国 际 电 信 联 盟

ITU-T X.1060

国际电信联盟
电信标准化部门

（06/2021）

X系列：数据网、开放系统通信和安全性

信息和网络安全 – 安全管理

创建和运营网络防御中心的框架

ITU-T X.1060 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
IMT-T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.1060 建议书

创建和运营网络防御中心的框架

摘要

ITU-T X.1060建议书将网络防御中心（CDC）定义为在组织中发挥核心作用以应对网络安全风险的一个实体。CDC应实际实施的三个过程（建造、管理和评估）被描述为一个框架。还提供了组织为实施更具体的网络安全措施而应拥有的服务。

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.1060	2021-06-29	17	11.1002/1000/14721

关键词

网络防御中心，CIRT，安全运营中心（SOC）。

* 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

组织中的网络安全风险对其整体活动有重大影响。组织面临的风险是环境变化（从社会和业务角度来看）以及法规和不断增加的威胁带来的外部压力。因此，作为C-套件（CxO）的最高管理层负责管理整个组织的控制措施，以应对这些风险和变化。作为在网络安全中实施控制的一个重要方面，在制定和控制符合业务目标之安全政策方面的领导力是预期的，通常由首席安全官（CSO）或首席信息安全官（CISO）来提供。为了切实执行安全措施，基本上需要一个在组织一级进行战略管理的实体来支持CSO或CISO的活动。该实体在本建议书中被描述为网络防御中心（CDC）。

本建议书为CDC的建造和管理及其有效性的评估提供了一个框架。该框架指明了CDC应如何确定和实施安全服务，以实现组织的安全性。该框架有助于组织应对其网络安全风险。

ITU-T X.1060 建议书

创建和运营网络防御中心的框架

1 范围

本建议书为组织建造和管理网络防御中心（CDC）并评估其有效性建立了一个框架。该框架指明了CDC应如何确定和实施安全服务，以实现组织的安全性。

本建议书适用于组织最高管理层负责安全的人员，如首席安全官（CSO）或首席信息安全官（CISO）以及协助他们的安全主管。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITU-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

3 定义

3.1 他处定义的术语

本建议书使用下列他处定义的术语：

3.1.1 外包[b-ITU-T X.1053]：企业将其一个或多个内部流程和/或功能外包给外部公司。外包将企业资源转移到外部企业，并保留管理与外包流程之关系的能力。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 网络防御中心（CDC）：组织内提供安全服务以管理其业务活动之网络安全风险的实体。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

APT 高级持续威胁

CDC 网络防御中心

CISO 首席信息安全官

CSIRT 计算机安全事件响应小组

CSO 首席安全官

CxO C-套件

IDS 入侵检测系统

IPS 入侵防御系统

IT 信息技术

SIEM 安全信息和事件管理

SLA 服务水平协议

WAF 网络应用防火墙

5 惯例

无。

6 本建议书的结构

在本建议书中，第7节解释了CDC的概念。第8节概述了用于创建和运营CDC的框架。在随后的章节中对该框架做了详细描述：CDC建造过程（第9节）；CDC管理过程（第10节）；以及CDC评估过程（第11节）。在第12节中，作为最佳做法，对由CDC提供的安全服务做了整体描述，并在附件A中对每个服务做了进一步的详细描述。

7 网络防御中心概述

组织采取行动使之业务取得成功。为了管理业务活动面临的风险，CISO制定安全策略，尤其从网络安全角度。CDC是一个实体，作为CDC服务，它专门实施安全策略（由负责安全的小组所执行的安全活动组成）。CDC服务可以指定安全功能，作为执行安全相关处理工作的系统的功能。图1显示了利益攸关方及其有关CDC运营的角色。

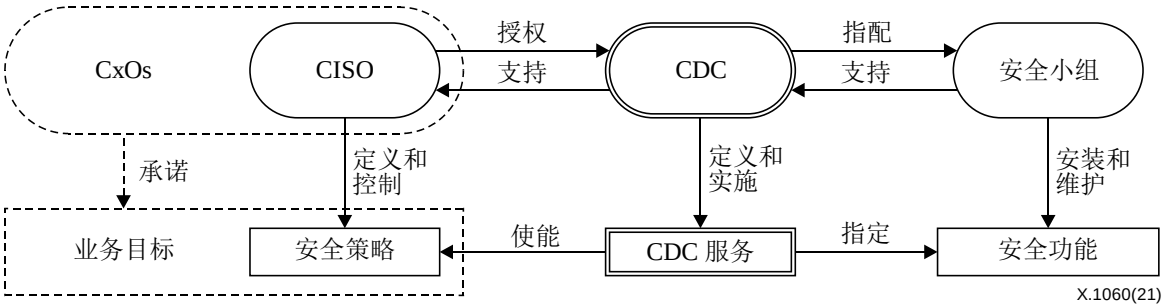

图 1 – 利益攸关方及其有关CDC运营的角色

根据组织的规模和类型，CDC可以是一个独立的单位、一个委员会或一个小的团队。无论其格式如何，它都应作为组织中的一个实体而存在，并拥有实施安全服务的权限和资源，以确保组织的安全。这种安全服务应符合安全策略的要求，并确保安全活动的质量；每项服务的水平都应通过文档化的安排来明确约定，例如，服务水平协议（SLA）。CDC安全服务的整体质量通过第9.4节中指定的措施进行评估。

8 创建和运营CDC的框架

图2显示了用于创建和运营CDC的框架。该框架包括三个过程：建造、管理和评估。为确保组织的安全稳固，应建立和适当管理CDC。也应该以一种及时和规则的方式来对之进行评估，并持续予以改进。本框架使组织能够维持安全活动。

