Version 2.1

TLP:WHITE

2019 □ 11 □

□ □ □ □ □ □ □ □ □ □ □ □ CSIRT□

□ □ □ □

□ □ 2.1

注意：本文档描述了事故响应和安全团队论坛（**FIRST.Org**）认为的最佳做法。这些描述仅供参考。**FIRST.Org** 对因使用此信息而造成的或与之相关的任何性质的损害概不负责。

□ □

CSIRT 服务框架

1 □ □

计算机安全事故响应团队（CSIRT）服务框架是一个高层文档，以结构化的方式描述了计算□ 服务的 □ □ □ □ □ □ □ □ □ □ □ 服务和相关功能集。该框架由 FIRST 社群的知名专家开发，并得到了 CSIRT 工作组（TF-CSIRT）和国际电信联盟（ITU）的大力支持。

CSIRT 服务框架的使命和目的是 □ □ □ □ □ □ □ CSIRT 操作，特别是在支持安全团队方面，它们正在选择、扩展或改进其服务包。所描述的服务是 CSIRT 可以提供的那些潜在服务。不能期望 CSIRT 提供所有描述的服务。每个安全团队都将需要根据其任务授权来选择支持其使命和服务对象的服务。

本框架旨在通过确定和定义服务的核心类别及其子组件来为安全团队提供帮助。这 □ □ □ 个服务、子服务、功能以及可选的子功能的标题和描述 □ □ □ □ □ □ □ □ □ □ □ □ 一个起点，旨在提供一个一致的服务框架，以 □：本文档没 □ □ □ □ □ □ □ □ □ □ CSIRT □ 1 □ □

CSIRT 服 □ □ □ □ □ □ □ □ □ □ □ □ □ CSIRT 提供有关能力、容量、□ □ □ □ □ □ □ □ □ □ 此类主题对任何 CSIRT 为其服务对象提供的价值而言都很重要，但有意地未在本框架文件中纳入这些内容。同样，本框架也不涉及实施方案，也不 □ □ □ □ □ □ 任何特定服 □ □ □ □ □ □ □ □ 要的是要理解，可以有多种不同的方式来实施这些服务，同时仍要确保满足服务对象和利益攸 □ □ □ □ □ □ □ □

2 □ □ □ □ □

□ 命，为定义的服务对象提供服务和支持，以防止、检测、处置和响应计算机安全事故。

正确部署的 CSIRT 具有明确的任务授权、治理模型、量身定制的服 □ 服务。

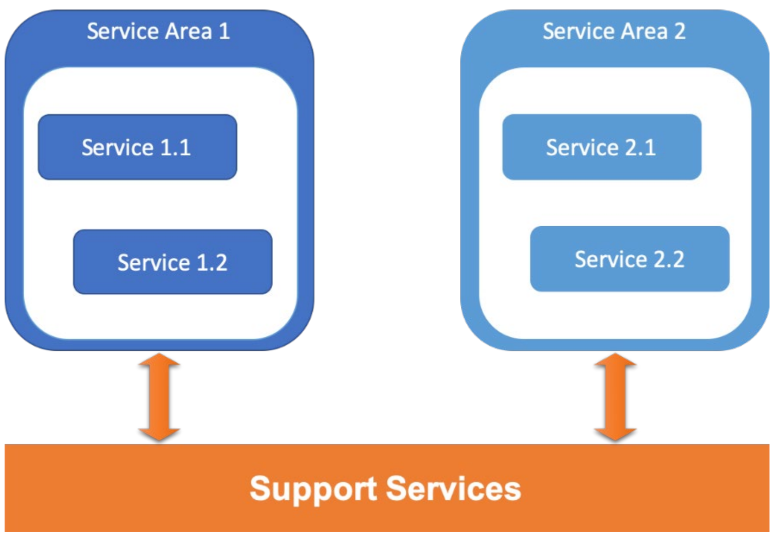
这些年来，CSIRT □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 服务列表或框架。随着技术、工具和流 □ CSIRT □ □ □ □ □ □ □ □ □ FIRST □ □ □ □ □ □ □ □ □ CSIRT □ □ □ CSIRT □ FIRST 成员的地理和功能范围，可以确定的是，对于明确地获取和表示由 CSIRT 提供的服务，其

□□CSIRT服务框架，并于2017年发布了初始版本。

认识到许多运营方面的工作□□□□的服务集和相应的活动□□□□□□□□□□□□□的方法来开发产品安全事故响应团队（PSIRT）服务框架。所有的服务框架都可以在FIRST网站□□□□[1]

这是CSIRT服□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□对必要处进行了重组和扩展。特别是，内部活动已被删去，因为这些活动不构成向服务对象提供的服务。支持任何服务提供全□□□□□□□□□□□□□□□服务和功能来□□□□□□□□□要提供给服务对象的服务一样。这些服务和功能通常称为支持服务□□□□□□和雇佣、差旅费补偿或培训活动组织等，就是行政管理活动的一些例子。[2]

□□□□□□□□□□□□□□□□□□□□□服□□□□□□□□□□□□CSIRT或相关服务产品的组织。例如，在支持CSIRT时确实需要雇佣和管理员工，但这被认为是典型的组织支□□□□□□□□□CSIRT。



□□□□□

Service area：服务区

Service：服务

Support services：支持服务

---

[1] CSIRT 相关资料：https://www.first.org/standards/frameworks/csirts/

[2] 查看[Kossakowski 2001]，它讨论的是内部支持服务及其与其他服务的关系。

尽管内部服□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□持服务被认为超出了范围，因此在 FIRST 服务框架内未对之做进一步详细介绍或讨论。

由于 CSIRT 将需继续应对不断变化的挑战，以确保其服务对象安全并免遭新出现之威胁的侵□□□□□□□□□□□□□，将对本框架涵盖的服务进行审议、审核、扩展或修正。[3]

3 CSIRT 与 PSIRT 之间的区别

对服务对象以及所提供服务的关注焦点是组织的 CSIRT 与同一组织中出现的其他安全团队（如 PSIRT□□□□□□□□□□□□□□□□□□焦点是 PSIRT 与任何其他安全团队（包括但□□□□□□□□ CSIRT□□□□□□□□□

□□□□□□□□ CSIRT□□□□□□□□□□□□□□□□□□□□□□□□□□□□□在一个大型组织内有多个安全团队和 CSIRT，则其中一个可以充当协调员以及与外部各方的单一联系点。此类安全团队被称为协调 CSIRT。

此类协调 CSIRT 也被建成为独立的实体，为一组特定的个人和/或组织（称为服务对象）提供服务。属于某特定服务对象的各组织拥有一些共同的特性（例如，是□□□□□□□□□□或属于某个特定国家）。协调 CSIRT 是整个团队的单一联系点，其专注焦点在这些组织的整体安全问题。

如今，国家 CSIRT 已经建成为协调 CSIRT 的一种独特类型，来推动并经常性地□□□□某特定国家内的 CSIRT 活动，或者为该国的所有公民、关键基础设施实体的特定部门等提供有限的服□□

尽管任何 CSIRT 与 PSIRT 之间都有重要的区别，但重要的是要认识到两个实体之间也存在协同。重要的一点是，CSIRT 和 PSIRT 都不是彼此独立运行的，例如，许多 CSIRT 都会向服务对象□□□□□□□□□警告□□□□□□□□□□□□□□ PSIRT 所提供的信息。

4 CSIRT 服□□□□□

CSIRT 服务的框架基于四个关键元素的关系：

服务区 → 服务 → 功能 → 子功能

□□□□□□□□

---

[3] 已成立一个 FIRST 特别利益小组（SIG）来指导“CSIRT 框架开发”。

服□□

与公共方面有关的服务区群服务。它们有助于按顶层分类来组织服务，从而便于理解和沟通。每个服务区的规范都将包括一个“描述”字段，该字段由描述该服务区以及该服务区内服务列□□□□□□□□□□□□□

服务

服□□□□□□□□□□□□□□□□□□□□□□□□□□□□服务对象□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

服务通过以下模板来规定：

- 描述服务性质的“描述”字段；
- 描述服务意图的“目的”字段；
- 描述服务任何可度量结果的“结果”字段。

□□

功能是旨在实现特定服□□□□□□□□□□□□□□□□□□□□□□服务情境中共享□□□□

□□□□□□□□□□□□

- 描述功能的“描述”字段；
- 描述功能意图的“目的”字段；
- 描述功能任何可度量结果的“结果”字段；
- 可以作为功能的一部分来执行的子功能列表。

□□□

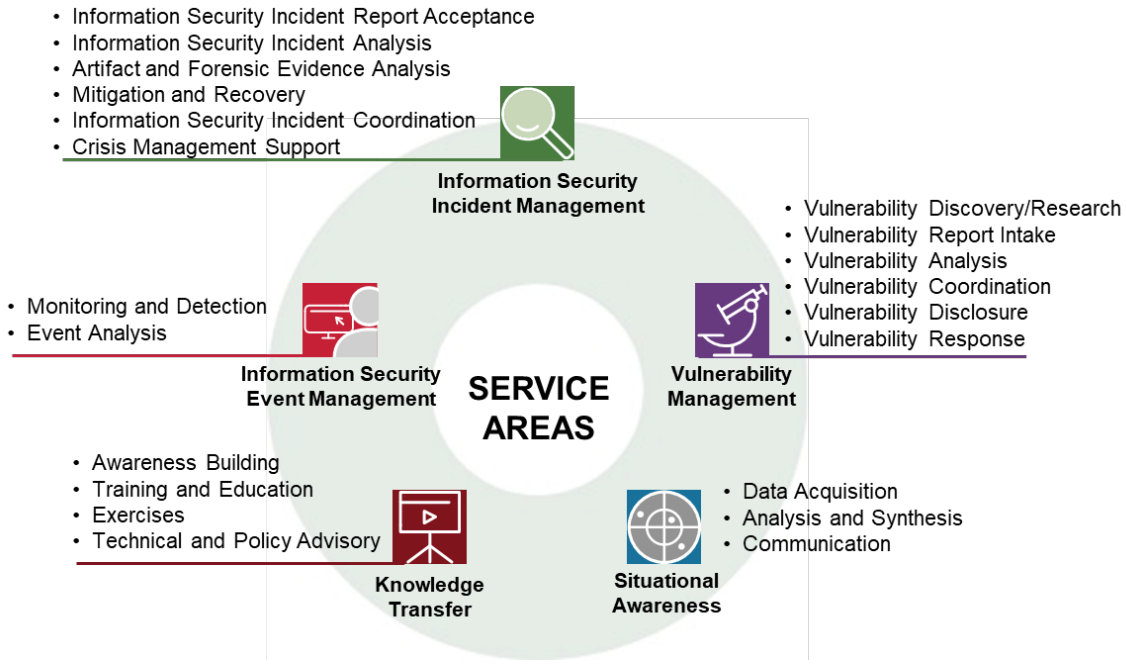
子功能是旨在实现特定功能目的的一项或一组活动。任何子功能都可以在若干功能和/或服务情境中共享和使用。可以为这些功能和/或服□□□□□□□□/或服务来可选地执行或要求子□□□

□□□□□□□□□□□□□□

- 描述子功能的“描述”字段；
- 描述子功能意图的“目的”字段；
- 描述子功能任何可度量结果的“结果”字段。

出于 CSIRT 服务框架的目的，没有对任何子功能做完整描述。对每个仅做了简短描述。

下图显示（下一页）CSIRT 服务框架服务区和服务。有关服务区、服务和功能的完整表，请参见附录 4。



□ □ □ □ □

Service areas□ □ □ □

Information Security Event Management□ □ □ □ □ □ □ □ □

Monitoring and detection□ □ □ □ □ □

Event analysis□ □ □ □ □

Information Security Incident Management□ □ □ □ □ □ □ □ □

Information security incident report acceptance□ □ □ □ □ □ □ □ □ □ □

Information security incident analysis□ □ □ □ □ □ □ □ □

Artifact and forensic evidence analysis□ □ □ □ □ □ □ □ □ □

Mitigation and recovery□ □ □ □ □ □

Information security incident coordination□ □ □ □ □ □ □ □ □

Crisis management support□ □ □ □ □ □ □

Vulnerability Management□ □ □ □ □

Vulnerability discovery/research：漏洞发现 /研究

Vulnerability report intake：漏洞报告获取

Vulnerability analysis：漏洞分析

Vulnerability coordination：漏洞协调

Vulnerability disclosure：漏洞披露

Vulnerability response：漏洞响应

Situational Awareness：态势感知

Data acquisition：数据采集

Analysis and synthesis：分析和综合

Communication：沟通

Knowledge Transfer：知识转化

Awareness building：树立意识

Training and education：培训和教育

Exercises：训练

Technical and policy advisory：技术和策略咨询

5 服□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□安全事故。在较大规模的组织中，有时会将该服务区全部或部分指配□□□□□□□□SOC），□□□□□□额外执行第一级或甚至第二级的信息安全事故管理，例如，□□□□□□□□□安全控制措施。由于任何信息安全事故管理服□□□□□□□□□□□□□□□□□□□□据，因此 SOC 与指配的 CSIRT 之间的接口显得至关重要。[4]

以下服务被视为该特定服□□□□□服务:

---

[4] 尽管本服务框架并非旨在定义 SOC 服务框架，但可以预期的是，在定义 SOC 服务的同时，来自信息安全事件和事故管理区的服务将是有用的和直接适用的。

- 监视 和 检测；
- 事件分析 。

5.1 服 □□□□□□□

目的： 对各种信息安全事件源和情境数据实施自动的 、 连续 的 处理，以 确定 □□□□□□□□ 故，例如， 攻击 、 入侵 、 数据泄露或违反安全策略 等 。

描述： 基于日志 、 NetFlow 数据 、 IDS 警报 、 传感器网络 、 外部源或其他可用的信息安全事件数 □□□ □□□□□□□□□□□□□□□□□□□□□□□□□□ 的 工具 进行处理， 例如， 安全信息 □□□□□□SIEM□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 服 务一部分 加以 分析的 虚警 数量。

