الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1546

(2014/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – نظرة عامة على أمن الحوسبة السحابية

تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها

التوصيـــة ITU-T X.1546

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 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.

تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها

ملخص

تتضمن لغة تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها (MAEC) تعدادات نعوت البرمجيات الخبيثة ومظاهر سلوكها لتوفير مصطلحات مشتركة. وتكون هذه التعدادات على مستويات مختلفة من التجريد: أحداث قابلة للملاحظة في المستوى المنخفض، ومظاهر سلوك في المستوى المتوسط، وتصنيفات رفيعة المستوى. والتوصية ITU-T X.1546، التي تعتبر الإصدار الأولي للغة MAEC، تركز على إنشاء تعداد نعوت البرمجيات الخبيثة منخفضة المستوى، وتستفيد من الحالات القليلة للعمل المماثل الذي أُنجز من قبل في هذا المجال. وبالتالي فهي قادرة أولاً على تحديد خصائص أكثر أنواع البرمجيات الخبيثة شيوعاً، بما فيها الفيروسات المتخفية (أحصنة طروادة) والديدان وبرمجيات الحزم الجذرية، علماً بأنه يمكن تطبيقها في نهاية الأمر على أنواع أكثر تخفياً من البرمجيات الخبيثة.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1546	2014-01-24	17	11.1002/1000/12038

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان بمتصفح الويب الخاص بك، متبوعاً بمعرف الهوية الفريد للتوصية. على سبيل المثال، http://handle.itu.int/11.1002/1000/11830-en.

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/.

جدول المحتويات

الصفحة

مقدمة

التوصية ITU-T X.1546 بشأن استعمال تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها (MAEC) هي معيار دولي لمجتمع أمن المعلومات يرمي إلى النهوض بمحتوى أمني مفتوح ومتاح للجمهور بشأن البرمجيات الخبيثة ومظاهر سلوكها. وتهدف هذه التوصية إلى تقييس نقل هذه المعلومات عبر كل أنواع أدوات الأمن وخدماته التي يمكن استعمالها لرصد وإدارة عمليات الدفاع ضد البرمجيات الخبيثة. واللغة MAEC هي لغة تُستخدم لتشفير تفاصيل ذات صلة بالبرمجيات الخبيثة.

وترمي لغة MAEC إلى ما يلي: 1) تحسين التواصل فيما بين البشر، وبين الإنسان والآلة، وفيما بين الآلات، وبين الآلة والإنسان، بشأن البرمجيات الخبيثة، و2) الحد من التكرار المحتمل للجهود التي قام بها الباحثون بشأن تحليل البرمجيات الخبيثة، و3) إتاحة إمكانية وضع التدابير المضادة بسرعة بتوفير إمكانية الاستفادة من الاستجابات لحالات البرمجيات الخبيثة التي رصدت من قبل. ويعد تحليل التهديدات وكشف الاقتحامات وإدارة الحوادث من العمليات التي تعالج جميع المسائل المتعلقة بالتهديدات السيبرانية. وتوفر لغة MAEC، من خلال تشفيرها الموحد لنعوت البرمجيات الخبيثة، نسقاً موحداً لإدراج المعلومات العملية عن البرمجيات الخبيثة في هذه العمليات.

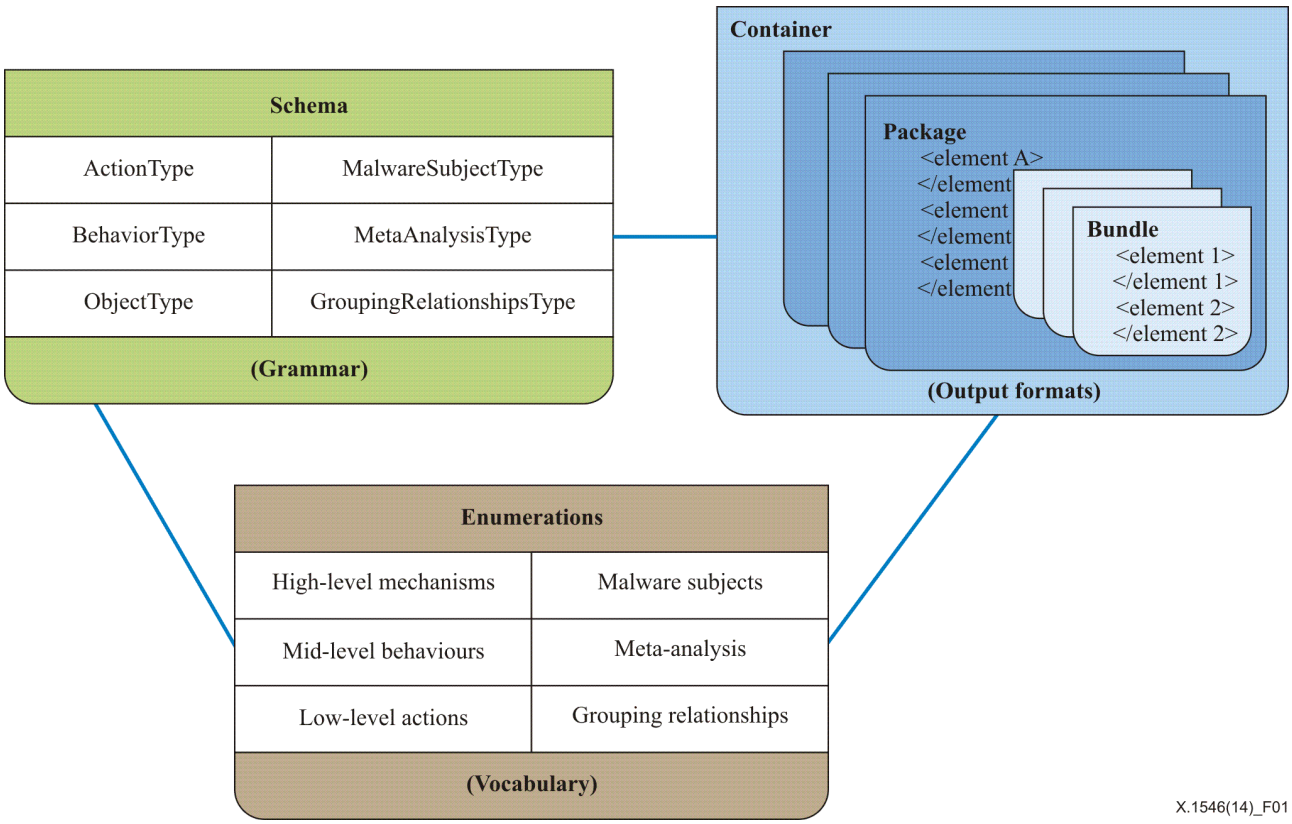
لقد وجدت البرمجيات الخبيثة بشكل أو بآخر منذ ظهور أول فيروس للحاسوب المكتبي في عام 1971. وهي حالياً مسؤولة عن استضافة أنشطة خبيثة تتراوح بين توزيع السواد الأعظم من الرسائل الإلكترونية الاقتحامية عبر الشبكات الروبوتية، وسرقة المعلومات الحساسة عن طريق هجمات التحايل الاجتماعي المحددة الأهداف. والبرمجيات الخبيثة، التي هي فعلياً وكيل مستقل ذاتياً يعمل بالنيابة عن المهاجم، قادرة على القيام بأي عمل يمكن التعبير عنه بشكل شفرة، وهي تشكل بالتالي تهديداً خطيراً للأمن السيبراني.

