国 际 电 信 联 盟

ITU-T X.1546

(01/2014)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

事件/事故/探索法信息交换

恶意软件属性的列举和特性化

ITU-T X.1546 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	**X.1540–X.1549**
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1546 建议书

恶意软件属性的列举和特性化

摘要

恶意软件属性的列举和特性化（MAEC）语言包括提供通用词汇的恶意软件属性和行为的列举，这些列举分为不同抽象层次：低层可觉察到的行为、中等程度行为和高等程度分类法。作为MAEC初始版本的ITU-T 1546建议书的重点是创建低层恶意软件属性的列举，并充分利用通过该领域已完成的类似工作获得的一些实例。因此，作为起步，将能够描述多数常见恶意软件类型（包括特洛伊木马、蠕虫和隐匿程式），但最终也将适用于更多的秘传恶意软件类型。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1546	2014-01-24	17	11.1002/1000/12038

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/ ，随后输入建议书的唯一识别码，例如， http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

关于恶意软件列举和特性（MAEC）的 ITU-T X.1546 建议书是一项涉及信息安全和业界的国际标准，旨在促进公开提供有关恶意软件和恶意软件行为的安全内容。本建议书还旨在实现涵盖所有安全工具和服务的此类信息（被用于对恶意软件进行监测并管理相应防卫行动）传送的标准化。MAEC 是用于对相关恶意软件细节进行编码的语言。

MAEC 语言旨在：1) 改善人与人、人与工具、工具与工具和工具与人之间有关恶意软件的通信，2) 减少研究人员之间有关恶意软件分析的重复工作，3) 通过充分利用此前对所觉察到的恶意软件实例的相应能力，促进更快地制定相关对策。威胁分析、入侵发现和事件管理是处理各种网络威胁的程序。MAEC 通过其统一的恶意软件属性编码，提供一种标准化格式，以便在上述程序中纳入针对恶意软件的、并可采取行动的信息。

恶意软件 – 亦称作“malware”（恶意软件）自1971年首次出现个人电脑（PC）病毒以来即以不同形式存在。目前的一系列恶意活动均由恶意软件造成，从通过僵尸网络传播的绝大多数垃圾邮件，到敏感信息窃取（以有针对性的社交工程攻击实现），不一而足。实事上，恶意软件是代表攻击方的自治代理，有能力从事可由代码表述的任何行动，因此对网络安全造成了极大威胁。

有鉴于此，保护计算机系统免受恶意软件危害是各组织和个人目前最为关切的信息安全问题之一，因为仅一次未得到阻止的恶意软件即可极大地危害系统并使数据受到破坏。不与计算机网络连接并不能完全消除这种这种传染风险，最好的例证便是将USB作为其插入载体的恶意软件。有鉴于此，多数打击恶意软件工作的重点一直是通过早期发现避免破坏性影响的产生。

目前存在若干进行恶意软件发现的通用方法，其主要基础是物理签名和试探法（heuristics）。这些方法在小范围内比较有效，但各有其不足，如签名不适合于处理零天、针对具体目标的多态恶意软件，以及正在出现的其它形式的恶意软件。同样，试探发现法可能能够总体发现特定类型的恶意软件，但可能漏掉不具备规律的恶意软件，如，内核级隐匿程式。因此，可以有把握地说，这些方法尽管依然有用，但不能仅依靠它们处理目前涌现的恶意软件。

恶意软件属性列举和特性化（MAEC，其发音为“mike”）的目的是消除目前恶意软件描述中存在的歧义和不准确性，并减少对签名的依赖。由此，MAEC旨在改善人与人、人与工具、工具与工具和工具与人之间有关恶意软件的通信，减少研究人员开展的恶意软件分析方面的重复工作，并通过利用以此前观察到的恶意软件实例的响应能力，更快地制定相关对策。以下将以示图说明根据诸如行为、人工因素（artifacts）和攻击规律等属性，MAEC语言如何实现相互关联性、集成性和自动化，以分享有关恶意软件的结构信息。