结果： 将潜在 的信息安全事故确定为分析 服 务的一部分，以进行分析。

以下功能被视为本 服 □□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.** 。

5.1.1 □□□□□□□□□□□

目的： 管理日志源和传感器

描述： □□□□□□□□□□□□□□□□□□□□□□□□□□□□ 加以 部署 、 “上机操作 ”并 □□□□□□□□□□□□□□□□□/□□□□□□□□□□□□□□□□□□□□□□□□ 配置（例如，样式 定义）的传感器 的配置 。 □□□□□□□□□□□□□□□□□□□□□□ 括外部检测 服 务或开放源代码情报（ OSINT□□□

结果： □□□□□□□□□□□□□□□□□□□□□□□

5.1.2 □□□□□□□□□

目的： 在整个检测周期内 对 □□□□ 宝实施管理。

描述： 开发 、 □□□□□□□□□□□□□□□ 之 引入生产的检测用例 中 □□□□□ 有关 分析 人员分类 、资质 界定 和 关联 的 说明，例如， □□□□□□□□□□□SOP）的形式。 对 表现不佳 的用例，即效益 /□□□□□□□□□□□□□□□ 、 重新定义或 废弃 。 对 检测用例 包， 应以面 □□□□□□□□□□□□□□□□□□□□□□

结果： 开发与 服 务对象相关的有效检测用例 包。

5.1.3 □□□□□□□□□

目的： 管理情境数据源， 旨在 检测和充实 之目的。

描述： 涉及检测和 充实之目的 □□□□□□□□□□□□□□□□□□□ 加以 □□□□□□□ 是到其他 IT 系统（例如， 配置管理数据库（ CMDB）、 □□□□□□□□ IAM）或 威胁情报系统）或从中导出 的活动 API， 或者是需要手动管理的完全独立的数据集。 □□□□□ 指标列表、监视列表和白名单 等 情况， 用于 抑制误报。

结果： 最新的情境数据可用于检测和 充实 之目的。

5.2 服 □□□□□□

目的： 对 检测到的潜在信息安全事故及其 性质 进行分类 和界定，作为 □□□□□□□□□□□ 信息安全事故管理 服 务区 或者 作为 虚警 。

描述： □□□□□□□□□□□□□□□□□□□□□□□□□□□ /或自动分析将 每一项归 为信息安全事故（真）或 虚警 （假）。根据检测用例，这可能需要手动或自动 采集额外 信息。应该优先考虑对潜在的更关键的信息安全事故 进行 分析，以确保及时 地 □□□□□□□□□ 反应。通过 确定 检测用例、 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□

结果： 合格 的 和 关联 的信息安全事故可以作为信息安全事故管理 服 □□□□□□□ 对 误报可 以 □□□□□□□

以下功能被视为本 服 □□□□□□□□□□

- 关联；
- 界定。

5.2.1 □□□□□

目的： 确定 与其他潜在或正在进行的安全事故直接相关的 事件。

描述： 将 与相同资产（例如，系统、 服 务、 □□□□□□□□□□□□□□□□□□□□□□ □□□ 安全性事故， 以 避免重复 劳动。与正在进行的信息安全事故直接 有关 □□□□□□□□□□□ 将 指配 给该信息安全事故，而不是 作为一个 □□□□□□□□□□□□

结果： 为组合性质， 对 有关 □□□□□□□□□□□□□□ 或者 更新 为 □□□□□□□□ 服 务区已 做 处理的现有信息安全事故。

5.2.2 □□□□□

目的： 对检测到的潜在信息安全事故进行分类和 界定， 以识别、 分类和确定真实肯定的优先级。

描述： 需要对潜在的信息安全事故进行分类，并将每 个 事故 界定 为信息安全事故（真）或 虚警 □□□ 自动化是关键。成熟的工具通过 充实 情境信息 、 □□□□□□□□□□□□□□ 指配 风险分数 和 / 或自动 识别有关 的信息安全事故，来 推动 □□□□□□ 对 □□□□□□□ 、反复 发生的案 例， 应 予 识别并 实现 自动化。关键程度较高的潜在信息安全事故应在关键程度较低的事故之前 予以 分析。除了 界定 为真 或 假 之外，更细粒度的 界定 对于持续改进检测用例以及 管理 日志源、 传感器和情境数据源 而言 也是一个 重要 的输入 □□□□□□ 界定 □□□□□□□□□□□ KPI， 以 度量 本 服 务 区 成功 与否 。

结果： 合格的潜在信息安全事故可作为信息安全事故管理 服 务区的一部分 来 处理。

6 服□□□□□□□□□□□

本 服 务区是任何 CSIRT 的核心，并包含对攻击或事故期间帮助 服 务对象 而言 至关重要的 服 务。 CSIRT 必须准备 好 □□□□□□□□□□□□□□□□□□□□ 技能，不仅能够收集和评估 □□□ □□□

通过此分析，可以 提出关于 □□□□□□□□□□□ 之 步骤 的建议，并 为 服 务对象提供支 持以应用 这些 □□□□□□□□□□□□□□□ ， 对等 CSIRT □□□□□ 、 供应商或 PSIRT）进 □□□□□□□□□□□□□□□□□□□□□□□□□□□□

CSIRT 可以提供的特殊专业 技能 对于解决（信息安全）危机也 是 至关重要 的 。尽管在许多情 □□□ CSIRT □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 以大大改善 对 所需缓解步骤或更好保护机制的应用。

应用知识和可用 的 基础 设施 来支持其 服 务对象 □□□□□□□□□□□□□□□□□

以下 服 务被视为该 服 □□□□□□□ 服 务:

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- 危机管理支持 。

6.1 服□□□□□□□□□□□□

目的： 从 服 务对象、信息安全事件管理 服 务或第三方处接收并处理有关潜在信息安全事故的报 □□

描述： 对于 CSIRT，最重要的任务是在服务对象内部接受有关信息安全事故和可能影响网络、设□□□□□□□□□□□□□□□□□□“□□”□□□□□□□□□□□□□□CSIRT □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

为了使服务对象能够更有效地报告信息安全事故， CSIRT 应该提供一种或多种机制以及关于什么□□□

□□□□□□□□□□□□服务可能检测到存在大量会自动升级的潜在信息安全事故，因此必须在采用此类接口或授权服务对象使用它们之前做好计划。[5]

结果： 将以专业且一致的方式获取每份信息安全事故报告，并对其进行初步检验和分类。

以下功能被视为本服 □□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**。

6.1.1 □□□□□□□□□□□□□

目的： 接受或接收服 □□□□□□□□□□□□□□□□□□□□□□□

描述： 有效获取信息安全事故报告需要机制和过程来接收来自服务对象、 □□□□□□第三方（例如，发现者、研究人员、 ISAC、其他 CSIRT）的报告。信息安全事故报告可能包括受影响的设备/网络/用户/组织、已经确定的条件（例如，已被利用的漏洞）、对技术和业务水平的影响以及为开始补救和/或缓解步骤以及可能的解决措施而采取的行动。有时，信息安全事故信息可能作为对其他服务的输入的一部分而被联合接收，最常见的是获取 □□□

结果： 信息安全事故报告由服务对象或第三方进行适当处置，包括启动记录或跟踪报告。

□□□□□□□□□□□□□□□□

- 定期监视沟通 □□□□□□通报的与 CSIRT 联系的方式是否有效并可提交报告；
- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□与报告者设定期望值。

---

[5] 可以预期，与信息和数据获取有关的所有服务都有诸多 □□□□□□□，通常将来自 □□服□□□□□服务组合为一项服务 /功能来提供。由于这不是强制性的，并且没有服务区的固定组合，因此我们选择在 CSIRT 服务框架内将这些服务分开，尽管每个安全团队都可以自由地选择最佳的组织模型来建立自己的服□□

6.1.2 □□□□□□□□□□□□□□

目的：对报告的信息安全事故进行 □□□ 审查、分类、优先排序和处理。

描述：对信息安全事故报告进行审查和分类，以初步了解所议 □□□□□□□□□□□□□□ 有真正的信息安全影响并可导致（或已导致）信息资产或其他资产的机密性、可用性、 □□□ 和 /或真实性遭到破坏，这一点尤为重要。根据初始报告中提供的信息的详细程度和质量，是否发生了真正的信息安全事故或者是否存在其他原因（例如， □□□□□□□□□□□□□□ 也可能不明显。将基于初步评估结果来确定 □□□□□□□□□□□□□□ 做进一步分析；从报 □□

攻击可能源自 CSIRT 服务对象内部，可能针对本服务对象，或者本服务对象仅受附带影响。如果 CSIRT 不为确定的目标提供信息安全管理服务，则应将报告安全地转发给一个外部组来进行处置，例如，受影响的组织或 CSIRT。

除非有理由拒绝信息安全事故报告或 □□□□□□□□ 处置的另一个 □□□□□□□□□□□ 给漏洞分析服务以做进一步评审、分析和处置。

结果：可以确定报告的事情是否确实是一件需要由 CSIRT 来处置 □□□□□□□□□□□□□□ □□

以下子功能被视为本服务实施方案的一部分：

- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□ CSIRT 的成功攻击；
- 基于可用的分类或优先级排序结果，通过对进一步的 □□□□ 某些反馈意见，来更新对报告的确认；
- 将有关已处理的信息安全事故的新信息合并到可用的数据中，以做一致的分析和处理。

6.2 服 □□□□□□□□□□

目的：分析并了解已确认的信息安全事故。

描述：本服务包含以下功能：了解信息安全事故及其实际的和潜在的影响，以确定导致成功攻击、破坏或利用的基本 □□□□□□□□□□□□□□□

□□□□□□□□□□□□□ 目的是根据当前了解信息安全事故影响所需的或合理的详细程度，确定和表征信息安全事故。可以通过范围、受影响的实体、 □□□□□□□□ 、时间线等来表征信息安全事故。在提供信息安全事故协调服务和功能或者采取缓解 /恢复行动时，可以并行地继续本服务。

CSIRT 可以 □□□□□□□□□□□□□□□□□□ 请参见下文）或者供应商和产品安全团 □□□□□□□□□□□□□□□ 来 □□□□□□□□□□□□□□□□□□□□□□□□□□□

结果：对信息安全事故关键细节（例如，描述、影响、范围、攻击 /利用和补救措施）的了解有□□□□

以下功能被视为本 服 □□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.** 事故关联。

6.2.1 □□□□□□□□□□□□□□□□□□□□□

目的：□□□□□□□□□□□□□□□□□□□□□□□□□

描述：分析信息安全事故 服 务始于对可用信息的审查，以 □□□□□□□□□□□ 信息安全事故对与 CSIRT 职权范围有关的 系统 造成 的影响。如果信息安全事故是由 服 务对象 或 第三方报告给 CSIRT，则其中一些可能已在 （信息安全事故报告获取 服 务的） □□□□□□□□□□□□□□ 能中 得以记录。

□□□□□□□□□□□□□□□□□□□□□□ 指配 给主题专家，该专家可以 在 技术 上予以 确认，它对所涉及的系统有一定 的 影响，并与 CSIRT 的职权范围 相关（即对 网络或系统潜在安全影响，根据 CSIRT 的 职权范围，它 可 对 CSIRT 职权范围内的 信息资产的机密性 、 可用性或完□□□□□□□□

结果：对信息安全事故的信息记录进行分类、确定 优先级 和 更新。

6.2.2 □□□□□□□

目的：获取、 分类、 存储和跟踪与信息安全事故以及被认为是其中一部分的所有信息安全 事件□□□□□□

描述：使能 收集所有有价值的信息， 以获得对情境的最佳 了解 □□□□□□□□□□□□□□ 息的来源和内容， 以用于任何进一步的处理。

□□□□□□□□□□□□□□□□□□□□□ 以及有关 在 什么 情况下 可以 使用 什么 数据或者 以 什么 形式 来 处理 数据 □□□□□□□□□□□□□□□□□□□□□□□□□ 标记 和 属性，以便 后续检验 来源以及适当性或真实性。

结果：可获得有关 所 收集数字 化 和非数字 化 □□□□□□□□□□□□□□ 带有 跟踪信息以及处理和存储完整性的控制点。 取决于是 将结果用于将来（非正式 的 ）分析还是 将之用于 执法活动，在建立正式的 监管 链方面存在不同的要求， 这 可以在 后续 的某个阶段 □□□□□□ 辩护。

□□□□□□□□□□□□□□□□□□□□

- □□□□□□□□□□□□□□□□□□□□
- 从 服 □□/□□□□□□□□□□
- 收集和分类可能会但不保证有助于了解事故活动的数字数据（例如， 磁盘和内存映像、□□□□□□□□□□□□、网络架构 特性、日志）， □□□□□□□□□□□ 对抗性□□□□□□□
- 收集和分类 非数字数据（例如，物理 的签到单、 □□□、业务模型、 □□□□□□、策略、 企业风险框架）；
- □□□□□ 关于来源、收集方法、处置 数据或对象 之 人、 □□□□□□□□□□□□□ 尤其是 因为后续它 可能被视为 取证 分析或执法活动的证据。

6.2.3 □□□□□□□□□□

目的： 启动和跟踪有关信息安全事故的任何其他技术分析 结果。

描述： 由于可能需要 进行 更详细的技术分析，因此此类分析可以由其他专家（宿主组织或 CSIRT 内部或外部）或其他 的第三方 （例如， 专门从事此类分析 工作 的 服 务提供商） 来进行。这需要启动和跟踪此类活动， 直至 成功交付所需 的 分析 结果 为止。

结果： 从 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□， 对待处理清单， 可以 采用 外包分析 的形式来进行。

