威胁情报平台 TIP

产品简介

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【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。

文档目录

版权所有：腾讯云计算（北京）有限责任公司

产品简介
产品概述

最近更新时间：2025-04-18 11:44:22

背景

网络空间的攻防是一场“非对称”的战争。高级持续性威胁（Advanced Persistent Threat，APT）等新型攻击层出不穷，攻击者拥有较长的准备时间、丰富的攻击工具和较低的攻击成本。传统的安全防护方法通常依赖于在边界或特定节点部署防火墙等安全设备，以实现静态防御，这种方法主要依赖于特征检测进行安全监控，并基于规则匹配生成警报。然而面对各类新型威胁，传统的安全防御方式显得愈发捉襟见肘。

产品定义

威胁情报平台 TIP（Threat Intelligence Platform, TIP）是一套威胁情报运营管理分析平台，协助企业级客户构建本地化威胁情报中心，基于腾讯安全大数据挖掘和攻防经验，提供多源情报聚合应用，本地化情报生产运营，可视化威胁分析，日志威胁检测等功能，支持对接各类安全产品平台进行威胁情报赋能，有效提升安全运营和应急响应效率。

主要威胁情报数据类型介绍

失陷检测情报 IOCs

此类情报一般用于与出站请求目的地址匹配，以协助识别内网是否存在失陷主机。可检出 APT、网银木马、窃密木马、勒索软件、僵尸网络、挖矿软件、常规木马、漏洞利用、SinkHole、DGA、远控木马、黑灰产等威胁类型造成的攻击事件。常用的匹配的日志源包括流量检测、防火墙等。

IP 活跃攻击来源情报（入站）

此类情报一般用于与入站请求的来源地址 IP（互联网 IP）进行匹配，以协助识别有风险的外部访问请求。可检出的威胁类型包括：WEB 攻击 、网络爆破、网络扫描、网络蜜罐、DDoS、垃圾邮件等攻击迹象的来源。常用的匹配的日志源包括 Web 防火墙等。

文件信誉情报

此类情报一般用于与网络中传输的文件 Hash 进行匹配，以协助识别有风险的文件样本。查询值为 Hash（MD5、SHA1等）。可检出文件黑白判定，风险等级，对应家族团伙信息，关联 IOC，相关 ATT&CK 攻击手法。

主要功能介绍

情报概览

提供接入情报数据的分类和统计信息，包括各类数据的本地化存储数量，每日录入趋势，API 情报查询与命中统计数据。

版权所有：腾讯云计算（北京）有限责任公司

情报源管理

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

提供页面以供用户查询情报结果，在查询栏输入检索值（如域名），单击**查询**后系统会根据接入的多源情报，呈现情报判定的结果页。单击**详情**，可获取每个情报源的详细上下文信息，包括判定依据、威胁线索、关联样本等。

本地情报管理

支持用户提供白名单、自定义情报的运营管理功能。以便实现自建情报数据的全生命周期管理，补充外部情报源的数据覆盖度。

数据运营统计

提供可视化的界面，为情报应用日志提供统计分析，以便了解各用户命中的威胁信息和历史风险。

日志威胁分析

支持 Syslog、Kafka、自定义格式等多种接入告警日志的模式，与本地威胁情报进行高速匹配，以实现威胁事件的发现和定位。

版权所有：腾讯云计算（北京）有限责任公司

产品优势

最近更新时间：2025-04-18 11:44:22

数据来源丰富全面

整合腾讯全网海量攻防实战数据，覆盖移动端、PC 端、云端多场景。通过专家威胁分析建模和结构化清洗运营，形成覆盖黑客攻击、漏洞利用、恶意代码检测等多维度的立体情报源。

攻防经验深度运营

依托科恩实验室多年攻防实战积累，融合 AI 模型与安全专家运营经验，实现99.99%的高精准 IOCs 检出率。情报生产运营流程结合 ATT&CK 框架，动态优化威胁狩猎规则与响应策略，确保情报实时性与对抗性。

多源情报灵活兼容

支持腾讯自运营云端情报源、三方情报源及用户本地运营情报源异构融合管理。可为 SOC/SIEM 等20+类安全设备提供标准私有化 API 接口与日志对接集成方案，适用于企业级威胁情报生命周期管理的异构系统联动需求。

海量数据本地下沉

通过云端情报本地化部署，实现分钟级威胁情报自动更新与手动离线更新双模式。同时，基于异构多源情报，在企业级客户内网构建本地威胁情报库，实现私有化情报的再运营与应用。

本地接口高速查询

结合高性能嵌入式存储引擎与高并发轻量化 API，提供万级 QPS 查询性能和毫秒级响应效率。同时，通过预加载核心研判数据与缓存优化，确保与 SOC、XDR 等系统的无缝对接，单机日均处理查询量可达20亿次。

系统平台快速部署

提供软件化，软硬一体化等多种交付方式，实现物理机、虚拟化及混合云环境快捷部署。通过自动化配置流程，企业可在48小时内完成平台上线，降低运维复杂度，助力安全能力快速落地。

版权所有：腾讯云计算（北京）有限责任公司

应用场景

最近更新时间：2025-04-18 11:44:22

隔离网本地化使用情报场景

部署本地化情报系统平台（软、硬、虚拟机），通过单向导入更新方式，实现本地化情报的高速查询调用需求。

多源异构情报统一接入使用场景

支持接入多个来源，多种情报数据，提供统一的 API 对接方式和 Web 人工使用界面。

本地化多设备，高速情报调用场景

提供 RestFul 的高速调用接口，赋能 SOC/SIEM、防火墙、WAF 等传统安防设备提升威胁发现能力。

本地情报生产运营场景

提供情报降噪、辅助研判、丰富上下文流程，支持单独存储本地导入的情报数据，并提供高速调用的接口和 Web 查询服务。

多平台情报共享场景

提供用户自建情报的导入导出功能，并支持多平台间情报数据的推送接收。

日志的威胁检测场景

支持通过 Syslog、Kafka、自定义等方式对接日志，实现威胁事件发现、告警推送和设备联动。

版权所有：腾讯云计算（北京）有限责任公司