SRD 文档

2021-01-10

目录

产品描述

概述

安全检测服务（Security Risk Detection，简称SRD）是百度智能云面向用户提供的安全风险检测服务，能够检测出SQL注入、XSS跨站脚本等多种常见Web漏洞，也能检测出系统软件中存在的安全漏洞。安全检测服务可以帮助用户快速的发现业务系统中存在的问题，及时修复，提升业务安全性和稳定性。

核心概念

系统漏洞

系统漏洞通常是指云服务器上的应用软件或操作系统软件在设计上存在的缺陷或错误。

Web漏洞

Web漏洞通常是指网站程序上的漏洞，可能是由于代码编写者在编写代码时考虑不周全等原因而造成的漏洞，常见的WEB漏洞有SQL注入、CSRF、XSS漏洞、上传漏洞、任意文件读取漏洞、命令执行、文件包含等。

0day漏洞

0day漏洞通常泛指被发现或披露后立即被恶意利用的安全漏洞。由于这类漏洞从披露到发布官网漏洞补丁中间存在时间差，攻击往往具有很大的突发性与破坏性。

产品功能

常见Web漏洞的检测

快速准确发现Web业务中的SQL注入、XSS跨站、信息泄漏等各种常见Web安全漏洞。

系统漏洞的检测

快速准确发现软件系统中的安全漏洞。

高危0day漏洞极速更新

百度智能云安全运营专家会第一时间获取各种0day漏洞信息，及时更新检测规则策略，极速提醒客户，降低0day漏洞攻击带来的影响。

漏洞修复建议

所有漏洞都有针对性的修复建议，帮助客户妥善修复安全漏洞。

修复确认功能

漏洞修复以后可以发起漏洞复检，确认漏洞是否已经得到修复。

产品优势

检测用例无害化处理

所有的安全检测用例都经过无害化处理，只发现问题，不会对客户业务造成影响。

规则策略准确有效

安全检测服务经过百度多项业务进行实地测试多年，规则策略准确有效，漏洞覆盖率和找出率好。

系统信息画像

通过安全检测确认客户的系统信息画像，有针对性的对弱点进行检测。

事件可追溯

完整的记录漏洞的各项信息元素，附带修复方案，方便客户了解和修复问题。

应用场景

新业务上线

新业务上线之前可以通过安全检测服务对新业务做一次完整扫描，防患于未然，及时处理，防止漏洞被利用。

业务例行安全检测

周期性的业务例行安全检测，全面整体评估安全性。

操作指南

登录SRD

1.进入百度智能云官网。

2.登录百度智能云平台：

- 若没有用户名，请先完成注册，操作请参考注册。
- 若有用户名，登录操作请参考登录。

3.登录成功后，选择“产品服务>安全和管理>安全检测服务 SRD”，进入安全检测服务。

安全检测服务

查看安全检测记录

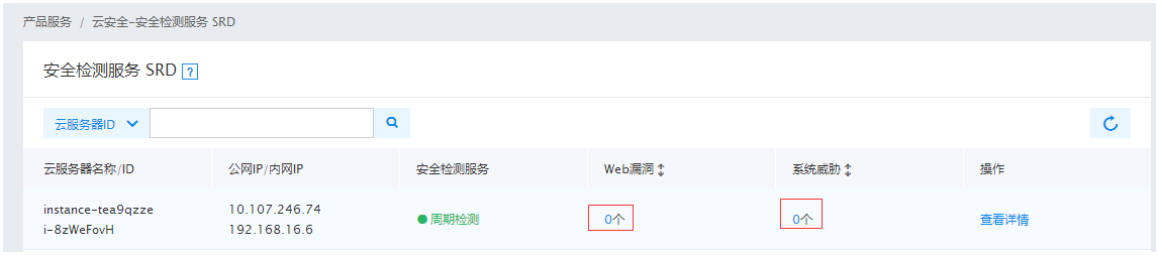
应用场景

用户能够查看所有云资源实例的WEB漏洞数量和开放端口数量。

操作步骤