6.2.4 □□□□□□□□□□□□□□□

目的： □□□□□□□□□□□□□□□□□□□□□□□ 存在或者 允许被利用成功（包括但□□□□□□□□□□□□

描述： 本功能 涉及了解架构、 用法或 实施方案 □□□□□□□□ 行动 □□□□□□□□ 使 系统、 网络、 用户、 组织等 暴露于 攻击、被 利用或损害，成为 □□□□□□□□□□□□□□□ 者 在当中 可能 造成 更多系统 损坏的情况有关，它基于 初始 的 访问 □□□□□□□□□□□

□□□□□□□□□□□□ CSIRT □□□□□□□□□□□□□□□□□□□□□□□□□ 受影响的目标本身 来 □□□□□ 尤其 在协调 CSIRT 的情况下，没有 任何 关于已 受损 系统或网络的详细技术知识 可用。

结果： □□□ 未来 □□□ 被 □□□□□□

6.2.5 □□□□□□□□□

目的： 启用所有可用 的 信息，以最好地理解情境并检测相互关系 □□□□□□□□□ 对之 采取措施。

描述： 本功能 □□□□□□□□□□□□□□□□□□□□□□□□□□□ 结束之 信息安全事故的相互关系 、 趋势或适用的缓解措施， □□□□ 对当前 所处置 信息安全事故的响应。

结果： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 对 其他 □□□□□□□□□□□□ 被 怀疑 之 相互关系的详细了解。

6.3 服 □□□□□□□□□□□

目的： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

描述： 与理解构件（例如，恶意的软件、利用的漏洞、易失 的 □□□□□□□□□ 、 应用程序代码 、 日志 、 文档）的能力和意图有关的 服 务 及其 传递机制 、 传播 、 检测 、 缓解 以及 解除 警戒或 保持中立。 这适用于任何格式和来源：硬件 、 固件 、 内存 、 □□□□□□ 构件 或证据都必须未经修改地 予以 □□□□□ ， 并隔离存放。由于某些 构件 □□□□□□□□□□□ 变 成为证据， □□□□□□□□□□□□□□□

即使不保留监管链， 本 服 务 通常也涉及复杂且耗时的任务，并且需要专业技能，建立专用 □□□□□□□□□ - □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□

作为 信息安全事故 处理的一部分，可能会在受影响的系统或恶意软件分发站点 上 发现数字 □□ □□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 看作是一个 完整 的 列表：

- 无论是否恶意，构件运行和执行其预期任 务所需的情境；
- □□□□□□□□□□ ： □□□□□□□□□ 内 上载 、 下载 、 复制 、 □□□□□ ；
- 哪些系统在 本地和远程参与 了对 分发和 行动的支持；
- 确定 入侵者 对 曾经访问 的 系统 、 网络 、 组织或基础设施 □□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□□ 行动 请求 、 更新自身或在 受损（本地）网络 内部进行横向移动；
- 用户帐户或用户设备遭到破坏后，用户 、 □□□□□□□□□□□□□□□ ；
- □□□□□□□□□□ 或 受损 系统 □□□□□□□□□□□□□□□□□□□□□□□ 或互联网， 或者 以任何组合 的 方式；
- □□□□□□□□□□□□□□□□□□□□ 、 初始目标或 逃避 检测技术） 建立连接；
- □□□□□ 通信 架构（点对点 、 命令和控制 、两者 ）；
- 威胁 实施 者的行动是什么 、其 网络和系统足迹是什么；
- 入侵者或构件如何 逃避 检测（即使是很长一段时间， 这 □□□□□□□□□□□□□ 化） 。

□□□□□□□□□□□□□□□□□□□

- □□□□□□□ ;
- 逆向工程；
- □□□□□□□□ ;
- 比较分析。

□□ □□□□□ 的 比较、观察构件在运行 时或活动 环境 下 □□□□□□□□ 和 □□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 评估损害、制定缓解构件的解决方案，并向 服 □□□□□□□□□□□□□□□

结果： 了解 了 已恢复 之 数字构件和经分析 之 取证 证据的性质，以及与其他构件 、 内部或外部对象或组件 、 对框架 攻击、 工具 和被 利用漏洞的关系 ，以及 关于威胁 实施 者所做 事情的 有效假设或 证明。这些知识对评估损失 、 损害 、 业务影响等以及制定抑制 和 缓解 措施或 恢复策略 而言 至关重要。了解了攻击者或入侵者用来破坏系统 、 用户 、 网络 、 组织和 /或基础 设施 的 战术、 技术和 过程 □□□□ 那些 用于传播 、 泄露 、 更新 、 修改或伪造其行为 、 数据 、 □□□□□□□□□ □□□□□□□□□□□□□□□□□□□□□

被视为 本 服 务 □□□□ 一部分的功能列表:

- □□□□□□□ ;
- 逆向工程；
- 运行时和 /或动态分析；
- 比较分析。

6.3.1 □□□□□□□□□□

目的： □□□□□□□□□□□□□□□□ 私有的 构件和 /或签名存储库进行比较。

描述： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 、字符串输出 、 加密散列 、 证书 、 文件大小 、 文件 /目录名称。随着所有可用信息的收集和进一步分析，可将其用于 查看 任何公共 /开放或私有 /封闭 的 源信息存储库，以了解有关构件或其行为的更 □□□□□□□□□□□□□□□□□□□□

结果： 确认数字构件的 特性 和 /或签名，以及关于该构件的 任何已知的 信息，包括恶意、影响和 缓解 。

6.3.2 □□□□□□□

目的： 对构件 进行 □□□□□□□□□□□□□□□ 而不考虑 它可能运行其中的环境。

描述： 提供对恶意 软件 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 示 所有的 源码或者将二进制反汇编成汇编语言并解释 之 □□□□□□□□□□□□□□□□□ □□□

□□

结果： □□□□□□□□□□□，以了解它是如何工作的、如何被触发的、可以利用的相关系统弱点、它的全部影响以及潜在的危害，以便形成缓解 □□□□□□□□□□□ 在适当时 □□□□□□□□，□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□

- 静态分析；
- 代码逆向工程；
- □□□□□□□□□；
- □□□□□□。

6.3.3 □□□□□□□□□□□

目的： 深入了解构件的操作。

描述： □□□

□□□

结果： 通过观察数字构件在执行期间的行为来获得对其运行情况的额外认识，以确定受影响之主机 □□□□□□□□□□□□□□□□ 最终的网络流量，从而更好地了解系统的损害和影响，建立新的构件签名，并确定缓解措施。

□□□□□□□□□□□□□□□□□□□□□□□□ 从运行时分析中 □□

□□□□□□□□□□□□□□□□□□□□

- □□□□□□□□□/受限/封闭、仿真/模拟）；
- 准备采集器、传感器和/或探针；
- 采集初始行为数据和元数据；
- 在各种情境下多次探查构件；
- 开展短期和长期的系统和/或网络行为分析；
- □□□□□□□□□ 采集的数据、□□□□□□ 以及为与 □□□□ 匹配的现有技术成果 □□□□□□□□，□□□□□。

6.3.4 □□□□□□□

目的： 执行关注于确认公共功能或意图 □□□□□□□□ 分类 □□□□□□□□

描述： □□□□□ 探究一个构件与其它构件的关系， 这 可以确认在代码或者做法、目标、意图和作者方面的相似性，这些相似性可 用来 得到攻击的范围（例如， □□□□□□□□、类似的□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□版本如何被使用以及如何随时间变化的更宽阔视角，有助于理解 对 恶意软件或者 其他 恶意构件□□□□□□

结果： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□缓解的 额外见解 或理解的趋势或者相似性。

□□□□□□□□□□□□□□□□□□□□

- 定义 有关特性 和观察 之 行为的 基线；
- 在可用的存储库 /□□□□□□□□□□□□特性；
- 更新有关新观察到的或以前未知的症状 、 行为和 /或签名的可用存储库 /知识库，这些存□□/□□□□□□□□□□□□□□□□□□□□□

6.4 服□□□□□□□

目的： 尽可能 抑制 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□被 利用的漏洞或弱点 来 □□□□□□□□□□□□□□□□□□□□□□□□□□

描述： 一旦分析确认 一个 □□□□□□□□□□□□□□□□□□□□□□□□□□一个 响应计划。即使在最终确定 一个 响应计划之前，也可能会采取 特别 措施。 本 服 务 □□□□□□□□所执行的所有活动， 直到 信息安全事故 被认为 已 停止或者需要 进一步分析的新信息 已变得 可用□□□□□□□□□□□□□□□□□□

结果： 缓解 信息安全事故并改善网络安全状况。恢复受 基本 攻击或攻击者活动影响的系统完整性，以及受到破坏的网络和系统的可 用 □□□□□□□□□□□□□□□□□□□□□□

以下功能被视为本 服 □□□□□□□□□□

- □□□□□□；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.** 恢复；
- **Error! Bookmark not defined.** 。

□□□ CSIRT □□□□□□□□□□□□□□□□“□□□□□□□□□□”□□□□□□□提供的一项活动，但有时它们也有助于 “制定 响应计划 ”。

6.4.1 □□□□□□□□□

<u>目的</u>： 定义并执行一项 □□□□□□□□□□□□□□□□□□□□□□□□、系统和网络返回到未劣化的运行状态，将受影响的服务恢复为完全功能状态，而无需重建能 □□□□□□□再次被利用的情境。

<u>描述</u>： 如果不完全了解业务影响以及缓解和恢复的要求 □□□□□□□□□□□□□□□□□利益冲突（跟踪攻击以获得更多情报 - 抑制攻击以避免进一步损失），因此有必要考虑到所有利益，并制定合理的响应计划，以应对已知的事实并在要求的时间框架内 □□□□□结果。

与所有计划一样，必须考虑到， □□□□□□□□□□□□□□□□□□□□成果 □□□查。实际上，通常需要更改响应计划，以提供持续的指导和指南 □□□□□□□□□□□□划，除非响应由一个很小的组织小组来处理，且对外部接口或其他实体的要求很低，否则因缺乏协调，可能无法有效地开展活动。

<u>结果</u>： 商定的响应计划，如果有可用的资源和支持提供协助 □□□□□□□□□□□□□□□行该计划。 CSIRT 的跟踪和协调将由 “协调”服务来提供。

□□□□□□□□□□□□□□□□□□□□

- □□□□□□□□□□□□□；
- □□□□□□□□□□□□□□框架；
- 定义决策过程和准则 □□□□□通过策略定义的话）；
- 确定要恢复的对象：环境、系统、应用程序、 □□□□□；
- □□□□□□□□□□□□□□□□□；
- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□响应的响应计划。

6.4.2 □□□□□□□□□□□□

<u>目的</u>： 采取措施确保信息安全事故不会进一步蔓延，即抑制于当前受影响的系统、用户和 /或域内，以确保不会发生进一步的损失（包括文档泄漏、 □□□□□□□□□□□

<u>描述</u>： 在发生信息安全事故的情况下，面临 □□□□□□□□□□□□□□□□□□□□□恶□□□□□□□□□□□□□□□□□□□会造成进一步的数据丢失和更多 □□□□□□□□要目标通常是触达特定数据和系统，包括对 □□□□□□□□影响的组织 □□□□□□其他组□□，需要采取短期措施，例如， □□□□□□□□□□□□□□服务或系统的访问，还可能导致关□□□□□□□□

拒绝进一步访问潜在的关键证据数据， □□□□□□□□□□□□的分析。拒绝进一步访□□□□□□□络，也将限制因 □□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□阻断□□□□□□□□□□□□□□□□可以□□□□□□□□□□□□□□□□□□□□□□□□□□已经 访问更多 的 □□□□□□□不可能 回到 正常 的 操作。

结果： 重新获得对所涉及系统和网络的控制。 拒绝 □□□□□□□□□□□□、 系统和网络，以 免遭受更多 的 攻击和 /或破坏系统和数据。

□□□□□□□□□□□□□□□□□□□□

- 暂时删除用户 /系统 /服务 /网络的访问权限；
- 暂时断开系统或网络与网络或骨干网的连接；
- 暂时停用 服 务；
- 要求用户更改其密码或加密 证书；
- □□□□□□□□□□□；
- □□□□□□/系统 /服务 /网络均 未 受 到 影响。

6.4.3 □□□□□□□

目的： 在受影响的领域、基础设施或网络中 实施必要的 改变， □□□□□□□□□□□□□现。

描述： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□劣化 的运行状态，将受影响的 服 务恢复到全功能状态。 □□□□□□□□□□□□□□□□□□□□□□□□□无法成功删除所有未经授权访问的风险。 □□

结果： 采取措施将系统和 服 □□□□完全的 功能和容量 状态 □□□□□□□□□□□□□□、□□

□□□□□□□□□□□□□□□□□□□□

- 从 可信的 备份 媒质恢复 用户 /系统数据；
- 从 可信 的备份 媒质 或重建内容 恢复 配置；
- 启用禁用的 服 务并重建对用户 /系统 /□□□□□；
- 执行功能测试， 以在基础设施和应用 层面对 系统 /服务 /网络的容量和能力 进行检验。

6.4.4 □□□□□□□□□□□□□

目的： 使 服 务对象能够执行所需的管理和技术活动， 以便 □□□□□□□□□□□□□□□过来。

描述： CSIRT □□□□□□□□□□ 援助 □□□□ 服 □□□□□□□□□ 过来 并消除漏洞。这可能是对现场提供分析 服 务的 一种 □□□□□□□□□□□□□□□□□ CSIRT 可能选择通过更详细的解释、 建议等方式来支持 服 务对象对信息安全事故 做出响应。

结果： 改善 服 务对象的 响应， 使 □□□□□□□□□□□□□□□□□□□□□□□□□□□ 的未 来效能 和效率。此外，它有助于 为 服 □□□□ 那些缺乏详细技术知识的实体 提供支持，以 □□□□□□□□□□□□

6.5 服 □□□□□□□□□□

目的： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 体参与对信息安全事故的响应；并确保执行响应计划， 以及 相应地 对 □□□□□□□□□□□ 偏差 进行管理。

