国　际　电　信　联　盟

ITU-T X.1217

(01/2021)

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

网络空间安全 – 网络安全

电信网络运营中的威胁情报使用导则

ITU-T X.1217建议书

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
消息处理系统	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	X.1080–X.1099
安全应用和服务（1）	
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（1）	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	
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（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	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指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1217建议书

电信网络运营中的威胁情报使用导则

摘要

从电信运营商的角度来看，威胁情报是经过组织、分析和提炼的关于可能威胁某个组织的潜在和当前攻击的信息集合。这些信息还可以包括攻击者的动机、意图、特征和方法，以及他们的操作方式或技术、战术和程序。

在网络和信息安全领域，大规模突发网络安全事件的发生引发了对威胁情报的迫切需求。威胁情报可以帮助一个组织降低风险，提高整体安全性。已经定义了威胁情报的统一分类、语法和表示，以便不同组织之间可以共享威胁情报。

ITU-T X.1217建议书规定了在进行概述分析后，在电信网络运营中使用威胁情报的导则。

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.1217	2021-01-07	17	11.1002/1000/14443

关键词

安全性，威胁情报。

* 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ID，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、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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，国际电联已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

从电信运营商的角度来看，威胁情报是经过组织、分析和提炼的关于可能威胁某个组织的潜在和当前攻击的信息集合。这些信息还可以包括攻击者的动机、意图、特征和方法，以及他们的操作方式或技术、战术和程序。

在网络和信息安全领域，大规模突发网络安全事件的发生引发了对威胁情报的迫切需求。威胁情报可以帮助一个组织降低风险，提高整体安全性。威胁情报可以通过了解谁最有可能发起攻击，将攻击什么，想要达到什么目的，为什么希望达成此目的以及计划如何实施，帮助一个组织降低风险，提高整体安全性。

[OASIS STIXv2]定义了用于交换网络威胁情报的语言和序列化格式。[OASIS taxiv 2]指定了一个用于交换HTTPS网络威胁情报的协议。[ITU-T X.1215]描述了如何使用结构化威胁信息表述（STIX）语支持提供网络威胁情报和进行信息共享。

已经定义了威胁情报的统一分类、语法和表示，以便不同组织之间可以共享威胁情报。下一个需要考虑的问题是如何利用威胁情报来解决网络中的安全问题。

[OASIS OpenC2-L]指定用于控制网络安全功能的命令和控制(C2)语言。[OASIS OpenC2-H]指定HTTPS的应用编程接口将OpenC2命令传输至网络安全设备。[OASIS OpenC2-P]指定使用OpenC2语言控制无状态防火墙。OASIS正在开发其他网络安全功能的配置文件。

本建议书规定了概述分析后使用威胁情报的导则。

ITU-T X.1217建议书

电信网络运营中的威胁情报使用导则

1 范围

本建议书规定了进行概述分析后在电信网络运营中使用威胁情报的导则。

2 参考文献

下列ITU-T建议书和其他参考文献包含的条款，通过本文的引用构成本建议书的条款。在出版时，所指示的版本有效。所有建议书和其他参考文献均可能进行修订；因此，鼓励本建议书的用户研究应用建议书最新版本和下面列出的其他参考文献的可能性。定期发布当前有效的ITU-T建议书清单。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T X.1215] Recommendation ITU-T X.1215 (2019), *Use cases for structured threat information expression*

[OASIS OpenC2-H] OASIS Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0, <https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html>

[OASIS OpenC2-L] OASIS Open Command Open Command and Control (OpenC2) Language Specification Version 1.0. <https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs01/oc2ls-v1.0-cs01.html>

[OASIS OpenC2-P] OASIS Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0, <https://docs.oasis-open.org/openc2/oc2slpf/v1.0/oc2slpf-v1.0.html>

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

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

3 定义

3.1 其他地方定义的术语

本建议书使用了其他地方定义的以下术语：

3.1.1 僵尸网络[b-ITU-T X.1231]：远程控制的恶意软件机器人，自主或自动地与由僵尸主控机拥有的服务器指令和控制一起运行于中病毒的计算机中。

3.1.2 欺诈[b-ITU-T Y.140.1]：通过虚假陈述或未经授权的行为获取金钱利益的行为。

3.1.3 恶意软件[b-ITU-T X.1211]：旨在专门破坏或干扰系统，攻击其保密性、完整性和/或可用性的恶意软件。

3.1.4 网络钓鱼[b-ITU-T X.1244]：在电子通信中，通过伪装成可信实体，违法并欺诈性地企图获得敏感信息，如用户名、密码和财务账号详细资料的行为。

3.1.5 漏洞[b-ITU-T X.1524]：所有可被用来破坏系统或系统所存信息的软件弱点（根据ITU-T X.1500 建议书）。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 数据清理：删除原始数据集中的无关数据和重复数据，用以平滑噪声数据、处理缺失值和异常值的过程。

