安全加社区

公益译文项目

2016

网络威胁信息共享指南

NIST 特别刊物 800-150（第二版）

美国国家标准与技术研究院（NIST）
美国商务部

2016 年 4 月

文档信息			
原文名称	Guide to Cyber Threat Information Sharing		
原文作者	Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka	原文发布日期	2016 年 4 月
作者简介			
原文发布单位	美国国家标准与技术研究院 美国商务部		
原文出处	http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

“安全加”社区　　小蜜蜂公益翻译组

目录

授权

本文由 NIST 依据《2014 年联邦信息安全现代化法案》（FISMA）（美国法典第 44 卷第 3541 节、113–283 公法）规定的 NIST 法定职责拟定。NIST 负责开发信息安全标准和指南，包括联邦信息系统的最低要求。但是，未经相关系统决策联邦官员的明确许可，这些标准和准则不得用于国家安全系统。该指南符合美国行政管理和预算局（OMB）A-130 通告的要求。

由商务部长依法授权制定的标准和指南具有强制性与约束力，本文内容与其冲突时，以前者为准。本文所述准则并不会更改或取代商务部长、行政管理和预算局局长或其他联邦官员的现有权力。本刊不受美国版权保护，非政府组织可自愿使用，但组织在使用本文时提及作者，NIST 将不胜感激。

美国国家标准与技术研究院特别刊物 800-150

NIST SP800-150, 共 39 页（2016 年 4 月）

分类编号：NSPUE2

本文中可能提到的商业实体、设备或资料，仅为准确描述规程（procedure）或概念之用， 并非暗示 NIST 推荐或者认可，也不表明这些实体、资料或设备是实现目的的最佳选择。

本文提及的 NIST 依据法定职责制定的其他文档，有些可能处于开发过程中。也就是说，联邦机构在使用本文信息（包括概念和方法）时，所提及的同系列其他文档可能并未完成。这种情况下，在上述文档完成之前，现有的要求、指南和规程依然有效。为满足规划及过渡需要，联邦机构或会密切追踪 NIST 新文档的开发。

欢迎各组织在公开征求意见期间评审所有文档草案，并向 NIST 提供反馈意见。 欲了解 NIST 有关网络安全的其他刊物，请访问：http://csrc.nist.gov/publications。

计算机系统技术报告

美国国家标准与技术研究院（NIST）信息技术实验室（ITL）为美国的测量和标准基础架构提供技术领导，促进美国经济与公共福利。ITL 负责开发测试项目、制定测试方法，并提供参考数据、概念验证实现和技术分析来推动信息技术的发展和生产应用。ITL 的职责包括制定管理、行政、技术及物理方面的标准和指南，实现经济高效的安全，并保护联邦信息系统中非国家安全相关信息的隐私。SP 800 系列文件聚焦于 ITL 在信息系统安全方面的研究、指导和外展活动以及联合业界、政府和各学术机构开展的协作活动。

摘要

网络威胁信息指可帮助组织识别、评估、监控及响应网络威胁的任何信息。此类信息包括攻陷指标（indicator of compromise，亦有译为“攻击指示器”、“入侵指示器”的）、威胁源起方（threat actor）使用的策略、技术与过程（TTP）、检测、控制或防护攻击的建议方法以及安全事件分析结果。网络威胁信息的共享可同时提高分享组织与其他组织的安全状况。本文为建立、参与网络威胁信息共享关系提供了指导，帮助组织设定信息共享目标、识别网络威胁信息源、确定信息共享活动范围、制定威胁信息发布与分发规则、加入现有共享社团、有效利用威胁信息，以支持其总体网络安全实践。

关键词

网络威胁，网络威胁信息贡献，指标，信息安全，信息共享

致谢

本文作者包括 NIST 的克里斯·约翰逊（Chris Johnson）、李·贝杰（Lee Badger）、大卫·沃尔特米尔（David Waltermire）以及 MITRE 公司的朱莉·斯奈德（Julie Snyder）和克莱姆·斯科鲁普卡（Clem Skorupka）。在此，他们特向为本文做出贡献的同事表示感谢，包括 US-CERT 的汤姆·米勒（Tom Millar），MITRE 公司的凯伦·奎格（Karen Quigg）、理查德·穆拉德（Richard Murad）、卡洛斯·布拉斯克斯（Carlos Blazquez）、乔恩·贝克（Jon Baker），NIST 的穆若盖依尔·塞皮亚（Murugiah Souppaya），卡耐基·梅隆大学软件工程学院的瑞安·米尔夫（Ryan Meeuf），G2 公司的乔治·塞勒、格雷格·维特（Greg Witte）、马特·史密斯（Matt Smith），斯卡尔丰网络安全公司的凯伦·斯卡尔丰（Karen Scarfone），乔治敦大学乔治敦安全通信中心的艾瑞克·伯格（Eric Burger），网络工程服务公司的乔·德雷塞尔（Joe Drissel），互联网安全中心的托尼·萨格尔（Tony Sager），英特尔安全事业部的肯特·兰德菲尔德（Kent Landfield），KEYW 公司的布鲁斯·波特（Bruce Potter），戴尔 SecureWorks 的杰夫·卡朋特（Jeff Carpenter），北美电力可靠性公司（NERC），Gartner 公司的安东·楚卫肯（Anton Chuvakin），SANS 技术研究所的约翰尼斯乌尔里希（Johannes Ullrich），国防工业基地协同信息共享环境（DCISE）的帕特里克邓普西（Patrick Dempsey），Mass Insight 的马修·舒斯特（Matthew Schuster），美联储的詹姆斯·考尔菲尔德（James Caulfield），Biogen 公司的鲍勃瓜伊（Bob Guay）以及 Courion 公司的克里斯沙利文（Chris Sullivan）。

执行摘要

网络攻击日益频繁，复杂度也与日俱增，为组织保护数据及系统免受强大的威胁源起方的攻击带来了巨大挑战。这些威胁源起方或为自主发起攻击的个人攻击者，或为有充足资源、行动一致的群体，多为犯罪集团成员或代表某国政府利益。威胁源起方持续发起攻击，动机明确，动作敏捷，使用各种 TTP 入侵系统、中断业务、进行金融诈骗、泄露或窃取知识产权及其他敏感信息。考虑到这些威胁所带来的风险，组织应更加重视共享网络威胁信息，利用这些信息提高自己的网络防护能力。

网络威胁信息指可帮助组织识别、评估、监控及响应网络威胁的任何信息，包括指标（与攻击相关的系统组件或可观察事件（observable））、TTP、安全警报、威胁情报报告、推荐安全工具配置等。多数组织在信息技术与安全运营实践中，生成了各种网络威胁信息在内部共享。

通过与共享社团其他参与者交流网络威胁信息，组织可利用共享群体的集体知识、经验及能力，更全面地了解所面临的威胁。组织可利用这些知识，基于威胁信息，对防护能力、威胁检测技术及缓解策略进行决策。通过关联、分析从多个数据源获得的网络威胁信息，组织可丰富已有信息，使其更具有操作性。要丰富已有信息，可独立确认其他社团成员的观察结果或通过减少含糊之词及错误提高威胁信息的整体质量。共享社团成员在接收信息后修复威胁，抑制了威胁的传播能力，这为其他成员（甚至是未收到网络威胁信息或收到但并未响应的成员）提供了一定程度的防护能力。此外，通过共享网络威胁信息，组织可更有效地检测针对特定行业、业务实体或社会团体的攻击活动。

本文旨在帮助组织建立、参与网络威胁信息共享关系，介绍了共享的益处与挑战，明确了信任的重要性，梳理了处理数据时需考虑的具体事项。作为指导性文件，本文讨论了如何通过安全有效的信息共享实践来促进网络安全运营与风险管理活动，帮助组织规划、实施与维护信息共享。

NIST 鼓励组织间进行更广泛的网络威胁信息共享，一方面，组织可以从其他组织获取威胁信息，另一方面，组织可将内部产生的威胁信息提供给其他组织。组织可参考如下建议，更有效地利用信息共享能力：

设定信息共享目标（goals and objectives），以支持业务流程与安全指导方案（security policies）。

组织的信息共享目标应对整体网络安全战略有促进作用，可帮助组织更有效地管理网络相关风险。组织应将自己员工及其他人员（如网络威胁信息共享组织的成员）的知识与经验结合起来，共享威胁信息，同时按照安全、隐私及合规性要求进行运营。

识别内部现有的网络威胁信息源。

组织应识别当前收集、分析及存储的威胁信息。在库存流程中，组织应确定如何使用信息。具体说，基于网络威胁信息，组织可识别机遇，优化决策流程，制定从其他（或为外部）来源或通过部署额外工具或传感器获得威胁信息的策略，判断哪些威胁信息可与外界共享。

指定信息共享活动范围。

组织信息共享活动的范围应与组织的资源、能力及目标相匹配。信息共享工作应聚焦于能为组织及其共享合作伙伴带来最大价值的活动。确定范围时，应判断哪类信息可经组织关键利益主体授权进行共享、此类信息在哪些情况下可进行共享以及信息可以并应该共享给谁。

制定信息共享规则。

共享规则旨在控制威胁信息发布和分发，防止传播敏感信息（这些信息若被不当披露，可能会为组织、客户或业务合作伙伴带来不利影响）。信息共享规则应考虑到接收人的可信性、共享信息的敏感性以及共享（或不共享）某类信息的潜在影响。

参与信息共享工作。

组织应判断哪些共享活动可作为对现有威胁信息能力的补充，并积极参与这样的活动。为了满足运营需要，组织或需要加入各种信息共享论坛，包括公共或私有社团、政府知识库 (repository)、商业网络威胁情报流以及诸如公开网站、博客与数据流之类的公开源。

