SRD Document

2020-10-20

Contents

Product Description

Introduction

SRD is a security risk detection provided by Baidu AI Cloud for users. It can detect a variety of common web vulnerabilities such as SQL injection and XSS cross-site scripting. It can also detect the existence of system software security vulnerabilities. Security risk detection can help users quickly find problems in business systems, repair them in a timely manner, and improve business security and stability.

Core Concepts

System Vulnerability

System vulnerabilities usually refer to defects or errors in the design of application software or operating system software on the cloud server.

Web Vulnerability

Web vulnerabilities usually refer to vulnerabilities in website programs, which may be caused by code writers' inadequate consideration when writing code. Common web vulnerabilities include SQL injection, CSRF, XSS vulnerabilities, upload vulnerabilities, and arbitrary file reading, command execution, file inclusion, etc.

0day Vulnerability

0day vulnerabilities generally refer to security vulnerabilities that are maliciously exploited immediately after being discovered or disclosed. Due to the time lag between the disclosure of these vulnerabilities and the release of official website vulnerability patches, attacks are often very sudden and disruptive.

Product Feature

Detection of Common Web Vulnerability

Quickly and accurately discover various common web security vulnerabilities such as SQL injection, XSS cross-site, and information leakage in web services.

Detection of System Vulnerability

Quickly and accurately discover security vulnerabilities in software systems.

Fast Update of High-risk 0day Vulnerability

Baidu AI Cloud security operations experts will get various 0day vulnerability information as soon as possible, update detection rule policies in a timely manner, and promptly remind customers to reduce the impact of 0day vulnerability attacks.

Bug fix Recommendations

All vulnerabilities have targeted remediation suggestions to help customers properly fix security vulnerabilities.

Fix Confirmation Function

After the vulnerability is repaired, a vulnerability review can be initiated to confirm whether the vulnerability has been fixed.

Product Advantages

Harmless Treatment of Test Cases

All security detection use cases are harmlessly processed, only problems are found, and no impact on customer service will occur.

Rule Strategy Is Accurate and Effective

The security risk detection has been tested on-site by many Baidu service for many years. The rules and policies are accurate and effective, and the coverage and detection rate of vulnerabilities are good.

System Information Portrait

Confirm the customer's system information portrait through security detection, and detect the weaknesses in a targeted manner.

Events Traceable

Various information elements of the vulnerability are completely recorded, and repair solutions are provided to facilitate customers to understand and repair the problem.

Application Scenarios

New Service Goes Online

Before the new service goes online, you can perform a complete scan of the new service through the security risk detection to prevent problems before they occur and deal with them in a timely manner to prevent vulnerabilities from being exploited.

Service Routine Security Detection

Periodic service routine security detection, comprehensive assessment of security.

Operation Guide

Log-in SRD

1.Log in to Baidu AI Cloud Official Website.

2.Log in to Baidu AI Cloud Platform:

- If there is no user name, please complete registration first. Please refer to Account Registration for operation.
- If there is a user name, please refer to Login for the log-in operation.

  3.After successful login, select "Product Services > Security and Management > Security Risk Detection" to enter the security risk detection.

Security Risk Detection

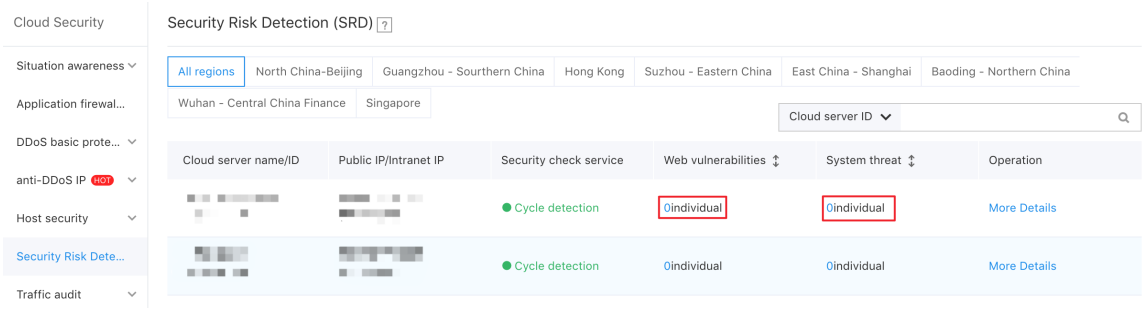
View Safety Inspection Records

Application scenarios

Users can view the number of web vulnerabilities and the number of open ports for all cloud resource instances.

