الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1217

(2021/01)

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

مبادئ توجيهية بشأن استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل شبكات الاتصالات

التوصية ITU-T X.1217

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
آمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
آمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
آمن البث المتعدد	X.1109–X.1100
آمن الشبكة المحلية	X.1119–X.1110
آمن الخدمات المتنقلة	X.1139–X.1120
آمن الويب	X.1149–X.1140
بروتوكولات الأمن (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
آمن معرفات الهوية عبر الشبكات	X.1179–X.1170
آمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
آمن 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
آمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
آمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
آمن إنترنت الأشياء (IoT)	X.1369–X.1360
آمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
آمن سجل الحسابات الموزع	X.1429–X.1400
آمن سجل الحسابات الموزع	X.1449–X.1430
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
آمن الحوسبة السحابية	
نظرة عامة على آمن الحوسبة السحابية	X.1601–X.1600
تصميم آمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن آمن الحوسبة السحابية	X.1659–X.1640
تنفيذ آمن الحوسبة السحابية	X.1679–X.1660
آمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار آمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم آمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات آمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
آمن البيانات	
آمن البيانات الضخمة	X.1759–X.1750
آمن شبكات الجيل الخامس	X.1819–X.1800

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

التوصية ITU-T X.1217

مبادئ توجيهية بشأن استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل شبكات الاتصالات

ملخص

إن المعلومات المتعلقة بالتهديدات، من وجهة نظر مشغل الاتصالات، هي مجموعة معلومات منظمة تم تحليلها وتنقيحها بشأن الهجمات الحالية والمحتملة التي قد تهدد منظمة ما. ويمكن أن تشمل هذه المعلومات أيضاً دوافع المهاجمين ونواياهم وخصائصهم وأساليبهم، إلى جانب طريقة عملهم أو تقنياتهم، وتكتيكاتهم وإجراءاتهم.

وفي مجال أمن الشبكات والمعلومات، أدى وقوع حوادث واسعة النطاق وغير متوقعة إلى نشوء حاجة ملحة إلى المعلومات المتعلقة بالتهديدات. فهذه المعلومات يمكنها أن تساعد المنظمة في الحد من المخاطر وتحسين أمنها العام. وجرى تعريف تصنيف موحد وقواعد وطريقة عرض للمعلومات المتعلقة بالتهديدات، بحيث يمكن تبادل هذه المعلومات بين المنظمات المختلفة.

وتحدد التوصية ITU-T X.1217 مبادئ توجيهية بشأن استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل شبكات الاتصالات، بعد تقديم تحليل عام.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1217	2021-01-07	17	11.1002/1000/14443

مصطلحات أساسية

الأمن، المعلومات المتعلقة بالتهديدات

* 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 "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" 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 2021

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

مقدمة

إن البيانات المتعلقة بالتهديدات، من وجهة نظر مشغل الاتصالات، هي مجموعة معلومات منظمة تم تحليلها وتنقيحها بشأن الهجمات الحالية والمحتملة التي قد تهدد منظمة ما. ويمكن أن تشمل هذه المعلومات أيضاً دوافع المهاجمين ونواياهم وخصائصهم وأساليبهم، إلى جانب طريقة عملهم أو تقنياتهم، وتكتيكاتهم وإجراءاتهم.

وفي مجال أمن الشبكات والمعلومات، أدى وقوع حوادث واسعة النطاق وغير متوقعة إلى نشوء حاجة ملحة إلى المعلومات المتعلقة بالتهديدات. فهذه المعلومات يمكنها أن تساعد المنظمة في الحد من المخاطر وتحسين أمنها العام من خلال فهم الكيانات التي من المرجح أن تكون مصدر الهجوم، وما هي أهدافها، ودوافعها، وكيف تعتزم القيام بذلك.

يعرّف المعيار [OASIS STIXv2] لغة ونسق التسلسل المستخدمين لتبادل معلومات التهديدات السيبرانية. ويحدد المعيار [OASIS TAXIIv2] بروتوكولاً يُستخدم لتبادل معلومات التهديدات السيبرانية عبر بروتوكول HTTPS. وتوضح التوصية [ITU-T X.1215] كيفية استخدام لغة التعبير المهيكل عن معلومات التهديدات (STIX) لدعم معلومات التهديدات السيبرانية وتبادلها.

وجرى تعريف تصنيف موحد وقواعد وطريقة عرض موحدة للمعلومات المتعلقة بالتهديدات، بحيث يمكن تبادل هذه المعلومات بين المنظمات المختلفة. والمشكلة التالية التي يجب أن تؤخذ بعين الاعتبار هي كيفية استخدام معلومات التهديدات لحل المشاكل الأمنية في الشبكة.

ويحدد المعيار [OASIS OpenC2-L] لغة الأوامر والتحكم (C2) للتحكم في وظائف الأمن السيبراني. ويحدد المعيار [OASIS OpenC2-H] سطحاً بينياً لبرمجة التطبيقات (API) للبروتوكول HTTPS لنقل أوامر اللغة OpenC2 إلى أجهزة الأمن السيبراني. ويحدد المعيار [OASIS OpenC2-P] استخدام اللغة OpenC2 للتحكم في جدران الحماية غير محددة الحالة. ويجري حالياً تطوير مواصفات وظائف الأمن السيبراني الأخرى في منظمة النهوض بمعايير المعلومات المهيكلة (OASIS).

وتحدد هذه التوصية المبادئ التوجيهية بشأن تطبيق المعلومات المتعلقة بالتهديدات بعد تقديم تحليل عام.

مبادئ توجيهية بشأن استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل شبكات الاتصالات

1 مجال التطبيق

تعرض هذه التوصية مبادئ توجيهية بشأن استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل شبكات الاتصالات بعد تقديم تحليل عام.