通过提供额外上下文、 修订或建议优化措施， 设法丰富指标。

组织应尽可能编制元数据，为每个指标提供上下文，描述指标应如何使用、理解，以及它与其他指标的关系。此外，共享流程应包括指标发布、指标与相关元数据更新、错误或无意误共享的信息撤回机制。这样的反馈对于社团内部共享指标的丰富、成熟与质量提升发挥着重要的作用。

利用自动化安全机制发布、 使用、 分析与响应网络威胁信息。

使用标准化数据格式与传输协议共享网络威胁信息可简化威胁信息处理的自动化过程。使用自动化手段，可减少人为干预，快速共享、转换、丰富与分析网络威胁信息。

主动制定网络威胁共享协议。

组织应提前规划，在安全事件发生前制定共享协议，而不是在网络安全事件发生时才仓促草就。提前规划可确保参与组织明白其角色、职责与信息处理要求。

保护敏感网络威胁信息的安全与隐私。

在处理网络威胁信息时可能会涉及个人验证信息（PII）、知识产权及商业秘密等敏感信息。这些信息若不当披露则会导致经济损失，违反法律、法规、合同，引起法律诉讼，或损害组织声誉。因此，组织应实施必要的安全与隐私控制措施及操作规程以保护信息不被非法泄露或修改。

持续支持信息共享活动。

每个组织都应制定信息共享计划，为持续的基础设施维护与用户支持做准备。计划内容应包括如何收集、分析内外部威胁信息以及在制定与部署防护措施时如何使用这些信息，方法应具有可持续性，以保证资源充分，能满足收集、存储、分析与传播网络威胁信息的需要。

1.0 导言

1.1 目的与范围

本文为组织共享网络威胁信息提供指导，介绍了如何使用从外部接收的网络威胁信息以及如何生成可与其他组织共享的网络威胁信息。文档中还阐述了在参与信息共享社团时应考虑的具体事项。

本文针对 NIST SP 800-61《计算机安全事件处理指南》第 4 节“统筹与信息共享”中提出的信息共享概念进行了详细论述。

1.2 读者对象

本文目标读者为计算机安全事件响应团队（CSIRT）、系统与网络管理员、安全人员、隐私管理人员、技术支持人员、首席信息安全官（CISO）、首席信息官（CIO）、计算机安全项目经理以及网络威胁信息共享活动中涉及的其他关键利益主体。

虽然本指南主要读者为联邦机构，也同样适用于其他的各种政府及非政府组织。

1.3 文档结构

本文档其他部分还包括：

- 第 2 节介绍了基本的网络威胁信息共享概念，阐述了共享信息的益处，讨论了组织在实施共享时所面临的挑战；
- 第 3 节为组织之间建立共享关系提供了指导；
- 第 4 节描述了在参与共享关系时应考虑的事项；
- 附录 A 提供了各种场景，说明共享网络威胁信息可提升相关组织效率，并可以通过利用合作伙伴的网络经验与能力来增强自己的网络防护能力；
- 附录 B 列举了本文中使用的术语及其定义；
- 附录 C 列举了本文中使用的缩略语；
- 附录 D 列举了本文所引用的材料。

2.0 认识网络威胁信息共享

本章介绍了网络威胁信息共享的基本概念，将网络威胁信息进行了分类，定义了常用术语，并探讨了共享网络威胁信息的潜在用途以及威胁信息共享的益处与挑战。

2.1 威胁信息类型

网络威胁指“对信息系统的未授权访问、损害、信息披露或修改和 / 或拒绝服务可能会对组织运营（包括任务、职能、形象或声誉）、组织资产、个人、其他组织或国家造成潜在不利影响的情形或事件。”【2】为了简洁起见，本文用“威胁”指代“网络威胁”，造成威胁的个人和群组亦称为“威胁源起方”或简单说成“源起方”。

威胁信息指与威胁相关、可帮助组织防护威胁或检测威胁活动的任何信息。威胁信息主要分为如下几类：

- **指标：**指可表明攻击即将或正在发生、或可能已出现入侵的技术因素（technical artifact）或可观察事件 [1]，包括可疑命令和控制（C&C）服务器的 IP 地址、可疑 DNS 域名、引用恶意内容的 URL、恶意可执行文件的哈希值及恶意邮件的主题。
- **策略、技术与过程（TTP）：**指源起方行为。策略是对行为的概括描述，技术是对策略涉及行为的具体描述，过程是对技术的进一步、更详细的描述。从 TTP 可看出源起方倾向于使用何种恶意软件变种、运算顺序、攻击工具、传递机制（如钓鱼或水坑攻击）或攻击。
- **安全警报：**亦称为公告（advisory/bulletin）和漏洞说明（vulnerability note），一般是对用户发布的有关现有漏洞、攻击及其他安全问题的简要技术通知。安全警报来源包括美国计算机紧急响应小组（US-CERT）、信息共享与分析中心（ISAC）、国家漏洞库（NVD）、产品安全事件响应小组（PSIRT）、商业安全服务提供商、安全研究员等。
- **威胁情报报告：**一般用平实的语言写成，主要内容涉及 TTP、威胁源起方、目标系统与信息类型以及使组织获得更高态势感知能力的其他威胁相关信息。威胁情报指汇总、转换、分析、解释或提炼后的威胁信息，为决策流程提供必要上下文。
- **工具配置：**对于搭建并使用工具（机制）提供的建议，这些工具（机制）为自动化采集、交换、处理、分析与使用威胁信息提供支持。工具配置信息可包括安装与使用 rootkit 检测与清除工具、创建并定制入侵检测特征、路由器访问控制列表（ACL）、防火墙规则或 Web 过滤配置文件等说明。

许多组织已经在内部产生并共享威胁信息。例如，组织的安全团队在响应安全事件时识别入侵系统中的恶意文件，制定相关指标集（如文件名、文件大小、哈希值），然后将这些指标分享给配置安全工具（如主机型入侵检测系统）的系统管理员，以便检测其他系统中存在的这些指标。另外，安全团队在发现组织内钓鱼攻击增多时可启动 email 安全感知活动。这些做法都属于组织内的信息共享活动。

本文的主要目的是统一不同组织间的威胁信息共享实践，这种共享是双向的，一方面从其他组织获取威胁信息，另一方面将内部产生的威胁信息分享给其他组织。

2.2 信息共享的益处

威胁信息共享使威胁信息被更多的人获取。基于共享资源，组织可采取主动，利用合作伙伴的知识、经验与能力来提高自己的安全状况。“你之检测，我之防御”[2]，这个模式卓有成效，组织积极进行共享可提高自己的整体安全能力。

对于分享的威胁信息，组织有多种使用方法。有的以运营为导向，比如用新指标与配置更新企业安全控制措施，进行持续监控，以检测最新攻击与入侵。有的以战略为导向，比如在规划组织安全架构的重大变更时将分享的威胁信息作为输入。

1 可观察事件指网络或系统中发生的恶意或非恶意事件。

2 这句话已在多个报告与讨论中提及，出自互联网安全中心的高级副总裁兼首席布道官托尼·萨格尔（Tony Sager）之口。

在行业（或具有其他共同特征的）社团内部交流威胁信息好处尤其大，因为成员组织面临的威胁源起方会使用通用的 TTP 攻击同类系统与信息。组织间若成功协作，共同对抗组织良好又颇具威力的威胁源起方，网络防护便会事半功倍。通过合作，组织可建立与维持可信任关系，作为安全、负责与高效的信息共享的基础。

信息共享会带来如下好处：

- **共享的态势感**知。进行信息共享，组织可利用同一社团内分享伙伴的集体知识、经验与分析能力，共同提高防护能力。即使只贡献了一个新指标或只检测到一个威胁源起方，也可以提高整个社团的安全意识与能力。
- **对威胁的深入了解。**通过生成并共享威胁信息，组织可更深入地了解威胁环境，基于威胁信息进行网络安全运营与风险管理。利用共享来的信息，组织可判断哪些平台或系统受到影响，采取防护措施，提升检测能力，观察现有威胁环境发生的变化，以更有效地响应与恢复安全事件。
- **完善知识。**当看似毫无关联的观察数据被某个组织分享及分析后，可与其他组织收集的数据相关联。在这个过程中，优化了现有指标，获取了与特定安全事件、威胁或威胁活动相关的威胁源起方 TTP 的知识，因而提升了信息的价值。通过数据关联，组织会洞悉指标之间的关系。
- **群体免疫性。**群体免疫性原则源自于生物学，指通过为多数（非全部）成员接种疫苗使整个群体对某种疾病产生免疫力。与此类似，组织基于收到的威胁信息修复自己的威胁，减少威胁源起方的活跃攻击向量，降低脆弱性，为其他还未启用相应防护措施的组织（还未收到威胁信息或收到后还未响应）提供了一定程度的防护。
- **更敏捷的防护能力。**威胁源起方不断调整 TTP 以规避检测、绕过安全控制措施并利用新漏洞。分享信息的组织一般可及时了解 TTP 的变化，因而可迅速检测并响应威胁，降低攻击成功实施的可能性。这样的敏捷性可为网络防护方产生规模效益，同时迫使威胁源起方开发新的 TTP，增加其攻击成本。

