



虚拟化漏洞扫描（龙巡）

产品文档





文档目录

产品简介

什么是龙巡

产品架构

产品架构

功能特性

多维度资产信息发现

验证式漏洞发现

友好的扫描报告

资产脆弱性生命周期管理

快速入门

部署龙巡漏洞扫描

系统界面布局介绍

菜单导航

正文区域

快速入门

前提条件特别提示

选择vpc

添加资产

扫描资产漏洞

查看漏洞结果

漏洞修复

用户指南

扫描管理

扫描管理-任务统计

扫描管理-扫描策略

扫描管理-任务列表

资产管理

资产统计

风险资产

主机资产

Web站点资产

服务资产

域名资产

漏洞管理

漏洞统计



漏洞列表

报告管理

报告列表

生成报告

系统信息

系统状态

常见问题

部署龙巡准备工作

漏洞扫描原理

扫描的影响

扫描前确认信息

扫描时间选择

什么是转发端口

转发端口的处理

配置UA或添加Referer字段

扫描特殊端口的配置

扫描出现告警如何处理



产品简介

什么是龙巡

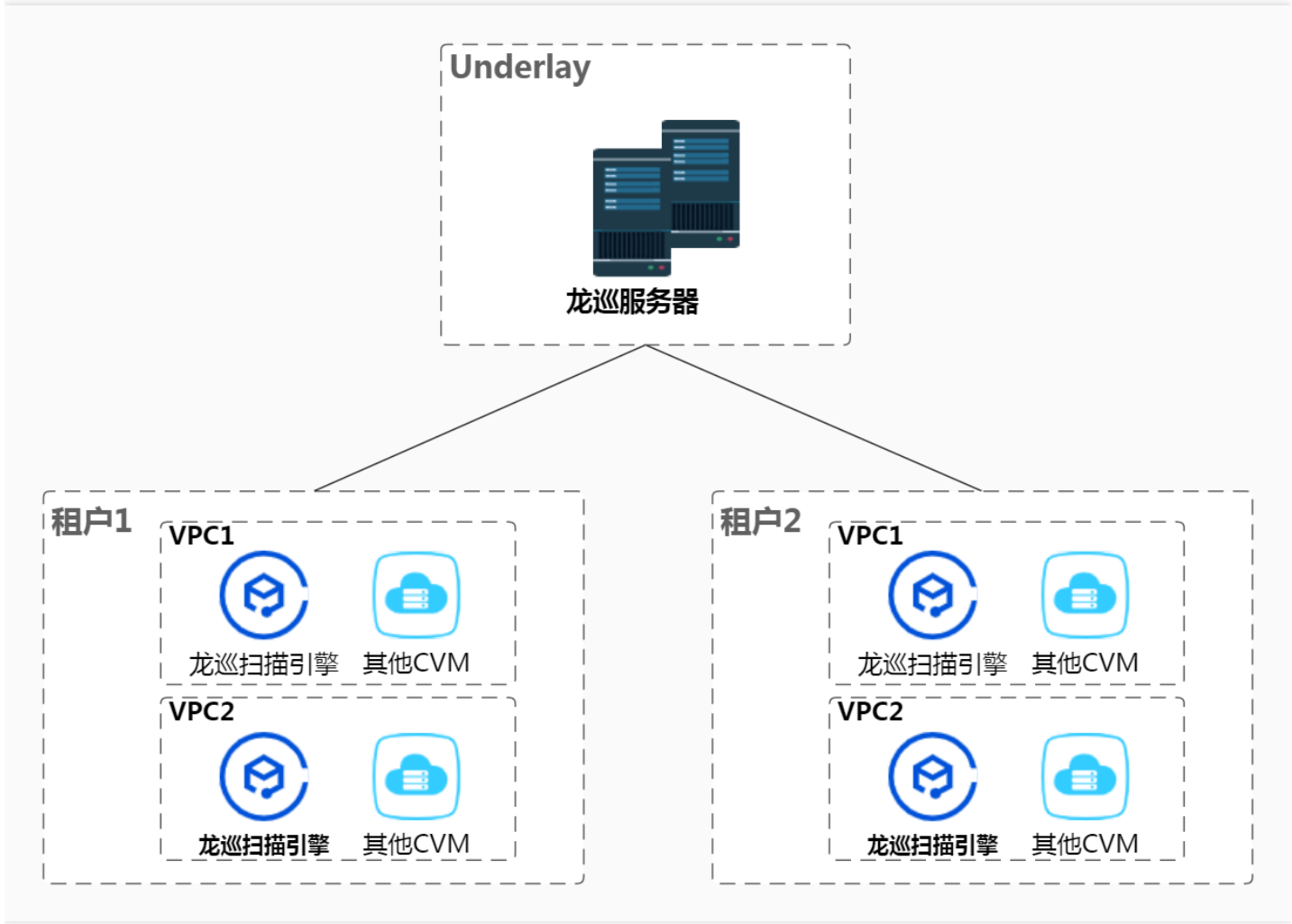
最近更新时间: 2023-01-05 14:24:15

龙巡是建行云引入的一款虚拟化漏洞扫描产品，租户无需关注产品部署逻辑细节，通过一键部署方式即可获得龙巡服务。包括资产发现，域名发现，Web应用漏洞扫描，基础漏洞扫描等功能。帮助租户识别发现和管理风险资产，从而实现漏洞的全生命周期管理。

产品架构

产品架构

最近更新时间: 2023-01-05 14:24:15



管理节点部署在underlay平台端，引擎节点部署在overlay租户端，每个VPC至少需部署一台龙巡扫描引擎，可对VPC内部主机资产进行漏洞扫描。



功能特性

多维度资产信息发现

最近更新时间: 2023-01-05 14:24:10

龙巡具备主机服务探测、域名探测、综合Web探测等多个资产发现功能，提供了主机系统、Web应用和域名的多维度资产信息发现功能，能够又快又全的获取目标资产的全部信息，避免因资产信息掌握不全而导致的脆弱点遗漏。

- 主机服务探测：提供快速便捷的主机服务资产探测功能，用户仅需输入目标IP范围即可快速实现主机服务资产信息的准确采集。
- 域名探测：支持从多个维度分析域名资产，如搜索引擎、HTTPS证书、Passive DNS、域传送漏洞等，并结合更加适用于国内常用命名习惯的内置字典，实现全面的子域名发现。
- 综合Web探测：采用综合Web探测引擎，以应对复杂多样的Web应用架构。能够根据目标URL对页面进行识别分析，根据页面类型选取普通爬虫 或浏览器爬虫，力求全面采集目标站点的页面信息。



验证式漏洞发现

最近更新时间: 2023-01-05 14:24:10

采用验证式漏洞检测技术，通过内置漏洞扫描插件，模拟真实攻击行为，发送攻击载荷，根据分析发送和返回数据内容，智能判断是否存在漏洞，相较于漏洞特征匹配的猜测式检测，具有准确性高、误报率低的优势。

漏洞类型	支持检测的漏洞种类
主机服务漏洞检测插件	操作系统、系统服务、数据库服务等开源和商用软件的不安全配置、未授权访问、后门、信息泄露等
网络设备漏洞检测插件	常见交换机、防火墙、VPN、邮件网关等设备的命令注入、未授权访问、不安全配置等
通用web应用漏洞检测插件	SQL注入、CSRF、CRFL注入、命令注入、XXE、SSRF、XSS、文件上传、服务器错误信息、敏感信息泄露、表单弱口令、不安全的HTTP配置、路径穿越、任意跳转等
常见Web组件检测插件	Apache、IIS、JBoss、WordPress等常用组件的不安全配置、注入、未授权访问、权限绕过等