لذلك تعد حماية الأنظمة الحاسوبية من البرمجيات الخبيثة حالياً أحد أهم الشواغل بالنسبة للمنظمات والأفراد في أمن المعلومات، لأن مجرد وجود حالة واحدة غير ملتقطة من البرمجيات الخبيثة يمكن أن تؤدي إلى تعطل الأنظمة وإفساد البيانات. كما أن فك التوصيل عن الشبكة الحاسوبية لا يخفف تماماً من خطر الإصابة بها، كما بينت ذلك البرمجيات الخبيثة التي استغلت الأداة USB كمسوّغ لإقحام نفسها في الشبكة. وبالتالي فإن التركيز الأساسي للجهود التي بذلت لمكافحة البرمجيات الخبيثة قد انصب حتى اليوم على منع آثارها الضارة من خلال كشفها المبكر.

وتستعمل حالياً عدة أساليب شائعة لكشف البرمجيات الخبيثة تستند أساساً إلى التواقيع المادية والمعلومات الحدسية. وهذه الأساليب فعالة من حيث ضيق مجال تطبيقها، على الرغم من أن لكل أسلوب منها عيوبه الفردية الخاصة به، من قبيل أن التواقيع ليست ملائمة لمعالجة البرمجيات الخبيثة التي يكون مفعولها فورياً، أو التي تكون أهدافها محددة، أو المتعددة الأشكال، أو الأشكال الأخرى من البرمجيات الخبيثة الناشئة. وبالمثل، قد يكون الكشف الحدسي قادراً على كشف بعض الأنواع المحددة من البرمجيات الخبيثة بينما يعجز عن كشف الأنواع التي لا يتوفر لديه أنماط محددة عنها، مثل برمجيات الحزم الجذرية على مستوى النواة. وبالتالي فمن الأسلم القول إن هذه الأساليب، رغم فائدتها المستمرة، لا يمكن التعويل عليها لمعالجة التدفق الحالي من البرمجيات الخبيثة.

ويرمي تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها (MAEC تلفظ "مايك") إلى إزالة أوجه الغموض وعدم الدقة القائمة حالياً في أوصاف البرمجيات الخبيثة والحد من الاعتماد على التواقيع. بهذه الطريقة، تسعى لغة MAEC إلى تحسين التواصل فيما بين البشر، وبين الإنسان والآلة، وفيما بين الآلات، وبين الآلة والإنسان، بشأن البرمجيات الخبيثة، والحد من التكرار المحتمل للجهود التي قام بها الباحثون بشأن تحليل البرمجيات الخبيثة، وإتاحة إمكانية وضع التدابير المضادة بسرعة بتوفير إمكانية الاستفادة من الاستجابات لحالات البرمجيات الخبيثة التي رصدت من قبل. وكما سيتم توضيحه، فإن لغة MAEC تتيح إمكانية الترابط والتكامل والأتمتة في تبادل المعلومات المنظمة القائمة على النعوت بشأن البرمجيات الخبيثة، من قبيل مظاهر السلوك والتشويش المصطنع وأنماط الهجمات وما إلى ذلك.

وكما هو مبين في الشكل 1، تتألف لغة MAEC من نموذج بيانات يغطي عدة مخططات مترابطة، ويمثل بالتالي القواعد النحوية التي تعرّف اللغة. وتسمح هذه المخططات بتوليد أشكال مختلفة من خرج لغة MAEC يمكن اعتبارها بمثابة استعمالات محددة للقواعد النحوية المذكورة أعلاه.



الشكل 1 – لمحة عامة عن لغة MAEC الرفيعة المستوى

تستهدف مخططات كل من حاوية لغة MAEC ورزمة لغة MAEC وحزمة لغة MAEC حالات استعمال مختلفة، وبالتالي فهي تلتقط أنواعاً مختلفة من المعلومات المتعلقة بالبرمجيات الخبيثة.

