

安全运营中心

产品动态

产品文档



腾讯云

【 版权声明 】

©2013-2021 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 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。

产品动态

最近更新时间：2021-07-22 17:35:36

2021-07

动态名称	动态描述	发布时间	相关文档
安全事件升级	<ul style="list-style-type: none"> 支持检测恶意请求、高危命令、本地提权、反弹 Shell 事件。 优化 WAF 事件展示。 攻击链分布支持批量处理安全事件。 	2021-07-13	安全事件
云安全配置功能升级	部分检测项优化。	2021-07-13	云安全配置管理
漏洞管理功能升级	来自主机安全的 Web 漏洞支持查看漏洞路径。	2021-07-13	查看和处理漏洞
自动编排响应功能升级	<ul style="list-style-type: none"> 支持自定义图谱编排。 优化概览页指标。 新增剧本中心。 新增响应事件列表。 新增操作记录。 新增白名单设置 	2021-07-05	自动编排响应

2021-04

动态名称	动态描述	发布时间	相关文档
自动编排响应功能升级	新增2个自动编排响应剧本： <ul style="list-style-type: none"> 资产高危漏洞风险统计剧本。 公网暴露资产风险排查剧本。 	2021-04-07	自动编排响应
安全事件功能升级	“处理”操作文案优化。	2021-04-07	安全事件

2021-03

动态名称	动态描述	发布时间	相关文档
------	------	------	------

动态名称	动态描述	发布时间	相关文档
自动编排响应功能升级	<ul style="list-style-type: none"> 封禁 IP 时长由“30分钟”改成“24小时”。 封禁 IP、隔离病毒文件支持撤回。 	2021-03-15	自动编排响应
安全评估报告功能升级	安全评估报告内容升级。	2021-03-15	安全评估
风险周报功能升级	风险周报全新升级。	2021-03-15	产品设置

2021-02

动态名称	动态描述	发布时间	相关文档
安全事件功能升级	“异地登录”改成“异常登录”。	2021-02-25	事件列表

2021-01

动态名称	动态描述	发布时间	相关文档
云安全配置管理功能升级	对检查项及资产忽略检查时，支持添加备注。	2021-01-13	云安全配置管理
合规管理功能升级	对检查项及资产忽略检查时，支持添加备注。	2021-01-13	合规管理
安全事件功能升级	<ul style="list-style-type: none"> 攻击链分布支持时间筛选与攻击阶段、事件子类联动。 事件列表支持导出全部字段。 	2021-01-13	安全事件
泄露监测功能升级	自定义泄露事件支持导出。	2021-01-13	自定义泄露事件
日志审计功能升级	支持检索堡垒机日志。	2021-01-13	日志检索
自动编排响应功能升级	对图谱进行优化。	2021-01-13	自动编排响应

2020-12

--	--	--	--

动态名称	动态描述	发布时间	相关文档
仪表盘功能升级	安全评分的评分看板支持取消纳入评分。	2020-12-22	安全评分
报表中心功能升级	报表列表支持管理剧本响应生成的报表。	2020-12-22	报表列表
资产中心功能升级	风险标签支持筛选。	2020-12-22	云资产
漏洞管理功能升级	<ul style="list-style-type: none"> 接入漏洞扫描服务网站、API 类漏洞库。 待处理漏洞看板支持根据漏洞导出漏洞详情及修复方案。 漏洞列表导出功能支持导出修复方案。 漏洞列表支持忽略记录管理。 	2020-12-22	查看和处理漏洞
互联网攻击面测绘功能升级	新增NAT网关测绘。	2020-12-22	互联网攻击面测绘
网络安全功能升级	流量威胁感知白名单管理支持加白 IP 段。	2020-12-22	流量威胁感知
自动编排响应功能升级	<ul style="list-style-type: none"> WAF 巡检报表剧本新增报表。 剧本列表页新增事件响应趋势图、最新报表、需人工跟进事件、响应失败事件、累计记录黑 IP 个数及累计封禁次数。 剧本详情页新增封禁次数、TOP5 攻击源IP威胁情报查询情况、最新封禁IP记录、漏洞种类分布、TOP5 被攻击资产、最新发现的病毒文件及存在病毒最多的 TOP5 资产。 支持联动云防火墙封禁 IP 等。 	2020-12-22	自动编排响应
产品设置功能升级	通知管理支持设置通知接收人。	2020-12-22	产品设置