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.

[ITU-T X.1215] التوصية ITU-T X.1215 (2019)، *حالات الاستعمال المتعلقة بلغة التعبير المهيكل عن معلومات التهديدات*

[OASIS OpenC2-H] مواصفة المنظمة OASIS بشأن نقل الرسائل باللغة OpenC2 عبر البروتوكول HTTPS، الإصدار 1.0 للمواصفة <https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html>

[OASIS OpenC2-L] مواصفة منظمة OASIS بشأن لغة القيادة والتحكم المفتوحة (OpenC2) الإصدار 1.0 للمواصفة <https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs01/oc2ls-v1.0-cs01.html>

[OASIS OpenC2-P] مواصفة لغة القيادة والتحكم المفتوحة (OpenC2) لمنظمة OASIS من أجل ترشيح الرزم غير محددة الحالة، الإصدار 1.0 <https://docs.oasis-open.org/openc2/oc2slpf/v1.0/oc2slpf-v1.0.html>

[OASIS STIXv2] مواصفات OASIS STIX 2.1 <https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html>

[OASIS TAXIIv2] مواصفات OASIS TAXII 2.1 <https://docs.oasis-open.org/cti/taxii/v2.1/cs01/taxii-v2.1-cs01.html>

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

تَستعمل هذه التوصية المصطلحات التالية المعرّفة في مصادر أخرى:

1.1.3 شبكة برمجيات روبوتية (botnet) [b-ITU-T X.1231]: روبوتات برمجية خبيثة (برمجيات روبوتية) يتم التحكم فيها عن بُعد وتشغيلها بشكل مستقل أو أوتوماتي على حواسيب مخترقة جنباً إلى جنب مع مخدم التحكم والمراقبة الذي يملكه خبير البرمجية الروبوتية.

2.1.3 الاحتيال [b-ITU-T Y.140.1]: فعل الحصول على ميزة مالية عن طريق تحريف أو عمل غير مجاز.

3.1.3 البرمجيات الضارة [b-ITU-T X.1211]: برمجيات خبيثة مصممة خصيصاً لإلحاق الضرر بنظام أو تعطيله، مهاجمةً الكتمان و/أو السلامة و/أو التيسر.

4.1.3 التمويه [b-ITU-T X.1244]: محاولة للحصول بالإجرام والاحتيال على معلومات حساسة، مثل اسم المستعمِل وكلمات السر وتفاصيل حساباته المالية، عن طريق انتحال صفة كيان موثوق في الاتصالات الإلكترونية.

5.1.3 نقطة ضعف [b-ITU-T X.1524]: أي موطن ضعف في البرمجيات يمكن استغلاله لانتهاك حرمة نظام ما أو المعلومات التي يحتويها.

2.3 المصطلحات المعرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 تنقية البيانات: عملية تشمل حذف البيانات غير ذات الصلة والبيانات المكررة في مجموعة البيانات الأصلية، لتقليل أثر بيانات الضوضاء، ومعالجة القيم المفقودة والقيم المتطرفة.

2.2.3 تقليم البيانات: عملية تشمل تقليم البيانات عديمة الفائدة أو غير العادية.

3.2.3 إلغاء البيانات المكررة: عملية تشمل حذف البيانات المكررة في مجموعة البيانات الأصلية.

4.2.3 إزالة حساسية البيانات: عملية لإخفاء البيانات الحساسة.

5.2.3 ترشيح البيانات: عملية تشمل حذف البيانات غير ذات الصلة وترشيح البيانات غير المهمة في مجموعة البيانات الأصلية.

6.2.3 مقابلة البيانات: عملية تشمل إجراء تقابل بين عناصر البيانات في نظام بيانات المصدر مع البيانات في نظام بيانات المقصد.

7.2.3 دمج البيانات: عملية تشمل دمج سجلات البيانات المتماثلة في سجل واحد.

8.2.3 استخلاص البيانات: عملية حاسوبية لاكتشاف أنماط في مجموعات البيانات الكبيرة باستخدام أساليب الذكاء الاصطناعي وتعلم الآلة والإحصاءات وأنظمة قواعد البيانات.

9.2.3 الحد من الضوضاء في البيانات: عملية تشمل تقليل أثر بيانات الضوضاء.

10.2.3 اعتيان البيانات: تقنية إحصائية تستخدم لمعالجة القيم المفقودة والقيم المتطرفة.

11.2.3 تجزئة البيانات: عملية تشمل تجزئة البيانات من مستويات مختلفة.

12.2.3 فرز البيانات: عملية تشمل فرز البيانات حسب ترتيب معين أو فئة معينة.

13.2.3 تحويل البيانات: عملية تشمل تحويل البيانات إلى نسق معين ونقل البيانات إلى مدى محدد.

14.2.3 جمع الحوادث: عملية تشمل جمع البيانات عن الحوادث الأمنية.

15.2.3 إدراك الحالة: عملية تشمل عرض الوضع العام والتنبؤ بالتهديدات والهجمات المحتملة.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

API السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*

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

C&C القيادة والتحكم *(Command and Control)*

DDoS رفض الخدمة الموزّع *(Distributed Denial of Service)*

DNS نظام أسماء الميادين *(Domain Name System)*

FW جدار الحماية *(Firewall)*

GW بوابة *(Gateway)*

HTTPS بروتوكول نقل النصوص التشعبية المؤمن *(Hypertext Transfer Protocol Secure)*

ID هوية *(Identity)*

IDS نظام كشف التسلل *(Intrusion Detection System)*

IP بروتوكول الإنترنت *(Internet Protocol)*

MD5 الخوارزمية 5 لموجز الرسالة *(Message Digest Algorithm 5)*

IPS نظام منع التسلل *(Intrusion Prevention System)*

O&M التشغيل والصيانة *(Operations and Maintenance)*

SDN شبكة معرّفة بالبرمجيات *(Software Defined Network)*

SIEM إدارة المعلومات والأحداث الأمنية *(Security Information and Event Management)*

