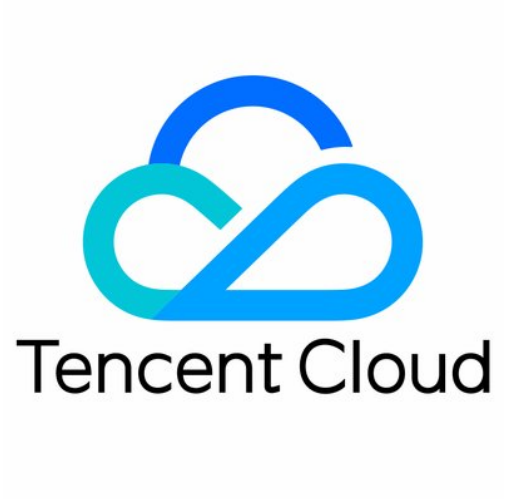
Cloud Security Center

FAQs

Product Documentation



FAQs

Last updated：2024-08-02 10:14:18

Does CSC Only Collect and Analyze Logs from Other Cloud Security Products?

In addition to collecting logs from other security products for unified management, CSC also provides various security detection capabilities, such as cloud security configuration risk detection, compliance risk detection, and risky operation behavior detection of users.
These detection capabilities comprehensively and effectively supplement the detection capabilities of cloud security products. At the same time, CSC integrates various cloud security products to form a joint response and handling mechanism, helping users enhance threat response and handling efficiency.

Which Cloud Assets Are Currently Supported by CSC for Security Configuration Detection?

Currently, CSC supports cloud security configuration risk detection and unified security management for 10 types of cloud assets, including CVM, CLB, MySQL, Redis, MariaDB, PostgreSQL, COS, CBS, container images, and SSL certificates.

Which Security Logs Does CSC Support Collecting in the Cloud?

Currently, CSC supports collecting two types of security-related logs in the cloud:
The first type is security event logs from cloud security products, including CWPP, WAF, and Anti-DDoS.
The second type is user operation-behavior-related data, and the logs include cloud user attribute information, user operation records, and user risky operations.

How Should CSC Process the Situation Where the Current Number of Assets in CSC Exceeds the Number of Purchased Licensed Assets?

The number of purchased licensed assets in CSC can not be less than the current actual number of assets. When the user's actual number of assets exceeds the number of purchased licensed assets by 20%, CSC will prompt the user to increase the number of licensed assets.