2.3 信息共享面临的挑战

共享威胁信息的好处显而易见，但也不无挑战。有些挑战在使用与产生威胁信息时均须面对，包括：

- **建立信任。**信任关系是信息共享的基础，需要花费功夫建立并维持。通过面对面会议、电话或社交软件定期沟通可加速建立信任。
- **实现互通。**标准化数据格式与传输协议是实现互通的重要组成部分，有助于在不同的组织、知识库与工具间实现安全的结构化威胁信息自动交换。不过采用特定的格式与协议会要求大量时间与资源。若共享伙伴要求不同的格式或协议，则投资价值会大幅度降低。
- **保护非机密的敏感信息。**泄露诸如个人验证信息（PII）、知识产权、商业秘密、其他专有信息之类的敏感信息会带来经济损失，违反共享协议，卷入法律诉讼，或损害组织声誉。共享信息会暴露组织的防护或检测能力，威胁源起方可乘机进行威胁转移 [3]。非法泄露信息会阻碍或打断调查过程，破坏信息，妨碍日后的法律诉讼，或中断响应行动（如打击僵尸网络）。组织对共享信息应有具体的处理标记，并实施指导方案、规程与技术控制措施，以积极管理泄露非机密的敏感信息所带来的风险。
- **保护机密信息。**来源于政府的信息可能被标记为机密，为组织使用此类信息带来困难。组织每次访问机密信息，都得请求获取相关权限并对此进行维护，长期看需耗费大量时间与经济成本。此外，许多组织雇佣非美籍人士，这些人无权获得安全权限，因而不允许访问机密信息。[3]

有些挑战只在使用他方分享的信息时才会遇到，包括：

- **访问外部信息。**要访问外部信息源，将从外部获得的信息融入本地决策流程，组织应有相应的基础

3 NIST SP 800-30《风险评估指南》【2】将“威胁转移”定义为“攻击者在发现安全设置及 / 或措施（如安全控制措施）后作出的反应，具体表现为改变攻击意图 / 目标的某个特征以规避和 / 或对抗该安全设置 / 措施。威胁转移可在一个或多个域进行，包括（1）时间域（如推迟攻击或非法入侵以进行额外监控）；（2）目标域（如选择防护不太完善的其他目标）；（3）资源域（如增加攻击资源以减少不确定性或对抗安全设置及 / 或措施）；（4）攻击规划 / 攻击方法域（如改变攻击武器或路径）。”

设施。从外部获取信息后，若无能力进行响应，此等信息则毫无价值。

- **评估接收信息质量。**组织从某信息共享社团获得信息后，需验证该信息是否满足某已识别需求，并了解信息使用成本与风险，然后再采取安全相关措施（如配置防护设备）。
- 有些挑战仅在组织欲向外提供信息时才会出现，包括：
- **符合法律及组织要求。**组织的高级主管与法务团队可能会约束外传信息种类，具体包括指定可外传的信息种类与限制可披露的技术细节。出于合法经营、法务或隐私的考虑实施安全手段是合理的，但约束措施若毫无根据或随意制定，则会影响共享信息的实用性、可用性、质量与及时性。
- **限制具名。**某些组织虽然公开参与信息共享社团，但在提供信息时会要求匿名。共享匿名信息允许组织共享更多的信息，同时控制了对组织声誉带来的风险。然而，匿名提供信息会限制信息的有用性，因为用户可能不信任未知来源的信息。若原始信息源无从查起，组织便无法确认信息来源于自主方，因而降低对接收信息的信任。
- **信息生成能力。**组织应根据目标信息类型，提供必要的基础设施、工具与培训，以生成相应信息。收集、发布基本的威胁信息（如指标）相对容易，但是分析诸如威胁源起方动机与 TTP 之类的信息则会比较麻烦。

3.0 建立共享关系

要培育威胁信息共享能力，建议进行如下的规划与准备活动[4]：

- 定义信息共享目标（3.1 节）；
- 识别内部威胁信息源（3.2 节）；
- 定义信息共享活动范围（3.3 节）；
- 制定信息共享规则（3.4 节）；
- 加入共享社团（3.5 节）；
- 做好计划，为信息共享活动提供持续支持（3.6 节）。

在整个流程中，鼓励组织咨询组织内外的主题专家（subject matter expert），包括：

- 经验丰富的网络安全人士
- 业界认可的威胁信息共享组织的成员及运营者
- 可信业务合作伙伴、供应链合作商及业界同仁
- 通晓法律问题、内部业务流程、规程及系统的人士

组织应利用从这些专家获得的知识与经验，培养威胁信息共享能力，根据自己的安全、隐私及合规要求，为组织实现使命与日常运营提供支持。因为风险、要求、优先考虑事项、技术及 / 或规定不断变化，上述过程常反复进行。组织应根据情况变化，必要时重新评估与调整自己的信息共享能力。此等变化可能涉及重复进行上述全部或部分规划及准备活动。

3.1 定义信息共享目标

首先，组织应制定目标，从组织的业务流程与安全政策方面，阐述信息共享的期望结果。这些目标有助于组织划定信息共享工作范围，选择并加入共享社团，为信息共享活动提供持续支持。由于技术及 / 或资源的限制，可能需要为目标指定优先级，以保证要事先办。

3.2 识别内部网络威胁信息源

信息共享工作的一个关键步骤是识别组织内部的潜在威胁信息源。威胁信息源包括传感器、工具、数据流及知识库。可能需要进行的具体步骤包括：

- 确定生成威胁信息的传感器、工具、数据流及知识库，保证其生成的信息准确无误，生成频率满足要求，可充分支持网络安全决策；
- 从收集并经过分析的安全信息中，找出用于组织持续监控策略的数据；
- 从收集并储存的威胁信息中，找出可能没有进行持续分析或评审的数据（如操作系统默认审计日志文件）；
- 查明哪些威胁信息适合与外界共享以及哪些数据有助于高效响应网络威胁。

该流程还包括识别组织内威胁信息源的负责人及操作人。理想情况下，人员对自己所操作的传感器、工具、数据流及知识库有深入了解，可推动数据输出、转化及整合能力培养流程，支持信息共享计划。在培养此等能力时，重要的是要了解信息的本地存储方法、数据的输出格式以及与信息源互动可使用的查询语言、协议及服务。有些信息源存储、发布的是结构化的机器可读数据，有些提供的是无固定格式的非结构化数据（如自由文本或图像）。基于开放、标准格式的机器可读结构化数据一般可被更多工具获取、搜索并分析。所以说，信息格式在很大程度上影响了使用、分析及交换信息的效率及便利性。

在上述流程中，组织还应留心是否有信息鸿沟会妨碍目标的实现。识别信息鸿沟后，组织可更好地规划投资，将其优先投入到发展新能力中，并可通过从其他（或为外部）来源获取威胁信息或部署额外的工具或传感器

4 虽然下述活动按前后顺序描述，实际操作中，活动顺序可以不同，多项活动甚至可同时进行。例如，参加业界认可的共享组织时，可将制定信息共享规则视为加入群体的必要步骤。

来识别机遇，消除鸿沟。

表 3-1 列举了组织内常见的网络安全相关信息源，并给出从这些信息源可获得的、安全运营人员可能会关注的数据元素例子。

表 3-1：内部信息源示例

数据源	示例
	网络数据源
路由器、防火墙、远程服务（如远程登录或远程执行命令）及动态主机配置协议（DHCP）服务器日志	时间戳 源 / 目的 IP TCP/UDP 端口号 MAC 地址 主机名 动作（拒绝 / 允许） 状态码 其他协议信息
诊断与监控工具（网络入侵检测与防护系统、抓包与协议分析）	时间戳 IP 地址、端口及其他协议信息 报文负载 特定应用信息 攻击类型（如 SQL 注入、缓冲区溢出等） 针对性漏洞 攻击状态（成功 / 失败 / 阻断）
	主机数据源
操作系统及应用配置设置、状态与日志	绑定及建立的网络连接及端口 进程与线程 注册表设置 配置文件条目 软件版本及补丁级别信息 硬件信息 用户与用户组 文件属性（如文件名、哈希值、权限、时间戳、大小等） 文件存取 系统事件（如启动、关机、失败等） 命令历史记录
杀毒产品	主机名 IP 地址 MAC 地址 恶意软件名 恶意软件类型（如病毒、黑客工具、间谍软件、远程访问等） 文件名 文件位置（如路径） 文件哈希值 采取的行动（如隔离、清洗、重命名、删除等）
Web 浏览器	邮件信息： 邮件头内容 • 发送人 / 接收人邮件地址 • 主题 • 路由信息 附件 URL 嵌入式图形
	其他数据源
安全信息与事件管理（SIEM）	整合各数据源（如操作系统、应用程序及网络日志）获取数据的总结报告
技术支持工单系统、安全事件管理 / 追踪系统以及组织内部人员	分析报告与观察数据，内容包括： • TTP • 攻击内容 • 关联事物 • 动机 • 攻击代码与工具 • 响应及缓解策略 • 推荐行动方案 用户屏幕截图（如错误消息或对话框）
取证工具包与动态及 / 或虚拟执行环境	恶意软件样例 系统组件（网络、文件系统、内存等）

在新部署了传感器、知识库或能力后，组织应及时更新库存信息。此外，设备配置、所有权或管理接口人等的重大变化应有文字记录。

3.3 定义信息共享活动的范围

组织应定义信息共享活动的范围，包括规定可共享的信息类型、信息共享的条件和对象。组织应在界定信息共享活动时审核其信息共享目标，以确保要事先办。在定义这些活动时，重要的是要确保具有支持每项活动的信息源和能力。组织还应考虑开展能够弥补已知信息鸿沟的共享活动。例如，组织内部可能没有恶意软件分析能力，但可以通过加入共享社团获取恶意软件指标。

信息共享活动的范围因组织的资源和能力的不同而不同。通过缩小范围，资源有限的组织可以专注于更少的活动，为自身和共享伙伴提供最大价值。在获得额外能力与资源后，组织可以扩大信息共享活动的范围。这种增量的方法有利于确保信息共享活动能够支持组织的信息共享目标，同时充分利用可用资源。有更多资源和更先进能力的组织一开始就可以确定比较大的活动范围，开展更多活动，支持目标实现。

