

重要时期安全保障服务

常见问题



腾讯云

【 版权声明 】

©2013–2025 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或 95716。

常见问题

最近更新时间：2022-04-01 17:41:29

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），在重大事件期间或法定节假日期间，为用户提供针对于云上资产的安全保障服务。整体服务周期包含保障前期的风险面探测、服务器协助加固，保障期间的安全设备监控、安全事件的应急响应处理，保障后期的整体过程复盘与提升。使用重要时期安全保障服务，高效发现并阻断安全事件，降低资产的网络攻击风险。

重要时期安全保障服务具备哪些安全能力？

重要时期安全保障服务提供了保障前期的安全评估、风险检测、风险处置、渗透测试，保障中期的漏洞感知与泄漏监测、安全监控、应急响应等能力，覆盖重要时期安全保障服务的各个关键阶段。

重要时期安全保障服务主要分析哪些安全事件？

重要时期安全保障服务主要分析安全产品的事件、产品安全策略配置事件、最新安全漏洞事件及数据泄露事件等。

重要时期安全保障服务有什么条件限制么？

建议在重要时期安全保障服务开始前至少五天完成购买，需要为安全评估以及加固预留时间。

在处置安全事件时，是否会告知风险或危害？

重要时期安全保障团队在重要时期安全保障服务前期会与用户明确在服务期间，各类安全事件的应急预案和处置办法。当处置操作可能会影响用户业务自身稳定性及可用性时，会与用户沟通并在取得用户同意后会进行处理。