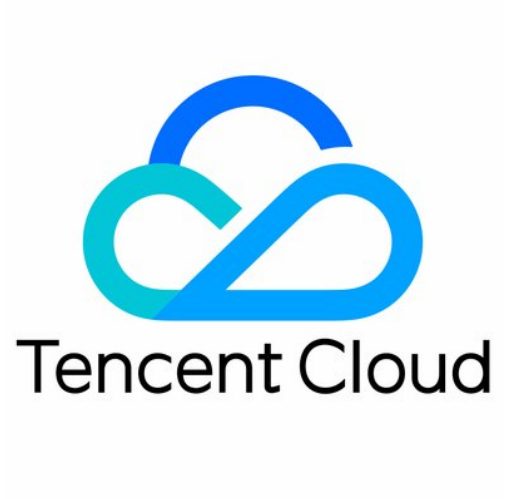
Cloud Workload Protection Platform

Glossary

Product Documentation



Glossary

Last updated：2023-12-26 16:41:41

Security baseline

A security baseline is a specific set of standards and basic requirements that relevant system and service security configurations must meet to satisfy security needs. Projects of different configurations and policies, such as account configuration security, password configuration security, authorization configuration, log configuration, and network configuration, can be used to evaluate whether a product has met the security baseline. The evaluation result reflects the server security to some extent.

Host vulnerability detection

Host vulnerability detection refers to the method of CWPP Agent to detect vulnerabilities on a host (server). The vulnerability detection module runs on the server and can directly verify or collect information to determine whether the server has vulnerabilities.

System component

In a general sense, a component (or common component) at the host layer refers to a web container or software program corresponding to a service or application, such as Nginx and WordPress. A system component mainly refers to non-web system software.

Common component vulnerability

A common component vulnerability (aka common vulnerability) mainly refers to a vulnerability in a common component instead of business code, such as SQL injection in WordPress and ShellShock in a component's Bash.

Unauthorized access

Unauthorized access is a type of problems caused by failure to meet the security baseline and mainly refers to the lack of restrictions on the conditions for access to certain services, such as password setting and access source restriction. In this case, anyone can directly connect to the service and perform operations, resulting in security problems.

Login audit

Login audit collects RDP and SSH login logs from the server, reports information such as source IP address, time, login username, and login status to the cloud for risk calculation, and alerts you to illegal login behaviors in real time.

File quarantine

The quarantine technology is to quarantine and store malicious trojans and virus files to prevent them from spreading.

Lexical analysis

The scanning and blocking module extracts sequences that meet the configured PHP lexical rules from text files and excludes other characters in the files, which greatly improves the detection accuracy.