2020-10

动态名称	动态描述	发布时间	相关文档
安全事件功能升级	<ul style="list-style-type: none"> 支持联动云防火墙拦截 IP。 支持管理云防火墙和 Web 应用防火墙拦截列表。 事件列表支持查看关联分析告警。 	2020-10-23	安全事件
流量威胁感知功能升级	<ul style="list-style-type: none"> 支持联动云防火墙拦截 IP。 支持管理云防火墙和 Web 应用防火墙拦截列表。 	2020-10-23	流量威胁感知

新增自动编排响应	新增4个自动编排响应剧本： <ul style="list-style-type: none"> 流量威胁外连黑主机剧本 流量威胁漏洞利用剧本 主机安全反病毒木马剧本 WAF 巡检报表剧本 	2020-10-23	自动编排响应
----------	--	------------	------------------------

2020-09

动态名称	动态描述	发布时间	相关文档
资产中心功能升级	资产类型增加 VPN 网关。	2020-09-09	云资产
漏洞管理功能升级	<ul style="list-style-type: none"> 接入漏洞扫描服务数据并支持下发扫描。 新增资产漏洞列表，支持从资产维度查看来源主机安全和漏洞扫描服务的风险分布情况。 	2020-09-09	查看和处理漏洞
泄露监测功能升级	高级版自定义监测规则上限增为50条。	2020-09-09	泄漏监测
体验优化	<ul style="list-style-type: none"> 列表支持资产 ID 筛选功能。 资产列表及资产详情支持查看资产名称。 列表时间筛选新增“近半年”快捷按钮。 云安全配置管理、合规管理“全部检测”及“自动检测设置”入口优化。 流量威胁感知拦截列表位置调整。 	2020-09-09	<ul style="list-style-type: none"> 泄漏监测 合规管理 云资产 云安全配置管理 流量威胁感知

2020-07

动态名称	动态描述	发布时间	相关文档
报表中心功能升级	报表中心预设一个周期为7天的报表任务，支持编辑。	2020-07-30	报表任务
资产中心功能升级	资产列表、全局资产详情新增风险标签。	2020-07-30	<ul style="list-style-type: none"> 云资产 网络可视化分析
互联网攻击面测绘功能升级	<ul style="list-style-type: none"> 暴露端口新增加固建议。 测绘设置入口优化。 	2020-07-30	互联网攻击面测绘
云安全配置功能升级	检查项的事件列表支持查看资产的风险描述。	2020-07-30	-

攻击链分布功能升级	密码破解在攻击链分布中细化为爆破尝试和爆破成功。	2020-07-30	安全事件
安全事件、流量威胁感知功能升级	支持联动 Web 应用防火墙拦截 IP。	2020-07-30	流量威胁感知
体验升级	<ul style="list-style-type: none"> 未通过资产或安全事件，用比例展示。 互联网攻击面测绘暂无暴露时文案优化。 全局 IP 支持复制。 	2020-07-30	-
安全评估功能升级	安全评估报告新增漏洞概况、失陷资产、关联规则告警、GitHub API 密钥泄露告警内容。	2020-07-27	-
安全评估功能升级	支持申请安全专家免费解读。	2020-07-17	-

2020-06

动态名称	动态描述	发布时间	相关文档
新增关联事件功能	关联分析功能可将安全运营中心的流量威胁感知功能，检测到的云上流量威胁与资产漏洞、资产中安装组件及资产对外开放攻击面等信息进行关联分析，同时也可对不同安全产品产生的安全事件进行自动化关联分析，帮助您识别云上有效的事中攻击及高风险威胁，提升云上安全运营和分析效率。	2020-06-23	安全事件
新增网络可视化分析	网络可视化分析功能为您提供可交互图形化的云上网络可视化分析能力，帮助您直观掌握云上VPC、子网与实例间的网络拓扑关系，并快速在图形中进行云资产风险的运营与加固。同时，您可在网络拓扑中按需快速查看资产的网络流量情况，对云资产的网络流量进行直观监控，可帮助您全面掌握云上资产整体网络安全情况。	2020-06-23	网络可视化分析
流量威胁感知功能升级	支持白名单管理。	2020-06-23	流量威胁感知
细节优化	<ul style="list-style-type: none"> 调查中心更名为日志审计。 响应中心>忽略规则管理入口调整。 有资产数据的列表支持资产 IP、资产 ID、资产名称搜索。 	2020-06-23	日志检索
安全评分升级	安全评分新增重新检测功能。	2020-06-03	安全评分