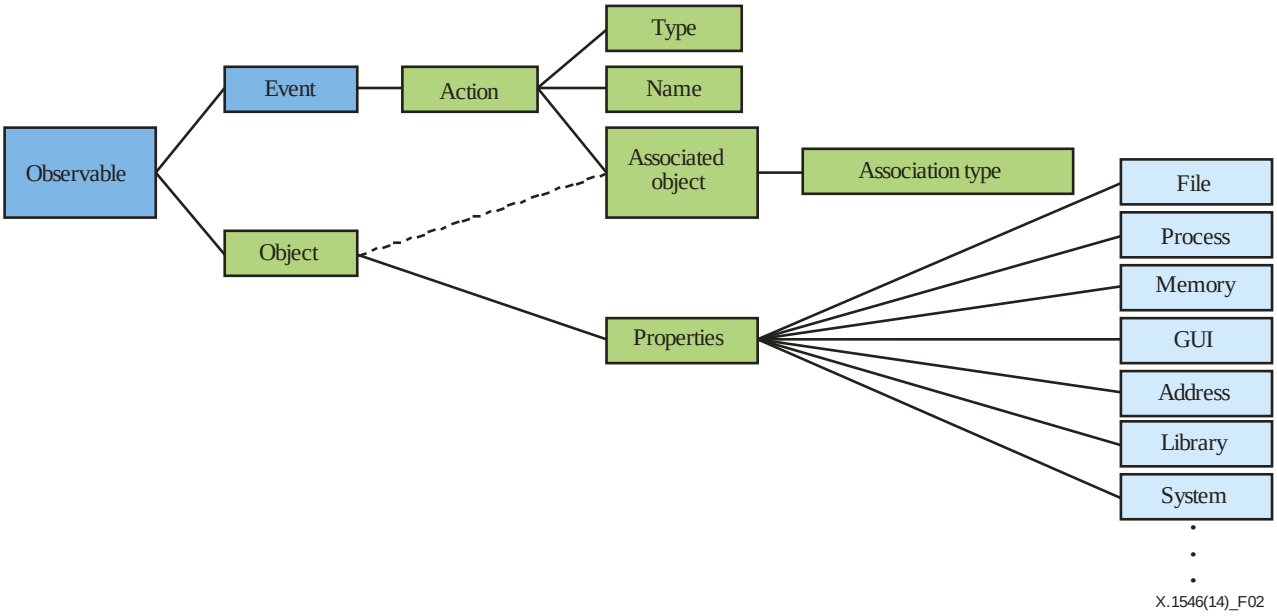
وترتبط لغة MAEC بكل من لغة CybOX وبنسق تبادل البيانات الشرحية للبرمجيات الخبيثة (MMDEF) الذي وضعه الفريق المعني بأمن التوصيلات الصناعية (ICSG) التابع لمعهد المهندسين الكهربائيين والإلكترونيين (IEEE).

ولغة CybOX هي لغة معيارية من أجل تحديد مواصفات الأحداث أو الخصائص المتعددة الحالات القابلة للملاحظة في المجال التشغيلي والتقاطها وتحديد خصائصها ونقلها. وتطبق الأحداث القابلة للملاحظة في عدة مجالات من بينها: تقييم التهديدات وتحديد خصائصها (الأنماط التفصيلية للهجمات)، وتحديد خصائص البرمجيات الخبيثة، وإدارة الأحداث التشغيلية، والتسجيل، والتوعية السيبرانية الظرفية، والاستجابة للحوادث، والأدلة القضائية الرقمية، وتبادل المعلومات عن التهديدات.

ومعظم الحقول في لغة CybOX اختيارية، بحيث يمكن استعمال الحقل المناسب وإغفال الحقول الباقية. ويمكن استعمال لغة CybOX لتحديد مواصفات وخصائص فئة واسعة من الكيانات السيبرانية وتعريف التشكيلات المترابطة والمنطقية لعدة كيانات و/أو أفعال و/أو أحداث و/أو أحداث قابلة للملاحظة.

ويعتمد تحديد خصائص البرمجيات الخبيثة بواسطة لغة MAEC على الآلية المشتركة (الهيكل والمحتوى) التي توفرها لغة CybOX لمعالجة الأحداث السيبرانية القابلة للملاحظة عبر المدى الكامل لحالات استعمال لغة MAEC وضمنه. وفيما توفر لغة MAEC سياق التحليل والمؤشرات ومظاهر السلوك والآليات، توفر لغة CybOX الأفعال والكيانات العامة المستعملة في المجال السيبراني التشغيلي. وتشمل الأمثلة على *الأحداث القابلة للقياس* إنشاء مفتاح السجل وحذف ملف وتلقي طلب HTTP GET؛ أما الأمثلة على الخصائص المتعددة الحالات فتشمل تخليط ملف وفق خوارزمية MD5، وقيمة مفتاح السجل، ووجود برنامج mutex.

تستورد لغة MAEC الفعل والكيان من لغة CybOX وتقوم بتوسيعه. ويُظهر الشكل 2 لمحة عامة مبسّطة للغاية عن مخطط CybOX، حيث تظهر مكونات CybOX التي تستعملها لغة MAEC باللون الأخضر.



الشكل 2 – لمحة عامة بسيطة عن مخطط لغة CybOX

يعتبر هيكل خصائص CybOX بديلاً مؤقتاً ملخصاً لمختلف المخططات المعرّفة مسبقاً لأنواع الكيانات (مثلاً ملف أو عملية أو ذاكرة) التي يمكن تطبيقها في مكانه. أما مخططات الخصائص، المبينة باللون الأزرق الفاتح، فيتم الاحتفاظ بها بمعزل عن نواة مخطط CybOX.

وقد قام بوضع نسق تبادل البيانات الشرحية للبرمجيات الخبيثة (MMDEF) الفريق المعني بأمن التوصيلات الصناعية (ICSG) التابع لمعهد المهندسين الكهربائيين والإلكترونيين (IEEE). وقام برعاية وضع المخطط الأساسي بالدرجة الأولى فريق من بائعي المنتجات الخاصة بمكافحة الفيروسات (AV) بهدف امتلاك وسيلة لإغناء عينات البرمجيات الخبيثة المشتركة ببيانات شرحية إضافية. ويسمح ذلك بالتالي بتحديد خصائص بعض السمات الساكنة مثل دوال التخليط وأسماء الملفات، إلى جانب بعض السمات السلوكية الأساسية.

ويسهم مجتمع أمن المعلومات في تطوير لغة MAEC من خلال المشاركة في إنشاء هذه اللغة عبر قوائم مناقشات مطوّري لغة MAEC وبوابة التعاون ومن خلال إدماج لغة MAEC في قدرات الأدوات ووسائل التخزين الخاصة بهم. ويتألف مجتمع لغة MAEC من ممثلين من طيف واسع من دوائر الصناعة والهيئات الأكاديمية والمنظمات الحكومية من مختلف أنحاء العالم، وهو يشرف على لغة MAEC واستعمالاتها وأدواتها من خلال وسيلة تخزين متاحة للجمهور. وهذا يعني أن لغة MAEC تعبر عن الرؤى والخبرة المشتركة لأوسع مجموعة ممكنة من الاختصاصيين العاملين في جميع أنحاء العالم في تحليل البرمجيات الخبيثة ومنعها.