扫描插件覆盖Web和主机常见漏洞类型，根据目标资产的响应信息自动调整参数，扫描结果中能详细阐述漏洞位置、危害和利用方式，在不影响业务正常运行前提下，精准报告漏洞信息。



友好的扫描报告

最近更新时间: 2023-01-05 14:24:10

提供友好的报告展示系统，支持以任务、漏洞、资产维度 独立生成各类报告，针对目标系统的安全评级、资产信息统计、漏洞分类与统计进行直观展示。 扫描报告中漏洞描述内容包括以下维度：

漏洞描述	说明
编号	漏洞在公开漏洞库中的编号
描述	1.漏洞类型及其原理性描述 2.漏洞存在的URL路径 3.漏洞存在的参数位置
危害	攻击者可利用该漏洞实现哪些操作
验证方式	提供PoC代码和验证方式指导，用户可手动验证
利用方式	指导构造攻击载荷的代码，用户可实际利用漏洞
修复方式	穷举出可以修正该漏洞的方法，包括但不限于：调整设计、修改代码、部署防护设备等



资产脆弱性生命周期管理

最近更新时间: 2023-01-05 14:24:10

提供目标资产的全生命周期管理功能，为用户每项资产建立独立的脆弱性档案，完整记录漏洞从发现、修复中、已修复的处理过程，并且提供自动化验证功能，辅助用户追踪风险点，促进安全管理制度流程的高效运转。