Operation steps

1. In the left navigation, select "Security Risk Detection" to enter the inspection list.
2. You can view the number of web vulnerabilities and the number of open ports of the cloud service instance. Click the corresponding data to enter the corresponding details page.



Web Vulnerability Detection

Background information

Web vulnerability detection can detect the vulnerability of user websites in real time. If vulnerabilities are found, you can verify whether the repair is complete by rechecking. By setting the notification method, users can be notified of website vulnerability information in a timely manner.

> **Note:**
>
> The security detection service initiates detection from the public network. Cloud servers without public IP addresses cannot be detected.

Record Web Vulnerability Detection

Application scenarios

Users can view the WEB vulnerability scan records of a single BCC instance.

Operation steps

1.In the left navigation, select "Security Risk Detection" to enter the service list page.

2.Select the instance you want to view and click "View Details" to enter the "Web Vulnerability" tab.

3.View the scan record of the corresponding instance.

Handle Web Vulnerability Detection Results

Application scenarios

Users can follow up on a web vulnerability scan record.

For a pending or ignored Web vulnerability, the supported operations include re-detection.

Operation steps

1.For the operation, please see Record Web Vulnerability Detection.

2.In the "Action" column, click to re-detect the vulnerability.

Set the Web Vulnerability Detection Result Notification Method

For details, please see Set Alarm.

System Threat Detection

Background information

System threat detection, including "Specific Software Threats" and "Weak Password Threats", prompts for ports with service vulnerabilities and the names of services running on the ports, and finally provides a repair plan.

Record System Threat Detection

Application scenarios

Users can view system threat scan records of a single BCC cloud server.

Operation steps

1.In the left navigation, select "Security Risk Detection" to enter the service list page.

2.Select the instance you want to view and click "View Details" to enter the "System Threat" tab.

3.View the scan record of the corresponding instance.

Set System Threat Scan Notification Method

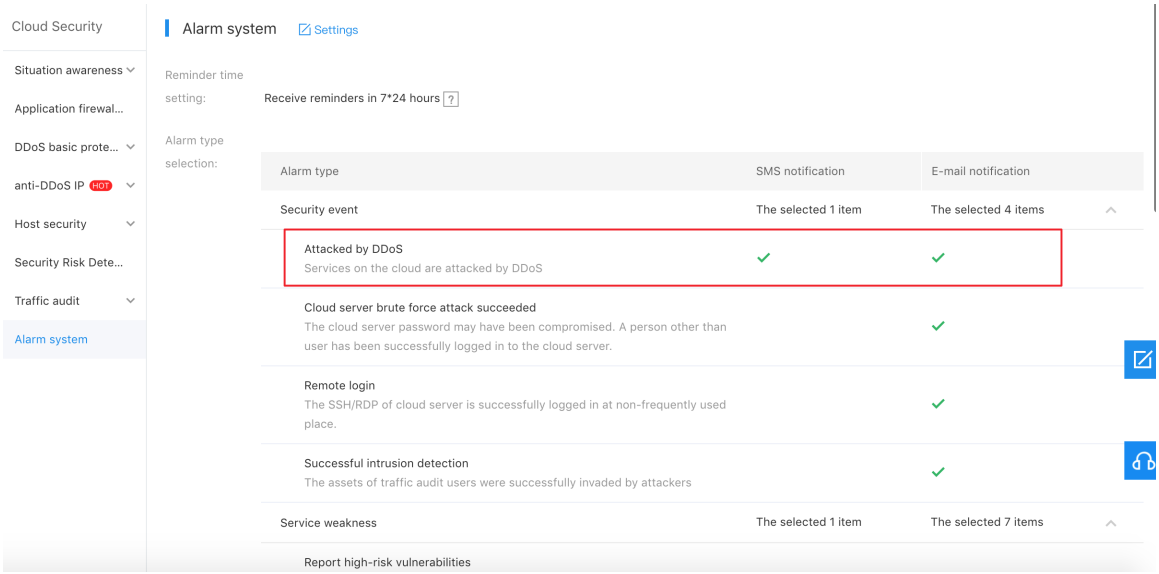
Application scenarios

Users can uniformly set alarm methods and policies for different security services.