如图1所示，MAEC包含一种跨越若干互连一体模式（schemas）的数据模型，因此代表定义该语言的语法。这些模式便于产生不同形式的MAEC输出，可将这些输出视作上述语法的具体应用。

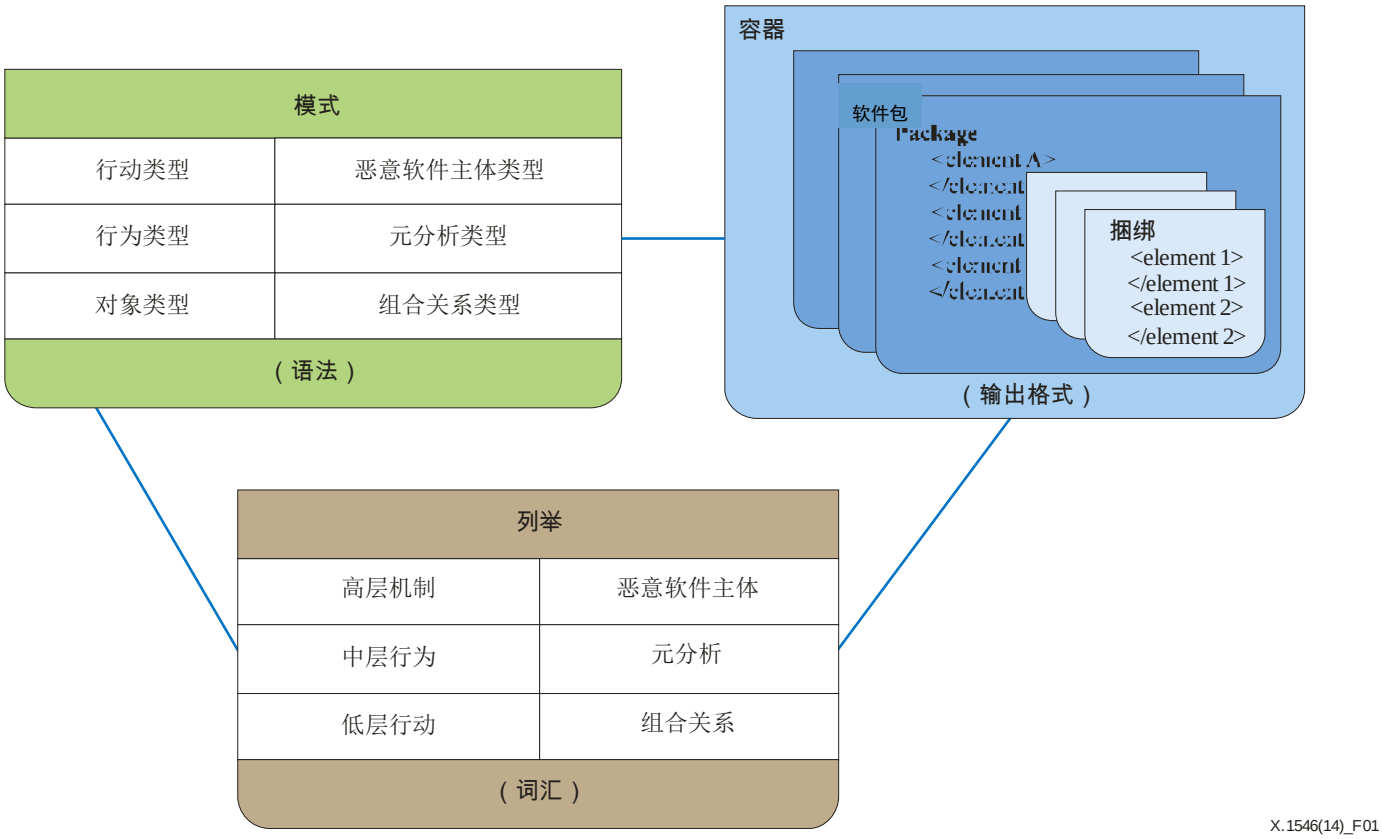

图1 – MAEC高层概述

MAEC容器、MAEC软件包和MAEC捆绑模式针对不同使用情况，因此，捕获与恶意软件有关的不同类型信息。

MAEC语言既与网络可觉察表述（CybOX）语言有关，也与IEEE ICSG的恶意软件元数据交换格式（MMDEF）有关。

CybOX是一种标准化语言，旨在规范、捕获在操作层面观察到的事件或状态特性，并对其予以特性化和沟通。网络可觉察语言适用于诸多领域：威胁评估和特性化（详细的攻击规律）、恶意软件特性化、操作事件管理、登录、网络状态意识、事件响应、数字取证以及网络威胁信息共享等。

CybOX的几乎每个场都是可选的，因此，人们只选择使用适合其需要的内容而摒弃其余内容。可用CybOX规范一系列网络对象并确定其特性，同时可用该语言定义多种对象、行动、事件和/或觉察事物的关系和逻辑构成。

利用MAEC确定恶意软件的特性依赖的是通用机制（结构和内容），即CybOX提供解决跨所有MAEC使用情形的网络可觉察事物。MAEC提供分析语境、指标、行为和机制，CybOX提供在网络操作领域使用的总体行动和对象。网络可觉察事物是网络领域可衡量的事件或状态属性。可衡量事件示例包括注册密钥创建、文档删除和接收HTTP GET请求；状态属性示例包括文档的MD5散列、注册密钥数值以及互斥体（mutex）的存在。