新增安全评估功能	<ul style="list-style-type: none"> 免费版支持一次免费云安全评估，支持导出安全评估报告。 高级版支持安全评估功能，可持续进行一键安全评估和风险汇总，支持评估报告导出。 	2020-06-03	安全评估
安全大屏功能升级	新增安全大屏： <ul style="list-style-type: none"> 新版本云安全总览大屏。 资产安全中心大屏。 	2020-06-03	安全大屏
云资产功能升级	<ul style="list-style-type: none"> 新增支持容器镜像仓库、云硬盘 CBS、云数据库 MongoDB 类型资产的自动化盘点。 资产详情优化。 	2020-06-03	云资产
应急漏洞功能升级	最近检测结果优化，存在风险资产支持查看和忽略。	2020-06-03	应急漏洞
云安全配置管理功能升级	新增10个检查项： <ul style="list-style-type: none"> 支持容器镜像仓库 - 权限检查。 支持 CBS - 定期快照检查。 支持 CBS - 加密状态检查。 支持 MariaDB - 开启数据库备份检查。 支持 MySQL - 开启数据库备份检查。 支持 Redis - 开启数据库备份检查。 支持 PostgreSQL - 开启数据库备份检查。 支持 CVM - 安全组配置检查。 支持 MySQL - 数据库安全组配置检查。 支持 Redis - 数据库安全组配置检查。 	2020-06-03	-
合规管理功能升级	新增15个检查项： <ul style="list-style-type: none"> 容器镜像仓库：安全通用要求 - 安全计算环境 - 访问控制(8.1.4.2)。 CBS - 定期快照：云计算安全扩展要求 - 安全计算环境 - 数据备份恢复 (8.2.4.6)。 CBS - 加密状态：云计算安全扩展要求 - 安全计算环境 - 数据完整性和保密性。(8.2.4.5)。 CVM：安全通用要求 - 安全区域边界 - 访问控制 (8.1.3.2)。 MySQL：安全通用要求 - 安全计算环境 - 数据备份恢复 (8.1.4.9)。 Redis：安全通用要求 - 安全计算环境 - 数据备份恢复 (8.1.4.9)。 PostgreSQL：安全通用要求 - 安全计算环境 - 数据备份恢复 (8.1.4.9)。 MariaDB：安全通用要求 - 安全计算环境 - 数据备份恢复 (8.1.4.9)。 	2020-06-03	-

	<ul style="list-style-type: none"> • MySQL: 云计算安全扩展要求 – 安全物理环境 – 基础设施位置 (8.2.1.1)。 • Redis: 云计算安全扩展要求 – 安全物理环境 – 基础设施位置 (8.2.1.1)。 • MongoDB: 云计算安全扩展要求 – 安全物理环境 – 基础设施位置 (8.2.1.1)。 • PostgreSQL: 云计算安全扩展要求 – 安全物理环境 – 基础设施位置 (8.2.1.1)。 • MariaDB: 云计算安全扩展要求 – 安全物理环境 – 基础设施位置 (8.2.1.1)。 • MySQL: 安全通用要求 – 安全区域边界 – 访问控制 (8.1.3.2)。 • Redis: 安全通用要求 – 安全区域边界 – 访问控制 (8.1.3.2)。 		
泄露监测功能升级	<ul style="list-style-type: none"> • 与 Github 官方合作实现云 SecretKey 的泄漏监测。 • 新增泄露防护方案。 • 泄露事件、监测规则更名为自定义泄露事件、自定义监测规则。 	2020-06-03	<ul style="list-style-type: none"> • Github API 泄露监测 • 泄露防护方案
响应中心功能升级	新增支持 Linux 反弹 shell、Windows 反弹 shell 的编排响应剧本。	2020-06-03	响应中心
全局优化	<ul style="list-style-type: none"> • 安全事件、流量威胁感知、漏洞列表支持全部处理。 • 其他交互优化。 	2020-06-03	-