وقد جرى إعداد التوصية على أساس تعاوني مع شركة MITRE مع مراعاة أهمية الحفاظ، قدر المستطاع، على التوافق التقني بين هذه التوصية و"المتطلبات والتوصية المتعلقة بالتوافق مع لغة MAEC"، الإصدار 1.1، المؤرخ 7 يوليو 2013 والصادر عن [https://maec.mitre.org/compatible/Requirements_for_MAEC_Compatibility_V1.1.pdf].

تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها

1 مجال التطبيق

توفر هذه التوصية وسيلة منظمة للنهوض بمحتوى أمني مفتوح ومتاح للجمهور عن البرمجيات الخبيثة ومظاهر سلوكها، ولتقييس نقل هذه المعلومات عبر كل أنواع أدوات الأمن وخدماته التي يمكن استعمالها لمراقبة وإدارة عمليات الدفاع ضد البرمجيات الخبيثة.

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.

[ISO/IEC 19757-3] المعيار ISO/IEC 19757-3: 2006، *تكنولوجيا المعلومات – لغة تعريف مخطط الوثائق (DSDL) – الجزء 3: التحقق على أساس القواعد – Schematron.*

[W3C XML Schema] الجزء 2 من W3C XML Schema (2004)، *الجزء 2 من مخطط اللغة XML الصادرة عن اتحاد الشبكة العالمية (W3C): أنواع البيانات*، الطبعة الثانية <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 المالك (owner) [b-ITU-T X.1520]: القيّم (شخص حقيقي أو شركة) المسؤول عن القدرة.

2.1.3 مستعمِل (user) [b-ITU-T X.1520]: مستهلك للقدرة أو مستهلك محتمل لها.

2.3 مصطلحات معرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 قدرة (capability): هي وظيفة أو وظائف محددة لمنتج، أو خدمة، أو وسيلة تخزين.

2.2.3 نتائج اختبار القدرة (capability test results): بيانات تمثل نتائج اختبار الصِحة.

3.2.3 محتوى (content): أي شكل من أشكال لغة تعداد البرمجيات الخبيثة وتحديد خصائصها (MAEC)، بما في ذلك وثائق نسق خرج لغة MAEC فضلاً عن العناصر/الأنواع المدمجة.

4.2.3 اختبار الصحة (correctness testing): عملية لتحديد ما إذا كان تنفيذ لغة MAEC قد تم بالشكل الصحيح.

5.2.3 حزمة MAEC (MAEC bundle): شكل معياري لخرج لغة MAEC يضم جميع الخصائص المستقاة من تحليل حالة واحدة من البرمجيات الخبيثة، بما في ذلك أي مظهر سلوك أو فعل للغة MAEC، وأي كيان متصل بلغة MAEC.

6.2.3 حاوية MAEC (MAEC container): شكل معياري لخرج لغة MAEC يضم واحدة أو أكثر من رزم MAEC.

7.2.3 نسق خرج لغة MAEC (MAEC output format): أي من الأنساق المعيارية الثلاثة للغة MAEC، بما فيها حاوية أو حزمة أو رزمة لغة MAEC.

8.2.3 رزمة MAEC (MAEC package): شكل معياري لخرج لغة MAEC يستعمل لتحديد جميع البيانات المعروفة بالنسبة لواحد أو أكثر من مواضيع البرمجيات الخبيثة، بما في ذلك خصائصها المستقاة من التحليل (عن طريق حزم MAEC) وأي تحليل أو بيانات شرحية أخرى مرتبطة بها.

9.2.3 حالة برمجيات خبيثة (malware instance): نسخة محددة من البرمجيات الخبيثة.

10.2.3 عنصر برمجيات خبيثة (malware element): مظهر سلوك أو نعت أو استغلال أو حمولة نافعة أو أي عنصر آخر مرتبط بحالة محددة من البرمجيات الخبيثة، أو بفئة أو صنف من البرمجيات الخبيثة.

11.2.3 نمط برمجيات خبيثة (malware pattern): تجريد لبعض النعوت التي تشترك فيها مجموعة من حالات البرمجيات الخبيثة (فئات أو أصناف). ويمكن أن يكون لنمط واحد من البرمجيات الخبيثة عدد كبير من حالات البرمجيات الخبيثة المتنوعة التي يمكن ربطها به.

12.2.3 موضوع برمجيات خبيثة (malware subject): كيان في لغة MAEC يضم جميع التفاصيل المتعلقة بحالة واحدة من البرمجيات الخبيثة، بما في ذلك بيانات التحليل الشرحية المقابلة ومحتوى التحليل والمعلومات بشأن العلاقات.

13.2.3 منتج (product): أي أداة أو خدمة أو وسيلة تخزين مضادة للبرمجيات الخبيثة ولها قدرة واحدة أو أكثر.

14.2.3 وسيلة تخزين (repository): مجموعة واضحة أو ضمنية من عناصر البرمجيات الخبيثة أو أنماط من البرمجيات الخبيثة، تدعم أداة أو خدمة إنشاء محتوى ما، مثل قاعدة بيانات خاصة بالأنماط السلوكية، أو مجموعة من حالات البرمجيات الخبيثة التي جرى تحليلها في أداة اختبار وضع الحماية، أو الخرج المجمع لأداة التحليل الثنائي الساكنة أو الدينامية. وقد تكون وسيلة التخزين أيضاً مجموعة من وثائق نسق خرج لغة MAEC.

15.2.3 مراجعة (review): عملية تحديد توافق أو عدم توافق قدرة ما مع لغة MAEC.

16.2.3 سلطة المراجعة (review authority): كيان يقوم بإجراء اختبار الصحة ويكون مخولاً رسمياً بالاعتراف بأن قدرةً ما متوافقة مع لغة MAEC.

17.2.3 عينة مراجعة (review sample): نسخة عن قدرة ما تقدّم لسلطة المراجعة لاستعمالها في تحديد توافق أو عدم توافق قدرة ما مع لغة MAEC.

18.2.3 إصدار المراجعة (review version): الإصدار المحدد التاريخ للغة MAEC والذي استُعمل لتحديد توافق قدرة ما مع لغة MAEC.

19.2.3 خدمة (service): نشاط لتحليل البرمجيات الخبيثة أو كشفها أو علاجها ينفّذ قدرة واحدة أو أكثر.

