Situation Awareness

Service Overview

Issue 06

Date 2022-10-26

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

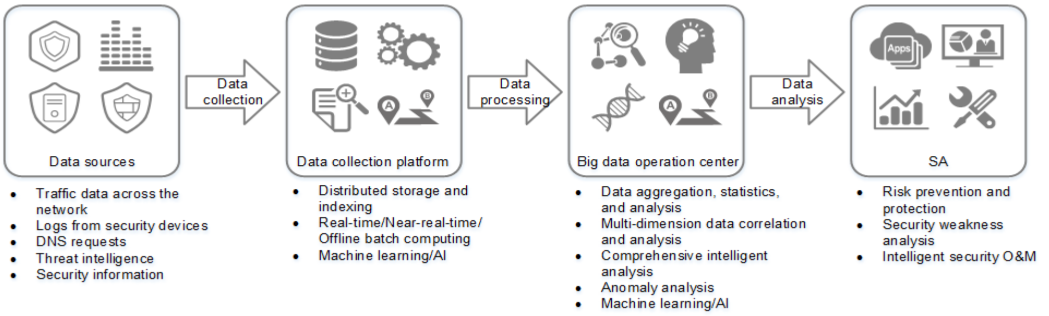
Contents

1 What Is Situation Awareness?

Situation Awareness (SA) is a security management and situation analysis platform of Huawei Cloud. SA comprehensively analyzes attack events, threat alarms, and attack sources by leveraging the big data technique, making it simple for you to understand security situation across all your cloud assets.

How SA Works

SA collects network-wide traffic data and security device logs and identifies threat alarms using a big data analysis platform. It also aggregates and displays alarm data reported by other security services, such as Host Security Service (HSS), Web Application Firewall (WAF), and Anti-DDoS. You can count on SA to make better informed decisions on handling security events.


Data sources
Data collection
Data collection platform
Data processing
Big data operation center
Data analysis
Apps
SA
Traffic data across the network
Logs from security devices
DNS requests
Threat intelligence
Security information
Distributed storage and indexing
Real-time/Near-real-time/ Offline batch computing
Machine learning/AI
Data aggregation, statistics, and analysis
Multi-dimension data correlation and analysis
Comprehensive intelligent analysis
Anomaly analysis
Machine learning/AI
Risk prevention and protection
Security weakness analysis
Intelligent security O&M

2 Functions

You can use SA to centrally manage security posture of your cloud services. It includes **Security Overview**, **Resource Manager**, **Event Analyses**, **Threat Alarms**, **Baseline Inspection**, **Events**, **Logs**, **Integrations**, and more. For more information, see **Table 2-1**.

Table 2-1 SA functions

Function	Description	Reference
Security Overview	Displays a comprehensive overview of asset security posture together with other linked cloud security services. ● Security Score: SA evaluates and scores your cloud asset security. You can quickly learn of unhandled risks and their threats to your assets. ● Security Monitoring: You can view how many threats, vulnerabilities, and compliance violations that are not handled and view their details. ● Security Scores over the Time: You can view the trend of the asset health scores for the last seven days. ● Threat Detection: You can view how many alarms are detected for the last 7 days and their types.	**Security Overview**
Event Analyses	You can view alarms aggregated from HSS, WAF, and DBSS. This gives you an overall overview of the security status and risks of all your assets on the cloud.	**Event Analyses**
Resource Manager	SA synchronizes information about your resources and displays overall security posture in one place.	**Resource Manager**

Function	Description	Reference
Threat Alarms	In this module, SA reports alarms based on real-time monitoring, displays details of alarms for the last 180 days, and defends against typical threats by using varied preset protection policies. ● **Alarms**: SA lists statistics on threat alarms. You can view details of threat alarms and details of threatened assets. You can also export all alarms. ● **Threat Analysis**: You can query the number of threats or attacks by attack source or attacked asset. ● Alarm monitoring: You can create a custom threat list, alarm type, and risk severity to view only the threat alarms of your concerns. ● Alarm notifications: SA allows you to customize alarm notifications. You can set scheduled daily alarm notifications and real-time alarm notifications to learn about threat risks in a timely manner.	**Threat Alarms**
Baseline Inspection	SA can scan cloud baseline configurations to find out unsafe settings, report alarms for events, and offer hardening suggestions to you.	**Baseline Inspection**
Events	SA aggregates detection data from a variety of related services so that you can monitor all events in one place.	**Events**
Logs	You can authorize Object Storage Service (OBS) to store SA logs in OBS buckets. This makes it easier for you to store and export SA logs securely and meet audit requirements for storing logs for 180 days.	**Logs**
Integrations	SA integrates a variety of security products to aggregate their detection data and manage the data sources of events. You can view the amount of transmitted data and manage the health status of data reporting.	**Integrations**

3 Application Scenarios

Asset Management

To keep up with your business expansion, you may need more cloud assets. With more cloud assets used, the risks to your services also increase.