描述： 告知和知晓 与信息安全事故有关的详细信息和正在进行的活动对所有 □□□□□□□□ 和组织 而言 □□□□□□□□□□□□□□□□□□□□□□□□□□□ 需要 管理 者 的批准，因此在 对 任何信息安全事故 进行有效和高效处置 之前，这要求 □□□□□□□□□□□□□ CSIRT □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□′ □□□□□□ 确保 参与 活动的 所有各 方报告 和反馈情况，以提供准确的态势感知，直到 认为 信息安全事故 已停止且不再 需要 做 进一步协调 为止。

利益攸关方应有途径 来 提交问题、检查 □□□□□□□□□□□ CSIRT 报告问题。为了 吸引内部利益攸关方 参与， CSIRT □□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 益攸关方 参与， CSIRT 应保持与其他 CSIRT 和 CSIRT □□□□□□□□□□□□□□□□□□□ □□□□□□

结果： 基于对信息安全事故做出响应的、 消息灵通的实体，成功协调响应。

以下功能被视为本 服 □□□□□□□□□□

- 沟通；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- 活动协调；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.** 沟通。

6.5.1 □□□□□

目的： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

描述： 在 进行沟通 时， CSIRT 必须 精准考虑所沟通 的受众。 另一方面， □□□□□□□□□ CSIRT 还必须具备接收 来自 □□□□□ 输入 反馈、 报告、 □□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□CSIRT□□□□□□□□、安全和私密的方式与利益攸关方共享 信息。

□□□□□ 早地 提前 □□□□□ 协议，并相应地 确立沟通 资源。作为扩展，也可以使用 “禁令 下的信息 ”概念。因此，还必须建立保留策略，以确保 根据约束条件（如时间）来适当处置、□□□□□ 用于 制作 □□□□□ 和 信息本身，直到这些 约束条件 变 为 □□□□□ 可以 公开 披露 □□□

根据 利益攸关方 和 服 务对象 □□

结果：根据所有接收方和发送方的安全要求，所有 沟通渠道 均可用。

□□□□□□□□□□□□□□□□□□□□

- □□□□□□□□;
- □□□□□□□□。

6.5.2 □□□□□□□

目的：向 受到信息安全事故影响的实体 发出警报，或者向可 对响应 发挥作用 的实体 发出警报 并向这些实体提供所需的信息， 以了解其参与 响应将扮演 □□□□□ 对 □□□□□□□□□□□□

描述：安全事故涉及许多内部 实体 □□□□□□□□□□□□□□□□□□□□□ CSIRT 是接收潜在信息安全事故报告的中心，因此它们也 充当向经 授权 的联系 点 □□□□□□□ 中心。该通知通常不仅 将向任何同事 提供适当的技术 细节， 而且将向任何同事 □□□□□□□□ 和 联系点 □□□□

结果：需要参与响应 行动 或 需要了解信息的 实体 □□□□□□□□□□□□□□。

6.5.3 □□□□□□□□□

目的：□□

描述：随着对信息安全事故响应的 进展， 可能 会有 更多的、来自其他潜在安全专家、 CSIRT 或受 □□□□□□□□□□□□□□□

将某些信息和经验教训传递给知识转化 服 □□□□□□□ 的话 □□

结果：将可用信息分发给负责参与响应或需要随时了解 进度 □□□□□□□□□

6.5.4 □□□□□□□

目的： 跟踪所有沟通和活动的状态。

描述： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□态。 这涉及 CSIRT 请求采取的行动，或者 请求 共享更多 的 信息，以及 请求 对构件进行技术分析或共享损害指标 、关于 其他受害者 的 信息 等。 这主要 发生于 当 CSIRT 依赖于在其直接控制之外的 技能 和资源 的时候， 以 完成 缓解事故 影响所必需的行动。 但这也会发生于需要内部 CSIRT 来协调缓□□□□□□□□□□□□□

通过提供双边 的 或多边 的 协调， CSIRT 参与信息交换，使 这些 资源有能力 采取行动这样做，或者协助其他人 检测、保护或纠正 攻击者 正在 开展 的活动， 并 帮助 □□□□□□□□。

结果： 感知所有活动的当前状态以及参与响应之实体的状态的态势。

6.5.5 □□□□□

目的： 确保 涉及某项业务的所有 实体都 拥有关于 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

描述： 提供 关于 为响应信息安全事故而请求或进行 之 活动当前状态的简明 □□□□ 信息。及时的报告对实现有效的协调 而言 至关重要， □□□□ 着此类信息来，获得信息是持续 进行的 经 协□□□□□□□□□□□□□□□□□□□□□□□□

结果： □□□□□□□□□□□□□□□□□´□□□□□□□□□□□□□□□□□□□□影响的评估结果、 建议和要求 采取的 行动， 从而 有可能了解 有关 □□□□□□□ 所 制定计划的□□□□□

6.5.6 □□□□□□□

目的： □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 事实 信□□□□□□□□□□□□□□□□□

描述： 在许多情况下无法与媒体进行 沟通 □□□ CSIRT 通常会尝试避免这种接触，但重要的是要意识到媒体可以 帮助缓解 造成信息安全事故的 、 □□/□□□□□□□□□□□□□ CSIRT □□□□择 以 已适合向公众发布的方式 来 提供 本 □□□□□□□□□ CSIRT 内部的特定技能，而这些技能在大多数情况下都不容易获得。无论如何，如果 CSIRT 与媒体进行 沟通， 都 必须格外小心，以尽□□□□□□□□□□□□□□□□□□

结果： 开发 旨在 提供有关正在进行 之 信息安全事故的清晰 概要 □□□□□□□□□□□□□□采取的步骤， 或者 概述 所选响应策略，以便 □□□□□□□□□□ 过来。

6.6 服 □ □ □ □ □ □ □ □

目的： 向其他安全专家、 CSIRT 和 CSIRT 社群提供专业 技能 和联系人，以帮助缓解危机。

描述： 尽管当今的信息安全事故很少 会造成组织危机 或国家危机，但 它们 □ 少威胁着一个组织的存在。正如在危机管理中 所 确立的那样，高职位 角色 将接管 处理 危机的责 □

由于系统和网络可能 对 紧急情况 发挥作用或者 需要 将之 用于 响应 危机情况，因此 CSIRT 通常 □ 而且 提 供已建立的 服 □ □ □ □ □ □ □ □

结果： 危机管理团队可以使用 CSIRT 的资源来解决当前危机的网络安全方面 问题 。同时， 可将 CSIRT 的 沟通 资源用于与 服 务对象和外部 各方 的 □ □ □ □ □ □ □ □ □ □ □ 行动 或帮助。 利用 已建立的 沟通 方式和 可信 网络，也可以用一种 □ □ □ □ □ 来与 服 □ □ □ □ □ □ □ □

以下功能被视为本 服 □ □ □ □ □ □ □ □ □ □

- 向 服 务对象 分发信息；
- □ □ □ □ □ □ □ □ ；
- □ □ □ □ □ □ 。

6.6.1 功能： 向 服 务对象分发信息

目的： 提供已建立的沟通资源， 以帮助应对危机。

描述： 随着对危机响应 的进展 □ □ □ □ □ □ □ □ □ □ □ □ □ CSIRT 已为自己的目的建立了此类资 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 的 □ □ □ □ □

结果： 将 可用的信息分发给 服 务对象 □

6.6.2 □ □ □ □ □ □ □ □ □ □ □

目的： □ 之 视为其总体优先 级 和策略的一部分。

描述： 本功能 涉及提供有关 服 务对象内部网络安全当前状态的简明 而真实 □ □ □ □ □ □ □ □ 利用 危机 来 发起其他攻击，或者由于发生的攻击可能是导致此危机的 整体 □ □ □ □ □ □ □ 因此 对 □

CSIRT □ □ □ □ 服 务和 服 务对象提供 此类 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 策略 所要求的 或 所 期望的。无论如何，由于危机管理只能基于既定的信息流来成功 实施， 原因是 它依赖于协调资源来解决危机的最关键方面 问题 □ □ □ □ □ □ □ □ □ 而 准确。

由于正在进行的信息安全事故需要资源来处置它们，因此必须做出决定，在事故持续时间内是终止响应（并将当前可用的资源分配给其他区域）还是继续响应。只能根据可用的最佳态□□□□□□□□□□□□

结果：将向危机管理团队告知当前活动的范围、已完成的行动和未完成□□□□□将传达经评估的、对延误、□□□□□□□□□□□□□□□□□□有关用于□□□□□□□□□□□□□□□□□

6.6.3 □□□□□□□□□□

目的：□□□□□□□□□□□□□□□□□造成的影响通知其他实体。

描述：□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□之清楚地了解在危□□□ CSIRT □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□可能与 CSIRT □□□□□□□□□他们可能会认为危机正在过去。

□□□□□□□□□□□□□□□□□□而□□也可能导致丧失对 CSIRT 和 / 或宿主组织的信任。

结果：有关危机对 CSIRT 操作的影响的信息已分发给涉及响应公开的信息安全事故的服务对象和□□□□□□□□□□ CSIRT □□□□□□□□□□□□□□□□ CSIRT □□□□□□

7 服□□□□□□□

漏洞管理服务区包括与发现、分析和处置□□□□□□□□□□□□□□□□□□服务。漏洞管理服务区还包括与检测和响应已知漏洞有关的服务，以便□□□□□□□□□□□□服务区包含与新漏洞和已知漏洞有关的服务。

尽管有时使用“漏洞管理”这一术语来指代简单的、防止已知漏洞被利用的过程（例如，“扫描和修补”），但在本 CSIRT 服务框架中，这些活动被视为漏洞响应服务下的功能和子功能，该服务只是 CSIRT 可能提供的一种服务。对于许多 CSIRT，这些漏洞响应功能是负责安全漏洞扫描□□□□□□□□□□□□

以下服务被视为该服□□□□□服务:

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**。

很少有 CSIRT 会提供所有这些 服 务，而只会 提供 在其职责范围内 的那些 服 □□□□□CSIRT □□□□□服□□□□□□□□□□□□□□/研究）或者 从 第三方（漏洞报告 获取）中 了解 新漏洞，然后在需要时向其 服 务对象 发布 一个 □□□□□□□□□□□□ 不必 □□□□□□□□ 或开发解决方案的其他人员的任何协调工作（漏洞协调），或者不必 □□□□□□□□□□ 的 □□□□□□□□□

7.1 服 □□□□□□/□□

目的：查找、了解或搜索新的（以前未知的）漏洞；漏洞管理 服 务区的成员或通过其他相关的 CSIRT □□□□□□□□□

描述：□□□□□□□□□□□□□□□□□□□□□□□□□□ 本 服 务 包括 CSIRT □□□□□ 研究或其他 服 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 服 务 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ CSIRT □□□□□□□ □□□ □□□□□□□□□□□□□□□□□□□[6]）、其他外部资源（例如，高级 服 务、订阅），或 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ CSIRT □□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

结果：本 服 务可以增加对未直接报告给 CSIRT 的潜在漏洞的发现概率。

以下功能被视为本 服 □□□□□□□□□□

- 事故 响应漏洞发现；
- 公共 来源 漏洞发现；
- 漏洞研究。

这些功能可能是由其他人（例如，研究人员、供应商、PSIRT □□□□□□□□□ CSIRT 执行的 服 务（或功能）。

7.1.1 □□□□□□□□□□□

目的：确定作为安全事故一部分的、被利用的漏洞。

描述：在 分析安全事故的过程中，可能会发现表明 某个 漏洞 被攻击者利用 □□□□□□□□ 一个 以前未打补丁或未 予 缓解的已知漏洞，可能已 造成一个 事故；或者 可能 由 新的漏洞（零日漏 □□□□□

如果某个漏洞被用作事故的一部分，则 该 漏洞 的某些 信息可能作为信息安全事故管理 服 务区 服 务之一的输出 结果 而 被 接收。然后可以根据需要将信息传递 给 □□□□□□□□□□□ 服 □□

结果：将关于漏洞（怀疑它已被利用，作为安全事故的一部分）的信息 传递 给 漏洞管理 服 务

---

[6] 通过电子邮件接收到的新漏洞信息可被 看作是一项 漏洞发现 服 务、公共来源漏洞发现功能、漏洞报告 获取 服 □□□□□□□□□□□□□，□□□□□ CSIRT □□□□□□□□□□□□□ 漏洞信息。

□ □

7.1.2 □ □ □ □ □ □ □ □ □ □ □

目的： 通过 读取 公共资源或其他 第三方 □ □ □ □ □ □ □ □ □

描述： CSIRT □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 来 了解新漏洞。来源可以包括供应商公告、 安全网站、 邮件列表、 漏洞数据库、 安全会议、 社交媒体等。本功能还可以通过可能未完全向公众开放的其他 第三方 来源来 了解 新漏洞，例如， 通过付费 的 订阅或高级 服 务， 当中的 信 □ 进一步 审查 和共享。也可能从态势感知 服 务区的 服 务中接收类似的漏洞信息。

结果： 确定经 公共或其他外部来源 已 披露的新漏洞。

7.1.3 □ □ □ □ □ □ □

目的： 通过 审慎 活动或研究发现或搜索新的漏洞。

描述： 本 功能包括 因 特定 的 CSIRT 活动而导致的新漏洞发现，例如， □ □ □ □ □ □ □ 模糊化）或通过恶意软件 的 逆向工程，来 对系统或软件进行测试。

