暴露面管理服务

产品简介

腾讯云

【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

产品简介

产品概述

最近更新时间：2024-03-21 14:17:51

暴露面管理服务是一个主动的风险管理服务，旨在根据企业的授权，通过一系列脆弱性发现、威胁监测等工具对企业资产的暴露面及潜在威胁进行挖掘分析，借助攻击模拟等手段进行攻击路径验证，动态评估企业在数字和物理资产的可访问性、暴露面及可利用性，帮助企业降低漏洞利用风险，优化运营流程。

主要功能介绍

威胁暴露面监测

从互联网层面，定期监测识别企业及组织在数据中心、云供应商、组织员工、供应链供应商、第三方合作商等层面存在的暴露面及威胁（如 IP、域名、端口、网站指纹、管理后台、邮箱、源代码、数据库、员工失陷账号等），包括但不限于以下暴露面风险：

- **互联网资产风险监测**：对互联网侧的暴露面、威胁和脆弱性（漏洞、配置）风险进行持续监测和评估。
- **云服务风险监测**：利用 XSPM 引擎，基于 ATT&CK 云攻防矩阵，识别企业云服务配置安全风险（如存储桶、云密钥、安全组配置等风险）。
- **代码仓库监测**：监测识别企业在 GitHub、Gitlab 等代码仓库中的机密账户、敏感代码等暴露面信息。
- **移动应用监测**：监测企业公众号、小程序、App、新媒体等资产的仿冒信息。
- **供应链风险监测**：持续监测和分析企业分支机构、供应链合作商等外部攻击面风险。
- **人员暴露面监测**：识别企业员工账号泄露、登录凭据泄露等暴露面风险。

风险分析及验证

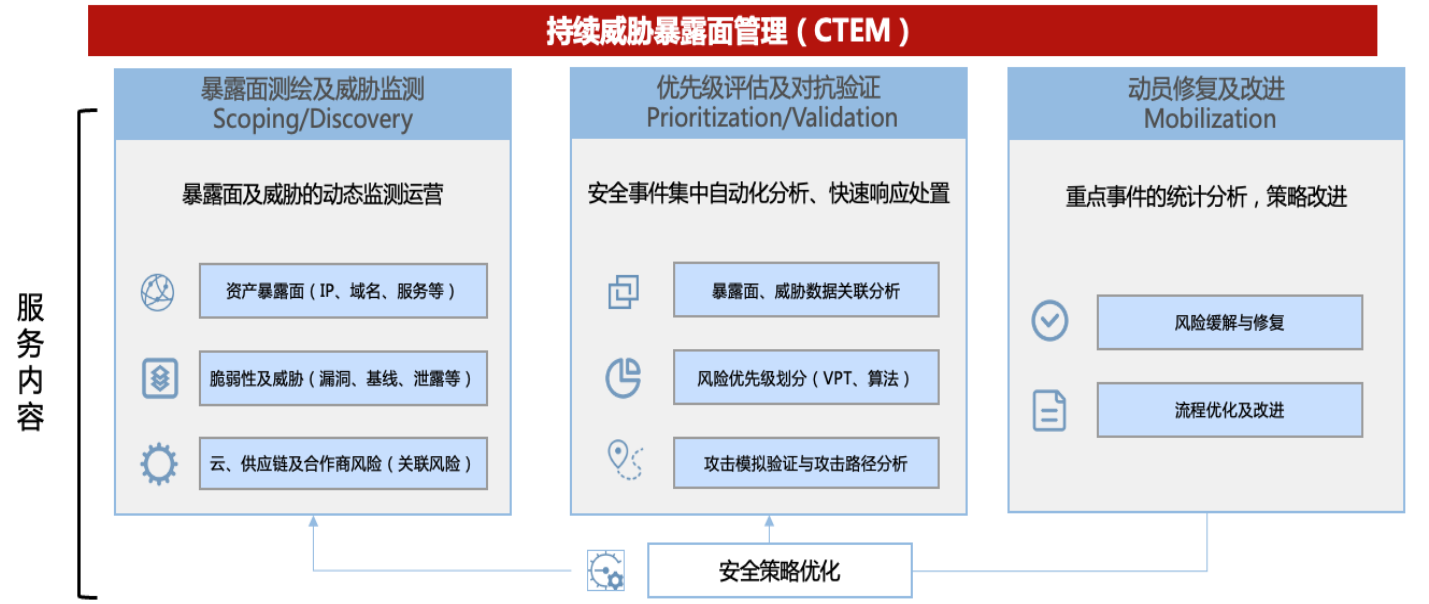
基于监测期间捕获的企业暴露面数据，通过自动化攻击模拟及红队手段对测绘发现的数据进行关联分析和验证，分析攻击者可能采用的攻击战术和实施手段（如重点漏洞利用、基线、云账号或密钥泄露、员工账密等），识别潜在攻击路径及受影响资产情况，并基于风险程度进行优先级划分，提供攻击路径描述及风险优先级列表。