2020-05

动态名称	动态描述	发布时间	相关文档
漏洞功能升级	<ul style="list-style-type: none"> • 新增待处理漏洞看板。 • 漏洞列表新增漏洞概况汇总和待处理漏洞趋势图。 • 状态变更升级。 	2020-05-08	查看和处理漏洞
安全事件功能升级	<ul style="list-style-type: none"> • 新增根据攻击链分布汇总安全事件。 • 支持批量处理来源为流量威胁感知的安全事件。 	2020-05-08	安全事件
合规管理功能升级	处置操作支持精确跳转。 新增检查项: <ul style="list-style-type: none"> • COS-Bucket: 安全通用要求-安全计算环境-访问控制 (8.1.4.2) • COS-Bucket: 安全通用要求-安全计算环境-安全审计 (8.1.4.3) 	2020-05-08	-

	<ul style="list-style-type: none"> • COS-Bucket:安全通用要求-安全区域边界-访问控制 (8.1.3.2) • COS-Bucket:安全通用要求-安全计算环境-数据保密性 (8.1.4.8) 		
云安全配置管理功能升级	处置操作支持精确跳转。 新增检查项： <ul style="list-style-type: none"> • COS-Bucket 策略设置 • COS-Bucket 日志配置管理 • COS-Bucket 防盗链检查 • COS-Bucket 存储桶加密检查 	2020-05-08	-
攻击面测绘功能升级	支持设置和删除评分白名单。	2020-05-08	互联网攻击面测绘
调查中心功能升级	支持堡垒机日志接入和检索。	2020-05-08	日志接入
通知管理升级	<ul style="list-style-type: none"> • 支持合规管理、泄露监测通知。 • 漏洞通知支持设置允许通知漏洞来源、漏洞类型。 • 安全事件通知支持设置允许通知事件来源、事件子类。 • 泄露监测支持设置允许通知情报来源。 	2020-05-08	产品设置

2020-04

动态名称	动态描述	发布时间	相关文档
新增计费模式	支持后付费模式。	2020-04-16	计费概述
安全评分升级	新增安全评分看板，展示评分详细风险点及处理建议。	2020-04-16	安全评分
资产中心升级	<ul style="list-style-type: none"> • 支持查看资产发现时间与下线时间。 • 支持历史资产的管理。 • 支持自定义选择是否展示历史资产相关记录。 	2020-04-16	<ul style="list-style-type: none"> • 历史资产 • 产品设置
免费版风险周报升级	免费版风险周报升级。	2020-04-16	产品设置
基础功能升级	<ul style="list-style-type: none"> • 漏洞列表、安全事件、合规管理、云安全配置支持导出列表数据。 • 合规管理和云安全配置管理支持批量取消忽略 	2020-04-16	<ul style="list-style-type: none"> • 安全事件 • 合规管理
导航升级	导航栏增加分段名、部分功能入口位置调整。	2020-	-

		04-16	
体验升级	交互文案优化。	2020-04-16	-
计费升级	支持按月自动续费。	2020-04-03	续费说明
UBA 功能升级	新增用户权限提升、用户权限遍历、资产高风险权限修改、新用户高危操作4个风险场景检测。	2020-04-01	<ul style="list-style-type: none"> UBA 概览 风险场景
漏洞管理功能升级	漏洞列表支持确认处理、标为修复中、忽略、取消忽略，漏洞详情可查看更多漏洞信息和修复方案。	2020-04-01	漏洞管理
互联网攻击面测绘功能升级	互联网攻击面测绘支持设置测绘模式，包括轻度、中度及深度模式。	2020-04-01	互联网攻击面测绘
全局资产“详情提示”升级	全局资产“详情提示”支持查看攻击面、云产品配置、安全事件及漏洞等风险情况。	2020-04-01	安全事件
体验升级	交互文案优化。	2020-04-01	-