3.2.2 数据裁剪：裁剪无用或异常数据的过程。

3.2.3 删除重复数据：删除原始数据集中重复数据的过程。

3.2.4 数据脱敏：隐藏敏感数据的过程。

3.2.5 数据筛选：删除无关数据，筛选原始数据集中无关数据的过程。

3.2.6 数据映射：将数据元素从源数据系统映射到目标数据系统的过程。

3.2.7 数据合并：将相似的数据记录合并成一条记录的过程。

3.2.8 数据挖掘：在大型数据集中发现模式的计算过程，涉及人工智能、机器学习、统计和数据库系统的方法。

3.2.9 数据降噪：平滑噪声数据的过程。

3.2.10 数据采样：处理缺失值和异常值的统计技术。

3.2.11 数据分段：从不同层次对数据进行分段的过程。

3.2.12 数据排序：按照一定的顺序或类别对数据进行排序的过程。

3.2.13 数据转换：将数据转换成某种格式，并将数据缩放到指定范围的过程。

3.2.14 事件收集：收集安全事件数据的过程。

3.2.15 态势感知：展示整体态势，预测可能的威胁和攻击的过程。

4 缩写和首字母缩略词

本建议书使用以下缩写和首字母缩略词：

API	应用编程接口
CVE	常见漏洞和暴露
C&C	命令和控制
DDoS	分布式拒绝服务
DNS	域名系统
FW	防火墙
GW	网关
HTTPS	超文本传输协议安全
ID	身份
IDS	入侵检测系统
IP	互联网协议
MD5	消息摘要算法 5
IPS	入侵预防系统

O&M 运营和维护

SDN 软件定义的网络

SIEM 安全信息和事件管理

SoC 安全运行中心

STIX 结构化威胁信息表述

TAXII 可信赖的自动情报信息交换

URL 统一资源定位符

WAF 网络应用防火墙

5 惯例

在本建议书中：

关键词“要求”（is required to）指的是一项必须严格遵守的要求，如果宣称遵循本建议书，则不得违反。

关键词“建议”（is recommended）指的是一项建议性的、并非绝对需遵守的要求，因此，宣称遵循本建议书时无需提及该项要求。

关键词“禁止”（is prohibited from）指的是一项必须严格遵循的要求，如果宣称遵循本建议书，则不得违反。

关键词“可选”（can optionally）指的是一项允许的可选要求，不隐含任何建议的意味。本术语无意暗示供应商的实施方案必须提供选项，以及网络运营商/服务提供商可以选择启用该功能。相反地，本术语意味着供应商可以选择提供该功能，并仍宣称遵循本规范。

6 威胁情报概述

从电信运营商的角度来看，威胁情报是经过组织、分析和提炼的关于可能威胁某个组织的潜在和当前攻击的信息集合。这些信息还可以包括攻击者的动机、意图、特征和方法，以及他们的操作方式或技术、战术和程序。

在电信网络运营中，威胁情报是用于防止或减轻网络攻击的知识，其内容包括攻击者的动机、意图、特征、方法、作案手法、技术、战术和程序。与个人可识别信息无关。

在网络和信息安全领域，大规模突发网络安全事件的发生引发了对威胁情报的迫切需求。威胁情报可以帮助一个组织降低风险，提高整体安全性。威胁情报可以通过了解谁最有可能发起攻击，将攻击什么，想要达到什么目的，为什么希望达成此目的以及计划如何实施，帮助一个组织降低风险，提高整体安全性。

[OASIS STIXv2]定义了用于交换网络威胁情报的语言和序列化格式。[OASIS TAXIIv2]指定了一个用于交换 HTTPS 网络威胁情报的协议。[ITU-T X.1215]介绍了如何使用结构化威胁信息表述（STIX）语支持提供网络威胁情报和进行信息共享。