20.2.3 أداة (tool): تطبيق أو جهاز برمجيات ينفذ واحدة أو أكثر من الوظائف. وتقوم الأداة بتحليل أو كشف أو علاج البرمجيات الخبيثة من خلال أساليب متنوعة، على سبيل المثال أداة التحليل الساكن أو أداة التحليل الدينامي أو الماسح القائم على التوقيع أو الماسح الحدسي وما إلى ذلك. كما تستطيع الأداة أن تقوم باستحداث المحتوى.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

AV مكافحة الفيروسات *(Antivirus)*

CybOX لغة CybOX *(Cyber-Observable expression)*

ID معرّف الهوية *(Identifier)*

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

MMDEF نسق تبادل البيانات الشرحية للبرمجيات الخبيثة *(Malware Metadata Exchange Format)*

SIM إدارة معلومات الأمن *(Security Information Management)*

XML لغة تشفير قابلة للتوسيع *(extensible Markup Language)*

5 الاصطلاحات

يستخدم المختصر MAEC في هذه التوصية كاسم.

6 الشروط رفيعة المستوى

تعرِّف البنود الواردة أدناه المفاهيم والأدوار والمسؤوليات المتصلة بالقدرات المختلفة الخمس التي تستهدف كل منها استعمالاً مختلفاً للغة MAEC، والتي تشكل الاستخدام المناسب لهذه اللغة. وتمكِّن هذه القدرات أعضاء مجتمع لغة MAEC من أن يفهموا بيسر الكيفية التي يستخدم فيها منتج ما اللغة المذكورة والطريقة التي يمكن أن يلبي فيها احتياجاتهم.

وتطبق المتطلبات التالية على جميع القدرات التي تحقق الدعم للغة MAEC، بغض النظر عن الوظائف المحددة المنفذة (ترد المتطلبات المحددة للوظائف في الفقرة 10 أدناه "متطلبات التوافق المحددة"). وإذا ما تبين أن قدرة ما تلبي كل المتطلبات النافذة، فإن مالك القدرة سيتلقى إقراراً رسمياً من سلطة المراجعة بالتوافق مع لغة MAEC.

الشروط الأساسية

1.6 يجب أن يكون مالك القدرة كياناً قانونياً صحيحاً، أي منظمة أو شخص محدد، وأن يكون في حوزته رقم هاتف صالح وعنوان بريدي إلكتروني وعنوان بريدي عادي.

2.6 يجب أن يوافق مالك القدرة على أن يتقيّد بجميع الشروط الإلزامية المتعلقة بالتوافق مع لغة MAEC، والتي تشمل الشروط الإلزامية المتعلقة بالوظائف المعنية.

3.6 يجب أن يزوّد مالك القدرة سلطة المراجعة بنقطة اتصال تقنية مؤهلة للإجابة على الأسئلة المتصلة بالأداء الوظيفي المرتبط بلغة MAEC للقدرة ولتنسيق إعداد القدرة لاختبار الصِحة.

4.6 يجب أن يزوّد مالك القدرة سلطة المراجعة بنسخة مكتملة من "استمارة استبيان التوافق مع لغة MAEC". وينبغي أن تُرسل هذه الاستمارة إلى مالك القدرة بعد معالجة سلطة المراجعة "لاستمارة إعلان التوافق مع لغة MAEC".

5.6 يجب أن يعمل مالك القدرة مع سلطة المراجعة لإتاحة المنتج، أو الخدمة، أو وسيلة التخزين لاختبار الصِحة.

6.6 يجب أن يوفر مالك القدرة لسلطة المراجعة حرية النفاذ إلى البنود اللازمة لأداء اختبار الصِحة، بما في ذلك نتائج الاختبار و/أو عينات المراجعة، وذلك لتحديد مدى الالتزام بشروط التوافق المرتبطة.

7.6 وكجزء من تلقي الإقرار الرسمي بالتوافق مع لغة MAEC، فإن على مالك القدرة الموافقة على دعم سلطة المراجعة في أنشطة اختبارات المتابعة، حيث سيتم تبادل أنواع مناسبة من الملفات مع المنظمات الأخرى سعياً وراء إثبات صحة قدرتها. وستتولى سلطة المراجعة إدارة ذلك على أن يظل ضمن مستويات معقولة من الجهد بالنسبة لكل المشاركين.

8.6 يجب أن تتاح القدرة للجمهور أو لمجموعة من المستهلكين.

9.6 يجب أن تحدد القدرة بوضوح إصدار (إصدارات) مراجعة لغة MAEC والمخطط (المخططات) المرتبط الذي يتوافق معه.

متفرقات

تتناول هذه المتطلبات الأوجه المختلفة للتوافق مع لغة MAEC.

10.6 إذا لم تستوفِ القدرة جميع المتطلبات المعمول بها أعلاه (الفقرات من 1.6 إلى 9.6)، فيجب ألا يعلن مالك القدرة حينها عن أن القدرة متوافقة مع لغة MAEC.

11.6 إذا لم تستوفِ القدرة جميع المتطلبات الخاصة بوظائفها (المحددة في الفقرات من 1.10 إلى 27.10)، فيجب ألا يعلن مالك القدرة أنها متوافقة مع لغة MAEC.

12.6 يجب أن يحصل مالك القدرة على موافقة رسمية من سلطة المراجعة قبل الإعلان عن أن القدرة متوافقة مع لغة MAEC.

7 الصِحة

تتناول هذه المتطلبات أخطاء الصحة المرتبطة بالتوافق مع لغة MAEC، بما في ذلك، وإن لم يكن على سبيل الحصر، الأخطاء المتصلة بصلاحية المخطط والاستعمالات الباطلة لهياكل وعناصر معينة في لغة MAEC.

1.7 يجب أن يتيح مالك القدرة الوسائل اللازمة لكي يتقدم المستعمل بأخطاء الصحة المكتشفة في استخدام لغة MAEC وفي أي محتوى لهذه اللغة صادر عن القدرة.

2.7 يجب أن يضع مالك القدرة خطة لمعالجة أية أخطاء للصحة يتم إبلاغه عنها.

3.7 يجب أن يصحح مالك القدرة أي خطأ في الصِحة أبلغ به خلال فترة معقولة بعد إبلاغه لأول مرة عن الخطأ.