SoC مركز العمليات الأمنية *(Security Operation Centre)*

STIX لغة التعبير المهيكل عن معلومات التهديدات *(Structured Threat Information expression)*

TAXII التبادل المؤتمت الموثوق لمعلومات التحقيقات *(Trusted Automated exchange of Intelligence Information)*

URL محدِّد مواقع الموارد الموحَّد *(Uniform Resource Locator)*

WAF جدار حماية لتطبيق ويب *(Web Application Firewall)*

5 الاصطلاحات

يتعين فهم المصطلحات الأساسية التالية في هذه التوصية على النحو التالي:

"**يجب**" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

"**يوصى**" كلمة تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

"**يحظر**" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

"**من الجائز**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه التوصية في نفس الوقت.

6 نظرة عامة على المعلومات المتعلقة بالتهديدات

إن المعلومات المتعلقة بالتهديدات، من وجهة نظر مشغل الاتصالات، هي مجموعة معلومات منظمة تم تحليلها وتنقيحها بشأن الهجمات الحالية والمحتملة التي قد تهدد منظمة ما. ويمكن أن تشمل هذه المعلومات أيضاً دوافع المهاجمين ونواياهم وخصائصهم وأساليبهم، إلى جانب طريقة عملهم أو تقنياتهم، وتكتيكاتهم وإجراءاتهم.

وفي عملية تشغيل شبكات الاتصالات، فإن المعلومات المتعلقة بالتهديدات هي المعارف التي تُستخدم لمنع الهجمات السيبرانية أو التخفيف من حدتها بما في ذلك دوافع المهاجمين، ونواياهم، وخصائصهم، وأساليبهم، وطريقة عملهم، وتقنياتهم وتكتيكاتهم وإجراءاتهم. وهي غير مرتبطة بالمعلومات المحددة لهوية الأشخاص.

وفي مجال أمن الشبكات والمعلومات، أدى وقوع حوادث واسعة النطاق وغير متوقعة إلى نشوء حاجة ملحة إلى المعلومات المتعلقة بالتهديدات. فهذه المعلومات يمكنها أن تساعد المنظمة في الحد من المخاطر وتحسين أمنها العام من خلال فهم الكيانات التي من المرجح أن تكون مصدر الهجوم، وما هي أهدافها، ودوافعها، وكيف تعتزم القيام بذلك.

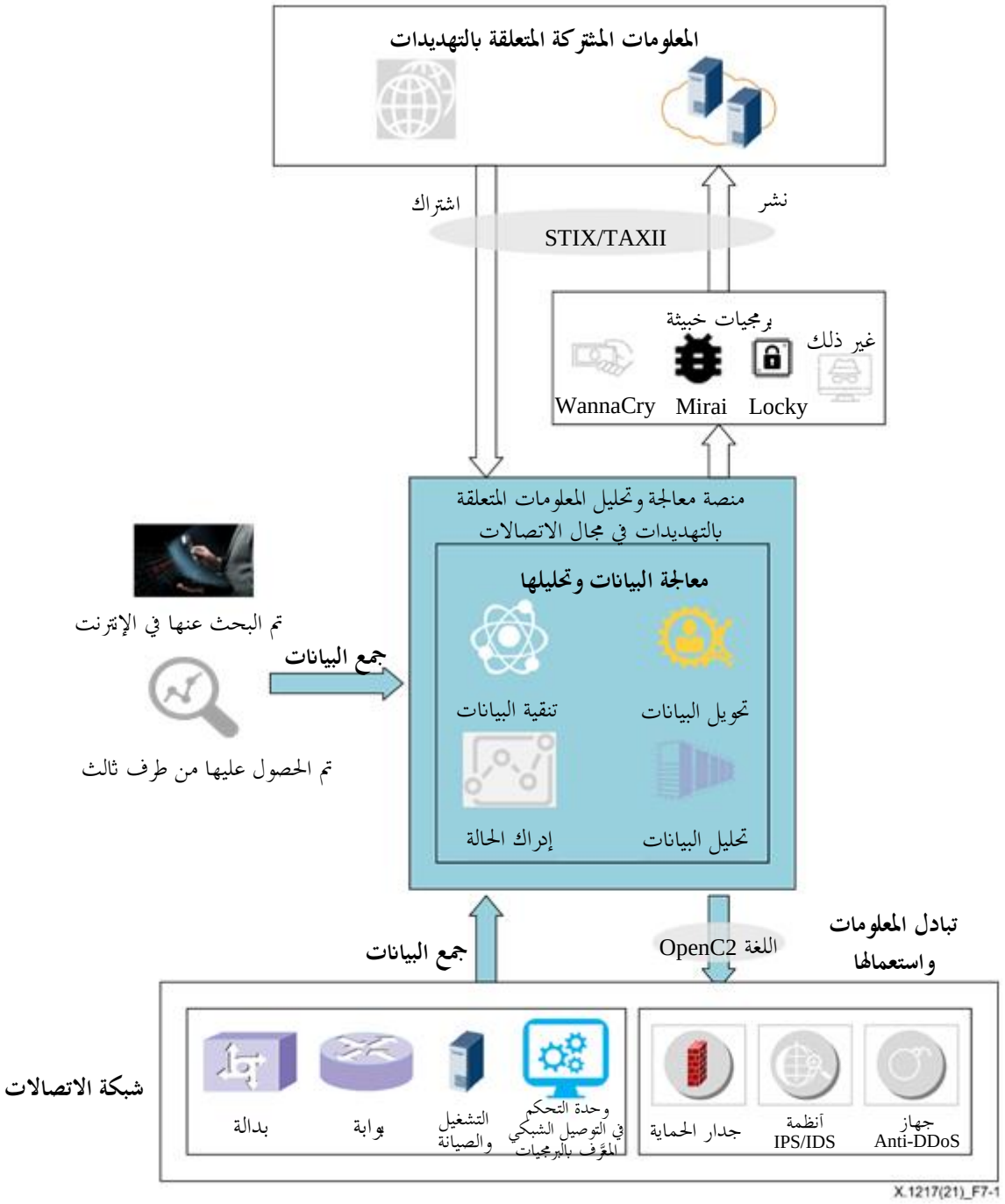
ويعرّف المعيار [OASIS STIXv2] لغة ونسق التسلسل المستخدمين لتبادل معلومات التهديدات السيبرانية. ويحدد المعيار [OASIS TAXIIv2] بروتوكولاً يُستخدم لتبادل معلومات التهديدات السيبرانية عبر البروتوكول HTTPS. وتبين التوصية [ITU-T X.1215] كيفية استخدام لغة التعبير المهيكل عن معلومات التهديدات (STIX) لدعم معلومات التهديدات السيبرانية وتبادلها.