本功能还可以从信息安全事故管理 服 务区或 □ □ □ □ 服 务区的 服 务 中 □ □ □ □ □ □ □ □ □ 启动本功能， 以查找可疑的漏洞。

由于 本 漏洞研究功能而导致 发现 新 的 □ □ □ □ □ □ □ 事故 响应 服 务 之 □

结果： 通过研究确定新的漏洞。

7.2 服 □ □ □ □ □ □ □ □

目的： 接收和处理 服 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

描述： 漏洞信息的主要来源之一可能是 CSIRT 服 务对象或其他 第三方 □ □ □ □ □ □ □ □ □ CSIRT 应预期可能从这些各种 各样的 来源报告漏洞，并为漏洞报告提供机制、 □ □ □ □ □ □ □ □ □ □ 设施 可能包括电子邮件或基于 万维网 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 服 务对象或 第三方 通过已建立的渠道直接报告给 CSIRT。支持指南应包括报告指南、 联系信息和任何披露政策。

为了使 服 □ □ □ □ □ □ □ □ □ □ □ □ □ □ CSIRT 应该提供一种或多种机制以及有关 报告什么以及如何安全 地 报告漏洞的 指南 或 指令 □ □ □ □ □ □ □ □ □ □ □ □ □ 、网站、 □ □ □ □ □ □ □ 或门户网站， 或者 其他适当的方法，以使报告 能够 安全可靠地 予以 □ □ □ □ □ □ □ □ □ □ □ 纳入 作为漏洞报告表本身的一部分）应在单独的文档中或通过网页 来 □ □ □ □ □ □ □ □ □ 纳入 报 □ □ □ □ □ □ □

结果： 接收 漏洞报告，以专业且一致的方式 来获取 □ □ □ □ □ □ □ □ □ □ □ □ 检验 和分类。

以下功能被视为本 服 □ □ □ □ □ □ □ □ □ □

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**。

7.2.1 □□□□□□□□□

目的：接受或接收服务对象或第三方报告的、关于漏洞的信息。

描述：有效获取漏洞报告需要一定的机制和过程来从服务对象、利益攸关方和第三方（发现者、研究人员、供应商、PSIRT、其他 CSIRT 或漏洞协调员等）接收报告。漏洞信息可包括受影响的设备、利用漏洞所需的条件、□□□□□□□□□□′□□□□□□□□□□□□□□□采取的行动、修复和/□□□□□□□□□□□□□□□□□□□可作为其他服务输入的一部分□□

结果：妥善处理来自服务对象或第三方□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□

- 定期监视沟通□□□□□□□□□□的、与 CSIRT 的联系方式是否有效以及报告是否可□□□；
- □□□□□□□□□□□初始确认信息，必要时请求额外□□□□□□□□确立期望的结果。

7.2.2 □□□□□□□□□□□□

目的：对漏洞报告进行初始□□□□□□□□□□□□□□□

描述：对漏洞报告进行审查和分类，以对所议□□□□□□□□□□□□□□□□□□□□□对漏洞进行处理以进行进一步分析、从报告者或其他来源寻求额外信息、确定不需要对漏洞采取进一步行动）。根据漏洞报告中提供的信息的详细程度和质量，□□□□□□□□□□□是否存在新的漏洞。

除非有理由拒绝漏洞报告，否则应将漏洞□□□□□□□□□服务以做□□□□□、分析和处理。如果 CSIRT 不提供漏洞分析服务，则应将报告安全地转发给一个外部的小组进行处理，例如，受影响的供应商、PSIRT 或漏洞协调员。

结果：确定可用的信息，以决定下一步的行动。

以下子功能被视为本服务实施方案的一部分：

- □□ CSIRT 成功实施攻击；
- 基于可用的分类或优先级排序结果□□□□□□□□□□措施的一些反馈意见，来更新对报告的确认；
- 将有关已处置之漏洞的新信息与可用的数据合并，以便□□□□□□□□□□□

7.3 服 □□□□□□

目的：分析并了解已确认的漏洞。

描述：漏洞分析 服 □□□□□□□□□□□□□□□□□□，□□□□□□□□□□ 基本 问题或缺陷（根本原因），以及确定一种或多种 修复 或缓解策略 来 防止 或 □□□□□□□□□□

漏洞分析 服 务和功能可以并行地继续进行，而漏洞协调 服 务和功能则与 经 协调的漏洞披露（CVD）[7]流程 中 的 其他 参与者一起 进行。

结果：增加 对漏洞关键细节 的了解（例如，描述、影响、解决方案）。

以下功能被视为本 服 □□□□□□□□□□

- □□□□□□□□□□□；
- □□□□□□□□；
- 漏洞 修复措施 开发。

7.3.1 □□□□□□□□□□□□□□

目的：□□□□□□□□□□□□□□□□□□□□□□

描述：漏洞分析 服 □□□□□□□□□□□□□□□□□□□□□ˊ □□□□□□□□□□□否对所涉及的系统 有 某种影响 以及是否 与 CSIRT 的职责 权限 相关。如果漏洞 是 由 服 务对象 或第三方报告给 CSIRT 的，则其中一些漏洞可能已在（漏洞报告获取 服 务的）□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□ 指配 给 某个 □□□□□□□□□□□□□□□认，证明该漏洞对所涉及的系统有一定影响 以及 与 CSIRT 的 职责权限 相关（即对网络或 系统潜在安全影响，在 根据其职责 权限的 CSIRT 区域内，可导致 信息资产机密性、可用性或完整性 的损害）。

结果：□□□□□□□□□□□□□□□□□□□□□□

7.3.2 □□□□□□□□□□□

目的：□□□□□□□□□□□□□□□□□□□□□□□

描述：本 分析的 目标 □□□□□□□□□□□□□□□□□ 存在 的 情形 □□□□□□□□□□下可 因此而 利用 该 漏洞。本 分析还可能试图了解用于引发事故的弱点以及用于利用该弱点的 对抗性间谍情报手段。依据 漏洞性质，CSIRT □□□ 的 产品供应商或开发 人员或者其各自的 PSIRT 来执行。漏洞也可能存在于 一个以上的产品中，在这种情况下，可能需要对受影响软件或系统进行多次分析，因此 需要与多个供应商、PSIRT 或利益攸关□□□□□□

---

[7] 有关 经 协调的漏洞披露（CVD）的相关信息，请参阅漏洞协调和漏洞披露 服 务区。

结果： 了解漏洞以及恶意行为者能够使用此漏洞的方式， 将 有助于 确定 修复 □□□□□□□□ 以最大程度地降低 漏洞 暴露或 被 利用的风险。

7.3.3 □□□□□□□□□□□

目的： 确定 必要的步骤，以修复（修补） 潜在的 漏洞 或者缓解（减轻） □□□□ 漏洞的影响。

描述： 理想情况下，本功能 将 确定 漏洞的 修复 或 修补措施 □□□□□□□□□□□□ 的 补丁 或 修补 程序，则建议 采用称为缓解措施的暂时 解决方案或 变通 方法，例如，□□□□□□□□ 或者做 配置更改，以最大程度地降低 该 □□□□□□□□□□□□□□ 修复 □□□□□□□□□ 缓解措施（变动 方法）的实际应用或部署是 某 单独 服 务的 一项 功能，在 本 □□□□□□□□ □□

作为漏洞分析 服 务和 修复措施 □□□□□□□□□□□□□□□□□□□□□□□□□□ 如，对 程序或设计的更改 进行检验、 由 第三方对修复措施进行 审查， 或者确定在修复步骤 中 引 □□□□□□□□□□□□□□□□□□□□□□□□□□□□

本功能通常 将 □□□□□□□□□□□□□□□□□□□□□□□□ 由其他 服 务或功能 来 □□□□□□□□□□□□□□□

结果： 建立计划，以更改（修补）软件代码、 实施 变通 方法，或者 改善流程、 □□□□□ /或设 □□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□

- 漏洞修复 /补丁程序开发；
- 漏洞缓解 措施 开发。

□□□□□□□□□□□□□□□□□□□□ PSIRT□□□□□

7.4 服 □□□□□□

目的： 与参与经协调的漏洞披露（ CVD）流程的参与者交换信息，并对活动进行协调。

描述： □□□□□□□□□□□□□□□□□□□□□□□□□ /研究人员、受影响的供应商、 □□□□□ PSIRT□□□□□□□□□□□□□□□□□□□□□□□□□□ CSIRT□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□

结果： 与 CVD □□□□□□□□ 他们 可帮助 提供信息，以有效而 及时地 修复 /缓解 漏洞。

以下功能被视为本 服 □□□□□□□□□□

- 漏洞通知 /报告；
- 漏洞利益 攸关方 协调。

7.4.1 □□□□□□□ /□□

目的： 与将要参与 CVD 过程的其他人初步共享或报告新的漏洞信息。

描述： 大多数漏洞的 处置都 涉及 通知多方、 □□□□□□□□□□□□□、开发人员、 PSIRT，或者 其他可以一起工作的 可信 的专家（例如，研究人员、 CSIRT、 漏洞协调员））合作以及 与多方 协调 交换 相关信息， 以 分析 并 修复漏洞。

结果： 告知 □□□□□□□ CVD 参与者） 有关 漏洞 的情况， 供应商 可以采取行动制定补救或缓□□□□

7.4.2 □□□□□□□□□□□□

目的： 在 涉及经 协调 的 漏洞披露（ CVD）工作的 各个 □□□□□□□□□□□ 开展 后续的协调和□□□□□

描述： 在 发现者 /研究 人员、 供应商、 PSIRTS 和参与 经 协调 的 漏洞披露（ CVD） 工作 的任何其他参与者之间 协调 交换 信息， 以分析和修复漏洞并为漏洞 披露 做 好 准备。这种协调还应包括 各 参□□□□□□□□□□□□□□□□□□

结果： 在 能 开发或宣布 修复 /缓解解决方案的参与者间更有效、更 及时和 更 负责 地 共享 漏洞信息。

□□□□□□□□□□□□□□□□

- □□□□□□。

7.5 服 □□□□□□

目的： 向 服 务对象传播关于 已知漏洞的信息，以便 其 可以根据 这些 □□□□□□ 来 预防、 检测和 修复 /□□□□ 的 漏洞。

描述： 将任何 已知的 漏洞 （攻击 者可能 的进入点） 告知 服 务对象， 以便其 □□□□□□□□□ 情况 保持最新状态 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□、电子邮件、 社交媒体） 、 漏洞数据库或其他媒体来发布信息。 本 服 务通常但并非总是 发生 在漏洞□□□□

结果： 知情的 服 □□□

□□□□□□□□服□□□□□□□□□□

- □□□□□□□□□□□□□；
- 漏洞公告 /沟通 /传播；
- 漏洞披露 后的 反馈。

7.5.1 □□□□□□□□□□□□□□□□

目的： 制定并维护一种策略，这种策略为 CSIRT 如何处置和披露漏洞以及用于披露漏洞的机制提□□□□□□□□□□□

描述：处理漏洞报告的 CSIRT 应该确定其漏洞披露政策，并将之提供给其服务对象、利益攸关方和 CVD 参与者，最好将之发布在 CSIRT 网站上。漏洞披露政策将为利益攸关方提供透明度，并有助于推动制定适当的披露政策。政策范围可以从不披露（不披露任何□□□□□、有限公开（仅披露某些信息）到完全披露（披露所有信息），当中可包括对漏洞□□□□□。披露政策应包括诸如政策范围、对任何报告机制和导则□□□□□□□□□□□□□□表和机制等因□□

结果：增加对披露的信任、协作和控制，并改善与 CVD □□□□□□□□□□

7.5.2 □□□□□□□/□□/□□

目的：向服务对象（或公众）提供有关新漏洞的信息，以便他们可以采取检测、补救或缓解措□□□□□□□□□□□□□□□

描述：将漏洞信息披露给已定义的服务对象□□□□□□□□□□□□确定□□□□□□□□来□□□□□□□□□□□□□□□□□□□□□□□□□□□□沟通可以采取公告或安全咨询报告的形式，通过电子邮件或文本消息发布□□□□□□□□□□□□□□□□□□□网站或社交媒体渠道上，或者采取其他适当的沟通和渠道形式。□□□□□□□□□□应遵循某种确定的格式，它通常可以包括以下信息：概述或描述、唯一的漏洞标识符、影响、严重性或 CVSS 评分、解决方案（修复或缓解措施）以及支持性参考文献或材料。

结果：通过向服务对象（或公众）提供及时、高质量、有效的信息来预防、检测和修复/缓解漏□□

7.5.3 功能：漏洞披露后的反馈

目的：接收并响应来自服务对象的、□□□□□□□□□□□□□□□□

描述：在披露一个新漏洞后，CSIRT 可期望以问题形式从某些服务对象处收到有关漏洞文档的后续通报。如果有保证□□□□□□指明□□□□□□□□□□□□□´□□□□□□□□服务对象的信息可能只是对漏洞文档的确认或接收，或者服□□□□□□□□□所建议的修复/缓解措施时存在问题或困难。如果确定漏洞已被利用，则因漏洞披露而使服□□□□□□□□□□的事故。此类报告应纳入 CSIRT 事故报告服务的功能中。

结果：漏洞披露后，任何问题或协助请求都将得到及时响应。

7.6 服□□□□□□[8]

目的：主动获取有关已知漏洞的信息，并根据信息采取行动，以防止、检测和修复/缓解这些漏□□

描述：本服务下的功能旨在确定服□□□系统中是否存在透露的漏洞，这通常通过刻意的行动来进行，以查找是否存在此类漏洞。本服务还可以包括后续操作，以便□□□□□□□□□变

---

[8] 尽管有时将检测漏洞的功能和子功能称为“漏洞管理”，但本 CSIRT 服务框架将这些功能和子功能称为本漏洞响应服务的一部分，它是本框架中名为漏洞管理的更大服务区的一部分。

