云安全中心

实践教程

腾讯云

【版权声明】

【商标声明】

【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。

文档目录

实践教程
等级保护测评解读

最近更新时间：2024-02-26 14:43:01

云安全中心产品符合等级保护2.0标准体系主要标准。根据《网络安全等级保护基本要求》（GB/T 22239-2019），云安全中心高级版满足第三级及以下安全要求：

等保标准章节	等保标准序号	等保标准内容	云安全中心对应功能	功能解读
安全区域边界-安全审计	8.1.3.5 a)	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	日志审计	云安全中心可集中存储 xx 时间的日志数据，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
安全区域边界-安全审计	8.1.3.5 b)	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
安全区域边界-安全审计	8.1.3.5 c)	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	日志审计	云安全中心日志通过多副本实时存储多分，保障用户日志在其存储周期内不丢失、可恢复
安全计算环境-安全审计	8.1.4.3 a)	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
安全计算环境-	8.1.4.3 b)	审计记录应包括事件的日期和时间、用户、事件类型、事件	日志审计	云安全中心日志审计模块可审计相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息

安全审计		是否成功及其他与审计相关的信息		
安全计算环境-安全审计	8.1.4.3 c)	应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	日志审计	云安全中心日志通过多副本实时存储多分，保障用户日志在其存储周期内不丢失、可恢复
安全区域边界-集中管控	8.1.5.4 f)	应能对网络中发生的各类安全事件进行识别、报警和分析	威胁告警	云安全中心可通过威胁分析将全网不同安全产品识别的告警进行分析，并结合威胁情报及事件调查能力，将告警串联起来，形成事件攻击链，帮助安全管理员更好的判断与处置问题