وجرى تعريف تصنيف موحد وقواعد وطريقة عرض موحدة للمعلومات المتعلقة بالتهديدات، بحيث يمكن تبادل هذه المعلومات بين المنظمات المختلفة. والمشكلة التالية التي يجب أن تؤخذ بعين الاعتبار هي كيفية استخدام معلومات التهديدات لحل المشاكل الأمنية في الشبكة.

ويحدد المعيار [OASIS OpenC2-L] لغة القيادة والتحكم (C2) للتحكم في وظائف الأمن السيبراني. ويحدد المعيار [OASIS OpenC2-H] سطحاً بينياً لبرمجة تطبيقات البروتوكول HTTPS لنقل الأوامر باللغة OpenC2 إلى أجهزة الأمن السيبراني. ويحدد المعيار [OASIS OpenC2-P] استخدام اللغة OpenC2 للتحكم في جدران الحماية غير محددة الحالة. ويجري حالياً تطوير مواصفات وظائف الأمن السيبراني الأخرى في منظمة النهوض بمعايير المعلومات المهيكلة (OASIS).

7 نظرة عامة على استعمال المعلومات المتعلقة بالتهديدات السيبرانية في إطار تشغيل شبكات الاتصالات

يبين الشكل 7-1 كيفية استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل شبكات الاتصالات.



الشكل 7-1 استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل الشبكات

وفقاً للشكل 7-1، يشمل استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل شبكات الاتصالات ثلاث عمليات رئيسية هي: جمع البيانات، ومعالجة البيانات وتحليلها، وتبادل المعلومات واستعمالها.

1.7 جمع البيانات

هناك نوعان من مصادر بيانات المعلومات المتعلقة بالتهديدات:

- البيانات المستمدة من عناصر الشبكة الداخلية والأجهزة الأمنية.
- البيانات المستمدة من مصادر خارجية.

تتضمن البيانات المستمدة من عناصر الشبكة والأجهزة الأمنية الداخلية بشكل رئيسي السجلات والإنذارات والسياسات الأمنية مثل سجلات الحوادث وسجلات أنظمة أسماء الميادين (DNS) وسجلات جدران الحماية وما إلى ذلك.

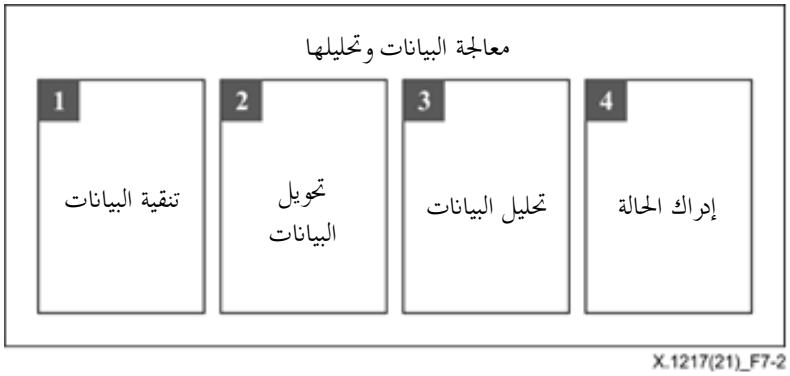
هناك بعض المصادر المحددة لجمع البيانات من الخارج، مثل البحث عنها عبر الإنترنت، والحصول عليها من أطراف ثالثة عن طريق التبادل المؤتمت الموثوق لمعلومات المؤشرات/ التعبير المهيكل عن معلومات التهديدات (STIX/TAXII)، وما إلى ذلك. وتتعلق البيانات المشتركة أساساً بعناوين بروتوكول الإنترنت، والميادين، وعناوين URL، والحوادث، ومواطن الضعف وغيرها.

ومن الضروري إزالة حساسية البيانات قبل جمعها.

2.7 معالجة البيانات وتحليلها

تشمل معالجة البيانات وتحليلها أربعة عناصر وظيفية هي: تنقية البيانات، وتحويل البيانات، وتحليل البيانات، وإدراك الحالة.

ويوضح الشكل 7-2 العناصر الوظيفية لمعالجة البيانات وتحليلها.