1.在左侧导航选择“安全检测服务”，进入检测列表。

2.可以查看云服务实例的web漏洞数量和开放端口数量，点击相应数据，可进入到相应详情页。



Web漏洞检测

背景信息

Web漏洞检测，可以实时检测用户网站的漏洞情况。如果发现漏洞，可以通过重新检查验证是否修复完成。通过设置通知方式，可以将网站漏洞信息及时通知给用户。

> **说明：**
>
> 安全检测服务是从公网发起检测，没有公网IP地址的云服务器无法检测。

记录Web漏洞检测

应用场景

用户能够查看单个BCC实例的WEB漏洞扫描记录。

操作步骤

1.在左侧导航选择“安全检测服务”，进入服务列表页。

2.选择需要查看的实例，点击“查看详情”，进入“Web漏洞”页签。

3.查看相应实例的扫描记录。

处理Web漏洞检测结果

应用场景

用户能够针对一条Web漏洞扫描记录进行后续处理。

针对一个待处理或者已忽略的Web漏洞，支持的操作包括重新检测。

操作步骤

1.查看操作请参考记录Web漏洞检测。

2.在“操作”列，点击<重新检测>，对该漏洞进行重新检测。

设置Web漏洞检测结果通知方式

具体方式请参考设置报警。

系统威胁检测

背景信息

系统威胁检测，包括“特定软件威胁”和“弱密码威胁“两类，提示存在服务漏洞的端口以及端口上跑的服务名称，最终给出修复方案。

记录系统威胁检测

应用场景

用户能够查看单个BCC云服务器的系统威胁扫描记录。

操作步骤

1.在左侧导航选择“安全检测服务”，进入服务列表页。

2.选择需要查看的实例，点击“查看详情”，进入“系统威胁”页签。

3.查看相应实例的扫描记录。

设置系统威胁扫描通知方式

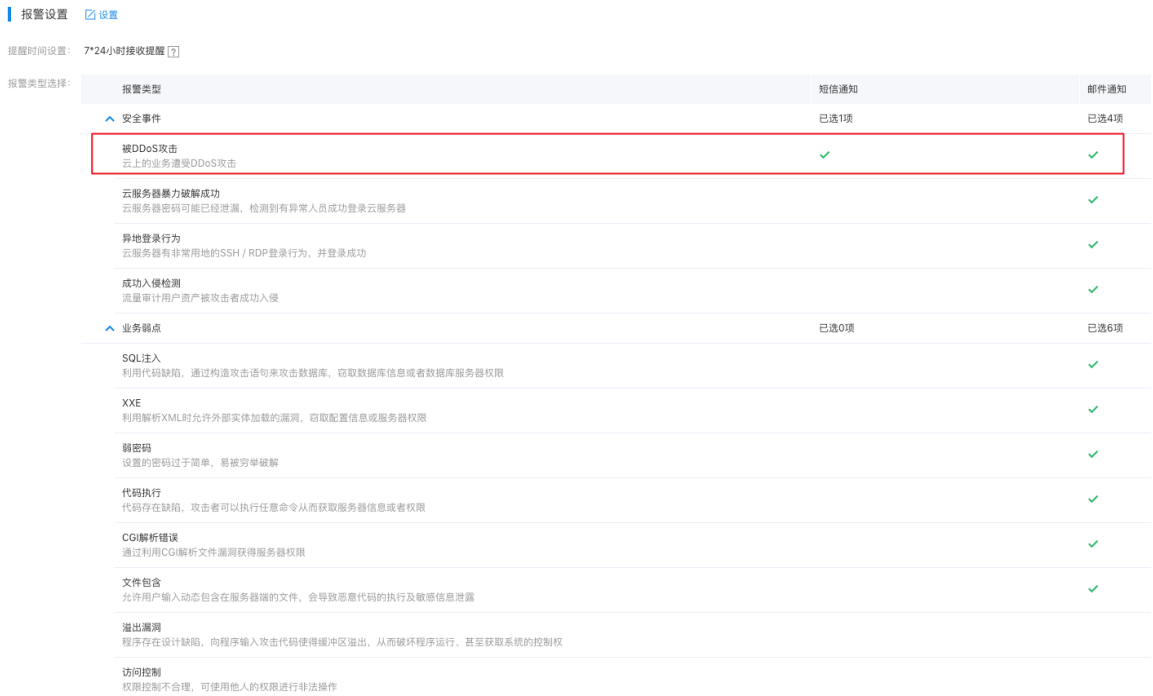
应用场景

用户能够统一设定针对不同安全服务的报警方式和策略。

用户可以设置针对不同安全服务报警方式以及短信报警时间：邮件或者短信。

操作步骤

1.选择左侧导航的“报警设置”，进入“云安全-报警设置”界面。



3.根据实际情况，选择通知方式，短信或者邮件，并设置提醒时间。

4.点击“确定”，完成报警设置。

多用户访问控制

介绍

多用户访问控制，主要用于帮助用户管理云账户下资源的访问权限，适用于企业内的不同角色，可以对不同的工作人员赋予使用产品的不同权限，当您的企业存在多用户协同操作资源时，推荐您使用多用户访问控制。

适用于下列使用场景：

- 中大型企业客户：对公司内多个员工授权管理。
- 偏技术型vendor或SAAS的平台商：对代理客户进行资源和权限管理。
- 中小开发者或小企业：添加项目成员或协作者，进行资源管理。

创建用户

1. 主账号用户登录后在控制台选择“多用户访问控制”进入用户管理页面。
2. 侧导航栏点击“用户管理”，在“子用户管理列表”页，点击“新建用户”。