现已经定义了威胁情报的统一分类、语法和表示，以便不同组织之间可以共享威胁情报。下一个需要考虑的问题是如何利用威胁情报来解决网络中的安全问题。

[OASIS OpenC2-L]指定用于控制网络安全功能的命令和控制(C2)语言。[OASIS OpenC2-H]指定 HTTPS 的应用编程接口将 OpenC2 命令传输至网络安全设备。[OASIS OpenC2-P]指定使用 OpenC2 语言控制无状态防火墙。OASIS 正在开发其他网络安全功能的配置文件。

7 威胁情报在电信网络运营中的使用综述

图 7-1 显示了威胁情报在电信网络运营中的应用。

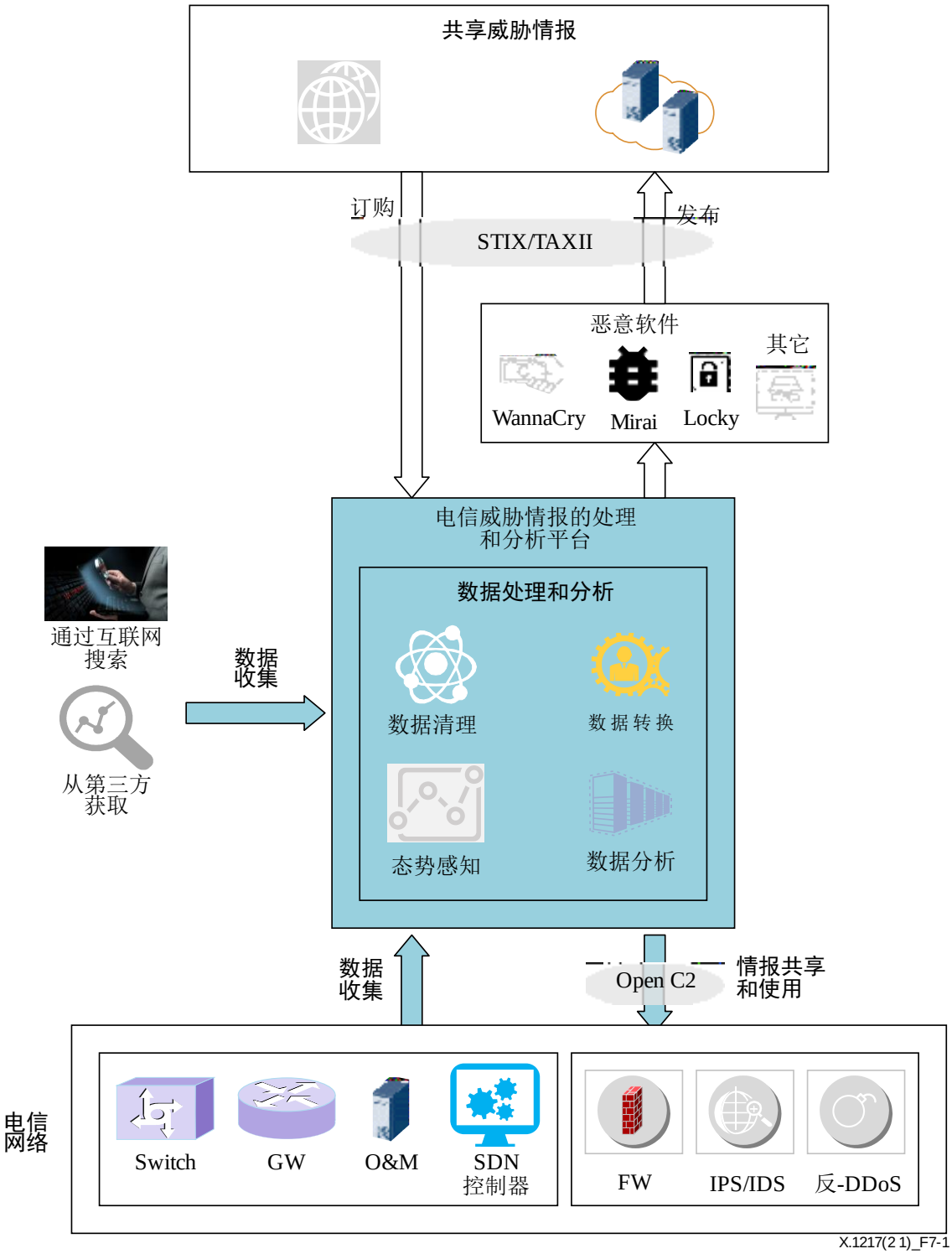

图7-1 – 在电信网络运营中使用威胁情报

根据图 7-1，在电信网络运营中使用威胁情报涉及三个主要过程：数据收集、数据处理和分析以及情报共享和使用。

7.1 数据收集

威胁情报的数据源有两种：

- 来自内部网元和安全设备的数据；
- 外部来源的数据。

来自内部网元和安全设备的数据主要包括日志、告警和安全策略，如事件日志、域名系统（DNS）日志、防火墙日志等。

另外还有一些从外部收集数据的特定来源，如通过互联网搜索、通过 STIX/TAXI 从第三方获取等。共享数据主要包括 IP、域、URL、事件、漏洞等。

在收集数据之前，需要进行数据脱敏。

7.2 数据处理和分析

数据处理和分析包括四个功能组件：数据清理、数据转换、数据分析和态势感知。

图 7-2 说明了数据处理和分析的功能组件。

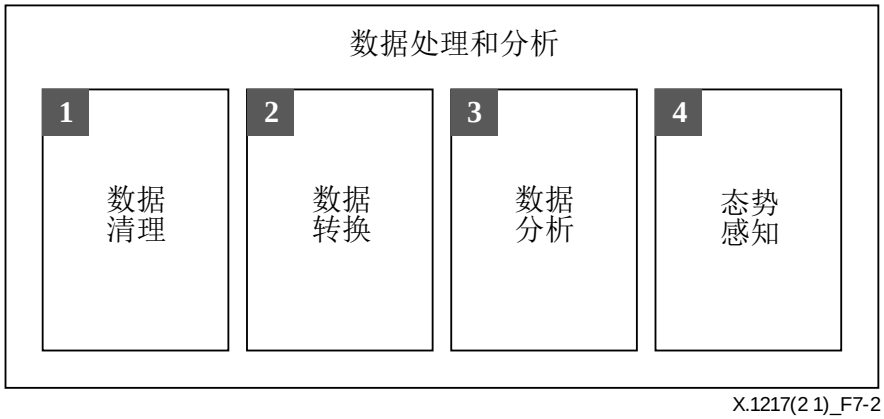

图7-2 – 数据处理和分析的功能组件

- 通过数据清理删除原始数据集中的无关数据和重复数据，以平滑噪声数据，处理缺失值和异常值。
- 数据转换包括数据集成和数据规范化。
  - 数据集成是以某种格式统一多个数据源的存储。
