ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团 体 标 准

T/GBA XXXX—XXXX

网络安全威胁信息服务能力集成技术要求

Technical requirements for Cyber security threat information service capability intergration

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

粤港澳大湾区标准创新联盟　发布

目　　次

前　　言 II
1 范围 3
2 规范性引用文件 3
3 术语和定义 3
4 缩略语 3
5 威胁信息服务能力集成方式 4
6 威胁信息服务能力集成要求 4

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由粤港澳大湾区标准创新联盟产业互联网委员会提出并归口。

本文件起草单位：。

本文件主要起草人：。

网络安全威胁信息服务能力集成技术要求

1 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。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3 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。

4 缩略语

API：应用程序编程接口（Application Programming Interface）
AppKey：应用程序密钥（Application Key）
IOC：威胁指示器（Indicators of Compromise）
IP：网际互连协议（Internet Protocol）
MCP：模型上下文协议（Model Context Protocol）
SDK：软件开发工具包（Software Development Kit）
SOC：安全运营中心（Security Operations Center）
TI：威胁信息（Threat information）
URL：统一资源定位符（Uniform Resource Locator）

5 威胁信息服务能力集成方式

5.1 概述

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。

5.2 本地服务集成

在威胁信息服务能力需求方（简称需求方）的本地，以集成 SDK、部署独立的 API 服务等方式，供需求方在产品开发过程中集成威胁信息服务能力。该集成方式主要用于对实时性要求比较高的串行威胁检测场景。

5.3 云 API 集成

威胁信息服务能力提供方（简称提供方）以云端 API 服务接口的方式（宜支持直接调用云端 API 或者通过 MCP 模型上下文协议调用云端 API），供需求方通过在线调用的方式集成威胁信息的能力。该集成方式主要用于对实时性要求不是很敏感的异步威胁检测场景。

5.4 平台集成

提供方将产生的威胁信息实时/离线更新到需求方的本地，以部署威胁信息平台的方式提供用户界面、API 等访问接口，供需求方在本地使用。该集成方式主要用于对实时性要求不是很敏感的异步威胁检测场景。

5.5 威胁信息内容集成

提供方提供威胁信息内容，需求方解析相关内容以应用威胁信息服务能力。该集成方式主要用于对实时性要求不是很敏感的异步威胁检测场景。

6 威胁信息服务能力集成要求

6.1 本地服务集成要求-SDK 方式

6.1.1 SDK 下载和安装要求如下：

a）根据提供方提供的地址，下载 SDK 软件包；

b）根据提供方的说明文档解压软件包到合适位置；

c）获取 SDK 的使用授权，并激活授权；

d）编译并调试运行 SDK 程序；

6.1.2 SDK 接口要求如下：

a）SDK 初始化接口：初始化 SDK 程序；

b）加载元数据接口：加载威胁信息检测接口用到的元数据到到内存映射中；

c）加载上下文数据接口：获取相关元数据的上下文信息；

d）释放 SDK 句柄接口：释放使用初始化 SDK 时创建的句柄；

e）获取证书文件信息接口：解析证书文件，获取证书文件内容，如 AppKey、数据类型、证书过期时间、产品类型等；

f）获取激活码信息接口：解析激活码文件，获取激活码文件包含的内容；

g）获取 SDK 版本信息接口：获取当前 SDK 版本号信息；

h）获取设备指纹接口：获取当前机器设备指纹，用于申请激活码等；

i）数据升级接口：用于数据升级，包括全量和增量的元数据、上下文数据升级；

j）威胁信息检测接口：用于检测用户输入的数据（IP、域名、文件哈希值、可疑文件等）的威胁信息情况，包括是否是威胁信息、威胁等级、相关样本信息等。

k）激活码获取接口：根据授权文件和设备指纹等信息，获取激活码信息。

6.1.3 SDK 升级要求如下：

a）提供增量和全量升级能力；

b）支持通过网页界面或者接口调用等方式下载升级包；

c）支持对升级包文件的完整性校验。

6.2 本地服务集成要求-本地 API 服务方式

6.2.1 本地 API 服务部署要求如下：

a）需求方应根据提供方的部署要求，准备本地部署环境；

b）部署完成后，应调试调用 API 接口的可用性；

6.1.2 本地 API 服务接口：

本地 API 服务接口的要求参见 6.3.1 的相关要求。

6.1.3 本地 API 服务升级

提供方应具备对本地 API 服务能力及相关数据的在线或离线升级能力。

6.3 云 API 集成要求

6.3.1 威胁信息查询接口如下：

a) IOC 失陷威胁信息接口：可查询 IP/域名是否恶意、风险等级、可信度级别等；
b) 活跃攻击来源 IP 接口：可查询 IP 是否恶意、风险等级、可信度级别、威胁类型等。
c) 子域名查询接口：可查询子域名的相关信息，如子域名列表、子域名数量等。

6.3.2 威胁信息分析接口如下：

d) IP 分析接口：分析 IP 相关地理位置、自治域系统号（ASN）信息、威胁类型、相关攻击团伙标签或安全事件标签、相关威胁信息上下文、相关样本信息。
e) 域名分析接口：分析域名对应的 IP 地址、域名相关信息（Whois 信息）、威胁类型、攻击团伙标签或安全事件标签，相关威胁信息上下文、相关样本信息等。
f) 文件信誉分析接口：通过文件 hash 的方式进行文件信誉分析，获得黑白判定、威胁类型、风险等级、报毒名、相关家族团伙标签等。
g) URL 信誉分析接口：通过 URL 扫描引擎和 URL、域名黑名单服务对 URL 进行检测，同时对 URL 下载的文件进行分析；
h) 文件沙箱鉴定接口：将可疑文件上传到云端沙箱进行检测并获取检测结果，包括文件上传子接口和获取沙箱报告子接口。