8 الوثائق

تطبق المتطلبات التالية على الوثائق التي تُقدَّم مع قدرة متوافقة مع لغة MAEC.

1.8 يجب أن تتضمن وثائق القدرة وصفاً موجزاً للغة MAEC والتوافق مع لغة MAEC، وهو ما يمكن أن يتضمن أجزاءً حرفية من الوثائق المحمّلة من الموقع الإلكتروني الخاص بلغة MAEC.

2.8 يجب أن تحدد القدرة في وثائقها بوضوح تغطيتها للغة MAEC والمخططات المرتبطة بها، بما في ذلك تلك المستوردة م الجهود المشتركة للغة CybOX ونسق تبادل البيانات الشرحية للبرمجيات الخبيثة (MMDEF)، إما من خلال العناصر أو الكيانات الفردية للغة CybOX التي لا تدعمها القدرة، أو من خلال العناصر أو الكيانات الفردية للغة CybOX التي تدعمها القدرة. وعلى سبيل المثال، إذا كانت القدرة تتقدم بطلب للإقرار الرسمي بأنها متوافقة مع لغة MAEC باعتبارها أداة أو خدمة دينامية لإنشاء المحتوى وبأنها لا تدعم كيان ملفات CybOX و/أو الإجراءات المرتبطة بكيان ملفات CybOX، عندئذ يجب الإشارة إلى عدم التوافق هذا في القدرة.

3.8 يجب أن تشير وثائق القدرة بوضوح إلى الإجراء الذي يجب أن يستخدمه المستعمل لتقديم أخطاء الصِحة المكتشفة في أي محتوى للغة MAEC يقوم المنتج بإصداره.

4.8 إذا كانت الوثائق المرفقة بالقدرة تتضمن فهرساً، فينبغي أن تشمل إحالات إلى الوثائق المتصلة بلغة MAEC تحت مصطلح "MAEC".

9 الصلاحية

تُستمد المتطلبات التالية من المتطلبات التي تشترط على القدرات المتوافقة مع لغة MAEC العمل بوثائق صالحة. وتساعد هذه المتطلبات على ضمان تنسيق المعلومات بصورة صحيحة والتزام هيكل الوثيقة بلغة MAEC.

1.9 على القدرة التحقق من صلاحية كل محتوى لغة MAEC (سواء ما هو منتج أو مستهلك) باستخدام التحقق من مخطط W3C XML (انظر [W3C XML Schema]) بالمقارنة مع إصدار لغة MAEC الذي ذُكر أنه يتوافق معها.

2.9 على القدرة إخطار المستعمل بأية أخطاء في التحقق من صلاحية مخطط W3C XML.

3.9 على القدرة التحقق من كل محتوى لغة MAEC (سواء ما هو منتج أو مستهلك) باستخدام التحقق من لغة Schematron (انظر [ISO/IEC 19757-3]) بالمقارنة مع إصدار لغة MAEC التي ذُكر أنه يتوافق معها.

4.9 على القدرة إخطار المستعمل بأية أخطاء في التحقق من لغة Schematron.

10 متطلبات القدرات المحددة

تطبق المتطلبات التالية على القدرات التي من أجلها ينشد مالكو القدرة توافق لغة MAEC مع الوظائف المرتبطة بها. وتوفر القدرة المتوافقة مع لغة MAEC وظيفة محددة واحدة على الأقل: إنشاء المحتوى، أو تخزين المحتوى، أو استهلاك المحتوى.

إنشاء المحتوى	أداة أو خدمة تُنشئ أو تساعد في عملية إنشاء ملفات جديدة للغة MAEC، بما في ذلك تلك التي تدمج الوثائق القائمة لنسق خرج لغة MAEC في ملف واحد. وفيما يلي تعريف الأنواع الفرعية لوظيفة إنشاء المحتوى: • إنشاء محتوى التحليل الساكن: أداة أو خدمة تجري نوعاً من التحليل الساكن لحالة دخل واحدة أو أكثر من البرمجيات الخبيثة وتعرض النتائج في وثيقة نسق خرج لغة MAEC. • إنشاء محتوى التحليل الدينامي: أداة أو خدمة تجري نوعاً من التحليل الدينامي (أي تنفيذ بواسطة الأجهزة) لحالة دخل واحدة أو أكثر من البرمجيات الخبيثة وتعرض النتائج في وثيقة نسق خرج لغة MAEC. • استحداث إنشاء المحتوى: أداة أو خدمة تدعم الإنشاء والتنقيح اليدوي لوثائق نسق خرج لغة MAEC.
تخزين المحتوى	وسيلة تخزين لمحتوى لغة MAEC تكون متاحة للمجتمع (مجاناً أو لقاء مبلغ).
استهلاك المحتوى	أداة أو خدمة تقبل وثائق نسق خرج لغة MAEC كمدخلات وتعرض محتوى هذه الوثائق على المستعمل أو تستخدمها لأداء عمل ما (العلاج، إدارة معلومات الأمن (SIM)، وما إلى ذلك).

إنشاء المحتوى العام

تطبق هذه المتطلبات على جميع الأدوات والخدمات المصممة لتوفير خرج محتوى لغة MAEC.

1.10 يجب أن تولِّد الأداة أو الخدمة التي توفر محتوى للغة MAEC نوعاً واحداً على الأقل من نسق خرج لغة MAEC (حزمة أو رزمة أو حاوية لغة MAEC).

2.10 يجب أن تولِّد كل أداة أو خدمة تهدف إلى توفير خرج لحالة واحدة من البرمجيات الخبيثة ولا تهدف إلى جمع المعلومات عن النعوت الخاصة بها حزمة MAEC واحدة لحالة البرمجيات الخبيثة.

3.10 يجب أن تولِّد الأداة أو الخدمة، التي تهدف إلى توفير خرج لحالة واحدة من البرمجيات الخبيثة و/أو لا تهدف إلى جمع المعلومات عن النعوت الخاصة بها، واحدة أو أكثر من رزم MAEC ذات واحد أو أكثر من مواضيع البرمجيات الخبيثة المدمجة بلغة MAEC، ويجب أن تولِّد بعدئذ حاويات MAEC التي تحتوي على رزم لغة MAEC المدمجة.

