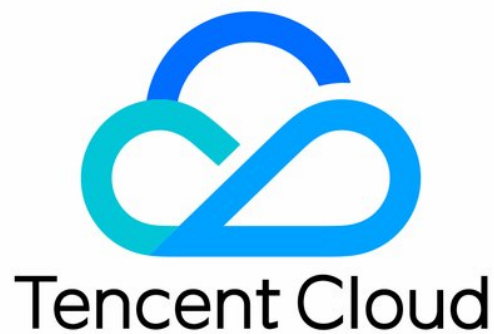


Security Situation Awareness

Product Introduction

Product Documentation



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



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

Product Introduction

Overview

Features

Product Introduction

Overview

Last updated : 2018-12-06 11:12:16

What Is SSA?

Tencent Cloud Security Situation Awareness (SSA) is a big security data visualization platform that provides visibility into businesses, assets, threats and risks based on the customer's cloud security data and Tencent's massive security data. Through multi-dimensional, intelligent, continuous analysis of massive amounts of data, SSA helps identify potential internal and external risks and predict impending security threats.

Main Features

Security Events

SSA can monitor and audit various attacks such as DDoS attacks, web attacks, off-site logins and brute force attacks and detect trojan files.

Security Situation Overview

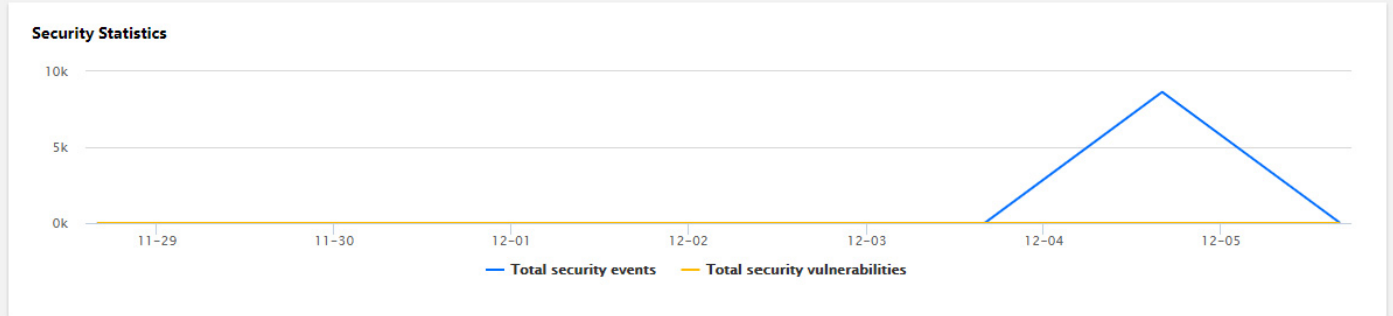
Outstanding security events 9426	Outstanding security vulnerabilities 30	Total resources 191 CVM(s)	Protected assets① 98 CVM(s)	Unprotected assets① 93 CVM(s)
--	---	--------------------------------------	---------------------------------------	---

Top 5 High Risk Assets

10.0.0.154 (云鼎_云镜测试机_WIN_2_weikunlin)	8635
10.105.145.42 (云鼎_云镜测试机_Linux_5_weikunlin)	587
10.135.152.112 (vincenli_test)	70
10.135.124.181 (CentOS)	17
10.0.0.29 (云鼎_云镜测试机_Linux_7_weikunlin)	14

Outstanding issues

Detected time	Event name	Affected assets	Operation
2018-12-06 02:21:53	Trojan	10.163.51.72	View Details
2018-12-06 02:21:53	Trojan	10.163.51.72	View Details
2018-12-06 02:21:47	Trojan	10.163.51.72	View Details
2018-12-06 02:21:47	Trojan	10.163.51.72	View Details
2018-12-06 00:06:19	Trojan	10.135.152.112	View Details



Service Management [View more](#)

<p>Host Security Premium</p> <p>Host Security</p> <p><input checked="" type="button" value="Activated"/> View Details</p>	<p>Dayu Anti-DDoS</p> <p>A value-added service that help protect customer from large-traffic DDoS attacks</p> <p><input checked="" type="button" value="Activated"/> View Details</p>	<p>Website Application Firewall</p> <p>A platform specialized in providing one-stop intelligent security protection services for websites. It protects website...</p> <p><input checked="" type="button" value="Activated"/> View Details</p>
--	--	--

Vulnerability Management

SSA provides real-time alerts and repair solutions for high-risk vulnerabilities on hosts (including system and web vulnerabilities), enabling you to quickly respond to them.

