2020 年春

产品安全事故响应团队（PSIRT）服务框架
版本 1.1

请注意：本文件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。

目录

PSIRT 服务框架

宗旨

服务框架是一套详细阐述计算机事故响应团队（CSIRT）和产品事故响应团队（PSIRT）服务范围的高层文件。文件起草者为 FIRST 公认的专家。FIRST 力求兼收并蓄，收集来自肩负国家责任的 CSIRT、私营部门 CSIRT 和 PSIRT 以及其它利益攸关方的反馈。服务框架旨在为开发新的培训材料奠定基础。如今这些文件已得到广泛使用，例如，为新团队定义初始服务的目录。

在创建 CSIRT 服务框架的过程中，不难看出 PSIRT 确实提供了完全不同的服务且通常在迥然不同的环境中运行。因此，我们决定编制一份涵盖 PSIRT 独立文件。这两份文件将形成互补，突出诸多相似之处。教育咨询委员会是制定框架的主要推手。

该框架存在的意义在于帮助相关组织建立、维护并发展其 CSIRT 或 PSIRT 的能力。作为指南性文件，这些框架可以提供指导并确定各种模型、功能、服务和输出结果。相关团队可通过这一方式，自由运用自建模型，形成能够满足利益攸关方独特需求的能力。这些框架旨在确定核心职责、为如何构建履行这些职责的能力提供指导，洞察相关团队如何能为上级组织创造并输送价值，并藉此为安全事故响应团队（SIRT）提供支持。

引言

产品安全事故响应团队（PSIRT）属于组织内的实体，其核心任务是关注与产品安全漏洞相关的风险识别、评估和处置，其中包括组织生产和/或销售的产品、解决方案、组件和/或服务。

合理部署的 PSIRT 并非是与组织产品开发无关的独立运作团队。相反，该团队是相关组织实施的更广泛安全工程举措的组成部分。这种结构可确保将安全保障活动融入安全开发周期（SDL）。

鉴于大多数产品的安全漏洞在产品投放市场后被作为质量漏洞上报，因此产品安全事故响应通常与 SDL 的维护阶段存在关联。然而，PSIRT 有能力对制定架构、设计、规划和风险建模阶段的早期需求收集产生影响。PSIRT 各职能的价值，亦可通过为处理内部发现的安全问题提供指导和监督得以体现。

PSIRT 的框架结构

服务领域 –服务 –功能 –子功能

服务领域

服务领域重组与公共问题有关的服务。这些服务领域有助于按顶层分类来组织服务，从而为理解提供方便。各服务领域的规范将包括一个“描述”字段，其内容由描述服务领域的一般性高层叙述文本以及服务领域内的服务列表构成。

服务

服务是相关代表或事故响应团队的成员，为实现特定结果而采取的一系列可识别的一致性行动。

服务由以下模板指定：

- 阐述服务性质的“描述”字段。
- 阐述服务意图和结果可衡量的“目的和结果”字段。

功能

功能是旨在实现特定服务目的的一项或一组活动。任何功能均可在多项服务的背景下共享和使用。

功能用以下模板描述：

- 阐述功能的“描述”字段。
- 阐述服务意图和结果可衡量的“目的和结果”字段。
- 可作为功能的一部分加以执行的子功能列表。

子功能

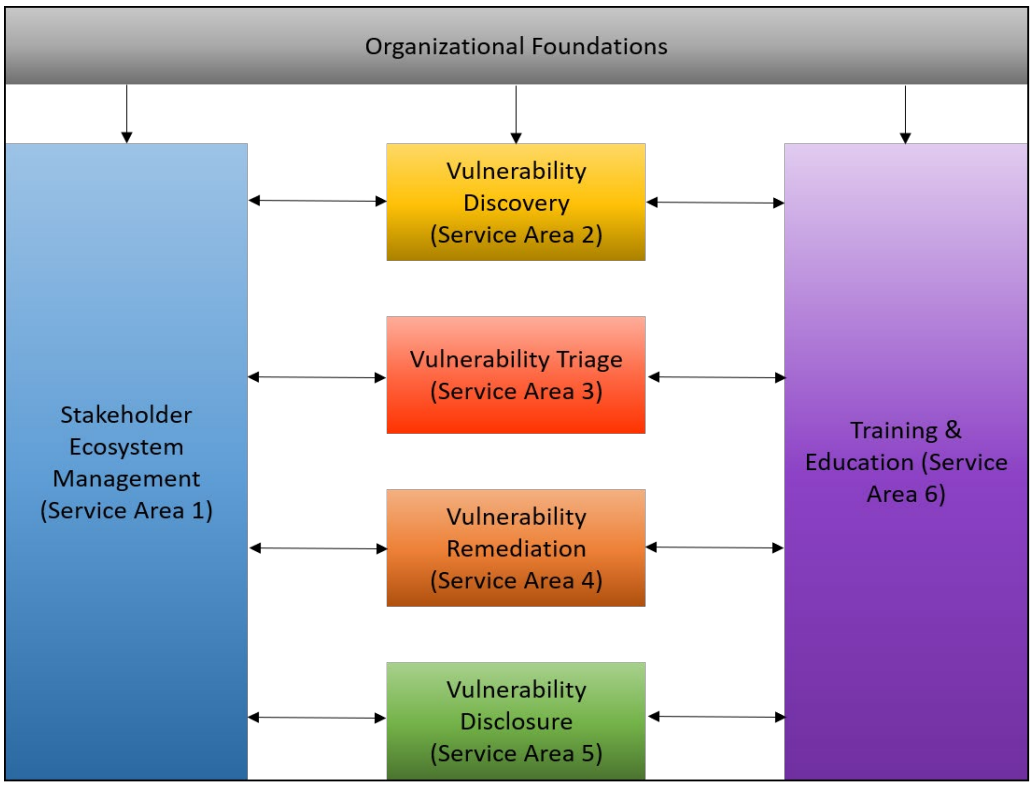
子功能是旨在实现特定功能目的的一项或一组活动。任何子功能均可在多项功能的背景下共享和使用。

PSIRT 与 CSIRT 的差异

对产品的关注点不同，是某组织 PSIRT 与同一组织内其它事故响应团队（如 CSIRT）之间的主要区别所在。一般而言，企业 CSIRT 关注的是构成某组织基础设施的计算机系统和/或网络的安全性。

虽然企业 CSIRT 和 PSIRT 之间存在重要区别，但关键是要认识到这两个群体亦会形成合力。需要重点指出的是，PSIRT 的运作并不独立于组织的其它部分而是在整个框架中，我们将突出强调应加以培育的协作和协同领域。

PSIRT 的组织结构



图中文字：

组织的基础　　利益攸关方生态系统管理（服务领域 1）

发现漏洞（服务领域 2）　　漏洞分类（服务领域 3）漏洞补救（服务领域 4）

漏洞披露（服务领域 5）　　培训和教育（服务领域 6）

图 1：组织结构

PSIRT 可具备与其保护对象相同的独特性和多样性。在同一部门或行业的组织之间，业务特征、运营模式、产品组合、组织结构和产品开发策略会存在差异。因此，并不存在适用于所有产品安全事故响应的万全之策，亦无统一的团队模板可供所有组织遵循。然而，大多数公司使用三种 PSIRT 模型：分布式、集中式和混合式。

分布模式

分布模式通过小规模的核心 PSIRT，与产品团队代表一起解决产品中的安全漏洞。在此模型中，更下一级的 PSIRT 运营部门有若干核心职责：

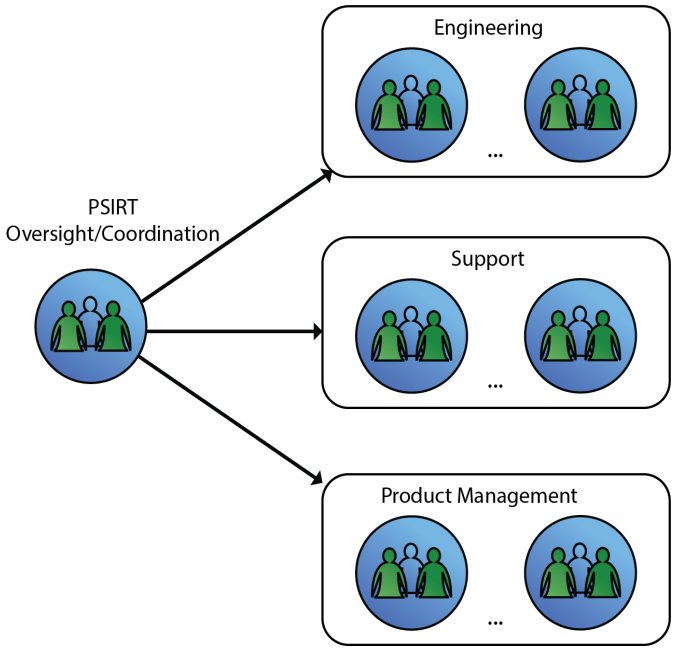


图 2：分布式模型

图中文字：

PSIRT 监督/协调　　工程　　支持　　产品管理

- 为消除安全漏洞，制定有关分类、分析、补救以及通报修复、缓解信息或发布其它公报的政策、流程、程序和导则。
- 在整个组织内建立（分层）产品安全工程代表间的对应关系。
- 就产品安全漏洞响应和业务潜在风险提供管理和指导。
- 充当输入性安全漏洞的采集点，利用中央控制点实现规模经济。
- 向产品所有者/经理和安全工程师通报新的安全漏洞，协助制定补救计划，起草/发布包括事故管理在内的有关修复或缓解措施的信息。

产品组合丰富的组织可从分布模式受益的原因在于 PSIRT 任务的成本由整个组织摊分。该模型还可通过产品工程团队中的技术人员拓展 PSIRT 任务的范围。

分布式 PSIRT 模型面临的挑战是，负责分类和修复安全漏洞的人员既不受 PSIRT 运营部门的直接控制，亦不向其报告。

集中模式

集中模式的 PSIRT 员工数量更多，他们来自多个部门，向一个或多个负责组织产品安全的高级管理人员汇报。此模型的结构可能与以下结构相仿：

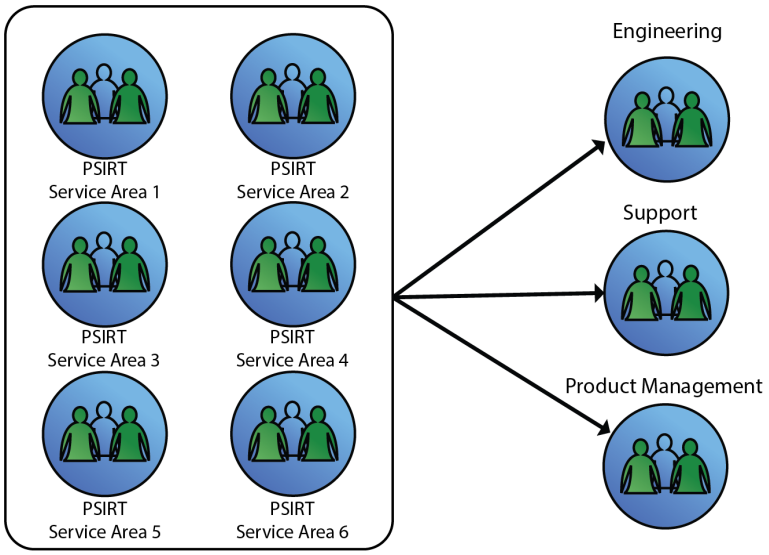


图 3：集中模式

图中文字：

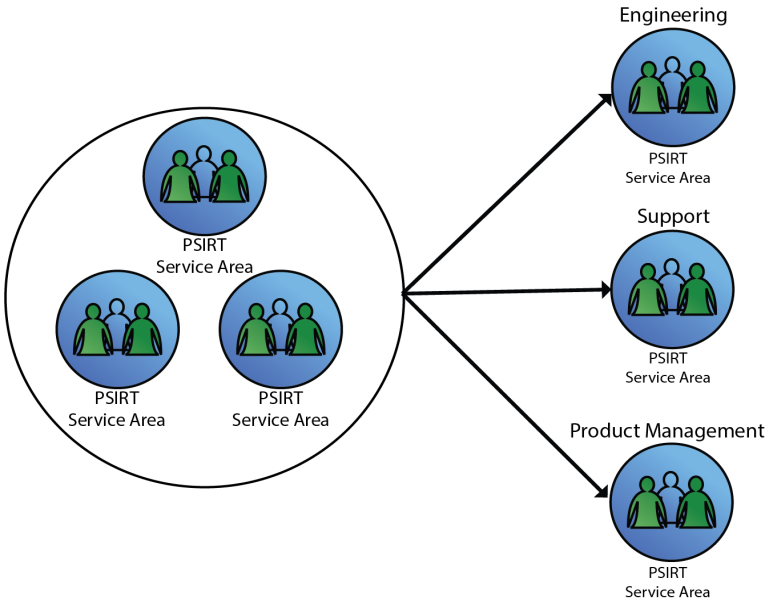
PSIRT 服务领域 1　　PSIRT 服务领域 2　　PSIRT 服务领域 3　　PSIRT 服务领域 4
PSIRT 服务领域 5　　PSIRT 服务领域 6　　工程　　支持　　产品管理

- PSIRT 计划管理部门：为修复安全漏洞的分类、分析、补救和信息沟通制定政策、流程、程序和导则。管理整个 PSIRT 举措、工单系统的运作，并作为 PSIRT 在组织内的领导。
- PSIRT 的安全情报及分类：监控各种外部来源的安全漏洞。评估安全漏洞给组织产品组合造成的初始影响。
- PSIRT 补救和沟通：直接为产品工程团队提供安全漏洞的修复代码。

这种模式适用于规模较小的组织和/或拥有同质产品组合的组织。该模式将高水平的安全技能和专业知识集中到组织内的同一领域并进一步加以拓展。这种模式面临的挑战在于，如果产品组合不断增长和/或变得更加多样，维护一个集中的专业化团队的费用并不会随之增加。

混合模式

- 混合模式是一种变体，同时涵盖分布和集中式模式的特征。组织可以选择同时使用这两种模式的一些特征和特性，创建一种将以下因素考虑在内的混合模式：
- 公司的组织结构和规模
- 产品组合的规模和多样性
- 产品开发策略



图中文字：

PSIRT 服务领域　　工程　　支持　　产品管理

图 4：混合模式

其它考虑

对 PSIRT 而言，在某组织产品的安全漏洞问题上，拥有保持独立客观立场的自主权很重要。因此，在制定组织 PSIRT 战略和结构时，相关组织应考虑如何将团队更好地融入组织及其报告结构。重要的是 PSIRT 应向公司高管，即 PSIRT 权威的背书人汇报。

随着 PSIRT 的不断成熟壮大以及任务的不断发展，团队的组成或报告结构可能会发生变化。PSIRT 发展和成熟的驱动力源自其主要利益攸关方，以及（不幸的是）严重漏洞给其广大利益攸关方造成的影响。利益攸关方通常依据组织采用的模型及其规模定义。

利益攸关方

鉴于利益攸关方的需求和要求是界定 PSIRT 战略和结构的关键组成部分，因此某组织建立 PSIRT 时采用的模型，决定了利益攸关方的身份及其影响力。继续保持积极的关系至关重要。服务领域 1：利益攸关方生的态系统管理中包含关于利益攸关方生态系统及其管理方式的更多细节。

组建产品事故响应团队和制定策略时最后要考虑的是影响因素。影响因素与利益攸关方不同，并非是分散的个人或群体。相反，影响因素是指行业和政府的标准、立法、法规和趋势。与利益攸关方相比，这些因素可能会对 PSIRT 的建立、战略、政策和运营特征提出更高要求。

PSIRT 承担哪些职责？

组织所用模型将定义 PSIRT 的范围和运营活动，但不一定会改变组织在消除其产品安全漏洞方面需要采取的行动。该模型细化了直接归属于 PSIRT 而非分布在整个组织内的能力、行动和责任的范围。

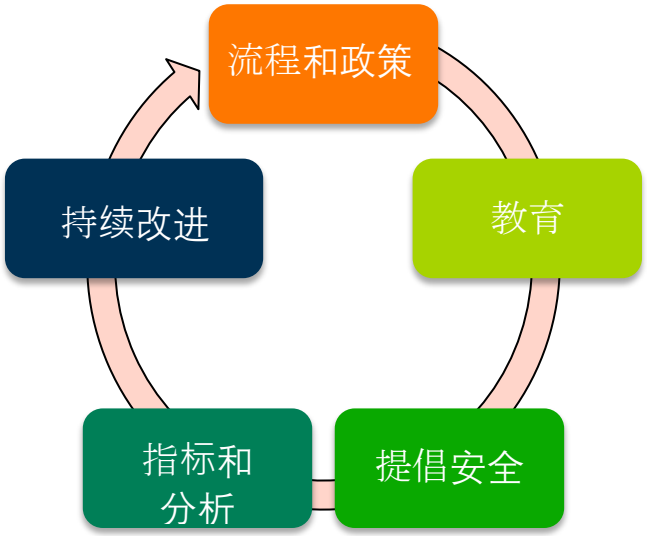


图 5：PSIRT 的一般活动

持续的过程和政策的制定

PSIRT 制定了组织关于产品安全的政策。业务需求驱动并提出有关了 PSIRT 的要求，而非 PSIRT 的要求推动业务需求。在 PSIRT 政策得以实施之前，相关组织的领导必须对这些政策进行审查并为其赋权。获批政策必须制定明确的程序，遵循这些程序，便可确保组织遵守上述政策。

利益攸关方教育

除 PSIRT 政策和程序之外，PSIRT 还需建立工作流程和管理系统，以简化消除产品安全漏洞所需执行和完成的操作。这些工作流程和管理系统的应用，为组织将产品安全性作为日常业务活动的一部分，打开了方便之门。

部署 PSIRT 任务、政策和程序时可能犯的最大错误，是将其视为一项单独的责任或要求。因此，对组织所有成员开展产品安全基础知识和职责教育至关重要。教育必须涵盖整个组织，为其赋能并使整个组织能够满足 PSIRT 的政策要求。

度量指标的重要性

衡量产品安全事故响应任务的成功与否至关重要。度量报告并不规定要求，而是为项目提供支持，帮助确定所需资源，并可帮助确定有必要对过程/工具加以完善之处。度量指标的创建和跟踪揭示了与部署和采用 PSIRT 有关的问题或瓶颈，因此亦或有助于 PSIRT 的成熟。服务 1.7 利益攸关方度量指标和服务 5.3 漏洞度量指标更加详细地介绍了有跟踪价值的指标类型。

定义

在此文件中，我们定义了某些术语的使用。请注意服务领域、服务和功能是以不同的详细程度确认正在做什么，而任务和行动则是以不同的详细程度确认怎样做。任务和行动在附带文件中发布，且更新能够/将会更加频繁：

公告（Advisory） - [1]用于通报产品漏洞、提出建议和发布警告的通知或公告。

漏洞条（Bug bar）-定义可视为安全漏洞的漏洞类型标准。符合这些标准的缺陷将通过 PSIRT 标准操作程序作为漏洞处理。

协调员（Coordinator）-[2]可帮助供应商和漏洞搜索方处理并披露漏洞信息的可选参与人。

暂缓信息发布（Embargo） - 在受影响的供应商有能力为保护客户发布安全更新、缓解措施以及变通之法前，暂停发布有关漏洞的详细信息。

漏洞搜索方（Finder） - [3]识别产品或在线服务潜在漏洞的个人或组织。请注意，漏洞搜索方的身份可以是研究人员、记者、安保公司、黑客、用户、政府或协调员。

开放源代码（Open Source） - 指以可自由再分发并能修改的方式获得许可的代码，其中源代码公开提供且可自由分发，既不歧视任何个人、团体或领域，又秉持技术中立。开放源代码软件通常由共同创建并维护该软件的个人和实体团队负责维护。

合作伙伴（Partner） - 原始设备制造商（OEM）、供应商、原始设计制造商（ODM）

产品（Product） - [4] 为销售或免费提供而实施或开发的系统。

质量门（Quality Gate） - 在产品进入下一开发或发布阶段前必须满足的一组标准。

补救（Remediation (或 Remedy)） - [5]为消除或缓解漏洞，对产品或在线服务做出更改。补救操作通常采用替换二进制文件、更改配置或修补和重新编译源代码的形式。‘修复’使用的不同术语包括修补、修复、更新、热修复和升级。缓解亦称变通或对策。

风险（Risk） - [6]‘不确定性对目标的影响 ’。在此定义中，不确定性包括事件（可能发生，也可能不发生）以及因模糊或信息不足造成的不确定性。

接受风险（Risk Acceptance） - [7]一种风险应对策略，项目团队根据此策略决定承认风险存在，但除非发生风险，否则不采取任何行动。

风险登记簿（Risk Register） - [8]记录风险分析结果和风险应对计划的文件。

---

[1] ISO/IEC 29147:2014 信息技术—安全技术— 漏洞披露—术语/定义 3.1
[2] ISO/IEC 30111:2013 信息技术—安全技术— 漏洞处理流程—术语/定义 3.1
[3] ISO/IEC 29147:2014 信息技术—安全技术— 漏洞披露—术语/定义 3.3
[4] ISO/IEC 29147:2014 信息技术—安全技术— 漏洞披露—术语/定义 3.5
[5] ISO/IEC 29147:2014 信息技术—安全技术— 漏洞披露—术语/定义 3.6
[6] ISO 31000:2009/ ISO 指南 73:2002 风险管理—原则和指南—术语/定义 2.1
[7] 项目管理知识体系（PMBOK）指南和标准
[8] 项目管理知识体系（PMBOK）指南和标准

安全开发周期（Secure Development Lifecycle (SDL)）- 旨在帮助开发人员构建更安全的产品，满足安全合规性要求，同时降低开发成本的开发过程。