MAEC对CybOX对象和行动进行移植和扩展。图2所示为得到极为简化的CybOX模式概况图；MAEC使用的CybOX成份以绿色表示。

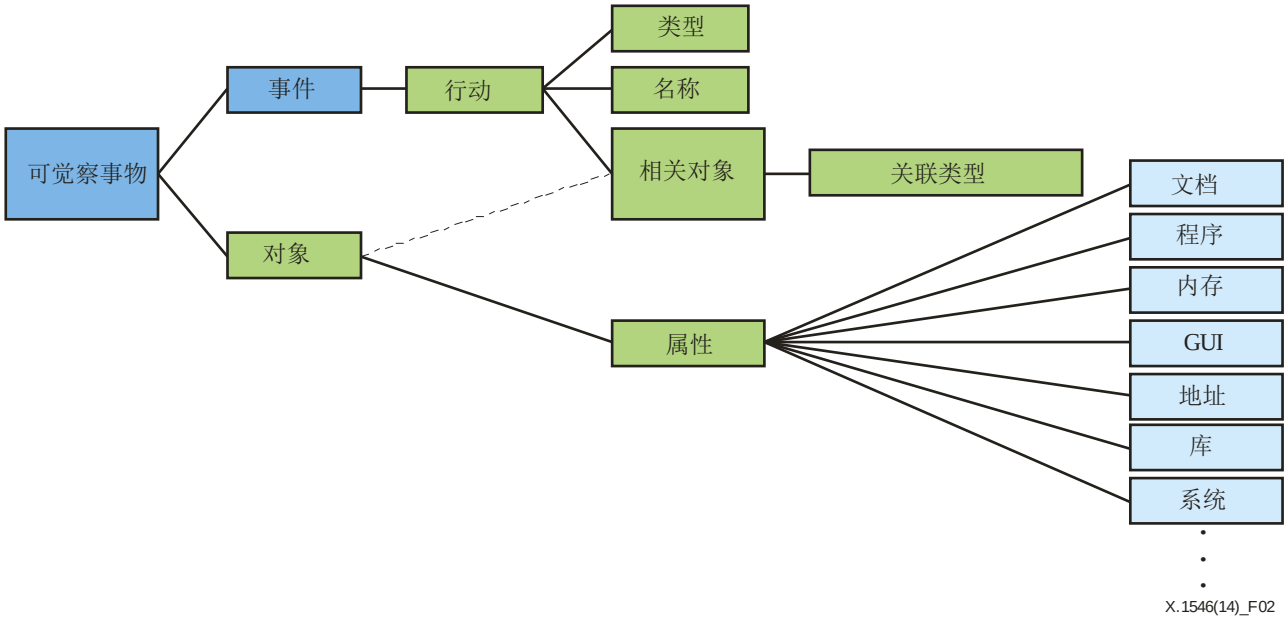

图2 – 网络可觉察表述（CybOX）模式的简单概况图

CybOX属性结构是多种不同预先定义的对象类型模式（如，文档、程序、内存）的抽象占位符，该占位符可在其位置上被举例说明。以蓝线表示的模式属性独立于CybOX核心模式。

目前，电气和电子工程师学会（IEEE）的业界连接安全小组（ICSG）正在开发MMDEF。初始模式的开发工作主要由反病毒（AV）产品厂商集团领导开展，目的是以某种方法增加带有更多元数据的共享恶意软件样品。因此，有助于确定某些静态功能特点（如散列和文档名称）的特性，以及一些非常基本的行为特性。

信息安全界通过参加 MAEC 语言创建工作为 MAEC 开发工作贡献力量，他们被列入 MAEC 开发商讨论名单和协作门户网站，同时他们还将 MAEC 语言纳入其自身工具和存储库功能之中。MAEC 这一团体包括来自世界各地的业界、学术机构和政府组织的广泛代表，该团体通过 MAEC 公开提供的存储库，对 MAEC 语言以及 MAEC 的功用和工具实行监督并开展协作。这意味着，MAEC 代表了全球最为广泛的恶意软件分析和预防专家集体形成的远见卓识和综合一体的专业技术。

本建议书是在与 MITRE 公司协作基础上制定的，在此过程中，我们始终牢记尽可能保持本建议书和“MAEC 兼容性要求和建议”版本 1.1（2013 年 7 月 7 日）之间的技术兼容性十分重要

[https://maec.mitre.org/compatible/Requirements_for_MAEC_Compatibility_V1.1.pdf].

ITU-T X.1546 建议书

恶意软件属性的列举和特性化

1 范围

本建议书提供一种结构手段，旨在促进公开提供有关恶意软件和恶意软件行为的安全内容，并实现用于监测和对恶意软件做出防卫的所有安全工具和业务之间此类信息传送的标准化。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ISO/IEC 19757-3] ISO/IEC 19757-3:2006, *Information technology – Document Schema Definition Languages (DSDL) – Part 3: Rule-based validation – Schematron.*

[W3C XML Schema] W3C XML Schema Part 2 (2004), *W3C XML Schema Part 2: Datatypes*, Second Edition. <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>

3 定义

3.1 它处定义的术语

本建议书使用了下列它处定义的术语：

3.1.1 拥有方[b-ITU-T X.1520]：对能力拥有责任的保管人（实实在在的个人或公司）。

3.1.2 用户[b-ITU-T X.1520]：能力的消费者或潜在消费者。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 能力：产品、服务或存储库的一个（数个）特定功能。