支持威胁信息共享和接收的自动化程度是在确定共享活动范围时应考虑的一个因素。自动化程度低的方法或手动方法在循环中直接涉及人工干预，这可能会增加人力资源成本，并限制处理信息的广度和信息量。使用自动化可减少人力成本，使组织能够选择更大范围的活动。关于自动化威胁信息共享概念，参见第 4 节。

3.4 制定信息共享规则

在共享威胁信息前，做好以下工作是非常重要的：

- 列出可能要共享的威胁信息类型
- 描述允许信息共享的条件和情况
- 确定已被批准的威胁信息接收人
- 描述编辑或筛选共享信息的要求
- 说明是否允许来源具名
- 应用信息处理标记，描述信息接收人的信息保护义务

以上这些步骤规定了控制威胁信息发布和分发的规则，有助于防止传播敏感信息（这些信息若被不当披露，可能会为组织、客户或业务合作伙伴带来不利影响）。信息共享规则应考虑到接收人的可信性、共享信息的敏感性以及共享（或不共享）的潜在影响。例如，组织可要求限制在内部个人或团体之间交流高度敏感性的信息，允许与特定的信任合作伙伴共享中度敏感性的信息，允许在封闭共享社团内发布低敏感性的信息，并允许在公共信息共享论坛上自由交流非敏感信息。

在建立和审核信息共享规则时，组织应征求法律和隐私管理人员、信息责任人、管理团队和其他利益相关主体的意见，以确保共享规则符合组织成文的政策和流程。组织可能选择通过《谅解备忘录》（备忘录）、《保密协议》（NDA）、《框架协议》[5] 或其他协议来制定共享规则。鼓励组织在日常网络安全运营过程中主动订立网络威胁信息共享协议，作为正在进行的网络安全业务的一部分，而不是在网络安全事件发生时才被迫仓促草就。

应定期重估组织的信息共享规则。以下安全事件可触发规则重估：

- 监管或法律要求发生变化
- 组织政策更新
- 引入新的信息源
- 风险容忍度发生变化

5 《国防工业基础（DIB）网络安全 / 信息安全保障（CS/IA）计划标准化框架协议》[4] 就是一个框架协议，它贯彻了《美国联邦法规》第 236 部分 236.4 至 236.6 章节的内容。

- 信息责任人发生变化
- 运营 / 威胁环境发生变化
- 组织兼并与收购

3.4.1 信息敏感度与隐私

很多组织处理的信息根据监管监管、法律或合同义务要求，需要进行保护。这包括个人验证信息和其他在《萨班斯法案》（SOX）、《支付卡行业数据安全标准》（PCI DSS）、《健康保险携带与责任法案》（HIPAA）、《2014 年联邦信息安全现代化法案》（FISMA）和《格雷姆 - 里奇 - 比利雷法》（GLBA）中规定应受到保护的敏感信息。组织识别和适当保护这些信息是很重要的。在制定识别和保护敏感信息的流程时，应咨询组织的法务团队、隐私官、审计员和熟悉各种监管框架的专家。

从隐私角度看，威胁信息共享的主要挑战是可能会泄露个人验证信息 [6]。对负责处理威胁信息的个人进行教育和意识培养，让其了解如何识别和保护个人验证信息 [7]，这一点是很重要的。信息的内部共享可能会导致个人验证信息泄露给那些按照工作职能原本不能例行访问这些信息的人。例如，取证分析师或事件响应人可能会查找硬盘中的恶意软件指标、审核与可疑钓鱼攻击相关邮件中或进行抓包检查时接触到个人验证信息。分析师对于这些信息有合理的审查需求，以调查攻击、制定检测策略或制定防御措施。如果分析结果与他人共享，需要采取措施保护个人验证信息的机密性。

组织应有信息共享的指导方案和流程，指导如何处理个人验证信息。这些指导方案和流程中应包括如何识别可能包括个人验证信息的安全事件数据类型。指导方案应描述适当的安全措施来管理与共享数据相关的隐私风险。常见的做法是最大程度地关注指标的变化。一些指标，如文件哈希值、网络端口号、注册表键值和其他数据元素，不属于个人验证信息。然而，在个人验证信息被识别后，组织应在信息共享前，对包含与调查或处理网络威胁不相关的个人验证信息的字段进行修改。采取的防护类型和防护程度应根据信息的预期用途、敏感性和目标接收人而定。在可行的情况下，应鼓励组织使用自动化方法（而非人工方法）来识别和保护个人验证信息。手动识别、提取和模糊个人验证信息可能是一个缓慢、易出错的过程，需要大量资源。自动化方法可能包括根据列表中的允许值检查数据字段的内容，使用模式匹配技术（如正则表达式）查找个人验证信息，并对包括个人验证信息的数据进行去标识化、隐藏和匿名处理 [8]。自动化程度将因数据的结构和复杂性、信息的敏感性和所用工具的能力不同而不同。

组织还应采取措施防止非法披露知识产权、商业秘密和其他专有信息。这样的信息披露可能会导致经济损失，违反保密协议或其他共享协议，引起法律诉讼或损害组织的声誉。

表 3-2 介绍了部分类型的威胁信息，提供了这些类型的威胁信息中可能包含的敏感数据示例，并提供了处理这类数据时的一般建议。

6 行政管理和预算局（OMB）备忘录 07-16 [5] 中对个人验证信息的定义为“可用于识别或跟踪个人验证信息，如姓名、社保号码、生物特征记录等，或与其他个人或识别信息（如出生日期、出生地、母亲家族姓氏等）结合使用，可联系到具体个人的信息”。OMB 备忘录 10-22 [6] 中进一步说明“个人验证信息的定义并不是指某一类信息或技术”。并且，识别个人身份的风险需要逐例评估。评估时，机构还要认识到这一点：根据公开的附加信息（无论来自何种媒介或来源），非个人验证信息可以结合其他已知信息一起用来识别个人身份。”NIST SP 800-122 [7] 在广义上提出了略有不同的个人验证信息定义，更注重保密性的安全目标，而不是隐私。根据对附加监管要求的不同考虑，联邦政府之外的组织对个人验证信息的定义也不尽相同。无论组织如何定义个人验证信息，本指南均可适用。

7 了解更多关于隐私控制措施的指南和示例，参见 NIST SP 800-53（第 4 版）中的附录 J《隐私控制措施目录、隐私控制、增强和补充指南》[8]。

8 NIST SP 800-122 [7] 中描述了“去标识化”过程，可剔除或模糊化个人验证信息。因此，剩下的信息就不能用户识别个人身份了。

表 3-2：敏感数据处理建议

威胁类型	敏感数据元素示例 [9]	建议
网络指标	任何一个网络指标都是敏感的，但整体网络指标往往更加敏感，因为它们可以显示网络实体之间的关系。通过研究这些关系，可能会推断出用户身份，收集设备状态信息，进行网络侦察，并归纳出组织采用的安全防护措施和工具的特点。	专注于网络指标的交换，如与威胁源起方的 C&C 制基础设施、恶意 URL/ 域名和演示服务器有关的目的 IP 地址。在信息共享前，对包含目标系统的 IP、MAC 地址或公司注册地址的网络指标，以及能暴露内部网络结构的指标或端口 / 协议进行过滤或进行匿名化处理。
抓包（PCAP）	除了前面讨论的网络指标，未加密或解密数据包可能包含验证凭证和敏感组织信息，如个人验证信息和知识产权。	抓包文件不易处理，因为网络指标可能同时呈现在报文头和载荷中。例如，抓包文件可能显示协议（例如 DHCP 协议、地址解析协议（ARP）、文件传输协议（FTP）和 DNS 协议）和运行在网络栈各层中的应用。这些协议和应用生成的网络信息可能被抓取，需要进行过滤或匿名化处理，防止敏感信息泄露。 在信息共享前，通过提取与特定安全事件或事件模式调查相关的报文对抓包文件进行过滤： • 与特定网络会话相关（即特定 IP 地址之间的信息交换） • 发生在特定时间内 • 特定的目的端口或源端口 • 使用特定的网络协议 修改包含个人验证信息或其他敏感信息或与安全事件或相关事件特点不相关的载荷内容。 当编辑网络信息或进行匿名化处理时，保留足够的信息以支持对抓包文件内容进行有意义的分析，是很重要的。
网络流数据	网络流数据包括以下信息： • 源 IP（如发送者） • 目的 IP（如接收者） • 端口和协议信息 • 字节数 • 时间戳 如果不能进行有效的匿名化处理，网络流量数据可用于识别特定用户，观察用户行为（例如用户访问过的网站），显示应用和服务的使用模式，以及网络路由信息和数据量。	在共享网络流数据前，组织应考虑使用加密加密、保留前缀和 IP 地址匿名技术修改部分会话历史记录，以避免出现网络标识或具体会话跟踪中的具体字段（例如时间戳、端口、协议或字节数）。为了从信息中获得最大价值，使用一个能够转换网络流数据而不破坏参照完整性的工具是很重要的。网络流分析和关联操作通常要求 IP 地址替换和转换操作在文件内或不同文件间保持一致。不采用一致替换策略的匿名技术可能会减少或消除分享这类信息的价值。
钓鱼邮件示例	邮件头可能包括以下信息： • 邮件代理 IP 地址 • 主机或域名 • 邮箱地址 邮件正文可能还包括个人验证信息或其他类型的敏感信息。	组织应对邮件样本进行匿名化处理，并删除与描述相关安全事件或普通事件无关的敏感信息。
系统、网络和应用日志	日志文件可能包括个人验证信息或其他类型的敏感信息。日志数据可能包含 IP 地址、端口、协议、服务和 URL，以及连接字符串、登录凭证、财务交易的部分内容或在 URL 参数中捕获的其他活动。	组织应对 IP 地址、时间戳、端口和协议进行匿名化处理并删除与描述相关安全事件或普通事件无关的敏感信息。在共享日志数据前，有必要对包含识别信息（如会话或用户 ID）的 URL 进行过滤。特定格式的应用日志可能需要编辑和匿名化处理。
恶意指标和样本	虽然组织不太可能在恶意软件指标或样本中见到个人验证信息，但是个人验证信息或其他敏感信息的显示取决于恶意软件有多强的针对性和所使用的收集样本的方法。	组织应删除个人验证信息或与描述相关安全事件或普通事件无关的敏感信息。