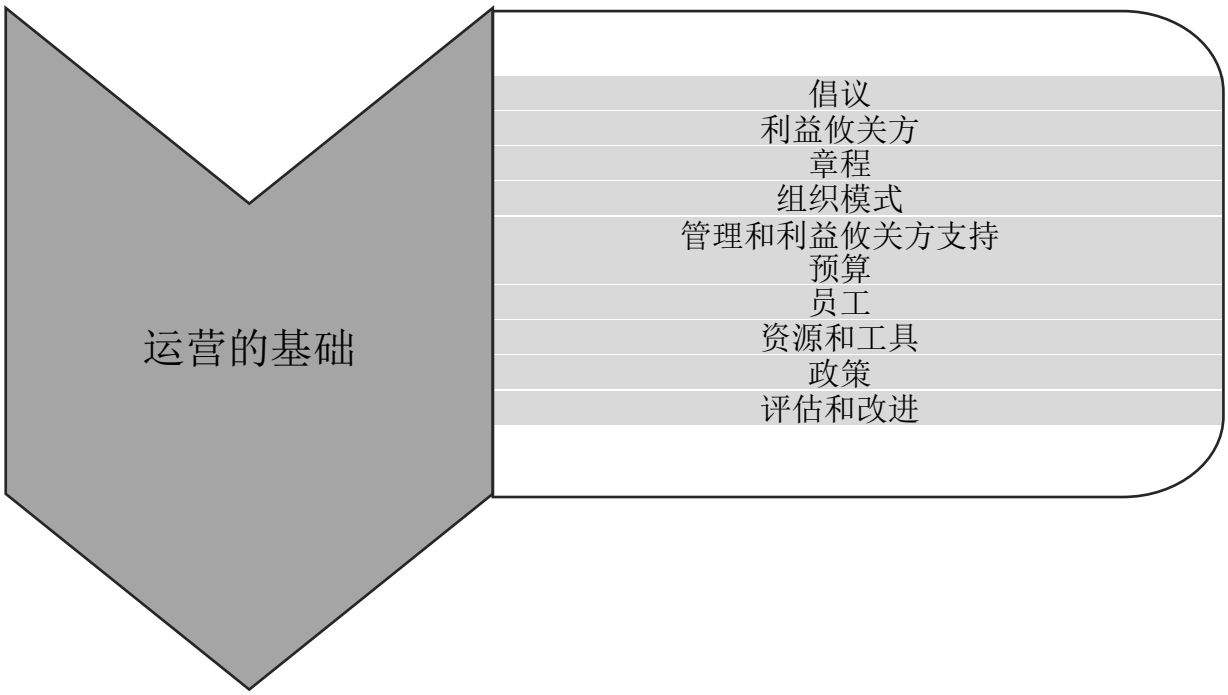
服务水平协议（Service Level Agreement (SLA)）- 服务提供商（内部或外部）与最终用户为定义期望服务提供商所提供服务的水平而签署的合同。

利益攸关方（Stakeholders）- [9] PSIRT 利益攸关方是构建和修改产品或产品组件的群体，在确保提出适当产品宣传策略的同时，得益于产品的安全性。简而言之，PSIRT 利益攸关方要么为产品安全和事故响应做出贡献，要么从中受益。

第三方（Third-Party）- 提供产品或解决方案/服务所含组件的任何上游供应商或生产商。

供应商（Vendor）- [10]开发产品或服务，或负责维护产品或服务的个人或组织。

漏洞（Vulnerability）- [11]可以利用的软件、硬件或在线服务的弱点。



[9] 架构内容框架
[10] ISO/IEC 30111:2013 信息技术—安全技术— 漏洞处理流程—术语/定义 3.7
[11] ISO/IEC 30111:2013 信息技术—安全技术— 漏洞处理流程—术语/定义 3.8

本节确定并描述了某组织规划、建立并有效运行 PSIRT 所需的核心组成部分的基础。

目的： 使组织能够规划和实施 PSIRT 的基础组成部分，以建立并运行 PSIRT。

成果： 确认、规划并实施 PSIRT 运作的基础组成部分，有助于相关组织建立 PSIRT，并使 PSIRT 为执行任务做好准备，保持公司向确定利益攸关方提供产品和服务的能力。

I. 策略

A. 请高管发起倡议

请组织高管和关键决策者发起倡议。

目的： 向组织高管（如高级管理者、董事会）通报并获得组织高管或其它决策者的支持（认可），以使 PSIRT 有效运行。

成果： 基于预期业务度量指标的持续融资和支持。

为获得管理层的支持，相关组织应通过向管理层提供计划和其它辅助信息的方式，向管理层通报或吹风，帮助他们了解 PSIRT 的目的、重要性、安全漏洞的潜在风险以及建立 PSIRT 的好处。（参见下文的“PSIRT 章程”和“预算”。）

相关信息参见服务 1.1 内部利益攸关方管理 。

B. 利益攸关方

确定利益攸关方及贵 PSIRT 与这些团队的关系。

目的： 了解 PSIRT 将为谁服务以及 PSIRT 将与谁互动。

成果： 明确定义的利益攸关方列表。

这其中应包括组织的客户、外部安全研究人员、CSIRT 和其它 PSIRT 等外部利益攸关方，以及软件开发人员、工程师、客户支持、法律和公共/公司/媒体关系人员等内部利益攸关方。

相关信息参见服务领域 1 利益攸关方生态系统管理（服务 1.1 内部利益攸关方管理、服务 1.2 漏洞搜索方团体的参与、服务 1.3 相关团体和组织的参与和服务 1.4 下游利益攸关方管理）。

C. PSIRT 章程

制定章程或编写文件（例如，战略规划、实施计划或运作概念文件）。

目的： 确定、描述和记录 PSIRT 运作的基本计划要素。

成果： 描述为什么要创建/资助 PSIRT 以及 PSIRT 期望成果的文件。

PSIRT 章程/计划应定义以下内容：

- PSIRT 的任务（应支持并与组织的任务保持一致）
- 目的、职能和责任。
- 产品和服务(例如，接收漏洞报告、开发修复程序或修补程序、发布修补程序公告)。

D. 组织模式

确定并记录 PSIRT 将使用的组织结构和模型。

目的： 确定、描述和记录 PSIRT 运作的组织模式。

成果： 建立定义明确的团队结构，明确记载相关职能和职责。

文件记录的组织模型应描述 PSIRT 的内部报告结构，并确定 PSIRT 运作的权限。参见“PSIRT 组织结构”，以了解一些常见组织模式（例如，分布模式、集中模式、混合模式）。更多相关信息，请参见服务 1.5 组织内部的事故通报协调。

E. 管理和利益攸关方支持

获得组织管理层和内部利益攸关方的支持。

目的： 向其它内部管理层和利益攸关方通报并获得其支持，使 PSIRT 能够有效运行。

成果： 向利益攸关方通报关键业务度量指标，以确保支持得以持续。

相关信息参见 服务 1.1 内部利益攸关方管理 。

II. 策略

A. 预算

确定 PSIRT 运作所需的资源成本，并为这些资源获得相应的资金。

目的： 确定、描述和记录 PSIRT 运作和融资的组织模式。

成果： 记录 PSIRT 的运作成本、费用和融资模式。

预算应包括为 PSIRT 配备人员的费用（工资、福利和其它费用）、设备和其它资本支出（如信息技术系统/设备、软件许可）以及培训预算（包括差旅费）。

B. 员工

确定提供 PSIRT 服务所需的人力资源，并获得熟练的员工。

目的： 确定、描述和记录 PSIRT 人员配备的组织模式。

成果： 记录 PSIRT 的人力资源需求。

这方面的工作包括确定 PSIRT 不同的员工岗位以及个别成员的职能与职责，以及这些职能应具备的能力（知识、技能和能力，[KSAs]）及其应满足的其它要求（例如，教育、经验、认证）。这些职位或职能包括全职员工、供应商、承包商或他们的组合。

作为人员配备计划的一部分（或在单独的文件中确定），应制定并规划相关培训要求，其中包括对全体 PSIRT 员工的一般培训以及针对个人的岗位职能培训（例如，入职培训/指导；继续培训、教育和意识培养；专业发展特别培训）。

相关信息参见服务 6.1 PSIRT 培训。

C. 资源和工具

确定并获得其它必要的资源和工具。

目的： 确定并获得 PSIRT 运行所需的资源、设备和工具。

成果： 记录并了解 PSIRT 的工具和资源需求。

这些资源和工具包括：

- 基础设施，如设施（办公空间）
- 工具/技术/设备（硬件、软件）（例如，参见服务 3.3 漏洞再现）
- 漏洞报告系统/方法（例如，网站、电子邮件、电话）（参见服务 2.1 漏洞报告简介）
- 安全通信（例如，PGP/加密）（参见功能 1.5.2 安全通信管理）
- 漏洞数据库/跟踪系统（例如，参见功能 1.5.3 安全缺陷跟踪系统更新和功能 3.2.1 漏洞搜索方数据库）

III. 运作

A. 政策和程序

记录与 PSIRT 运作相关的政策、流程和程序。

目的： 确定、描述和记录 PSIRT 运作的政策和程序。

成果： PSIRT 将出台正式的政策，阐述 PSIRT 的权力及其将推行的治理/运作方式。PSIRT 还将编制有正式文字记载的程序/导则，对如何履行职责加以描述。

记录政策和程序将确保所有 PSIRT 员工达成共识，实现 PSIRT 产品和服务的一致性与可重复性，同时作为新 PSIRT 员工的培训资源。

B. 评估和改进

确定评估绩效和/或有效性的度量指标，用以找出需要改进之处。

目的： 评估 PSIRT 的运作情况，确定潜在的改进领域。

成果： PSIRT 能够衡量其绩效并了解有哪些领域需要改进。

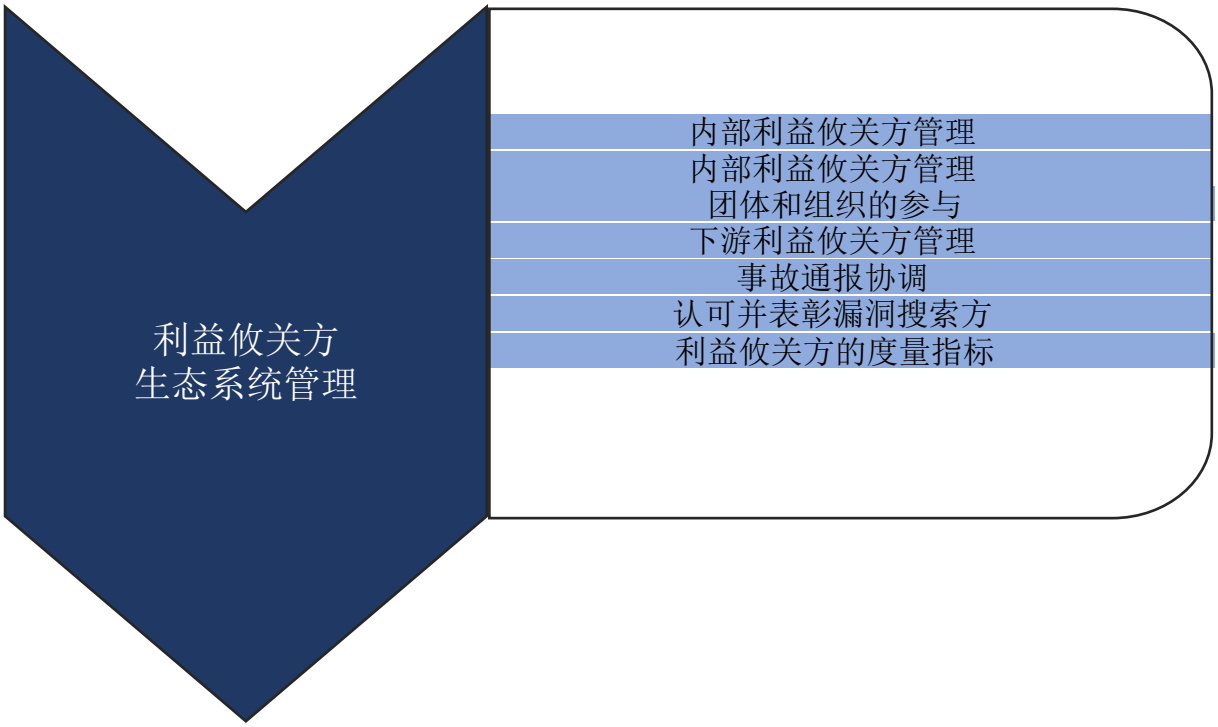
PSIRT 应持续和/或定期评估其表现（产品和服务的提供），并确定所有潜在的

改进领域。

评估的度量指标和方法既可以采用非正式形式（例如，从利益攸关方收集反馈）也可以采用正规形式，并且可按需（例如，记录从吸取的经验教训[参见功能 1.1.3 事故事后分析流程]）或按照指定的时间表进行。

本 PSIRT 框架文件中提供的信息可以作为评估 PSIRT 运作的标准来源或能力之一。

服务领域 1



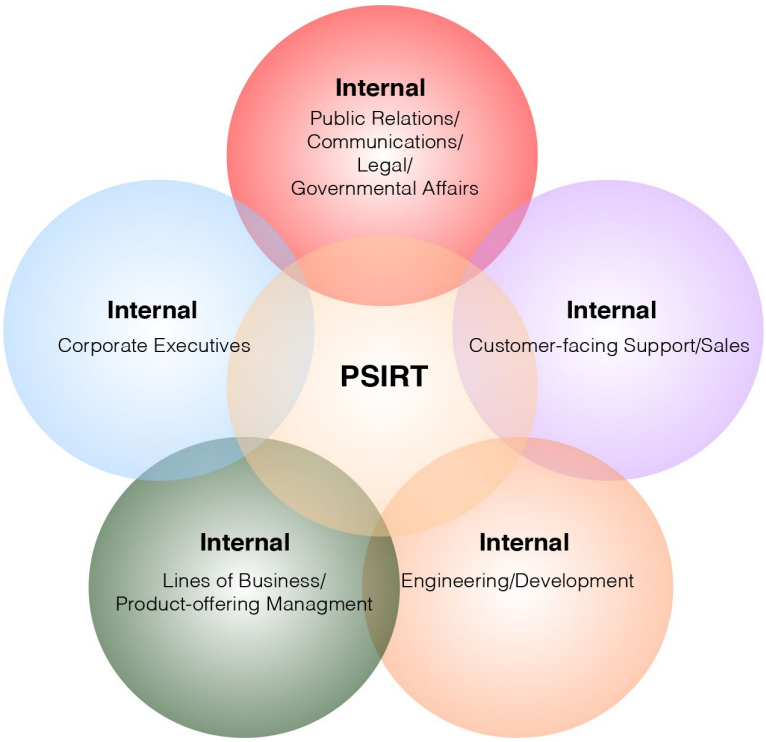
此服务领域描述了 PSIRT 为与内外部利益攸关方开展适当合作所能提供的服务和功能。这方面的服务实际将贯穿事故的整个寿命周期或 PSIRT 的成熟寿命周期。该服务领域致力于确保 PSIRT 的所有利益攸关方均收到适当通报并参与事故响应流程。

在正式提供这些服务之前，PSIRT 必须首先确定与其业务相关的独特利益攸关方。利益攸关方包括行政或业务领导、内部研发团队、外部组件提供商或开发人员，甚至是相关组织的客户群。编制一个利益攸关方与产品/版本的对应关系表，非常有助于简化沟通流程。在与这些利益攸关方沟通之前，了解他们观点、工具或沟通手段（门户网站、个性化电子邮件、互联网聊天、工单系统等）将大有裨益。就本文档而言，利益攸关方分为几组（针对您的具体业务环境，亦可确定其它组）：漏洞搜索方、同行/合作伙伴、内部团队和产品的消费者。

目的： 重点介绍能与 PSIRT 并应与之互动的各类利益攸关方的共享信息流程和机制。

成果： 与 PSIRT 利益攸关方生态系统的成功合作将确保及时报告发现的漏洞，并在必须将安全漏洞通报给组织的利益攸关方时，令利益攸关方/合作伙伴满意。

服务 1.1 内部利益攸关方管理



图中文字：

内部　公共关系/沟通/法律/政府事务　　内部　公司高管

内部　面向客户的支持/销售　　内部　业务线/所推产品的管理　　内部　工程/开发

图 6：内部利益攸关方管理

定义与内部利益攸关方接触的流程，以确保事故意识并在发生事故期间提供协助。内部利益攸关方的成功参与将以明确通报 PSIRT 在组织内的职能，和在产品团队与安全分析师间建立内部联系的方式，完善沟通和响应工作。

目的： 在内部利益攸关方面前确立 PSIRT 的权利和专业知识权威，让漏洞补救和产品安全协调更加顺利。

成果： 有了高度投入的内部利益攸关方，所有 PSIRT 流程和成果的取得均会变得更加顺畅。例如，员工发现的缺陷缓解了暂缓对发发布信息或媒体进行审查带来的直接压力，使问题能够按照有利于组织、消费者和更广泛群体的时间表得以解决，同时最大限度地降低公开披露未消除漏洞的风险。

功能 1.1.1 请内部利益攸关方参与

围绕某组织的产品开发、测试、包装和维护，与内部团队保持积极对话。内部利益攸关方不仅是工程资源，还可能是测试/质量保证的提供者、发布小组、面向利益攸关方的支持团队、销售和营销人员，或该领域的其它技术主题专家。

目的： 利用内部消息/信息平台，向内部员工通报 PSIRT 的存在、流程和功能。

成果： PSIRT 将出台一份正式记录的内部利益攸关方清单，并了解他们的职能和职责。

子功能 1.1.1.1 请公司/企业的领导人和高管参与

为使 PSIRT 有效，该团队必须理解并能对当前的组织环境做出反应。与企业领导和高管合作可在多个层面为 PSIRT 提供帮助。管理层的支持有助于实现组织内 PSIRT 工作的合法化。此项职能使 PSIRT 可与领导分享信息，助力制定商业决策。此外，此职能还允许领导层传达政策和组织方向的变化，这些变化可能会改变 PSIRT 的使命。

子功能 1.1.1.2 请公共关系、法律和企业宣传部门参与

与一系列内部沟通和法律团队合作，将确保 PSIRT 符合当前的品牌和信息标准，且该组织能够融入其必须融入的法规/法律环境（如隐私、联邦空间）。这些利益攸关方均为 PSIRT 的关键利益攸关方提供了独特的路径，并应该在发生关键事件或事故之前建立沟通渠道，以确保各方能够有效合作。

子功能 1.1.1.3 请各业务线参与

与开发领域的利益攸关方合作，可确保将问题相应记录在案、分清问题主次并解决这些问题。例如，PSIRT 的工程师或授权代表需要与负责错误代码的软件工程团队协调漏洞补救工作。在发生事故时，这些伙伴关系亦有助于迅速传递信息以及有效、快速地解决问题。这里的利益攸关方包括项目或产品经理、SDL 监督小组、项目经理、产品所有者以及其它承担类似业务职责的人员。

子功能 1.1.1.4 请开发/工程人员参与

PSIRT 的工程师需要与负责缺陷代码的软件工程团队协调漏洞补救工作。与开发领域的利益攸关方合作，可确保将问题相应记录在案、分清问题主次并解决这些问题。在发生事故时，这些伙伴关系亦有助于迅速传递信息以及有效、快速地解决问题。

子功能 1.1.1.5 请面向客户的销售团队和支持人员参与

PSIRT 工程师需要为利益攸关方支持团队提供解释和工具，以便随着问题的发展和公开化，支持组织对利益攸关方提出的问询和支持请求做出响应。“支持”人员可能包括一线（也称为“服务台”）人员、高端支持资源（例如，技术客户管理员、确保利益攸关方取得成功的负责人等）、内部/外部销售团队或现场资源（咨询、销售工程等）。

子功能 1.1.1.6 内部工作组的参与

在更为成熟的组织中，PSIRT 工程师可通过参与各种内部举措或工作组，建立并加强与内部利益攸关方的关系。这有助于再次确认/建立 PSIRT 的技术专长，为未来的工作建立网络/沟通渠道。

功能 1.1.2 内部安全开发周期

维护并实施安全开发周期，是利益攸关方树立对组织产品的信心与信任的基石。如果不能展示安全标准可在产品寿命周期中重复应用，则利益攸关方可能会对组织的产品失去信心，进而可能会对组织提出更苛刻的要求（举证、审计权等），并可能最终导致收入和利益攸关方信心方面的双重损失。

目的： 遵循优秀安全开发周期实践的组织，将通过在产品开发早期发现安全缺陷的方式，减少补救产品安全缺陷的花费。此寿命周期过程的所有参与方均将清楚地了解人们对安全特性、功能和产品要求的期望，并了解他们在寿命周期中的职能与职责。

成果： PSIRT 将拥有清晰的产品发布信息，并能提供有关交付绩效的度量指标和数据。在成熟的组织内，PSIRT 可以围绕以往产品的常见弱点提供数据，从而避免在未来的工作中出现类似错误。

子功能 1.1.2.1 参加 SDL 活动

SDL 是一个关键的治理过程，有助于组织生产出稳定、可重复且遵循共同标准的产品。PSIRT 参与组织 SDL 的创建和维护，有助于确保采取适当的安全措施并进行相应的检查。

子功能 1.1.2.2 参与 SDL 治理

SDL 是一个关键的治理过程，有助于组织生产出稳定、可重复且遵循共同标准的产品。PSIRT 参与组织 SDL 的治理和执行有助于确保遵循适当的安全实践和检查，并。PSIRT 参与组织 SDL 的治理和实施，有助于确保采取适当的安全措施并进行相应的检查，同时适当记录并审查例外情况。

功能 1.1.3 事故后续处理流程

一旦在组织的产品中发现漏洞，那么无论是代码、流程还是与人员相关的问题，PSIRT 都需要采用某种流程来审查这些问题，以便向参与的利益攸关方和组织领导提供反馈。有些严重或非常严重的公共安全漏洞，可能需要对公司如何应对和纠正这些问题开展更加深入的分析。事后分析是一个内部利益攸关方会议，涉及所有参与补救和沟通工作的利益相关方，目的是记录哪些工作进展顺利，哪些工作可以做得更好，以及未来事件将会发生哪些变化。

目的： 从所有相关方/团队的角度，针对漏洞响应期间发生的事件(包括安全事故)提供清晰、真实的描述。出现重大问题时，PSIRT 可以帮助或领导相关组织就众所周知、影响广泛问题做出补救。

成果： PSIRT 将提供有关组织对软件漏洞所做反应的数据。这些数据将纳入“经验教训”，为在未来事件中做出改进提供依据。

子功能 1.1.3.1 建立产品安全缺陷审查流程

为事后回顾问题建立一个统一的流程，确保在吸取经验教训的同时不断改进产品。

子功能 1.1.3.2 审查流程及发布更新的时间安排

跟踪强项和弱点。

子功能 1.1.3.3 审查重大事故

协调收集组织取得经验教训，对重大事故做出的响应和反思，并按需向业务部门和其它利益攸关方提供报告数据。

服务 1.2 漏洞搜索团体的参与

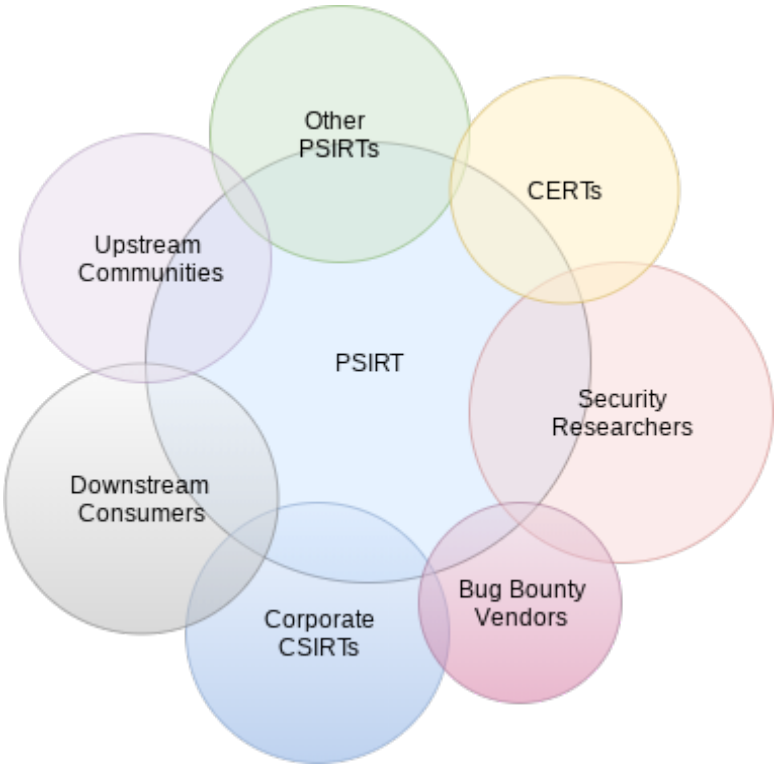


图 7：PSIRT 外部利益攸关方示例

图中文字：

其它 PSIRT　CERT　上游团体　安全研究人员　下游消费者

公司 CSIRT　Bug Bounty 厂商

与邀请研究团体作为利益攸关方参与工作有关的服务。漏洞搜索方有诸多不同职能和独特的视角—他们可能是学者、开发专业人员、专业的安全漏洞搜索人或业余爱好者。漏洞搜索方可能正在研究理论攻击或缺陷，希望发布相关成果并取得学术成就，而另外一些搜索方或许是金融或公司聘请的专业安全漏洞搜索人。还有一些搜索方可能是业余爱好者或有闲暇的狂热爱好者，其动机或许是为了获得相关团体的尊重和赞誉。漏洞搜索社团的参与是一种主动的产品安全事故响应方法。