3.2.2 能力测试结果：代表正确性测试结果的数据。

3.2.3 内容：任何形式的恶意软件属性列举和特性（MAEC）实体，包括MAEC输出格式文件以及嵌入式成份/类型。

3.2.4 正确性测试：确定一种工具是否已正确实施MAEC的程序。

3.2.5 MAEC捆绑：一种MAEC输出的一周标准形式，旨在捕获单一一个恶意软件的实例的、通过分析得出的所有特性，包括任何观察到的MAEC行为或行动，以及任何相关的MAEC对象。

3.2.6 MAEC容器：MAEC输出的一种标准形式，旨在捕获一个或多个MAEC软件包。

3.2.7 MAEC输出格式：MAEC输出的三种标准形式中的任何一种，包括MAEC容器、软件包或捆绑。

3.2.8 MAEC软件包：MAEC输出的一种标准形式，旨在确定一个或多个恶意软件主体所有已知数据的特性，包括通过分析得出的特性（通过MAEC捆绑进行）和任何相关的分析或其它元数据。

3.2.9 恶意软件实例：恶意软件的特定副本。

3.2.10 恶意软件成份：与特定恶意软件实例、系列或恶意软件实例等级相关的行为、属性、开发利用和有效载荷等。

3.2.11 恶意软件规律：一套恶意软件实例（系列或等级）共有的一些属性的抽象化。单一一种恶意软件规律可能拥有多种变化不定的、与之相关的恶意软件实例。

3.2.12 恶意软件主体：捕获有关单一恶意软件实例所有细节的MAEC实体，包括任何相应的分析元数据、分析内容和关系信息。

3.2.13 产品：具有一种或多种能力的任何反恶意软件工具、服务或存储库。

3.2.14 存储库：支持内容创建工具或服务的任何隐含或明显的一系列恶意软件成份或恶意软件规律，如，行为规律数据库、由沙盒工具分析的一套恶意软件实例、或一种静态或动态二进制分析工具的汇总结果。存储库也可以是一系列MAEC输出格式文件。

3.2.15 审查：确定一种能力是否与MAEC兼容的程序。

3.2.16 审查机构：进行正确性测试的实体，且被授权正式确认某一项能力与MAEC兼容。

3.2.17 审查样本：向审查机构提供的能力结果副本，以便在确定该能力是否与MAEC兼容时使用。

3.2.18 审查版本：用于确定能力是否与MAEC兼容的、标明日期的MAEC版本。

3.2.19 服务：实施一项或多项能力的恶意软件分析、发现或补救活动。

3.2.20 工具：实施一项或多项功能的软件应用或装置。工具通过多种不同方法分析、发现恶意软件并做出补救，如静态分析工具、动态分析工具、基于签名的扫描仪、基于试探法的扫描仪等。工具还可进行内容编写。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

AV 反病毒

CybOX 可觉察网络表述

ID 识别符

MAEC 恶意软件属性的列举和特性化

MMDEF 恶意软件元数据交换格式

SIM 安全信息管理

XML 可扩展标记语言

5 惯例

本建议书中MAEC作为名词加以使用。

6 高层要求

以下各分段定义了五种不同能力的相关概念、作用和责任，每一能力均针对MAEC语言的不同用途，包括MAEC语言的正确使用。这些能力使得MAEC的成员轻而易举地理解特定产品如何使用MAEC语言，以及该语言如何适合其需求。

下列要求适用于正在实施的支持MAEC的所有能力，无论实施的特定功能如何（针对特定功能的要求见以下第10节所述的“特定兼容性要求”）。如果一种能力能够满足所有适用的要求，则该能力拥有方须从审查机构处收到有关于MAEC兼容的正式确认。

前提

6.1 能力拥有方须是有效的法律实体，即，组织或具体个人，拥有有效电话号码，电子邮件地址和邮政地址。

6.2 能力拥有方须同意遵守所有有关MAEC兼容性的强制性要求，包括适用于某个特定功能的强制性要求。

6.3 能力拥有方须向审查机构提供技术联系人的信息，该联系人有资格回答所有与MAEC相关的能力功能方面的问题，并对能力的正确性测试准备工作做出协调。

6.4 能力拥有方须向审查机构提供填妥的“MAEC兼容性问卷调查表”。在审查机构处理过“MAEC兼容性声明表”后，将向能力拥有方提供上述问卷调查表。

6.5 能力拥有方须与审查机构合作，确保产品、服务或存储库可供正确性测试使用。

6.6 能力拥有方须免费向审查机构提供进行正确性试验所需的所有项目，包括测试结果和/或审查样品，以确定是否符合所有相关兼容性要求。

6.7 为收到有关与MAEC兼容的正式确认，能力拥有方须同意支持审查机构进行后续测试活动，在此过程中，将与试图证明其能力正确性的其它机构交换相关类型文件。这将由审查机构进行管理，并将所有参与方的努力保持在一个合理程度上。