通 策略来 修复 或缓解漏洞。

结果： 对信息采取行动，以检测 是否存在 漏洞 、对 □□□□□□ 进行修复 /缓解， 并防止漏洞被 □□□

以下功能被视为本 服 □□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.** 。

本 □□□□ 服 □□□□□□□□□□ 一个 □□□□□□□□□□□□□□□ CSIRT） 来 执行。 也不太可能由 协调 CSIRT 来 提供本 服 务。

7.6.1 □□□□□□□/□□

目的： 积极参与 搜寻 □□□□□□□□□□□□□□□

描述： 本功能的 目标 是在 漏洞被利用或者对 网络或设备 □□□□□□□□□□□□□□□□□ 未予缓解的漏洞进行 □□□□□□□□□ 响应 有关某个 新漏洞的公告而 被 □□□ 或者可能 作为对已知漏洞定期 、按 计划扫描的一部分来实现。为了有效提供漏洞检测 功能， 拥有系统清单 将是 有用 的 。拥有 这样一个清单以便 查询软件版本信息，可使组织 对 其基础 设施 中新报告漏洞的可能 流行情况快速做出评估 。

该功能可以接收输入 或者 从其他 服 务和功能 来 触发。

结果： 通过正式流程或旨在 识别 的工具来检测漏洞。

□□□□□□□□□□□□□□□□

- **Error! Bookmark not defined.**/搜寻；
- □□□□□□/渗透测试 。

□□□□□□□□□□□□□□ IT 服 务 商 、 SOC、第三方专家、系统所有者）来执行。

7.6.2 □□□□□□□

目的： 通常通过及时应用供应商提供的补丁 程序 或其他解决方案来 修复 □□□□□□□□□ 漏洞 被利用。

描述： 漏洞修复旨在解决或消除漏洞。对于软件漏洞， 这 通常以软件更新或补丁 程序 的形式 ，□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□/□□/□□□□□□ □□□□□□□□□□□□□□□□□□

结果： 防止或减少暴露在漏洞被利用的威胁下。

□□□□□□□□□□□□□□□□

- □□□□□□□□□□；
- 漏洞缓解。

□□□□□□□□□□□□□IT、SOC□□□□□□□□□ CSIRT 来执行。

8 服□□□□□□□

态势感知包含以下能力，即确定、处理、理解和传达有关 CSIRT 职责范围内以及周边正在发生之事情的关键要素，这些发生的事情可能会影响其服□□□□□□□□□□□□□□□□□解当前状态，以及确定或预测该状态的可能变化。本服务区包括确定如何从不同的领域收集相关信息、如何整合这些信息以及如何及时传播信息以帮助服务对象做出更加明智的决定。一些□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ CSIRT □□□□□□□性、对情境的了解、技术能力、对资产的访问、外部连接以及防止事故的使命来提供该功能。态势感知不仅仅专注于对事故的响应，它是一项服务，旨在确保数据、分析结果和行动可用于其他服务，例如，安全事件管理、事故管理和知识转化。它还确保将来自其他服务区的信息适当地整合在一起，并及时传回给适当的服务对象。

以下服务为本服务区提供的服务：

- 数据采集；
- 分析和综合；
- 沟通。

8.1 服□□□□□□

目的：收集有助于提高可视性的数据，指明有什么内部的和外部的□□□□□□□这些活动可能会影响服务对象的安全态势。

描述：征集、收集、□□□□□服务对象的信息需求□□□□□□□□□□□□□□□□□□活动。本服务包括以下保障活动：收集相关信息（□□□□□□□□□□□□□未来事件；报告和输入信息；过滤收集到的信息；组织信息，以用于事故分析、预防、□□□□□□□□例如，规划或趋势分析）；存储信息，以供后续使用；提高信息的“可搜索性”等等。收集到的数据□□□对重要环境要素的基本了解，其他服务形成错误图片的风险就会增加。CSIRT 需要制定政策和程□□□□□□□□□□□□□□□□□□

结果：

本服务产生以下构件：

- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
  □□□□□□□□□□□

- 有关 服 务对象资产和活动 的、 当前和预期 之 □□□□□□□；
- 有关外部事件或趋势的信息， 用于洞察 服 务对象的 周边 □□□□□□□□□□□、方法、 做法、 风险和威胁;
- □□□□□□□□□□□、适当 格式 化 的信息。

□□□□□□□□服□□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**。

8.1.1 功能： 策略 汇总、 提炼和指导

目的： 确立 服 □□□□□□□□□□□ 情境，以了解 应发生于 基础 设施 □□□□□

描述： 策略 的 收集、 □□□□□将□□□□□□□□□□□□□□□□□□□□□□□□ 它确立 服 务对象及其基础 设施 □□□□□□□□□□□□□□□□□□ CSIRT，情境包括了解组织可接受的政策、 计划、 正常 的 工作条件、 接受的风险和 做出的 权衡。 了解情境 将为 评估 观察 结果 □□□□□

结果： 了解在 服 务对象中 正在 发生的、 可接受的 观察 结果。 专注于了解对 基础 设施 和 资产 的更 □□□□□

8.1.2 □□□□□□□□□□□□□□□□□□□□□□

目的： 提供有关现有资产、 □□□、基 线 □□□□□□□□□□□□□□□□ 异常 态势 观察 结 □□□□□□□

描述： CSIRT 团队需要了解 服 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□

- □□□□□□□□□□□□□□□□□□□
- 经 授权 的 设备及其用途;
- 经 批准的 过程 □□□□□□□□□□□□□□□□□□□□□□□□□□ 服 务对象 提供 服 务。

本信息有助于确定潜在风险 之 资产的优先级，从而可以为事故管理活动提供 情境 。 CSIRT 团队可获得的信息越 准确 ，就越容易推断出安全问题并对 之 采取措施。准确的信息可能意味着 CSIRT □□□□□□□□□□□□ˊ □□□□□□□ 、最新的硬件和软件清单以及详细的网络 □□

结果：

□□□□□□□□□□□□

- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□
- 资产和功能面临的主要风险的列表。

□□□□□□□□□□□□□□□□

8.1.3 □□□□□

目的：收集信息以支持分析和解释服务和/□□□ CSIRT 服务。

描述：□□□□□□□□□□□□□□□□□□要求。收集包括识别□□□□□□□□，与信□□□□□□□□□□□□□□□服务对象、□□□□□□□ CSIRT □□□□□□□□、内部活动（例如，组织变更）、技术发展、外部事件、政治事件、攻击趋势、□□□□、会议、可获得的培训等等。

数据收集功能支持其他服务，例如，□□□□□□□□□□□□□□□□□□□□□□□服务中的功能和活动，例如，分析、预测、响应和风险缓解。最新收集的信息可表明，对服务对象的攻击比以往更可能发生。外部事件可能揭示可在一段时间内用于□□事故处置。

结果：收集和生成数据与数据集以提供可被其他服□□□□□□□□□□□□□□□□□□情境，以便为服务对象创建态势状况、确定警报，或者制定计划以缓解资产和支持性基础设施面临增大的风险区域。

8.1.4 □□□□□□□□□□□

目的：建立可靠、一致且最新的数据集，以支持 CSIRT 活动和分析服务的需求。

描述：数据处理和准备包括对一组数据进行转换、处理、归一化和检验。通常由于大量误报，□□□完整分析之前，需要将新数据与历史数据结合起来。作为准备过程的一部分，对某些类型的数据（例如，新闻报道）可能需要进行分析或处理。一个例子是从新闻报道□□□□□□□□□息（例如，名称、日期、地点、技术信息、弱点、□□□□□□□□□□□□□□□□□□□□□□□□□□

某些分析方法要求数据以相同的格式进行存储，或者要求□□□IP □□□□□□信息，例如，自治系统标识符、国家/□□□□□□□□□□□□□□□□□□□□□安全团队□□□地点等等，来充实其资产清单数据。

结果： 数据可用， 并 可供其他 服 务或功能使用。

8.2 服 □ □ □ □ □ □ □

目的： 当状况 与预期不符时（例如， 当 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 进行评估 。

描述： 使用当前数据 、 历史记录和分析技术来确定 正在发生之事件 □ □ □ □ □ □ □ 服 务对象的资产和安全状况） 的过程 □ 可 揭示事件 □ 示对当前和未来 情况 的影响。例如， 系统可记录用户 ID 已成功登录系统，但系统 不指明 事件是否由合法 的 用户 来 执行。 将需要把 新的来源（例如， 与用户的访谈）纳入分析中，以便为团队提供更 加 准确的 景象， 以确定事件的合法性。可使用多种技术来分析和解释 所 收集的数据及其对 服 务对象的影响。

结果： 得出 一组 关于 服 务对象 内 可能 之 历史 、 当前和 / 或 未来 可能发生 之 事件的结论。它还可能包括有关 服 务对象 正 面临 之 某些 决定 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ ， □ □ □ □ □ □ □ 来源收集的 观察 数据，以及分析人员通过各种方法对 该 证据 所做 □ □ □ □ □ □ □ 可能涉及 需要告知 其 结果的 服 务对象 以及需要告知 服 务对象 的内容。

以下功能被视为本 服 □ □ □ □ □ □ □ □ □ □

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**。

8.2.1 □ □ □ □ □ □ □ □

目的： 分析数据采集过程中收集的信息，以 确定 当前 的 或预测 未来 的 态势状况 。

描述： 根据 所 □ □ □ □ □ □ □ □ □ □ □ □ □ 态势 □ □ □ □ □ □ 近期 可能的 状况 □

结果： 更新 态势状况 以及 有关态势状况 何时 □ □ □ □ □ □ □ □ □ □ □ □ 的知识。

8.2.2 □ □ □ □ □ □ □ □ □ □ □ □ □ / □ □ □ □

目的： 确定并确认 服 务对象 当前 态势 状况的详细信息。

描述： 基于外部 的 和内部 的 信息 与 趋势， 系统 地和 经常 地 针对网络边界 □ □ □ □ □ 的异常活动进行搜索。 协助 服 务对象 □ 论 。 例如，如果防病毒传感器发送了 有关 可疑文件的警报，则 安全 团队可以 对 系统配置 、 传感器配置 、 被 告警 的文件 、 当时的用户活动 等等进行分析， 以得出有关 观察结果 严重性 的结论 。 本 功能可 接收 来自安全事件管理 服 务区的重要输入 。 来自用于检测事件的传感器的 观察 结果可以在多个 服 务之间共享。

CSIRT 团队还需要根据有关威胁的特定信息片段来确定当前的态势状况。有时将这种活动称为“威胁搜寻 ”。通常，威胁搜寻涉及准备环境以检测特定的威胁活动，或者搜索可能已经存在的特定的威胁活动。

结果：根据对服务对象中事件的检测情况来更新态势状况。

8.2.3 □□□□□□□□□□□□□□□

目的：在事故期间确定新的见解，以帮助限制损失、缓解未来风险或确定新出现的弱点。

描述：对特定证据进行分析有助于确定见解以支持事故解决。有时，CSIRT 可能会集中其态势分析以支持特定的预期结果，例如，□□□□□□□□□□□□□□□□□□□□□□□□□□影响，响应者可能会要求对选择进行分析（例如，影响、成本、失败风险）。服务对象的决策需求可能会随其态势状况的变化而变化，CSIRT □□□□□□□□□□□□□□□其提供协助。该活动与事故管理服□□□□□□□□□□□□□□□□□□□□态势状况□□□□□□□□□□□□□□□□□

结果：基于新的观察结果，增强事故管理功能的态势感知能力。基于□□□□□□，更新态势状况。

8.2.4 □□□□□□□

目的：确定给定观察结果或可能观察结果对态势状况的预期潜在影响。

描述：本功能确定推测或推断可能对当前或□□□□□□态势□□□□□□□□□□□□□□或降低某些风险，例如，数据丢失、系统宕机或者□□□□□□/可用性 /完整性的影响。

结果：对推断或推测可能对态势产生的影响做出分析。

8.3 服□□□□

目的：通知安全社群中的服务对象或其他人员有关态势状况中的风险变化情况。

描述：从态势感知中获得的知识必须传达给服务对象。这将使之能够对观察结果做出反应并采取行动来改善防御状况，例如，□□□□□□□□□□□□□□□□□□□□第三方的风险。

结果：将准确、可行和及时的态势信息传递给服务对象，使之□□□□□□□□□□□□□□善其当前和将来的态势状况。

以下功能被视为本服□□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- 传播 /整合 /信息共享；

- □□□□□□。

8.3.1 □□□□□□□□□□

目的：告知服务对象（和其他成员□□□□态势状况及其变化情况。

描述：一旦完成分析和解释的结果，就可以通过内部和外部沟通流程将之□□□□□□□对特定的信息片段，根据谁需要了解之来分配。沟通包括交付方法和要交付□□□□CSIRT 团队可能会传达新的信息及其将如何改变态势状况。这样的一个例子就是报告预期的变化，即在一个事故期间它所观察的新恶意技术将对服务对象成员造成何种□□□□□□□□□□□□□□□如，最有用的充实数据来源，以及服务对象可以用来提升自身态势感知能力的措施。

结果：服务对象能更好地了解情况，并准备采取行动或做出决定，以改善其安全或状况。

8.3.2 □□□□□□□□

目的：创建结果、构件或调查结果，以其可以理解的方式和格式，□□□□□□□□□□□□关键信息传达给受众。

描述：报告和建议应明确指出服□□□□□□□□□□□□□□□□□□□□□□□之预期结□□□受众清楚地说明用于创建调查结果的方法，以便其也可以对提出的主张□□□□。CSIRT 团队可以创建有关单个事件、一系列事件、趋势、样式、可能发生之□□□□□□□□□□□□□□其服务对象了解态势状况的需求。

结果：改善提供关于态势发展状况之准确、及时和完整报告、提供支持结论之证据和/或提供关于可能采取之行动及其对服务对象之□□□□□□□□□□

8.3.3 □□□□□

目的：根据沟通情况来适应服务对象环境，以便更加从容地应对态势变化□□□做出反应。

描述：在某些情况下，CSIRT 团队可能还会对安全基础设施的某些部分做出□□□□□□□□□根据态势分析，更改针对特定蜜罐的防火墙规则。

结果：根据接收到的通报（包含分析、推测和/或建议），服务对象采取行动或对基础设施进行□□□

8.3.4 □□□□□/□□/□□□□

目的：汇编、□□□□□□□□□□□服□□□□服务对象外的其他人共享信息。

描述：

□□□□□□□□□□□□□

- □□□□□□□□与□□□□□□□□□服务的结果；

- 确定正确目标，以接收信息；
- 使 分析结果 可用；
- 确保交付成功；
- 跟踪和报告信息共享 情况；
- 将相关信息发送 给 □□□□ 服 务， 以进一步使用和传播。