3. 在弹出的“新建用户”对话框中，完成填写“用户名”和确认，返回“子用户管理列表”区可以查看到刚刚创建的子用户。

配置策略

SRD支持系统策略和用户自定义策略两种，分别实现BLB的产品级权限和实例级权限控制。

- 系统策略：百度智能云系统为管理资源而预定义的权限集，这类策略可直接为子用户授权，用户只能使用而不能修改。
- 自定义策略：由用户自己创建，更细化的管理资源的权限集，可以针对单个实例配置权限，更加灵活的满足账户对不同用户的差异化权限管理。

系统策略

包含只读权限、运维权限和管理权限3种策略，权限范围详细如下：

策略名称	权限说明	权限范围
SRDReadPolicy	只读访问百度智能云负载均衡（SRD）的权限	查看被检测的EIP实例列表、查看检测结果详情
SRDWritePolicy	运维操作百度智能云负载均衡（SRD）的权限	查看被检测的EIP实例列表、查看检测结果详情、对EIP实例发起重新检测
SRDFullControlPolicy	完全控制管理百度智能云安全检测服务（SRD）的权限	查看被检测 的EIP实例列表、查看检测结果详情、对EIP实例发起重新检测

自定义策略

是从实例维度进行授权，与系统策略不同，只对选定的实例生效。 子用户先通过左侧导航栏进入【策略管理】，然后点击“创建策略”，用户填写策略名称并选择服务类型为负载均衡BLB，其中策略生成方式默认为策略生成器，不需要修改。 自定义权限范围详细如下：

权限说明	权限范围
只读权限	查看被检测的EIP实例列表、查看检测结果详情
运维权限	查看被检测的EIP实例列表、查看检测结果详情、对EIP实例发起重新检测
管理权限	查看被检测 的EIP实例列表、查看检测结果详情、对EIP实例发起重新检测

用户授权

在“用户管理->子用户管理列表页”的对应子用户的“操作”列选择“添加权限”，并为用户选择系统权限或自定义策略进行授权。

> 说明：如果在不修改已有策略规则的情况下修改某子用户的权限，只能通过删除已有的策略并添加新的策略来实现，不能取消勾选已经添加过的策略权限。

子用户登录

主账号完成对子用户的授权后，可以将链接发送给子用户；子用户可以通过IAM用户登录链接登录主账号的管理控制台，根据被授权的策略对主账户资源进行操作和查看。 其他详细操作参考：多用户访问控制

常见问题

常见问题

安全检测带来的EIP费用说明 根据《中华人民共和国网络安全法》及相关法律法规规定，网络运营者对其提供的产品和服务应履行网络安全保护义务。我们据此提供的安全检测服务SRD会模拟攻击者行为基于公网发出漏洞测试请求，并对网站的响应内容进行对应的安全分析，以找出安全漏洞。当您的网站响应这些请求的时候会产生一定的网络流量，如果您使用的是EIP按流量计费，这部分流量会体现在账单中。敬请知悉。