2020-03

动态名称	动态描述	发布时间	相关文档
等保合规功能升级	合规管理等级保护检查项及检查资产支持忽略和取消忽略。	2020-03-12	合规管理
网络安全-流量威胁感知功能升级	新增攻击 payload 的详情展示，支持批量取消已忽略资产。	2020-03-12	网络安全
安全事件功能升级	新增支持流量威胁原始事件管理。	2020-03-12	安全事件
互联网攻击面测绘功能升级	支持批量取消已忽略资产。	2020-03-12	互联网攻击面测绘
体验升级	漏洞管理、安全事件、泄露监测等功能交互升级。	2020-03-12	-

2020-02

动态名称	动态描述	发布时间	相关文档
------	------	------	------

高级版正式发布	新增以下高级版功能： <ul style="list-style-type: none"> 提供安全检测和响应处置能力，包括流量威胁检测、互联网攻击面测绘、云安全产品配置检查、等保合规检查、应急漏洞预警、响应中心自动化响应等。 提供安全运营管理功能，包括资产自动盘点、日志审计与检索、安全报表、安全仪表盘、安全大屏、告警通知配置等。 	2020-02-18	购买方式
新增流量威胁检测功能	威胁感知能力，可帮助您实现云上外到内和内到外的双向流量威胁检测，覆盖漏洞利用、Web 攻击、口令爆破、僵尸网络主机、挖矿行为、对外漏洞攻击等多种威胁的检测。	2020-02-18	网络安全
新增互联网攻击面测绘功能	互联网资产测绘功能，帮助您发现暴露在互联网上的资产 IP、端口及服务暴露面。同时安全运营中心高级版将资产测绘与安全情报相结合，实现自动化的监测与预警，帮助您全面收敛互联网攻击暴露面，提升安全预防能力。	2020-02-18	互联网攻击面测绘
新增云安全产品配置检查功能	提供腾讯云上相关云产品的安全配置检查功能，包括计算与应用配置安全、网络配置安全、存储与数据安全及身份接入安全四大维度的安全配置检查与管理，为您在腾讯云上业务的安全运行提供坚实的基础保障。	2020-02-18	云安全配置管理
新增等保合规检查功能	根据等级保护等合规标准要求，为您实现合规风险的自动化持续评估，并为您提供合规态势及合规建议。	2020-02-18	合规管理
新增应急漏洞预警功能	依托腾讯云全网威胁情报为您提供应急漏洞推送功能，帮助您快速感知最新漏洞事件。	2020-02-18	漏洞管理
新增响应中心自动化响应功能	提供云原生的安全编排与自动化响应处置功能，可针对云上安全事件为您提供安全编排剧本，实现高效的自动化响应处置。	2020-02-18	响应中心
新增日志审计与检索功能	云上的统一安全日志审计与检索调查平台，包含主机安全告警、Web 应用防火墙告警、DDoS 防护告警、云用户操作行为等安全相关日志数据，您可根据实际不同安全场景，按需进行检索调查。	2020-02-18	调查中心
新增安全报表功能	提供完善的报表管理功能，您可以根据需要创建单次或周期报表任务生成安全报表，构建云上常态化安全报表。	2020-02-18	报表中心
新增安全仪表盘功	安全可视仪表盘实时展示云上整体安全态势信息，包	2020-	仪表盘

能	括安全评分信息、最新待处理问题、合规管理、云安全配置、漏洞趋势、安全事件趋势、用户活动趋势和泄露事件趋势，帮助您对云上安全态势进行统一的安全管控。	02-18	
新增安全大屏功能	提供安全总览、网络安全及主机安全等安全大屏功能，帮助您实现云上安全态势及安全建设成果的直观可视化呈现。	2020-02-18	安全大屏
新增告警通知配置功能	提供告警通知配置功能，您可根据风险等级、通知时间等对周期报表任务、单次报表任务、互联网攻击面测绘、漏洞列表、应急漏洞、云安全配置管理、安全事件、响应中心项目进行配置。	2020-02-18	产品设置