4.10 يجب أن تولِّد الأداة أو الخدمة، التي تهدف إلى توفير خرج لأكثر من مجموعة واحدة من حالات البرمجيات الخبيثة، واحدة أو أكثر من حاويات لغة MAEC ذات واحدة أو أكثر من رزم MAEC لكل مجموعة من حالات البرمجيات الخبيثة التي تقوم بتحليلها.

5.10 يجب أن توثّق الأداة أو الخدمة التي تهدف إلى جمع المعلومات عن النعوت الخاصة، كحد أدنى، اسمها وإصدارها والبائع باستخدام الكيانات المناسبة في موضوع البرمجيات الخبيثة للغة MAEC، وأن تولِّد بالتالي رزم MAEC أو حاويات رزم MAEC المدمجة.

6.10 على كل أداة أو خدمة تولِّد رزم MAEC أن تكون قادرة على توليد حزم MAEC قائمة بذاتها.

7.10 على كل أداة أو خدمة تولِّد حاويات MAEC أن تكون قادرة على توليد رزم MAEC قائمة بذاتها.

8.10 على كل أداة أو خدمة أن تستخدم جزءها الخاص من حيز الاسم الثابت الوحيد من معرف الهوية (ID) على امتداد كل محتوى للغة MAEC الذي تولده.

إنشاء محتوى التحليل الساكن

تطبق هذه المتطلبات على جميع أدوات وخدمات التحليل الساكن المصممة لإنشاء محتوى للغة MAEC.

9.10 عند توليد ملف نسق خرج لغة MAEC، على كل أداة أو خدمة في التحليل الساكن أن تقدم تقريراً بنتائجها باستخدام الكيانات الأنسب للغة MAEC (بما في ذلك على سبيل المثال لا الحصر أفعال و/أو كيانات و/أو مظاهر سلوك و/أو تصنيفات برامج مكافحة الفيروسات) فضلاً عن أنسب نسق خرج للغة MAEC.

إنشاء محتوى التحليل الدينامي

تطبق هذه المتطلبات على جميع أدوات وخدمات التحليل الدينامي المصممة لإنشاء محتوى للغة MAEC.

10.10 عند توليد ملف نسق خرج لغة MAEC، على كل أداة أو خدمة في التحليل الدينامي أن تقدم تقريراً بنتائجها باستخدام الكيانات الأنسب للغة MAEC (بما في ذلك على سبيل المثال لا الحصر أفعال ومظاهر سلوك لغة MAEC) فضلاً عن أنسب نسق خرج للغة MAEC.

استحداث إنشاء المحتوى

تطبق هذه المتطلبات على جميع الأدوات والخدمات المصممة لإنشاء محتوى للغة MAEC أو للمساعدة على تسهيل إنشاء أو تعديل محتوى للغة MAEC.

11.10 ينبغي لأداة أو خدمة الاستحداث أن تشجع على إعادة استعمال المواضيع والأفعال والكيانات والمؤشرات المقترحة القائمة للبرمجيات الخبيثة.

12.10 ينبغي لأداة أو خدمة الاستحداث أن تتيح للمستعمل تنفيذ عملية التحقق من الصلاحية على وثيقة مكتوبة للغة MAEC، وإخطاره بكل أخطاء مخطط W3C XML ولغة Schematron.

13.10 يجب أن تتيح أداة أو خدمة الاستحداث للمستعمل استيراد وتحرير المحتوى القائم للغة MAEC (يشمل ذلك كل أنساق خرج لغة MAEC).

14.10 يجب أن تتيح أداة أو خدمة الاستحداث للمستعمل تصدير المحتوى، الذي أنشأته الأداة، كوثائق صالحة من وثائق نسق خرج لغة MAEC.

15.10 ينبغي أن تبلغ أداة أو خدمة الاستحداث المستعمِل بالمحتوى المزدوج.

16.10 يجب أن توفر أداة أو خدمة الاستحداث القيمة والقدرة بما يتجاوز قدرة محرر لغة الوسم القابلة للتوسيع (XML)، كما حددتها سلطة المراجعة.

تخزين المحتوى

تطبق هذه المتطلبات على جميع وسائل التخزين المصممة لتوفير مجموعة من محتوى للغة MAEC.

17.10 ينبغي أن تحتوي كل حاوية للغة MAEC أو رزمة أو موضوع برمجيات خبيثة أو تحليل أو حزمة أو فعل أو كيان أو مظهر سلوك أو مؤشر مقترح أو مجموعة مظاهر سلوك أو مجموعة أفعال أو مجموعة كيانات أو مجموعة مؤشرات مقترحة على معرف هوية (ID) وحيد بالنسبة لباقي الحاويات والرزم ومواضيع البرمجيات الخبيثة والتحليلات والحزم والأفعال والكيانات ومظاهر السلوك والمؤشرات المقترحة ومجموعات مظاهر السلوك ومجموعات الأفعال ومجموعات الكيانات ومجموعات المؤشرات المقترحة في وسيلة التخزين.

18.10 ينبغي أن يحتوي كل فعل أو كيان للغة MAEC على معرف هوية بالنسبة لباقي أفعال أو كيانات لغة MAEC وأن يكون معرف الهوية هذا فريداً بالنسبة لباقي أفعال أو كيانات لغة MAEC في وسيلة التخزين.

19.10 ينبغي أن يكون الجزء الخاص من حيز الاسم في معرف الهوية (ID) ثابتاً على امتداد كل محتوى للغة MAEC وأن يكون فريداً في وسيلة التخزين.

20.10 ينبغي أن يكون لكل حاوية للغة MAEC أو رزمة أو موضوع برمجيات خبيثة أو تحليل أو حزمة أو فعل أو كيان أو مظهر سلوك أو مؤشرات مقترحة أو مجموعة مظاهر سلوك أو مجموعة أفعال أو مجموعة كيانات أو مجموعة مؤشرات مقترحة معرف الهوية (ID) نفسه خلال وجودها. ولا ينبغي إعادة كتابة بند قائم لغايات أخرى حيث إن المستعملين قد يقومون بالإحالة إلى هذا البند في محتواهم الخاص.

21.10 على مالك وسيلة التخزين أن يوثق العملية التي يقوم المستعمل من خلالها باستعادة تحديثات المحتوى.