目的： 将组织的 PSIRT 定位为研究团体的积极参与方，针对可能影响组织产品安全的威胁建立情况感知。与漏洞搜索方关系不良或存在敌对关系可能导致研究无法获得早期通知，使组织在应对安全漏洞时处于不利地位，从而影响利益攸关方对组织的看法。

成果： 研究团体的成功参与将强化组织在确保产品安全方面的声誉和市场地位。此外，与漏洞搜索方的积极合作可以尽早获得研究和/或安全漏洞披露方面的信息，有助于组织为最终的公开发布做好准备。

功能 1.2.1 请漏洞搜索方参与

通过开展一系列活动，与在公司产品安全和获得不同渠道方面拥有专长的漏洞搜索方保持积极对话。PSIRT 可以开展大量活动，以便更深入地融入漏洞搜索团体。这方面的操作可能包括与合格的漏洞搜索方签订专项合同，在大会和其它活动期间与他们合作，甚至是为学术研究提供赞助。

目的： 在社交媒体网站上建立影响力。监控社交媒体网站和其它常见网站/论坛，寻找漏洞搜索方或利益攸关方有可能发现的问题的指标。考虑定期参加安全会议，与漏洞搜索方进行面对面的会晤。

成果： 由于提出了明晰的沟通预期，PSIRT 将更频繁地收到质量更高的报告，并得到高参与度漏洞搜索方提供的提前量更大的通知。

功能 1.2.2 请其它 PSIRT 参与

培养与伙伴 PSIRT 之间的关系有助于信息共享且在事故期间有可能开展互助和/或协调。与这些对等组织合作有利于以填充重要数据的方式修复漏洞，并在两个团队就相关问题进行协商时，使组织得到对等组织的专业帮助。PSIRT 应与关键对等 PSIRT 建立通信渠道（正常和安全）。对信息共享和协调同时影响两个组织的问题而言，与业界同行建立并培养关系至关重要。

目的： 在贵组织与其它 PSIRT 之间建立通信渠道，共享漏洞信息、有关威胁的情报和最佳实践。

成果： 在应对与软件供应链相关的漏洞方面，对等 PSIRT 团体极具价值。有望

获得更快的响应速度。

子功能 1.2.2.1 记录和定义对等 PSIRT

收集联系信息和参与流程，以备将来使用。PSIRT 应与更大的 PSIRT 团体接触并互动，分享有关经验教训的最佳实践和见解。随着漏洞的出现，人们通常以协作、多团体参与的方式消除这些漏洞，并允许 PSIRT 利用从这些外部对等团体获得的信息和/或帮助，扩展其内部能力。

子功能 1.2.2.2 定义协调披露流程

PSIRT 应仔细记录漏洞信息的共享参数和协议。PSIRT 应该遵守漏洞搜索方和/或报告组织设定的暂缓信息发布参数（并认为 PSIRT 参数亦得到遵守）。

子功能 1.2.2.3 建立安全信息共享流程

PSIRT 应制定方法，与协调披露协议所涉各方安全地共享漏洞信息及其它机密信息。可选方案包括紧急传送、非电子通信、加密电子邮件/门户或私人邮件列表等。

子功能 1.2.2.4 参与行业 SIG 和工作组

在业界感兴趣的话题上与同行合作，支持建立并加强联系，并通过齐心协力解决问题进一步推进行业专业化。

功能 1.2.3 与协调员合作（CSIRT 和其它协调中心组织）

与政府 CSIRT 合作不仅有助于建立信息共享信任，亦有助于 PSIRT 赢得同行的信任和尊重。其它对此感兴趣的组织或团体包括 FIRST、MITRE、推进信息社会开放标准（OASIS）组织、互联网安全推进行业联合会（ICASI）、国际标准化组织（ISO）等。我们可以从国家、企业、区域或工业部门的视角看待参与团体。

目的： 组织经常成为威胁的目标，这些威胁发起者经常利用以前未知的漏洞渗透网络。与 CSIRT 建立关系可以获得必要的信任和联系，从而在早期阶段便得到有关潜在漏洞的报告。

成果： 与 CSIRT 和其它协调中心组织建立良好关系有助于及早发现漏洞，并有望获得更快的响应速度。

子功能 1.2.3.1 请团体和合作伙伴参与

PSIRT 应研究心目中的外部团体在哪里参与对话，并努力加入这些论坛。

功能 1.2.4 与安全研究人员互动

安全研究人员种类繁多，例如学者、业余爱好者和专业的安全事务从业者。这些人员是搜索行业漏洞的主力军。研究人员将尝试联系产品的所有者，但由于各种原因，并非总能如愿。PSIRT 被动地接收来自这些个人或团体的报告，被迫

在由外部控制的时间框架内工作。主动接触在会给 PSIRT 产品造成影响的领域开展研究的安全研究人员，并与相关团体积极互动从而更深入地了解发现的问题，符合 PSIRT 的最佳利益。

子功能 1.2.4.1 与安全供应商合作

大规模的商业安全供应商在安全遭破坏期间与利益攸关方合作，通常会获得 PSIRT 一般无法获取的取证数据。发展与这些供应商的关系有助于建立信任和相互尊重，并且可帮助 PSIRT 完美地获得其它方式可能无法获得的关键威胁数据。

子功能 1.2.4.2 记录相关的安全供应商

了解安全供应商并与之适当合作，可以在这些供应商向 PSIRT 报告问题时，加快有关漏洞报告/补救的沟通与处理。同样重要的是要了解这些供应商将获取和保留哪些信息。在建立关系之前，应充分记录并审查组织与 bug bounty 供应商之间的关系，让所涉各方知晓供应商的行为方式、可以接入哪些资源、如何共享数据以及与谁共享数据。

子功能 1.2.4.3 记录与安全供应商合作的方法

PSIRT 应研究其心目中的外部团体在哪里参与对话，并努力加入这些论坛。

功能 1.2.5 与 Bug Bounty 供应商合作

与 bug bounty 供应商建立关系，围绕漏洞管理加强沟通和数据共享。

目的： 如果贵组织经常收到为漏洞搜索方付费的供应商/经纪人提供的漏洞报告，则请考虑与这些组织保持直接关系。这些组织经常针对有待消除的漏洞制定服务水平协议(SLA)。

成果： 与 bug bounty 供应商直接建立关系，便可就通报产品安全补丁的发布过程开展建设性对话。除制定经一致认可的服务水平协议外，这种关系有助于降低零日漏洞（zero-day vulnerabilities）的风险，对所有利益攸关方均有利。

子功能 1.2.5.1 记录并定义相关 Bug Bounty 计划

记录并定义适用于组织所提供产品的 bug bounty 供应商。

子功能 1.2.5.2 请 Bug Bounty 供应商参与

确定渠道，让这些 bug-bounty 供应商积极参与对话。

功能 1.2.6 预测 CSIRT 的需求

CSIRT 属于特殊类别的“下游”利益攸关方，仅关注安全问题。虽然人们通常可以通过标准的利益攸关方参与做法和客户管理方式与这些团体互动，但 PSIRT 应当了解这些以安全为关注重点的团队的独特要求与观点。这些团队将联系 PSIRT

并使用来自 PSIRT 的信息。相关信息包括披露的格式和时间表（见服务 5.3 披露），以及特定请求的沟通渠道。

服务 1.3 相关团体和组织的参与

PSIRT 将与之互动的两个利益攸关方团体需要更多关注。相关团体的参与有时被称为“上游”和“下游”，是联合开展补救或为组织内其它同行团体间的互助提供帮助的关键所在。“上游”这一术语是指某些团体或个人，他们为贵组织提供基本组件或贵组织使用其产品。“下游”是指亦是指某些团体或个人，他们将贵组织的输出内容作为其产品的一部分。下游参与请参见服务 1.4 下游利益攸关方管理。

活跃的上游团体有助于将创新注入产品流，并可缓解补救复杂漏洞带来的负担，通常可以弥补组织在关键主题方面的专业知识不足。同样，与其它组织的下属个人及团队建立专业关系，可通过外部视角、专业技能和沉淀的知识，帮助扩展 PSIRT 的能力。主动让安全团体作为利益攸关方参与进来、与合作伙伴和对等 PSIRT 建立关系，可作为实现这一目标的手段。

目的： PSIRT 需要建立和维护一个活跃的合作伙伴和同行生态系统。这些团体协会可采用“多人监督”（“many eyes”）的方法发现缺陷并做出补救，并在不同群体之间分享优良做法，以提升漏洞补救的总体经验。

成果： 良好的合作伙伴和同行关系以及活跃的生态系统，将促进有关威胁情报的信息共享，有利于最佳做法的推行。在安全界中享有良好声誉的 PSIRT 可能有助于吸引资源并与合作者共同应对紧急情况。

功能 1.3.1 定义上游团体及合作伙伴并与之合作

本文所述产品经常包含并非由组织创造的代码或组件。这些产品的原始制造商有时被称作第三方、供应商或上游供应商、原始设备制造商或合作伙伴。在您的生态系统中找出这些合作伙伴，并确定在第三方代码中发现漏洞时，组织将如何联系第三方及这些合作伙伴，将非常有帮助。

目的： 与为您提供组件的个人或团体或从您这里获得组件的团体建立友好的工作关系。知晓与谁联络以及如何联络这些团体将使 PSIRT 能够了解即将发生的问题，并清楚当 PSIRT 发现他人从 PSIRT 收到受影响的组件时，需要向谁通报。

成果： PSIRT 将更好地了解组件的生产方及产地。当发现这些组件存在缺陷时，应能更迅速的获取信息并进行修复。

子功能 1.3.1.1 记录并定义上游团体及合作伙伴

上游团体和合作伙伴提供代码和/或知识以及专业技能，并将其纳入组织提供的产品。了解这些供应商并与他们合作至关重要，这有助于在 PSIRT 收到安全漏洞报告并加以处理时，与供应商进行快速有效地互动。理想情况下，合同、保密协议及其它旨在保护组织的文件会记载这些关系。

子功能 1.3.1.2 请相关团体及合作伙伴参与

各个上游团体或合作伙伴可能使用不同的方法或工具开发并交流其软件/产品。PSIRT 应了解如何与这些外部团体合作，并确保为与这些外部团体就安全问题开展合作，指定联系人/规定方法。

子功能 1.3.1.3 参与上游团体的活动

参加上游团体的活动和合作伙伴的参与有助于建立宝贵的团体间互信，也有助于利用组织其拥有的专业知识增强外部团队的能力。

子功能 1.3.1.4 参与团体和行业活动

专业组织的大会和会议是 PSIRT 与利益攸关方和合作伙伴进行互动的绝佳场所，可以获得组织的直接反馈，并在外部团体中建立良好的信誉和积极的声誉，以便未来开展协调/协作。

子功能 1.3.1.5 请相关团体的安全团队参与

至关重要的是，PSIRT 要知晓通过谁以及如何联系上游软件/硬件/服务提供商的安全团队（PSIRT、CSIRT、安全工程师）。在 PSIRT 和这些团体之间建立沟通和汇报渠道，有助于确保危机或漏洞修复期间的顺利互动。

功能 1.3.2 定义下游团体及合作伙伴并与之合作

“下游”有许多含义，但这并不意味着 PSIRT 应该忽略这些重要的利益攸关方群体。“下游”是指接受 PSIRT 公司的产品和服务并利用这些产品和服务实现自身目的的任何产品、组织或个人。顾客或商品和服务的消费者是下游团体最常见的形式，但情况并非总是如此。通常，另一家公司可以使用或授权他人使用 PSIRT 公司的产品，并通过第三方将其作为产品转售，或者在开源软件的情况下（这种情况经常发生），某个团队将负责提供并维护软件，而一批附属方将使用这些资源（亦称为源的下游）。

子功能 1.3.2.1 记录并定义下游团体、消费者和合作伙伴

下游团体和合作伙伴使用已整合到组织产品中的代码和/或知识以及专业技能。理想情况下，合同、保密协议及其它旨在保护组织的文件会记载这些关系。

子功能 1.3.2.2 参与下游团体的活动

每个下游团体或合作伙伴都可能使用不同的方法或工具开发交流其软件/产品。PSIRT 应了解如何与这些外部团体合作，并确保为与这些外部团体就安全问题开展合作，指定联系人/规定方法。

服务 1.4 下游利益攸关方管理

为使您的利益攸关方群成为利益攸关方，PSIRT 必须围绕产品安全响应建立与利益

攸关方团体互动的流程和方法。最为重要的是令与组织产品有关的利益攸关方始终保持满意，因为他们为组织当前和未来取得收入提供了机会。

目的： PSIRT 需要与组织的利益攸关方群体建立沟通渠道并加以维护，用以发布关于产品安全漏洞的信息或在事故响应工作中传递信息。

成果： 与利益攸关方保持的良好关系不仅能够确保（或在某些情况下增加）收入，还能让利益攸关方对贵方的产品发表意见，对他们参与设计解决方案起到鼓励作用。

功能 1.4.1 与下游利益攸关方合作

贵方产品和服务的利益攸关方应在分享信息、意见渠道，以及如何处理安全漏洞问题上得到支持。主动与相关组织的利益攸关方合作有助于提供积极的品牌体验，并可保持/提高利益攸关方的忠诚度。

目的： 为组织的下游利益攸关方提供与 PSIRT 沟通的方法，并获得有关安全问题的支持。如果对利益攸关方的问询或要求反应不当，则可能会给品牌造成负面影响，例如出现负面的公众评论、丧失续约机会或失去新业务。

成果： 下游利益攸关方应快速获得有关安全缺陷的明确指导。这将提升对产品的信任度，并有助于提高品牌忠诚度。在 PSIRT 的帮助下创造积极的整体体验，并与利益攸关方分享 PSIRT 专业知识。从总体上改善利益攸关方对整个品牌的看法。

子功能 1.4.1.1 提供清晰的寿命周期和支持策略

组织应该明确地公开描述利益攸关方对修复安全漏洞的期望，以及产品可获得支持的时长。更多信息请参考 服务领域 4。

子功能 1.4.1.2 请利益攸关方参与

组织产品和服务的利益攸关方将会提出问题，请求帮助或者需要对上报的安全缺陷做出补救。PSIRT 应积极响应利益攸关方的请求，就安全漏洞提供清晰准确的指导并提供风险缓解措施，直至可以为利益攸关方提供补救。

服务 1.5 组织内部的事故通报协调

安全事故涉及组织内的诸多内部团体，可能还包括其产品。PSIRT 是协调漏洞修复工作的中心，亦是与获得授权的内部利益攸关方共享事件信息的枢纽。

目的： 确保企业内部各方均了解安全漏洞响应的状态，以便他们能就接下来要采取的步骤做出明智决策。沟通可以采取多种形式(电子邮件、传统邮件、RSS 提要、社交媒体等)。但最终所有渠道都会为利益攸关方提供清晰、及时、准确的安全漏洞和事故信息。

成果： 内部利益攸关方将被告知组织产品所面临威胁的范围和影响。应通知利益攸关方，以便他们能在补救安全漏洞和缓解措施可用时，采取适当的后续步骤。

功能 1.5.1 提供沟通渠道/出口

为了有效地与利益攸关方合作，PSIRT 必须提供各种沟通渠道。利益攸关方可能更偏爱某些渠道。PSIRT 的信息编写与发布，应考虑到尽可能多的受众。PSIRT 还应具备从各种来源获取安全报告、评论和问题的能力。

目的： 为利益攸关方提供方法，使其能与 PSIRT 沟通。

成果： 这些渠道，无论是电子邮件，聊天还是网络形式，都允许内部利益攸关方与 PSIRT 沟通、分享信息。

子功能 1.5.1.1 提供明确的沟通渠道

利益攸关方应该拥有提交问题的渠道，对缺陷状态进行检查并向 PSIRT 报告问题。如果利益攸关方受到安全漏洞的影响或发现安全漏洞，他们应能够轻松地起草报告并将报告提交给 PSIRT。

子功能 1.5.1.1.2 提供内部沟通渠道

为邀请内部利益攸关方参与，PSIRT 应为公布漏洞的补救状态提供沟通渠道。内部利益攸关方应能方便地联系 PSIRT，了解通过询问可以获得哪些信息。

子功能 1.5.1.1.3 提供外部沟通渠道

为邀请外部利益攸关方参与，PSIRT 应为公布漏洞的补救状态提供沟通渠道。相关操作包括围绕外部沟通开展审查/资格认定活动，以确保沟通的有效性并同时确保将这些沟通内容传递给相应的内部员工。

功能 1.5.2 安全通信管理

通常情况下，PSIRT 必须处理机密信息（即处于暂缓信息发布状态的问题）。PSIRT 需要能够与漏洞搜索方、其它组织或各种内部资源进行安全的私下沟通。遵守披露协议且只通过私下方式沟通，有助于让漏洞搜索方建立信心。根据暂缓信息发布的条款，保护机密漏洞信息免受未授权方的攻击，亦有助于确保问题得到适当、有效的管控。安全通道还有助于保护希望保持匿名的漏洞搜索方的身份。应建立保留策略，以确保数据在使用结束后得到妥善处置。

目的： 为各方就安全漏洞私下交换信息提供便利。这些渠道为安全漏洞和漏洞搜索方的保密性提供保护，直至可将这些信息公诸于众。

成果： 为安全问题提供支持的各方可与需要了解某问题的其它相关方私下分享信息。如果漏洞搜索方觉得他们关注的问题受到组织的保护，他们将来很有可

能仍会向组织报告有关问题。

子功能 1.5.2.1 提供安全的沟通渠道

PSIRT 应确保漏洞搜索方和致力于消除组织产品漏洞的合作伙伴拥有保密且安全的方法来共享信息。

功能 1.5.3 安全缺陷跟踪系统的更新

PSIRT 应能访问记录全部产品缺陷的系统，并能创建和使用某种系统来跟踪、共享关于安全漏洞的信息。

目的： 对安全缺陷的正确记录和跟踪，使组织能够指出在何时何地消除了漏洞。此缺陷处理系统亦使 PSIRT、漏洞搜索方与正在积极解决问题的工程师进行交流成为可能。

成果： 利用系统适当地跟踪安全漏洞，所有需要获取缺陷信息的各方均可查看该缺陷的历史、变化以及关于它的评论。

子功能 1.5.3.1 为产品提供安全缺陷跟踪

相关方应跟踪安全缺陷并能访问这些系统（在最低权限模型内），且内部和外部各方（如果适用）可以更新并跟踪进度。外部漏洞搜索方应就其向 PSIRT 提交报告的状态进行充分沟通。

子功能 1.5.3.2 创建和发布安全缺陷跟踪流程

PSIRT 应确保漏洞搜索方和致力于消除组织产品漏洞的合作伙伴拥有保密且安全的方法来共享信息。

功能 1.5.4 信息共享和发布

在问题得到解决后，PSIRT 应提供有关什么是安全漏洞的信息，若将 CVSS 作为一项因素，其严重性和影响是什么，漏洞可以利用哪些潜在风险，以及如何解决或缓解问题。目前，一种在大范围/公共范围内广泛使用的提供漏洞信息的方法是，获取漏洞的 CVE 条目。这种方式通过提供识别号、说明和至少一个公共参考等手段，确保以独特的方式引述相关问题。

目的： 分享已报告并修复的安全漏洞的详细信息。利益攸关方应能接受采用相应处理办法或替代性缓解措施对风险加以控制，直至正式修复方法出台。

成果： 利益攸关方将获悉安全问题、其可能受到的影响以及使用的补救措施。能及时收到信息和软件更新的利益攸关方，更倾向于对组织抱有积极的看法，他们要么继续使用组织目前提供的产品，要么将拓展组织产品未来的用途。

子功能 1.5.4.1 提供多个沟通渠道

随着漏洞的公开披露，不同利益攸关方倾向于采用不同的互动/沟通方法。

除了传统的咨询式更新之外，PSIRT 还应确保使用其它方法确保受漏洞影响的利益攸关方，能最大程度地参与其中并意识到漏洞的存在。修复漏洞后，PSIRT 应使用多种手段公布修复结果。

子功能 1.5.4.2 向利益攸关方提供反馈

反馈有助于改进流程并提升未来的响应水平。通过反馈可以突出 PSIRT 擅长的领域，并应在 PSIRT 需要进一步发展和改进的领域继续发挥作用。

服务 1.6 通过表彰和认可奖励漏洞搜索方

对漏洞搜索方的认可有助于在相关团体内，树立起漏洞搜索方及其组织（如适用）的信誉，此外亦可对 PSIRT 在缺陷问题上的合作表示感谢。

目的： 漏洞搜索方因努力协调披露产品漏洞而得到认可。这些搜索方可凭借认可赢得声誉，构建一个专业知识库，并向组织展示其价值。

成果： 与漏洞搜索方积极合作将提高产品安全性。对漏洞搜索方的认可，有利于内部员工确立自己的声誉并展示自身的专业技能。

功能 1.6.1 认可

对发现安全漏洞人员的认可是安全漏洞工作流程中的一个要素。表达小小的感激不仅可以在团体内部建立信任和尊重，亦能表明组织对安全问题做出了响应。

目的： 漏洞搜索方因努力负责地披露产品漏洞而得到认可。这些搜索方可凭借认可赢得声誉并构建一个专业知识库。

成果： 与漏洞搜索方积极合作将提高产品安全性。对漏洞搜索方的认可有利于内部员工确立自己的声誉，并可鼓励漏洞搜索方将来继续向 PSIRT 发送漏洞报告。

子功能 1.6.1.1 认可

对漏洞搜索方所付出努力及其参与发现安全漏洞工作的书面认可，是 PSIRT 奖励这些搜索人最有效且最为廉价的工具。传统做法是在安全公告、软件版本说明和 CVE 文本中表达漏洞搜索方的感谢。PSIRT 需要知晓如何通报已发现漏洞的内部属性。