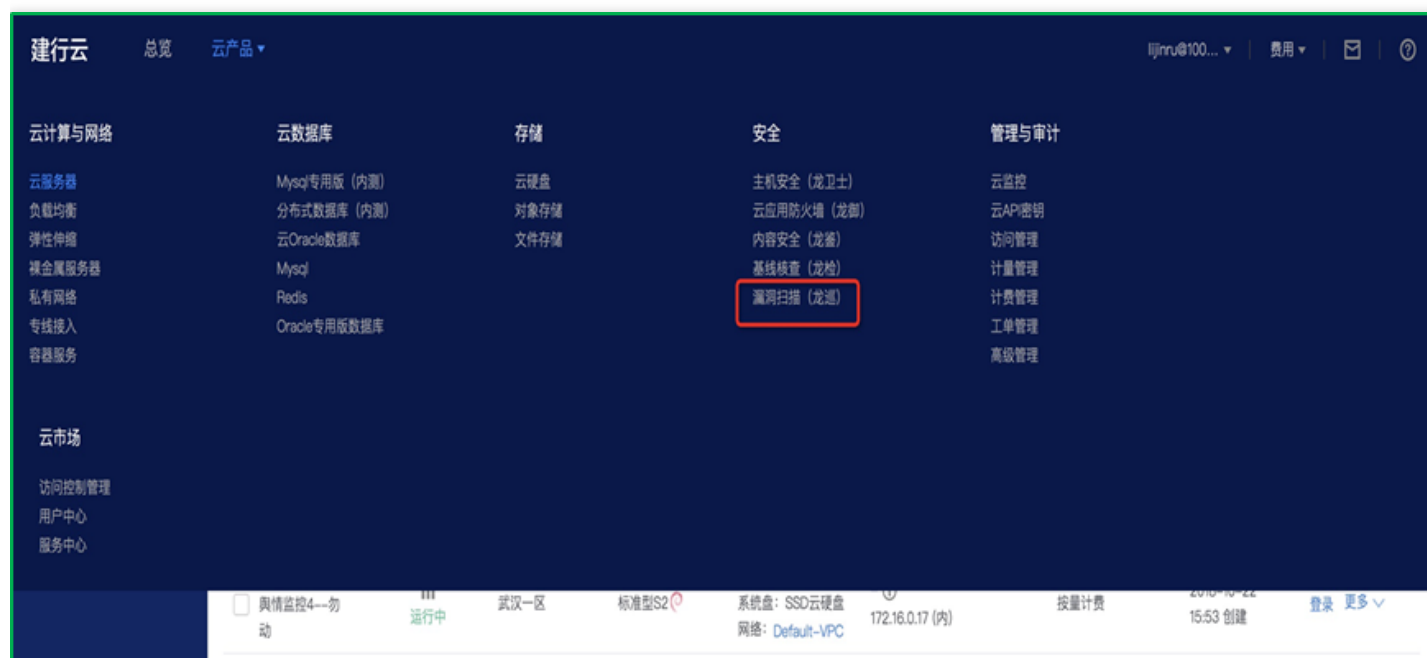


快速入门

部署龙巡漏洞扫描

最近更新时间: 2021-08-31 18:34:31

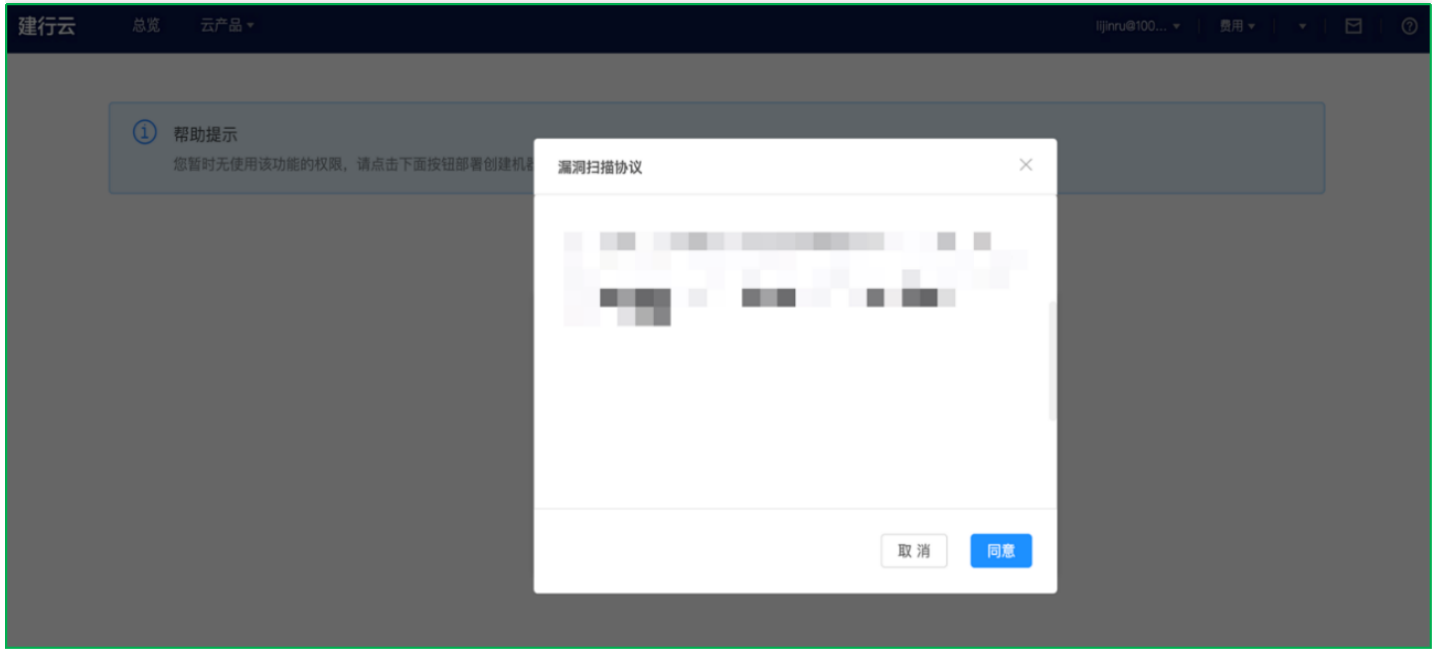
1、主账号登录建行云，在云产品，安全产品选择虚拟化漏扫（龙巡）；



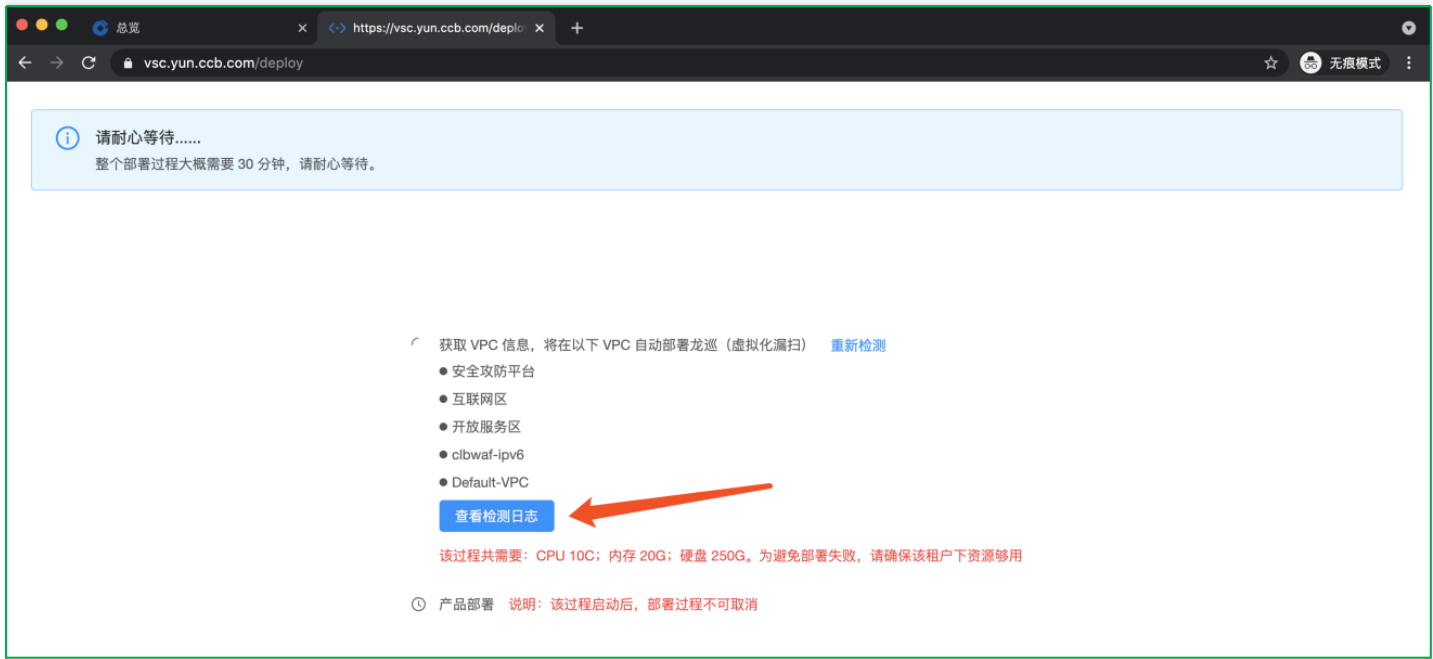
2、第一次访问，进入一键部署页面，点击部署龙巡开始部署流程；



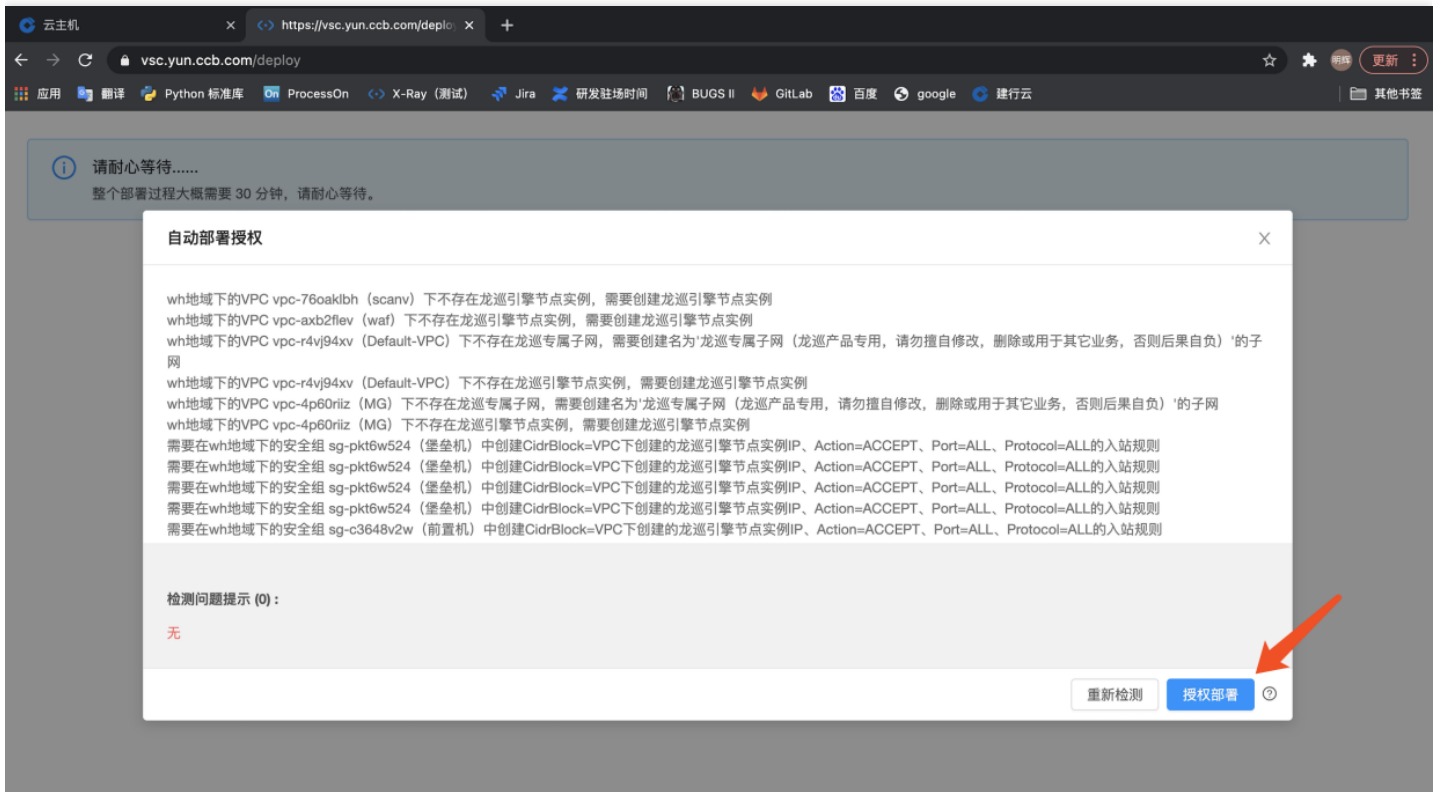
3、漏扫协议确认，请认真阅读协议内容，选择同意继续部署；



4、系统按VPC自动检查部署所需资源及网络环境，点击查看检查日志按钮查看详细日志，并继续操作；

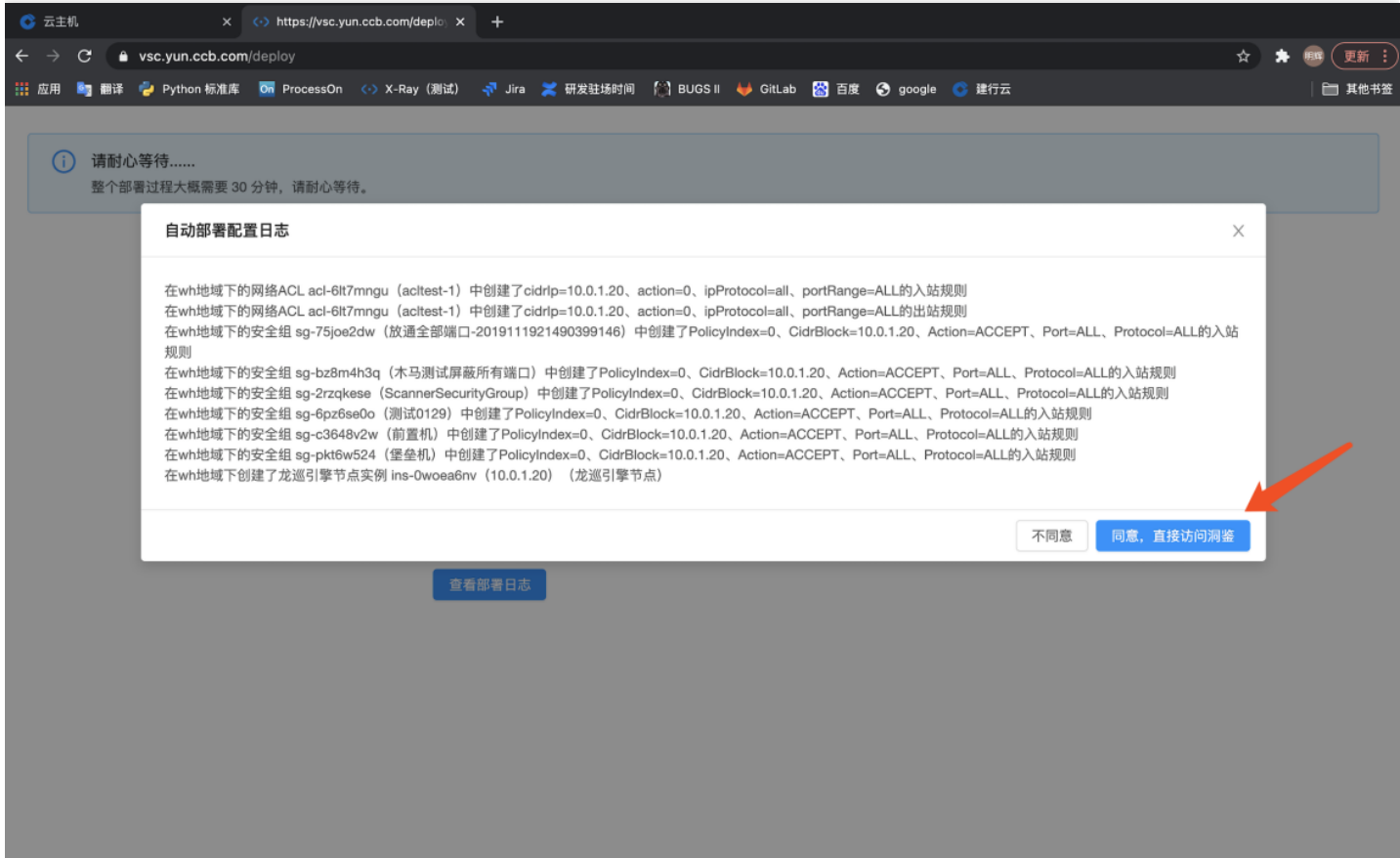


5、资源及网络环境检查完成后如无问题（红色字体文字），点击授权部署开始部署；



检查如有问题，按照提示进行处理，确认处理完成后点击重新检测按钮进行检查，直到检查无问题，点击授权部署进行部署。

6、引擎节点开始自动部署，弹出自动部署过程记录日志，显示系统自动部署过程的详细内容，点击同意，直接访问龙巡按钮访问龙巡页面。



7、VPC部署概览页查看详细部署信息，部署过程根据不同情况大概需要5-30分钟，所有引擎状态显示空闲就表示部署完成；



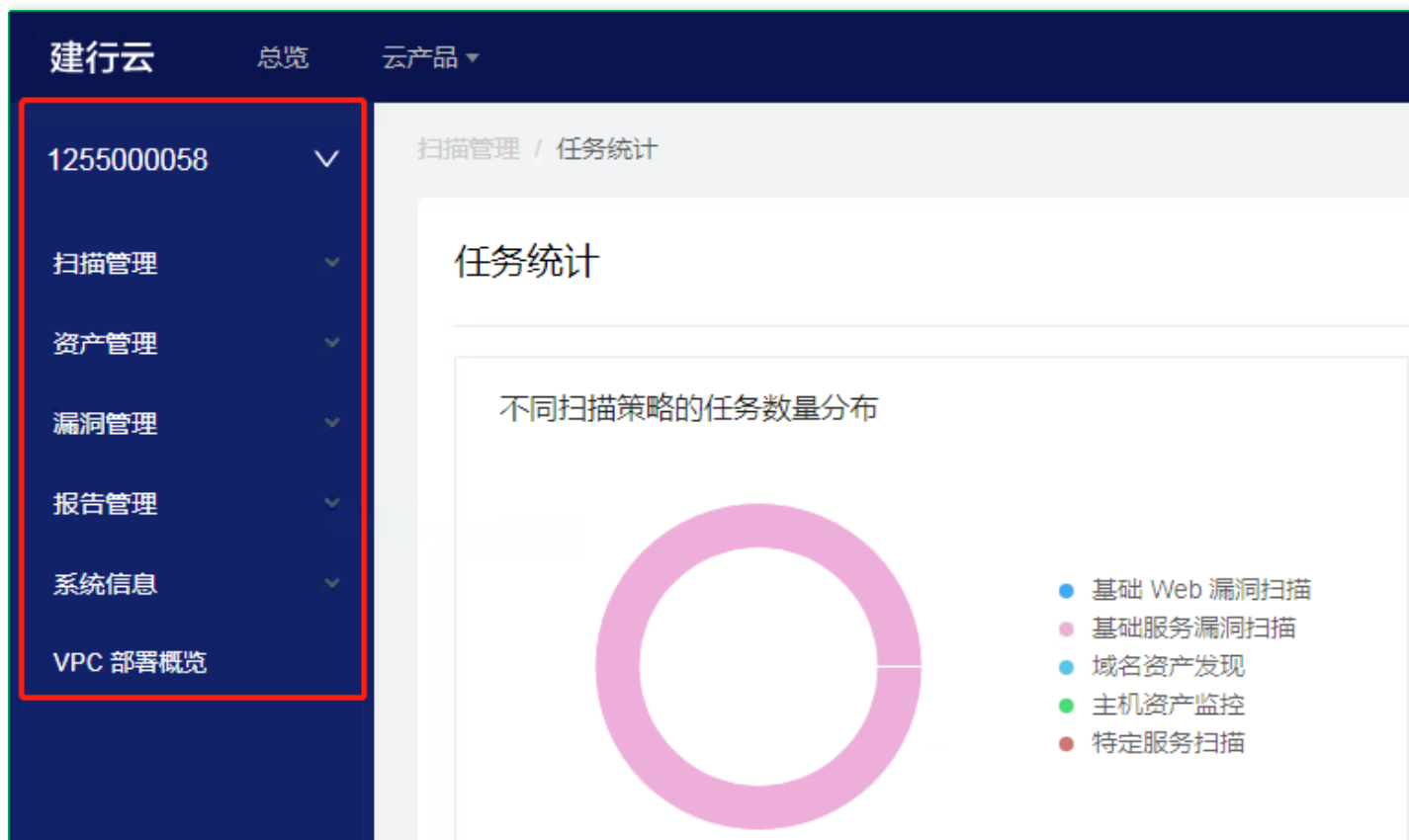