在建造过程中，应考虑组织中的安全活动。CDC安全服务的最佳做法列于附录A中。一个组织可以通过从清单中选择服务并添加特定于组织的服务来建立自己的服务目录。目录中的每个服务还应建立一个配置文件，其中包括：所有者、角色和职责以及服务指配类型（内包、外包或组合）。一旦建立服务配置文件，就应确定用于评估过程的、每个CDC服务的当前和目标分数。

管理过程有三个阶段和两个循环。战略管理阶段管理CDC的整体活动，运营阶段管理有关监测和分析的日常工作，响应阶段管理应急响应。对这些阶段在短循环和长循环中都进行管理；运营和响应需要在短循环中及时做出决定。同时，战略管理应考虑长期改进以及来自一个长循环中各短循环的输出。长期改进通常需要对新业务投资做出决策并对系统架构进行彻底更改。

评估过程对CDC服务的目录、配置文件和组合进行评估（参见图4），应在每个适当时间对之做出客观评估。

应对评估结果进行审查，并体现在所有三个CDC过程中。应在组织中建立和维持有关建造、管理和评估过程的反复循环，以改进安全活动。

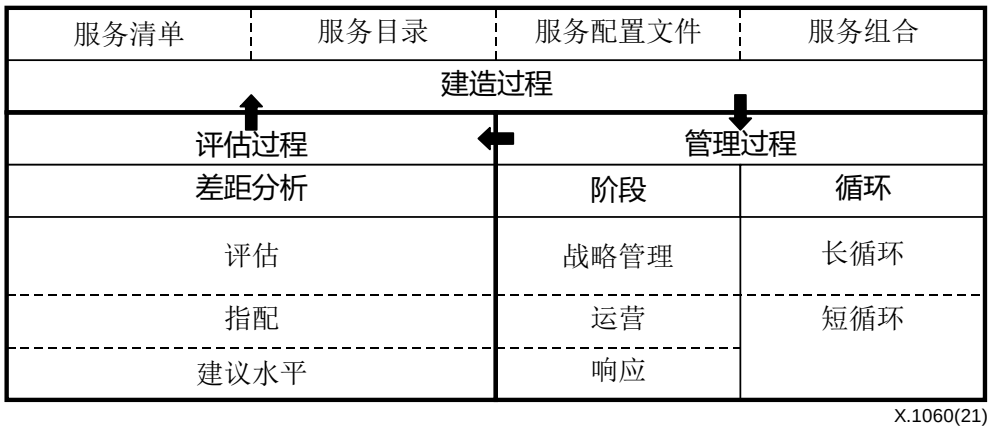

图 2 – 创建和运营CDC的框架

9 建造过程

9.1 概述

CDC有一个建造过程来确定应在组织中实现哪些安全服务。要实现的候选服务选自CDC服务清单，该服务清单基于组织的最佳做法。对于CDC服务清单，请参见第12节。

图3显示了为CDC建造服务的三个阶段。

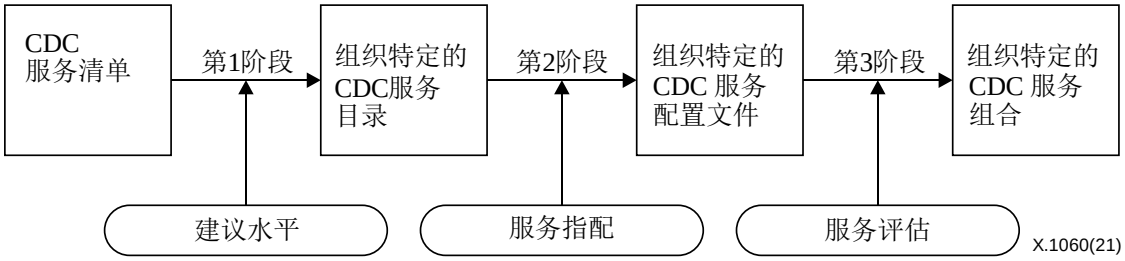

图 3 – 为CDC建造服务的阶段

1) 第1阶段：创建CDC服务目录

本组织应首先创建一个CDC服务目录。

在此阶段，从总的服务清单中提取要实施的候选服务。总的清单的详细信息在第12节中描述。如果有缺失的服务，那么应新定义此类服务并添加到CDC服务目录中。

2) 第2阶段：创建CDC服务配置文件

对于CDC服务目录中列出的服务，组织应确定提供服务之团队的角色和责任。在此阶段，应考虑第9.3节中所述的CDC服务指配。

因此，组织应生成CDC服务配置文件。

3) 第3阶段：创建CDC服务组合

在确定CDC服务配置文件后，组织应测量每个服务的当前服务分数（当前），并设置中长期目标服务分数（未来）。

一旦设置了当前和未来的水平，组织应生成CDC服务组合。

图4显示了CDC服务的一个示例矩阵。将在第1阶段到第3阶段后填充该矩阵。

服务	建议水平	服务指配	服务分数	
			当前	未来
服务示例 1	基本的	内包 (AB Dept.)	3	5
服务示例 2	标准的	外包 (Z-MSSP)	2	4
服务示例 3	高级的	不可指配	1	2

