风险评估服务

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：2024-05-29 17:56:21

风险评估服务（Risk Assessment Services，RAS），是指腾讯云在客户授权后，结合工具及专家服务对用户业务进行安全风险发现，提供安全加固建议，提升整体安全能力。包含云安全风险评估、暴露面风险评估、防御能力风险评估、安全检查等服务。

主要功能介绍

云业务风险评估

评估云环境安全状态，提供云资产盘点、云身份权限检查、云安全风险识别、云暴露面发现等服务，帮助企业发现潜在安全风险和威胁。可支持跨云、跨账号的安全风险评估。

暴露面风险评估

对企业及其关联公司、供应链的资产暴露面、脆弱性及外部威胁进行挖掘分析，并借助攻击模拟等手段进行攻击路径验证，帮助企业进行资产梳理、风险分析及风险修复。

防御有效性评估

借助攻击模拟平台及内置/自定义的攻击剧本，自动化、场景化验证企业现有安全设备及防御体系的有效性，可覆盖边界防御、主机防御、邮件安全、内网安全、终端安全等多场景的安全验证。

云安全检查服务

结合腾讯云安全专家人员和安全工具，提供各类型安全检查支持服务，配合进行脆弱性检查、风险发现、合规项校验等工作，协助用户应对各项场景安全检查，并提供定向支持服务。

专家分析及支持服务

针对各项技术性评测中发现的安全弱点问题，提供专家风险分析及安全加固指导服务，帮助企业制定与落地风险修复计划。

产品优势

最近更新时间：2024-05-29 10:40:11

全局视角风险评估，维度更广更全

融合攻击者及防守者视角，从资产梳理、业务脆弱性识别、外部风险识别、防御体系验证等多维度发现、验证企业安全风险，评估范围覆盖数据中心业务、云业务、人员、供应链等多类型资产，可帮助企业从不同的风险类别、资产类型及组织架构来全面/专项的检测安全问题，兼顾风险评估的广度与深度。

整合多方测绘引擎，风险精准识别

传统的资产梳理、漏洞扫描时间长和容易出错，腾讯风险评估服务集成 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、快速的识别业务风险。

无害化攻击模拟，深入验证高风险

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。验证过程安全无害，模拟攻击操作可控，不会影响业务系统的正常运行。

增值专家服务，高效闭环风险处置

企业可据自身需求增购远程/驻场的专家支持服务，针对各项安全评估中识别的安全风险问题，提供定制化、个性化的风险发现、分析及加固服务，适配不同企业的安全建设需求。

应用场景

最近更新时间：2024-05-29 10:40:11

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，规避未知资产、影子资产、数据泄漏等带来的安全风险。

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。

安全防御体系有效性验证

通过自动化的攻击模拟帮助企业持续评估整体的网络安全防御态势，及时发现安全控制中存在的策略问题或者防护漏洞，及时找出企业防御措施的不足，优化攻击链路上的薄弱点。辅助企业在各类攻防演练前开展安全自检，或建设常态化实战对抗能力。