安全托管服务

服务协议

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2023 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】

腾讯云

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。

文档目录

服务协议
服务等级协议

最近更新时间：2023-05-16 16:22:11

详细信息，请参见 安全托管服务服务等级协议 。

漏洞扫描与安全测试授权协议

最近更新时间：2021-07-06 10:13:55

致：腾讯云计算（北京）有限责任公司

鉴于：

贵司的腾讯云安全托管（以下简称“MSS”）提供的安全评估服务，是通过漏洞扫描、安全测试对腾讯公有云资产的安全状况进行评估，同时针对发现的问题提供修复建议参考，旨在帮助我单位降低网络安全风险。我单位已详细阅读 腾讯官网 MSS 产品的有关介绍，且已详细了解 MSS 服务及其相关的安全检测原理，我单位对该服务相关方案的风险已知悉并同意自行承担由此产生的一切责任，在此同意并授权贵司对我单位部署在腾讯云公有云上的全部系统和资产（包括但不限于主机、域名）进行安全评估。具体授权内容如下：

我单位现同意并不可撤销地授权贵司：

1. 对我单位部署在腾讯云公有云上的全部系统和资产（资产包括我单位部署在腾讯云公有云的全量主机资产、域名资产等，全文同）通过漏洞扫描、安全测试等方式进行安全评估。
2. 贵司可采取的安全评估方式包括：
   2.1 漏洞扫描：贵司可远程自动探测我单位部署在腾讯云公有云上的全部系统和资产并识别其风险、对前述系统和资产的互联网暴露风险面、N Day 漏洞与合规性进行安全扫描。
   2.2 安全测试：贵司可利用工具远程自动化或半自动化探测我单位部署在腾讯云公有云上的系统和资产并识别其风险、对前述系统和应用资产的漏洞、OWASP TOP10漏洞进行测试。
3. 授权时间为 MSS 服务开通之日起至MSS正式服务有效期届满之日止。

我单位理解并同意：

1. 我单位确认已阅读并详细了解 MSS 的全部内容和扫描测试细节，知晓扫描和测试期间可能会影响我单位系统和资产的正常运行（如服务带宽的占用、服务器或数据库异常），可能导致我单位系统无法正常使用，对此贵司无需任何责任。

2. 我单位通过使用 MSS 获得的安全评估结果与实际是否相符由我单位自行掌握和判断，贵司不对我单位因使用或参考安全评估结果的内容或信息而造成的损失负责。

应急响应授权协议

最近更新时间：2022-10-13 16:46:52

致：腾讯云计算（北京）有限责任公司
鉴于：
贵司的腾讯云安全托管服务（以下简称“MSS”）提供的应急响应服务，是通过漏洞探测、登录主机进行入侵排查以帮助我单位对安全事件应急和溯源。我单位已详细阅读 腾讯云官网 MSS 产品的有关介绍，且已详细了解 MSS 服务及其相关的应急响应流程和原理，我单位对该服务相关方案的风险已知悉并同意自行承担由此产生的一切责任，在此同意并授权贵司对我单位部署在腾讯云公有云上的授权资产（如主机）进行应急响应。具体授权内容如下：

我单位现同意并不可撤销地授权贵司：

1. 对我单位部署在腾讯云公有云上需要应急响应的主机进行登录排查和攻击溯源分析。
2. 贵司可采取的应急响应处置方式包括：
   2.1 漏洞探测：贵司可远程自动探测我单位部署在腾讯云公有云上的授权资产（如主机）进行漏洞探测，分析和排查攻击手段和路径等。
   2.2 登机排查：贵司可通过远程端口登录、VNC 登录或 VPN 登录等形式访问我单位部署在腾讯云公有云上的授权资产（如主机）进行入侵排查、攻击溯源等。
3. 授权时间为应急响应服务开通之日起至应急响应服务结束止。

我单位理解并同意：

1. **我单位确认已阅读并详细了解MSS的全部内容和应急响应细节，知晓应急响应需登录主机进行排查和进行漏洞探测等操作，可能会影响我单位系统和资产的正常运行，对此贵司无需承担责任，我司授权贵单位进行远程漏洞探测、登机排查等应急响应服务所需的所有必要操作权限。**
2. **我单位通过使用贵司服务获得的结果与实际是否相符由我单位自行掌握和判断，贵司不保证服务结果的真实性、准确性和适用性。如果我单位使用贵司的服务对未获授权的系统及产品进行应急响应操作，给我单位或第三方造成了任何损失，由我单位负责解决并承担相关责任。**

版权所有：腾讯云计算（北京）有限责任公司