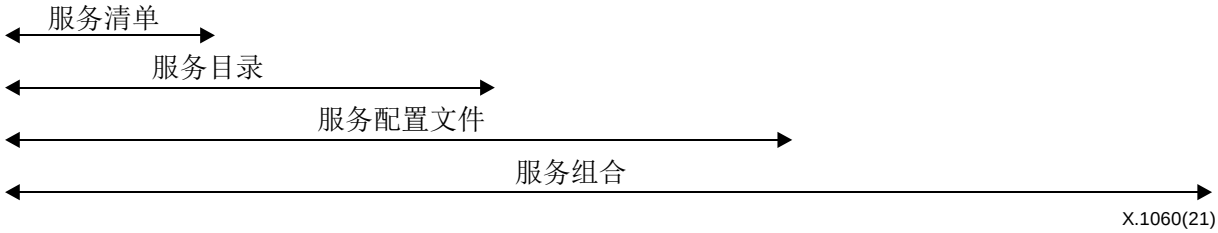

图 4 – CDC的服务矩阵

9.2 CDC服务建议水平

要为组织实现最合适的CDC服务，可在表1中列出的五个水平上来对每项服务的必要性进行考虑。服务实现的优先级可以通过测量水平来阐明。

表 1 – CDC服务建议水平

权重	描述
不必的	服务认为是不必要的
基本的	要实现的最低服务
标准的	通常建议实现的服务
高级的	实现更高级CDC循环所需的服务
可选的	根据CDC的预期形式任意选择的服务

9.3 CDC服务指配

组织应该明确哪个团队应实施CDC服务。根据在组织中实施服务的能力，组织应确定CDC服务指配，这可能包括外包。参见表2。

表 2 – CDC服务指配

类型	描述
内包	服务由组织内的一个团队来提供。组织应指定负责的团队。
外包	服务由组织外的一个团队来提供。组织应指定外包者。
组合	组织一起使用内包和外包。应由组织来指定负责的团队和承包商。
未指配的	虽然组织认可服务，但组织中没有任何受让者。

使用外包时，应明确点A)和B）。

A) 所处置信息的性质

组织应对所处置信息的性质进行分类，包括对组织的“内部”和“外部”的定义或区分。例如，在发生事故的情况下，包括攻击造成的损害或影响在内的信息应被视为内部信息，而关于攻击本身的信息应被视为外部信息。

B) 需要专门的安全技能

组织应考虑是否需要安全领域的专业技能来提供服务。

基于这两个指标点，可将CDC服务划分为象限I)到象限IV)。参见图5。

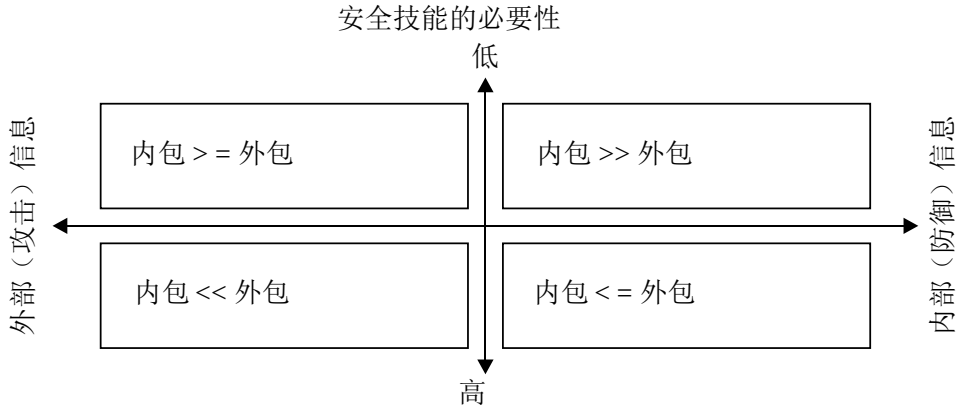

图 5 – 采购象限

I) 内包 >> 外包

当不需要安全专业技能来处置组织内的机密信息时，内包是最佳，外包非首选。

II) 内包 >= 外包

如果需要的专业技能并不那么高，虽然它是组织外部的信息，也应主要由组织来完成活动和管理，并由外包来提供支持。

III) 内包 << 外包

为了处置主要有关攻击的信息，它在组织外部，应由具有专业技能的组织来提供服务（例如，外包）。除非内部有具有专业技能的专家，否则组织本身很难提供服务。

IV) 内包 <= 外包

当需要专业技能来处置组织内的内部信息时，应主要由专门组织来完成活动（例如，外包），组织应提供管理和支持。

9.4 CDC服务评估

创建CDC服务组合时，应使用表3中列出的服务分数来评估每个服务当前和未来的实施状态。应该注意的是，不同的服务类型，例如内包和外包，应根据指配给服务分数的标准来进行评估。

表 3 – CDC服务分数

对内包	
记录的操作由CISO或其他具有适当职责的组织负责人来授权	+5 分
对操作做记录，其他操作可以发挥现有运营商的作用	+4 分
不对操作做记录，其他操作可以暂时发挥现有运营商的部分作用	+3 分
不对操作做记录，且现有运营商可以发挥作用	+2 分
操作不起作用	+1 分
决定不通过内包来实施	N/A

对外包	
了解服务内容和预期输出，且其输出如预期	+5 分
了解服务内容和预期输出，但其输出不如预期	+4 分
不了解服务内容或不了解预期输出	+3 分
不了解服务内容也不了解预期输出	+2 分
对输出和报告都不做审查	+1 分
决定不通过外包来实施	N/A