الشكل 7-2 العناصر الوظيفية لمعالجة البيانات وتحليلها

- تشمل تنقية البيانات حذف البيانات غير ذات الصلة والبيانات المكررة في مجموعة البيانات الأصلية، وتقليل أثر بيانات الضوضاء ومعالجة القيم المفقودة والقيم المتطرفة.
- يشمل تحويل البيانات تكامل البيانات وتقييسها.
  - يشمل تكامل البيانات توحيد تخزين مصادر البيانات المتعددة في نسق معين.
  - يشمل تقييس البيانات إزالة التأثير الناجم عن بعد ومدى القيم بين المؤشرات ونقل البيانات إلى مدى معين، بما في ذلك تحويل الوظائف وبناء النعوت وغير ذلك.
- يستخدم تحليل البيانات خوارزميات مختلفة لتحليل البيانات واستخراج الكلمات الرئيسية، والقواعد الواضحة، وربط التحليلات للحصول على المعلومات المتعلقة بالتهديديات، وتحليل التدابير المضادة المقابلة.
- يشمل إدراك الحالة التصور والتحذير التنبؤي.
  - التصور هو عرض مرئي للحالة العامة من خلال البيانات التي تم تحليلها، مثل التصنيف والفرز وما إلى ذلك.
  - يشير التحذير التنبؤي إلى التنبؤ بالمدى المحتمل للتهديدات ومسارات الهجوم، وأساليب الهجوم، وما إلى ذلك من خلال تحليل البيانات والوضع العام، وإصدار إنذارات مبكرة لتوفير استراتيجيات أمنية للدفاع ضد الهجمات المحتملة.

3.7 تبادل المعلومات واستعمالها

يشمل تبادل المعلومات واستعمالها جانبين:

- وفقاً للمعلومات المتعلقة بالتهديدات، يمكن لمديري التشغيل والصيانة تطبيق السياسات الأمنية على عناصر الشبكة والأجهزة الأمنية.
- يمكن تبادل المعلومات المتعلقة بالتهديدات مع أطراف ثالثة.

وتشمل المعلومات المتعلقة بالتهديدات التي يمكن تبادلها واستعمالها في إطار تشغيل شبكات الاتصالات، المعلومات المتعلقة بالتهديدات، ومعلومات التحذير التنبؤي، والتدابير المضادة المتعلقة بأمن الشبكة وما إلى ذلك.

وتشمل أغراض تبادل المعلومات المتعلقة بالتهديدات واستعمالها في إطار تشغيل شبكات الاتصالات عناصر الشبكة والأجهزة الأمنية مثل نظام كشف التسلل (IDS) ونظام منع التسلل (IPS)، وجدران الحماية، والأجهزة anti-DDoS. وفيما يتعلق بتطبيق وظائف القيادة والتحكم الأمنية على الأجهزة الأمنية، يوصى باستخدام مواصفات اللغة OASIS OpenC2.

والهدف من المعلومات المتعلقة بالتهديدات واستعمالها في إطار تشغيل شبكات الاتصالات هو منع الحوادث الأمنية وتقليلها وفي الوقت نفسه تحقيق استجابة سريعة وفعالة لكل حادث أمني في شبكة الاتصالات.

8 المبادئ التوجيهية بشأن استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل الشبكات

تصف الفقرة 7 العمليات الرئيسية الثلاث المتمثلة في جمع البيانات ومعالجة البيانات وتحليلها وتبادل المعلومات واستعمالها من أجل استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل شبكات الاتصالات. وتُحدد الفقرات من 1.8 إلى 3.8 المبادئ التوجيهية بشأن استعمال المعلومات المتعلقة بالتهديدات في إطار تشغيل الشبكات.

1.8 جمع البيانات

جمع البيانات شرط مسبق لاستعمال المعلومات المتعلقة بالتهديدات، والغرض هو جمع كل المعلومات والبيانات المتعلقة بالتهديدات. ويوصى بأن تتضمن هذه البيانات بيانات مستمدة من عناصر الشبكة والأجهزة الأمنية الداخلية مثل السجلات، والإنذارات، والسياسات الأمنية. وفي الوقت نفسه، يوصى بأن تتضمن البيانات بيانات مستمدة من مصادر خارجية، مثل البيانات التي يتم البحث عنها عبر الإنترنت، والبيانات التي يتم الحصول عليها من أطراف ثالثة وغيرها. وتشمل البيانات المتبادلة أساساً عناوين بروتوكول الإنترنت، والميادين وعناوين URL والحوادث ومواطن الضعف وما إلى ذلك.

ومن المستحسن أن يُنفذ جمع البيانات بفعالية خاصة فيما يتعلق بسجلات الأنظمة SDN وسجلات جدار الحماية وما إلى ذلك. ويوصى بجمع البيانات بشأن الحوادث الأمنية. ويوصى بجمع المعلومات الحرجة مثل عناوين بروتوكول الإنترنت، والميادين، وعناوين URL والحوادث ومواطن الضعف وما إلى ذلك.

وإذا كانت البيانات مجمعة من عناصر الشبكة والأجهزة الأمنية الداخلية، يمكن تنفيذ عملية جمع البيانات وفقاً لأنماطها المختلفة مثل المعلومات المتعلقة بالحوادث أو أنشطة الشبكات الروبوتية.

ويمكن جمع المعلومات بشأن الحوادث من الأجهزة IDS أو IPS، وجدار حماية تطبيقات الويب (WAF)، وأجهزة anti-DDoS، ومنصة إدارة المعلومات والأحداث الأمنية (SIEM) ومنصة مركز العمليات الأمنية (SoC). ويوصى بأن تشمل المعلومات المجمعة المتعلقة بالحوادث اسم ووصف وفئة الحادث والأصول المتضررة. ويوصى بتضمين الوقت الذي يقع فيه الحادث. ويمكن جمع معلومات بشأن أنشطة الشبكات الروبوتية من أجهزة DNS وIDS وجدار WAF، والأجهزة anti-DDoS، وما إلى ذلك. ويوصى بتضمين معلومات أنشطة الشبكات الروبوتية المجمعة الاسم والوصف والفئة والأصول المتضررة الخاصة من نشاط الشبكات الروبوتية. ويوصى أيضاً بتضمين الوقت الذي يحدث فيه نشاط الشبكة الروبوتية.

