安全托管服务

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：2023-01-17 11:40:32

什么是安全托管服务

安全托管服务（Managed Security Service，MSS）为您提供持续、高效的安全监控和运营管理服务。通过安全托管服务，能够快速响应主机、网络、应用及数据等安全产品的各类安全风险事件，利用安全编排自动化与响应（SOAR）技术进行智能分类和高效运营处置，并针对云资产进行持续风险监视和泄露监控等，同时提供应急值守团队进行全天候安全保障，提升用户运营效率。

安全托管服务分为标准版和增强版两个版本，具体功能如下所示：

标准版 MSS 服务

安全评估服务

安全托管服务，可梳理用户云上资产情况，通过技术手段对互联网上的暴露面进行识别。同时对暴露的资产、云上主机、安全产品策略、云产品配置、应用 Web 端口、弱口令等风险进行扫描和探测，评估用户云上资产安全现状，并结合腾讯专家经验对安全风险等级进行划分。扫描类型包含两种：

- 全网资产扫描：针对全网系统进行系统层、Web 层扫描及风险分析。
- 对外系统扫描：针对面向公网开放的业务进行系统层、Web 层扫描及风险分析。

风险管理服务

对云上资产的防护覆盖度、安全产品策略评估、云账号配置等进行评估和安全通告。

威胁管理服务

安全托管服务可针对云安全产品运行状态、安全策略、安全事件及告警进行巡查，提供处置及优化建议：

- 开展安全产品的安全巡检和事件主动监控，及时发现安全隐患。
- 提供安全事件或告警处置建议或加固修复方案。

安全加固服务

安全托管服务可对安全评估过程中发现的风险，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）。

应急响应服务

安全托管服务可针对异常及入侵事件进行响应处置：

- 对黑客入侵等异常事件进行应急处理，帮助尽快恢复业务。
- 帮助用户进行入侵分析及溯源，提供应急响应分析报告。

服务经理对接

提供专业的服务经理进行项目对接，提供项目统筹协调、安全咨询、日常沟通、推动风险修复服务。

增强版 MSS 服务

增强版 MSS 服务包含了标准版MSS服务的内容，**以下仅展示差异点**:

安全评估服务

增强版 MSS 服务的安全评估服务，除提供标准版中的内容外，还额外提供安全运营能力评估，通过访谈、调查的方式，对用户的安全建设成熟度进行评估。

风险管理服务

对扫描到的安全风险，提供漏洞有效性验证，对暴露在互联网侧的高危及严重漏洞进行人工验证，每日对增量资产进行漏洞扫描（按需）。

对安全评估中所发现的漏洞和风险进行优先级管理，分级通告。

安全加固服务

安全产品配置，帮助用户进行安全产品接入和策略配置。

威胁管理服务

提供每日安全事件及情报类汇总信息，同步安全状态，实现状态可视化。同时提供代码等其他敏感信息的泄露监测。

漏洞情报服务

新型漏洞预警通报，实时同步互联网新型公开漏洞，对新型公开漏洞进行预警。同时针对受影响的资产进行匹配，对新型公开漏洞进行预警与排查。预警信息中包含漏洞信息、影响资产范围。

产品特性

最近更新时间：2023-01-17 11:40:31

智能驱动的运营

基于整体和近实时的威胁检测策略，云运营团队通过安全产品事件行为进行多因素关联分析，对捕获安全事件及处置用例进行分类，利用情报团队研究的预置检测框架，分析出用户云环境中存在的高优先级事件和触发原因，帮助企业制定安全防护和加固方案，提升对安全事件的可见性。

更快的响应速度

利用安全编排自动化与响应技术构建的风险处置引擎，可汇聚收集云端各类安全事件源，结合腾讯云用户安全最佳实践库，利用编排手段对高级别风险事件进行自动化响应处置，降低了人工运营和响应的时延，提升了事件处置的效率。