10 管理过程

CDC通过实施CDC管理过程，在整个组织中实现安全活动，这包括如图6所示的三个阶段和两个循环。

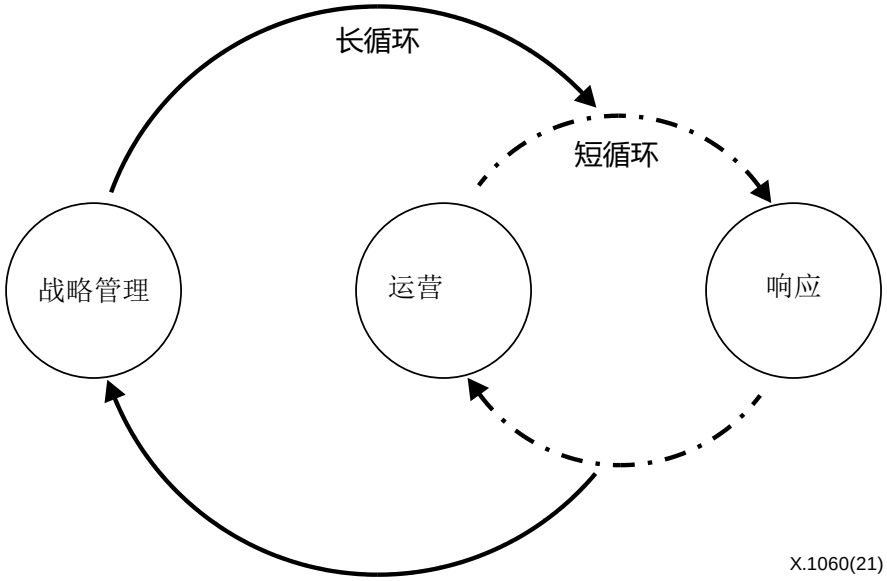

图 6 – CDC管理过程

(1) 战略管理阶段

战略管理负责所有与定义、设计、规划、管理、认证等相关的战略服务，确保CDC的长期发展。

(2) 运营阶段

对引入之框架的维护工作应在运营阶段进行。这是平时或平常的工作，通常包括日常活动，例如，事件检测分析、安全响应系统的监测和维护。负责此类运营的团队通常被称为安全运营中心（SOC）。

(3) 响应阶段

当通过运营阶段的分析检测到某个事件时，应执行事件响应。该阶段始终是一种应急状态。响应事件的团队通常被称为计算机安全事件响应小组（CSIRT）。

对响应阶段的输入不限于来自运营阶段的输入，团队还应涵盖来自第三方的、对报告或通知所做的响应。

A) 短循环

运营和响应每天进行。在这些过程中，在安全响应系统的业务过程和事务中总会出现问题。因此，在短循环内分配的资源（人员、预算、系统）内，需要持续改进以解决这些问题，例如，简单任务的简单自动化、用于分析精度之工具的改进以及报告事项的审查等。

B) 长循环

需要分配新资源的审查应适用于长循环。

如果在审查短循环时发现任何当前系统无法解决的问题，那么应从长期的观点和计划角度来考虑响应，例如，引入新的安全产品、对安全策略进行彻底审查以及对安全系统进行大规模配置更改。

11 评估过程

11.1 概述

应该以一种及时和规则的方式来评估在建造过程中制定的CDC服务的目录、配置文件和组合。图7描绘了用于评估CDC服务的过程。

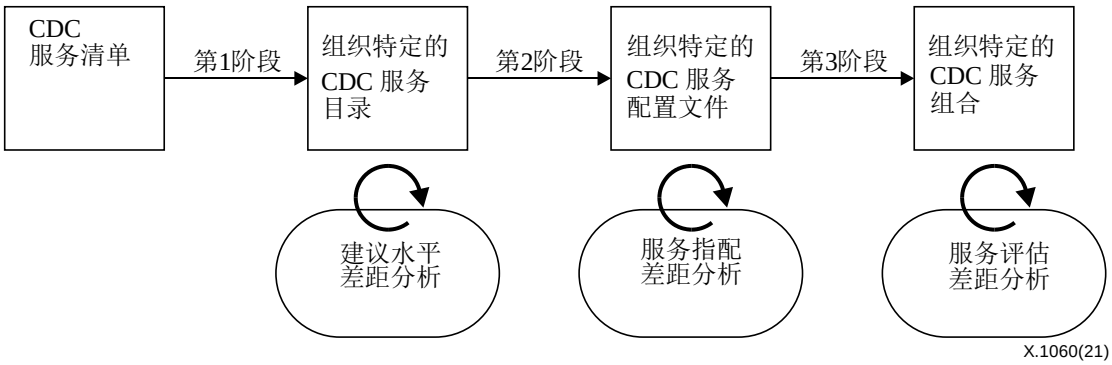

图 7 – CDC评估过程

11.2 CDC服务目录评估

应对CDC的服务建议水平进行差距分析。由于环境和威胁的变化，需要进行审查，特别是应对“不必要的”服务进行重新检查和审查，以确保没有遗漏。当业务引入变化时，如开始新的业务活动、响应新的风险和威胁时，应对CDC服务目录进行评估。

11.3 CDC服务配置文件评估

应对CDC的服务指配进行差距分析。通过确定服务指配，可以消除“不可指配的”服务，组织可以通过审查它们来改进成熟度水平。当组织变化发生时，例如内包类型的内部组织发生变化和外包类型的外包商发生变化，应对CDC服务配置文件进行评估。

11.4 CDC服务组合评估

应对单个服务的CDC服务分数进行差距分析。应明确“未来”目标分数与“当前”目标分数之间的差异，以便组织能够关注需要改进的地方，再次确认CDC服务分数并提取问题。应定期对CDC服务组合进行评估。