Users can set alarm methods and SMS alarm time for different security services: Email or SMS.

Operation steps

1.Select "Alarm Setting" on the left navigation to enter the "Cloud Security-Alarm Settings" interface.



3.According to the actual situation, select the notification method, SMS or email, and set the reminder time.

4.Click "OK" to complete the alarm setting.

Identity and Access Management

Introduction

Identity and access management is mainly used to help users manage the access rights of resources under the cloud account. It is applicable to different roles in the enterprise. Different workers can be given different privileges to use the product. It is recommended that you use identity and access management.

Suitable for the following usage scenarios:

- Modify the redis instance parameter values: Authorized management of multiple employees in the company.
- Technical vendors or SAAS vendors: Resource and authority management for agency clients.
- Small and medium developers or small businesses: Add project members or collaborators for resource management.

Create User

1.After the master account user logs in, select "Identity and Access Management" on the console to enter the user management page. 2.Click "User Management" on the navigation bar, and click "Create User" on the "Sub User Management List" page. 3.In the pop-up "Create User" dialog box, fill in the "User Name" and confirm, and return to the "Sub User Management List" region to view the newly created sub user.

Configure Policy

SRD supports system policy and custom policy to implement the control of BLB with product-level privileges and instance-level privileges, respectively.

- System policy: A set of privileges predefined by Baidu AI Cloud system to manage resources. They can directly authorize sub-users. Users can only use them and cannot modify them.
- Custom policy: A more detailed set of privileges created by users themselves to manage resources. They can be configured for a single instance so as to more flexibly meet the account's differentiated privileges management for different users.

System Policy

It includes read-only privileges, operation and maintenance privileges, and management privileges. The privileges are detailed as follows:

Policy name	Privilege description	Scope of privilege
SRDReadPolicy	Read-only access to SRD	View the list of detected EIP instances, and view the details of test results
SRDWritePolicy	Operation and maintenance of SRD	View the list of detected EIP instances, view the details of the detection results, and initiate a re-detection of the EIP instances
SRDFullControlPolicy	Full control over privileges to manage Baidu AI Cloud Security Risk Detection	View the list of detected EIP instances, view the details of the detection results, and initiate a re-detection of the EIP instances

Custom Policy

Authorize from the instance dimension. Unlike system policy, they only take effect on selected instances. The sub-user enters [Policy Management] through the left navigation bar, and then clicks "Create Policy". The user fills in the policy name and selects the service type as BLB. The policy generation method defaults to the policy generator and does not need to be modified. The details of custom privileges are as follows:

privilege description	Scope of privilege
Read only	View the list of detected EIP instances, and view the details of test results
Operation and maintenance	View the list of detected EIP instances, view the details of the detection results, and initiate a re-detection of the EIP instances
Management	View the list of detected EIP instances, view the details of the detection results, and initiate a re-detection of the EIP instances

User Authorization

Select "Add privilege" in the "Action" column of the corresponding sub-user in the "User Management > Sub-User Management List Page", and select system privileges or custom policy for users to authorize.

> Note: You can only delete existing policy and add new policy to modify the privileges of a sub-user without modifying the existing policy rules. You cannot uncheck the policy privileges that have been added.

Sub-user Login

After the master account authorizes the sub-user, the link can be sent to the sub-user; the sub-user can log in to the management console of the master account through the IAM user login link, and operate and view the master account resources according to the authorized policy. For other detailed operation, please see Identity and Access Management.

FAQs

FAQs

Description of EIP Fees Brought by Security Inspection

According to the "Cyber Security Law of the People's Republic of China" and related laws and regulations, network operators should fulfill the obligations of network security protection for the products and services they provide. The security risk detection that we provide based on this will simulate the behavior of an attacker and issue a vulnerability test request based on the public network, and perform a corresponding security analysis on the response content of the website to find out the security vulnerability. When your website responds to these requests, there will be a certain amount of network traffic. If you use EIP to charge by traffic, this part of traffic will be reflected in the bill. Please be aware of it.