威胁情报云查与本地引擎

产品简介

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2023-12-20 14:53:11

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。

什么是威胁情报云查与本地引擎

腾讯威胁情报云查与本地引擎依托腾讯近二十年的网络安全经验和大数据情报技术分析能力，通过云查接口（API）或本地化引擎（SDK）为客户提供威胁情报检测分析服务，包括基于 IP/Domain/文件 Hash 等维度的查询服务，帮助企业提升现有安全防御能力。通过对外提供如下5种类型 API 接口服务实现上述功能。

情报云查接口服务（TIX-API）

情报云查接口服务，是一种 SaaS 化轻量交付的情报应用接口服务。主要面向需提升威胁检测、分析能力的生态合作伙伴，以及企业级用户可联网的本地化安全运营平台或其他安全产品。

入站检测情报

针对入站场景的来源地址进行分析， 能够提供地理位置、 ASN 信息，通过判定规则判别来访设备是否恶意、风险严重级别、可信度级别；识别威胁类型，例如：漏洞利用（Exploit）、 傀儡机（Zombie）、代理（Proxy）、可疑（Suspicious）等及相关安全事件。同时，针对业务日志，以及企业基于防火墙、 WAF 等基础安全防护产品获取的外部 来源访问情况，进行分析，综合判定威胁类型如：远控（C2）、傀儡机（Zombie）、失陷主机（Compromised）、扫描（Scanner）、钓鱼（Phishing）等，相关攻击团伙或安全事件标签，原始情报，相关样本信息等。通过实时判定来访源状态，识别爬虫、撞库、薅羊毛等风险行为，主要用于协助运营人员对 WAF 结果判定提供基础数据支撑。

域名信誉情报

可针对开源情报或者相关报告出现过的域名，以及在腾讯沙箱库出现较多恶意样本链接的域名进行分析，综合判定威胁类型如：远控（C2）、恶意软件（Malware）、傀儡机（Zombie）、扫描（Scanner）、暴力破解（Brute Force）等，相关攻击团伙或安全事件标签，原始情报，相关样本信息等。

文件信誉情报

对于网络中传输的文件、主机上新出现的进程或文件，可以通过文件 hash 的方式进行文件信誉查询，获得相较传统本地单一静态引擎检测更精准、全面的结果，有效提升检测率并降低误报率。

API 查询结果不但可以判别黑白，还可以提供恶意文件的类型和家族信息，在报警管理和事件响应过程中可以依赖这类信息快速的筛选风险较高的报警，并针对不同类型采取直接有效的响应动作。API 查询结果针对特定恶意类型，如木马、蠕虫、黑客工具等，返回对应的分析结果数据。利用这些数据，大数据分析平台或者安全分析人员可以进行关联分析，匹配网络行为日志，获得更多攻击线索并对整个攻击链做还原。

URL 信誉情报

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。

高精准 IOC 情报

通过判定规则有效判别 IP 或域名是否恶意、风险严重级别、可信度级别；识别远控（C2）、恶意软件（Malware）、矿池威胁，提供相关安全事件或团伙标签等 。APT 攻击、蠕虫木马、僵尸网络、勒索软件等的远控服务器地址情报数据库，可以用来匹配 DNS、HTTP 日志中的域名。

情报本地引擎（TIX-SDK）

情报本地引擎是一种提升安全设备威胁情报检测分析能力的本地组件，情报数据与检测逻辑以本地文件形式存在，目前向生态合作伙伴开放商用。

情报引擎轻量版（SDK-Lite）

主要面向有情报本地化有使用需求，但计算性能有限的检测型产品，如防火墙，Web 应用防火墙（WAF）等。

- 可快速识别失陷外联行为，攻击来源，并进行阻断。
- 提供在线自动升级和离线导入2种情报更新形式。

情报引擎高级版（SDK-Pro）

主要面向对情报本地化有使用需求，且对情报数据的丰富度、覆盖度，以及专项场景化有灵活使用需求的平台性产品，如流量检测分析类产品（NTA、NDR、DNS），安全运营中心平台（SOC、SIEM），本地情报中心平台（TIP）。