功能 1.6.2 奖励漏洞搜索方

为给利益攸关方带来积极的结果并鼓励进一步分享研究成果，PSIRT 可以选择为奖励或激励这种合作制定一个计划，以使这种合作能在未来得以延续。

目的： 为报告组织产品和服务中安全缺陷的人员颁发奖励。奖励可以采取多种形式，既可以是电子/纸质感谢信、组织夸赞、货币礼品，也可以是其它商品/

礼物。PSIRT 需要保证奖励和奖励规则的透明。

成果：这种做法旨在表达 PSIRT 组织的善意，鼓励大家未来继续围绕安全问题开展协作。

子功能 1.6.2.1 制定漏洞搜索方奖励计划

PSIRT 可以赞助一项奖励计划，鼓励安全漏洞搜索方的积极表现。奖赏方式可以是金钱、公司夸赞，或者漏洞搜索方看重任何一种方式，其价值要高于对发现问题的认可。

子功能 1.6.2.2 发起一个货币 Bug Bounty

奖励的形式之一可以是货币报酬。有些组织会为向其披露漏洞信息的搜索方付费。

子功能 1.6.2.3 设立一个‘得分榜’（‘Points Board’）

另一种形式的报答是设立 “得分榜”。这种做法将发现和报告安全漏洞游戏化，通过宣传 “状元”和可资漏洞搜索方吹嘘的排名，鼓励开展良性竞争。

服务 1.7 利益攸关方度量指标

提供有关 PSIRT 数量、绩效或其它衡量结果的细节，对于让利益攸关方了解 PSIRT 的有效性而言至关重要。不同的利益攸关方都有各自独特的观点，必须以不同形式（或视图）加以处理。PSIRT 必须了解各利益攸关方团体希望如何使用这些信息。这些度量指标可以是 PSIRT 的关键绩效指标。功能 2.5.1 涉及运作报告以及 PSIRT 应如何考虑提供此类报告，以确保运作顺利。功能 2.5.2 负责审查 PSIRT 认为可以向利益攸关方提供的业务报告。

目的：提供关于 PSIRT 衡量和绩效的数据。这有助于利益攸关方了解 PSIRT 在特定领域或提供服务方面的有效性。

成果：通过审查 PSIRT 的度量标准，利益攸关方应当能够了解 PSIRT 提供服务的效率并能提供反馈，从而对服务交付做出调整。

功能 1.7.1 了解利益攸关方的工具需求

有效阐明 PSIRT 如何提供服务的第一步是要了解各利益攸关方群体的独特观点。有些利益相关方可能担心是否能够及时提供安全补丁，而其它利益相关方则可能关注 PSIRT 运作的财务问题。各种观点均有其道理，但需要不同的工具有效地提出希望得到的信息。应对所有利益相关方群体进行调查，以了解他们需要哪些方面的 PSIRT 数据，以及共享这些信息的最佳方法。

目的：了解利益攸关方对 PSIRT 运作和服务的关切。一旦需求收集完毕并就这些需求达成一致，人们就需要选择交付的方法/媒介以及更新的节奏。

成果： 编制利益攸关方工具(报告/视图/记录板)需求的记录表，以便于维护。

子功能 1.7.1.1 收集利益攸关方的度量指标要求

有些利益攸关方会关注一组特定数据，而其它一些利益攸关方则可能对此毫不关心。例如，此类度量指标可能涉及扩展补丁修复团队表现、成本和质量的衡量范围。

功能 1.7.2 收集利益攸关方的度量指标

记录为各利益攸关方群体规定的度量指标所需采用的流程和应采取的行动。只要有可能，PSIRT 使用的工具应能收集并提供关于 PSIRT 流程和绩效的信息。在理想情况下，度量指标应集中存储（数据库、电子表格或其它工具），以便定期审查以往绩效，并将处理不同利益攸关方观点所需的额外工作量降至最低。

目的： 围绕 PSIRT 的绩效维度，收集、生成、汇总和/或采集满足利益攸关方要求所需的数据点。这些信息应集中存储，用于审查以往的历史并供利益攸关方重新使用（即，两个或更多利益攸关方团体希望获得相同的信息)。

成果： 将为创建工具(报告、视图、记录板等)收集所需的利益攸关方度量指标。

子功能 1.7.2.1 收集利益攸关方度量指标

PSIRT 应创建流程和方法，以便在规定的时间间隔内收集所需度量指标（服务水平协议/OLA）。

子功能 1.7.2.2 存储利益攸关方度量指标

PSIRT 需对绩效和其它趋势进行历史分析，因此为这些数据开发一个存储库非常有益，可供将来继续使用。

功能 1.7.3 分析利益攸关方的度量指标

没有背景的数据是没有意义的。我们可以推断出不正确的假设，但可能不会调整服务以满足不断变化的业务或利益攸关方的需求。一旦 PSIRT 收集到所需数据，必须努审查，并就这些数据针对利益攸关方的意义提供必要的背景。

目的： 了解所收集数据的含义，并向利益攸关方提供如何处理信息的背景。理想情况下，利益攸关方应能了解给定的关键绩效指标（KPI）表现如何，报告期间哪些因素对其产生了影响，并且能够看清该 KPI 的趋势。

成果： 历史数据将得以保留并与当前绩效进行比较，以藉此确定趋势。

子功能 1.7.3.1 分析和审查度量指标数据

PSIRT 应花费时间和精力审查收集的数据，并提供与度量指标报告相关的背

景。

子功能 1.7.3.2 分析数据趋势和历史表现

随着历史数据的收集，可以确定 PSIRT 或其合作伙伴有能力应对的独特趋势或长期问题。

子功能 1.7.3.3 提供数据背景

提供数据背景，以便利益攸关方能够正确地了解他们将得到什么，同时提供解决问题或关切的方法。

功能 1.7.4 为利益攸关方提供度量指标工具

在收集和分析度量指标后，必须将其以商定的格式交付给利益攸关方。我们可将这种格式视作工具，或是处理利益攸关方观点的一种方式。这些工具可以采用网页、电子邮件、更正式的报告或其它形式。

目的：应该以利益攸关方能够理解的形式为其提供度量数据，让他们能够获得有关 PSIRT 在提供服务方面表现的洞见与理解。这些数据应不难理解，可为帮助利益攸关方在相应表现的基础之上做出决策，提供充分的背景信息。

成果：将在商定的时间框架内以适当形式向利益攸关方提供度量指标。

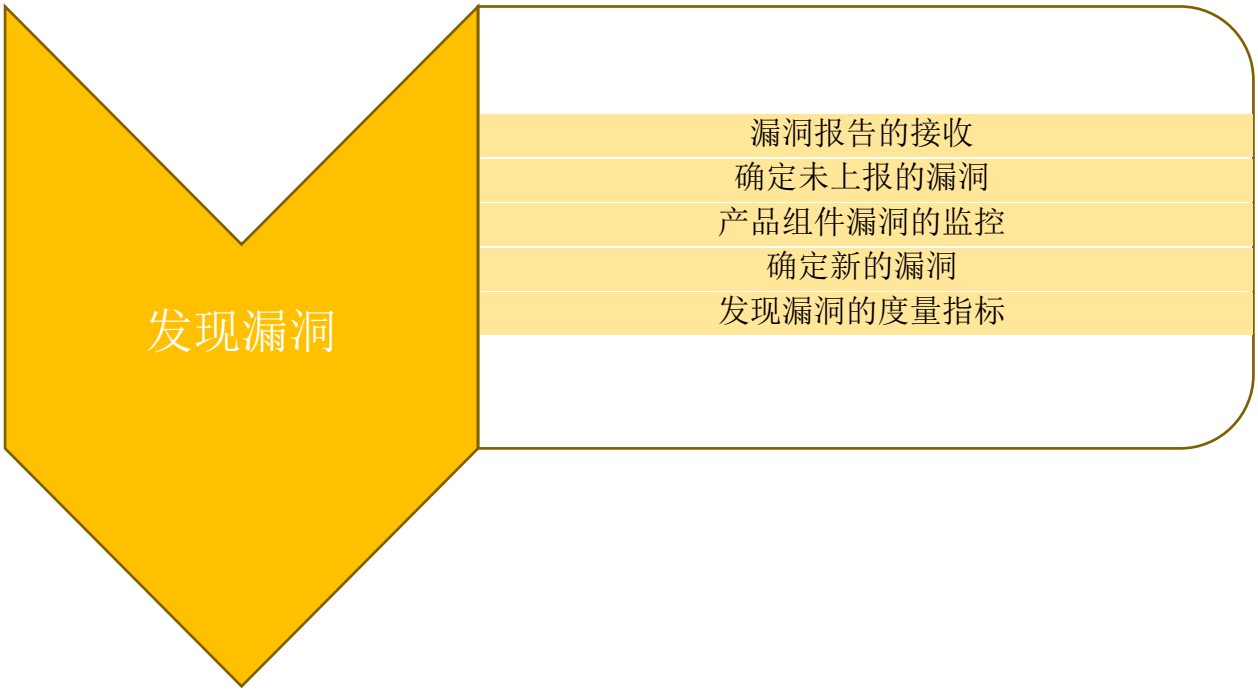
子功能 1.7.4.1 为利益攸关方提供度量指标工具

各利益攸关方都有自己独特的观点。各种观点都需要从某种报告工具形式的数据视角加以处理。为匹配不同的观点，可能需要对这些工具进行调整。此类工具可能包括通过电子邮件发送或发布到网页的报告、动态门户网站、执行简报、图表、图形或任何其它数据传递机制。

子功能 1.7.4.2 回顾度量指标和经验教训

PSIRT 最重要的目标之一应是不断改进漏洞管理的过程。回顾绩效指标和利益攸关方反馈有助于 PSIRT 确定需要关注或改进的领域。

服务领域 2



这一服务领域介绍了 PSIRT 可能为发现潜在漏洞而执行的服务和功能。此服务领域的操作将触发本文其它章节所述的漏洞处理过程。PSIRT 的成熟度可以通过该服务领域规定的不同服务的可用性及效率加以衡量。

目的： 建立流程和机制，从各种来源收集与产品漏洞、易受攻击的第三方组件或架构缺陷相关的情报。

成果： 提高利益攸关方对需要采取行动的报告和潜在漏洞的情况感知。

服务 2.1 漏洞报告的接收

对 PSIRT 而言，主要工作场景是接收影响利益攸关方产品的报告。接收漏洞报告的一个关键要素是设置和维护所需的基础架构，确定并公布联系人，同时定义并保持就绪状态。

目的： 建立流程和机制，使实体轻松报告利益攸关方产品中的漏洞，并确保 PSIRT 在收到漏洞报告时保持就绪状态。

成果： PSIRT 为接收脆弱性报告做好准备并以专业的方式接收脆弱性报告。

功能 2.1.1 确保可达性

PSIRT 必须让相关方认识到他的存在，既向外部各方提供服务又让内部各方有上报途径。清晰明确的沟通渠道有助于漏洞搜索方、合作伙伴或利益攸关方向 PSIRT 报告漏洞。

目的：使有兴趣报告漏洞的实体能够轻松找到所需联系信息及其喜欢的提交方式。

成果：获取更多报告，排除任何关于 PSIRT 无法接受漏洞信息的说法。

子功能 2.1.1.1 确定首选的报告提交表单

我们有可能通过不同渠道接收不同质量的漏洞报告。确定处理报告的最佳方式仍然很有帮助。报告可能使用网络表单、公开的工单系统、电子邮件地址、支持热线或任何其它提交方式。

子功能 2.1.1.2 公开详细的联系信息

PSIRT 的首选联系信息应在产品文档中发布，通过公司网页广而告之，在搜索引擎中编制索引，在主要 CSIRT/PSIRT 列表中登记，向 CVE 编号机构（CAN）等发布常见漏洞陈列（CVE）的实体通报，并在安全团体内公布。

子功能 2.1.1.3 注册常用联系人

在贵公司的域名中保留‘psirt@’、‘incidents@’或‘security@’等与 PSIRT 相关的常用术语很有帮助。保留这些术语能够为将相关 PSIRT 信息直接发送给您提供方便。

子功能 2.1.1.4 连接公司内部的 PSIRT

确保利益攸关方服务部门（针对利益攸关方的请求或漏洞报告）、沟通部门（针对媒体请求）以及您的产品开发团队（针对逐步升级的重大内部调查结果）了解 PSIRT 并知道如何与 PSIRT 联系。

子功能 2.1.1.5 定义并维持就绪状态

根据行业和利益攸关方提出的要求，制定随时待命的机制或遵循 sun 的职责要求，为响应关键报告做好必要准备。

子功能 2.1.1.6 准备加密提交

漏洞报告通常包含有关已发现漏洞所在操作环境及相关产品的敏感信息。为避免意外的信息泄露或披露，提倡以加密方式提交报告，如采用 S/MIME 或 PGP 保护的电子邮件或使用支持 HTTPS 的网络表单。

功能 2.1.2 处理漏洞报告

漏洞报告的来源不同，形式各异。定期监控通信接收渠道并及时对接收的报告做出回应至关重要。对外部漏洞搜索方的响应时间应在公司内部的服务水平协议中定义。

目的：提供流程和机制，以接收来自供应商公司其它部门、利益攸关方和第三方(漏洞搜索方、其它 PSIRT、CSIRT 等的漏洞报告)。

成果：专业化的处理来自第三方的漏洞报告。

子功能 2.1.2.1 监控沟通渠道

定期查看对外公布的 PSIRT 联系方式以及其它可用的沟通渠道，例如一般用途的电子邮件收件箱或公司社交媒体账户。

子功能 2.1.2.2 独立处理报告

漏洞报告将由 PSIRT 调查，因此很容易通过恶意提交锁定目标。制定政策和技术程序，提供安全处理漏洞报告的方法，以保护工作环境免受此类企图的攻击。

子功能 2.1.2.3 报告的及时确认

报告的详细分析通常既复杂又耗时，但如果仅是确认报告则应能很快实现。迅速做出反应表明报告得到了认真对待，大大有助于建立信任关系。整个处理过程的后续沟通可建立在第一次合作的基础之上，同时这表明 PSIRT 致力于提供可理解的解决方案。

服务 2.2 确认未报告的漏洞

直接向供应商披露的漏洞或报告方提供漏洞都一目了然。然而，重要的是要认识到，还有一些其它漏洞可以通过非正式渠道披露，如新闻渠道、技术博客、专家数据库、社交媒体或技术出版物以及会议。

目的：保持情况感知，缩短发现利益攸关方产品面临的威胁所需的时间，并降低全面披露的可能性。

成果：利益攸关方产品组合在安全威胁方面的情况感知增强。

功能 2.2.1 监控漏洞数据库

应积极监控公开可用的漏洞数据库或商业反馈，藉此发现需要调查的潜在零日漏洞。仍然存在的漏洞可能会导致相关公司与利益攸关方主动沟通。

目的：发现从未通过适当渠道报告的漏洞。

成果：增强对市场现存功能漏洞的了解。

功能 2.2.2 追踪大会的相关计划

应对安全会议进行追踪，以寻找感兴趣的提交资料。除直接提及相关产品或品牌外，提交资料可能会论及更广泛的话题，例如可能需要 PSIRT 处理的协议缺陷。如果资料摘要提出问题，最好在早期阶段就与漏洞搜索方联系，澄清是否需要采取行动。此外，出席大会和与作者积极接触能够促进相关方与 PSIRT 直接联系，便于未来开展研究。

目的：防止出现任何未经协调的披露感，或发现可能直接或间接影响到利益相

关者的产品而作者又尚未考虑的缺陷。

成果：在澄清利益攸关方的任何产品是否受到影响或提交报告时是否存在问题之前，有机会主动联系作者。

功能 2.2.3 关注知名漏洞搜索方的发布信息

关注那些曾在业界或针对特定公司产品和服务发布过相关信息的，或在这方面拥有广泛专业知识的漏洞探索方。他们的科学作品、博客或邮件联系人可能暗示了值得关注的潜在漏洞或弱点。

目的：维护关乎利益攸关方安全的专题科技与知识的状态。

成果：在解决产品安全问题时，支持利益攸关方化解常见威胁、弱点和制定可能对策的专业知识。

功能 2.2.4 关注大众媒体

大众媒体的报道通常先知先觉，尤其是在利益攸关方设施或人员遭遇灾难性事故的情况下。对大众媒体的追踪，有助于发现 PSIRT 的利益攸关方可能是哪些领域的重要或主要供应商。

目的：驳斥因产品漏洞导致事故的发生。

成果：更充分地为利益攸关方或媒体询问可能导致事故的产品漏洞做好准备。

服务 2.3 产品组件漏洞的监控

漏洞大致分为三类：(1)产品自身源代码存在漏洞，(2)供应商内部维护的产品组件存在漏洞，和(3)供应商外部（第三方）提供的组件存在漏洞。从产品的角度来看，(2)和(3)属于外部组件，但是这些组件中的漏洞会影响最终产品。虽然产品所有者只能间接控制底层问题的补救，但利益攸关方认为其对供应链和受影响产品的漏洞补救，拥有一定程度的所有权。当无法在不影响最终产品的情况下对易受攻击的组件进行独立补救时，情况尤甚。这其中包含的开放源代码组件亦被视为第三方组件。

目的：确认、收集和监控利益攸关方产品供应链中的漏洞，并向相关产品团队通报影响其产品的漏洞。

成果：更深入地了解如何及早确认从供应链继承且会给利益攸关方产品造成影响的漏洞。

功能 2.3.1 产品组件的库存

保存一份由外部和内部各方提供的，已纳入产品的供应商、产品及版本列表。这对快速确认受影响产品继承的漏洞至关重要。

目的：确认包含易受攻击组件的产品，这些产品可能导致产品本身产生漏洞。

成果：填妥所有产品的物料清单，用于搜索易受攻击的产品组件。

功能 2.3.2 关注第三方公告

通过订阅供应商公告或建立与供应商的特定沟通渠道，及时获取有关第三方组件漏洞的信息。订阅开放源代码项目的安全邮件列表。漏洞信息提供商可为此提供支持。

目的： 确定第三方组件中导致利益攸关方产品漏洞的缺陷。

成果： 可能在起草受影响产品外部报告之前启动漏洞处理流程。

功能 2.3.3 监控漏洞的情报来源

订阅第三方组件供应商公告的做法并非总能成功。当供应商不发布公告、停业或组件的开放源代码团体不积极时，可能无法获得相关信息。国家漏洞数据库（NVD）或商业情报等资源，有助于确认尚未通报的漏洞。

目的： 确认尚未通报的第三方组件漏洞。

成果： 更深入地了解可能被忽视的漏洞。

功能 2.3.4 引入供应商内部供应链漏洞的设置程序

供应商内部产品组件大多数情况下不会就已解决的安全问题向大众发布公告。为获得有关供应商内部供应链漏洞的信息，应与此类供应商建立特定的沟通渠道。

目的： 确认供应商内部供应链中导致利益攸关方产品漏洞的缺陷。

成果： 更深入地了解供应商内部供应链可能会被忽视的漏洞。

功能 2.3.5 通知内部开发团队

建立自动渠道，将已确认的第三方漏洞通知直接分发给受影响产品的开发团队。通常，遵循上游供应商的指示便足以解决下游产品的问题。根据优先策略，确定何时对漏洞进行分类并将其提交 PSIRT 处理。如果利益攸关方需要获得修补后的产品版本以确保操作安全，那么后者就显得尤其重要。

目的： 有选择地告知开发团队易受攻击的依赖关系和补丁信息(如有)，以便在下一产品版本中修复。

成果： 减少 PSIRT 手动处理漏洞的工作量，因为来自第三方的公告信息可以在开发过程中直接处理。

服务 2.4 确认新的漏洞

PSIRT 可以积极参与内部发现新漏洞的工作，借此机会来解决产品安全问题，从而减少管理对外关系的负担，并有可能减少整体协调的工作量。此类活动应作为 SDL 安全验证活动的补充。PSIRT 活动可能包括产品发布前或维护阶段的产品安全评估，以及向研发部门提供安全测试工具方面的专业知识。内部发现的影响最终用户的漏洞，应与外部发现的漏洞同等对待（包括评分和报告）并与修复的发布进行协调。

目的： 在外部人员发现之前检测并修复产品漏洞。

成果：获得发现内部产品漏洞的专业知识、程序和机制，并有可能减少协调的工作量。

功能 2.4.1 产品安全评估

产品安全评估是一种积极寻求发现当前未知漏洞的实践。这种实践可以使用渗透测试或漏洞扫描器等广泛的技术和工具。灰盒/黑盒安全评估技术模拟公司外部黑客攻击，是在攻击者对被攻击系统知之甚少或一无所知的情况下采用的方法。

目的：通过主动机制检测漏洞。

成果：为 SDL 安全核查活动提供补充的质量保证措施。

子功能 2.4.1.1 产品安全性评估

对产品安全控制提出质疑的安全评估分析结果，对希望在产品上市前或制定补救措施时改善产品状态的开发人员而言，会有很大的帮助。

子功能 2.4.1.2 第三方组件的安全评估

对于从第三方获得的组件，建议在一般采购管理程序的基础之上，增设专门的安全评估。这对于旨在确保高质量尽职调查的关键组件而言尤为必要。

功能 2.4.2 维护安全测试工具的专业知识

商业实体和相关团体都在不断开发新的安全分析和攻击工具。PSIRT 应不断更新有关可用工具的最新知识。这对于产品评估、验证外部漏洞搜索方的发现成果，或指导开发团队为其内部测试选择正确的工具非常有用。

目的：提供一个准备充分的专家团队，他们不仅具备处理复杂工具的技能，还可提供使用建议。

成果：利用现有的最佳工具。

子功能 2.4.2.1 对 PSIRT 工作人员进行安全测试工具培训

员工培训是保持现有安全测试工具最新知识不会落伍的关键因素。服务 6.3 安全验证更加详细地阐述了 PSIRT 员工培训的内容。

服务 2.5 漏洞搜索度量指标

图 8：漏洞搜索度量指标的流程

提供有关 PSIRT 数量、绩效或其它衡量结果的细节，让利益攸关方了解 PSIRT 的有效性（另见运作的基础第三节：评估和改进）。不同的利益攸关方都有各自独特的观点，必须使用不同形式的方式（或视图）加以处理。PSIRT 必须了解各利益攸关方团体希望如何使用这些信息。这些度量指标可以是 PSIRT 的关键绩效指标。

