威胁情报平台 TIP

操作指南

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

操作指南

最近更新时间：2025-04-18 11:44:23

概览

概览页面作为威胁情报平台 TIP 的概述界面，包含了多种数据的汇总以及分析展示。

- 情报概况：按照情报分类展示情报接入数量，包含：IP 类情报、域名类情报、IOC 情报、入站情报、文件信誉情报、本地自定义情报等。
- 情报源每日录入趋势（近7日）：针对情报概况中的四类情报作为统计分类项，按照时间对接入数量进行趋势分析与展示。
- API 查询与命中情况（近7日）：按照 API 查询与命中的次数，按照时间线对命中次数进行趋势分析与展示。

情报管理

情报源

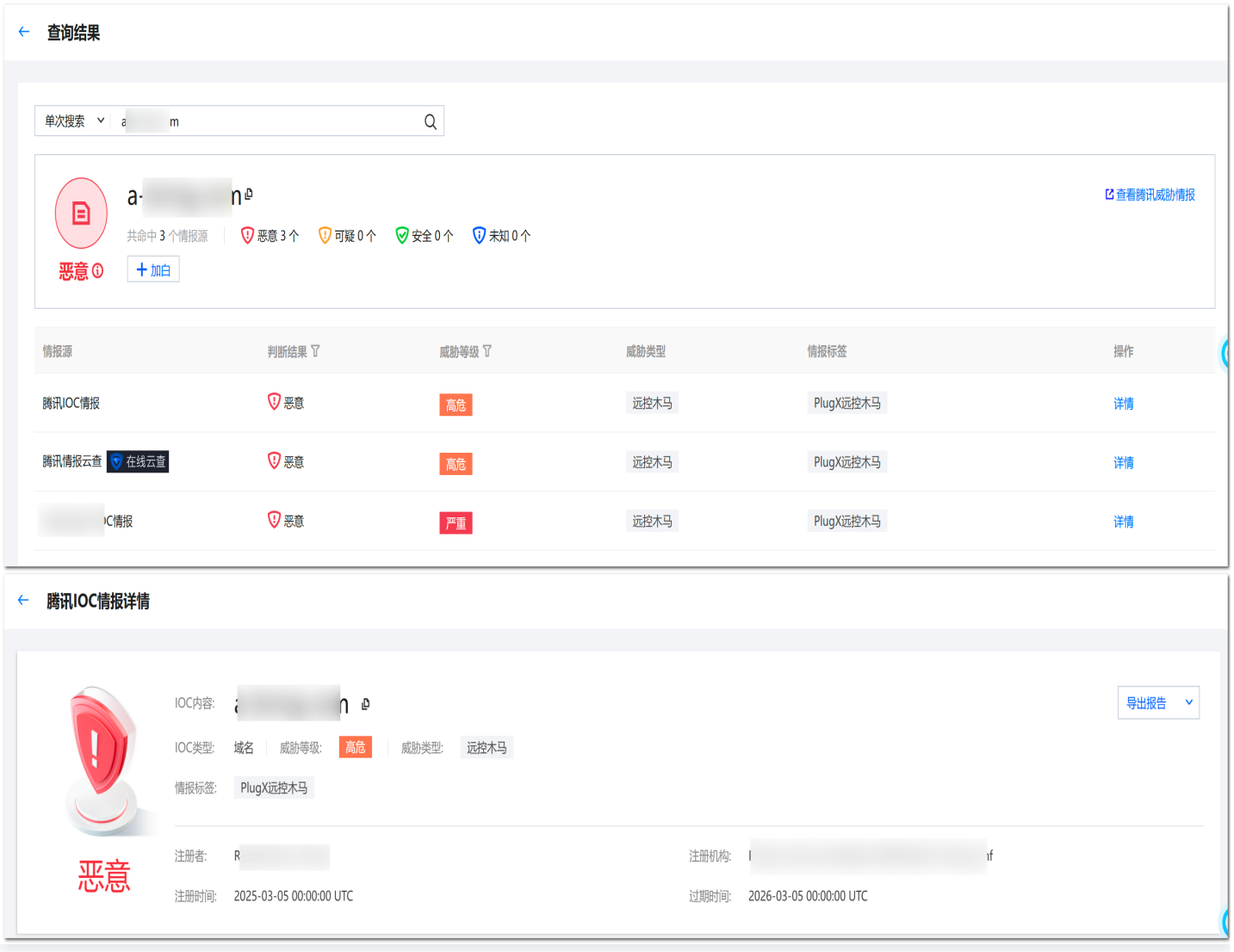
该模块主要对腾讯威胁情报云，本地运营情报源，其他三方情报源等多来源数据进行统一管理。支持添加和编辑情报源，查看当前接入情报的状态和数据统计。

情报查询

用户可以自行在此页面查询情报，在查询栏输入情报即输入 IP、域名、MD5，单击**查询**后系统会在全局范围内查找一个 IOC 条目（包括生效的情报源和失效的情报源）。该功能支持单次搜索以及批量搜索。

