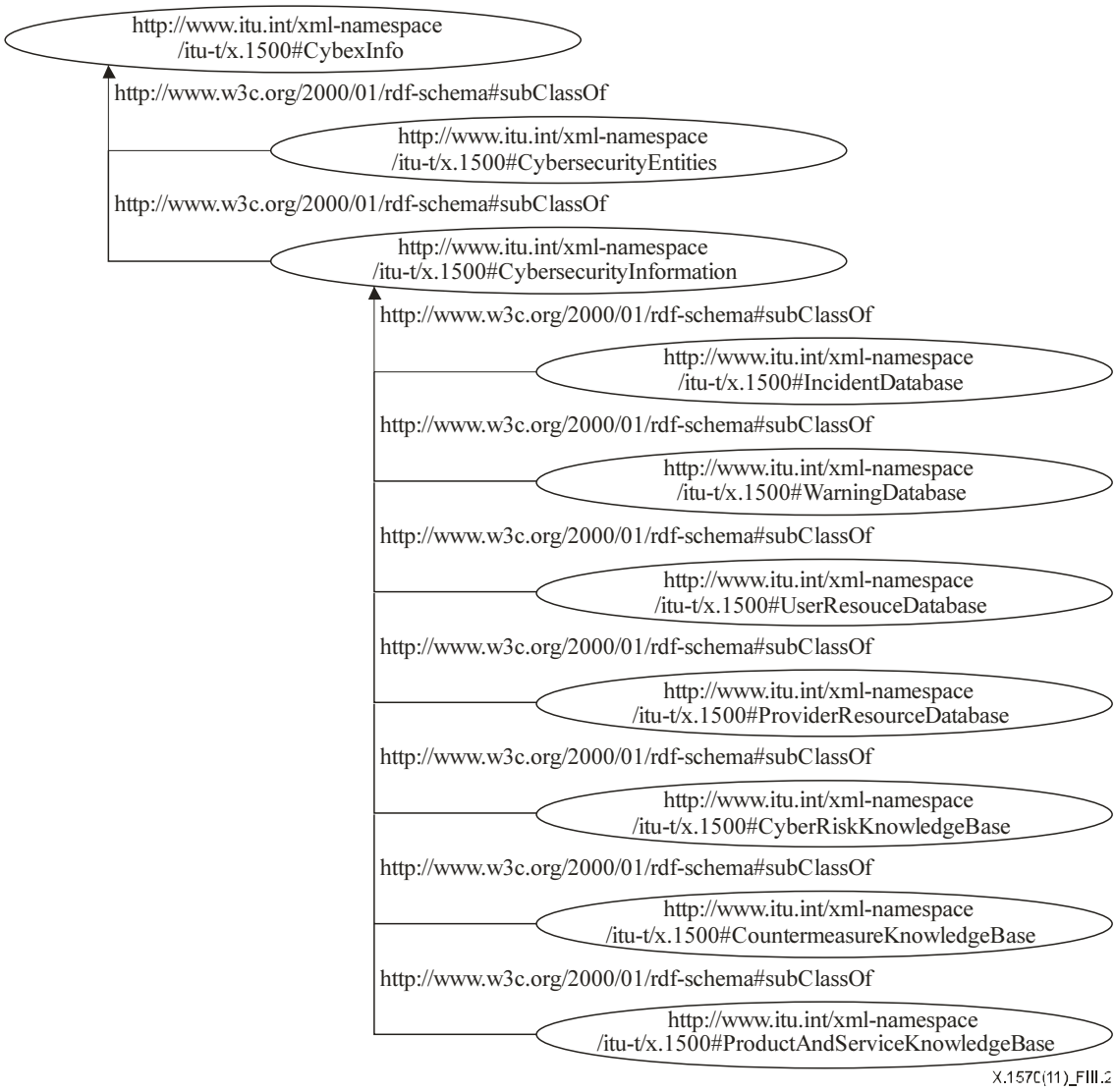
ولضمان قابلية التدرج القياسي في بيئة عملية، يمكن تسجيل المصدر وإدارته تراتبياً على النحو المبين في الشكل III-1. فيمكن للمستوى 1 أن يكون محرك بحث إطار وصف الموارد يعمل في الواقع كوكيل الاكتشاف. ويمكن للمستوى 2 أن يكون كياناً مسجلاً في إطار قواعد تشغيل سجل إقليمي من قبيل السجل الأمريكي لأرقام الإنترنت (ARIN) أو شبكات بروتوكول الإنترنت الأوروبية (RIPE) أو مركز معلومات شبكة آسيا والمحيط الهادئ (APNIC). ويمكن إدخال المزيد من التراتبية حسب التنفيذ. ويمكن أن يكون المصدر فريق الاستجابة للطوارئ الحاسوبية (CERT) أو أي جهة أمن سيبراني أخرى.