12 CDC服务类别和服务清单

在建造和管理过程中需要CDC服务类别和清单（参见第9节和第10节）。

CDC服务有九个服务类别：

A) CDC的战略管理；

B) 实时分析；

C) 深度分析；

D) 事件响应；

E) 检查和评估；

F) 威胁情报的收集、分析和评估；

G) CDC平台的开发和维护；

H) 支持内部欺诈响应；

I) 与外部各方的积极关系。

A. CDC的战略管理

本类别包括在组织（包括CDC）中有关类别A)到I)中提及之所有安全活动的策略和资源规划，以确保其稳定运营。

B. 实时分析

本类别不断监测和分析来自各种系统的日志和数据，例如，网络设备、服务器和安全产品。目标是实时发现威胁，这可带来快速和适当的事件响应。

C. 深度分析

这是与事件相关的一个类别，例如，调查受影响的系统、审查受损的数据，并分析攻击中使用的工具和方法。

目的是阐明事件的全部范围并确定影响。

D. 事件响应

本类别根据实时分析结果和威胁信息采取具体措施，以阻止和消除威胁。

目的是尽量减少对系统和业务的影响，包括与利益攸关方的协调和报告。

E. 检查和评估

本类别用于待保护系统的漏洞评估、事故响应培训及其评估。本类别的目的是提高安全水平。

F. 威胁情报的收集、分析和评估

本类别收集在互联网上可得的、关于漏洞和攻击的威胁信息（外部情报），并处理关于实时分析和事件响应的信息（内部情报）。

目的是提高实时分析和事件响应的精度，并改善安全资产。

G. CDC平台的开发和维护

本类别管理、改进或开发安全响应所需的新系统（例如，安全产品、日志收集数据库和操作系统）。

目的是在其他类别中实现平滑和可持续的安全活动。

H. 支持内部欺诈响应

本类别收集审计数据以支持对内部欺诈做出响应。

本类别的目的是通过提供日志和分析来支持对内部欺诈的响应和问题解决。

I. 与外部各方的积极关系

本类别包括与内部利益攸关方和外部组织的协调和协作。

目的是提高组织的安全水平，增加组织的安全价值，从而进一步发展和加强组织。

图8显示了服务类别与管理过程的映射，表4列出了各服务。

对CDC服务清单中每个服务的详细描述在附件A中提供。

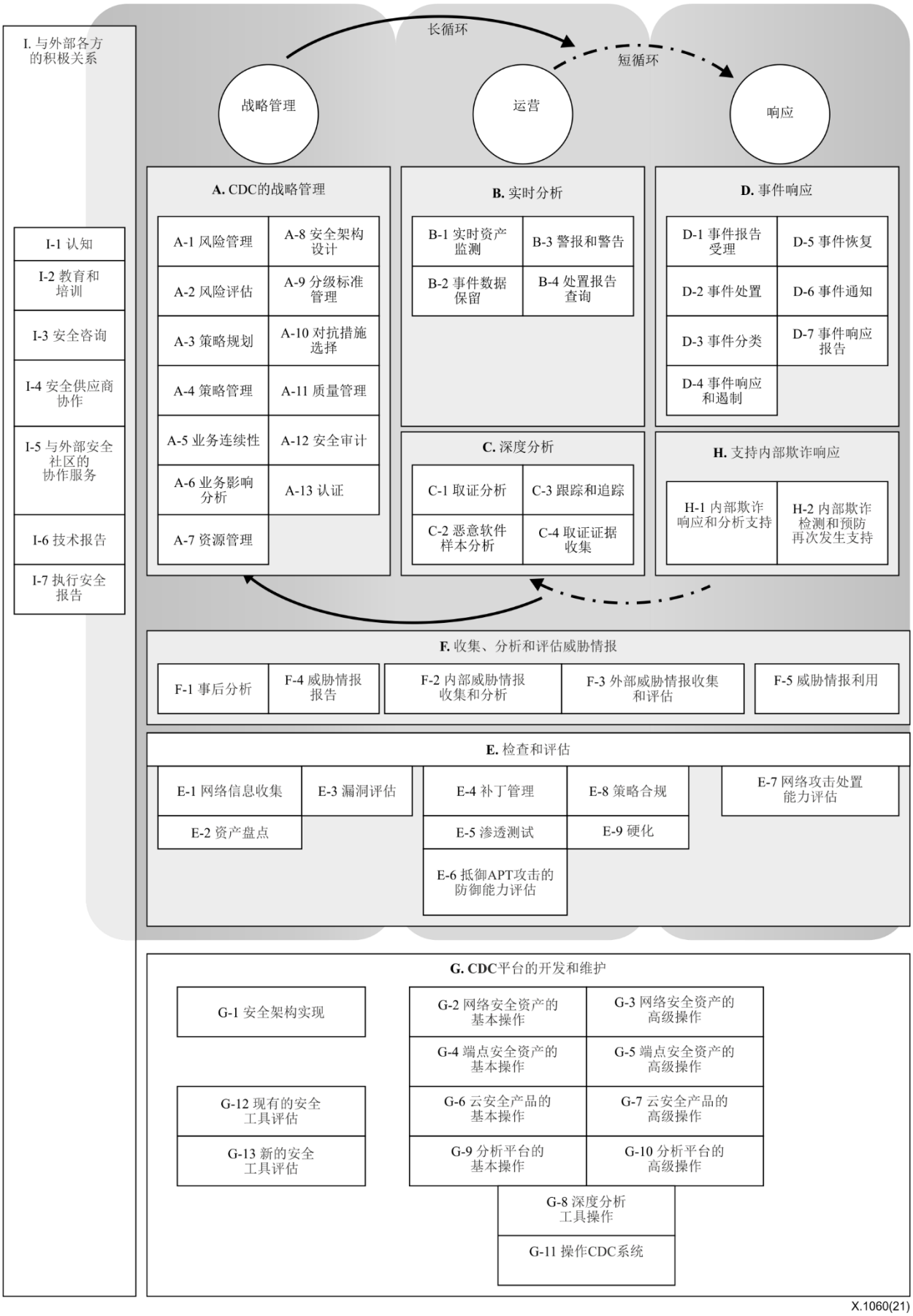
I. 与外部各方的积极关系
I-1 认知
I-2 教育和培训
I-3 安全咨询
I-4 安全供应商协作
I-5 与外部安全社区的协作服务
I-6 技术报告
I-7 执行安全报告
长循环
短循环
战略管理
运营
响应
A. CDC的战略管理
A-1 风险管理
A-8 安全架构设计
A-2 风险评估
A-9 分级标准管理
A-3 策略规划
A-10 对抗措施选择
A-4 策略管理
A-11 质量管理
A-5 业务连续性
A-12 安全审计
A-6 业务影响分析
A-13 认证
A-7 资源管理
B. 实时分析
B-1 实时资产监测
B-3 警报和警告
B-2 事件数据保留
B-4 处置报告查询
C. 深度分析
C-1 取证分析
C-3 跟踪和追踪
C-2 恶意软件样本分析
C-4 取证证据收集
D. 事件响应
D-1 事件报告受理
D-5 事件恢复
D-2 事件处置
D-6 事件通知
D-3 事件分类
D-7 事件响应报告
D-4 事件响应和遏制
H. 支持内部欺诈响应
H-1 内部欺诈响应和分析支持
H-2 内部欺诈检测和预防再次发生支持
F. 收集、分析和评估威胁情报
F-1 事后分析
F-4 威胁情报报告
F-2 内部威胁情报收集和分析
F-3 外部威胁情报收集和评估
F-5 威胁情报利用
E. 检查和评估
E-1 网络信息收集
E-3 漏洞评估
E-2 资产盘点
E-4 补丁管理
E-8 策略合规
E-5 渗透测试
E-9 硬化
E-6 抵御APT攻击的防御能力评估
E-7 网络攻击处置能力评估
G. CDC平台的开发和维护
G-1 安全架构实现
G-2 网络安全资产的基本操作
G-3 网络安全资产的高级操作
G-4 端点安全资产的基本操作
G-5 端点安全资产的高级操作
G-12 现有的安全工具评估
G-6 云安全产品的基本操作
G-7 云安全产品的高级操作
G-13 新的安全工具评估
G-9 分析平台的基本操作
G-10 分析平台的高级操作
G-8 深度分析工具操作
G-11 操作CDC系统
X.1060(21)