系统界面布局介绍

菜单导航

最近更新时间: 2023-01-05 16:54:47

龙巡漏洞扫描主要从扫描管理、资产管理、漏洞管理、报告管理、系统信息、VPC部署概览这六部分进行分类展示和管理，顶部菜单为建行云菜单，龙巡漏洞扫描菜单具体见左侧导航栏；



具体工作区模块简要说明如下：

- 工作区：在此可切换工作区，默认显示租户工作区，可切换到VPC工作区；
- 扫描管理：主要存放扫描相关的各项操作和数据展示内容，导航菜单有任务统计、扫描策略、任务列表；
- 资产管理：用户可在此方便地对 Web 站点、主机、服务和域名这四类资产进行管理，导航菜单有资产统计、风险资产、主机资产、服务资产、Web站点资产、域名资产；
- 漏洞管理：方便用户对系统所有漏洞、有风险的资产进行管理，导航菜单有漏洞统计、漏洞列表；
- 报告管理：对已生成的不同类型报告的管理，包含主机资产报告、Web 站点资产报告、漏洞报告、扫描任务结果报告，用户可以在此生成报告，将已经生成的报告下载到本地，导航菜单有报告列表、生成报告；
- 系统信息：展示系统状态；
- VPC部署概览：显示租户下各vpc龙巡漏扫引擎部署情况信息；



正文区域

最近更新时间: 2021-08-31 18:44:34

左侧导航栏右方的区域展示正文的详细内容。用户可在此进行查看、扫描和管理等等各种操作。详情可以查阅下文第三章中的“用户指南”，对各功能模块的详细介绍和操作说明等。

- ▲ 三、用户指南
 - ▷ 3.1 扫描管理
 - ▷ 3.2 资产管理
 - ▷ 3.3 漏洞管理