结果： 态势感知分析输出 结果 用作关键决策流程（例如， 威胁搜寻 、 事故分析 、 解决方案）的输入（在 内部 以及在 服 务对象间）。 分发 输出 结果，作为 处理或检测事故的一部分。来自态势感知的信息和数据也可以通过知识转化 服 务区 而 成为最佳做法 、 报告 、 培训和 宣传 材 □□

8.3.5 □□□□□□□□□

目的： 确保信息传输成功且可用。

描述：

□□□□□□□□□□□□□

- □□□□□□□□□□
- □□□□□□□□□□□
- □□□□□□□□□□□

结果： □□□□□□□□□□□□□□□□□□□□ 服 务对象和其他社群成员就会收到信息。 □□□□□□□□□□□□

8.3.6 □□□□□

目的： 提高从内部和外部来源接收 之 数据的质量 、时效 性 、 □□□□□□□□

描述： 本功能涉及提供和接收有关 服 务对象 、 其他 服 □□□□□□□□□□□□□□ 、 接收和使用 之 信息的反馈 意见 。收到的信息是否准确 、 适用 、 及时 、 具有战略意义 、 是否新 / 新颖等？ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ CSIRT□□□□□ 来源）提供有关签名 □□□□□□□ 蜜罐 □□□□□ IOC、 警告 、 威胁 、 缓解措施等的 信息 。知识转化 服 务区也可以执行 此 活动 。 如果是这样，则应将结果传回态势感知 服 务区。

结果： 向内部和外部来源提供 观察 结果 和反馈 意见 ， 以便 提高所接收信息的准确性 、时效 性 、 □□□□□□□

9 服□□□□□□□

凭借其服务的性质，CSIRT 处于独特的位置，可以收集相关数据、执行详细分析并确定威□□□服□□□□□□□□□□□□□□□□□□

以下服务被视为该特定服□□□□□服务:

- 树立意识；
- 培训和教育；
- 训练；
- 技术和策略咨询。

9.1 服□□□□□□

目的：增强服务对象的整体安全状况，并帮助其成员检测、预防事故以及从事故中恢复过来；确保服务对象更好地处于就绪状态并得到□□□

描述：本服务包括与服务对象、专家和可信的合作伙伴一起工作□□□□□□□□共同了解，□□□□□□□□□□□□□□□□□□□□□□□□□□

结果：使服务对象树立以下必要的意识：

- □□□□□□□和安全操纵能力的事件、活动和趋势；
- 检测、预防和缓解威胁与恶意活动应采取的步骤；
- 安全及运营最佳做法。

以下功能被视为本服□□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- 外展。

9.1.1 □□□□□□□□□□

目的：汇总、整理可分发给服务对象的信息□□□□□□□，以改善安全状况并防止和缓解风□□

描述：本功能涉及研究和汇总与编写宣传材料和报告有关的信息，包括来自其他服务/功能的结果，尤其是来自安全事件管理、事故管理和态势感知服务区的信息。

结果：汇总关于相关趋势、正在发生之□□□□□□□□□□□□□□□□□□□□编写报告□□□□□□

9.1.2 □□□□□□□□□□□□

目的：使用经汇总和研究的相关信息来生成不同媒体中的材料，目标是□□□□好的方式来触达不同的受众或交付特定的内容。

描述：本功能涉及为各种受众（技术人员、管理人员、最终用户等）生成□□□□□□□□□式，例如，演示文稿、短片、卡通、小册子、技术分析结果、□□□□□□□□□□

结果：利用各种有效的交付技术和平台，生成质量适当的 CSIRT 报告和宣传材料，以满足服务对□□□□□

9.1.3 □□□□□□□

目的：传播与安全有关的信息，以提高对安全实践的意识和实施。

描述：本功能涉及实施信息传播过程，该过程可帮助 CSIRT 根据不同受众和内容的特性，为其服□□□□□□□□□□□□□□□□

结果：实施信息传播框架，以使 CSIRT 服务对象能够通过不同的方法（包括播客、博客文章、社交媒体文章和视频、新闻稿、广告、活动、公共报告等）来访问及时和□□□□□□

9.1.4 □□□□□

目的：建立和维护与专家或组织的关系，这些关系可能对履行 CSIRT □□□□□□□□□□□□□

描述：本功能涉及建立合作伙伴关系、促进合作以及吸引服务对象内或服□□□外的关键利益攸关方，其目标是：传播意识和最佳做法；帮助服务对象和外部利益攸关方了解 CSIRT 可以提供的服务和利益；帮助 CSIRT 更好地了解服务对象的需求；并促成完成 CSIRT 的使命。这可能涉及□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

结果：□□□

9.2 服□□□□□□□

目的：针对与网络安全、信息保证和事故管理有关的主题，为 CSIRT 服务对象（可能包括组织和 CSIRT □□□□□□□□□□□

描述：一个培训和教育计划可帮助 CSIRT 建立关系并改善其服务对象□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

- □□□□□□□□；
- 帮助服务对象了解不断变化的形势和威胁；
- 促进 CSIRT 与其服务对象之间的信息交换；
- □□□□□□□□□□□□□□□□□□□□□□□服务对象进行培训。

这可以通过各种类型的活动来完成，包括记录所需的知识、 □□□□□□KSA）、编写教育和培训材料、提供内容、指导以及专业和技能开发。这些活动中的每一项都将共同为服务对象和安全团队的能力发挥作用。

结果： 提供一致的培训和教育计划，使 CSIRT 的服务对象能够适当地获得。

- □□□□□□□□□□□□□；
- 帮助保护关键资产的工具和做法；
- 了解事故管理流程以及如何获得帮助。

□□□□□□□□□服□□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**。

9.2.1 □□□□□□□□□□□□□□□□

目的： 根据必需的 KSA，正确评估、识别和记录服 □□□□□□□□□□□□□□□□□□□□□□□□□□□□

描述： 本功能涉及收集知识、技能和能力（ KSA） 需求以及服务对象关于确定应提供什么培训和□□□□□□

结果： 表征和记录服务对象的 KSA 需求，作为编写相关教育和培训材料的基础。

9.2.2 □□□□□□□□□□□□

目的： 以服务对象的 KSA □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□方法被确定为是针对 □□□□□交付特定内容的最佳方法。

描述： 本功能涉及创建或者获得教育和培训材料的内容，例如演示文稿 □□□□展示内容、仿□□□□□□□□□□□□□□□

结果： 使用各种各样的和有效的展示技术与平台来制作 CSIRT □□□□□□□，这些材料具备适当的质量，并满足服 □□□□□□□

9.2.3 □□□□□□□

目的： 根据不同受众和内容的特性，制定正式的内容交付流程，以帮助 CSIRT 最好地将内容交付给其服务对象。

描述： 本功能涉及将知识和内容 传递 给 “学生 ”。这可以通过多种方法来实现，例如， 基于计算机的 形式 /□□□□□ CBT/WBT）、 讲师指导 下进行、 虚拟 方式、 会议、展示、 实验室 、 夺旗（ CTF）竞赛 、 书籍 、 在线视频等。

结果： 设计了一个内容交付框架，以帮助 服 □□□□□□□ 可选的 方法 □□□□□□□□□□ 流程等， 包括书籍 、 手册 、 在线视频 、演示文稿、 动手实验室 、 CTF、 CBT/WBT、 亲自参加 培训等， 其结果是使 服 务对象成员了解所 交付 □□□□

9.2.4 □□□□□

目的： 为 CSIRT 员工、 服 务对象成员或外部可信合作伙伴制定计划，以通过建立的关系向经验丰 □□□□□□□

描述： 指导 计划可以帮助 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□ 识、人生和职业经验（超出了 安全团队 的 正式 □□□□□□□□□□□□□□□

结果： CSIRT 安全团队 的 坚持 、 忠诚 、 □□□□□□□□□□□□ 总体能力 都得到了提升。 服 务对象提高了技能水平，与其 CSIRT 建立了更好的关系。 服 务对象和 CSIRT □□□□□□ 得到提升 □□□□□□□□□□□□□□□□□

9.2.5 □□□ CSIRT □□□□□□

目的： 帮助 成员 成功地并且适当地规划和发展其职业。

描述： 一旦确定适当 的技能， CSIRT □□□□□□□□□□□□□□□□□□□□□□□□□ □□□ □□□□□□□□□□□□□□□

结果： 有 具备 所需 之 技术 和 软技能 并了解 过程的 、 成熟的 且 经过培训的 □□□□， 且根据工作 □□□□□□□□□□□□□□□□ CSIRT □□□□□□□□□□□□□□□□□□□□□□□ □□□□□

9.3 服 □□□□

目的： 开展训练旨在提高网络安全 服 务和功能的有效性和效率。

描述： 组织向 服 务对象 提供的 服 务，用于 □□□□□□□□□□□□□□□□□□□□□ /或评估单个 服 务对象 或者作为一个整体的 利益攸关方社群的 □□□□□□□□□□□□□□□

- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□， 这 通常 是在 纸上 /桌面 □□□ 训练；
- 测试操作 就绪 情况：评估 组织 是否 □□□□□□□□□□□□□□□□□□□□ 响应 和缓解事故， 以及测试是否有适当的人在位、目录是否最新、 程序是否 被 □□□□□

本服务既解决组织□□□□□□□□□服□□□□需求问题。□□□□□□□□仿真网络安全事件/事故□□□□□服务于一个或几个目标：

- 演示：说明网络安全服务和功能，以及漏洞□□□□□□□□□□□□□；
- 培训：给员工讲授新的工具、技术和程序：
  - ○ 训练：为员工提供一个使用期望其了解之工具、技术和程序的机会。训练对于易逝之技能而言是必需的，有助于提高并保持效率；
  - ○ 评估：分析并了解网络安全服务和功能的有效性和效率，以及员工的就绪水平；
  - ○ 验证：对于网络安全服务和功能，确定能否达到特定水平的有效性和/或效率。

<u>结果：</u>提高网络安全服务和功能的有效性和效率，并确定进一步改进的机会。

取决于训练的具体目标，还可向内部的或外部的利益攸关方□□□□□□□□员工□□□训，对服务和功能的效率和有效性进行评估和/或验证，还可确定用于改进未来训练的课程，并□□□□□□□□□□□□□□□□□□□□□□

以下功能被视为本服□□□□□□□□□□

- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**；
- **Error! Bookmark not defined.**。

9.3.1 □□□□□□□

<u>目的：</u>通过专注于有关给定范围和训练焦点的特定问题，确保训练取得□□□□□

<u>描述：</u>确定学习目标和训练范围。定义训练要涵盖的特定服务、能力□□□□□□训练包括与参与者要求或期望之□□□□□□□□□□□□□□□□□□□□□□

<u>结果：</u>确定对训练□□□□□□□□□□□□□□□□□□

9.3.2 □□□□□□□□□□

<u>目的：</u>规定并确定开展训练□□□□□□□□□□□□□□设施。

<u>描述：</u>定义实现目标并交付预期训练□□□□□□□□□□□

<u>结果：</u>确定训练类型（桌面、亲自动手、仿真□□□□□开展训练□□□□□□□□□□□

9.3.3 □□□□□□□

<u>目的：</u>通过处理仿真的网络安全事件/事故，包括沟通方面的问题，为目标受众提供一个提高其服务和功能之效率和有效性以及技能、知识和能力的机会。

描述： 开发 训练 场景 以支持 利益攸关方的 目标。 可交付成果还包括对参与者和训练管理者的 指令 和指导；这些指令包括针对参与者的、详细说明部分 /全部场景步骤的建议行动。

结果： □□□

9.3.4 □□□□□□□

目的： 开展 操练 /训练，使 CSIRT 安全团队能够提高信心，增加 组织 CSIR 计划 的 □□□□□□□□□

描述： 本功能涉及 对 研究对象 “学生 ”的就绪 情况进行测试， 以 测试 其 开展培训并履行工作或任务□□及哪里有空间 来做进一步改善 。

结果： CSIRT □□□□□□□□□□□□□□□□□ KSA、关键流程和执行都可以成功地一起工□□□□□□□□□□/□□□

9.3.5 □□□□□□□□□

目的： □□□□□□□□□□□□□□□□□□□□□□

描述： □□□□□□□□□□□□□□□□□□□□□□□□□/最佳 做法，并向利益攸关方 /管□□□□□□□□□□□

结果： 创建可交付成果，以突出 训练 的成功、 □□□□□□□、总 □□□□□□ 以及为改进 以下诸项 而应采取的建议 措施：组织事故管理能力、 CSIRT 团队流程， 以及单个 服 务对象的能力 和□□□□□□□□□□□□□□□□□□□□□□□

9.4 服 □□□□□□□□□

目的： 确保 服 务对象的 策略 和程序包括适当的事故管理 注意事项，并最终使 服 □□□□□□□ 地管理风险和威胁， 以及 使 CSIRT 更加有效。

描述： □□□□□□□□□□□□□□□□□□□ 为 CSIRT 服 □□□□□□□□□ CSIRT 服 务对象和关键 利益攸关方 □□□□□ 根据需要提供技术建议，并为 创建和实施 服 务对象 策略 做出贡献， 以及对之施加影响，以 使 CSIRT 更加有效。策略对使 CSIRT 服 务合法化 而言 也很重要。

结果： 使 服 务对象 能够 根据 运营安全最佳做法（ □□□□□□□□□□□□□□□□□□□ 起） 来做出组织 决定， 同时 还 理解适当的时候需要 在业务 决策 中 纳入 □□□□□□□□□□□□□□□