3.4.2 共享标记

标记共享威胁信息处理要求的方法有很多。这些标记能够识别可能不适合公开发布或需要特殊处理的未分类信息。运用于威胁信息的标记可以传达特定的处理要求，识别敏感数据元素和应在共享前加以修改的信息。鼓励组织为共享威胁信息提供明确的处理指南。同样地，威胁信息的接收者应遵守源组织处理指南中描述的处理、具名、传播和存储要求。

表 3-3 中介绍的流量指示灯协议（TLP），提供了表达共享标记的框架。[9]

9 NIST SP 800-122 [7] 中将个人验证信息的影响级别定义为判断个人验证信息敏感度的有效工具。

表 3-3：流量指示灯协议

颜色	何时使用?	如何共享?
红色	当另一方不能有效响应信息，并且如果信息使用不当可能影响自己的隐私、名誉或运营时，源可以使用 TLP:RED。	接收者不能将交流、会议或会话中透露的 TLP：RED 信息分享给与交流、会议或会话无关的任何其他方。
琥珀色	当信息需要支持以做出有效响应，但如果在组织外共享，可能会有影响隐私、名誉或运营的风险时，源可以使用 TLP:AMBER。	接收者可以与组织内部成员共享 TLP:AMBER 信息，但应根据响应需求控制范围。
绿色	当信息有利于提高所有参与组织以及更广泛的社团或行业同仁的意识时，源可以使用 TLP:GREEN。	接收人可以与行业同仁组织共享 TLP:GREEN 信息，但不会通过公开渠道去共享 TLP:GREEN 信息。
白色	当按照公共发布的适用规则和流程，信息的可预见的被滥用的风险最小或者为零时，源可以使用 TLP:WHITE。	TLP:WHITE 信息可以不受限制地分发，受版权控制保护。

TLP 协议是一系列的颜色编码限制，表明一项记录适用于哪些限制。在 TLP 协议中，红色是指最严格的规则，可共享的信息只能在特定的交流或会议范围内，甚至不能在参与者自己的组织范围内。琥珀色、绿色和白色所代表的规则依次宽松。

反网络钓鱼工作组（APWG）提出了一个共享标记的表达模式。APWG 模式描述了可扩展的分级标记系统，可用于表述共享信息的分布限制。标签可用来表示那些可以或不可以与之共享信息的人（如只与接收人共享、与受影响的各方共享，或没有限制）和表示其他注意事项（例如允许匿名）。

对于一些威胁信息，收集方法可能被视为机密或专有的，但实际观察的指标可以共享。在这种情况下，组织可能会用撕裂报告（tear line reporting）的方法。撕裂报告的方法是对报告进行整理，不同敏感度的信息不会混在一起（例如指标信息和收集方法分别呈现在文档的不同部分中）。通过这种架构的报告，组织能够很简单地生成只包含指定接收人被授权接收的信息的报告。

组织应仔细选择或者制定表示共享标记的方法。不管组织如何表示共享标记，都应确保将共享标记应用到威胁信息的流程已形成文件并得到批准，并且负责指定共享标记的人员训练有素。

3.4.3 网络威胁信息共享与跟踪流程

随着时间的推移，经过各种网络安全活动，组织可累积大量来自内外部的威胁信息。虽然跟踪数据源很有挑战性，但是这对于保护信息责任人和确保使用信息的组织能够履行数据保护的法律承诺是很重要的。此外，保存数据源对于分析目的也是极为重要的，可分析得知信息提供者，以及信息的收集、转化或处理方式。有了这些信息，组织可以根据共享信息得出结论。

组织应制定流程，允许在及时共享威胁信息的同时能够履行保护潜在敏感数据的义务。这些流程应尽量平衡无效共享与保护不力的风险。组织的信息共享和跟踪流程应该是：

- 确定可以随时与可信方共享的威胁信息。
- 制定对可能包含敏感信息的威胁信息的评审、过滤和保护流程。
- 在可能的情况下实现威胁信息处理和交换自动化。
- 描述信息处理标记的应用、监控和执行方式。
- 在需要时容许匿名信息交换。
- 跟踪威胁信息的内外部源头。

这些流程应列举出所有利益相关主体的角色、职责和权限（包括范围和持续时间）。这些流程可获得有效的权力转让和共享信息传达，并在需要时，允许与批准的外部群体合作。

3.5 加入共享社团

当评估潜在的共享合作伙伴时，组织应了解其组成现有威胁信息资源的源头，以及可提供弥补组织态势感知已知空白的可操作信息的源头。由于共享社团可能只专注于某一特定类型的网络威胁信息的交换，组织

可能需要参与多个信息共享论坛，以实现信息共享目标。

威胁信息可以从公共和私有共享社团、政府知识库、商业网络威胁情报源和开源中获取。共享社团通常具有共同的特点或兴趣。社团的组成可能是基于地理区域、政治边界、行业部门、商业利益或威胁空间（例如专注于网络钓鱼攻击）。很多社团都是跨国和全球范围的。潜在的共享合作伙伴包括信息共享分析中心(ISAC)、国内外计算机紧急响应小组（CERT）或计算机安全事件响应小组（CSIRT）、威胁和漏洞知识库、执法机构、产品厂商、管理安全服务提供商、互联网服务供应商、供应链合作伙伴、行业同仁、业务伙伴和客户。

一些社团是非正式的、开放的、自发组织的团体，在很大程度上是自愿合作运营。这些社团的成员往往并不固定（即没有正式固定的会员），有时是匿名的。他们可以保持充分的自主权，接受最小的集中协调。这些社团一般遵循基本的行为规则，而不是正式的协议。在这样的社团中，成员自愿随时在社团中发布威胁信息，并且个人负责确保他们提供给社团的内容是适合共享的。希望使用信息的组织可以订阅或使用社团提供的各种交付机制（例如 web 服务、电子邮件或短信提醒和 RSS 订阅）来访问。这样的共享社团一般不保证成员提供数据的质量和准确性，信息的可信度取决于提交者的声誉（如果知道的话）。

相比之下，正式的共享社团可能会定义特定的成员规则。如下：

- 对机构的资格要求（例如必须在一个特定的行业部门内）
- 对个人的资质要求（例如必须承担企业范围内的安全职责）
- 提名或赞助要求（即代理信任）
- 会员试用期要求
- 会费结构
- 社团提供 / 接受的威胁信息种类
- 社团支持的标准交付机制、格式和协议
- 所要求的组织网络安全能力

正式社团可能会通过要求或赞助的形式招收会员，会员也会受到审查。正式社团的会员一般比非正式区更稳定。正式社团的信息交流往往遵守服务水平协议（SLA）、保密协议和其他明确列出成员责任和参与组织的协议。一些社团收取会员年费，以支付社团的服务和行政花费。不同社团的会费也不尽相同，会费结构是分级别的，即提供不同级别的会员身份和服务。

在签订信息共享协议前，需要获得组织各方的批准，包括：

- 负责监督信息共享活动和控制必要的资源以支持组织信息共享目标的领导团队的批准
- 法律团队或有权承担该项义务者的批准
- 隐私官员和在收集、提取、储存、分析、发布或保护威胁信息方面发挥作用的其他相关利益主体的批准

在选择共享社团时，应考虑到在社团内共享的信息类型、社团的结构和动态，以及吸收和维护会员的成本。当评估如何在社团内共享信息时，组织应该考虑以下问题：

- 社团内共享的威胁信息是否相关？是否能够提供组织威胁环境的有意义见解，为现有的威胁信息提供补充？
- 社团内分享的威胁信息是否可执行？
- 社团是否有适当的机制来接受匿名提交的网络威胁信息，并能够保护提交者的身份？
- 传播的威胁信息是否及时可靠，并且质量一贯的好？
- 社团使用的信息交换格式是否与组织使用的基础设施和工具兼容？
- 考虑到社团传播数据的频率和量级，组织是否有吸收、分析和储存这些信息的能力？

- 除了在社团内共享的信息，还应考虑社团的动态和参与者，包括：
- 社团的规模和组成是怎样的？（例如参与人数、信息提供者和信息使用者）
- 社团活跃度怎么样？（例如每天的信息提交或请求数量）
- 是否招收和审查社团会员？如果是，怎么招收和审查呢？
- 社会成员的技术能力和熟练程度如何？
- 社团的管理模式是什么？
- 会员制的初始成本和维护成本是多少？
- 社团使用的是什么共享协议？
- 共享协议是否符合组织的目标和业务规则？

研究共享社团时，鼓励组织与目前或以前的会员进行谈话，了解他们作为社团参与者的各种经历。这样的谈话可以提供额外的洞察力，并帮助组织评估未来社团的可信度。

3.6 为信息共享活动提供持续支持的计划

为了确保信息共享活动能够得到持续支持，组织应制定计划，描述如何维护信息共享基础设施，以及如何为用户提供支持。计划中应确定支持人员、基础设施和以下流程：

- 收集和分析内外部来源的信息的流程
- 获取和部署防护措施的流程
- 获取和部署监测与风险检测基础设施的流程

要确保以下几项：（1）确保人员、基础设施和培训资金的充足性，为数据收集、存储、分析和传播提供持续的业务支持；（2）确保技术更新；（3）确保社团参与所需的会费或服务费。虽然参与信息共享活动需要持续的资金支持，有效利用威胁信息可以避免受到成功攻击后花费更大的成本。