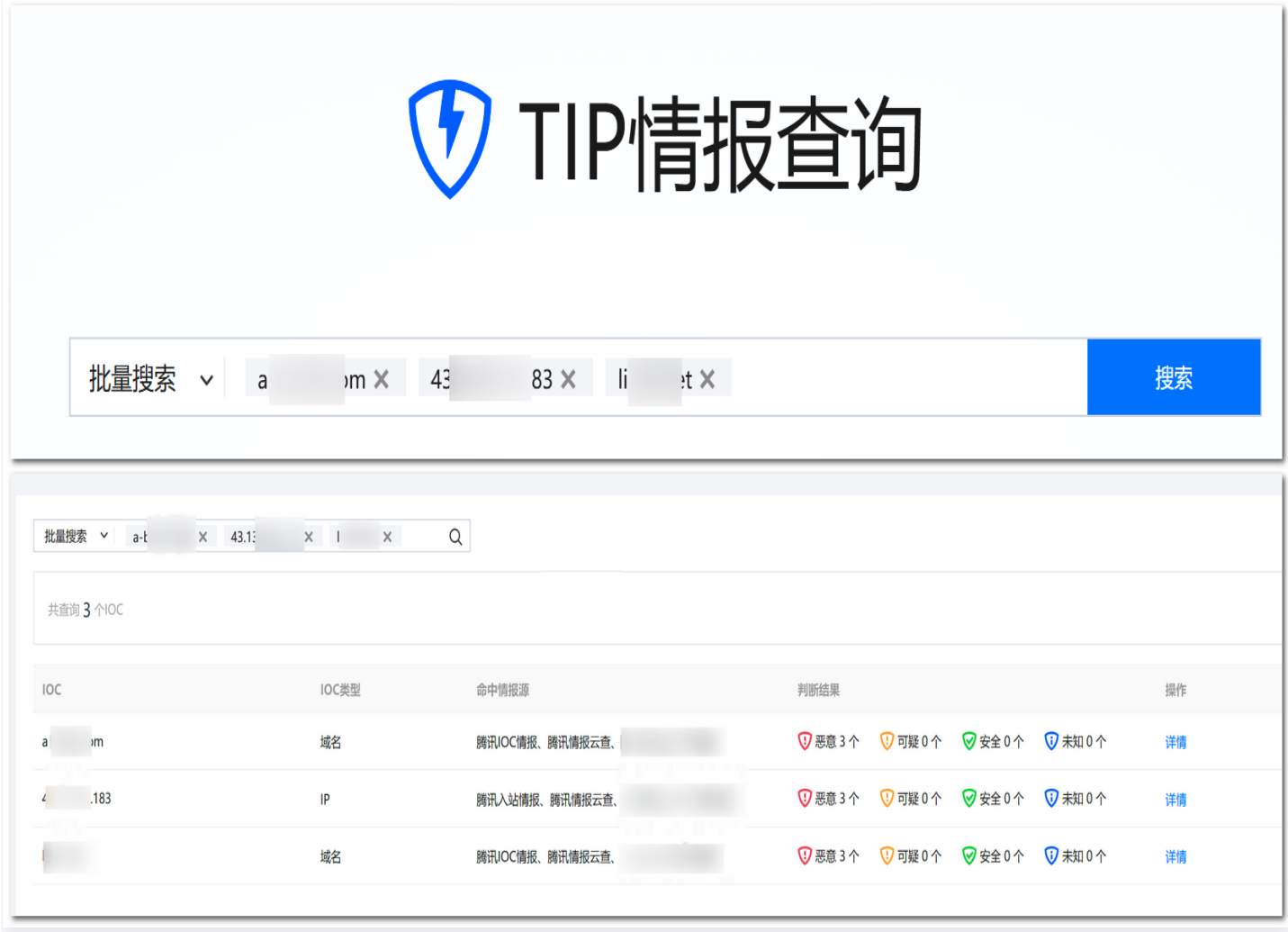
单次查询

如下图所示，在搜索栏输入查询值后，可查看到相关的 IOC 信息，可以根据情报情况对当前域名进行加白（添加入白名单）处理。



批量查询

如下图所示，在搜索栏可连续输入查询值，一边批量获取查询结果。



漏洞情报

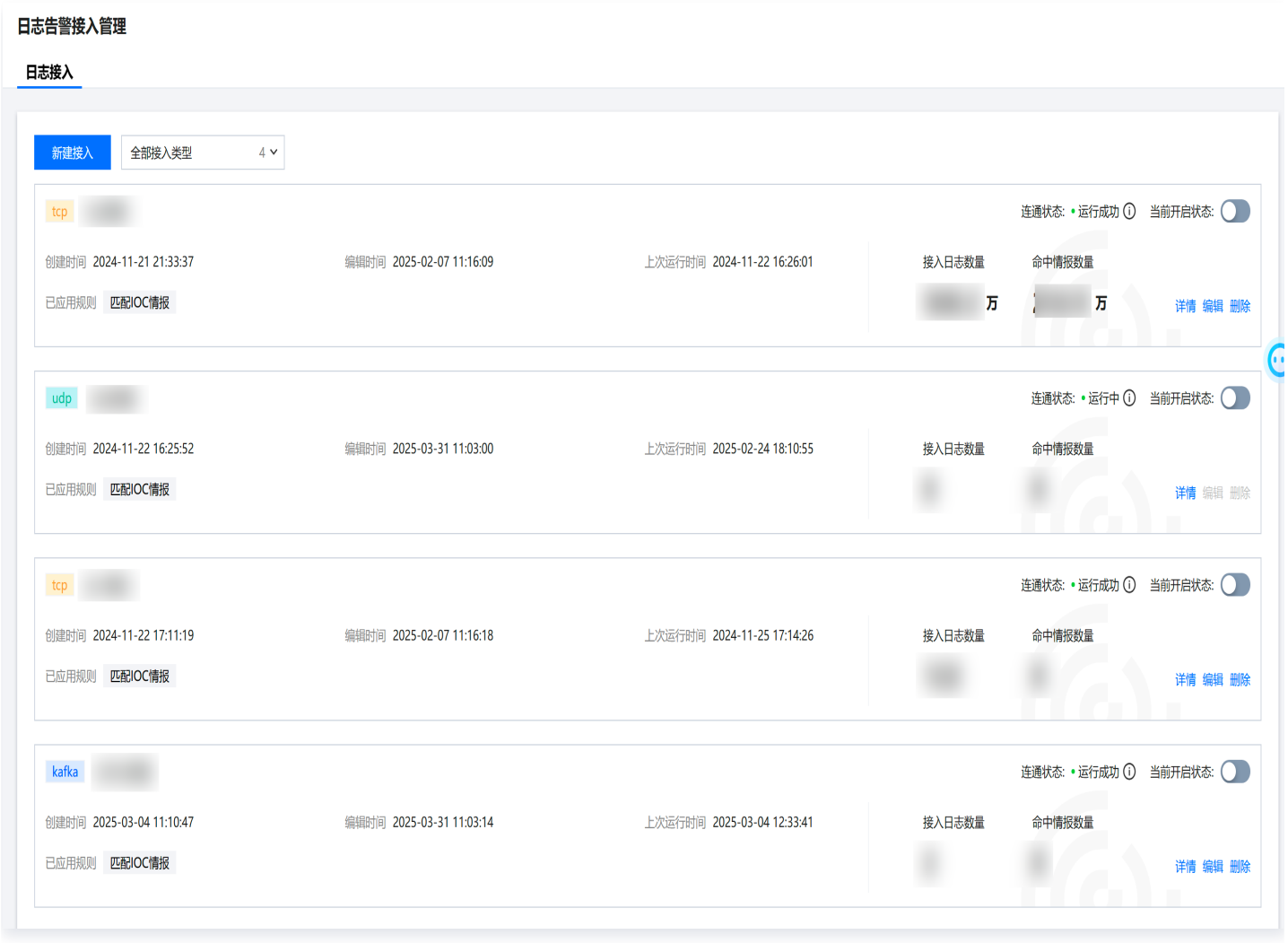
提供腾讯威胁情报中心运营的漏洞情报。漏洞情报定期从云端进行下沉更新，支持基于最新1天、3天、7天，或指定时间区间进行漏洞情报筛查。另外，也支持根据风险等级进行过滤。可单击查看详情跳转漏洞详情页获取更多上下文信息。

情报加白

该功能主要是对平台中已经加白的情报做统一管理展示当前已经加白的 IOC 列表，包括 IOC 内容、类型和添加时间，操作部分可以取消加白。

数据运营

此模块提供条日志接入的查看、配置、统计功能。支持添加 TCP、UDP、Syslog、Kafka、自定义格式的日志数据，以便进行威胁情报分析或本地情报数据运营。



统计分析

主要是针对 API 调用态势分析和调用日志记录查询。

查询趋势

查询趋势页面主要是查询趋势的展示界面，包含：最近1天命中、最近7天命中、最近30天命中、最近1天查询量、最近7天查询量、最近30天查询量。

查询日志

提供威胁情报命中记录的查询能力，可根据时间区间、查询值检索具体的历史查询结果，查询结果中包括：查询时间，使用的 API 账户名称，查询内容，查询值类型，威胁判定结果，威胁等级等信息。

系统管理

该功能主要是针对 TIP 平台的基础功能进行维护，如情报授权的更新与管理、云端威胁情报的自动更新、平台账号管理、API 管理。

安全性及其他设置

- 登录安全：支持配置失败次数上限、锁定时间、页面超出时间、密码过期时间等信息。
- 密码安全：支持配置密码规则强度，区分为高、中、低三档配置。

系统运维

系统提供平台相关授权信息如下图，包括版本更新日期、版本规格类型，授权 ID，授权单位，授权有效期，授权剩余时间，具体订阅的情报数据类型等。