图 8 – CDC服务类别

表 4 – CDC服务清单

A	CDC的战略管理
A-1	风险管理
A-2	风险评估
A-3	策略规划
A-4	策略管理
A-5	业务连续性
A-6	业务影响分析
A-7	资源管理
A-8	安全架构设计
A-9	分级标准管理
A-10	对抗措施选择
A-11	质量管理
A-12	安全审计
A-13	认证
B	**实时分析**
B-1	实时资产监测
B-2	事件数据保留
B-3	警报和警告
B-4	处置报告查询
C	**深度分析**
C-1	取证分析
C-2	恶意软件样本分析
C-3	跟踪和追踪
C-4	取证证据收集
D	**事件响应**
D-1	事件报告受理
D-2	事件处置
D-3	事件分类
D-4	事件响应和遏制
D-5	事件恢复
D-6	事件通知
D-7	事件响应报告
E	**检查和评估**
E-1	网络信息收集
E-2	资产盘点
E-3	漏洞评估
E-4	补丁管理
E-5	渗透测试
E-6	抵御APT攻击的防御能力评估
E-7	网络攻击处置能力评估
E-8	策略合规
E-9	硬化

F	收集、分析和评估威胁情报
F-1	事后分析
F-2	内部威胁情报收集和分析
F-3	外部威胁情报收集和评估
F-4	威胁情报报告
F-5	威胁情报利用
G	**CDC平台的开发和维护**
G-1	安全架构实现
G-2	网络安全资产的基本操作
G-3	网络安全资产的高级操作
G-4	端点安全资产的基本操作
G-5	端点安全资产的高级操作
G-6	云安全产品的基本操作
G-7	云安全产品的高级操作
G-8	深度分析工具操作
G-9	分析平台的基本操作
G-10	分析平台的高级操作
G-11	操作CDC系统
G-12	现有的安全工具评估
G-13	新的安全工具评估
H	**支持内部欺诈响应**
H-1	内部欺诈响应和分析支持
H-2	内部欺诈检测和预防再次发生支持
I	**与外部各方的积极关系**
I-1	认知
I-2	教育和培训
I-3	安全咨询
I-4	安全供应商协作
I-5	与外部安全社区的协作服务
I-6	技术报告
I-7	执行安全报告

附件A

CDC服务清单及描述

（此附件是本建议书不可分割的组成部分。）

A.1 类别A：CDC的战略管理

A.1.1 A-1. 风险管理

风险管理服务旨在实现协调的活动，包括A-2到A-13，以就风险为组织提供指导和控制。

A.1.2 A-2. 风险评估

风险评估服务在资产、威胁和安全措施方面提供关于组织风险水平的快照。

A.1.3 A-3. 策略规划

策略规划服务为有关确定具体安全策略、编制导则的所有活动提供支持。

A.1.4 A-4. 策略管理

策略管理服务旨在实现对策略和组织规则评估结果的定期审查，以遵循新的或外部的要求（例如，法规和导则）。

A.1.5 A-5. 业务连续性

业务连续性服务支持确保正确实施和执行组织业务连续性计划所需的运营功能。

A.1.6 A-6. 业务影响分析

业务影响分析服务旨在实现对源自各种事件或场景的可能影响的系统评估。本服务可帮助组织了解可能发生的损失范围。它可能不仅涵盖直接的经济损失，还可能涵盖其他影响，例如，利益攸关方信任的失去和声誉的损害。