4.0 参与共享关系

通常，组织参与信息共享社团包括以下部分或全部活动：

- 参与持续沟通（第 4.1 节）
- 使用和响应安全告警（第 4.2 节）
- 使用指标（第 4.3 节）
- 组织和存储指标（第 4.4 节）
- 产生和发布指标（第 4.5 节）

以下章节将详细描述这些活动。刚开始开展威胁信息共享的组织应初步选择一两个重点关注的活动，并在其信息共享能力日趋成熟后考虑增加额外的活动。无论组织的信息共享成熟度如何，重要的是要明白信息共享应该是增强组织的基本网络安全能力，而不是取代后者。

4.1 参与持续沟通

信息共享社团采用不同的沟通方式与成员分享威胁信息。大多数组织都能够通过电子邮件列表、文本告和门户网站接收威胁信息，而不用专门为信息共享进行基础设施投资。虽然通过这些传递渠道接收到的内容可能需要手动处理（例如，“剪切和粘贴”到工具中）。对于拥有支持标准数据格式的安全工具的收件人而言，使用标准的数据源可以实现威胁信息采集、处理和使用的半自动化。其他的信息共享方法，如会议和研讨会，需要专门的工作人员，还会要求出差。积极生成和共享威胁信息的组织可能会产生更高的沟通成本。沟通可以是事件驱动的（即对威胁源起方的动作或行为的响应）或周期性的，如双周评论、远程会议和年度会议。

使用人类可读格式传递的信息的详细程度、数量和频率因信息共享社团不同而不同。一些社团寻求交付潜伏期最短的最新威胁信息。与之相反，一些信息接收人使用威胁信息了解趋势和进行分析时可能更喜欢汇总数据，并且可能不需要近实时交付的详细信息。为了减少生成的消息数，共享社团有时提供摘要订阅（即定期编译信息）而不是接收每条信息。

最近已加入信息共享社团的组织可能需要花时间把新的威胁信息源整合到现有的网络安全实践中，配置安全工具，并培训决策者如何诠释威胁信息和采取相应行动。在上升期，组织应参照社团提供的最佳实践指南，通过与经验更丰富的成员互动进行观察和学习，以及查询社团支持资源（例如社团知识库、常见问题解答和博客）。同时，社团赞助的培训活动为尚不成熟的组织和经验不足的员工提供了从熟练的从业者那里获得实用见解的机会。组织还应制定人才招聘和人才保留流程，减少人员流失，以形成共享社团和组织之间可信的专业关系。对熟练员工的保留减少了机构的知识损失，并能保护培训投资。

持续参与共享社团对促进与其他成员的关系并不断改进做法是必不可少的。积极参与社团赞助的电话会议和面对面会议的组织能够更好地建立起与其他成员的信任关系，从而能够有效地合作。

4.2 使用和响应安全警报

信息共享社团可能会发布安全警报，为社团成员提供关于新的漏洞、攻击和其他安全问题方面的通知。一般在安全告警中出现的字段包括 US-CERT 警报、NVD 漏洞公告和供应商的安全公告，包括 [10]：

- 包括指标的简要概述 / 执行摘要和详细描述
- 受影响的平台（例如操作系统、应用和硬件）
- 预估影响（例如系统崩溃、数据泄露和应用劫持）[11]
- 严重度分级（例如常见漏洞评分系统，CVSS [11]）

10 数据来源：美国计算机紧急响应小组（US-CERT）。

11 更详尽的可能影响，参见 MITRE 通用弱点枚举（(http://cwe.mitre.org/)和通用漏洞披露(http://cve.mitre.org/)中的列表。

- 缓解措施，包括永久性修复和 / 或临时解决方案
- 更多信息参考
- 警报元数据（例如警报创建和修改日期、致谢）

一旦收到安全警报，组织应首先确定警报来源是否可信、可靠。当警报来自未知或不可信来源时，进行额外的审查和 / 或在采取行动前再次确认是有必要的。如果警报被认为是可信的，组织应确定自己是否拥有或操作了任何在警报中列出的受影响的系统、应用程序或硬件；如果是，组织应做出恰当响应。

在做出响应时，组织应通过评估警报的严重程度、组织内受影响系统的数量、攻击可能对组织关键职能的影响以及部署缓解安全控制措施对操作的影响等因素，了解警报的整体影响。此等评估可为确定响应措施的优先级和具体方法提供参考。响应措施包括这些活动，如从告警中识别和提取指标、使用指标来开发和部署检测特征、改变配置、应用补丁、通知威胁人员，以及实施或加强安全控制措施。如今，指标提取和响应措施在很大程度上都是手动过程，但有很明显的自动化需求。手工处理指标耗时繁琐、容易出错，且缓慢；而自动化操作可以让分析师专注于信息理解，而不是乏味的数据操作。

4.3 使用指标

对外部指标的使用通常是一个多步骤过程，包括以下活动（并非全部）：

- 验证：通过数字签名、加密哈希或其他手段验证指标内容的完整性以及指标的来源。
- 解密：将加密的指标文件或数据流恢复成初始格式。
- 解压缩：对压缩的指标文件、存档文件（如 zip 或 tar）或数据流进行解压缩，以获取这些文件。
- 优先级排序 基于以下因素处理指标 相对重要性、数据源的感知价值、数据的整体置信度、运行要求(规定应按某种顺序处理数据源）、将数据转换为可行信息所需付出的努力，以及其他因素。
- 内容提取：解析指标文件提取组织所关心的指标信息。
- 分类：查看指标元数据，确定其安全状况以及处理要求。敏感信息或需加密存储、更严格的访问控制以及分发限制。诸如恶意软件样本之类的内容，在处理时可能需格外谨慎，防止将恶意代码点带入生产网络。

一般，这些活动按上述的描述顺序执行，不过这一顺序因具体运行或安全要求不同而异。

建议组织适时自动化这些活动，以加快指标利用并尽量减少人工干预。当进行指标的非正式共享（如邮件）时，对指标进行优先级排序和分类就显得非常重要，而这一工作应由接收人完成。

理想情况下，指标应具备以下特征：

- 及时性：指标的传输延时越低，接收人就越有充足时间作出合理回应。这一时间取决于威胁特征，包括危险级别、速度、传输难易度、目标基础设施、TTP，以及源起方的能力。某些决策周期或要求，指标在数秒或数分钟内完成传输以阻止行动迅速的源起方；而有的威胁的有效解决可能需几小时、几天，甚至是数月前的指标。
- 相关性：对于接收人来说，那些适用于他们的运营环境，并能够消除组织面临的潜在威胁的指标更为有用。他们可基于这些指标更有效分析特定威胁所带来的风险。
- 准确性：含义清晰、准确以及全面的指标最为有用。含义不准确或不完整的信息会引发不确定性、妨碍关键行动、带来不必要的操作、导致无效响应或使人产生安全错觉。
- 针对性：指标应清晰描述检测到的事件，使接收人能够基于此检测威胁，将误报 / 漏报率降至最低。
- 可行性：指标应提供充足信息，清晰描述背景环境，使接收人可基于此做出合适的回应。

实际使用过程中，指标还应具备以下特征（并非全部）：例如，由于接收人缺乏检测手段、信息缺失或威胁发生变化，指标无法实现。不过，这并不意味着这些指标对于组织来说毫无价值，而是可通过数据聚合、

与其他威胁信息关联以及额外分析而变得更丰富。随着指标的成熟，对组织来说，分享新观点非常重要，因为这可使整个社团受益。

组织可通过多种方式使用内部和外部生成的指标达成目的，如：

- 重新配置防火墙、入侵检测系统、数据泄露防护系统和 / 或其他安全控制措施，以阻断与指标（如黑名单上的地址相关的链接）相匹配的活动或上报告警。
- 配置安全信息和事件管理方案或其他日志管理相关的系统，协助安全日志数据分析。
- 利用指标，如搜索键值对，扫描安全日志、系统或其他信息源，识别可能已经被入侵的系统。
- 调查事件或潜在事件时，找到匹配的记录进一步了解威胁，加速事件响应和恢复操作。
- 通告人为安全分析结果。
- 为员工提供有关威胁特点的培训。
- 识别那些可能会导致安全控制措施长期变动的威胁趋势。

一般情况下，组织使用外部指标的意愿深受对其信任程度的影响。来自可信源的指标可能会立即被用于威胁检测和响应。而对于那些来自非可信源的指标，使用前，需对其进行独立验证、额外研究或测试。指标的使用还可能受到其他因素的影响，如组织对业务中断的容忍度。对于某些组织来说，虽然安全是第一位的，但正常业务活动的偶尔中断是可以接受的。而有的组织，服务可用性至关重要，潜在恶意活动可能只触发监控。

组织应认真考虑所接收的指标的特点，采取基于风险的方法确定如何最有效地利用指标。组织可能会发现，某个指标可能只在特定场景下非常有用，而在其他情况下未必奏效。最终，应由每个组织自己决定如何最有效地利用指标。

4.4 梳理与存储指标

组织可能会从各类源收集指标，包括开源知识库、商用威胁数据源以及外部合作伙伴。收集之后，需根据使用方式将这些指标存储在知识库中。自由表格非常方便灵活，适于创建工作便条和指标元数据。并且，结构化数据库对于存储、梳理、跟踪、查询和分析所收集的指标来说非常有用。

知识库中记录的每条指标一般包含以下信息：

- 指标来源
- 指标使用和分享规则
- 指标收集日期或时间
- 指标有效期
- 是否存在指标关联的攻击，针对于特定组织或部门
- 通用漏洞枚举（CVE）、通用配置枚举（CCE）以及通用缺陷列表（CWE）中是否存在指标关联的记录
- 指标关联的团队或源起方
- 任意关联源起方的别名
- 源起方常用 TTP
- 指标关联源起方的动机或意图
- 关联攻击所针对的员工或员工类型
- 攻击的目标系统