 - ▷ 3.4 报告管理
 - ▷ 3.5 系统信息



快速入门

前提条件特别提示

最近更新时间: 2021-09-01 09:46:40

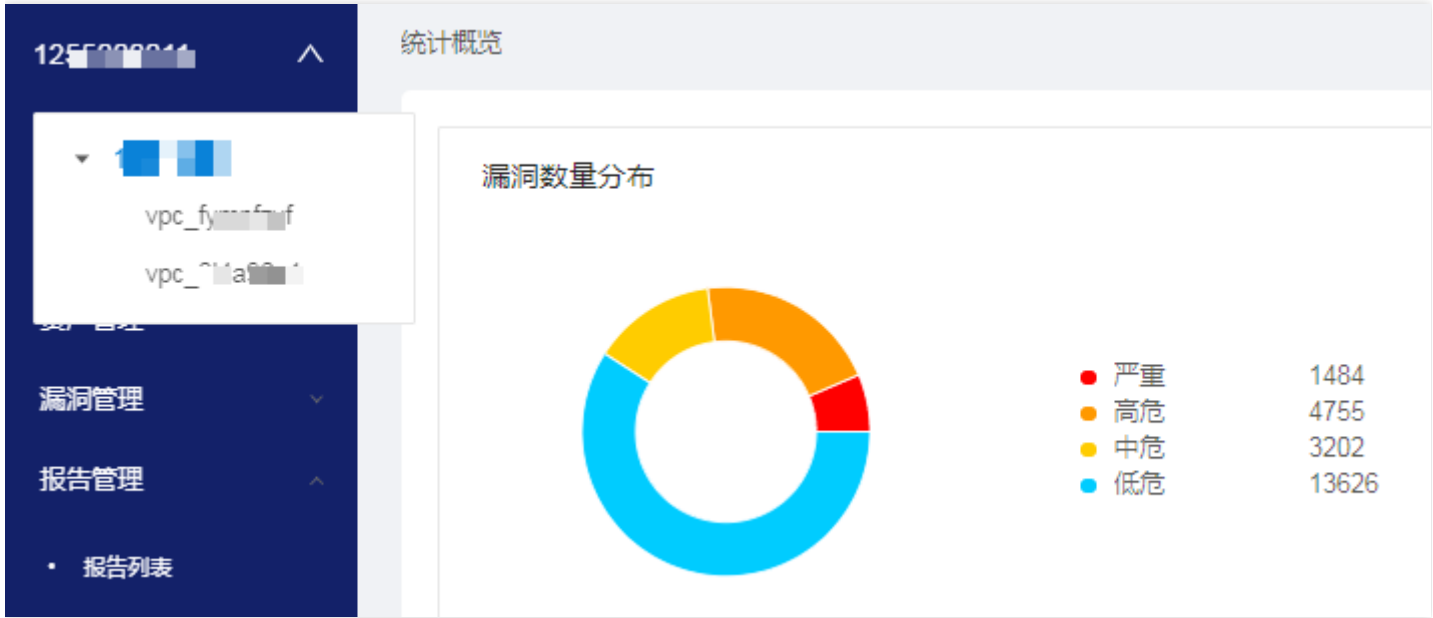
漏洞扫描时，会模拟黑客入侵攻击，对用户的服务器进行安全扫描，如果用户服务器有安全防护或监控部署，分析处理告警时可将扫描IP加白或者忽略。



选择vpc

最近更新时间: 2023-01-05 14:24:00

首先在页面左上角选择将要扫描资产所属VPC。





添加资产

最近更新时间: 2021-09-01 09:47:10

1、在资产管理可以添加各类资产，添加主机资产为例，在左侧导航菜单选择资产管理，选择主机资产；



2、在右侧主机列表，点击手动添加主机；

主机列表

+ 添加筛选条件

已选择 0 个主机

生成主机资产报告

删除选中的主机

扫描选中的主机

导出选中的主机

+ 手动添加主机

<input type="checkbox"/> IP 地址	操作系统	来源	所属工作区	负责人	最后存活时间
<input type="checkbox"/> 10.10.10.13	Linux	扫描发现	默认工作区-125500...	-	2020-09-25 14:20:36
<input type="checkbox"/> 10.10.10.9	Windows/a	扫描发现	默认工作区-125500...	-	2020-09-25 14:45:31