目的： 提供关于 PSIRT 衡量和绩效的数据。这有助于利益攸关方了解 PSIRT 在特定领域或提供服务方面的有效性。

成果： 通过审查 PSIRT 的度量标准，利益攸关方应当能够了解 PSIRT 提供服务的效率并能提供反馈，从而对服务交付做出调整。

功能 2.5.1 运作报告

运作报告提供了所发现漏洞数量以及类型的信息。这些报告可以在 PSIRT 内部定期发布，也可以与内部利益相关方一起发布。

目的： 定期收集用于普通报告的数据。

成果： 确定需要分析、资源和改进的领域。

子功能 2.5.1.1 发现漏洞的总数与确认漏洞的总数

这些数据有助于从资源角度收集 PSIRT 处理的总量。这些数据可按业务单元级别、产品类型或特定产品加以细分。

子功能 2.5.1.2 按第三方组件细分的已确认漏洞总数

这些数据有助于收集与嵌入式特定第三方组件相关的风险。

子功能 2.5.1.3 按 CWE 细分的已确认漏洞总数

这些数据可以反馈到安全开发周期的上游，并对培训和教育造成影响。这些数据可按业务单位级别、产品类型或特定产品细分。

子功能 2.5.1.4 按漏洞发现方法细分的已发现漏洞总数

此数据有助于识别容易发现的漏洞，并可以将其反馈到安全开发周期的上游。这些数据可按业务单元级别、产品类型或特定产品加以细分。

子功能 2.5.1.5 按来源细分的已发现漏洞总数

此数据有助于描述 PSIRT 的知名度。

功能 2.5.2 业务报告

业务报告提供了组织漏洞响应状况的信息，其内容与处理和响应安全漏洞相关。

目的： 为衡量组织对成功的定义建立度量标准，并定期收集数据，用于编制旨在确认风险的管理报告。

成果： 突出介绍成功案例和改进机遇的展示板。

子功能 2.5.2.1 准时回应率

此数据记录了 PSIRT 在各自 SLA 时间框架内，对漏洞报告做出初始响应的及时程度。

子功能 2.5.2.2 PSIRT 沟通渠道的总停用时间

此数据捕获的信息是关于 PSIRT 交通渠道的可用程度是否达到了 SLA 规定的水平。

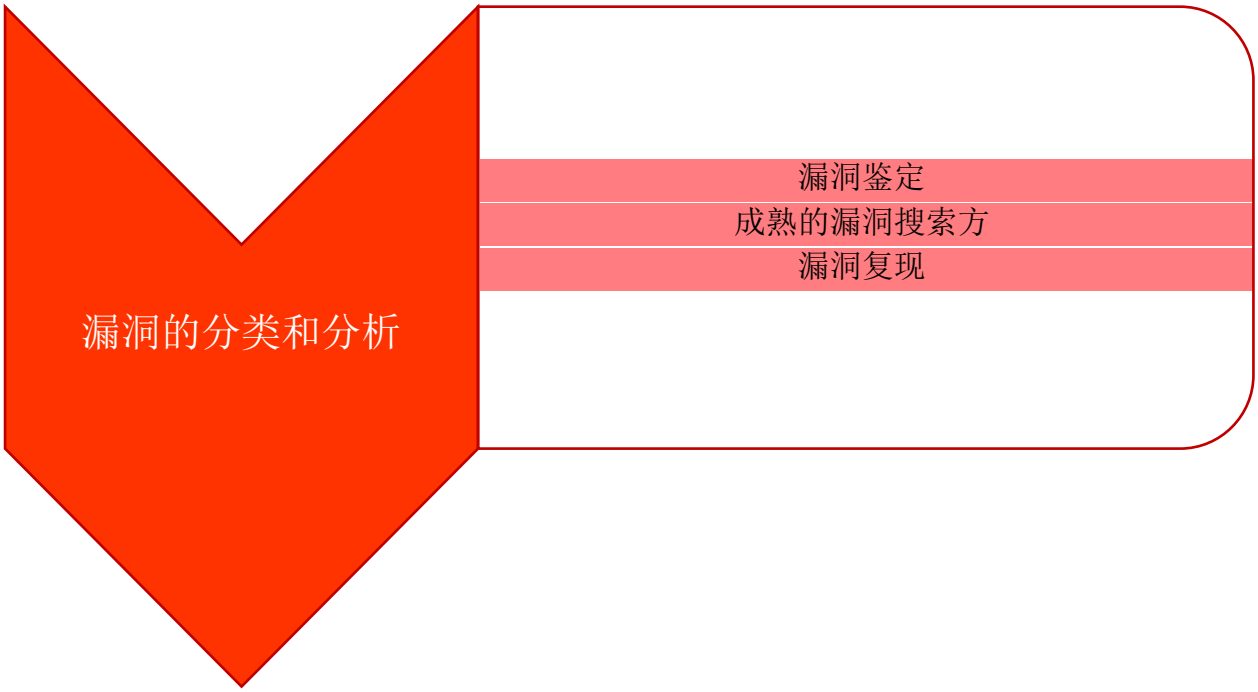
子功能 2.5.2.3 分类所需时间

此功能衡量了从接收到初始报告至分类活动完成的时间。该数据记录了 PSIRT 员工的表现和/或工作量。

子功能 2.5.2.4 完全披露的数量、在野（in the Wild）利用的漏洞以及通过媒体发现的漏洞

此数据捕获了利益攸关方产品的风险。

服务领域 3 漏洞的分类和分析



PSIRT 的案例管理功能由漏洞接收和分类构成。尽管 PSIRT 内部的操作顺序非常相似，但也存在差异，例如创建‘案例’的确切时间点或是案例中执行不同功能的人员。当组织收到大量漏洞报告时，可能会考虑在创建案例之前，通过初始分类对报告加以验证。相比之下，漏洞报告量较低的组织可能会在分类之前创建案例。PSIRT 的最终目标是建立一个高效、明确的流程。

目的： 定义如何对漏洞报告进行分类。

成果： 建立跨 PSIRT 和相关工程团队的流程。

服务 3.1 漏洞鉴定

组织就有意解决问题的类型和范围定义适当了的鉴定标准。这种鉴定标准将有助于设置安全基线，同时对接收的漏洞报告进行有效分类。

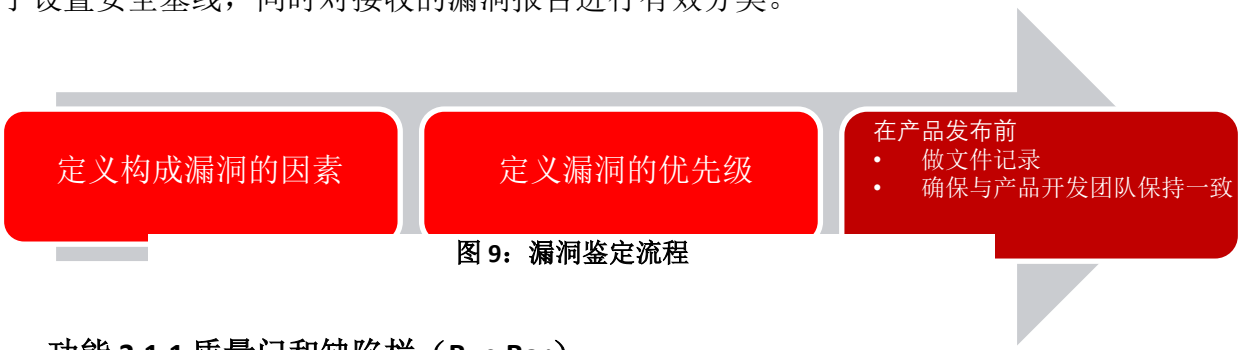


图 9：漏洞鉴定流程

功能 3.1.1 质量门和缺陷栏（Bug Bar）

共同漏洞评分系统（CVSS）则为捕捉漏洞的主要特性提供了一种方法，通过评分的方式反映其严重性。接下来，将对分数进行定性分类（例如，低、中、高、严重），帮助组织合理评估其漏洞管理流程，排定轻重缓急。有时我们称

之为质量门和/或缺陷栏，用于建立可接受的最低安全质量水准并确定安全漏洞的优先级标准。在产品发布之前定义这些标准，为漏洞处理流程提供了透明度，其采用的方式是预先确定 PSIRT 会将哪些产品漏洞认定为应加以补救的产品漏洞。常见漏洞和暴露（CVE）使用的条目列表带有标识号、说明和至少一条公共参考，经常用于明确正在解决哪一问题。

目的： 明确定义最低标准和优先标准，为内外部利益相关方提供透明度。

成果： 向工程师和漏洞搜索方提供关于漏洞构成的明确预期。更多的优先级划分标准，将减少漏洞寿命周期管理中的混乱与争议—无论采用初始分类还是发送补丁的方式。

子功能 3.1.1.1 记录产品安全漏洞的定义

质量门或缺陷栏应记录在案，集中保存并作为开发人员/工程师标准培训的一部分。

子功能 3.1.1.2 与产品开发团队合作

在组织内有多个产品和产品开发团队的情况下，让所有产品开发团队都参与产品安全漏洞定义的标准化工作至关重要。

功能 3.1.2 持续改进

成熟的 PSIRT 应采用持续改进的思维方式，酌情修改其鉴定标准，使之能够体现以往的经验、行业最佳实践、产品的变化和利益攸关方的反馈。向内外部利益攸关方通报发生的变化从而实现期望管理是关键的一环。

目的： 认识到鉴定标准可能会修订。PSIRT 的动态变化，如利益攸关方的期望、行业趋势或将来漏洞的数量，可能会导致频繁调整。

成果： 不断变化的漏洞鉴定标准将催生出有效的漏洞鉴定实践。

子功能 3.1.2.1 收集数据

收集分类过程中的数据，包括收到报告的数量、有多少可判定为漏洞、多少无法判定为漏洞以及是否出现了任何差异。

目的： 在数据的基础上推动改进。

成果： 对质量门和缺陷栏的改进是由数据驱动的。

服务 3.2 成熟的漏洞搜索方

随着组织的 PSIRT 逐渐成熟，相关团队可能会发现存在一群习惯致力于此的漏洞搜索方，负责报告超出正常数量的漏洞。我们建议应在考虑到漏洞搜索方的信誉及其高质量史的前提下，跳过资格鉴定和分类等功能，直接进入根本原因分析和补救措施的开发。这或许有助于提高流程效率，培育与漏洞搜索方的关系。

目的： 了解研究团体和最积极的产品和服务漏洞报告人，同时考虑立即上报由

高度可信的漏洞搜索方提交的报告。

成果：缩短高水平漏洞搜索方的响应时间。

功能 3.2.1 漏洞搜索方数据库

开发并维护曾报告过漏洞的个人和组织的数据库，以便对该漏洞搜索方的搜索历史、搜索结果和处理任何其它案例需考虑的事项进行跟踪。

目的：提高分类流程的效率，并与有高质量提交记录的漏洞搜索方建立更好的关系。

成果：有资质漏洞搜索方的报告在系统中处理速度更快。漏洞搜索方对结果感到满意，并在任何可能的公开披露时间之前完成补救。

功能 3.2.2 加速处理成熟漏洞搜索方提交的报告

在发现和上报产品或服务中的软件缺陷时，有些漏洞搜索方不仅高产且具有一致性（经过审查/可信）。例如，他们可能使用定制的模糊化工具，并在没有具体写明或证明概念的情况下上报崩溃信息。如果您已熟知这些漏洞搜索方，且能确定他们报告的大多数问题都将得到解决，那么可以考虑跳过资格鉴定/审查过程，直接进行补救。

目的：提高分类流程的效率，并与有高质量提交记录的漏洞搜索方建立更好的关系。

成果：有资质漏洞搜索方的报告在系统中处理速度更快。漏洞搜索方对结果感到满意，并在任何可能的公开披露时间之前完成补救。

功能 3.2.3 漏洞搜索方的特征

用户应考虑构建漏洞搜索方特征，以便告知处理者如何最好地与漏洞搜索方合作。特征信息可能包含地理位置、语言、出席的会议、发现漏洞的方法、漏洞搜索方通常关注的产品/技术、漏洞搜索方是否与相关方协调漏洞披露事宜、漏洞搜索方是否乐于在大会上展示他们的发现、您是否向漏洞搜索方支付奖金或您是否为他们提供了其它激励等内容。咨询法律和/或合规团队，以确定可以收集哪些信息以及这些信息可以保留多长时间。

目的：了解发现您产品漏洞的人。

成果：可为特定的漏洞搜索方量身定制处理方式，以获得最积极的结果。

功能 3.2.4 定义漏洞搜索方报告的质量

组织可能需要考虑定义并发布有关质量漏洞报告质量下限的导则，为漏洞搜索方提供有关快速评估报告所需信息类型方面的指导。基线内容可能包括但不限于编写报告、复现步骤、测试平台和概念证明。

目的： 为漏洞搜索方提供有关质量漏洞报告的基线指导。

成果： 供应商和漏洞搜索方之间的来回切换得以最小化，且供应商可迅速专注于修复计划。

服务 3.3 漏洞复现

除资格鉴定之外，若非另有规定，PSIRT 需确保漏洞搜索方的报告具有可复现性，以验证并了理解产生易受攻击状态的条件。

目的： 为鉴定漏洞报告提供工具和环境。

成果： 高效、安全、有保障的漏洞报告验证。

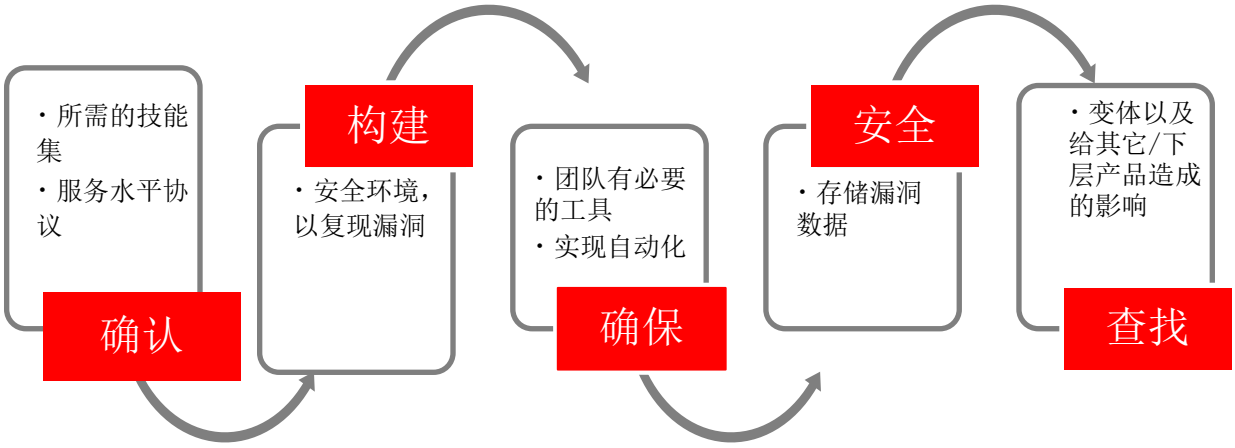


图 10：漏洞验证/复现流程

功能 3.3.1 为漏洞复现起草服务水平协议

PSIRT 可能并不充分具备重现所有收到漏洞的专业技术水平。PSIRT 可能需要咨询、与产品开发团队或其它团队合作或依赖他们的专业知识，因此至关重要是制定清晰统一且明确界定的协议，确保所需专业知识随时可供调用。在理想的情况下，我们建议使用专门从事此行业的全职或兼职资源。但是，如果因预算限制而无法做到这一点，那么至少应预先确定参与 PSIRT 流程的主题专家，请他们在接到事故通知后迅速提供短期服务。

目的： 认识到 PSIRT 不具备重现所有已发现漏洞的技术专长。

成果： 事先开展内部协调将确保专业知识随时可用于帮助复现漏洞。

功能 3.3.2 复现测试环境

应为 PSIRT 或专门的团队建立一个专项测试环境，用以复现漏洞。测试环境应当隔离，以避免恶意活动和验证漏洞搜索方的报告。可酌情使用专门的网络环境、模拟或虚拟化手段来创建安全环境。

目的： 为检查和复现漏洞创建一个安全环境。

成果： 部署良好的复现测试环境有助于漏洞的有效处理和鉴定，并可将漏洞限制在测试环境范围内。

功能 3.3.3 复现工具

参与复现上报漏洞的团队为执行这些操作（例如调试器），需要拥有相应的工具和更新后的产品许可证。

目的： 确保复现团队拥有所需的工具。

成果： 确保尽可能高效地复现报告漏洞。

功能 3.3.4 漏洞的存储

建议安全存储漏洞报告、概念证明文件等敏感信息，并且仅为那些需要访问者赋予访问权限，同时确保静态和传输中的信息安全。示例请参见 ISO 27001。

目的： 确保敏感和可能具有破坏性的漏洞信息的安全。

成果： 通过控制访问权限保证敏感信息的安全，且不容易遭受组织主要网络的威胁。

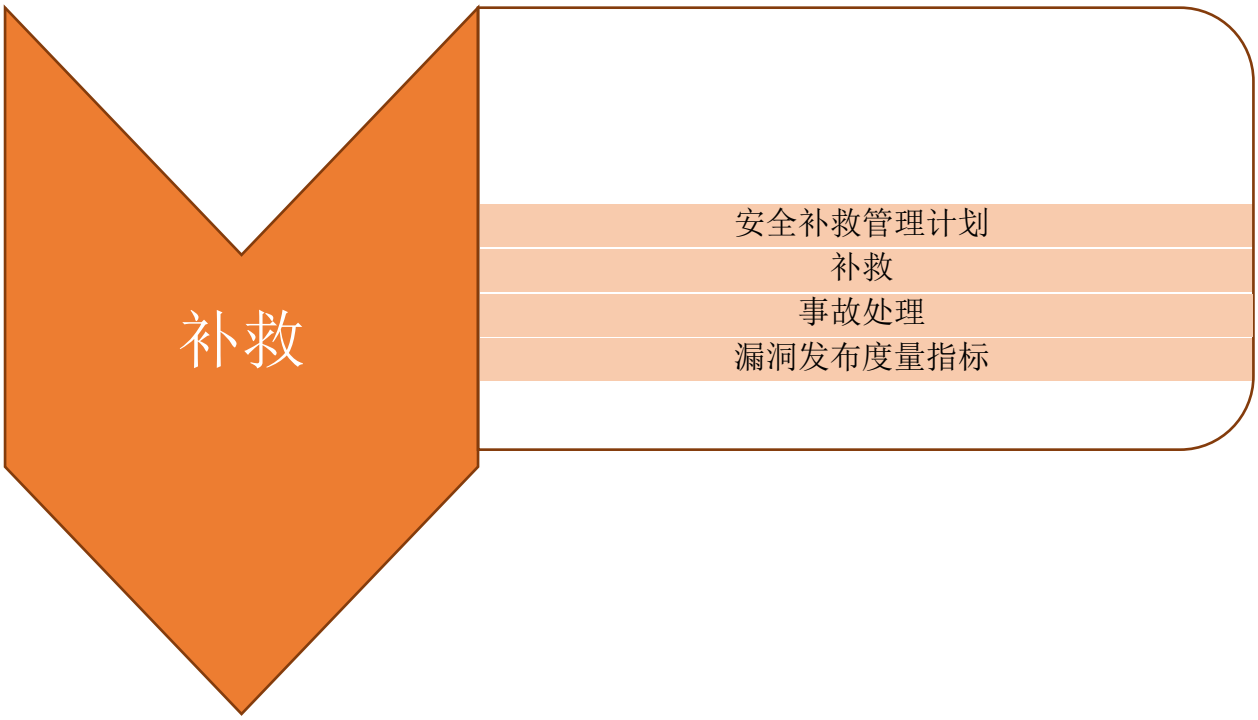
功能 3.3.5 受影响的产品

在复现过程中，开展分析的团队应确定哪些产品受到影响，以及是否存在漏洞的任何变体。另请参见产品寿命周期管理第 4.1.1 节。

目的： 全面了解跨产品的漏洞及其范围。

成果： 在支持的产品中，该漏洞的修复方法很全面。

服务领域 4



此服务领域是针对向利益攸关方和下游供应商交付和宣布补救措施所需的不同服务。补救交付机制应根据漏洞遭利用时对利益攸关方的影响来确定。应建立流程，以确保按可预测的时间表交付补救措施，让利益攸关方和下游供应商能够相应对这些补救措施的测试和部署做出规划。

目的： 强调向利益攸关方和下游供应商发布和宣布补救措施所需的流程和机制。

成果： 使利益攸关方和下游供应商能就采取补救措施做出相应规划。

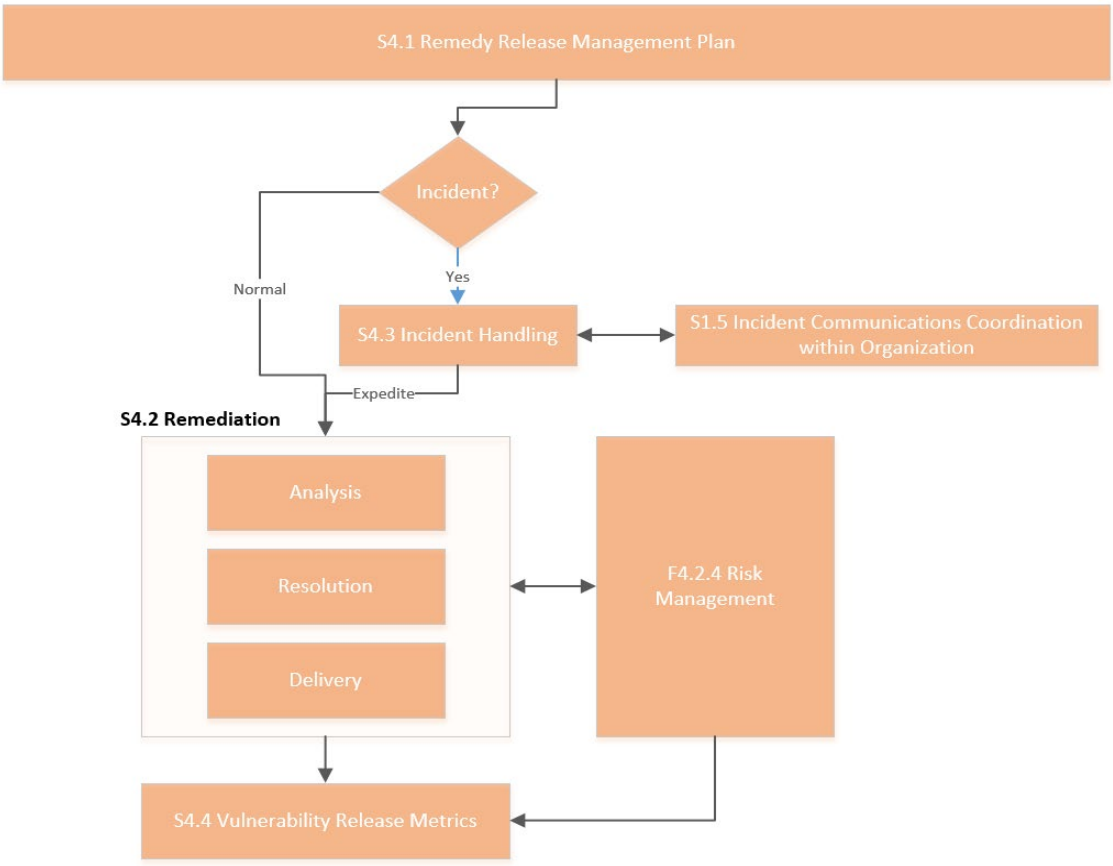


图 11：核心补救措施发布流程示例

图中文字：

S4.1 发布补救措施的管理计划　事故　发生　正常　S4.3 事故处理

S1.5 组织内部的事故沟通协调　加速　S4.2 补救　分析　解决　交付

F4.2.4 风险管理　S4.4 漏洞发布度量指标

服务 4.1 发布补救措施的管理计划

此服务侧重于就供应商如何为其支持的上市产品版本，规定补救措施的发布节奏提供指导。利益攸关方，尤其是企业领域的利益攸关方，需要规划补救措施的部署。有些部署（如云部署），可能会自动更新或制定不同的补丁管理策略。