高效的风险监视

将漏洞事件、用户代码或敏感信息泄露行为自动化纳入安全监控范畴，一旦出现可能影响用户资产和业务的漏洞或泄露行为，将自动化触发风险处置流程，同步详尽风险处置方法，实现近实时级防护。

云原生兼容服务

原生集成用户在腾讯云安全产品的事件原始数据，能更好的监视云上关键资产变更风险，通过监视云资产的动态变化行为，可使安全监控策略即时覆盖新创建的云资产，保持监测策略的一致性、全面性。

深度的事件分析

针对出现的意外安全事件，腾讯云应急值守团队提供事件分析和溯源取证支持，通过日志和事件分析更深入地研究事件原因，帮助快速止损并恢复业务，并提供事件复盘和整改建议。

服务内容

最近更新时间：2023-01-17 11:40:32

本文档将为您介绍安全托管服务的详细服务内容及交付内容。

标准版 MSS 服务

以下为**标准版 MSS 服务**的服务内容和交付物：

服务分类	服务内容	交付内容
安全评估服务	通过安全规范、策略库及评估分析引擎，全面评估用户云上主机安全现状，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： • **互联网侧风险评估**：对互联网侧的暴露面和安全风险进行识别和评估，根据风险等级进行分类。 • **云上资产安全评估**：针对云上主机的软件成分进行分析（此服务项需主机安装了主机安全产品），对云上网络架构及安全组划分进行分析判断，发现安全风险。 • **安全产品策略优化**：针对用户所使用的云上安全产品 WAF、主机安全、云防火墙的覆盖率及策略进行评估，发现安全风险。 • **安全风险检测**：针对云安全特有的安全风险项，对 COS 存储桶策略配置、AK密钥泄漏等进行检测，发现安全风险。 • **评估报告答疑（按需）**：可安排工程师或服务经理对评估报告中所发现的安全风险进行答疑。 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。	**每季度一次**：提供《安全评估报告》
风险管理服务	每周对主机安全基线、配置策略、云账号进行风险核查，协助进行管理： • **基线核查服务**：针对用户主机的安全基线进行分析，对弱口令、未授权访问等进行评估和通告。 • **配置策略核查**：对安全防护覆盖、安全产品策略、云产品配置等进行评估和通告。 • **云账号核查**：针对云账号的双因素认证、不活跃账号、AK 等进行评估和通告。	**持续性服务**：提供并每周更新《风险跟踪表》
威胁管理服务	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： • **安全监控分析**：5*8实时监测网络安全状态，及时进行分析与预警。 • **安全事件分析处置**：针对已失陷安全事件，进行溯源分析。	**持续性日常检测**：每周输出《服务运营周报》

	• **AK密钥泄漏检测**：在 GitHub 等代码平台上对用户云账号的 AK 密钥泄漏事件进行检测。	
安全加固服务	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： **安全加固建议**：提供漏洞和风险修复方案以及安全加固指导。	输出物并入《安全评估报告》、《风险跟踪表》
应急响应服务	在用户业务出现遭受黑客攻击等异常情况时，提供及时的事件响应分析和专业处置，降低突发事件损失： **应急响应服务**：针对勒索病毒、挖矿病毒、文件篡改、木马后门、僵尸网络等事件，通过工具和方法对其进行处置，帮助客户尽快恢复业务，消除和减轻影响。	**按需提供，每季度最多提供一次**：触发条件包含如下两类场景： 1. 用户主动请求应急响应支持 2. MSS 服务团队发现异常启动应急响应应急完毕后，提供《应急响应报告》
漏洞情报服务	标准版暂不提供	–