Vulnerability Management

Search for vulnerability

Vulnerability Type All Web vulnerability System vulnerability Security Baseline

Risk Level High Medium Low

Status

Vulnerability name	Vulnerabilit...	Risk Level	Affected assets	Detected time	Status	Operation
网站目录存在备份文件	Security Base...	High	172.16.32.17	2018-12-06 06:03:35	Outstanding	View Details
RPCBind 配置不当检测	Security Base...	High	172.16.32.11	2018-12-06 02:58:11	Outstanding	View Details
FTP 匿名登陆检测	Security Base...	Medium	10.105.145.42	2018-12-06 02:54:10	Outstanding	View Details
Elasticsearch未授权访问	Security Base...	High	172.16.16.8	2018-12-06 02:52:19	Outstanding	View Details
RPCBind 配置不当检测	Security Base...	High	172.16.16.8	2018-12-06 02:52:19	Outstanding	View Details
MySQL 弱口令检测	Security Base...	High	172.16.16.8	2018-12-06 02:52:19	Outstanding	View Details
Linux系统弱口令检测	Security Base...	High	10.186.50.84	2018-12-06 02:30:18	Outstanding	View Details
RPCBind 配置不当检测	Security Base...	High	172.16.32.3	2018-12-05 17:22:18	Outstanding	View Details
MySQL 弱口令检测	Security Base...	High	172.16.32.3	2018-12-05 17:22:18	Outstanding	View Details
Elasticsearch未授权访问	Security Base...	High	172.16.32.3	2018-12-05 17:22:18	Outstanding	View Details
MongoDB未授权访问	Security Base...	High	172.16.0.12	2018-12-05 02:45:13	Outstanding	View Details
RPCBind 配置不当检测	Security Base...	High	172.16.0.12	2018-12-05 02:45:13	Outstanding	View Details
Redis 基线合规检测	Security Base...	High	172.16.0.12	2018-12-05 02:45:13	Outstanding	View Details
Linux系统弱口令检测	Security Base...	High	172.16.0.12	2018-12-05 02:45:13	Outstanding	View Details
Linux系统弱口令检测	Security Base...	High	10.105.145.42	2018-11-22 02:02:30	Processed	View Details
Wordpress < 4.9.2 XSS 漏洞	Web vulnera...	Low	10.141.9.29	2018-11-21 05:08:45	Outstanding	View Details
WordPress核心组件潜在未授权密码重置	Web vulnera...	Medium	10.141.9.29	2018-11-21 05:08:45	Outstanding	View Details
WordPress 4.9.6 任意文件删除漏洞	Web vulnera...	Medium	10.141.9.29	2018-11-21 05:08:45	Outstanding	View Details
Apache server-status 未限制 IP 来源	Web vulnera...	Low	10.141.9.29	2018-11-21 05:08:45	Outstanding	View Details
WordPress Core 4.7 Stored XSS	Web vulnera...	Medium	10.141.9.29	2018-11-21 05:08:45	Outstanding	View Details

Visual Situation Representation

SSA offers three kinds of visual representation for real-time monitoring: security situation awareness overview, host security situation awareness and network security situation awareness.

- Security Situation Awareness Overview

SSA Overview displays the overall security situation of your cloud resources to help you understand the security conditions of various resources, including overview of host vulnerabilities, brute force attacks, trojans and off-site logins.

- Host SSA

Host SSA displays the security situation of your host assets to provide a data basis for addressing host security issues, including overview of host vulnerabilities, brute force attacks, trojans and off-site login, host security agent online status overview and host security intelligence overview.

- Network SSA

Network SSA displays the security situation of your enterprise network to help you identify the weaknesses in your network construction, including rankings of DDoS attack traffic and IPs attacking web applications, major attack types and total number of attacks in the past year as well as network situation intelligence overview.

Features

Last updated : 2018-12-06 11:12:26

SSA has the following core features:

Security Decision-making

By offering cloud- and terminal-based big data capabilities and serving as an auxiliary brain for security matters, SSA provides security decision-making suggestions and helps reduce security decision-making costs.

Risk Awareness

- Based on Tencent's big security data and rich experience in security, SSA continuously monitors Internet security conditions and alerts you to possible security issues.
- SSA provides channels for monitoring the latest vulnerabilities that enable you to understand trends in external vulnerabilities and take preventive measures before they cause damage.

Data Visualization

- SSA converges your own host, network and other security data for deep correlation analysis, provides key security metrics for monitoring and display security situation through visual representation in an intuitive and vivid manner.
- Taking the basic security data of your own business as the basis and integrating the online and offline big security data from Tencent Cloud and Tencent PC Manager, SSA provides you with objective and accurate security situation scores.