攻击面管理

产品简介

腾讯云

文档目录

产品简介
产品概述
产品优势
应用场景

产品简介
产品概述

最近更新时间：2024-09-05 15:24:51

什么是攻击面管理

攻击面管理（Threat Intelligence Attack Surface Management，ASM）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，提供面向客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。同时攻击面管理可基于企业多维度信息关联测绘，实时监测互联网风险暴露面，发现暴露资产、端口、服务与潜在风险。

产品功能

资产威胁面

提供暴露资产的风险监测服务。

- 暴露风险：包括暴露端口、暴露组件、暴露敏感服务、暴露敏感 URL 等。
- 漏洞风险：提供 POC 漏洞验证、订阅组件漏洞、企业关联漏洞、漏洞知识库等。
- 弱密码风险：针对用户涉及到登录入口、管理入口的资产或服务，进行弱密码验证。
- 资质风险：包括域名备案、证书安全、注册情况监测。
- 网站可用性：基于全球基础设施为用户资产进行持续可用性监测。

社工入侵面

- 信息泄露风险：涵盖代码泄露、邮箱泄露、用户信息泄露、员工信息泄露、文档泄露等维度风险监测。
- 钓鱼欺诈：识别与用户相关的钓鱼网站、公众号、小程序、App。

信息合规面

- 敏感内容：辅助用户识别自身资产涉及到的黄赌毒、涉政等不合规敏感内容。
- 篡改外链：协助用户识别资产存在的挂马事件、暗链事件。

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已发现的用户的漏洞风险、网站风险、威胁情报风险、敏感服务梳理、风险梳理信息。

资产管理

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。

产品优势

最近更新时间：2024-05-28 14:50:01

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，提供7*24小时风险感知。

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：2024-11-06 11:43:42

行业安全监管

攻击面管理助力推动立体化监测体系建设工作落地，适用于测绘、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的企业用户，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。

发现高危风险资产和服务场景

基于高危漏洞、敏感端口、弱密码入口等维度，预警用户高风险互联网暴露面。

识别未纳管关联资产和服务场景

监测影子资产，识别用户违规上线，脱离管控资产，以及相关仿冒服务（包含网站、IP、公众号、小程序、App等）。

追踪外网信息泄露事件场景

定位用户出现的员工信息外泄，客户信息售卖，源代码泄露、企业敏感文档传播等信息源。

监测内容合规性和服务健康度的场景

协助用户发现业务发布内容的敏感信息，满足合规性要求；实时监测核心网站资产、服务状态，识别对外服务的异常情况。