3、输入主机IP地址（必填项）、操作系统、设备名称、备注等信息，点确定添加主机

手动添加主机

✕

* 添加方式

添加一个 IP

添加多个 IP

上传 IP 文件

* IP 地址

172.16.0.1

操作系统

Unix

设备名称

主机

备注

AP服务器

取消

确定



扫描资产漏洞

最近更新时间: 2023-01-05 14:24:00

扫描方式1：从资产管理直接创建扫描任务快速扫描。

1、在资产管理，主机资产，选择要扫描的资产，可选一个或多个，点击扫描选中的主机

主机列表

+ 添加筛选条件

已选择 2 个主机

生成主机资产报告

删除选中的主机

扫描选中的主机

导出选中的主机

+ 手动添加主机

<input type="checkbox"/> IP 地址	操作系统	来源	所属工作区	负责人	最后存活时间
<input checked="" type="checkbox"/> 10.10.10.13	Linux	扫描发现	默认工作区-125500...	-	2020-09-26 22:50:03
<input checked="" type="checkbox"/> 10.10.10.9	Windows/a	扫描发现	默认工作区-125500...	-	2020-09-27 08:19:33
<input type="checkbox"/> 10.10.10.10	Linux	扫描发现	默认工作区-125500...	-	2020-09-24 09:10:04

2、选择扫描策略；

添加扫描任务

基础服务漏洞扫描

针对主机进行全面的资产发...

主机资产监控

对企业资产进行定期巡检，...

3、填写任务基本信息，输入任务名称，其他选项默认即可（带* 号为必填项），点击创建并立即扫描任务立即开始扫描，点击仅创建任务保存任务暂不扫描；



添加扫描任务

任务基本信息

* 任务名称

创建扫描任务

备注

服务漏洞扫描

仅创建任务

创建并立即扫描任务

4、在扫描管理 – 任务列表中可查看上面新创建的扫描任务；

扫描任务列表

我创建的任务

我管理的任务

其他相关任务

+ 添加筛选条件

已选择 0 个扫描任务

删除选中的扫描任务

启动任务

暂停任务

停止任务

+ 添加扫描任务

<input type="checkbox"/> 扫描任务名称	扫描策略	所属工作区	扫描计划	扫描状态
<input type="checkbox"/> 创建扫描任务	基础服务漏洞扫描	默认工作区-125500...	无	-

5、点击扫描任务所在行可查看任务详情；



创建扫描任务

结果对比

扫描历史

编辑扫描任务

暂停任务

停止扫描

服务漏洞扫描

任务统计

漏洞 (0)

域名 (0)

主机 (2)

服务 (4)

Web 站点 (0)

扫描进度

任务基本信息

漏洞探测

75%

任务状态

正在扫描

扫描策略

基础服务漏洞扫描

启动时间

2020-09-27 11:51:12

扫描方式2：从扫描管理创建扫描任务进行扫描（可自定义扫描选项）。

1、在扫描管理，任务列表，点击+添加扫描任务；

扫描任务列表

我创建的任务

我管理的任务

其他相关任务

+ 添加筛选条件

已选择 0 个扫描任务

删除选中的扫描任务

启动任务

暂停任务

停止任务

+ 添加扫描任务

<input type="checkbox"/>	扫描任务名称	扫描策略	所属工作区	扫描计划	扫描状态
<input type="checkbox"/>	创建扫描任务	基础服务漏洞扫描	默认工作区-125500...	无	扫描结束 (成功)
<input type="checkbox"/>	基础服务001	基础服务漏洞扫描	默认工作区-125500...	每天 08:19:00 定时扫描	扫描结束 (成功)
<input type="checkbox"/>	基础服务002	基础服务漏洞扫描	默认工作区-125500...	每天 22:50:00 定时扫描	扫描结束 (成功)
<input type="checkbox"/>	0729	基础服务漏洞扫描	默认工作区-125500...	每天 15:37:00 定时扫描	扫描结束 (成功)

2、选择扫描策略，以选择基础服务漏洞扫描为例；



添加扫描任务



基础 Web 漏洞扫描
针对 Web 站点进行全面的资...



基础服务漏洞扫描
针对主机进行全面的资产发现...



域名资产发现
针对域名进行全面的资产发现



主机资产监控
对企业资产进行定期巡检，监...



特定服务扫描
针对特定服务进行漏洞扫描



资产发现
初次资产发现扫描

3、填写和选择任务信息，分别有基本信息、任务控制、信息收集参数、漏洞探测参数四个选项卡，提供多个可定义的选项供调整扫描策略（详情见附件扫描参数详解一节），可使用默认值，最后点击创建并立即扫描任务立即执行扫描，点击仅创建任务可稍后再进行扫描；

添加扫描任务

基本信息

任务控制

信息收集参数

漏洞探测参数

任务信息

* 扫描任务名称 ?

备注

* 扫描目标

手动输入

上传目标文件

扫描目标格式：

1.1.1.1

1.1.1.1/24

1.1.1.1-255

www.chaitin.com

仅创建任务

创建并立即扫描任务

版权所有：

第23 页 共73页



查看漏洞结果

最近更新时间: 2023-01-05 14:24:00

1、在 扫描管理， 任务列表， 点击需要查看的任务， 进入任务详情页面， 点击 漏洞 选项卡， 可查看扫描发现的漏洞信息；

基础服务漏洞扫描

结果对比

扫描历史

生成报告

快速深度扫描

编辑扫描任务

立即扫描

任务统计

漏洞 (7)

域名 (0)

主机 (1)

服务 (1)

Web 站点 (0)

风险等级	确信程度	漏洞名称	漏洞影响位置	漏洞状态
<div>+ 中危</div>	疑似	CVE-2019-6111: OpenSSH 输入验证错...	1	<div><div>1</div><div>0</div><div>0</div></div>
<div>+ 低危</div>	疑似	CVE-2019-6110: OpenSSH 访问控制错...	1	<div><div>1</div><div>0</div><div>0</div></div>
<div>+ 低危</div>	疑似	CVE-2019-6109: OpenSSH 访问控制错...	1	<div><div>1</div><div>0</div><div>0</div></div>

2、点击+号， 显示漏洞影响的资产列表；

任务统计

漏洞 (7)

域名 (0)

主机 (1)

服务 (1)

Web 站点 (0)

风险等级	确信程度	漏洞名称	漏洞影响位置	漏洞状态
<div>- 中危</div>	疑似	CVE-2019-6111: OpenSSH 输入验证错...	1	<div><div>1</div><div>0</div><div>0</div></div>
影响目标 10.10.10.10:22/TCP				<div><div>待修复</div></div>