由于指标知识库颇具诱惑力，因此很容易成为攻击目标。为防止攻击，应采取合理措施确保使用合适的

安全实践保护指标知识库，如限制访问，仅允许授权用户进行访问，定期备份知识库，维护知识库系统的操作系统和应用，安装当前补丁和采用安全配置，以及生产用于知识库[12]的内部软件时采用软件开发最佳实践。

组织应制定指标（通常还包括威胁信息）部署政策和规程。这些政策和规程应明确数据保留要求，以确保指标信息在短期（在线）和长期（离线）内可用。一旦出现指标相关的威胁信息，指标信息的处理和保存要求就可能会有变动。例如，应收集和保存安全事件调查过程中获取的威胁信息证据。收集和保存时，应采用托管要求的数据保存追踪链的最佳实践并遵循证据提交法规。如欲了解有关托管链和保持信息完整性的取证技术的详细信息，请参见 NIST SP 800-86 [12] 以及 NIST SP 800-61（第三版）中的第 3.3.2 节。

对于那些无需用作威胁证据的指标，组织应确定合理的保存政策[13]。虽然保存这些威胁信息会产生一定费用，但这些信息颇具参考价值，也有助于共享社团的新成员与合作伙伴了解各类源起方和攻击类型的持续发展与演进。此外，还有其他方面的考虑，如由于财务、法律、合同或监管方面的要求，这些数据只能保留数月或数年。一旦确认了数据保留计划，组织按适用的政策归档或销毁指标。

4.5 编制和发布指标

很多组织只是使用指标,而还有一些组织,通常指具备更高级安全能力的组织,选择制定和发布自己的指标。组织可通过提供威胁信息获得很大收益。例如，组织可获得更强的专业技能，帮助其他组织在其环境中更有效地应对威胁，并与其他社团成员建立信任。这对于构建和维持威胁信息流来说至关重要，并最终可使提供威胁信息的组织受益。共享威胁信息的提供商须决定共享信息应使用何种元数据（如果有），采用何种数据格式，如何处理敏感数据，以及如何在一段时期内维护信息共享规则。后面的章节将介绍这些内容。

4.5.1 丰富指标

组织在编制和发布指标时应尽可能提供元数据，为每个指标提供上下文，描述指标应如何使用、理解，以及它与其他指标的关系。元数据可能也包含敏感性标识和来源信息（如使用的数据获取工具、数据处理方式和数据收集人）。在指标新建、聚合或丰富后，应重新评估其敏感性和分类。这是因为聚合、关联或丰富的过程可能对信息进行了重新识别（如利用数据挖掘技术）或提升了信息的敏感性，因此可能还需增加额外的数据处理限制。

此外，指标的编制流程应包括指标发布、指标与相关元数据更新、错误或无意误共享的信息撤回机制。应增强并测试所有自动化机制，防止其沦为威胁源起方手中的攻击向量。共享指标的组织应提供反馈机制，这样参与分享的合作伙伴就可以提交错误报告，提供改进意见，或要求提供指标相关的额外信息。这样的反馈对于丰富、发展与优化群体内部共享的指标发挥着重要的作用。

社团内共享的某些信息可能会标记为“当前正在调查中”，要求社团成员不得在社团之外共享此类信息。此外，社团成员也不应主动收集带有此类标记的信息（如在可疑网站检索恶意软件样本或查询可疑主机名的 DNS 设置），因为这些行为可能会使信息落入潜在源起方手中或妨碍调查活动。有时，人们可能会低估这些信息的发布与调查限制。鉴于此，应提供一种机制用于修改此类标记或添加修订的标记，如“于 2015 年 12 月 20 日降级为 GREEN”。

4.5.2 标准数据格式

利用标准数据格式进行指标传输不仅增强了互操作性，也加快了信息传输速度。非结构化格式（如文本文档和邮件）适用于高级威胁报表以及指标信息和由安全人员（而非机器）读取的其他资料的点对点传输。针对对时间要求严格的指标，如自动配置防火墙，阻断特定的通信，建议使用标准数据格式，将人为干预降至最低。评估数据传输的标准格式时，应选择具备以下特征的格式：应用广泛、可扩充（如花费最小的工程和设计工作量集成新数据元素或特性）、可扩展并可提供必要的数据安全特性。

12 NIST 软件保障度量和工具测量项目旨在制定标准的测量措施和方法实现软件保障。
http://samate.nist.gov/index.php/SAMATE Publications.html

13 联邦机构应遵守国家档案和记录管理局（NARA）的通用保存期限表以及机构特定的保存政策。

4.5.3 保护敏感数据

组织发布的指标可能会涉及敏感信息，因此防止未经授权的披露或修改非常重要。可采用各种方法保护指标数据，如网络通信加密、认证和授权机制、知识库安全加固。如果使用知识库，组织应编写库的服务级别协议（SLA），规定期望的可用性、安全状态要求及可接受的用户策略。编制包含敏感信息的指标时，应遵循合理的共享规则（参见 3.4 节），且应只在社团成员内共享信息，并保证这些成员值得信赖，遵循共享规则以及同意遵循此类规则。

附录

附录 A 网络威胁信息共享场景

本附录介绍了很多场景，描述实际应用环境中的威胁信息共享。这些场景旨在说明信息共享与协调如何能提升组织网络安全能力的效率和有效性。并且，这些场景仅是信息共享与协同的少量潜在应用场景。

场景 1：针对特定行业部门的国家级攻击

国家级攻击通常会在数月时间内锁定特定行业部门的公司。此类攻击通过发送针对性邮件，并在邮件附件包含一个软件漏洞利用程序来实现。如果用户打开附件，恶意软件就会侵入该用户的系统。恶意软件成功入侵系统后，将重新配置系统，使其连接到命令与控制服务器以及威胁源起方操控的其他基础设施，从而接收额外的指令、下载其他恶意软件，并导致数据渗漏。

此行业部门的很多公司参与了一个正式的威胁信息共享组织。该组织通过一个中央论坛发布所检测到的威胁的相关信息。该论坛上的帖文描述了威胁检测和防御详情，包括钓鱼邮件发件人地址，从攻击中收集的恶意软件样本、有关攻击者所使用的漏洞威胁程序代码的分析、攻击者的命令与控制服务器相关的 IP 地址与 URL，以及攻击涉及的其他基础设施。

一旦某个公司的安全团队检测出新攻击会立即与论坛内的其他公司分享攻击信息。论坛中的公司 A 具备高级恶意软件分析能力，并能够通过分析公司 B 在论坛上分享的恶意软件样本，进一步挖掘威胁源起方及其命令与控制基础设施的特征。然后，公司 A 分享其通过对恶意软件的深入分析得出的攻击信息。在这个场景中，公司 B 分享恶意软件样本，而公司 A 提供恶意软件分析，使社团内的其他组织获益，让其能够快速有效地检测并防御类似攻击。也就是说，一个公司分享所遭遇的攻击后，通过对此攻击的进一步分析，有助于其他公司防御此类攻击。

场景 2：行动分析

来自商界公司的网络安全分析师在过去的几年中一直通过在线论坛分享指标和恶意软件样本。每个公司均独立进行攻击分析，并观察一段时间内数组攻击事件的相同特征，如采用的恶意软件的类型、命令与控制通道的 DNS 域以及其他技术指标。有了这些发现，分析师猜测，这些攻击并非无序，而是一系列协调配合行动中的几个步骤。

论坛成员经常参与技术交流会议，分享数据、见解以及各类攻击的分析。通过数据聚合和联合分析，这些成员能够判断哪些活动可能由常见威胁源起方发起，或是各源起方协作的结果。本场景展示了数据融合与分析如何帮助揭露威胁源起方采取的集体行动和活动并识别攻击活动中特定源起方所采用的 TTP。

场景 3：针对行业部门的分布式拒绝服务（DDoS）攻击

黑客活动分子团伙精心选取了一组公司，对其发起大规模 DDoS 攻击。该团伙借助由其成员控制一个分布式僵尸网络，实现松散协作。在此次攻击的目标中，其中一个公司通过分析僵尸网络生成的流量，指出这些攻击者使用了当前非常流行的 DDoS 工具的一种变体。

此次攻击所针对的公司为 ISAC（信息共享和分析中心）成员，利用 ISAC 的讨论门户创建了工作组，旨在同心协力终止攻击。工作组与 ISAC 的执法部门保持联络。该部门将与联邦和国际机构共同合作，协助调查，获取法庭指令关闭攻击者系统。

工作组与各 ISP 保持联系，为其提供信息，协助识别其网络地址接收的异常流量。各 ISP 将协助受影响的公司和执法人员识别上游和下游流量源，更改路由，并限制这些攻击源的数据传输速率。借助 ISP 收集的网络流量，执法机构可发现命令与控制服务器，没收其资产，并识别黑客分子团伙中的成员。

受害公司召开技术交流会议后，数家公司决定寻求内容分发供应商的帮助，分发其网络业务，增强其业务系统抵御未来 DDoS 攻击的能力。

场景 4：财务会议遭遇钓鱼攻击

一网络犯罪团伙在公开发布的与会者名单上，锁定了攻击目标，通过发送一系列钓鱼邮件发起攻击。该团伙能够判断哪些与会者来自目标组织的会计团队，也就是确定谁有权授权支出或资金转账。通过在钓鱼攻击过程中传输针对性的恶意软件，该团伙试图入侵机器和账户，完成未授权的电子支付并将资金转账到海外企业。