A.1.7 A-7. 资源管理

资源管理服务对资源（人员、预算、系统等）进行规划，以支持安全活动，并适当地将之分配给各服务。

A.1.8 A-8. 安全架构设计

安全架构设计服务旨在建立一个架构，以保护业务。CDC平台（类别G）的开发和维护可以通过编制各种虑及系统设计和业务过程（例如，供应链）约束条件的安全测量来实现。

A.1.9 A-9. 分级标准管理

分级标准管理服务旨在在总体策略中的约定范围内，为事件（例如，事故、发现的漏洞、发现的威胁信息）设置具体的分级（响应优先级）标准。

A.1.10 A-10. 对抗措施选择

对抗措施选择服务旨在支持针对分级标准（A-9）的所有对抗措施选择活动，以及针对所有安全处置活动的最佳技术。

A.1.11 A-11. 质量管理

质量管理服务旨在检查安全活动质量的问题，无论它们是否对业务（例如，可用性，生产力）有负面影响（例如，一周或一个月）。

质量管理服务旨在检查安全活动的质量问题，无论它们在一段时间内（例如，一周或一个月）对业务是否有负面影响（例如，可用性、生产率）。

A.1.12 A-12. 安全审计

安全审计服务系统地和可测量地对组织如何在特定地点或时间内实施安全策略和控制进行审计。CDC工作人员间接参与审计活动，以便提供有关控制实施状态的必要信息和证据。

A.1.13 A-13. 认证

认证服务支持组织开展各种必要的活动，以符合各种标准和认证方案的要求。

A.2 类别B：实时分析

A.2.1 B-1. 实时资产监测

实时资产监测服务旨在监督和分析来自日志和网络流的系统状态或可疑活动，并支持分级为事故或事件，以收集所需信息。

A.2.2 B-2. 事件数据保留

事件数据保留服务收集和集中存储在安全监测和分析过程中收集的事件。

A.2.3 B-3. 警报和警告

警报和警告服务向涉及的内部功能通报事件，强调信息资产面临的潜在风险（例如，安全设备警报、安全公告、漏洞和扩散的威胁）。

A.2.4 B-4. 处置报告查询

处置报告查询服务旨在对有关分析数据和报告查询做出响应。

A.3 类别C：深度分析

A.3.1 C-1. 取证分析

取证分析服务分对收集自安全资产的数字证据进行分析，并将之与某个事件关联，以协助确定发生了什么事情。

A.3.2 C-2. 恶意软件样本分析

恶意软件样本分析服务旨在对每个取证过程中发现的攻击者部署的恶意软件、程序或脚本进行分析。

A.3.3 C-3. 跟踪和追踪

本服务指的是组织跟踪和追踪针对其基础设施的任何攻击源的能力，这是减少进一步发生和防止安全事件的一个关键的成功因素。跟踪和追踪内部与外部攻击者（例如，网络属性）的一个公认能力是可预先阻止未来的攻击。

A.3.4 C-4. 取证证据收集

取证证据收集服务收集和保存与所评估事件相关的数字电子证据，并确定和维持证据的有效性（“保管证据链”）。

A.4 类别D：事件响应

A.4.1 D-1. 事件报告受理

事件报告受理服务旨在接收有关运营情况的分析报告。不过，它可能会收到来自公司内部其他组织或来自外部组织的报告。

A.4.2 D-2. 事件处置

事件处置服务旨在处置受理的事件和协调活动，包括D3至D-7。

A.4.3 D-3. 事件分类

事件分类服务旨在对事件进行分类，以促进就发生的事件类型以及导致事件发生的原因形成共识。

A.4.4 D-4. 事件响应和遏制

事件响应和遏制服务旨在在事件扩散到所有资源并增加对资源的损害或影响之前对事件予以遏制。

A.4.5 D-5. 事件恢复

事件恢复服务旨在支持将目标的功能恢复到其正常的系统可操作性。

A.4.6 D-6. 事件通知

事件通知服务旨在将事件的发生情况传达给事件响应团队和其他相关团体。

A.4.7 D-7. 事件响应报告

事件响应报告服务旨在完成和分发已关闭事件响应的报告（如果对抗工作旷日持久，那么将移交给CDC的战略管理部门（类别A））。如果CDC工作人员在处置事件期间需要一份关于当前状态的报告，那么本服务会分发一份临时报告。

