《网络安全威胁信息服务能力集成技术要求》编制说明

一、项目背景

网络安全威胁信息正协同各类安全工具赋能企业安全运营建设，能够降低企业整体风险，但利用率却不高。已有威胁信息标准聚焦数据格式，忽略了威胁信息的使用场景、互联集成等技术要求。作为未来网络安全防御体系的关键组成部分，为了在众多的安全平台和安全产品之中更有效的集成威胁信息服务能力，从而帮助客户更好地利用信息，构建完整的威胁信息服务生态，有必要制定威胁信息服务能力集成技术标准，补上威胁信息使用的“最后一公里”。本标准以腾讯等企业优秀实践以及中国信息通信研究院等权威科研机构的研究成果为基础，打造当下和未来企业/组织及个人使用威胁信息服务能力作为技术指引。

在深圳市市场监督管理局指导下，粤港澳大湾区标准创新联盟发起本标准编制，腾讯公司牵头，参与单位包括中国信息通信研究院等。

二、工作概况

（一）任务来源

2023 年 9 月粤港澳大湾区团体标准《威胁情报能力集成技术要求》标准研制正式立项启动，并得到了深圳市市场监管局的大力支持。

标准化是网络安全威胁信息应用的必要前提，我国威胁信息的国家标准体系建设尚处于起步阶段，在未来将进一步

完善应用体系和机制，夯实威胁信息服务基础，赋能安全协同生态建设。针对不同规模企业，威胁信息服务能力可以根据需求去集成和应用。针对不同细分领域及行业，威胁信息服务能力的集成可以根据不同应用场景进一步细化。这都需要标准化的支撑和助力。

近年来，我国威胁信息服务市场保持着高速增长，相关厂商已经可以提供比较全面的威胁信息服务能力。与此同时，国家对网络安全工作的重视、以及企业对安全建设的需求，也大力推动了威胁信息服务的市场应用。集成威胁信息服务能力的安全产品逐渐出现在市场中，并被越来越多的企业客户所接受，具有非常广泛的应用前景。

（二）起草单位

腾讯云计算（北京）有限责任公司、中国信息通信研究院等，将包括产学研用等相关主体。

（三）起草过程

依据湾区标准制定程序，对起草工作组成立、标准征求意见稿起草与论证等重点工作阶段的时间节点和工作内容进行说明。

主要阶段包括：

（一） 标准研制预备会：2023 年 9 月 1 日，“粤港澳大湾区团体标准《威胁情报能力集成技术要求》标准研制预备会”成功举办。

（二） 立项： 2023 年 9 月 28 日，《威胁情报能力集成技术要求》粤港澳大湾区团体标准立项书经联盟执行委员

会批准，成功立项。

（三）2023 年 11 月，组织《威胁情报能力集成技术要求》线下讨论会，对标准范围、主要内容进行研讨。

（四）2024 年，组织多次标准讨论线上、线下会议，一致建议修改标准题目为《网络安全威胁信息服务能力集成技术要求》，更加贴合标准的目标和标准化对象。

（五）2025 年 6 月，讨论并修改阶段，通过不断交流、修订及补充，完善标准文本，形成标准征求意见稿。

三、编制原则和依据

编制组遵循“科学性、统一性、规范性”的原则，在编制过程中严格按照我国现行有效的国家标准和行业标准的要求，引用文件准确合理，文本结构严谨、逻辑清晰。

四、主要条款的说明

（一）范围

本文件规定了网络安全威胁信息服务能力集成方式、集成要求等内容。

本文件适用于各类安全产品、服务与网络安全威胁信息服务能力集成的设计、研发对接、运营等工作。

（二）术语和定义

本文件主要术语和定义。

3.1 威胁信息 threat information

一种基于证据的知识,用于描述现有或可能出现的威胁,从而实现对威胁的响应和预防。

注:威胁信息包括上下文、攻击机制、攻击指标、可能影响等信息。[来源：GB/T 36643-2018 《信息安全技术 网络安全威胁信息格式规范》]

3.2 威胁信息服务 threat information service
提供威胁信息的查询、分析、更新升级等服务的相关过程。

3.3 威胁信息服务能力集成 threat information service capability integration
能够将外部威胁信息服务能力进行接入、使用的过程和方法。

3.4 威胁信息服务能力需求方 threat information service capability demand side
需要集成威胁信息服务能力的组织。

注：例如安全厂商，在其提供的的防火墙、安全运营中心等安全产品中集成威胁信息服务能力。

3.5 威胁信息服务能力提供方 threat information service capability provider
提供威胁信息服务能力的组织。

3.6 威胁信息服务平台 threat information service platform
用于管理威胁信息并提供威胁信息服务能力的安全软件。

（三）基本要求

威胁信息服务能力的集成方式主要包括本地服务集成、云 API 集成、平台集成、威胁信息内容集成等方式。

五、国内外相关研究、技术标准

在标准方面，目前国际和国内在威胁信息领域的标准主

要聚焦在信息格式，如《信息安全技术 网络安全威胁信息格式规范》(GB/T 36643-2018)，主要定义了网络安全威胁信息的表达模型。目前还没有威胁信息服务能力集成方面的技术标准。已有标准与本标准在技术上形成互补的关系。

六、是否涉及专利等知识产权问题

无。

七、重大意见分歧的处理依据和结果

无。

八、实施标准的措施建议

建议本标准作为推荐性标准发布。

九、其他需要说明的事项

无。