الشكل III.1 – تراتبية سجل المصدر

2.III تراتبية أصناف معلومات الأمن السيبراني

يظهر الشكل III-2 تراتبية أصناف آلية الاكتشاف. ويمثل كل صنف الفئة المقدمة في التذييل II للتوصية [b-ITU-T X.1500]. ويحال إلى التوصية لمزيد من التفاصيل عن كل فئة؛ علماً أن حيِّز أسماء XML الذي عرّفه قطاع تقييس الاتصالات هو المستخدم [b-ITU-T X.1500].



الشكل 2.III – تراتبية أصناف معلومات الأمن السيبراني

ملاحظة: يظهر استخدام **int.** في اسم الميدان ذي المستوى الأعلى كمثال في الشكل 3.III، وليس المقصود أن يُستخدم تشغيلياً.

وتشمل نعوت صنف الأمن السيبراني عادة النعوت التالية:

- entry_date: يخزّن تاريخ إدخال البيانات/تعديلها
- issuer_name: يخزّن اسم الجهة المصدرة (يمكن أن تكون الجهة المصدرة جهة خاصة أو اعتبارية)
- contact_email: يخزّن عنوان البريد الإلكتروني لطرف الاتصال
- resources: يخزّن المعرفات مثل عناوين مزيد من الموارد على شبكة الإنترنت
- Info_type: يخزّن نمط المعلومات مثل CVE و[b-CWSS] CWSS و[b-ITU-T X.1521] CVSS و[b–OVAL] OVAL و[b-SCAP] SCAP و[b-XCCDF] XCCDF و[b-CPE] CPE و[b-CCE] CCE و ARF.

ويمكن لأي طرف يسعى للحصول على معلومات الأمن السيبراني طلب البيانات في وحدة من أي صنف معين. ويمكن البحث عن المعلومات وفق معايير معينة تشمل اسم الصنف والنعت، وتاريخ ووقت آخر تعديل.

ويمكن إجراء تنفيذ اختباري لنظام الاكتشاف على شبكة الإنترنت، على الرابط: http://cybiet.sourceforge.net/.

ملاحظة – يكتشف التنفيذ معلومات الأمن السيبراني المهيكلة وفقاً للأنطولوجيا التي جاء وصفها في الشكل 7-1.

بيبليوغرافيا

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

[b-ITU-T X.1500.1] Recommendation ITU-T X.1500.1 (2012), *Procedures for the registration of arcs under the object identifier (OID) arc for 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-AI] NIST, *The Asset Identification.* <http://scap.nist.gov/specifications/ai/>

[b-ARF] *Assessment Results Format* <https://measurablesecurity.mitre.org/incubator/arf/>

[b-CCE] *Common Configuration Enumeration.* <https://cce.mitre.org/>

[b-CPE] *Common Platform Enumeration.* <https://cpe.mitre.org/>

[b-CWSS] *Common Weakness Scoring System.* <https://cwe.mitre.org/cwss/>

[b-Gruber] Gruber T.R. (1993), *Toward principles for the design of ontologies used for knowledge sharing*. International Journal of Human-Computer Studies, Vol. 43, Issues 4-5, November 1995, pp. 907-928.

[b-Ontology] Takahashi T., Kadobayashi Y., Fujiwara H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks (SIN), September 2010.

[b-OVAL] *Oval – Open Vulnerability and Assessment Language.* <https://oval.mitre.org/>

[b-SCAP] *Security Content Automation Protocol (SCAP).* <http://scap.nist.gov/>

[b-XCCDF] *XCCDF – The Extensible Configuration Checklist Description Format* <http://scap.nist.gov/specifications/xccdf/>

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، 2012