威胁情报攻击面管理

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：2023-09-12 17:09:43

威胁情报攻击面管理是一款致力于解决用户互联网风险监测难题的 SaaS 化订阅服务产品。提供面向政企用户的互联网资产漏洞风险、内容风险与信息泄露风险等维度的监测服务。同时基于企业多维度的信息关联测绘，可实时监测互联网暴露面，发现暴露资产、端口、服务与潜在风险。

产品功能

机构管理

机构管理可以查看和管理监管范围内所有机构的安全情况，提供各机构安全评分、机构各类风险趋势和风险详情等信息，帮助用户快速定位需通报整改的危险机构。

报告中心

报告中心可以查看和导出安全报告，报告内容涵盖指定时间段内用户的所有漏洞风险、网站风险、威胁情报风险、敏感服务梳理、风险梳理信息。

情报中心

情报中心提供人工运营后的最新安全情报信息，情报类型含 APT 研究、信息泄露、勒索病毒、挖矿木马、漏洞情报等。

互联网暴露面

针对企业的资产进行持续性探测，可根据指定的公司名称、IP 段、域名从而主动采集网络空间的数据资产，数据资产包括子域名、Web 应用、开发框架及各种基于 TCP/IP 协议的服务组件、端口等。

漏洞风险监测

在授权的情况下对企业资产进行无感知的漏洞扫描，将漏洞扫描结果可视化呈现，并提供详细的漏洞风险信息及漏洞修复建议。

网站风险监测

通过语义分析、图像识别引擎和黑词提取等技术，帮助用户发现网站挂马、篡改、暗链、色情、赌博等网站风险。同时对发现的风险进行界面可视化，提供详细风险取证信息及修复建议。

威胁情报风险监测

通过布控暗网、文档、Github、Telegram、文库等渠道，实时监控企业是否存在信息泄露风险。当发现源码泄露、员工信息泄露、用户数据泄露等问题时，将及时向用户发送告警并提供相应修复建议。

产品优势

最近更新时间：2022-12-02 14:51:01

资产梳理

可快速提供全面的资产探测和精准漏洞测绘，对暴露在互联网的服务器、端口、组件、漏洞等进行纵深探测。通过网络空间测绘、无感知半连接技术、指纹库、DNS 数据发现等技术，发现互联网资产暴露面、未知资产、资产潜在漏洞风险等问题。

风险监测与通知

结合 Web2.0威胁检测引擎、情报大数据、深度机器学习以及腾讯安全二十年实战经验，提供全面的风险监测服务，包括漏洞风险、网页篡改、挂马暗链、敏感内容、信息泄露等。同时支持通过微信对风险进行实时告警，做到7*24小时风险感知零延时。

多维度风险评估

提供全局、下属单位、风险事件、资产多视角呈现风险，贴合“挂图作战”的综合指挥和统筹能力要求。围绕 Gartner 风险评估维度说明，与 ISO2700X 等评估标准，评分模型考虑因素全面，包括脆弱性、重要性、多样性、频率、持续健康度等。

应用场景

最近更新时间：2023-09-12 17:09:43

行业安全监管

威胁情报攻击面管理助力省市区县监管机构推动立体化监测体系建设工作落地，满足测绘、监测、专项、指挥工作需求。提供全局、单机构、风险事件、资产四种视角，可通过单机构视角了解各机构风险趋势和风险详情，并对单机构进行通报整改，帮助用户贴合“挂图作战”的综合指挥和统筹能力要求。

企业安全监测

对于业务资产众多且无下属监管机构的企业用户，威胁情报攻击面管理将地理、资产、风险事件、情报等大数据进行融合分析并关联化呈现，帮助用户提升安全管理效率。通过主动情报发现和被动测绘技术，对资产进行持续感知和测绘，以 SaaS 平台结合专业人工运营的模式，落实7×24深度网站监测和7×24 通报处置。

重点时期监测服务

提供重点时期的安全专家服务，包括但不限于渗透测试、安全巡检、安全加固、威胁溯源等。