  - 数据规范化旨在消除指标之间的维度和取值范围的影响，将数据缩放到指定的范围，包括函数转换和属性构造等。
- 数据分析使用各种算法分析数据、提取关键字、清除规则、建立分析关联，以获取威胁情报信息并分析相应的对策。
- 态势感知包括可视化和预测性警告。
  - 可视化是通过分析数据实现对整体情况的可视化显示，如分类、排序等。
  - 操作预测警告是指通过数据分析和整体情况预测威胁、攻击路径、攻击方法等的可能范围并发布预警，从而给出防御可能攻击的安全策略。

7.3 情报共享与使用

情报共享和使用包括两个方面。

- 根据威胁情报，运维管理员可以对网元和安全设备应用安全策略。
- 威胁情报可以与第三方共享。

电信网络运营中共享和使用的威胁情报包括威胁情报信息、预警信息、网络安全对策等。

电信网络运营中的情报共享和使用对象包括网元和安全设备，如入侵检测系统（IDS）、入侵防御系统（IPS）、防火墙和反分布式拒绝服务设备。当涉及到在安全设备中使用安全命令和控制时，建议使用OASIS OpenC2规范。

在电信网络运营中，情报共享和使用的目标是预防和减少安全事件，同时实现对电信网络中每一安全事件的快速有效响应。

8 电信网络运营中使用威胁情报的指南

第 7 条描述了三个主要过程：数据收集、数据处理和分析、情报共享以及在电信网络运营中使用威胁情报。在电信网络运营中使用威胁情报的指南在条款8.1 至 8.3中有相应规定。

8.1 数据收集

收集数据是使用威胁情报的前提，其目的是收集所有与威胁情报相关的信息和数据。我们建议收集的数据包括来自内部网元和安全设备的数据，例如日志、警报和安全策略。同时，我们亦建议数据涵盖外部来源的数据，如通过互联网搜索的数据、从第三方获取的数据等。共享数据主要包括 IP、域、URL、事件、漏洞等。

我们建议实施主动的数据收集，收集 DNS 日志、防火墙日志等数据。另外，我们建议采取事件收集的方式收集与安全事件相关的数据。建议采取情报收集的方式收集 IP、域、URL、事件、漏洞等关键情报。