增强版 MSS 服务

以下为增强版 MSS 服务的服务内容和交付物：

服务分类	服务内容	交付内容
安全评估服务	包含标准版全部内容，并额外提供服务如下： • **安全运营能力评估（每季度一次）**：通过访谈、调查等方式对安全成熟度进行评估，并给出安全建设建议。 • **漏洞扫描服务**：每周针对暴露在互联网上的资产进行全量的 Web 应用和主机漏洞扫描，每日对增量资产进行漏扫（需客户提供资产）。 • **风险修复规划**：对安全评估所发现的风险进行分类分级，按实际风险优先级给出风险修复建议。	**每月一次**：提供《安全评估报告》
风险管理服务	包含标准版全部内容，并额外提供服务如下： **漏洞优先级管理**：对漏洞扫描中发现的漏洞进行评估，基于漏洞的危害等级、互联网暴露情况、漏洞利用热度等多因素，对漏洞的修复优先级进行划分，分级通告。	**持续性服务**：提供《风险跟踪表》

威胁管理服务	包含标准版全部内容，并额外提供服务如下： • **每日安全状况汇总**：提供每日安全事件及情报类汇总信息，同步安全状态。 • **敏感数据泄漏监测**：对代码、用户数据等敏感数据的泄漏事件进行监测。	**持续性日常检测** • 每周输出《服务运营周报》 • 每日输出《安全状况日报》
安全加固服务	包含标准版全部内容，并额外提供服务如下： **安全产品配置服务**：帮助用户进行安全产品接入和策略配置。	输出物并入《安全评估报告》、《风险跟踪表》
应急响应服务	在用户业务出现黑客攻击等异常情况时，提供及时的事件响应分析和专业处置建议，降低突发事件损失： **应急响应服务**：针对勒索病毒、挖矿病毒、文件篡改、木马后门、僵尸网络等事件，通过工具和方法对其进行处置，帮助客户尽快恢复业务，消除和减轻影响。	**按需提供，不限制应急次数**： 触发条件包含如下两类场景： 1. 用户主动请求应急响应支持 2. MSS 服务团队发现异常启动应急响应应急完毕后，提供《应急响应报告》
漏洞情报服务	7×24持续监测、分析全网新型公开漏洞事件及数据泄露事件，进行漏洞影响资产排查，为用户提供云风险专业处置建议和参考解决方案，服务内容包括： • **新爆发漏洞预警通告**： 当监测到互联网上存在影响用户资产的新高危漏洞事件出现后，将开展分析并发布预警和修复方案，提醒用户修复。 • **新爆发漏洞受灾面排查**：当爆发新漏洞后，根据客户云上资产的比对，对漏洞的影响资产范围进行梳理，协助客户更快完成修复。	不定期，在法定工作日10:00 – 12:00、14:00 – 17:00时段，将会在30分钟内进行响应并输出：《重大漏洞通告》

优势能力

最近更新时间：2023-01-17 11:40:32

实时攻击者视角下的有效防守

基于攻防专家所积累的攻击面检测策略能力，实时发现企业暴露在外的攻击面并进行智能告警分类、威胁狩猎和事件响应。

云原生攻击防御能力矩阵

专业红队专家梳理的防御体系对抗策略，通过对实战演练的攻击经验沉淀，将新型攻击手法转化成验证策略，提升产品能力。

基于业务行为基线的威胁分析模型

腾讯丰富自研业务沉淀的业务行为基线机器学习模型，通过对业务行为动作的感知和分析，基于业务视角更快发现异常攻击行为。

KPI视角下的服务过程感知

通过平台实现工作调度及服务管理，记录服务交付节点及关键数据，事件通知驱动过程价值呈现，KPI 指标驱动结果价值呈现。

应用场景

最近更新时间：2023-01-17 11:40:32

日常安全运营支撑

适用场景

企业业务部署架构从传统 IT 机房模式转换为云模式，可能面临安全运营经验不足，人力缺失，监控系统不完善等问题。安全托管服务提供云上安全运营能力，能帮助企业降低人力压力，让企业专注业务建设。

解决方案

安全托管服务通过自研的自动化工作流系统，实现对用户日常安全产品事件进行5×8小时监控分析，帮助快速进行事件闭环响应，并提供日常安全事件咨询和应急响应支撑。具体流程如下图所示：