目的：就哪些产品将得到支持、提供补救措施的机制以及交付产品的节奏，开展服务对象教育。

成果：利益攸关方将能够提前规划安全修复的部署。

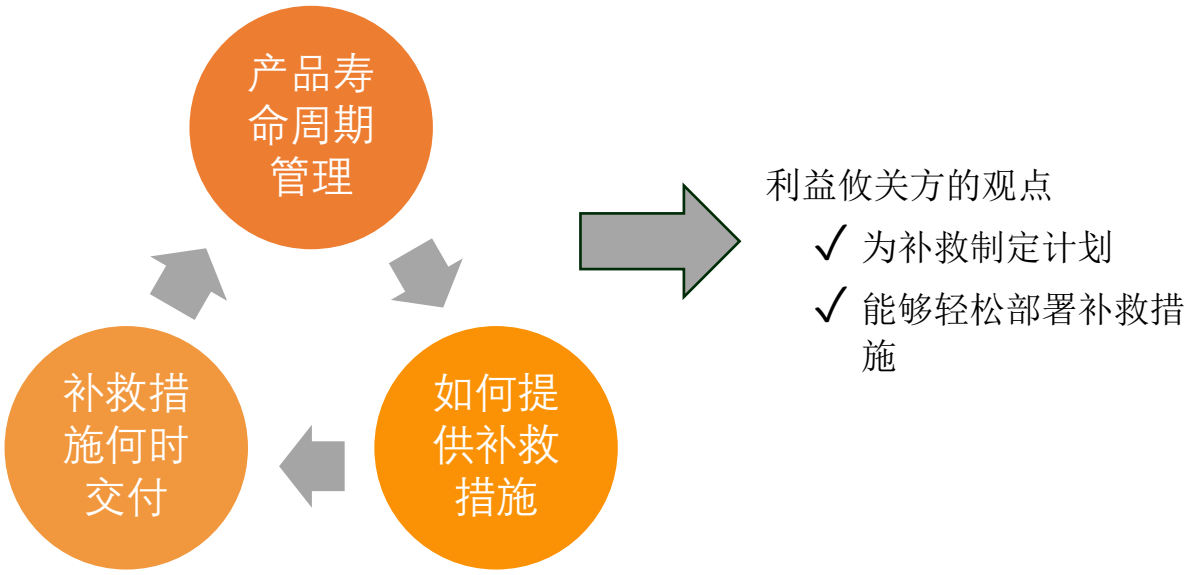


图 12：奠定一致性的基础

功能 4.1.1 产品寿命周期管理

公司可能制定了与利益攸关方不同的支持政策和协议。基于这些因素，PSIRT 可以与业务部门/业务线以及为利益攸关方提供支持的部门合作，确定这些部门将如何以及是否支持超出其支持范围或支持义务的产品。具体情况可能取决于漏洞的严重性，且可能涉及业务部门/业务线和利益攸关方支持部门的输入意见。

目的： 为产品团队提供一个清晰的策略，说明组织将如何支持存在安全漏洞的产品。

成果： 关于业务部门/业务线预计将为这些类产品提供哪些补救措施的明确政策。

子功能 4.1.1.1 产品库存

为所有投放市场的产品建立产品库存，以确保对所有受支持的适用产品做出评估并提供补救。

子功能 4.1.1.2 支持模式

了解不同类型的产品支持模式，包括付费服务、延长保修、维护协议或与特定利益攸关方签署合同。

子功能 4.1.1.3 产品寿命周期

确定产品在寿命周期的哪个阶段后不再获得支持。

功能 4.1.2 交付方式

PSIRT 可以与产品团队和利益攸关方支持部门合作，共同确定向利益攸关方提供补救措施的不同选项。此外还应制定标准，以确定何时通过确定的手段实施补救措施。

目的： 维护一个统一的机制，根据一系列条件针对漏洞提供补救。

成果： 利益攸关方可以规划并轻松部署补救措施。

子功能 4.1.2.1 产品的包装形式

了解与交付补救措施相关的不同包装形式（例如，二进制可执行文件、源代码差异等）。

子功能 4.1.2.2 交付补救措施

了解提供补救措施的不同机制，如热修复、补丁、版本维护、固件更新以及如何分发补救措施。

子功能 4.1.2.3 部署补救措施

确定不同产品如何部署补救措施，即远程部署、客户安装、自动更新或现场部署。

功能 4.1.3 交付的节奏

利益攸关方和下游供应商需要制定补救措施计划，以保持环境的安全态势。通过设定何时交付补救措施的节奏，使利益攸关方能够为环境的必要更新做出安排并规划资源。

目的： 在向利益攸关方发布补救措施时保持一贯的节奏。

成果： 利益攸关方可以规划并部署补救措施。

子功能 4.1.3.1 补救交付的节奏

与产品管理团队和发布管理人员合作，确定应何时交付补救措施。有些补救措施将与功能同时发布，并将与这些发布时间表保持同步。而其补救可能需要紧急修复，因而属于紧急补丁。

子功能 4.1.3.2 记录例外情况

确认并记录无法通过正常节奏提供补救措施的例外情况。

服务 4.2 补救

此服务与漏洞搜索方对报告漏洞的管理相关，其内容包括进行响应分析和提供缓解措施，定义为哪些版本提供补救，且有可能要考虑如何提供补救措施。此外，这一服务亦可能考虑利益攸关方在交付补救措施之前，可以马上应用的一切变通办法。

目的： 根据受影响的产品、版本和利益攸关方，给出向相应利益攸关方提供补救措施的流程和最佳实践。

成果： 与受影响产品和利益攸关方需求相适应的补救措施。

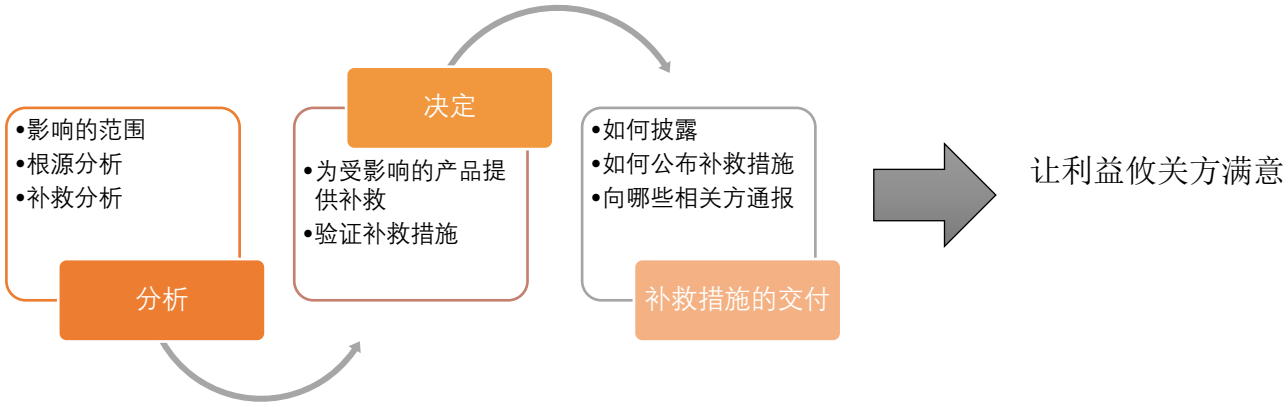


图 13：已上报漏洞的补救流程

功能 4.2.1 分析

受影响的产品可能包括单个软件应用程序、固件或有不同软件或固件版本的多个硬件程序。制定补救计划时需要考虑许多参数，以确保利益攸关方的需求得到满足。

目的： 确定受影响的产品、版本和利益攸关方。

成果： 与受影响产品和利益攸关方需求相适应的补救措施。

子功能 4.2.1.1 验证漏洞

根据质量门或缺陷栏，验证漏洞报告或事故。参见功能 3.1.1 质量门和缺陷栏。

子功能 4.2.1.2 产品版本的补救

确定受影响的产品和版本以及可能需要同时加以补救的任何变体。

子功能 4.2.1.3 审查支持协议

审查与受影响产品版本相关的支持协议和模型。参见子功能 4.1.1.2 支持模

型。

子功能 4.2.1.4 根源分析

了解导致该漏洞的设计缺陷或实施缺陷。

子功能 4.2.1.5 确定拒绝产生漏洞的机制

例如，造成漏洞的原因可能是误报或安全设计缺陷。

子功能 4.2.1.6 补救分析

确定减轻或补救漏洞所造成风险的方法。

子功能 4.2.1.7 变通性的补救措施

在开发补救措施时，确定是否有任何可以实施的变通方法可以减轻漏洞造成的伤害。

子功能 4.2.1.8 例外

确定漏洞无法补救的所有例外情况。参考功能 4.2.4 风险管理流程。

功能 4.2.2 做出进行补救的决定

在发布针对报告漏洞的补救措施之前，应通过质量保证（QA）、安全测试并由上报漏洞的搜索方（如果适用）进行验证。这些内容描述了内部验证补救措施以及与漏洞搜索方合作，验证并认可补救措施的流程和机制。

目的： 为内部验证补救措施提供流程和机制，并与漏洞搜索方共同认可补救措施(如果适用)。

成果： 内部和/或外部漏洞搜索方批准即将发布的补救措施。

子功能 4.2.2.1 验证已修复的上报漏洞

通过验证确保上报漏洞的所有实例在各受影响的产品版本中均得到了补救。

子功能 4.2.2.3 批准补救措施

补救措施获得质量保证工程师或工程师团队的批准。应将补救措施验证融入标准测试/质量保证实践。

子功能 4.2.2.4 与漏洞搜索方共同验证补救措施

与第三方漏洞搜索人或利益攸关方合作，验证补救措施。

功能 4.2.3 补救的交付

作为发布针对上报漏洞提出的补救措施的一部分，披露的时间框架可能会因组织业务需求而异。例如，有些披露可能与补救措施就绪的时间一致，而另一些则可能会在发布补救措施后披露，特别是在补救措施已经实施的情况下，还有一些披露可能会根据与利益攸关方的关系（例如合作伙伴或关键实体）而得到

优先考虑。无论如何，包括漏洞搜索方在内的整个行业的核心利益攸关方，都需要随时了解该时间框架。

目的：根据补救措施做出披露规划，并随时向利益攸关方通报这些时间框架。

成果：向利益攸关方披露的同时提供补救措施。

子功能 4.2.3.1 披露类型

确定披露漏洞的首选机制。该机制可能基于漏洞的严重性或类型。

子功能 4.2.3.2 协调披露（如果适用）。

子功能 4.2.3.3 在内部数据库发布补救措施

与利益攸关方的支持部门或其它利益攸关方合作，将补救措施作为示例发布到门户网站、利益相关方支持部门的网站或发布到制造（RTM）的网站。

子功能 4.2.3.4 披露补救措施

与利益攸关方支持部门或利益攸关方合作，披露上报的漏洞。

功能 4.2.4 风险管理流程

PSIRT 有责任向利益攸关方提供足够的信息，以便他们能够评估因系统和 PSIRT 组织所支持产品中的漏洞给系统带来的风险。当漏洞未在特定时间范围（根据服务水平协议或目标）内得到补救时，应对整个组织进行风险管理评估。这方面的工作包括为量化风险建立一个透明的机制，并将风险上报给组织风险登记簿所载的相应利益攸关方。

目的：为在内部服务水平协议规定的时间内未得到补救的任何漏洞，定义正式的风险接受流程。

成果：实现整个组织的风险透明，并保证风险得到适当的上报和确认。

子功能 4.2.4.1 权威职能

确定哪些职能的负责人有权接受风险，例如首席信息安全官（CISO）/首席安全官（CSO）或风险管理员，以及应将风险通报给哪些职能部门。

子功能 4.2.4.2 定义风险管理流程

定义组织内处理和应对风险的风险管理实践，包括确定触发流程的一系列条件。

子功能 4.2.4.3 评估和量化风险

开展风险评估工作以对风险做出评估和量化，从而了解风险给业务造成的威胁和影响。

子功能 4.2.4.4 在风险登记簿中记录风险

协助 CSO、风险管理员或其它利益攸关方跟踪风险评估的状态，并随后实施

建议。

子功能 4.2.4.5 建议

根据调查结果和建议，更新风险登记簿。

服务 4.3 事故处理

PSIRT 需要设立一种机制来缩短补救所需时间，以消除“重大”漏洞，这些漏洞可以是主动的在野漏洞利用、零日公开披露和未经协调的公开披露。此项服务为事故提供指导并向利益攸关方发出提醒，协调与事故响应、缓解和恢复相关的活动，以缩短从报告到提供补救措施所需的时间。

目的： 为管理重大漏洞制定一项计划并发展相应的能力，调动解决这些问题所需的一切资源。

成果： 针对未解决的漏洞、漏洞的公开披露或利益攸关方可能存在风险且需要快速行动的其它情况，提供紧急修复。

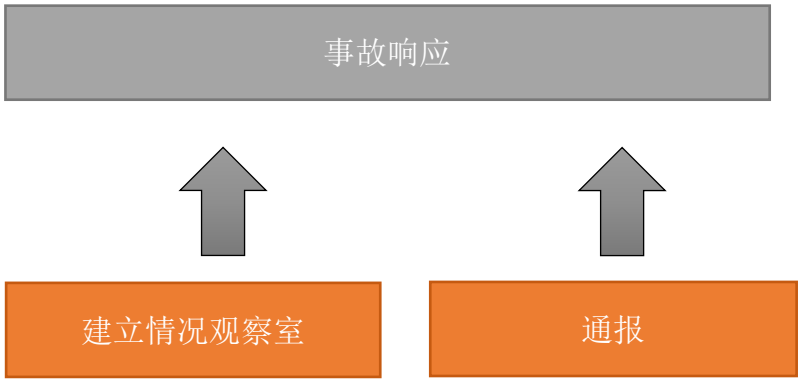


图 14：事故处理

功能 4.3.1 建立情况观察室

针对事故管理，应建立一个由 PSIRT、法律部门、沟通部门、开发部门、利益攸关方支持部门、供应商和其它必要职能部门组成的情况观察室。观察室既可以是一个实体，也可以是虚拟单位，其目标是各方均能以安全方式按需做出响应。通常，对确保利益攸关方的参与而言，实体和远程参加选项都有存在的必要。应提前确定资源，以便为事故管理流程提供充分的支持。

目的： 确保利益攸关方能够回答问题并提供指导。确保为管理事故分配适当资源。

成果： 组织协调已审查的资源。

子功能 4.3.1.1 事故管理计划

为管理重大漏洞制定一项计划并发展相应的能力，调动解决这些问题所需的一切资源。重要的是做好事故响应准备，以验证该计划处理意外事件和紧急

情况的就绪水平。

子功能 4.3.1.2 确定处理和管理事故所需的资源

这些资源可能包括会议室、专用线路和额外的人力。对于长期事故的处理，应考虑食宿问题。

子功能 4.3.1.3 请利益攸关方参与事故响应计划

作为事故响应计划的一部分，确定所有需要参与处理事故的关键利益攸关方。参见服务 1.1 内部利益攸关方管理 和 服务 1.5 事故通报。

子功能 4.3.1.4 为事故管理分配明确的职能与职责

当需要做出响应时，相关人员必须知道他们的职责和操作程序。应开展培训和桌面练习，使关键的响应参与方做好准备工作。

功能 4.3.2 事故管理

发布事故通报时，PSIRT 与其利益攸关方合作的重点是降低事故的影响，并努力恢复产品及其利益攸关方的业务功能。

目的： 为控制事故编制行动手册并执行相关计划。

成果： 尽快恢复产品团队和利益攸关方的运作。

子功能 4.3.2.1 信息收集

接收、编目和存储相关事故信息。

子功能 4.3.2.2 分析

事故处理取决于分析活动，分析活动的规定见“分析”一节。

子功能 4.3.2.3 响应

与减少事故影响以及努力恢复顾客内部业务功能有关的服务。

子功能 4.3.2.4 事故跟踪

记录关于为解决事故所采取行动的信息，包括收集的关键信息、开展的分析、采取的纠正和减轻措施、终止操作以及相应的决定。

子功能 4.3.2.5 事故后续处理流程

通过回顾确认如何对过程、策略、程序、资源和工具加以改进，有助于减轻和防止将来出现的危害。

功能 4.3.3 沟通计划

所有利益攸关方和行动负责人都必须了解最新计划和进展，以保持与时俱进。根据需要请管理层参与进来，打破任何可能阻碍事故期间开放、协作沟通的障碍。

目的： 制定一个沟通计划，并为事故指定一个核心联络人，让人人都了解最新

发展状况。

成果： 组织协调已经过审查的沟通。

子功能 4.3.3.1 向内部利益攸关方发布信息

管理用于分发通知、警报、数据订阅和其它情况感知发布的列表。

子功能 4.3.3.2 公共关系得到很好的管理和协调

确保将信息传递给媒体和利益攸关方，但只能通过授权的组织渠道传播。这其中包括通过社交媒体帖传播。

子功能 4.3.3.3 恢复活动

将恢复活动的信息传达给内部利益攸关方、高管和管理团队。

子功能 4.3.3.4 收集事故后的反馈

事故后的简报由 PSIRT 负责，通过收集反馈改进事故响应以及安全开发库（SDL）的活动（例如，哪些 SDL 活动可以或应该在问题出现之始便阻止其发展？）。

服务 4.4 漏洞发布的度量指标

要收集的数据应包括但不限于问题的数量、分类、解决的时间、受影响的产品或服务。

目的： 为管理报告定期收集数据。

成果： 确定需要分析、资源、改进的领域。

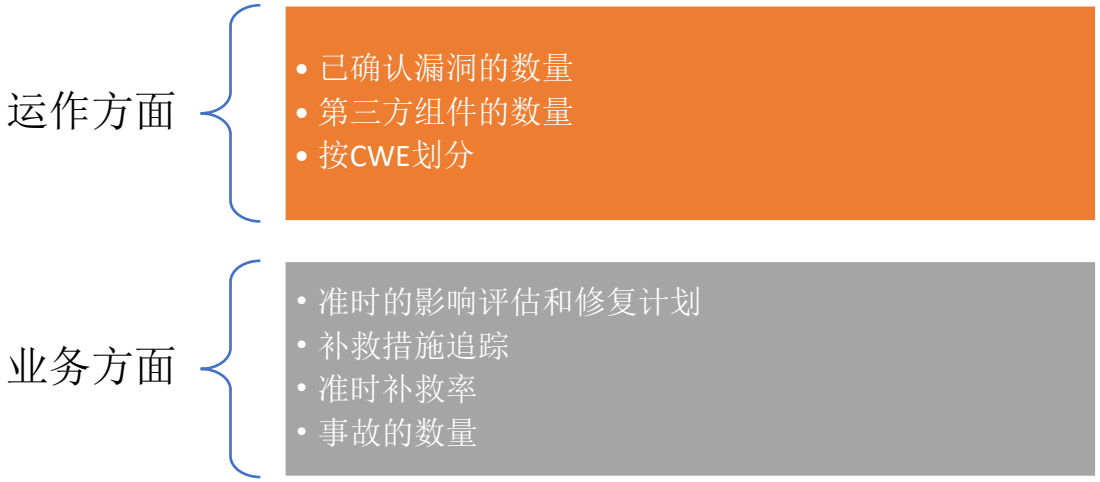


图 15：运作和业务度量指标

功能 4.4.1 运作报告

运作报告提供不同产品和版本上报并确认的漏洞数量和类型信息。这些报告应定期在 PSIRT 内部与内部利益攸关方一起发布。

目的： 定期收集用于普通报告的数据。

成果：确定需要分析、资源和改进的领域。

子功能 4.4.1.1 发现漏洞总数与确认漏洞总数（按产品/业务单位划分）

这些数据有助于从资源角度收集 PSIRT 处理的总量。

子功能 4.4.1.2 按第三方组件细分的已确认漏洞总数

这些数据有助于收集与嵌入式特定第三方组件相关的风险。

子功能 4.4.1.3 按 CWE 细分的已确认漏洞总数（按产品/业务单位划分）

这些数据可以反馈到安全开发周期的上游，并对培训和教育造成影响。

功能 4.4.2 业务报告

业务报告提供了有关某组织漏洞响应能力的健康状况信息。

目的：针对组织按时满足 SLA 中承诺的成功率建立衡量指标。定期收集、分析和传播衡量这些目标实现程度的数据。

成果：创建重点介绍成功案例和改进机遇的展示板。

子功能 4.4.2.1 实施影响评估的准时性

本度量指标反映了产品团队在各自的影响评估 SLA 时间框架内完成影响评估的情况。

子功能 4.4.2.2 修复计划的及时性

本度量指标反映了产品团队在特定 SLA 中提供修复计划的表现。

子功能 4.4.2.3 补救跟踪

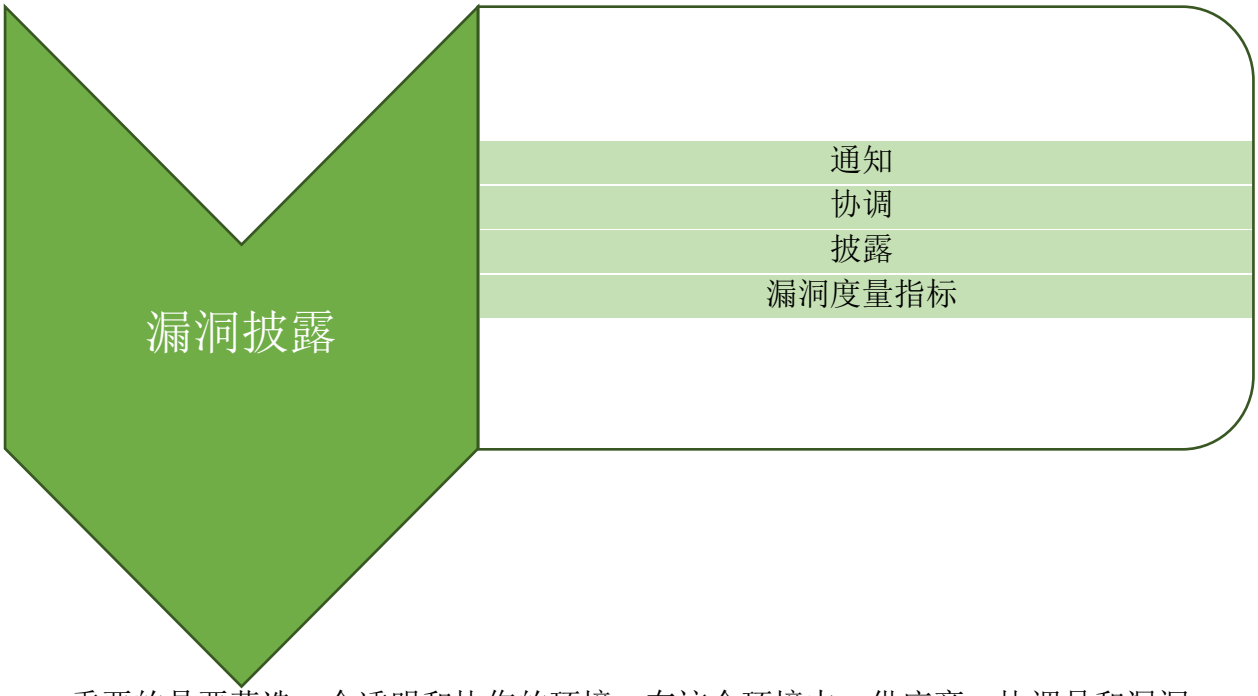
本度量指标反映了产品团队在特定 SLA 时间框架内进行修复的表现。

子功能 4.4.2.4 及时补救率

本度量指标反映了从报告到交付修复的整个过程中，产品团队在实现总体修复目标或满足协议方面的表现。表现可按严重性或漏洞类型（产品线、漏洞类型）细分。

子功能 4.4.2.5 事故的数量

此数据的收集组织所面临的风险。



重要的是要营造一个透明和协作的环境，在这个环境中，供应商、协调员和漏洞搜索方可以与利益攸关方和彼此分享信息，协商共同认可的披露计划。通过以这种方式合作，可以满足消除漏洞、保护利益攸关方和确认漏洞搜索方等需求。供应商应公布漏洞披露政策，以供协调员、其它供应商以及漏洞搜索方参考。