如果数据是从内部网元和安全设备收集的，则可按照事件信息或僵尸网络活动等不同活动类型收集数据。

事件信息可以从入侵检测系统设备、入侵防御系统设备、网络应用防火墙（WAF）、反分布式拒绝服务设备、安全信息和事件管理（SIEM）平台和安全操作中心（SoC）平台收集。推荐收集的事件信息包括事件的名称、描述、类别和受影响的资产。我们建议在收集的事件信息中纳入事件发生的时间。僵尸网络活动可以从 DNS 设备、IDS、WAF、反分布式拒绝服务设备等相关设备收集。我们建议收集的僵尸网络活动信息包括僵尸网络活动的名称、描述、类别和受影响的资产。另外，还建议将僵尸网络活动发生的时间包括在内。

如果数据是从互联网上收集的，则可依照漏洞信息、恶意域、恶意 URL、恶意 IP 地址、事件信息等不同数据类型实施数据收集。

漏洞信息可以从共同漏洞与暴露（CVE）网站等漏洞网站收集。我们建议收集的漏洞信息包括漏洞的标识、名称、描述、类型、受影响的版本、受影响的供应商、受影响的产品等。

恶意域名和网址信息可分为不同威胁类型的命令和控制（C&C）、僵尸网络、恶意软件、木马代码、网络钓鱼、欺诈等。恶意域名和网址信息可以从网站、供应商报告、第三方安全报告等中收集。建议收集的恶意域名和 URL 信息包括域名服务器、DNS 类型、威胁类型、可信度等。

恶意 IP 地址信息可以从各种网站和一些供应商和安全公司收集。恶意 IP 地址可分为不同威胁类型的分布式拒绝服务、攻击、垃圾邮件来源、网络攻击、僵尸网络、恶意软件、C&C 等。建议收集的恶意 IP 信息包括 IP、威胁类型、可信度等。

事件信息可以从安全新闻或供应商报告中收集。建议收集的事件信息包括事件的名称、描述、类别和受影响的资产。

从第三方获取的数据主要包括 IP、域名、URL、事件、漏洞等。每种类型的信息都与上述内容相同。

当从内部网元和安全设备收集数据时，我们建议通过自动化工具或脚本收集数据。当从外部来源收集数据时，则建议通过使用脚本或数据交换和共享机制收集数据。另外，我们建议收集数据的后续处理遵循[OASIS STIXv2]和[OASIS TAXIIv2]定义的标准格式。在共享威胁情报方面，建议数据收集遵循[OASIS STIXv2]和[OASIS TAXIIv2]定义的标准格式。

建议数据脱敏工作在数据收集之前进行，因为数据脱敏是用字符或数据隐藏原始敏感数据的过程，目的是保护敏感数据。

8.2 数据处理和分析

8.2.1 数据清理

数据清理是使用威胁情报的主要步骤之一，目的是对收集到的数据进行清理，使其成为统一的有用数据，为数据转换和数据分析做好准备。

– 建议实施数据筛选、数据降噪并删除重复数据。

– 建议实施数据筛选，删除无关数据，筛选原始数据集中的无关数据。

– 建议实施数据降噪并删除重复数据，以平滑噪声数据并删除原始数据集中的重复数据。

由于收集的数据包含入侵防御系统、域、URL、事件、漏洞等不同类型的数据，因此根据收集的数据，数据清理可能会有所不同。

删除重复数据主要是消除那些重复的数据，以节省存储空间。不同数据类型的标准不同。针对 IP 信息数据，如果 IP 地址相同而威胁类型、可信度等记录的其他部分相同，则认为其是重复数据，需要去重，否则需要合并。针对域名信息，如果域名服务器、DNS 类型、威胁类型、可信度的记录都相同则为重复数据，需要去重，否则需要合并。针对漏洞信息，如果漏洞标识相同则是重复数据，需要删除重复数据。对于其他类型的数据，建议计算相似率，如果相似率高于阈值，则需要删除重复数据。

我们建议将类似的信息合并到一条记录中。对于 IP、域、URL 和事件信息的类型，如果 IP、域名服务器、URL 和事件描述与另一信息相同，那么可以合并成一个记录。对于其他一些数据类型，可以计算相似率。如果相似率在阈值内，则需要合并信息。