其中一家公司检测出了针对其会计团队的钓鱼攻击，并在攻击调查中发现钓鱼邮件的收件人均参加了 6 个月前的财务会议。该公司的计算机事件响应团队（CSIRT）联系了会议组织者以及参与此次会议的其他组织的代表。攻击波及的组织安排了一次电话会议，分享此次攻击的详细信息，包括邮件标题、附件及所嵌入的 URL。财务会议的其他与会者基于这些分享的指标审查了其邮件和网络流量日志，确定可能被入侵的主机。这些公司一致同意通过非正式的邮件列表持续开展合作并分享未来攻击的相关信息。

场景 5：业务合作伙伴的入侵

公司 A 和公司 B 是业务合作伙伴，建立了网络连接传输业务信息。一个网络犯罪组织入侵了公司 B 的一台服务器，并将对该服务器的访问做为基石发起针对公司 A 的内部服务器的攻击。公司的运营人员发现了此次异常事件并上报了安全团队。安全团队发现此次攻击来自公司 B 的系统。业务合作伙伴连接协议规定，公司 A 将异常流量通知公司 B，且两公司根据制定的流程联合回应此次突发事件。公司 A 的事件响应团队描述所检测到的攻击活动，允许公司 B 的团队隔离受影响的服务器，开展调查，识别攻击源以及其他潜在受损设备。调查表明，攻击者利用

Web 应用的软件缺陷非法获取了服务器的访问权限。公司 B 的应用开发团队修改了存在漏洞的代码以修复此漏洞，安全运营团队又采用了其他日志和入侵检测特征，识别未来的类似攻击。

由于两公司的安全团队已制定了有关联合响应的协议和流程，建立了联系和信任关系，且非常熟悉彼此的网络和运营，因此他们能快速做出响应并恢复网络。

场景 6：美国计算机应急响应小组提供指标，接收反馈

美国计算机应急响应小组（US-CERT）从各类独立数据源接收信息。很多位于美国的服务器正被用于发起针对美国公司的网络攻击。目前了解到一个国外源起方控制了被入侵的服务器。US-CERT 识别出这些被攻击的公司并指出这些公司大部分属于航天业。US-CERT 联系了这些公司的安全团队并分享了初始威胁信息，包括 URL、恶意软件以及正在被威胁源起方利用的漏洞。

借助这些指标，很多受影响的公司能够检测针对他们基础设施的攻击并采取必要措施阻止这些攻击。在攻击调查过程中，这些公司也能够发现新指标或为 US-CERT 提供新的攻击环境，而 US-CERT 会在对这些指标源进行匿名化处理后将其分享给其他公司，实现更全面的威胁响应。

场景 7：某零售商店未能共享威胁信息

一个大型零售店遭遇了来自犯罪组织的网络攻击。在这次入侵事件中，数百万信用卡号和账户信息被盗，而该零售店在数周内竟然对此毫无察觉。该零售店仅是依靠自身的安全检测能力处理此次事件，并未共享威胁信息。而此次针对性的威胁非常复杂，且使用了自定义恶意软件。事实证明，该零售店仅依靠其自身的安全能力根本无法应对。

而此次入侵事件是信用卡公司在调查一系列的信用卡诈骗事件时发现的。这些诈骗事件的共同点是，购买活动均来自该零售店。信用卡公司就此事件联系了执法部门和该零售店，零售店才就此展开调查。

此次入侵造成了巨大损失。零售店向客户通告了此次个人信息失窃事件，但并未详细说明此次攻击的发起过程。结果，其他数家零售店在几周后也遭到了使用同一方法发起的攻击。如果这些零售店积极参与威胁信息共享，此次零售店、客户、信用卡发行商的财务损失本可以避免，至少可减少损失。

附录 B 术语表

本附件列出了文中出现的部分术语的定义。

源起方	请参见“威胁源起方”。
告警	亦称为公告（advisory/bulletin）和漏洞说明（vulnerability note），一般是对用户发布的有关现有漏洞、攻击及其他安全问题的简要技术通知。
网络威胁	请参见“威胁”。
指标	指可预示攻击即将或正在发生、或可能出现入侵的技术构件或可观测事物。
可观测事物	网络或系统中的事件（正常或恶意）。
策略、技术与过程（TTP）	威胁源起方的行为。战术是对行为的概括描述，技术是对战术涉及行为的具体描述，程序是对技术的进一步、更详细的描述。
威胁	指以下情形或事件：对信息系统的未授权访问、损害、信息披露或修改和 / 或拒绝服务可能会对组织运营（包括任务、职能、形象或声誉）、组织资产、个人、其他组织或国家造成潜在负面影响。 [2]
威胁源起方	带来威胁的个人或组织。
威胁信息	威胁信息指与威胁相关、可帮助组织防护威胁或检测威胁源起方活动的任何信息。威胁信息主要包含以下几类：指标、TTP（策略、技术与过程）、安全告警、威胁情报报告以及工具配置。
威胁情报	威胁情报指汇总、转换、分析、解释或丰富后的威胁信息，为决策流程提供必要上下文。
威胁情报报告	威胁情报报告是一种语言平实的文档，用于描述 TTP（策略、技术与过程）、源起方、针对的系统和信息的类型以及其他威胁相关信息。
威胁转移	源起方在发现安全预防措施及 / 或对策（如安全控制措施）后作出的响应，具体表现为改变攻击意图 / 目标的某个特征以规避和 / 或对抗该安全预防措施 / 对策。[2]
工具配置	对于搭建并使用工具提供的建议，这些工具为自动化采集、交换、处理、分析与使用威胁信息提供支持。

附录 C 缩略语

ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
CCE	Common Configuration Enumeration	通用配置枚举
CIO	Chief Information Officer	首席信息官
CISO	Chief Information Security Officer	首席信息安全官
CSIRT	Computer Security Incident Response Team	计算机安全事件响应小组
CVE	Common Vulnerability Enumeration	通用漏洞枚举
CVSS	Common Vulnerability Scoring System	通用漏洞评分系统
CWE	Common Weakness Enumeration	通用缺陷列表
DDoS	Distributed Denial of Service	分布式拒绝服务
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DIB	Defense Industrial Base	国防工业基地
DNS	Domain Name System	域名系统
FISMA	Federal Information Security Modernization Act	联邦信息安全管理法案
FTP	File Transfer Protocol	文件传输协议
GLBA	Gramm-Leach-Bliley Act	格雷姆 - 里奇 - 比利雷法案
HIPAA	Health Information Portability and Accountability Act	健康保险隐私及责任法案
IP	Internet Protocol	互联网协议
IR	Interagency Report or Internal Report	跨部门报告或内部报告
ISAC	Information Sharing and Analysis Center	信息分享与分析中心
ISP	Internet Service Provider	互联网服务提供商
IT	Information Technology	信息技术
ITL	Information Technology Laboratory	信息技术实验室
MAC	Media Access Control	介质访问控制
MOU	Memorandum of Understanding	谅解备忘录
NDA	Non-Disclosure Agreement	保密协议
NIST	National Institute of Standards and Technology	国家标准与技术研究院
NVD	National Vulnerability Database	国家漏洞数据库
OMB	Office of Management and Budget	管理和预算办公室
PCAP	Packet Capture	抓包
PCI DSS	Payment Card Industry Data Security Standard	支付卡行业数据安全标准
PII	Personally Identifiable Information	个人验证信息
PSIRT	Product Security Incident Response Team	产品安全事件响应小组
RSS	Rich Site Summary or Really Simple Syndication	简易信息聚合
SIEM	Security Information and Event Management	安全信息和事件管理
SLA	Service Level Agreement	服务级别协议
SOX	Sarbanes-Oxley Act	萨班斯 - 奥克斯利法案
SP	Special Publication	特别刊物
SQL	Structured Query Language	结构化查询语言
TCP	Transmission Control Protocol	传输控制协议
TLP	Traffic Light Protocol	流量指示灯协议
TTP	Tactics, Techniques, and Procedures	策略、技术与过程
UDP	User Datagram Protocol	用户数据报协议
URL	Uniform Resource Locator	统一资源定位器
US-CERT	United States Computer Emergency Readiness Team	美国计算机紧急响应小组

附录 D 参考资料

1. NIST SP 800-61，计算机安全事件处理指南（第二版）
   http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP800-61r2.pdf
2. NIST SP 800-30，“风险评估指南”（第一版） http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800 30 r1.pdf
3. 行政命令 12968，访问保密信息，http://www. gpo.gov/fdsys/pkg/FR- 1995-08-07/pdf/95-19654.pdf
4. 基于国防工业基地（DIB）网络安全 / 信息保障（CS/IA）计划的框架协议，联邦公报，
   http://www.gpo.gov/fdsys/pkg/FR-2013- 10-22/pdf/2013-24256.pdf
5. 管理和预算办公室备忘录 07-16，对个人验证信息的泄露做出响应，保障信息安全
   https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
6. 管理和预算办公室备忘录 07-16，网络测量和定制技术使用指南
   https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda 2010/m 10-22.pdf
7. NIST SP 800-122，个人验证信息机密性保护指南 http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
8. NIST SP 800-53，联邦信息系统与组织的安全与隐私控制措施（第四版）
   http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP800-53r4.pdf
9. 流量指示灯协议 http://www.us-cert.gov/tlp
10. 反钓鱼工作组，GitHub 项目站点：https://github.com/patcain/ecrisp/tree/master/schemas/apwg
11. NIST IR 7435，通用漏洞评分系统及其在联邦机构系统中的应用
    http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf
12. NIST SP 800-86，如何将取证技术集成至事件响应 http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
13. NIST SP 800-88，“介质清洗指南”（第一版） http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP800-88r1.pdf

网络威胁信息共享指南组织信息

NIST 特别刊物 800-150（第二版）

安全加社区

公益译文项目

2016

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。