3、点击资产所在行进入漏洞详情页，包括漏洞基础信息和技术细节，可详细了解漏洞信息；

CVE-2019-6111: OpenSSH 输入验证错误漏洞

技术细节		基础信息	
漏洞描述	漏洞描述	漏洞名称	CVE-2019-6111: OpenSSH 输入验证错误漏洞
漏洞危害	漏洞目标		
CVSS 风险评分	经过对以下目标进行扫描测试：	漏洞类型	其他
漏洞利用方式	1. 10. 2	风险等级	中危
漏洞验证方式	发现其中存在 CVE-2019-6111 漏洞。	确信程度	疑似
CWE 类型介绍	当前服务所对应的 CPE 信息如下：	漏洞编号	CNNVD-201901-76 7 CVE-2019-6111
漏洞修复方式	<ul style="list-style-type: none">cpe:/a:openbsd:openssh:7.4	发现时间	2020-09-24 09:10:04
	漏洞概述		



漏洞修复

最近更新时间: 2023-01-05 14:24:00

漏洞修复具体操作可参考漏洞详情页中漏洞修复方式，确认修复后，在漏洞管理，漏洞列表，点击漏洞验证，漏洞状态处理自动修改为已修复，说明漏洞修复成功，或者重新执行扫描任务，如果漏洞没有被扫出，说明资产漏洞已修复成功。

漏洞描述	CVSS 评分	待修复	扫描发现	2021-01-28 16:21:50
漏洞危害	无	待修复	扫描发现	2021-01-28 16:16:42
CVSS 评分	漏洞验证方式	待修复	扫描发现	2021-01-22 13:52:29
漏洞验证方式	见上述详情	待修复	扫描发现	2021-01-20 15:37:35
修复方案	漏洞验证	待修复	扫描发现	2021-01-19 16:16:15



用户指南

扫描管理

扫描管理-任务统计

最近更新时间: 2023-01-05 16:52:26

任务统计页，主要从几种维度展示扫描任务信息，以及扫描任务发现的资产和漏洞趋势分析等。

1、任务统计页面展示系统中任务的运行情况，不同扫描策略的任务数量分布，展示不同扫描策略的任务数量，鼠标悬浮在饼图上方可以看到具体的任务数最大并行任务数统计；



2、展示系统当前正在并行的任务数（正在运行的任务总数），以及剩余并行任务数（还能够同时运行的任务数量）；

最大并行任务数统计



3、新发现的漏洞数量趋势分析，展示系统最近15天内，新发现的漏洞数量趋势，鼠标悬浮在图形上方，可以看到每天新发现的，各个风险等级的漏洞数量；

新发现的漏洞数量趋势分析



4、新发现的资产数量趋势分析，展示系统最近 15 天内，新发现的资产数量趋势，鼠标悬浮在图形上方，可以看到每天新发现的资产数量，点击图形右上角的按钮，可以切换展示不同资产类型的趋势分析；



5、存在漏洞的任务，展示所有存在漏洞的任务，方便用户直观地找到最需要处理与排查的任务任务的排名由任务发现漏洞的风险程度决定：严重漏洞越多，排名越高；严重漏洞相同的任务，高危漏洞越多排名越高；

存在漏洞的任务

排名	任务名称	漏洞数量	扫描时间
1	扫描任务	<div><div>1</div><div>0</div><div>0</div><div>0</div></div>	2020-09-26 14:45:00
2	基础服务001	<div><div>1</div><div>0</div><div>0</div><div>0</div></div>	2020-09-27 08:19:00
3	RW0925001	<div><div>1</div><div>0</div><div>0</div><div>0</div></div>	2020-09-25 10:50:42



扫描管理-扫描策略

最近更新时间: 2023-01-05 16:52:26

扫描策略，主要用于在创建扫描任务时，提供扫描规则模板，实现一键式便捷快速扫描，有系统预定义策略，用户也可创建自定义策略。

1、扫描策略列表页中显示当前已创建扫描策略，也可添加自定义的扫描策略；

扫描策略列表

扫描策略快速筛选

☐ 应急策略

+ 添加筛选条件

已选择 0 个扫描策略

删除选中的扫描策略

+ 添加扫描策略

<input type="checkbox"/> 任务名称	扫描策略描述	扫描策略类型	扫描策略添加时间	操作
<input type="checkbox"/> 基础 Web 漏洞扫描	针对 Web 站点进行全面的资产发现和漏洞扫描	系统内置	2020-07-27 13:40:34	扫描
<input type="checkbox"/> 基础服务漏洞扫描	针对主机进行全面的资产发现和漏洞扫描	系统内置	2020-07-27 13:40:34	扫描
<input type="checkbox"/> 域名资产发现	针对域名进行全面的资产发现	系统内置	2020-07-27 13:40:34	扫描
<input type="checkbox"/> 主机资产监控	对企业资产进行定期巡检，监控企业资产的变更情况	系统内置	2020-07-27 13:40:34	扫描

2、扫描策略后均有扫描 操作按钮，可以快速创建扫描任务，作为启动任务的快速入口，按照步骤和提示进行添加任务操作；

扫描策略列表

扫描策略快速筛选

☐ 应急策略

+ 添加筛选条件

已选择 0 个扫描策略

删除选中的扫描策略

+ 添加扫描策略

<input type="checkbox"/> 任务名称	扫描策略描述	扫描策略类型	扫描策略添加时间	操作
<input type="checkbox"/> 基础 Web 漏洞扫描	针对 Web 站点进行全面的资产发现和漏洞...	系统内置	2020-07-27 13:40:34	扫描
<input type="checkbox"/> 基础服务漏洞扫描	针对主机进行全面的资产发现和漏洞扫描	系统内置	2020-07-27 13:40:34	扫描
<input type="checkbox"/> 域名资产发现	针对域名进行全面的资产发现	系统内置	2020-07-27 13:40:34	扫描

3、筛选操作-在此页面，可对扫描策略进行筛选操作，可根据扫描策略名称、扫描策略描述、扫描策略类型、扫描策略添加时间，自由添加一个或多个条件进行筛选；



添加筛选条件

扫描策略名称

请输入要筛选的内容

+ 添加筛选条件

取消

保存

4、应急策略，主要用于新爆发漏洞的检测，勾选应急策略可直接筛选出系统最新发布的应急策略，可进行编辑或直接创建扫描任务进行扫描；

扫描策略列表

扫描策略快速筛选

☒ 应急策略

扫描策略类型 应急策略 X

+ 添加筛选条件

已选择 0 个扫描策略

删除选中的扫描策略

+ 添加扫描策略

<input type="checkbox"/> 任务名称	扫描策略描述	扫描策略类型	扫描策略添加时间	操作
-------------------------------	--------	--------	----------	----

- 5、添加扫描策略，在扫描策略列表页，可进行自定义扫描策略的添加操作；
- 1) 点击+添加扫描策略创建自定义扫描策略；



扫描管理 / 扫描策略

扫描策略列表

扫描策略快速筛选 ☐ 应急策略

+ 添加筛选条件

已选择 0 个扫描策略

删除选中的扫描策略

+ 添加扫描策略

<input type="checkbox"/> v	任务名称	扫描策略描述	扫描策略类型	扫描策略添加时间	操作
<input type="checkbox"/>	基础 Web 漏洞扫描	针对 Web 站点进行全面的资产...	系统内置	2020-07-27 13:40:34	扫描
<input type="checkbox"/>	基础服务漏洞扫描	针对主机进行全面的资产发现...	系统内置	2020-07-27 13:40:34	扫描

2) 添加扫描策略界面配置扫描策略基本信息，包括输入扫描策略名称、扫描策略描述、扫描策略图片等，完成后点击下一步继续；

添加扫描策略

① 基本信息

② 选择基础策略

③ 扫描策略参数

* 扫描策略名称 添加扫描策略

* 扫描策略描述 添加扫描策略

扫描策略图标

+
上传

下一步

3) 选择基础策略，选择系统已有策略作为模板，可以是系统内置扫描策略，也可以是自定义的扫描策略，选择后点击下一步继续；



添加扫描策略

✓ 基本信息

2 选择基础策略

3 扫描策略参数



基础 Web 漏洞扫描
针对 Web 站点进行全面的资...