SA monitors the security status of all assets in the cloud in real time and displays vulnerabilities, threats, and attacks on servers, helping you easily handle risks.

Threat Alarms

For various security threats on the cloud, SA collects network-wide traffic data and security protection device logs, and detects and monitors security risks on the cloud in real time, making it easier for you to view alarm event statistics in real time.

In addition, SA uses preset security protection policies to effectively defend against common brute-force attacks, web attacks, and zombies, greatly improving defense and O&M efficiency.

System Configuration Management

SA can scan cloud services for risks in key configuration items, report scan results by category, generate alarms for events, and provide hardening suggestions and guidelines.

4 Edition Differences

Situation Awareness (SA) provides basic edition and professional edition to meet your needs. For more details, see **Functions**.

- The SA basic edition is automatically enabled for your account for free. You can go to the SA console and start using it straight away.

  The basic edition monitors security of your assets on the cloud but does not detect as many threats as the professional edition.
- The standard edition can only be billed on a yearly or monthly basis. The standard edition can display the security posture of some cloud assets. It can be used for security check, threat analysis, and more to meet security operation requirements.
- You can subscribe to the professional edition on a yearly/monthly or pay-per-use basis. If you buy the professional edition, SA displays the security of all of the assets under your account, performs dynamic security scans and threat analysis, and provides you with security hardening suggestions.

Function Differences Between SA Editions

NOTE

Functions of each module in different editions are shown in the following tables, where:

- X: indicates that the function is unavailable in the corresponding edition.
- √: indicates that the function is available in the corresponding edition.
- √+: indicates that the function is available at additional cost.

Table 4-1 Function differences between SA editions

Function	Function Module	Description	Basic Edition	Standard	Professional Edition
Security Overview	Security Score	SA scores security posture of your system, sorts out risks by severity, and summarizes the risk defense capabilities of your system.	√	√	√
	Security Monitoring	SA summarizes the alarms, vulnerabilities, and abnormal baseline settings that have not been handled.	√	√	√
	Your Security Score over Time	SA displays your security scores for the last 7 days.	√	√	√
	Threat Detection	You can view how many alarms are detected for the last 7 days and their types.	√	√	√
Resource Manager	Resource security situation	SA synchronizes information about your resources and displays overall security posture in one place.	×	√	√
Event Analyses	Security services	SA associates security event data from HSS, WAF, and DBSS to display the security status and risks of ECSs, web applications, and databases.	√+	√+	√+
Threat Alarms	Alarms	SA displays threat alarm event statistics and allows you to export alarm events.	√	√	√
		SA allows you to ignore an alarm or mark an alarm for offline processing.	×	√	√
	Threat Analysis	SA allows you to query the information about the attacked asset by IP address of the attack source, or query the information about the threat attack source by IP address of the attacked asset.	×	√	√

Function	Function Module	Description	Basic Edition	Standard	Professional Edition
	Alarm Monitoring Settings	SA allows you to configure monitored threats and alarm conditions so that you can focus on specific threat alarms.	×	×	√
	Alarm Notifications	SA allows you to customize alarm notifications to learn about threat risks in a timely manner.	×	√	√
Baseline Inspection	Cloud Service Baseline	SA scans cloud service baselines in one-click and displays the inspection results by category.	×	√	√
		SA scans cloud service baselines in one-click and displays the inspection results by category. SA allows users to view details of check results and provides fixing suggestions.	×	×	√
Events	Events	SA displays the events or detection results of security products in a centralized manner. You can export and mark events.	√	√	√
Integrations	Integration of security products	SA integrates a variety of security products to aggregate their detection data and manage the data sources of events.	√	√	√
Logs	Logs	You can authorize OBS to store SA logs. This helps you meet log audit and disaster recovery requirements.	×	×	√

5 Basic Concepts

This section describes concepts about SA.

Security Risk

Security risk is a comprehensive evaluation of your assets, reflecting the security level of your assets within a period of time by a security score. A security score is for your reference to learn of the security situation of your assets.

Threat Alarm

In general, threat alarms refer to threats that, due to natural, human, software, or hardware reasons, are detrimental to information systems or cause negative effects on the society. In SA, threat alarms are detected security incidents that threaten asset security through big data technology.

Website Vulnerability

A website vulnerability is the vulnerability detected by the web crawler and intelligent comparison of vulnerability features. SA can scan over 22 types of vulnerabilities and can also detect OWASP top 10 and WASC vulnerabilities. The scan rules are automatically updated on the cloud and take effect on the entire network, covering the latest vulnerabilities. HTTPS scan is as well as supported.

Cloud Service Baseline

Cloud service baseline helps you detect unsafe configurations in cloud-based products in public cloud scenarios and provides recovery suggestions. Currently, you can check your environment against security standards **Cloud Security Compliance Check 1.0** and **Network Security**.