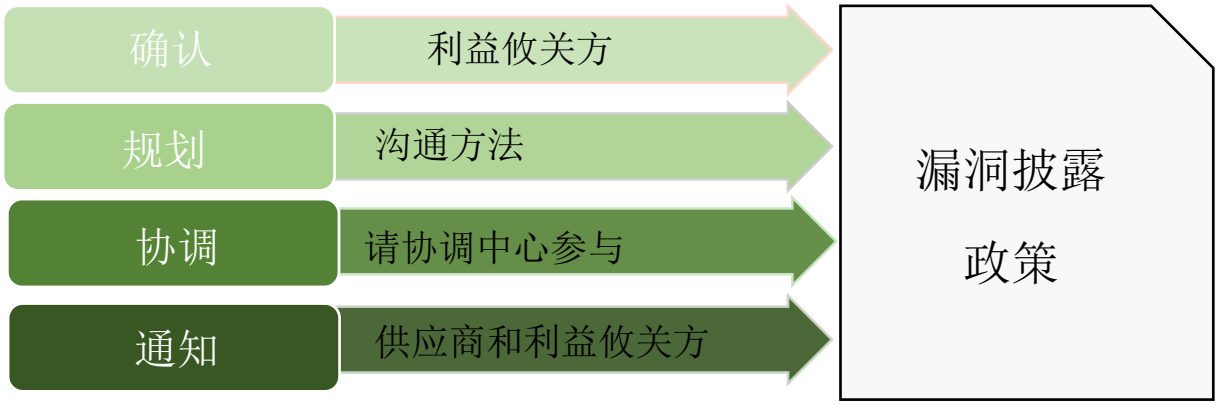


图 16：漏洞通知流程

目的： 与漏洞搜索方、协调员及下游供应商合作，实现对利益攸关方及合作伙伴的透明，负责任地披露漏洞并进行修复。

成果： 加强信任、合作和对披露的控制。

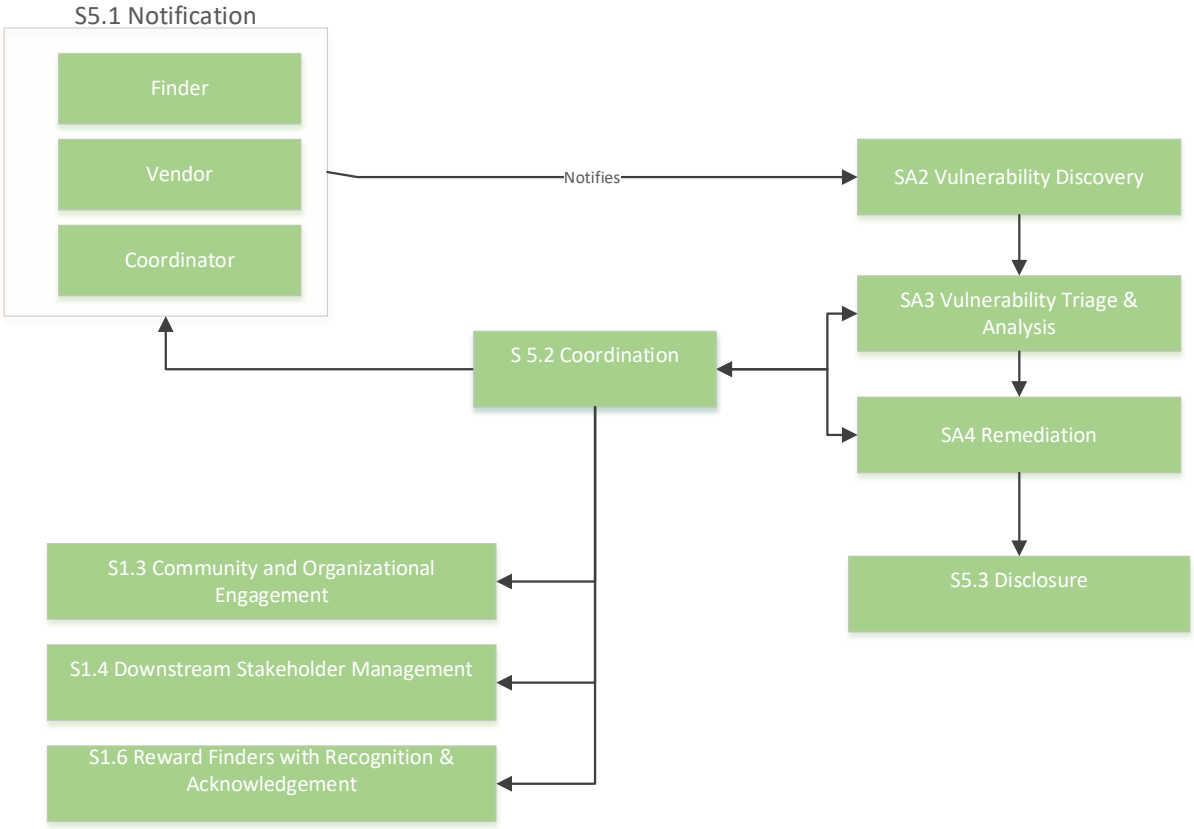


图 17：高层漏洞协调的示例

图中文字：

S5.1 通知　　漏洞搜索方　　供应商　　协调员　　通知　　SA2 发现漏洞

SA3 漏洞分别和分析　　SA4 补救　　S5.2 协调　　S5.3 披露

S1.3 相关团体和组织的参与　　S1.4 下游利益攸关方管理　　S1.6 以表彰和认可的方式奖励漏洞搜索方

服务 5.1 通知

此项服务通过确定适当的通知流程，及时向利益攸关方提供关于缓解策略、补救措施和变通办法的信息，从而让他们了解情况并据此进行规划。在某些情况下，供应商之间可能存在合同协议，例如，上游供应商需要向下游供应商通报已披露的漏洞或已知事故。通知流程旨在确保所有利益攸关方和供应商能够了解并管理漏洞带来的风险。

目的： 通过协作为供应商和漏洞搜索方提供透明度。

成果： 加强与漏洞搜索方间的信任与协作。

功能 5.1.1 中间供应商（下游供应商）

中间供应商（如原始设备制造商或合作伙伴）可以开发和/或生产用于另一个供应商最终产品的零件、子系统或软件。在这种情况下，其 PSIRT 应安排与这些供应商共享漏洞信息。PSIRT 应该了解不同供应商的漏洞处理策略。有时这些期

望会写入合同协议。应尽快协商补救和披露的时间表。

目的： 在原始设备制造商、合作伙伴和其他供应商之间打造一个协作且预期明确的环境。

成果： 加强各相关方对披露的信任、协作和控制。

子功能 5.1.1.1 PSIRT 向中间供应商报告

PSIRT 可能了解其利益相关方上报的漏洞，并应将这些漏洞通知中间供应商的 PSIRT。

子功能 5.1.1.2 中间供应商报告

为供应商提供组件或工具的中间供应商有可能了解直接向其上报的漏洞，并应通知其供应商的 PSIRT。

子功能 5.1.1.3 合同协议

PSIRT 应确定其所有中间供应商，并考虑与法律部门合作，通过在合同协议中添加条款的方式确保及时消除漏洞。

子功能 5.1.1.4 PSIRT 向利益攸关方发出通知

供应商 PSIRT 可能会通知其利益攸关方，特别是在中间供应商无法补救漏洞或需要为补救漏洞花费大量时间的情况下。针对某些情况，供应商 PSIRT 可能会采用分层的通知流程，并通知受特定漏洞影响最大的利益攸关方。

功能 5.1.2 协调员

PSIRT 可能会要求协调员参与通知其他供应商的工作，协调公告提出的补救时间，尤其是在涉及多个供应商的情况下。CERT 协调中心（如 CERT / CC）[12]或第三方协调员的价值体现在邀请众多不同组织合力解决漏洞。

目的： 可能请协调员介入并协助 PSIRT 组织发出通知，同时与所有供应商合作，共同解决该漏洞。

成果： 加强各相关方之间的信任、协作和对披露的控制。

子功能 5.1.2.1 协调员的确认

根据漏洞披露政策记录并了解不同的协调员。

子功能 5.1.2.2 协调员的参与

与协调员合作，确保所有受影响的供应商 PSIRT 都已收到通知。

功能 5.1.3 漏洞搜索方

客户或第三方研究人员等漏洞搜索方，可能会通过服务领域 2 发现漏洞所载渠道将漏洞通报 PSIRT。

[12] www.cert.org

目的：为漏洞搜索方打造一个协作且预期明确的环境。

成果：加强各与漏洞搜索方之间的信任、协作和对披露的控制。

服务 5.2 协调

在适当的情况下，供应商 PSIRT 应安排与协调员或其他供应商共享漏洞信息。他们应了解供应商的漏洞处理策略，尽快协商补救和披露的时间表。

目的：记录通过补救措施从产品中消除的漏洞。

成果：明确实施补救措施的益处以及可从哪里获得补救措施。

功能 5.2.1 双边协调

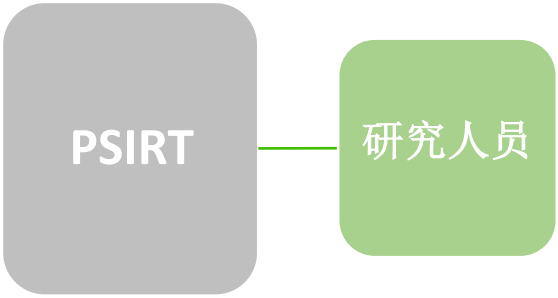


图 18：双边协调

供应商 PSIRT 负责与上报潜在漏洞的漏洞搜索方保持沟通。对于供应商而言，重要的是了解漏洞搜索方的意图、时间安排和立场，以便在商定的时间表内为协调披露提供便利。PSIRT 应考虑对坚持公开披露的漏洞搜索方表示认可。

目的：创造一个合作环境，让漏洞搜索方知道他们会得到认真对待。

成果：在尊重漏洞搜索方工作的基础上商定的披露计划。

子功能 5.2.1.1 接收报告

确认收到第三方漏洞搜索方提交的漏洞报告。

子功能 5.2.1.2 定期更新

向漏洞搜索方定期提供上报漏洞的最新状态。

子功能 5.2.1.3 漏洞搜索方进行验证

为漏洞搜索方提供补救措施，以便他们也能对这些措施进行验证。

子功能 5.2.1.4 漏洞搜索方认可

通过认可报告漏洞搜索方的贡献对其表示赞赏。供应商应与漏洞搜索方核实此表彰是否可以接受。

功能 5.2.2 多供应商协调

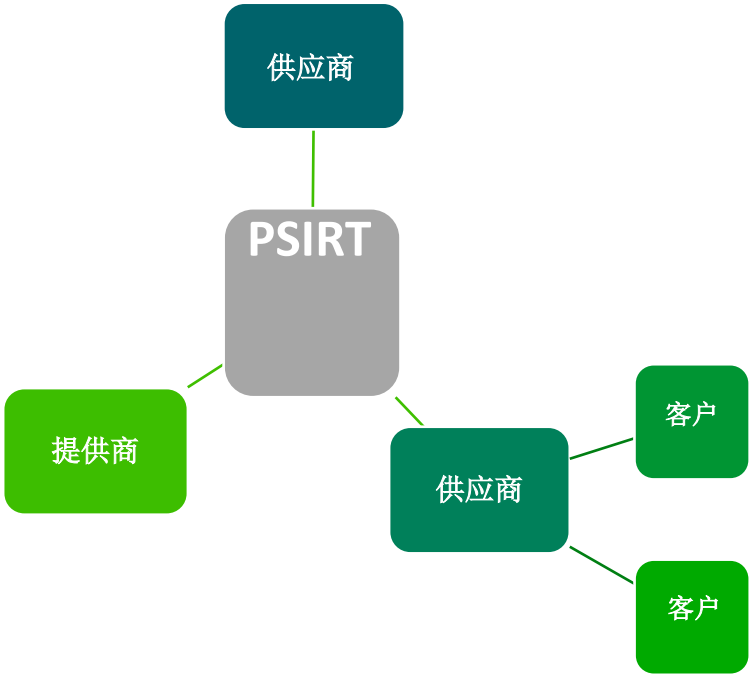


图 19：多供应商协调

在适当的情况下，供应商 PSIRT 应安排与协调员或其他供应商共享漏洞信息。他们应了解供应商的漏洞处理策略，应尽快协商补救和披露的时间表。

目的： 与各方合作，实现对利益攸关方和合作伙伴的透明，负责任地披露漏洞并进行修复。

成果： 加强信任、合作和对披露的控制。

多方利益攸关方	与自身的关系	协调中的利害关系
上游供应商	OEM 提供商可提供技术。	为提供补救措施，建议上游供应商管理其下游利益攸关方（参见服务领域 1.4）。
下游供应商	从上游供应商获得技术。	收到采取安全补救措施的通知。建议下游供应商就上游供应商团体和合作伙伴做出定义并与之开展合作（见功能 1.3.1）。

表 1：多方协调示例

子功能 5.2.2.1 报告的接收

PSIRT 供应商确认收到来自供应商或协调员的漏洞报告。

子功能 5.2.2.2 确认受影响的供应商

PSIRT 供应商或协调员可能需要确认受漏洞报告影响的供应商。

子功能 5.2.2.3 漏洞信息共享

PSIRT 供应商或协调员在不同供应商之间共享漏洞信息。

子功能 5.2.2.4 补救发布计划

PSIRT 供应商或协调员与供应商就补救的时间和可用性以及下游供应商如何获得补救开展合作。

子功能 5.2.2.5 补救验证

PSIRT 供应商或协调员与供应商一起验证旨在消除相关漏洞的安全补救措施。

子功能 5.2.2.6 披露协调

PSIRT 供应商或协调人与所有供应商协商，就如何披露以及何时公开披露漏洞达成一致。

服务 5.3 披露

发布安全补救措施时，应进行适当披露，以确保利益攸关方和供应商得到有关补救措施的适当通知。每条通知均需很好的定义（不同类型的通知可能有不同的受众）。

目的： 记录代码的更改和安全补救措施的发布。

成果： 明确对代码进行了哪些补救以及从哪里获得这些补救。

功能 5.3.1 版本说明

版本说明，包括自述文件和历史沿革记录，应包括补救措施的 CVE 参考。版本说明应该清楚地表达如何消除该漏洞。

目的： 提供包含在更新代码中的补救措施指示。

成果： 利益攸关方可以保护自己免于暴露在漏洞之下。

子功能 5.3.1.1 版本说明的披露

定义版本说明中应公开哪些漏洞。

子功能 5.3.1.1 版本说明审核

定义审核流程。

子功能 5.3.1.2 版本说明的批准

对披露进行审查和批准。

功能 5.3.2 安全公告

供应商应该建立一种机制，通过这种机制，可以在公共网页上向利益攸关方发布安全公告并披露已经修复的漏洞。

目的： *为发布的安全公告提供一个公共存储库。*

成果： *安全公告可供服务对象开展审查和采取行动使用。*

子功能 5.3.2.1 公告的模板

定义标准化的安全公告模板。模板内容包括标题、摘要、CVE、受支持产品产生的影响和状态、确认、参考和修订历史。

子功能 5.3.2.2 公告的交付方法

确定提供安全公告的机制，包括但不限于网络文件、RSS 提要或订阅。

子功能 5.3.2.3 公告的格式

为了让利益攸关方和服务对象使用自动化工具查询公告，可以考虑以机读格式发布公告，如公共安全咨询框架[13]（CSAF）。

子功能 5.3.2.4 公告的触发条件

定义触发发布安全公告的条件集。例如，如果需要采取措施通知利益攸关方托管环境已经得到补救（违规情形）。

子功能 5.3.2.5 CVE 指配

确定为漏洞分配 CVE 标识的过程。

子功能 5.3.2.6 漏洞搜索方认可

确定漏洞搜索方是想要公众的认可还是赞扬。

子功能 5.3.2.7 披露计划

定义审查流程，例如谁是利益攸关方以及应何时披露。

子功能 5.3.2.8 公告审核流程

针对定义的利益攸关方执行审核流程。

功能 5.3.3 以知识为依据的文章

供应商应为发布以知识为依据的文章建立一种机制，这些文章可能为某些严重性较低的漏洞提供安全补救措施，或者可以作为一种手段，传达因何特定的上报漏洞被作为误报遭到拒绝。

目的： *为以知识为依据的文章提供一个存储库*

[13] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf

成果：以知识为依据的文章可供服务对象审阅并采取行动。

子功能 5.3.3.1 以知识为依据的文章的披露

定义以知识为依据的文章应披露哪些漏洞。

子功能 5.3.3.2 以知识为依据的文章的审核

定义审核流程。

子功能 5.3.3.3 以知识为依据的文章的批准

对披露进行审批。

功能 5.3.4 内部利益攸关方流通

除了应当知晓漏洞沟通计划的高级业务负责人外；每天还有许多一线员工，与利益攸关方面对面或通过电话交流。针对即将发布的公告事先提供保密的信息通报和常见问题解答，使那些在发布时有可能会收到问询的人员预先做好准备。

目的：把“即将发布”的公告和批准所采用的回应方式，告知高级业务负责人、全球资讯部门和直面利益攸关方的员工。

成果：员工将能在公告发布日回应利益攸关方和媒体的提问，实现对信息的控制。

子功能 5.3.4.1 请内部利益攸关方参与

与内部利益攸关方协作，为其的团队设计和/或审查语言，以便在客户询问漏洞问题时使用。

服务 5.4 漏洞的度量指标

收集的数据应包括但不限于问题的数量、分类、补救时间表、受影响的产品或服务。

目的：为管理报告定期收集数据。

成果：确定需要分析、资源和改进的领域。

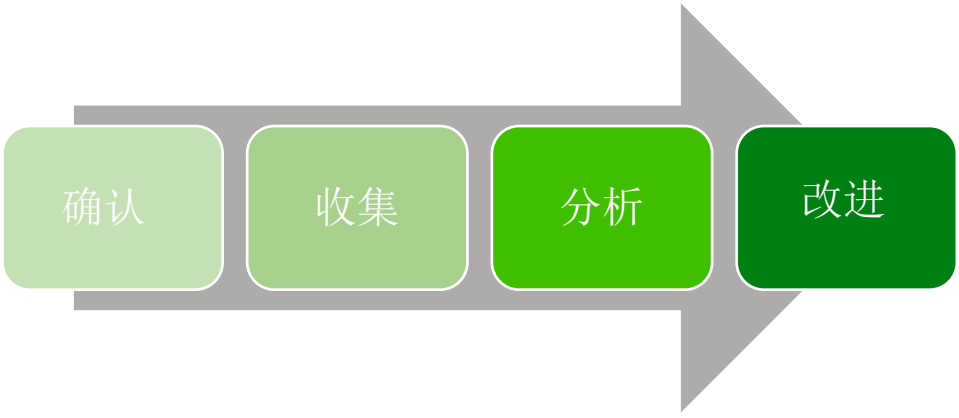


图 20：衡量漏洞的流程

功能 5.4.1 运作报告

运作报告可能提供有关已发布披露数量以及页面浏览量的附加信息。这些报告应定期在 PSIRT 内部与内部利益攸关方一起发布。

目的：定期收集用于普通报告的数据。

成果：确定需要分析、资源和改进的领域。

子功能 5.4.1.1 发布的安全公告数量

不同披露的数量可按产品上报并加以细分。这可能有助于推动团队分配技术资源。

子功能 5.4.1.2 发布到 NVD 的 CVE 数量

分配的 CVE 数量可用于将您的地位提升为 CVE 编号机构（CAN）。

子功能 5.4.1.3 安全公告的页面视图

如果查看您公告的利益攸关方数量很少，则您或应转而采用主动通知的策略。

服务领域 6

新技术、服务和集成使持续培训及教育成为安全专业人士的首要任务，产品安全领域的变化也是日新月异。随着软件渗透到我们生活中从汽车到冰箱的方方面面，满足产品保护需求变得空前重要。PSIRT 在支持强大课程方面发挥着关键作用，这些课程旨在让所有利益攸关方领略开发、验证和交付符合当今连通世界标准的产品/服务的复杂性。

整个公司的培训和教育需求可能存在很大差异。固件开发人员和软件服务开发人员的关注点各异，通常需要有的放矢的专门培训。就本文件而言，我们将阐述四个利益攸关方团体的培训需求：PSIRT、产品开发、产品验证和 PSIRT 流程中涉及的其他利益攸关方。

1) **PSIRT 培训**是独一无二的，因为 PSIRT 成员必须深入了解法律、沟通和开发等诸多领域。

2) **产品开发**（内部工程和开发）：开发人员需要接受特定领域的培训，因此需要培训有针对性。开发难以在现场更新的面向安全固件的要求，与对桌面应用工程师的要求存在巨大差异。

3) **产品验证**（内部工程和开发）：验证者需要不断接受培训，以熟悉最新的工具和技术，例如渗透测试（pen-testing）、漏洞扫描和早期设计审查，从而在需要解决问题之前便及早发现这些问题。

4) **所有其他利益攸关方：**此群体是指技术水平不高的受众，他们需要有坚实的基础方能理解有关开发、验证和交付安全产品的基础知识，才能在所交付产品存在漏洞时做出反应。