修复动员及改进

针对服务期间动态识别到的高优先级暴露面和威胁，提供修复建议和缓解参考，帮助企业从运营流程、技术防护等层面进行持续改进提升。

> ⚠ **注意：**
> 由于服务内容会结合外部风险态势不断丰富，具体以客户购买的服务内容为准。

产品架构或工作原理



相关产品

- 安全托管服务
- 渗透测试服务
- 重要时期安全保障服务
- 安全攻防对抗服务
- 应急响应服务
- 安全验证服务
- 云安全风险巡检服务

服务内容

最近更新时间：2024-03-21 14:17:51

本文档将为您介绍暴露面管理服务的详细服务内容及交付内容。

暴露面管理服务提供7*24小时监测，并辅助人工分析、对抗评估验证和组织修复计划，其主要包含如下服务内容：

服务分类	服务内容	交付内容
重大威胁暴露面监测服务	通过对企业资产的可访问性、暴露性和可利用性进行风险信息挖掘、分析和验证，并提供修复建议，帮助主动管理内部和外部威胁的影响，涉及暴露面监测范围包括但不限于： • **互联网资产风险监测**：对互联网侧的暴露面、威胁和脆弱性（漏洞、配置）风险进行持续监测和评估。 • **云服务风险监测**：利用 XSPM 系统引擎能力，基于 ATT&CK 云攻防矩阵，针对用户多云环境开展持续策略风险分析和监测，识别云服务配置安全风险（如存储桶、云密钥、安全组等配置风险）。 • **代码仓库监测**：监测识别企业在GitHub、Gitlab 等代码仓库中的机密账户、敏感代码等暴露面信息。 • **移动应用监测**：监测企业公众号、小程序、App、新媒体等资产的仿冒信息。 • **供应链风险监测**：持续监测和分析企业分支机构、供应链合作商等外部攻击面风险。 • **人员暴露面监测**：识别企业员工账号泄露、登录凭据泄露等暴露面风险。	**每周一次**：定期提供《暴露面管理分析报告》。 **按需提供**：监测发现重大暴露面或威胁后，即时同步暴露面风险概况。
重大威胁暴露面分析服务	通过自动化攻击模拟及红队手段，针对监测到的企业暴露面数据进行研判分析，识别优先级，并生成分析报告同步客户，分析内容包括但不限于： • **优先级分析**：基于攻防风险评估，识别暴露面风险风险修复优先级，识别高优风险。 • **攻击路径分析**：基于暴露面和威胁数据，结合攻防实战场景进行关联分析，验证识别真实攻击路径。	**按需提供**：监测发现重大暴露面或威胁后，进行研判、对抗验证，输出攻击路径及修复优先级建议。
风险分析改进服务（即服务阶段报告提交服务）	针对监测发现的重点暴露面风险及常态暴露面风险，提供阶段分析报告： • **重点暴露面风险**：在发现重大暴露面风险后，即时开展风险分析和报告编写，提交重点暴露面风险报告，指导具体风险修复。 • **常态化暴露面风险**：针对日常监测到的基础暴露面风险，每周定期开展数据分析，提交常态暴露面监测报告，提供安全运营改进建议。	**按需提供**：针对重点及常态化暴露面风险，提供阶段性服务报告。

产品优势

最近更新时间：2024-03-21 14:17:51

纳入云及供应链风险，更广的范围覆盖

- 在组织架构维度，除企业自身资产外，亦可覆盖供应链供应商、第三方合作伙伴合作商等存在的公开暴露面和威胁。
- 在风险类别维度，除传统基于 IP、端口的漏洞基线等脆弱性风险外，同时可覆盖员工失陷账号 、云服务相关攻击风险等。
- 在数据归属维度，除覆盖数据中心资产，亦可覆盖云供应商等存在的云安全配置风险。

整合多方测绘引擎，具备更精准暴露面发现能力

传统资产梳理时间长且容易出错，腾讯暴露面管理服务集成 T-SCAN 风险发现引擎，整合自研精准资产指纹和 PoC 库，同时引入各类互联网数据资产引擎，借助服务编排及自动化平台（SOAP 平台）实现资产发现-分析研判-风险验证的全路径编排，大幅降低误报、漏报风险，帮助企业更详细、快速的识别暴露面风险。

采用攻击模拟模式，深入识别高风险暴露面

基于多年大型安全攻防对抗实践，将风险严重经验固化到安全验证平台（BAS）的剧本中，并依托专职攻防团队人力，针对发现的安全风险面等进行持续动态评估验证，以深度复原黑客潜在攻击路径，并协助输出风险优先级。

应用场景

最近更新时间：2023-12-19 17:23:44

各类信息化资产梳理

复杂业务组织环境或安全架构模式下，想要了解企业信息化及数字资产对外暴露面情况。

资产脆弱性深度发现

想要了解企业在数据中心、云供应商，组织员工、供应链供应商、第三方合作商等存在的公开暴露面及威胁（IP、域名、开源框架、服务应用、漏洞、配置等）。

云服务安全策略分析

针对企业在不同云供应商存在的安全策略风险进行动态巡检，识别云服务存在的配置不当风险，如云密钥泄露、存储桶、安全组、安全产品等配置不当风险。

漏洞研判及治理

站在攻防视角，实战分析漏洞攻击真实危害性，提供漏洞修复必要性参考，企业漏洞治理实践参考。

敏感数据泄露监测

提供互联网等数据泄露监测能力，帮助识别企业云密钥、源码泄露、员工凭据等的数据和信息泄露风险事件。

供应链资产安全管理

分析、监测和识别企业在供应链供应商、第三方合作商等存在的公开暴露面及威胁，如供应链员工合作账号泄露及合作系统、采购产品的安全暴露面风险。