– 建议实施数据采样、数据合并和数据排序，以处理缺失值和异常值，并使数据对后一过程更加有用。

– 建议使用自动化工具进行数据筛选并消除重复数据。

8.2.2 数据转换

数据转换旨在消除指标之间的维度和取值范围的影响，将数据缩放到指定的范围，（包括函数转换和属性构造等）并将清理后的数据转换为统一格式的数据，为数据分析做好准备。

为实现数据转换，建议使用数据映射、数据裁剪和数据分割，将其转换为有价值的有用数据。另外建议进行拼写转换，将不同的拼写转换为统一拼写。格式标准化工作建议将多个数据源的数据做成一定的格式。建议实施数据融合，以实现多源统一存储。

各种类型的 IP、域、网址和事故漏洞数据转换程序均相似。对于每种类型，建议使用不同的数据映射规则。例如，事件信息的数据映射规则是将名称、描述、类别和受影响的资产字段转换为标准格式字段。建议将防火墙（FW）信息（如映射时间戳、请求 URL、主机名、攻击类型、攻击内容）映射至定义的格式。

对于数据裁剪和数据分割，建议通过自动化工具实现数据转换过程。对于拼写转换，建议由自动化工具实现数据转换过程。在格式标准化方面，建议数据转换过程遵循[OASIS STIXv2]和[OASIS TAXIIv2]定义的标准格式。

8.2.3 数据分析

数据分析是利用威胁情报使用各种算法分析转换数据、提取关键词、明确规则、建立分析关联等的关键步骤，以此获取威胁情报信息并分析相应的对策。

为开展数据分析，建议进行数据检索和数据挖掘，获取关键的威胁情报信息，从而生成警告或相应的对策。我们建议实施行为分析和事件关联分析，以便找到IP地址、域名、哈希摘要、攻击者信息、响应动作等有用的威胁情报。建议实施知识映射和威胁搜索，以获取深层威胁情报信息并采取对策和响应。

例如，DNS日志的机器学习算法可用于检测僵尸网络C&C。建议将FW日志与威胁源、类型、攻击时间等信息结合，共同计算威胁水平。URL 和 IP 信息可用于计算可信度。

建议自动实施数据分析算法。建议数据分析结果遵循[OASIS STIXv2]和[OASIS TAXIIv2]定义的标准格式。

8.2.4 态势感知

态势感知利用分析数据进行趋势预测和预警，同时显示全局。

为获得态势感知，我们建议实现态势可视化，从而通过分析数据显示整体态势。建议使用趋势预测和警告预测威胁的可能范围、攻击路径、攻击方法等。通过数据分析和整体情况并发布预警，提供防御可能攻击的安全策略。态势感知方法是基于包括机器学习、线性分析、概率统计和人工智能在内的算法。

建议自动实施趋势预测和预警。建议趋势预测和警告结果遵循[OASIS STIXv2]及[OASIS TaxiV 2]定义的标准格式。在态势可视化和显示方面，建议使用可视化工具显示整体数据态势。

8.3 情报共享和使用

情报共享和使用的目的是防止或减少安全事件，并对电信网络中的每个安全事件做出迅速有效响应。

从数据处理和分析阶段获得的情报包括威胁信息、预测警告信息、网络安全对策、安全策略等。这些情报可以与电信运营商的不同部门共享。情报共享可以采用多种形式。例如，可以以报告和咨询的形式共享。或者也可以以检测指标的形式共享。

建议从网元、安全设备、报警中心等处获取情报。运维管理员可以根据获得的情报生成安全策略，并将这些安全策略部署到网元和安全设备中。如有必要，管理员还可以更新软件版本并修改网元和安全设备的配置。

我们建议将 URL 类情报用于网关，然后网关可以通过将恶意网址加入黑名单的方式更新安全策略。建议使用对相应 URL 更新保护规则的方式，将其应用于 IDS 或 IPS。

建议将恶意域类型的情报用于 DNS 服务器，通过将恶意域设置进黑名单更新配置。

建议将恶意 IP 类情报用于防火墙，防火墙可以通过筛选恶意 IP 地址更新其安全策略。防火墙也可以通过使用相应 IP 地址更新保护规则的方式用于 IDS 或 IPS。

建议将漏洞类情报用于网元，通过更新软件或硬件修复漏洞。同时，其可以选择性地用于制作检测插件，然后用于更新检测扫描仪。该情报可以选择性地用于应急响应系统，以识别事件并帮助采取行动来防止攻击。

建议情报遵循[OASIS STIXv2]和[OASIS TAxiv 2]定义的标准格式。建议安全命令和控制使用 OASIS OpenC2 规范。

参考书目

[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*.

ITU-T 系列建议书

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