安全开发培训并非 PSIRT 计划的一部分，在 PSIRT 流程之外单独处理。然而，重要的是 PSIRT 应成为将安全产品推向市场的各个领域的倡导者，因此为确保推出适当的培训，应与各开发团队合作。在许多较小的组织中，可能并未设立一个单独的小组负责确保以安全为重点的产品开发。在这些情况下，PSIRT 可能会参与弥合差距的工作（这超出了本文件的讨论范围）。

在各节中，我们将确定各种利益攸关方团体，归纳某些重点领域，这或许有助于 PSIRT 参与关于培训和教育利益攸关方的富有意义的讨论。PSIRT 可以在内部编写所有培训材料，使用外部材料或利用外部培训资源培训其利益攸关方。

服务 6.1 培训 PSIRT

PSIRT 员工需要站在安全领域的前沿，这些领域涉及的内容包括但不限于发展趋势、新的漏洞和行业活动。这种广泛的知识始于在一般安全领域奠定的坚实基础，例如对领先的安全认证提出的要求。但认证只提供了一个基础，相关人员还需要通过安全会议、参与行业联盟，以及建立对整个行业的敏锐意识等活动不断磨炼，成为相关博客、行业新闻、联盟出版物等的忠实粉丝。PSIRT 成员还需要了解不断演进的安全和隐私立法。

功能 6.1.1 技术培训

重要的是 PSIRT 员工对基本安全概念和所支持产品的相关知识，有着扎实的理解。必须定期审查培训材料，以确保随着安全形势的变化，将新的漏洞处理技术纳入培训材料。

目的： 对 PSIRT 员工进行培训，使他们了解上报的问题并能在将问题移交给负责开发、测试和发布修复程序的团队之前，充分执行初始分类。

成果： PSIRT 工作人员在接受充分技术培训后，能够履行其职责。

安全概念培训将根据供应商支持的产品类型（例如硬件、固件、软件、网络、云产品或以上所有产品）而有所不同。在高层，培训必须涵盖基本安全主题，如常见攻击、加密、机密性、完整性、可用性、鉴权、授权、访问控制模型、多租户、相对合规性和法规等。此培训还应包括所有可能影响 PSIRT 活动的特定行业法规，如针对医疗保健及相关垂直行业的 HIPAA 和针对支付卡供应商和银行的 PCI DSS。此外，还必须为 PSIRT 员工提供一定程度的产品培训，以便他们能够了解报告的问题。

功能 6.1.2 沟通培训

鉴于外部漏洞搜索方向 PSIRT 报告问题，因此对 PSIRT 工作人员进行沟通政策和软技能方面的培训非常重要，其中包括如何及时与外部漏洞搜索方和内部利益攸关方沟通。

目的： 确保 PSIRT 员工在与外部实体互动时遵守组织的沟通政策，从而消除因不当沟通可能导致的任何监管/法律问题。

成果： PSIRT 工作人员将接受充分的沟通培训，从而清晰准确地履行分配给他们的职责，并且在沟通中不含糊其辞。

功能 6.1.3 流程培训

应为定义如何跟踪、管理和衡量上报的问题制定流程导则。此外，应当确定参与解决报告问题流程的各利益攸关方的角色。这一流程应涵盖对漏洞搜索方及时做出回复，并定期向他们发送所有未解决问题的最新信息。外部漏洞搜索方和供应商之间，亦应有一种定义明确且安全的信息交流方式。

目的： 确保产品安全事故的管理信息流动顺畅，从而使问题得到及时解决。

成果： PSIRT 员工将接受充分的内部流程培训，以便他们能够履行各自的职责。

功能 6.1.4 工具培训

子功能 6.1.4.1 缺陷跟踪和 PSIRT 及工程人员的其他管理工具

应该为给定组织中的每种产品（最好是所有产品相同）确定一个获得正式认可的缺陷跟踪工具。此工具应能识别所有缺陷，安全缺陷亦应照此统一识别。只有必要知晓者，方能查看并获取产品中与安全漏洞相关的信息。此外，该工具应具备满足计划度量指标要求的能力，包括拥有手动和自动报告功能。

目的： 确保问题得到有效跟踪，漏洞信息在经认证的跟踪工具中得到保护，只有必要知晓者方能访问、跟踪和管理这些问题。

成果： PSIRT 员工将接受充分的工具培训并掌握相关知识，以便能够履行各自的职责。

子功能 6.1.4.2 第三方跟踪工具

大多数产品均随附多个第三方组件（包括开源组件）。客户通常不了解产品中附带的第三方软件，因此有赖于供应商提供修复程序或补救信息。至关重要的是确认内部第三方跟踪工具，这种工具需涵盖供应商产品对各种第三方组件的依赖信息。此外，必须监控国家漏洞数据库（NVD）、第三方供应商的安全公告和其他外部站点，跟踪第三方组件的漏洞和修复程序，以便将这些修复程序提供给客户。

目的： 确定跟踪产品内嵌第三方组件的工具，以便跟踪和发布这些组件中漏洞。

成果： PSIRT 员工将了解并能跟踪交付产品中的第三方组件。

功能 6.1.5 跟踪所有培训举措

PSIRT 需跟踪各利益攸关方可以参加的所有培训。该团队需确保所有此类培训以一定的频率进行，因为安全环境变化非常之快，有必要不断重新制定培训内容和相应流程。

目的： 确保跟踪各利益攸关方可以参加的各类培训。。

成果： PSIRT 工作人员知晓各利益攸关方，已就各自在 PSIRT 流程中的角色接受了培训。

服务 6.2 培训开发团队

安全开发是指在整个开发过程中采取的方法和步骤，这些方法和步骤的设计意在减少软件相关产品和服务中的漏洞数量和漏洞的严重性。通过有强有力的课程和对安全开发方法的关注，可以在产品发布之前大幅减少漏洞，这比在产品入市之后再消除漏洞要经济得多。

安全开发始于产品需求和架构。此外，安全设计评审是在开发产品之前发现潜在漏洞的关键所在。

安全开发计划涉及许多活动，其细节远远超出了本文的覆盖范围。强烈建议制定单独的计划，对相应的安全开发周期实施管理。此计划应遵循公认的行业标准计划模式。微软安全开发周期模型[14]便是安全开发周期的一例。

目的： 鼓励组织制定适当的安全开发周期(SDL)计划，开发人员在该计划中接受的培训涉及编写安全代码，以及在创建产品的体系结构和设计时使用记录在案的安全准则。

安全开发培训并非始终被视作 PSIRT 服务对象的一部分，可在 PSIRT 流程之外加以处理。无论如何，这是一个重要的步骤，任何关心其产品安全状况的供应商都必须考虑。

功能 6.2.1 PSIRT 流程培训

开发流程的所有成员都需要理解为什么要制定 PSIRT 流程，此流程是如何工作的，以及他们应如何开发支持这一流程的产品。开发团队通常会在产品发布后转移到不同的项目，仅保持最低限度的后续跟进。开展团队培训并为他们提供存储产品关键信息的适当方法，对 PSIRT 全面解决产品漏洞问题而言至关重要。记录哪些人员是安全架构师、开发负责人和测试负责人等信息，以便 PSIRT 可以找到对风险评估和开发缓解措施了如指掌的人员。该文档还应包含以下内容：正在使用何种第三方组件，产品的更新流程，有哪些日志记录，允许存在安全例外，以及如何通知利益攸关方。该信息对 PSIRT 关闭安全漏洞至关重要。随着新开发团队成员的加入和离开，进修培训亦十分关键。

目的： 确保所有利益攸关方了解 PSIRT 流程及流程与利益攸关方在产品开发中的角色关系。

成果： 培育开发人员的安全文化并在处理漏洞方面加强合作。

[14] https://www.microsoft.com/en-us/sdl/

服务 6.3 培训验证团队

验证人员需要不断了解最新工具和技术，比如渗透测试、漏洞扫描、模糊化、道德黑客等。对验证人员进行这方面的培训属于 SDL 的范畴，不在本文件的讨论范围之内。然而，PSIRT 应鼓励组织成立一个专注于此项工作的小组。

目的： 鼓励组织制定适当的 SDL 计划，确定适当的安全测试工具。

成果： 更高的质量和更安全的产品。

与安全开发一样，安全验证培训未被视作 PSIRT 服务对象的一部分，而是在 PSIRT 流程之外处理。然而，这一步骤同样重要，供应商必须将其作为产品 SDL 的组成部分。

功能 6.3.1 PSIRT 流程培训

验证团队的一些成员可能会参与测试修复产品漏洞所需的修复程序。这些团队的成员需要了解 PSIRT 流程，此流程的工作方式，预期的时间框架，及其在流程中的角色。这些成员需要对产品寿命周期有很好的理解，从而能够知晓需要进行漏洞修复测试的受支持的版本。如果存在变通方法，他们亦需对此进行测试。对团队成员而言，回归测试也很重要。

目的： 确保所有利益攸关方了解 PSIRT 流程及流程与利益攸关方在产品验证中的角色关系。

成果： 培育验证人员的安全文化并在处理漏洞方面加强合作。

服务 6.4 继续教育所有利益攸关方

所有利益攸关方都需要一定程度的培训和对 PSIRT 计划有所了解。有许多利益攸关方参与了端到端 PSIRT 流程。因此，重要的是确定各种利益攸关方群体，并针对他们的需求开展培训。

目的： 确保所有利益攸关方团体均接受过培训或具备所需的基本意识，以履行其在 PSIRT 计划中的职责。

成果： 消息灵通的内部服务对象知晓他们将如何与 PSIRT 合作管理紧急漏洞问题，以及在这种情况下 PSIRT 将提供什么服务。

功能 6.4.1 培训高级管理人员

此小组通常参与公司沟通、漏洞保护和其他方面政策的初始签署工作。创建安全公告可能还需要管理层的批准。此外，高风险、高暴光度或责任重大的关键情况，通常需要高级管理层的批准。管理层可能还希望对所有产品的安全状况进行定期检查。因此，向管理层通报 PSIRT 流程的信息非常重要。

目的： 让管理团队了解其在 PSIRT 计划中的职能。

成果： 及时解决需要管理层签署的待批问题。

功能 6.4.2 培训法律团队

法律部门参与制定最初的公司政策。一些漏洞搜索方上报的问题可能存在责任问题，或许需要法律部门的协助，因此事先确定联系人非常重要。

目的： 让法律团队了解他们在 PSIRT 计划中的职能和相关时间表。

成果： 及时解决需要法律部门批准的安全问题。

功能 6.4.3 培训政府事务和合规团队

负责政府事务的人员参与了合规问题的处理。因此，事先确定联系人非常重要。

目的： 让政府事务团队了解他们在 PSIRT 项目中的职能。

成果： 及时处理需遵守特定监管标准的安全漏洞。

功能 6.4.4 培训营销团队

当品牌名誉面临风险时，通常会请营销人员参与。此外，营销人员还可以审查安全公告并发布相关的营销信息。营销团队亦参与产品安全方面的营销。

目的： 让营销团队了解他们在 PSIRT 计划中的职能，告知他们产品安全方面哪些可说哪些不可以说。

成果： PSIRT 与营销团队之间的适当协调，将使营销材料和安全公告的外部安全宣传保持高度一致。

功能 6.4.5 培训公共关系团队

公共关系（PR）团队或将负责回复外部安全帖或博客，或与回答与重大产品漏洞相关的新闻查询。应确定联系人，以便在任何需要对外发布的情况下请公共关系部门参与。

目的： 让公共关系团队了解他们在 PSIRT 项目中的职能。

成果： PSIRT 和公共关系团队之间的适当协调，将为供应商带来良好的外部安全态势。

功能 6.4.6 培训销售团队

销售团队可能会接受基本安全概念和安全实践沟通方面的培训。此外，对销售人员而言，知道可与外部人员分享哪些信息非常重要。建议销售员工将利益攸关方/潜在客户对安全性的任何担忧转呈 PSIRT 员工或支持人员，而不是直接解决这些问题。

目的： 让销售团队了解在产品安全方面哪些可说哪些不可以说，以及如何解决他们无法回答的问题。

成果： PSIRT 与销售团队之间的适当协调将有助于满足客户的期望。

功能 6.4.7 培训支持团队

为使支持团队能够处理来自客户的安全漏洞报告，必须对支持团队进行培训。在某些情况下，PSIRT 可能会参与解决这些问题。支持部门应发布策略，定义每个产品的寿命周期、支持的版本以及是否发布安全公告。大多数供应商只为支持的版本提供安全公告。因此，这些政策至关重要，必须在供应商网站上公布，以方便利益攸关方查阅。PSIRT 通常与支持部门保持密切关系，因此他们了解客户上报的问题。有时漏洞搜索方也可能是客户，因此问题的处理方可能会在支持部门和 PSIRT 之间切换。

目的： 让支持团队了解他们在 PSIRT 流程中的职能。

成果： PSIRT 与支持团队之间的适当协调将有助于满足客户的期望。

服务 6.5 提供反馈机制

使用在事故根源分析过程中获得的信息教育相关人员，防止将来出现类似的漏洞。

目的： 不断改进培训，以跟上安全行业快速变化的形势。

成果： 更高质量的培训将改善所有利益攸关方的体验。

附件 1：支撑资源

[15]架构内容框架

[16]ISO 31000：2009 风险管理—原则和指南

ISO/IEC 27000/2018 信息技术—安全技术—信息安全管理系统

[17]ISO/IEC 30111：2013 信息技术–安全技术–漏洞处理流程

[18]ISO/IEC 29147：2014 信息技术—安全技术—漏洞披露

[19]多方漏洞协调和披露指南与实践

项目管理知识体系指南和标准

[15] http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html

[16] https://www.iso.org/iso-31000-risk-management.html

[17] https://www.iso.org/obp/ui/#iso:std:53231:en

[18] https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en

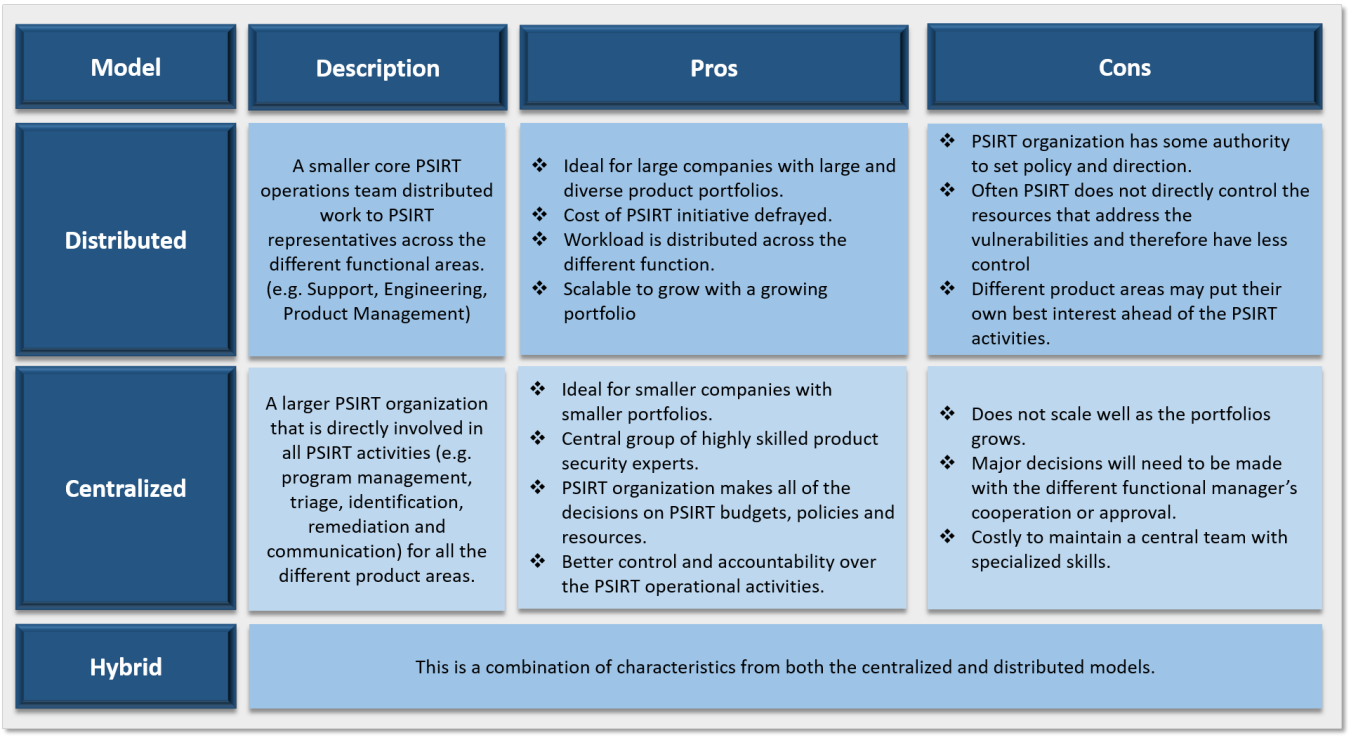
[19] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRSTMultiparty-Vulnerability-Coordination-v1.0.pdf

附件 2：鸣谢

- Barbara Cosgriff, MetLife
- Beverly Finch, Lenovo
- Carl Denis, Siemens
- Chris Robinson, Red Hat
- Jeff Hahn, Honeywell
- Jerry Bryant, Intel
- Josh Dembling, Intel
- Jean-Robert Hountomey, Broadcom
- Kevin Ryan, NetApp
- Langley Rock, Red Hat
- Lisa Bradley, Dell Technologies
- Peter Allor, Red Hat
- Reshma Banerjee, Oracle
- Rupert Wimmer, Siemens
- Shawn Richardson, NVIDIA
- Steve Brukbacher, Johnson Controls
- Tania Ward, Dell Technologies
- Vic Chung, SAP

附件 3：表格和插图

附件 4：PSIRT 组织模式的利弊



Model	Description	Pros	Cons
Distributed	A smaller core PSIRT operations team distributed work to PSIRT representatives across the different functional areas. (e.g. Support, Engineering, Product Management)	❖ Ideal for large companies with large and diverse product portfolios. ❖ Cost of PSIRT initiative defrayed. ❖ Workload is distributed across the different function. ❖ Scalable to grow with a growing portfolio	❖ PSIRT organization has some authority to set policy and direction. ❖ Often PSIRT does not directly control the resources that address the vulnerabilities and therefore have less control ❖ Different product areas may put their own best interest ahead of the PSIRT activities.
Centralized	A larger PSIRT organization that is directly involved in all PSIRT activities (e.g. program management, triage, identification, remediation and communication) for all the different product areas.	❖ Ideal for smaller companies with smaller portfolios. ❖ Central group of highly skilled product security experts. ❖ PSIRT organization makes all of the decisions on PSIRT budgets, policies and resources. ❖ Better control and accountability over the PSIRT operational activities.	❖ Does not scale well as the portfolios grows. ❖ Major decisions will need to be made with the different functional manager's cooperation or approval. ❖ Costly to maintain a central team with specialized skills.
Hybrid	This is a combination of characteristics from both the centralized and distributed models.		

图中文字：

模式	说明	益处	弊端
分布式	较小规模的核心 PSIRT 运作团队，将工作分配给不同职能领域的 PSIRT 代表（例如，支持部门、工程部门、产品管理部门）	• 产品量大且种类庞杂的大公司的理想之选 • 摊分 PSIRT 举措的成本 • 由不同职能分担工作 • 可随着产品组合的壮大而发展	• PSIRT 组织拥有一定的政策和方向制定权 • 通常 PSIRT 不直接控制处理漏洞的资源，因此控制力不强 • 不同产品领域可能将自身利益凌驾于 PSIRT 活动之上
集中式	直接参与针对不同产品领域各项 PSIRT 活动（例如计划管理、分类、确认、补救和沟通）的较大 PSIRT 组织	• 产品组合不大的小型公司的理想之选 • 技能高超的产品安全专家核心小组 • PSIRT 组织就自身的预算、策略及资源做出决策 • 更好的掌控 PSIRT 运作活动并进行问责	• 不能很好地随着产品组合的壮大而发展 • 重大决定需要与不同职能部门负责人合作做出或需要其批准 • 维持一个专业技能核心团队成本高昂
混合式	将集中模式和分布模式的特性集于一身。		

附件 5：事故响应团队类型

- **国家 CSIRT（计算机安全事故响应团队）（National CSIRT (Computer Security Incident Response Team)）**— 国家 CSIRT 指的是由国家当局设立的、提供国家级网络安全事故协调的一个实体，其顾客通常包括所有的政府部门和机构、执法和民间社会，通常它还是与其它国家的国家 CSIRT 以及地区的和国际的参与者进行交互的权威机构。

- **关键基础设施/部门的 CSIRT （Critical Infrastructure / Sectoral CSIRT）**— 负责监视、管理和响应与特定部门（例如能源、电信、金融）有关的网络安全事故。

- **企业（组织的）CSIRT（Enterprise (Organizational) CSIRT）** — 企业 CSIRT 通常指负责监视、管理和处理影响特定组织内部 ICT 基础设施和服务的网络安全事故的小组。

- **地区性的 / 多方的 CSIRT （Regional / Multi-Party CSIRT）**— 地区性的/多方的 CSIRT 指的是负责监视、管理和响应与特定地区或多个组织有关的网络安全事故的小组或者矩阵式小组。

- **产品安全事故响应团队（PSIRT）（Product Security Incident Response Team (PSIRT)）**— 产品 SIRT 是商业实体（典型的某一个厂家）内部的、管理与该组织商品化的产品或服务有关的安全脆弱点信息的接收、调查以及内部或公开报告的一个小组。

词汇表

- **行动（Actions）** — 怎样以变化的详细程度/成熟度完成某事的列表。

- **能力（Capability）** — 可能作为组织的任务和职责的一部分而执行的可度量的活动。对于 SIRT 服务框架来说，能力可以定义为更广泛的服务，也可以定义为必备的功能、任务或者行动。

-**容量（Capacity）** — 组织在达到某种形式的资源耗尽之前，能够履行特殊能力的并发进程的数量。

- **常见漏洞陈列（Common Vulnerability Exposures(CVE)）** - 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)）**[20]- 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)）**[21] - 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。

- **健康保险携带和责任法案（Health Insurance Portability and Accountability Act (HIPPA)）** - [22]一项美国法律，旨在建立相关隐私标准，为健康计划、医生、医院和其他医疗保健提供方掌握的患者病历和其他健康信息提供保护。

- **关键绩效指标（Key Performance Indicator(KPI)）**[23] - 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）** — 组织在其使命和授权范围内如何有效地履行特殊的能力，是行动或任务或者功能或服务集能够达到的熟练程度。

-**支付卡行业数据安全标准（PCI DSS）（Payment Card Industry Data Security Standard (PCI DSS)）** - [24]是一种旨在提高全球持卡人数据安全性的信息安全标准。

- **任务（Tasks）** — 完成该任务必须执行的系列行动。

[20] https://www.first.org/cvss/
[21] https://cwe.mitre.org/about/index.html
[22] https://www.medicinenet.com/script/main/art.asp?articlekey=31785
[23] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator
[24] https://www.pcisecuritystandards.org/pci_security/