重要时期安全保障服务

产品简介

产品文档

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。

文档目录

产品简介
产品概述

最近更新时间：2022-03-17 14:56:21

什么是重要时期安全保障服务

重要时期安全保障服务（Cybersecurity in Important Period, CIP）是指在特殊时期、重要活动、重大节日前期，由安全专家对企业在腾讯云上资产进行安全评估、风险探测、泄漏事件发现并提供修复意见，在特殊时期、重要活动、重大节日中期对企业在腾讯云上信息化资产进行安全监测，对监测到的安全事件进行分析、研判，根据用户的要求对攻击者 IP 进行阻断，同时根据用户的授权，对已发现的安全事件进行应急处置。

产品功能

安全评估服务

重要时期安全保障服务团队会在用户授权的情况下，对用户云上资产展开安全评估工作，发现系统、应用、安全配置中包含的安全风险，评估用户云上资产安全现状。

风险检测服务

重要时期安全保障服务团队会在用户授权的情况下，针对云上资产进行安全扫描工作，并针对扫描发现的安全漏洞提供修复方案，扫描类型包含两种：

- 互联网侧资产扫描：针对于暴露在互联网侧所开放端口，进行系统层和应用层的扫描及风险分析。
- Web 应用系统扫描：针对在互联网开放的 Web 应用系统，进行应用层和 Web 层的扫描及风险分析。

风险处置服务

重要时期安全保障服务团队可对安全评估过程和风险检测服务中发现的风险，提供安全加固建议，包括但不限于：

- 系统及应用的配置处置指导，针对高危漏洞及弱配置问题提供加固建议。
- 安全产品运营指导，针对安全产品运营提供指导建议（如防火墙策略配置等）。

渗透测试服务

重要时期安全保障服务团队会在用户授权的情况下，对用户重要级别的应用系统进行渗透测试工作，安排工程师人工挖掘应用漏洞，增加应用自身的防护能力并对发现的漏洞提供修复方案。

漏洞感知与泄漏监测服务

重要时期安全保障服务团队可提供最新漏洞情报及敏感信息泄漏情报服务，分析风险并提供解决方案。

- 高危漏洞安全通告服务，提供漏洞分析及修复方案。
- 实时检测用户 API 密钥在 GitHub 的泄漏情况，提供修复建议。

安全监控服务

重要时期安全保障服务团队在保障期间，提供针对于安全设备告警的24小时安全监控服务，分析并处理安全告警，找出其中真实的安全事件并在用户授权的前提下，进行处理并告知用户。

应急响应服务

重要时期安全保障服务团队在保障期间，提供 N × 24小时（N 为用户所实际购买的保障天数）的应急响应服务，在出现安全事件后，及时对事件涉及的服务器进行处理，阻断事件蔓延，控制事件的危害性。

服务内容

最近更新时间：2022-03-17 14:56:25

本文档将为您介绍重要时期安全保障服务的详细服务内容及交付内容。

服务名称	服务内容	交付内容
安全评估服务	通过复用腾讯自研安全规范、策略库及评估分析引擎，全面评估用户腾讯云上主机安全现状，发现用户主机、网络、应用及数据等方面存在的风险，评估内容包括： • 系统安全架构评估 • 云业务安全风险评估 • 云产品不安全配置风险评估 • 域名暴露面评估 • 主机安全风险评估 • 网络安全风险评估 • 应用安全风险评估 注意：由于计算机系统的复杂性和网络安全技术的局限性，**腾讯云无法保证在安全评估过程中发现所有的安全风险**	《安全评估报告》
风险检测服务	集成腾讯自研漏扫平台+第三方安全扫描引擎，针对用户腾讯云业务主机提供周期性漏洞检测和管理服务，人工分析报告内容，并输出修复指导和风险管理最佳实践，包括： • 高危端口扫描 • 系统漏洞扫描 • Web 漏洞扫描	《风险检测报告》
安全加固咨询服务	针对评估、监测、检测等不同阶段发现的严重或高危级别安全事件，通知并协助用户开展处置响应，包括： • 提供详尽的修复方案 • 提供风险修复验证 • 提供安全加固指导	根据事件提供详细的修复建议及方案，为用户解答事件的风险并验证事件是否完全修复
渗透测试服务	对核心业务系统安排工程师进行渗透测试工作，人工挖掘应用漏洞，针对发现的漏洞提出整改和修复方案。	《渗透测试报告》
漏洞感知与泄漏检测服务	重要时期安全保障服务团队 N × 24小时（N 为用户所实际购买的保障天数）监控漏洞情报及敏感信息泄漏情报服务，分析风险并提供解决方案。服务内容包括： • 高危漏洞安全通告服务，提供漏洞分析及修复方案。 • 实时检测用户 API 密钥在 GitHub 的泄漏情况，提供修复建议。	保障期间，会在监测到漏洞情报后响应并输出： 1.《重大漏洞通告》 2.《泄漏事件报告》

服务名称	服务内容	交付内容
安全监控服务	持续监视用户云上主机安全产品告警事件，对安全事件进行分析、响应和运营优化，服务内容包括： • 安全事件监控分析 • 安全产品策略配置指导	保障期间每日一次，提供《重保日报》
应急响应服务	重要时期安全保障服务团队在保障期间，提供 N × 24小时（N 为用户所实际购买的保障天数）的应急响应服务，在出现安全事件后，第一时间对事件涉及的服务器进行处理，阻断事件蔓延，控制事件的危害性。	《应急响应报告》

产品优势

最近更新时间：2022-03-17 14:56:28

云原生兼容安全服务

基于腾讯云服务团队安全运营经验，通过安全编排自动化与响应（SOAR）技术，快速响应主机、网络、应用及数据安全产品的各类安全风险事件，持续的自动化监控风险和泄漏事件。

全天安全保障

在重要时期安全保障服务期间，服务团队提供N × 24小时（N 为用户所实际购买的保障天数）的安全保障，包括安全产品的告警分析、安全事件监测、漏洞情报捕获等，在出现安全事件后实时安排安全工程师进行应急响应操作。

标准化的服务内容

基于服务团队的行业标准以及安全经验，梳理了标准化的服务检测项，服务的评估及交付依赖于服务检测项，确保整体服务评估内容的完整性，避免出现评估的遗漏。

智能驱动的运营

基于整体和近实时的威胁检测策略，通过安全产品事件行为进行多因素关联分析，对捕获的安全事件及处置用例进行分类，利用预置检测框架分析用户云环境中存在的高优先级事件。

应用场景

最近更新时间：2022-03-17 14:56:32

特殊敏感时期防护

在重大会议期间，对企业云上资产进行安全防护，避免因安全防护能力不到位，出现网站被挂恶意页面、DDoS 攻击导致业务中断等安全事故。

企业业务活动监控

在企业新系统或新功能上线、促销和商业活动期间，需要保障业务系统的正常运营，避免因为网络安全事件导致的业务中断、恶意入侵等情况。

网络安全攻防演练

安全攻防演练期间，云上资产往往容易成为企业安全被突破的第一道防线，需要提升企业云上资产整体的安全防护能力，实时对安全设备进行分析和处理。

重大节假日安全防护

在法定节假日期间，企事业单位可能由于人力不足而无法对企业资产的安全性形成有效的防护与响应，需要借助于重要时期保障服务确保企业资产安全。