6.8 须向公众或一组消费者提供相关能力。

6.9 能力须明确无误地表明MAEC的审查版本及与之兼容的相关模式。

杂项

这些要求涉及MAEC兼容性的其它相关方面。

6.10 如果能力不能够满足上述适用的所有要求（第6.1至6.9段），则能力拥有方不得声称该能力与MAEC兼容。

6.11 如果能力不能满足与其功能相关的要求（在第10.1至第10.27段确定），则能力拥有方不得声称该能力与MAEC兼容。

6.12 能力拥有方在公布能力与MAEC兼容之前，须获得审查机构的正式批准。

7 正确性

这些要求涉及与MAEC兼容性相关的正确性中的错误，包括但不限于与模式核实相关的错误，以及特定MAEC结构和成份的无效使用。

7.1 能力拥有方须出台一种手段，以便于用户提交在使用MAEC中发现的正确性错误，或由能力产生的任何MAEC内容的错误。

7.2 能力拥有方须出台计划，以解决向其报告的任何正确性错误。

7.3 能力拥有方须在错误初次得到报告后的合理时间范围内纠正其收到的任何正确性错误。

8 文件

以下要求适用于为MAEC兼容性能力提交的文件。

8.1 能力文件须简单描述MAEC和MAEC兼容性，其中可包含MAEC网站提供文件的逐字段落。

8.2 能力文件须明确无误地表明其对MAEC及相关模式的涵盖，包括移植自可觉察网络表述（CybOX）界和恶意软件元数据交换格式（MMDEF）的内容，方法亦或是其不支持的成份或单个CybOX对象，亦或是其支持的成份和CybOX对象。例如，如果申请获得MAEC兼容性正式确认的能力是一项动态分析内容创建工具或服务、且不支持CybOX文件对象和/或与CybOX相关的行动，则该能力文件须明确表明这一不兼容性。

8.3 能力文件须明确表明用户应使用何种程序提交由产品产生的任何MAEC内容中发现的正确性错误。

8.4 如果能力文件包含索引，则该文件须在“MAEC”术语下包含对相关MAEC文件的参引。

9 有效性

下列要求源自这样的要求，即，与MAEC兼容的能力需具有有效文件。这一要求有助于确保信息格式正确，且文件结构符合MAEC语言。

9.1 能力须按照其声称符合的MAEC语言版本，证实使用W3C XML模式验证（见[W3C XML模式]）的所有MAEC内容（产生和消费内容）。

9.2 能力须向用户报告任何W3C XML验证错误。

9.3 能力须按照其声称符合的MAEC语言版本，证实使用Schematron验证（见[ISO/IEC 19757-3]）的所有MAEC内容（创建和消费内容）。

9.4 能力须向用户报告任何Schematron验证错误。

10 特定能力要求

以下要求仅适用于能力拥有方只针对相关功能寻求MAEC兼容性的能力。MAEC兼容能力须至少提供一种特定功能：内容创建、内容存储或内容消费。

内容创建	创建或在创建新MAEC文件过程中给予帮助的工具或服务，包括将现有MAEC输出格式文件整合为单一文件的工具或服务。 现已确定了下列内容创建功能的子类型： • 静态分析内容创建：对一种或多种输入恶意软件实例进行某种静态分析的工具或服务，并在MAEC输出格式文件中输出结果。 • 动态分析内容创建：对一种输入恶意软件实例进行某种动态分析（即，感知化执行（instrumented execution））的工具或服务，并在MAEC输出格式文件中输出结果。 • 编拟内容创建：支持人工创建和编辑MAEC输出格式文件的工具或服务。
内容存储	向该领域全体人员提供的MAEC内容存储库（免费或收费）。
内容消费	将MAEC输出格式文件作为输入加以接受的工具或服务，并或向用户展示其内容，或利用该内容执行某种行动（补救、安全信息管理（SIM）等）。