وإذا كانت البيانات مجمعة من الإنترنت، يمكن تنفيذ جمع البيانات وفقاً لأنماطها المختلفة مثل المعلومات المتعلقة بمواطن الضعف، والميادين الخبيثة، وعناوين URL الخبيثة، وعناوين بروتوكول الإنترنت الخبيثة، والمعلومات المتعلقة بالحوادث وما إلى ذلك.

ويمكن جمع المعلومات المتعلقة بمواطن الضعف من المواقع الإلكترونية الخاصة بمواطن الضعف، مثل مواقع الويب المخصصة لمواطن الضعف والتعرض الشائعة (CVE). ويوصى بأن تتضمن المعلومات المجمعة المتعلقة بمواطن الضعف هوية موطن الضعف واسمه ووصفه ونوعه فضلاً عن الإصدارات المتضررة والبائعين المتضررين والمنتجات المتضررة بموطن الضعف هذا وغيرها من المعلومات.

ويمكن تصنيف المعلومات المتعلقة بميادين وعناوين URL الخبيثة على أنها أنواع مختلفة من التهديدات الخاصة بالقيادة والتحكم (C&C)، والشبكات الروبوتية، والبرمجيات الخبيثة، وشفرة حصان طروادة، والتصيد الاحتيالي، والاحتيال وغير ذلك. ويمكن جمع

المعلومات المتعلقة بالميادين وعناوين URL الخبيثة من المواقع الإلكترونية وتقارير البائعين وتقارير الأمن التي تعدّها أطراف ثالثة وما إلى ذلك. ويوصى بأن تتضمن هذه المعلومات المجمعة مخدم اسم الميدان، ونوع النظام DNS، ونوع التهديد، ومستوى المصداقية وما إلى ذلك.

يمكن جمع المعلومات المتعلقة بعناوين بروتوكول الإنترنت الخبيثة من مختلف المواقع الإلكترونية وبعض البائعين وشركات الأمن وغيرها. ويمكن تصنيف عناوين بروتوكول الإنترنت الخبيثة على أنها أنواع مختلفة من تهديدات رفض الخدمة الموزع، والاستغلال، ومصدر الرسائل الاقتحامية، والهجوم عن طريق الويب، والشبكة الروبوتية، والبرمجيات الخبيثة، والقيادة والتحكم وما إلى ذلك. ويوصى بأن تتضمن معلومات عناوين بروتوكول الإنترنت الخبيثة المجمعة عنوان بروتوكول الإنترنت ونوع التهديد ومستوى المصداقية وما إلى ذلك.

ويمكن جمع المعلومات المتعلقة بالحوادث من الأخبار الأمنية أو تقارير البائعين. ويوصى بأن تتضمن هذه المعلومات المجمعة الاسم والوصف والفئة والأصول المتضررة من الحادث.

وتتضمن البيانات التي يتم الحصول عليها من أطراف ثالثة بشكل رئيسي عناوين بروتوكول الإنترنت، وأسماء الميادين، وعناوين URL، والحوادث ومواطن الضعف وما إلى ذلك. وبالنسبة لكل فئة من هذه الفئات، تكون المعلومات مطابقة للمعلومات الواردة أعلاه.

ويوصى بأن يُنفذ تجميع البيانات بواسطة أدوات أو برامج نصية مؤتمتة عند جمع البيانات من عناصر الشبكة والأجهزة الأمنية الداخلية. ويوصى باستخدام النصوص أو آليات تبادل وتقاسم البيانات عند جمع البيانات من مصادر خارجية. ويوصى في المعالجة اللاحقة للبيانات المجمعة، باتباع النسق المعياري المعرف في المعيارين [OASIS STIXv2] و[OASIS TAXIIv2]. وفيما يتعلق بالمعلومات المتبادلة المتعلقة بالتهديدات، يوصى عند جمع البيانات، باتباع النسق المعياري المعرف في المعيارين [OASIS STIXv2] و[OASIS TAXIIv2].

ويوصى بإزالة حساسية البيانات قبل جمع البيانات، حيث إن إزالة حساسية البيانات هي عملية إخفاء البيانات الأصلية الحساسة باستخدام رموز أو بيانات من أجل حماية البيانات الحساسة.

2.8 معالجة البيانات وتحليلها

1.2.8 تنقية البيانات

تنقية البيانات هي إحدى الخطوات الرئيسية لاستعمال المعلومات المتعلقة بالتهديدات، وترمي إلى تنقية البيانات المجمعة وجعلها منتظمة ومفيدة وإعدادها لمرحلتي التحويل والتحليل.

- يوصى بتنفيذ ترشيح للبيانات، وتقليل أثر ضوضاء البيانات والتخلص من البيانات المكررة.
- يوصى بتنفيذ ترشيح البيانات أي حذف البيانات غير ذات الصلة وترشيح البيانات التي غير المهمة في مجموعة البيانات الأصلية.
- يوصى بتقليل أثر ضوضاء البيانات وحذف البيانات المكررة لتقليل أثر بيانات الضوضاء وحذف البيانات المكررة في مجموعة البيانات الأصلية.

وبما أن البيانات المجمعة تحتوي على أنواع مختلفة من البيانات مثل عناوين بروتوكول الإنترنت، والميادين، وعناوين URL، والحوادث ومواطن الضعف وما إلى ذلك، يمكن لعملية تنقية البيانات المجمعة أن تختلف وفقاً للبيانات المجمعة.