注：威胁类型如:远控（C2）、傀儡机（Zombie）、失陷主机（Compromised）、扫描（Scanner）、钓鱼（Phishing）等。

6.3.3 用户管理接口如下：

a) 用户使用信息查询接口：用于查询用户的账号威胁信息和接口使用情况，如账号启用时间、账号总使用限制、账号当前使用次数等。
b) 授权接口：用于获取提供方的 API 接口调用权限。

6.4 平台集成要求

6.4.1 部署能力要求

提供方应具备私有化部署威胁信息平台的能力，向需求方提出部署平台的软硬件环境要求。

6.4.2 升级能力要求

提供方应具备对威胁信息平台能力及相关数据的在线或离线升级能力。

6.4.3 接口能力要求

本地化部署的威胁信息平台提供的接口能力参考 6.3 节云 API 集成的相关内容。

6.5 威胁信息内容集成要求

6.5.1 获取要求

应提供威胁信息内容的获取方式、格式说明等。

6.5.2 更新要求

a) 应具备对威胁信息内容的在线或离线更新能力。
b) 应支持对威胁信息内容更新包文件的完整性校验。

附 录 A
（资料性）
威胁信息服务能力集成应用场景示例

A.1 防火墙类安全风险检测和阻断场景

基于威胁信息能力，实时监测主动外联行为，阻止用户访问恶意 IP 和域名。威胁信息感知的安全事件和黑客团队等组织信息，可以为防火墙、Web防火墙的防护策略提供明确依据。防火墙可以将基于威胁信息的防护策略设置为封禁模式，针对任何检测到的告警，自动阻断连接并自动将 IP 加入封禁列表，还支持分资产独立开启严格模式及采用梯度拉黑，防护更高效。

A.2 态势感知平台类安全分析场景

网络安全态势感知平台（如网络安全运营中心平台SOC、安全信息和事件管理平台SIEM等）建设规划中会接入大量的安全设备、网络设备和服务器、中间件日志。除了传统的关联规则，急需引入威胁信息对日志进行过滤、富化，从而更好地进行关联分析。在态势感的建设周期中，应用高精准 IOC，对 IP 和域名进行过滤，实现态势感知中海量数据的快速过滤和筛选，加速态势感知的效果产出；信誉威胁信息和基础数据威胁信息，对日志中的 IP、域名及 URL，进行维度扩展，例如区域、端口、服务、互联网广度等 维度进行扩展，有效地对告警事情中的数据进行维度扩充。

A.3 域名系统/网络地址转换流量失陷检测场景

本场景一般是企业有比较全的安全设备和系统，急需加入更多的威胁发现和威胁检测能力，增强已有设备的安全能力。通过域名系统（DNS）、网络地址转换系统（NAT） 流量里面的IOC 特征域名 IP 提取，然后和威胁信息匹配从而检测企业是否失陷。

A.4 安全事件溯源场景

对于已经发现的安全事件，通过威胁信息服务能力可以支撑对攻击者的基础设施信息等进行溯源查询，关联攻击者的其他攻击行为，有助于全面排查和溯源该攻击者发起的各类安全攻击事件，挖掘潜在威胁以提前预防其他攻击。

A.5 攻击面管理场景

可以利用威胁信息来进行攻击面管理，构建全面且实时的威胁信息收集与分析体系，不断捕获和整合来自各种渠道的威胁信息并深入分析，以识别出针对企业特定业务环境和资产的潜在攻击面，例如未修补的漏洞、对外暴露的服务端口、不安全的系统配置等；在识别攻击面后，可以根据威胁信息的指引，制定针对性的安全防护策略，以减少攻击面，降低被攻击的风险。

A.6 恶意文件检测场景

本场景适用于已经获得可疑文件，通过威胁信息的文件检测能力，在提供方侧运行和分析文件，对文件的安全性进行多维度检测，并可对确认感染的文件进行修复，。

A.7 攻防演练支撑场景

攻防演练成为网络安全行业实践的重点场景，以攻促防的模式牵引了各企业的安全建设，威胁信息可在攻防演练期间开展专项运营，从事前、事中、事后提供威胁信息全方位的支持。在事前可以对攻击面进行全面评估，在事中提供威胁检测和防护加固的支持，在事后威胁信息可以赋能溯源研判分析。

A.8 应用上架威胁检测场景

威胁信息可支撑应用上架的威胁检测。终端厂商应用商店在应用上架或日常巡检时，应将其检测依据及检测出的相关风险信息发送给应用程序和其他应用商店，减少被攻击的风险。

附 录 B
（规范性）
各类威胁信息服务集成方式的特点

集成方式特点的要求见表B.1的规定。

表 B.1 集成方式特点

方式分类	本地服务集成	云 API 集成	平台集成	威胁信息内容集成
威胁信息数据存储位置	需求方本地	提供方云端	需求方本地	需求方本地
服务部署方式	集成在需求方的产品内	提供方云端	在需求方独立部署，与需求方产品配合使用	集成在需求方的产品内
更新方式	定期更新（自动/离线） 一般全量更新	即时更新 一般增量更新	定期更新（自动/离线） 全量为主	定期更新 一般增量更新
更新频率	一般 小时级/天级	一般分钟级	一般小时级/天级	按需
查询性能比较	高	中	较高	--
使用场景	串行检测	异步检测	异步检测	串型检测
字段丰富度	中	高	较高	中