一般性内容创建

这些要求适用于所有旨在提供MAEC内容输出的工具和服务。

10.1 提供MAEC内容的工具或服务须至少生成一种类型MAEC输出格式（MAEC捆绑、软件包或容器）。

10.2 计划为单一恶意软件实例提供输出、且不打算捕获有关其自身属性信息的每一种工具或服务都应为该恶意软件实例生成单一一个MAEC捆绑。

10.3 计划为单一恶性软件实例提供传输和/或打算捕获有关其自身属性信息的工具或服务，应为其分析的每一种恶意软件实例都生成一个或多个MAEC软件包，且带有一个或多个嵌入式MAEC恶意软件主体。如果它不生成MAEC软件包，则须生成包含嵌入式MAEC软件包的MAEC容器。

10.4 计划为一套以上或一组恶意软件实例提供输出的工具或服务，应为其分析的每一套或一组恶意软件实例生成一个或多个MAEC容器，并带有一个或多个嵌入式MAEC软件包。

10.5 计划捕获有关其自身属性信息的工具或服务须在文件中至少记录其名称、版本和在MAEC恶意软件主体中使用相关实体的厂商，并须随后生成MAEC软件包或嵌入式MAEC软件包容器。

10.6 生成MAEC软件包的工具或服务应有能力生成自成一体的MAEC捆绑。

10.7 生成MAEC容器的工具或服务应能够生成自成一体的MAEC软件包。

10.8 工具或服务应在其生成的所有MAEC内容中使用其独一无二的识别符（ID）恒定命名空间部分。

静态分析内容创建

这些要求适用于计划创建MAEC内容的所有静态分析工具和服务

10.9 在生成MAEC输出格式文件时，静态分析工具或服务应利用最适当的MAEC实体（包括但不限于MAEC行动、对象、行为和/或AV分类）以及最恰当的MAEC输出格式报告其结果。

动态分析内容创建

这些要求适用于计划创建MAEC内容的所有动态分析工具和服务。

10.10 在生成MAEC输出格式文件时，动态分析工具或服务应利用最适当的MAEC实体（包括但不限于MAEC行动和行为）以及最恰当的MAEC输出格式，报告其结果。

内容编拟创建

这些要求适用于计划创建MAEC内容或帮助创建或修改MAEC内容的所有工具和服务。

10.11 编拟工具或服务应鼓励重复使用现有恶意软件主体、行为、行动、对象和候选指标。

10.12 编拟工具或服务应方便用户启动为MAEC语言所书写文件的验证，并向用户报告所有W3C XML模式和Schematron错误。

10.13 编拟工具或服务须方便用户导入和编辑现有MAEC内容（包括所有MAEC输出格式）。

10.14 编拟工具或服务须方便用户导出作为有效MAEC输出格式文件创建的内容。

10.15 编拟工具或服务应向用户报告重复内容。

10.16 编拟工具或服务须提供由审查机构确定的、超出可扩展标记语言（XML）编辑器能力的价值和能力。

内容存储

这些要求适用于计划提供一系列MAEC内容的所有存储库。

10.17 存储库中每一个MAEC容器、软件包、恶意软件主体、分析、捆绑、行动、对象、行为、候选指标、行为系列、行动系列、对象系列和候选指标系列均须包含针对所有其他MAEC容器、软件包、恶意软件主体、分析、捆绑、行动、对象、行为、候选指标、行为系列、行动系列、对象系列和候选指标系列的独一无二ID。