تشمل عملية إزالة البيانات المكررة أساساً حذف البيانات المكررة لتوفير حيز التخزين. وتختلف المعايير باختلاف نوع البيانات. وبالنسبة لبيانات المعلومات المتعلقة بعناوين بروتوكول الإنترنت، إذا كان عنوان بروتوكول الإنترنت هو نفسه وأجزاء أخرى من السجل مثل نوع التهديد ومستوى المصداقية هي نفسها، تعتبر هذه البيانات بيانات مكررة ويتعين حذفها وإلا فإنها تحتاج إلى الدمج. أما بالنسبة للمعلومات المتعلقة بالميادين، إذا كانت جميع السجلات المتعلقة بمخدم اسم الميدان ونوع النظام DNS ونوع التهديد ومستوى المصداقية هي نفسها، تعتبر هذه البيانات بيانات مكررة ويتعين حذفها وإلا فإنها تحتاج إلى الدمج. وبالنسبة للمعلومات المتعلقة بمواطن الضعف، إذا كانت هوية موطن الضعف هي نفسها، تعتبر هذه البيانات بيانات مكررة ويتعين حذفها. وبالنسبة لأنواع البيانات الأخرى، يوصى بحساب نسبة التشابه، وإذا كانت أعلى من العتبة المحددة، يجب حذف البيانات المكررة.

ويوصى بدمج المعلومات المتماثلة في سجل واحد. وبالنسبة للمعلومات المتعلقة بعناوين بروتوكول الإنترنت، والميادين، وعناوين URL والمعلومات المتعلقة بالحوادث، إذا كانت عناوين بروتوكول الإنترنت ومخدم اسم الميدان وعناوين URL ووصف الحادث هي نفسها، عندئذ، يمكن دمجها في سجل واحد. وبالنسبة لأنواع البيانات الأخرى، يمكن حساب نسبة التشابه. وإذا كانت نسبة التشابه ضمن العتبة المحددة، تحتاج المعلومات إلى الدمج.

- يوصى بتنفيذ اعتيان البيانات، ودمج البيانات وفرز البيانات لمعالجة القيم المفقودة والقيم المتطرفة وجعل البيانات أكثر فائدة للعملية اللاحقة.
- يوصى باستخدام أدوات مؤتمتة لترشيح البيانات وإزالة البيانات المكررة.

2.2.8 تحويل البيانات

تشمل عملية تحويل البيانات إزالة التأثير الناجم عن بعد ومدى القيم بين المؤشرات ونقل البيانات إلى مدى معين، بما في ذلك تحويل الوظائف وبناء النعوت وما إلى ذلك، وتحويل البيانات النظيفة إلى نسق موحد من أجل إعدادها للتحليل.

لتنفيذ تحويل البيانات، يوصى باستعمال تقابل البينات، وتقليم البيانات، وتجزئة البيانات لجعل البيانات ذات قيمة مفيدة. وعند اختلاف الهجاء، يوصى بتحويل الهجاءات المختلفة إلى هجاء موحد. ويوصى بتوحيد نسق البيانات المستمدة من مصادر متعددة في نسق معين. ويوصى بتحقيق التقارب بين البيانات المستمدة من مصادر متعددة لتخزينها بطريقة موحدة.

وتكون إجراءات التحويل لكل نوع من أنواع معلومات عناوين بروتوكول الإنترنت، والميادين، وعناوين URL ومواطن الضعف متشابهة. ويوصى باتباع قواعد تقابل البيانات لكل نوع من أنواع البيانات، التي قد باختلاف نوع البيانات. فعلى سبيل المثال، تتمثل قاعدة تقابل البيانات بالنسبة للمعلومات المتعلقة بالحوادث في استخدام نسق موحد للاسم والوصف والفئة والأصول المتضررة. ويوصى بتقابل المعلومات المتعلقة بجدران الحماية مثل تقابل الخاتم الزمني، وطلب العنوان URL، واسم المضيف، ونوع الهجوم، ومحتوى الهجوم في النسق المحدد.

وبالنسبة لتقليم البيانات وتجزئة البيانات، يوصى بتنفيذ عملية تحويل البيانات باستخدام أدوات مؤتمتة. وفيما يتعلق بتحويل الهجاء، يوصى بتحويل البيانات باستخدام أدوات مؤتمتة. وبالنسبة لتوحيد النسق، يوصى بتحويل البيانات، باعتماد النسق الموحد المحدد في المعيارين [OASIS STIXv2] و[OASIS TAXIIv2].

3.2.8 تحليل البيانات

يمثل تحليل البيانات الخطوة الحاسمة في استعمال المعلومات المتعلقة بالتهديدات وينطوي على استعمال خوارزميات مختلفة لتحليل البيانات المحولة، واستخراج كلمات رئيسية وقواعد واضحة، وتحليل الترابط وما إلى ذلك، للحصول على معلومات عن التهديدات وتحليل التدابير المضادة المقابلة.

ولتحليل البيانات، يوصى باسترجاع البيانات واستخلاصها للحصول على المعلومات الأساسية عن التهديدات وبالتالي إصدار إنذارات أو تحديد التدابير المضادة المقابلة. ويوصى بإجراء تحليل سلوكي وتحليل الترابط بين الحوادث من أجل تحديد المعلومات المفيدة عن التهديدات مثل عناوين بروتوكول الإنترنت، وأسماء الميادين، وخلاصة الاختزال ومعلومات عن المهاجم والإجراءات التي يتعين اتخاذها وما إلى ذلك. ويوصى بإجراء تقابل للمعارف والتقاط التهديدات للحصول على المعلومات الأساسية بشأن التهديدات واتخاذ التدابير مضادة والاستجابة لها.