A.5 类别E：检查和评估

A.5.1 E-1. 网络信息收集

网络信息收集服务旨在接收要保护网络配置的概述。

A.5.2 E-2. 资产盘点

资产盘点服务旨在实现与系统、资产和应用程序普查相关的信息管理，它们构成CDC支持范围内的整体业务基础设施。

A.5.3 E-3. 漏洞评估

漏洞评估服务旨在检查网络、系统和应用程序，以识别漏洞，确定如何利用它们，并就如何缓解风险提出建议。

A.5.4 E-4. 补丁管理

补丁管理服务旨在支持安装所需的任何安全补丁，同时维护信息技术（IT）服务的可用性。

A.5.5 E-5. 渗透测试

渗透测试服务旨在揭示可能被攻击者利用的安全漏洞，并强调可能的危害方法（例如，威胁引导的渗透测试）。

A.5.6 E-6. 抵御ATP攻击的防御能力评估

抵御高级持久威胁（ATP）攻击的防御能力评估服务旨在衡量组织对有针对性的攻击的抵抗力，同时开展有针对性的电子邮件培训和社会工程测试。

A.5.7 E-7. 网络攻击处置能力评估

网络攻击处置能力评估服务旨在确认基于假设发生攻击之场景的实际安全响应活动是否可以激活，以及事件是否可以立即结束（称为网络攻击响应演习）。

A.5.8 E-8. 策略合规

策略合规服务旨在支持验证与预定义安全策略的一致性和合规性。

A.5.9 E-9. 硬化

硬化服务旨在优化IT组件配置，以识别、评估和应用系统安全配置，并缓解或消除攻击风险。

A.6 类别F：收集、分析和评估威胁情报

A.6.1 F-1. 事后分析

事后分析服务描述对某事件的解决情况，以确保审查和改进CDC工作人员的过程和工具。

A.6.2 F-2. 内部威胁情报收集和分析

内部威胁情报收集和分析服务旨在收集关于实时分析和事件响应的信息（内部情报）。

A.6.3 F-3. 外部威胁情报收集和评估

外部威胁情报收集和评估服务旨在收集信息（外部情报），例如，新的漏洞、攻击趋势、恶意软件行为和恶性互联网协议地址或域名信息。

A.6.4 F-4. 威胁情报报告

威胁情报报告服务旨在编制内部和外部威胁信息并予归档，包括所有细节。

A.6.5 F-5. 威胁情报利用

威胁情报利用服务旨在汇编和传播有关所有类别安全响应的威胁信息。

A.7 类别G：CDC平台的开发和维护

A.7.1 G-1. 安全架构实现

安全架构实现服务旨在利用资产实现通过CDC战略管理（类别A）设计的安全架构。

A.7.2 G-2. 网络安全资产的基本操作

网络安全资产的基本操作服务旨在操作网络设备，例如，防火墙、入侵检测系统/入侵防护系统（IDS/IPS）、网络应用程序防火墙（WAF）和代理。

A.7.3 G-3. 网络安全资产的高级操作

网络安全资产的高级操作服务旨在为具有攻击检测能力的产品创建自定义签名，例如，IDS/IPS和WAF，如果供应商提供的签名不足，那么应用之。

A.7.4 G-4. 端点安全资产的基本操作

端点安全资产的基本操作服务旨在在端点处操作对抗产品，例如，防病毒软件。

A.7.5 G-5. 端点安全资产的高级操作

端点安全资产的高级操作服务旨在使用其保护产品在端点内检测可疑程序活动，并收集和分析注册表状态、过程执行情况等。如果需要，该服务建立自定义的危害指标，以启用端点检测。

A.7.6 G-6. 云安全产品的基本操作

云安全产品的基本操作服务旨在在云中操作安全服务。

A.7.7 G-7. 云安全产品的高级操作

云安全产品的高级操作服务旨在为具有攻击检测能力的云安全服务创建组织的自定义签名。如果供应商提供的签名不足，那么服务应用自定义签名。

A.7.8 G-8. 深度分析工具操作

深度分析工具操作服务旨在在深度分析中操作工具，例如，数字取证和恶意软件分析。

A.7.9 G-9. 分析平台的基本操作

分析平台的基本操作服务旨在操作分析基础设施，该基础设施存储所需的日志数据，并使分析经常进行，主要是实时分析，例如，安全信息和事件管理（SIEM）。

A.7.10 G-10. 分析平台的高级操作

分析平台的高级操作服务旨在使用组织自己的系统来实现更详细和准确的分析，以保留商业SIEM无法捕获的系统日志和分组捕获数据，并为这些数据开发定制的分析算法和逻辑以及系统。

A.7.11 G-11. 操作CDC系统

操作CDC系统服务旨在操作系统，执行安全响应操作所需的任务，例如，先前描述的各种安全响应工具、生成各种报告、响应查询以及漏洞管理系统。

A.7.12 G-12. 现有的安全工具评估

现有的安全工具评估服务旨在验证当升级或更改现有安全工具的设置时对其他系统和操作的影响，主要在可用性方面。

A.7.13 G-13. 新的安全工具评估

如果在安全活动中需要新的措施，那么新的安全工具评估服务旨在设计和安装新的安全资产。

A.8 类别H：支持内部欺诈响应

A.8.1 H-1. 内部欺诈响应和分析支持

内部欺诈响应和分析支持服务旨在通过根据安全活动收集的日志组织其活动，来支持组织在发现内部欺诈时做出响应。

A.8.2 H-2. 内部欺诈检测和预防再次发生支持

内部欺诈检测和预防再次发生支持服务旨在分析已发现的内部欺诈活动的细节，并考虑是否有可能从日志中检测到它们，如果可以，那么实施检测逻辑。

A.9 类别I：与外部各方的积极关系

A.9.1 I-1. 认知

认知服务旨在使CDC相关的人员准确地形成认识，推动使用正确工具、最佳做法，策略和资源，以确保对业务资产的保护。

A.9.2 I-2. 教育和培训

教育和培训服务旨在为CDC支持的组织的员工提供安全方面的专门培训活动。

A.9.3 I-3. 安全咨询

安全咨询服务就安全性为各种业务功能提供咨询服务。

A.9.4 I-4. 安全供应商协作

安全供应商协作服务旨在与所购置安全产品或服务的提供商建立直接通信，请求对安全响应中发现的任何缺陷做出响应，并就需要改进的地方积极交流反馈意见。

A.9.5 I-5. 与外部安全社区的协作服务

与外部安全社区的协作服务旨在通过参与外部社区来积极交换信息。此类信息可反映安全活动。

A.9.6 I-6. 技术报告

技术报告服务旨在提供关于监测和管理活动结果的报告。这些活动有助于显示系统和信息技术基础设施的安全水平。

A.9.7 I-7. 执行安全报告

执行安全报告服务旨在向最高管理层提供定期报告和统计分析结果，以强调组织的安全水平和运营性能指标。

参考书目

[b-ITU-T X.1053] Recommendation ITU-T X.1053 (2017), *Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations*.（基于ITU-T X.1051的中小电信组织信息安全控制行为守则）

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