以下功能被视为本 服 □□□□□□□□□□

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

9.4.1

9.4.2

9.4.3

CSIRT CSIRT

9.4.4

- □□□□□□□□□□□□□□□□□□□□□□□;
- 网络安全相关基础设施和工具的内部和外部 审计；
- 安全软件开发要求和安全编码。

结果 □□□□□□□□□□□□□□□□□□□□□ 本服务 □□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□

□ □ 1□ □ □

来自 CSIRT 社群的以下志愿者为该版本的 CSIRT 服务框架做出了重要贡献。按其姓氏字母顺□□□□□□□□□□□□□□□□□□□□□□□□□

- Vilius Benetis，NRD CIRT（立陶宛）
- Olivier Caleff（服务区协调员），openCSIRT Foundation（法国）
- Cristine Hoepers（服□□□□□□，CERT.br（巴西）
- Angela Horneman，CERT/CC，SEI，CMU（美国）
- Allen Householder，CERT/CC，SEI，CMU（美国）
- Klaus-Peter Kossakowski（编辑），Hamburg University of Applied Sciences（德国）
- Art Manion，CERT/CC，SEI，CMU（美国）
- Amanda Mullens（共同服务区协调员），CISCO（美国）
- Samuel Perl（服务区协调员），CERT/CC，SEI，CMU（美国）
- Daniel Roethlisberger（服务区协调员），Swisscom（瑞士）
- Sigitas Rokas，NRD CIRT（立陶宛）
- Mary Rossell，Intel（美国）
- Robin M. Ruefle（共同服务区协调员），CERT/CC，SEI，CMU（美国）
- Désirée Sacher，Finanz Informatik（德国）
- Krassimir T. Tzvetanov，Fastly（美国）
- Mark Zajicek（共同服务区协调员），CERT/CC，SEI，CMU（美国）

附件 2：术语和定义

本节定义了 CSIRT 服务框架中使用的某些术语。

行动（Action） - 描述如何在不同的详细程度上完成某件事情。

通报（Advisory）[9] - 用于通知、建议和警告产品漏洞的公告或简报。

能力（Capability） - 可以作为一组织的作用和职责的一部分来开展的一种可度量的活动。对于 FIRST 服务框架而言，能力可以定义为更广泛的服务，也可以定义为必备的功能。

容量（Capacity） - 一组织在达到某种形式的资源耗尽之前，能够履行某种特定能力的并发进程的数量。

常见漏洞陈列（Common Vulnerability Exposures）（CVE）[10] - 条目列表，其中包含一个标识号、一个描述和至少一个有关公开已知漏洞的公共参考。用作参考漏洞的标准标识符。

常见漏洞评分系统（Common Vulnerability Scoring System）（CVSS）[11] - 反映漏洞严重程度的一个计分系统。

常见漏洞枚举（Common Weakness Enumeration）（CWE）[12] - 创建的软件弱点类型的正式列表，用作用于描述架构、设计或代码中软件安全弱点的一种通用语言；用作针对这些弱点的软件安全工具的标准衡量尺度；并为弱点识别、缓解和预防工作提供一个通用的基线标准。

服务对象（Constituency） - 可以获取 CSIRT 提供的一组特定服务的特定人群和/或组织。

情境数据源（Contextual Data Source） - 情境数据源旨在为数据点提供情境，例如，身份、资产或信息安全事件。具体示例包括用户数据库、资产清单、IP 否认服务或威胁情报数据。

协调漏洞披露（Coordinated vulnerability disclosure） - 一个用于表示包括协调在内的披露过程的术语。来源：ISO/IEC 29147:2018，术语和定义。

协调员（Coordinator）[13] - 一个可选的参与者，可协助供应商和搜寻者来处置和披露漏洞信息。

检测用例（Detection Use Case） - 有待信息安全事件管理服务区检测的一个特定条件。该术语源于软件工程，但现已广泛用于检测工程。

禁令（Embargo） - 坚持不发布漏洞详情，直至受影响的供应商能够发布安全更新程序或缓解措施以及应变方法来保护客户。

搜寻者（Finder）[14] - 识别产品或在线服务中潜在漏洞的个人或组织。请注意：搜寻者可以是研究人员、报告人、安全公司、黑客、用户、政府或协调员。

---

[9] ISO/IEC 29147:2014 □ □ □ □ – □ □ □ □ □ – □ □ □ □ □ – □ □ /□ □ 3.1
[10] https://cve.mitre.org/
[11] https://www.first.org/cvss/
[12] https://cwe.mitre.org/about/index.html
[13] ISO/IEC 30111:2013 □ □ □ □ – □ □ □ □ □ – □ □ □ □ □ – □ □ /□ □ 3.1
[14] ISO/IEC 29147:2014 □ □ □ □ – □ □ □ □ □ – □ □ □ □ □ – □ □ /□ □ 3.3

功能（Function） - 旨在实现某特定服务目的的一项或一组活动。其他定义包括：一组相关的行动；[15]执行某项指定的行动或活动、工作、操作。[16]

信息安全事件（Information Security Event） - 在信息技术环境中可观察到的、与安全相关的事件；例如，用户登录或入侵检测（IDS）告警。信息安全事件通常会产生某种证据，例如，一条审计记录或日志文件中的一个条目，作为信息安全事件管理服务区的一部分，进行收集和分析这些信息。

信息安全事故（Information Security Incident）[17] - 指示用户、系统、组织和/或网络信息安全某些方面受到损害的、任何不利的信息安全事件（或信息安全事件集）。信息安全事故的定义在组织与组织之间可能有所不同，但通常至少以下类别是适用的：

- 失去信息保密性
- 损害信息完整性
- 拒绝服务
- 滥用服务、系统或信息
- 系统损坏

攻击，即使因适当的保护而失败，也可以视为信息安全事故。

关键绩效指标（Key Performance Indicator）（KPI）[18] - 一个可度量的值，用于表明公司有效实现关键业务目标的能力。组织在多个层面上使用关键绩效指标来评估其在达成目标方面的成就。

成熟度（Maturity） -指的是一个组织在其使命和授权范围内如何有效地履行特定能力，它是在执行特定功能或者功能或服务集的过程中能够达到的熟练程度，一个组织的能力将取决于已建立的策略和文档的范围和质量以及执行既定流程的能力。

开源（Open Source） - 允许自由地重新分发和修改的软件作品，其中的源代码是公开可用的，可以自由分发，不歧视任何个人、团体或工作领域，且技术中立。开源软件通常由共同创建和维护它的个人和实体社群来维护。

产品（Product）[19] - 一个为销售或免费提供而实施或开发的系统。

修复（或补救） （Remediation（or Remedy））[20] - 对产品或在线服务进行的更改，以消除或缓解漏洞。修复通常采取二进制文件替换、配置更改或源代码修补和重新编译的形式进行。用于“修复”的不同术语包括补丁、修复、更新、修补和升级。缓解措施也称为应变方法或对策。

负责任的披露（Responsible Disclosure） - 一个用于表示以下过程或模型的术语，在该过程或模型中，仅在补救措施（修补程序或补丁程序）变得可用的一段时间后才允许披露漏洞。该术语不一定等同“协调的漏洞披露”。

---

[15] Source: https://www.merriam-webster.com/dictionary/function
[16] Source: https://www.dictionary.com/browse/function
[17] □ □ RFC2350□ □ □ “□ □ □ □ ”□ □ “□ □ □ □ □ □ ”□ https://tools.ietf.org/html/rfc2350
[18] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator
[19] ISO/IEC 29147:2014 □ □ □ □ – □ □ □ □ – □ □ □ □ – □ □ /□ □ 3.5
[20] ISO/IEC 29147:2014 □ □ □ □ – □ □ □ □ – □ □ □ □ – □ □ /□ □ 3.6

风险（Risk）[21] - “不确定性对目标的影响”。在该定义中，不确定性包括事件（可能发生或可能不发生）以及因含糊或信息缺乏而引起的不确定性。

风险接受（Risk Acceptance）[22] - 指的是一种风险响应策略，项目团队据此来决定确认风险，除非风险发生，否则不采取任何行动。

风险注册表（Risk Register）[23] - 用于记录风险分析结果和风险响应计划的文档。

服务（Service） - 一项服务指的是针对某特定结果的一组可识别的、一致的功能。此类结果可能是服务对象或代表某实体的利益攸关方或为某实体的利益攸关方所预期或要求的。

服务水平协议（Service Level Agreement）（SLA） - 服务提供商（内部的或外部的）与最终用户之间的一个合同，用于定义期望从服务提供商处得到的服务水平。

利益攸关方（Stakeholders）[24] - 定义和修改服务区或服务并确保适当的服务沟通策略的个人或团体，以及可以从提供的服务中受益的团体。

任务（Tasks） - 完成某项特定功能必须执行的行动列表。

供应商（Vendor）[25] - 开发产品或服务或负责其维护的个人或组织。

漏洞（Vulnerability）[26] - 软件、硬件或在线服务中可以被利用的弱点。

[21] ISO 31000:2009/ ISO □ □ 73:2002 □ □ □ □ - □ □ □ □ □ - □ □ /□ □ 2.1
[22] □ □ □ □ □ □ □ □ PMBOK□ □ □ □ □ □
[23] □ □ □ □ □ □ □ □ PMBOK□ □ □ □ □ □
[24] □ □ □ □ □ □
[25] ISO/IEC 30111:2013 □ □ □ □ – □ □ □ □ – □ □ □ □ – □ □ /□ □ 3.7
[26] ISO/IEC 30111:2013 □ □ □ □ – □ □ □ □ – □ □ □ □ – □ □ /□ □ 3.8

附件 3□ □ □ □ □

Alberts, David S., et.al. Understanding information age warfare. In *DOD Command and Control Research Program Publication Series*. ADA395859. Booz Allen & Hamilton, McLean, VA. 2001.
https://apps.dtic.mil/docs/citations/ADA395859

Barford P., et al. (2010) Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, 2010. Boston, MA. ISBN 978-1-4419-0140-8_1
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_1

Boyd, John R. Destruction and Creation. Goal Systems International. September 3, 1976.
http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

Cartwright, James E. Joint Concept of Operations for Global Information Grid NetOps. *United States Strategic Command*. PDF August 10, 2005. Homeland Security Digital Library. August 10, 2005.
https://www.hsdl.org/?view&did=685398

Committee on National Security Systems Instruction CNSSI 4009. *Committee on National Security Systems Website.* June 23, 2019 [accessed].
https://www.cnss.gov/cnss/

Cybersecurity Situation Awareness. *The MITRE Corporation Website.* June 25, 2019 [accessed].
https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Endsley, Mica R. Toward a theory of situation awareness in dynamic systems. *Human factors* Volume 37. Number 1. March 1995 Pages 32-64.
https://journals.sagepub.com/doi/10.1518/001872095779049543

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.0, 2018. North Carolina: First.org, 2018
https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0

FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG). 2013-2015. North Carolina: First.org, 2015
https://www.first.org/global/sigs/vrdx/

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.0, 2017. North Carolina: First.org, 2017
https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Hawk, Robert. Situational Awareness in Cyber Security. [blog post]. *Hawk's Posts: Security Essentials from Robert Hawk.* June 11, 2015.
https://www.alienvault.com/blogs/security-essentials/situational-awareness-in-cyber-security

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Christopher. *The CERT® Guide to Coordinated Vulnerability Disclosure*. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. 2017
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Householder, Alan. Vulnerability Discovery for Emerging Networked Systems [blog post]. *Vulnerability discovery techniques*. November 20, 2014.
https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability disclosure.* Second Edition. ISO/IEC 29147:2018. Geneva, Switzerland: ISO: IEC. 2018
https://www.iso.org/standard/72311.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability handling processes*. First Edition. ISO/IEC 30111:2013. Geneva, Switzerland: ISO: IEC. 2013
https://www.iso.org/standard/53231.html

Jajodia, Sushil, et al., (Eds.). *Cyber Situational Awareness: Issues and Research*. Part of the Advances in Information Security book series (ADIS, volume 46). 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/book/10.1007/978-1-4419-0140-8

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590.

Kossakowski; Klaus-Peter & Stikvoort, Don. *A Trusted CSIRT Introducer in Europe*. Amersfoort, Netherlands: M&I/Stelvio, February, 2000.
http://www.ti.terena.nl/process/ti-v2.pdf

Manion, Art & Householder, Alan. *Vulnerability Analysis.* CERT Coordination Center (CERT/CC). May 30, 2019.
https://vuls.cert.org/

McGuinness, B. &, Foy, L. A subjective measure of SA: The crew awareness rating scale (cars). In Kaber, D.B.; Endsley, M.R.; p. 286-291. *Proceedings of the First Human Performance, situation awareness and automation conference; user-centered design for the new millennium*. Savannah, Georgia, October 2000.

Salerno, John; Hinman, Michael & Boulware, Douglas. Situation awareness model applied to multiple domains. In *Proceedings of the Defense and Security Conference*, Orlando, FL, March 2005.
https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5813/0000/A-situation-awareness-model-applied-to-multiple-domains/10.1117/12.603735.full?SSO=1

Stone, Steve. Data to Decisions for Cyberspace Operations. *The MITRE Corporation Website*. January 2016
https://www.mitre.org/publications/technical-papers/data-to-decisions-for-cyberspace-operations

Tadda G.P., Salerno J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA. 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_2

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs).* CMU/SEI-98-HB-001. Software Engineering Institute, Carnegie Mellon University. 1998.
http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

□ □ 4□ □ □ CSIRT □ □ □ □ □ □ □ □ □ □

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- □ □ □ □
- **Error! Bookmark not defined.**

Error! Bookmark not defined.□ □ Error! Bookmark not defined.□ □ □ □ □ □

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- □ □

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**

Error! Bookmark not defined.

- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**
- **Error! Bookmark not defined.**