فعلى سبيل المثال، يمكن استعمال خوارزمية تعلم الآلة من أجل سجلات النظام DNS للكشف عن وظائف القيادة والتحكم للشبكات الروبوتية. ويوصى باستخدام سجلات جدران الحماية جنباً إلى جنب مع مصدر التهديد ونوع التهديد ووقت الهجوم ومعلومات أخرى استخداماً مشتركاً لحساب مستوى التهديد. ويمكن استخدام المعلومات المتعلقة بالعناوين URL وعناوين بروتوكول الإنترنت لحساب مستوى السمعة.

ويوصى باستخدام خوارزميات تحليل البيانات بشكل تلقائي. ويوصى بأن تتبع نتائج تحليل البيانات النسق الموحد المحدد في المعيارين [OASIS STIXv2] و[OASIS TAXIIv2].

4.2.8 إدراك الحالة

يستخدم إدراك الحالة البيانات التي تم تحليلها لعمل تنبؤات وإنذارات بالاتجاهات وفي الوقت نفسه عرض الحالة العامة.

ولتحقيق إدراك الحالة، يوصى بتصور الحالة لعرضها بالكامل من خلال البيانات التي تم تحليلها. ويوصى بالتنبؤ بالاتجاهات والإبلاغ عنها لتوقع المدى المحتمل للتهديدات، ومسارات الهجوم، وأساليب الهجوم وما إلى ذلك من خلال تحليل البيانات والحالة العامة، وإصدار إنذارات مبكرة لتوفير استراتيجيات أمنية للدفاع ضد الهجمات المحتملة. وتعتمد طريقة إدراك الحالة على الخوارزميات مثل تعلم الآلة، والتحليل الخطي، وإحصاءات الاحتمال، والذكاء الاصطناعي.

ويوصى بالتنبؤ بالاتجاهات وإصدار الإنذارات بشكل تلقائي. ويوصى بأن تتبع نتائج التنبؤ والإنذار بشأن الاتجاهات النسق الموحد المحدد في المعيارين [OASIS STIXv2] و[OASIS TAXIIv2]. وبالنسبة لتصور الحالة وعرضها، يوصى بعرض الحالة العامة للبيانات باستخدام أدوات التصور.

3.8 تبادل المعلومات واستعمالها

الغرض من تبادل واستعمال المعلومات المتعلقة بالتهديدات منع وقوع الحوادث الأمنية والتقليل منها والاستجابة بسرعة وكفاءة كلما وقع حادث أمني في شبكة الاتصالات.

ويمكن لمختلف دوائر ومجتمعات مشغلي الاتصالات تبادل المعلومات التي يتم الحصول عليها من مرحلة معالجة البيانات وتحليلها، بما في ذلك المعلومات المتعلقة بالتهديدات، ومعلومات الإنذار التنبؤية، والتدابير المضادة المتعلقة بأمن الشبكات، والسياسات الأمنية، وغيرها. ويمكن تبادل المعلومات بأشكال مختلفة. فعلى سبيل المثال، يمكن تبادلها في شكل تقارير واستشارات. ويمكن أيضاً تبادلها في شكل مؤشرات للكشف.

ويوصى بالحصول على المعلومات من عناصر الشبكة، والأجهزة الأمنية ومراكز الإنذار وما إلى ذلك. ويمكن أن يقوم مديرو التشغيل والصيانة بوضع سياسات أمنية استناداً إلى المعلومات التي يتم الحصول عليها وتطبيقها على عناصر الشبكة والأجهزة الأمنية. ويمكنهم أيضاً تحديث إصدارات البرمجيات وتعديل تشكيلة عناصر الشبكة والأجهزة الأمنية حسب الحاجة.

ويوصى باستخدام المعلومات من نمط العناوين URL للبوابات، التي يمكنها بدورها تحديث السياسة الأمنية الخاصة بها عن طريق ترشيح العناوين URL الخبيثة إلى القائمة السوداء. ويوصى أيضاً باستخدام هذه المعلومات من أجل الأنظمة IDS أو IPS عن طريق تحديث قواعد الحماية باستخدام العناوين URL المقابلة.

ويوصى باستخدام المعلومات من نمط الميادين الخبيثة من أجل المخدمات DNS، التي يمكنها تحديث التشكيلة عن طريق وضع الميادين الخبيثة في القائمة السوداء.

ويوصى باستخدام المعلومات من نمط عناوين بروتوكول الإنترنت الخبيثة من أجل جدران الحماية التي يمكنها بدورها تحديث السياسة الأمنية الخاصة بها عن طريق ترشيح عناوين IP الخبيثة. ويمكن استخدام هذه المعلومات أيضاً للأنظمة IDS أو IPS عن طريق تحديث قواعد الحماية باستخدام العناوين URL المقابلة.

ويوصى باستخدام المعلومات من نمط مواطن الضعف لعناصر الشبكة التي يمكنها إزالة مواطن الضعف من خلال تحديث البرمجيات والعتاد. وبالإضافة إلى ذلك، يمكن استخدام هذه المعلومات، بصورة اختيارية، لإنشاء وحدات الكشف واستخدامها فيما بعد لتحديث ماسح الكشف. ويمكن استخدام هذه المعلومات أيضاً بصورة اختيارية في أنظمة الاستجابة للطوارئ لتحديد الحوادث والمساعدة في اتخاذ إجراءات لمنع الهجمات.

ويوصى بأن تتبع المعلومات النسق الموحد المحدد في المعيارين [OASIS STIXv2] و[OASIS TAXIIv2]. ويوصى باستعمال المواصفات OpenC2 للمنظمة OASIS من أجل وظائف القيادة والتحكم المتصلة بالأمن.

بيبليوغرافيا

[b-ITU-T X.1211] Recommendation ITU-T X.1211 (2014), *Techniques for preventing web-based attacks*.

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

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

[b-ITU-T Y.140.1] Recommendation ITU-T Y.140.1 (2004), *Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication services*.

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، 2021