10.18 每一个MAEC行动和对象都应包含针对所有其它MAEC行动和对象的一个ID，这一ID针对存储库中所有其它MAEC行动和对象都是独一无二的。

10.19 ID的命名空间部分须在所有MAEC内容方面都是恒定不变的，且针对存储库应是独一无二的。

10.20 每一个MAEC容器、软件包、恶意软件主体、分析、捆绑、行动、对象、行为、候选指标、行为系列、行动系列、对象系列和候选指标系列均须在其所有存在中拥有相同ID。现有项目不应被改写用于其它目的，因为用户可能在其自身内容中参引该项目。

10.21 存储库拥有方须记录用户进行内容检索更新的程序。

内容消费

这些要求适用于计划消费MAEC内容的所有工具和服务。请注意“消费”（以明智方法处理信息）和“解析”（从较大文件中摘录特定内容）之间的区别。

10.22 消费MAEC内容的工具或服务须至少消费一种类型MAEC输出格式（捆绑、软件包或容器）。

10.23 消费MAEC内容的工具或服务须支持每种类型MAEC输出格式的解析，以摘录其消费的任何嵌入式类型，无论相关类型在输出格式文件中的任何地点。例如，仅消费捆绑的工具或服务必须也能够解析软件包和容器，以摘录捆绑内容。

10.24 如果工具或服务仅需要与恶意软件实例相关的技术分析信息，则它应消费MAEC捆绑。

10.25 如果工具或服务需要与恶意软件实例相关的技术分析信息以及分析元数据和关系信息，则它应消费MAEC软件包。

10.26 如果工具或服务需要与多套或多组恶意软件实例相关的分析信息，则它应消费MAEC容器。

10.27 如果工具或服务在运行时不使用MAEC结果格式文件，则能力所有方须记录下该过程，通过它用户可以将MAEC结果格式文件提交给能力所有方，用于工具或服务的解释。文件须说明提交能力所有方的文件能多快提供给工具或服务。

11 审查机构的要求

以下是关于审查机构进行MAEC兼容性审查过程中须遵守的要求。

11.1 审查机构须清晰地区分能力审查版本、MAEC兼容性要求文件版本和MAEC语言版本，后者用于确定每个能力是否正式遵守了MAEC兼容性要求。

11.2 审查机构须具体规定能力的功能类型（内容创建、内容存储或内容消费）。

11.3 审查机构须定义和发布测试材料样本。

11.4 审查机构须公布如何参加正确性测试的信息，以使各组织可以提前做好准备。

11.5 审查机构须提供联系人，用于安排正确性测试，以便完成“MAEC兼容性问卷调查表”的能力声明支持MAEC。

11.6 审查机构可自行决定重新测试已被其正式确认与MAEC兼容的能力。

12 废止

如果审查机构已批准某能力为与MAEC兼容的能力，但是在稍后的时刻审查机构有证据表明其要求不再被满足，那么审查机构可以废止其批准，随后能力不再被正式确认为与MAEC兼容的能力。以下是审查机构在取消其确认时必须遵循的要求。

12.1 至少在废止发生的两（2）个月前，审查机构须对能力所有方发出废止警告。

12.2 审查机构可推迟废止日期。

12.3 如果审查机构发现能力所有方存在有意误导的行为或声明，那么审查机构可跳过警告期。审查机构可按照其意愿解释“有意误导”这一词句。

12.4 如果审查机构确定能力所有方在兼容性要求方面实施的行为存在故意误导，则废止须持续至少一年。

12.5 审查机构须确定未被满足的特定要求。

12.6 如果能力所有方认为要求都得到了满足，那么能力所有方须对废止警告做出回应，通过提供细节表明所述能力为何满足要求。

12.7 在警告期间，如果能力所有方修改能力使其符合所述要求，那么审查机构应结束关于该能力的废止行动。

12.8 审查机构须公布已废止相应能力为与MAEC正确兼容的正式确认。

12.9 审查机构可公布废止原因。

参考资料

[b-ITU-T X.1520] ITU-T X.1520建议书（2011年）– 常见漏洞和风险。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2014年，日内瓦