云安全中心

常见问题

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。

常见问题

最近更新时间：2024-09-05 10:12:51

云安全中心是否只是对其他云安全产品日志进行采集分析?

云安全中心产品除了采集其他安全产品的日志进行统一管理外，自身也提供了多种安全检测能力，例如云安全配置风险检查、合规风险检查及用户风险操作行为检测等。
这些检测能力对云上安全产品的检测能力进行了全面有效的补充，同时云安全中心也打通了云上的各类安全产品形成联动响应处置，帮助用户提升威胁响应处置效率。

云安全中心当前支持安全配置检查的云资产包括哪些?

目前支持对 CVM、CLB、MySQL、Redis、MariaDB、PostgreSQL、COS、CBS、容器镜像及 SSL 证书，共10类云资产的云安全配置风险检查及统一安全管理。

云安全中心支持采集云上哪些安全日志?

云安全中心目前支持采集云上的两类安全相关日志：

- 第一类为云上安全产品的安全事件日志，包括主机安全、容器安全服务、Web 应用防火墙及 DDoS 防护等产品。
- 第二类为云上用户操作行为相关数据，包括云用户属性信息、用户操作记录及用户风险操作等日志。

云安全中心如何帮助客户满足等保合规要求?

云安全中心提供的网络入侵检测功能，可以满足等保对外到内和内到外的攻击威胁检测要求，同时日志审计可满足等保针对“安全管理中心”的相关要求。具体可参见 等级保护测评解读 。

云安全中心当前资产数超过购买授权资产数该如何处理?

云安全中心的购买授权资产数不得少于当前实际资产数，当用户实际资产数超过购买授权资产数20%后，云安全中心将会提示用户扩展资产授权。