- 提供的情报种类较多，不仅包括高精准阻断类情报，还包括丰富的上下文信息，如归属者类型（运营商、公有云、企业 IDC、小区宽带），地理位置信息，匿踪标签（VPN、TOR）。
- 提供在线自动升级和离线导入2种情报更新形式。

产品优势

最近更新时间：2023-12-20 14:53:11

高实时性情报

威胁情报云查与本地引擎结合腾讯多年的安全经验和数据分析技术能力，可以7 × 24小时不间断地生产高可靠性威胁情报。

预知威胁

- 威胁情报云查与本地引擎提供有关恶意活动源、新兴威胁和攻击的可操作情报。
- 威胁情报云查与本地引擎能与现有方案自动集合，使用户提前感知可能存在的威胁并及时采取行动，降低安全事件发生，帮助用户减少安全威胁。
- 威胁情报云查与本地引擎在利用漏洞和发布供应商补丁之前，主动保护应用程序使其不受影响，确保安全操作人员能够占据主导地位。

评级信度

威胁情报云查与本地引擎可以帮助用户完善现有安全解决方案，根据活动频率计算恶意值，并基于检测活动传感器的数量类型分配置信度，您可以根据需求自定义警报。

节约成本

威胁情报查与本地引擎以 Web-API 或本地检测引擎（SDK）的方式为用户提供服务。在签约后，用户可以使用授权证书来访问相应的产品模块。威胁情报产品以 Json 格式提供返回结果，方便用户将产品智能集成到其它的应用程序和系统中，从而实现动态安全策略优化，无需额外的 IT 开销。

多元化标签

威胁情报查与本地引擎在收集威胁情报时，覆盖全球网络风险事件，分析攻击来源活动情况以确定其活动内容。

应用场景

最近更新时间：2023-12-27 17:48:21

辅助甲方运营团队

威胁情报是一种新的网络安全防御手段，防御思路从以漏洞为中心进化成以威胁为中心，因此威胁情报云查与本地引擎能够有效助力运营场景。在诸多的安全信息中，只有深刻掌握关键性资产的安全漏洞，了解所在行业当时存在的主要风险，才能快速且有针对性地构建起高效合理的安全体系结构。

支持失陷检测

适用于用户已经拥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情况。
腾讯云威胁情报支持通过情报办公网失陷资产，生产网失陷资产，威胁事件等信息，并及时处理，可有效控制威胁事件的危害范围，防范潜在的损失。通过在现有系统中接入情报 API 或情报 SDK 的相关系统或者设备，例如：NTA，EDR 系统，情报检测网关等，来增强现有设备和系统的威胁发现能力。

支持态势感知情报中心

- 在用户建设态势感知中心时，会接入大量的安全设备、网络设备、服务器、中间件等的日志；针对这些日志的分析，除了传统的关联规则，还亟需引入威胁情报对日志进行过滤、富化、降噪等关联分析。
- 在态势感知冗长的建设周期中，应用高精准 IOC，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。
  信誉情报和基础数据情报，对日志中的域名及 URL，从区域、端口、服务和互联网广度等10+维度镜像扩展，有效地对告警事情中的数据进行维度扩充。

支持 Bot IP 业务防御检测

适用于用户已经拥有防火墙系统（FW）或 Web 应用防火墙系统（WAF）等支持增强 API 或 SDK 能力的设备，通过威胁情报云查与本地引擎来增强业务风险防御能力。

- 针对 WAF 拦截 IP，避免企业出口、4G 出口、城域网出口等 IP 地址被封禁，造成误拦截。
- 针对入站访问，通过识别 Bot IP 标签进行拦截，海量云上 Bot IP 攻击情报实时同步，拦截爬虫、代理、秒拨等，提升业务系统的健壮性，防范数据损失。

支持 SIEM 和 SOC 类的安全产品

威胁情报云查与本地引擎可以区分不同类型的攻击事件，并从中识别出高危 APT 类型事件，确保能及时有效采取应对措施，使损失最小化。威胁情报云查与本地引擎可以通过预测指标来预测攻击者，可能会进行的恶意活动和攻击范围，并通过 SIEM 或 SOC 设备对历史的威胁情报进行索引，得到更全面的线索。