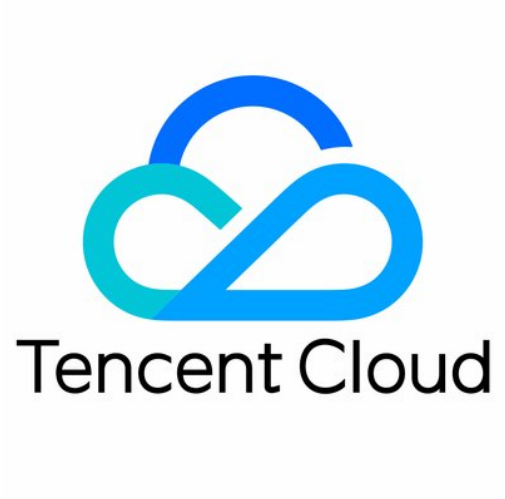
Security Operations Center

Product Introduction

Product Documentation



©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

©2013-2022 Tencent Cloud. All rights reserved.

Product Introduction
Overview

Last updated：2020-08-18 18:04:22

What is the Security Operations Center?

Security Operations Center (Security Operation Center,SOC) is Tencent Cloud native's unified security operation and management platform, which provides capabilities such as asset automation stocktaking, Internet attack surface mapping, cloud security configuration risk inspection, compliance risk assessment, Traffic threat awareness, leak monitoring, log audit and retrieval investigation, security orchestration and automatic response, and security visualization to help cloud users achieve security prevention in advance. Event monitoring and threat detection, one-stop, visual and automated cloud security operation management.

Features

Internet Traffic threat perception

Carry out threat awareness against Internet Traffic to help customers detect Internet internal attacks and abnormal outreach behaviors of internal assets to the Internet, including Vulnerability's perception of threats such as attacks, command injection attacks, Brute force attacks attacks, botnet hosts, host mining behavior, Proxy tunnel behavior and so on.

Asset Security Center

Help customers automate cloud assets stocktaking. Stocktaking includes Cloud Virtual Machine, Cloud Object Storage, cloud database, cloud Cloud Load Balancer and other assets. At the same time, through a variety of security dimensions such as cloud configuration risk, Vulnerability and security events, asset security risks are managed uniformly to reduce the risk of "shadow IT" (IT assets unknown to IT administrators) on the cloud.

Cloud Security configuration Management

Provide automatic inspection and assessment of Tencent Cloud services configuration risks, covering various Tencent Cloud services, such as Cloud Virtual Machine, Cloud Object Storage, cloud database and Cloud Load Balancer, to help customers reduce the security risks caused by Tencent Cloud services's incorrect security configuration and improve the overall cloud security level.

Internet attack surface mapping

©2013-2022 Tencent Cloud. All rights reserved.

Aiming at Open's cloud assets on the Internet, provide Internet attack surface mapping function to help users quickly identify potential attack surfaces such as Open ports, Open services and Open components of cloud assets, and take precautions.

Unified operation of security events

Uniformly collect and store the security events detected by various security products on the cloud to help customers achieve convenient and unified operation and management of security events on the cloud.

Log audit and retrieval investigation

Collect all kinds of cloud security-related data, such as cloud security product alarm data, cloud asset configuration change data, cloud user behavior data and some Tencent Cloud services log data, and provide a unified retrieval and investigation platform to help users achieve comprehensive cloud log audit and retrieval investigation.

Security visualization

Through the security dashboard, security screen and security report center to achieve the global visualization of security on the cloud, to help customers to achieve real-time monitoring of the security situation and intuitive visualization of security construction results.

Security orchestration and automatic response

Provide security orchestration and automatic response functions. Through the built-in security orchestration script, you can automatically respond to a variety of security events and improve the efficiency of security incident response handling on the cloud.

Compliance management

In response to some of the compliance requirements in Grade Protection 2.0, the Security Operations Center provides automated dynamic compliance assessment and reinforcement recommendations, and customers can continuously monitor and evaluate the compliance risks of cloud assets as needed.

Cloud UBA

Provide visual audit and monitoring for cloud users' actions and cloud API calls, and detect alarms for sensitive and risk operations to identify security risks caused by users' abnormal behavior and risk API calls.

©2013-2022 Tencent Cloud. All rights reserved.