استهلاك المحتوى

تطبق هذه المتطلبات على جميع الأدوات والخدمات المصممة لاستهلاك محتوى للغة MAEC. ويلاحظ وجود تمييز بين كلمة "استهلاك" (معالجة المعلومات بطريقة ذكية) وكلمة "تحليل" (استخلاص محتوى خاص من وثيقة أكبر).

22.10 ينبغي لكل أداة أو خدمة تستهلك محتوى للغة MAEC أن تستهلك على الأقل نوعاً واحداً من نسق خرج لغة MAEC (حزمة أو رزمة أو حاوية).

23.10 ينبغي لكل أداة أو خدمة تستهلك محتوى للغة MAEC أن تدعم تحليل كل نوع من أنواع نسق خرج لغة MAEC من أجل استخلاص أي نوع من الأنواع المدمجة التي تستهلكها بغض النظر عن موقع الأنواع في وثيقة نسق الخرج. وعلى سبيل المثال، يجب أن تكون الأداة أو الخدمة التي لا تستهلك إلا الحزم قادرة أيضاً على تحليل الرزم والحاويات من أجل استخلاص محتوى الحزمة.

24.10 عندما لا تتطلب الأداة أو الخدمة إلا معلومات التحليل التقنية المرتبطة بحالة البرمجيات الخبيثة، فينبغي أن تستهلك حزم لغة MAEC.

25.10 إذا تطلبت الأداة أو الخدمة معلومات التحليل التقنية المرتبطة بحالة البرمجيات الخبيثة بالإضافة إلى بيانات التحليل الشرحية والمعلومات بشأن العلاقات، فينبغي أن تستهلك رزم لغة MAEC.

26.10 إذا تطلبت الأداة أو الخدمة معلومات التحليل المرتبطة بعدة مجموعات من حالات البرمجيات الخبيثة، فينبغي أن تستهلك حاويات لغة MAEC.

27.10 إذا لم تستهلك الأداة أو الخدمة ملفات نسق خرج لغة MAEC في وقت التشغيل، فإن على مالك القدرة أن يوثق العملية التي يمكن من خلالها للمستعمل تقديم ملفات خرج لغة MAEC إلى مالك القدرة لتفسرها الأداة أو الخدمة. وعلى الوثائق أن تبين مدى سرعة إتاحة الملفات المقدمة إلى مالك القدرة للأداة أو الخدمة.

11 متطلبات سلطة المراجعة

ترد فيما يلي المتطلبات المتعلقة بالتوافق مع لغة MAEC التي يجب أن تمتثل لها سلطة المراجعة.

1.11 على سلطة المراجعة أن تحدد بوضوح إصدار المراجعة للقدرة وإصدار وثيقة متطلبات التوافق مع لغة MAEC وإصدار لغة MAEC المستخدمة في تحديد الامتثال الرسمي لمتطلبات التوافق مع لغة MAEC لكل قدرة.

2.11 على سلطة المراجعة تحديد نوع (أنواع) وظائف القدرة (إنشاء المحتوى أو تخزين المحتوى أو استهلاك المحتوى).

3.11 على سلطة المراجعة تعريف ونشر عيّنة من مواد الاختبار.

4.11 على سلطة المراجعة أن تنشر المعلومات المتعلقة بسبل المشاركة في اختبار الصِحة بحيث يُتاح للمنظمات الاستعداد في أبكر وقت ممكن.

5.11 على سلطة المراجعة توفير جهة اتصال لترتيب اختبار الصِحة للقدرات التي تعلن دعمها للغة MAEC والتي استكملت "استمارة استبيان التوافق مع لغة MAEC".

6.11 يجوز لسلطة المراجعة إعادة اختبار قدرة حصلت على إقرار رسمي بالتوافق مع لغة MAEC، وذلك وفقاً لما تراه هذه السلطة.

12 الإلغاء

إذا ما تحققت سلطة المراجعة من أن قدرة قد اعتبرت متوافقة مع لغة MAEC، ولكن توفر لهذه السلطة في وقت لاحق بيانات بأن المتطلبات لم تعد مستوفاة، فإنه يجوز لسلطة المراجعة أن تلغي موافقتها ولن تكون القدرة متمتعة بعد ذلك بالإقرار الرسمي بأنها متوافقة مع لغة MAEC. وفيما يلي المتطلبات التي يجب أن تتبعها سلطة المراجعة بغية إلغاء الإقرار.

1.12 يجب أن توجه سلطة المراجعة إلى مالك القدرة إنذاراً بالإلغاء قبل الوقت المزمع لتطبيق الإلغاء بشهرين (2) على الأقل.

2.12 يجوز لسلطة المراجعة أن تؤجل تاريخ الإلغاء.

3.12 إذا وجدت سلطة المراجعة أن إجراءات مالك القدرة أو مزاعمها مضللة بشكل مقصود فإن بمقدورها إسقاط فترة الإنذار. ويجوز لسلطة المراجعة تأويل عبارة "مضللة بشكل مقصود" حسبما يتراءى لها.

4.12 إذا حددت سلطة المراجعة أن إجراءات مالك القدرة فيما يتعلق بمتطلبات التوافق مضللة بشكل مقصود، يستمر الإلغاء لسنة واحدة على الأقل.

5.12 يجب أن تحدد سلطة المراجعة المتطلبات المعينة التي لم يتم الامتثال لها.

6.12 إذا رأى مالك القدرة أن المتطلبات مستوفاة، فيجوز له أن يرد على إنذار الإلغاء بتقديم تفاصيل محددة تبين الأسباب التي تقف وراء استيفاء القدرة للمتطلبات المعنية.

7.12 إذا عدّل المالك القدرة بحيث تتقيد بالمتطلبات المعنية خلال فترة الإنذار، فينبغي لسلطة المراجعة، خلال فترة الإنذار، إنهاء إجراء الإلغاء بالنسبة للقدرة.

8.12 يجب أن تعلن سلطة المراجعة عن إلغاء الإقرار الرسمي بالاعتماد الصحيح للتوافق الصحيح مع لغة MAEC بالنسبة للقدرة.

9.12 يجوز لسلطة المراجعة إعلان سبب الإلغاء.

بيبليوغرافيـــا

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

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	المطاريف وطرائق التقييم الذاتية والموضوعية
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، 2015