Attack Types

- Brute-force attack

  A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found to decrypt any encrypted data.

- Web attack

  A web attack is an attack against the Internet access or devices such as web servers. Common web attacks include SQL injection, cross-site scripting (XSS), and cross-site request forgery (XSRF) attacks.

- Zombie

  A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus, or Trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction. Attackers send commands to "zombies" through control channels and order them to send forged or junk packets to targets. As a result, the targets fail to respond and deny normal services. This is a common DDoS attack. Now, as virtual currencies, such as Bitcoins, grow in value, attackers start using zombies to mine Bitcoins.

- Abnormal behavior

  Abnormal behavior refers to the events that should not occur on hosts. For example, a user logs in to the system during an unauthorized time period, some file directories are changed unexpectedly, and unexpected actions were performed by a process. We should keep alert for those anomalies as most of them are caused by malware. The abnormal behavior data in SA is mainly reported by Host Security Service (HSS).

- Vulnerability exploit

  A vulnerability is a weakness that can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system. Gaining access, stealing sensitive data, or sabotaging software and hardware systems are all vulnerability exploits.

6 Permissions Management

If you want to assign different permissions to employees in your enterprise to access your SA resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your Huawei Cloud resources.

With IAM, you can create IAM users under your account for your employees, and assign permissions to the users to control their access to specific resource types. For example, you can use policies to grant different permissions to software developers in your enterprises to allow them to only use SA but not perform certain high-risk operations, such as deletion of SA data.

If your account does not need individual IAM users for permissions management, then you may skip over this chapter.

IAM is free. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

SA Permissions

By default, new IAM users do not have any permissions assigned. You can add a user to one or more groups to allow them to inherit the permissions from the groups to which they are added.

You can create IAM users in any region. SA is a global service for all geographic regions. SA permissions are assigned to IAM users in the global project, so IAM users can access SA in any region without having to switch over among regions.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. If one role has a dependency role required for accessing SA, assign both roles to the users. Roles are not ideal for fine-grained authorization and secure access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you

can grant SA users only the permissions for managing a certain type of resources. For the API actions supported by SA, see **Permissions Policies and Supported Actions**.

Table 6-1 lists all the system-defined roles and policies supported by SA.

Table 6-1 System-defined permissions supported by SA

Policy Name	Description	Type	Dependency
SA FullAccess	All permissions for SA	System-defined policy	None
SA ReadOnlyAccess	Read-only permission for SA. Users with the read-only permission can only query SA information but cannot perform configuration in SA.	System-defined policy	None

NOTE

Currently, the **SA FullAccess** or **SA ReadOnlyAccess** permission can be used only when you have the **Tenant Guest** permission. The details are as follows:

- Configure all SA permissions: **SA FullAccess** and **Tenant Guest**.

  To use SA **Resource Manager** and **Baseline Inspection**, configure the following permissions:

  - **Resource Manager**: Configure **SA FullAccess** and **Tenant Administrator**. For details, see **How Do I Assign Operation Permissions to an Account?**
  - **Baseline Inspection**: Configure **SA FullAccess**, **Tenant Administrator**, and IAM permissions. For details, see **How Do I Assign Operation Permissions to an Account?**
- Configure SA read-only permissions: Configure **SA ReadOnlyAccess** and **Tenant Guest**.

Related Topics

- **IAM Service Overview**
- **Creating User Groups and Users and Granting SA Permissions**
- **SA Custom Policies**
- **SA Permissions and Supported Actions**

SA FullAccess Policy Content

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "sa:*:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

SA ReadOnlyAccess Policy Content

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "sa:cssb:get",
                "sa:service:get",
                "sa:subscribe:get",
                "sa:subscribe:getList",
                "sa:threatevent:getAnalyze",
                "sa:threatevent:getAsset",
                "sa:threatevent:getDashboard",
                "sa:threatevent:getHostscreen",
                "sa:threatevent:getList",
                "sa:threatevent:getOverview",
                "sa:threatevent:getSafety"
            ],
            "Effect": "Allow"
        }
    ]
}
```

7 SA and Other Services

This topic describes SA and its linked services.

Security Services

SA obtains necessary security event records from security services such as **Host Security Service (HSS)**, **Web Application Firewall (WAF)**, and **Anti-DDoS**. SA then uses big data mining and machine learning to intelligently analyze and identify attacks and intrusions, helping you understand the attack and intrusion processes. SA also provides helpful protective measures for you. For more details, see **What Are the Dependencies and Differences Between SA and Other Security Services?**

ECS

SA detects threats to your **Elastic Cloud Servers (ECSs)** with linked service HSS, comprehensively displays ECS security risks, and provides protection suggestions.

IAM

Identity and Access Management (IAM) helps you to manage permissions and identity authentication for users of SA. For more details, see **Permissions Management**.