基础服务漏洞扫描
针对主机进行全面的资产发现...



域名资产发现
针对域名进行全面的资产发现



主机资产监控
对企业资产进行定期巡检，监...



特定服务扫描
针对特定服务进行漏洞扫描



资产发现
初次资产发现扫描



开放区扫描
开放区扫描

上一步

下一步

4) 配置扫描策略参数，可自行对每一项参数进行设置，包括任务控制、信息收集参数、漏洞探测参数，选择不同的基础策略，配置参数会有所不同。参数配置完成后点击完成，创建扫描策略成功；

添加扫描策略

✓ 基本信息

✓ 选择基础策略

3 扫描策略参数

任务控制

信息收集参数

漏洞探测参数

扫描任务限制

* 任务最大运行时间 ⓘ 180 分钟

* 最大并发主机数 50

* 最大带宽占用限制 ⓘ 2000 KB/s

☐ 智能流量管控



扫描管理-任务列表

最近更新时间: 2023-01-05 16:52:26

任务列表，可创建扫描任务，操作扫描任务（包括筛选、执行、暂停、停止、编辑、删除等），查看扫描任务及其扫描结果。

1、扫描任务列表，扫描任务列表显示账户下的扫描任务，包括 我创建的扫描任务，我管理的扫描任务 和 其他相关任务；

- 我创建的扫描任务：账户自己创建的扫描任务；
- 我管理的扫描任务：其他账户创建的扫描任务，具有操作权限；
- 其他相关任务：是管理员统一下发的扫描任务，只有查看权限；

扫描任务列表

我创建的任务我管理的任务其他相关任务

+ 添加筛选条件

已选择 0 个扫描任务删除选中的扫描任务启动任务暂停任务停止任务+ 添加扫描任务

<input type="checkbox"/>	扫描任务名称	扫描策略	所属工作区	扫描计划	扫描状态
<input type="checkbox"/>	创建扫描任务	基础服务漏洞扫描	默认工作区-125500...	无	-

2、筛选操作，在任务列表页可对任务进行筛选操作，可根据多种维度筛选，包括扫描任务名称、扫描策略、扫描计划、创建时间、下次执行时间、扫描状态、所属工作区等，自由添加一个或多个条件进行筛选；

添加筛选条件

扫描任务名称请输入要筛选的内容

+ 添加筛选条件

取消保存

3、操作任务，启动任务（立即扫描）、暂停扫描、停止扫描、删除选中的扫描任务、编辑扫描任务

- 1) 启动任务（立即扫描），对非正在扫描的任务，可以进行立即扫描的操作；
- 2) 暂停扫描，对正在扫描的任务，可以进行暂停扫描的操作；



- 3) 停止扫描，对正在扫描或等待扫描的任务，可以进行停止扫描的操作；
- 4) 删除选中的扫描任务，可删除选中的扫描任务；
- 5) 编辑扫描任务，编辑扫描任务信息及扫描参数；

4、添加扫描任务

- 1) 点击 +添加扫描任务 按钮，创建新的扫描任务；

扫描任务列表

我创建的任务

我管理的任务

其他相关任务

+ 添加筛选条件

已选择 0 个扫描任务

删除选中的扫描任务

启动任务

暂停任务

停止任务

+ 添加扫描任务

<input type="checkbox"/>	扫描任务名称	扫描策略	所属工作区	扫描计划	扫描状态
<input type="checkbox"/>	基础服务001	基础服务漏洞扫描	默认工作区-125500...	每天 08:19:00 定时扫描	扫描成功
<input type="checkbox"/>	基础服务002	基础服务漏洞扫描	默认工作区-125500...	每天 22:50:00 定时扫描	扫描成功
<input type="checkbox"/>	0729	基础服务漏洞扫描	默认工作区-125500...	每天 15:37:00 定时扫描	扫描成功

- 2) 选择扫描策略；

添加扫描任务

基础 Web 漏洞扫描

针对 Web 站点进行全面的资...

基础服务漏洞扫描

针对主机进行全面的资产发现...

域名资产发现

针对域名进行全面的资产发现

主机资产监控

对企业资产进行定期巡检，监...

特定服务扫描

针对特定服务进行漏洞扫描

资产发现

初次资产发现扫描

- 3) 填写和选择任务信息，分别有基本信息、任务控制、信息收集参数、漏洞探测参数四个选项卡，提供多个可定义的选项供调整扫描策略（详情见附件扫描参数详解一节），可使用默认值，最后点击创建并立即扫描任务立即执行扫描，点击仅创建任务可稍后再进行扫描；

- 4) 快速深度扫描，对当前任务扫描结果中的资产（主机、域名、Web、服务）快速创建扫描任务，在任务详情页点击快速深度扫描创建对相关资产的扫描任务；



选择快速深度扫描的模式

快速深度扫描是对本次扫描结果中的资产进行快速创建扫描任务的一种操作。

☐ 对扫描结果中的主机资产进行扫描

☐ 对扫描结果中的服务资产进行扫描

☐ 对扫描结果中的域名资产进行扫描

☒ 对扫描结果中的 Web 站点资产进行扫描

取消

确定

5) 生成报告，快速生成当前任务的扫描报告，在任务详情页点击 生成报告，点击 开始生成报告，可在 报告管理，报告列表 中查看；

生成扫描任务报告

报告名称

扫描报告0926

导出信息配置

☒ 导出资产信息

☒ 导出漏洞信息

取消

开始生成报告

基本信息 — 任务信息，包括任务名称、备注、扫描目标、执行类型、指定时间段等，带红色*号为必填项，如下图：



任务信息

* 扫描任务名称 ②

备注

* 扫描目标

手动输入

上传目标文件

扫描目标格式：

1.1.1.1
1.1.1.1/24
1.1.1.1-255
www.chaitin.com
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

* 执行类型

定时扫描一次

* 扫描时间 ②

2020-09-24 09:47

扫描任务创建成功后，将在 2020-09-24 09:47:00 开始执行

指定时间段

请选择时间

~

请选择时间

仅创建任务

创建并立即扫描任务

相关选项说明：

- 扫描目标支持IPv4，IPv6格式的IP地址或域名，可手工输入，也可以从文件导入；
- 执行类型有立即执行、定时扫描一次、每天循环扫描、每周循环扫描和每月循环扫描；
- 指定时间段，扫描任务只能在指定时间段内执行，设定时间段内扫描任务未执行完时将暂停，并等待下一个设定的时间段自动继续执行；

基本信息 — 引擎节点选择，默认情况下一个VPC下只有一个引擎节点，默认已勾选，无需操作，如下图：

<input checked="" type="checkbox"/> 引擎启用	引擎节点 IP	引擎状态	可用工作区
<input checked="" type="checkbox"/>	192.168.0.1	空闲	默认工作区-1255000058-vpc_ofn1s40f



资产管理

资产统计

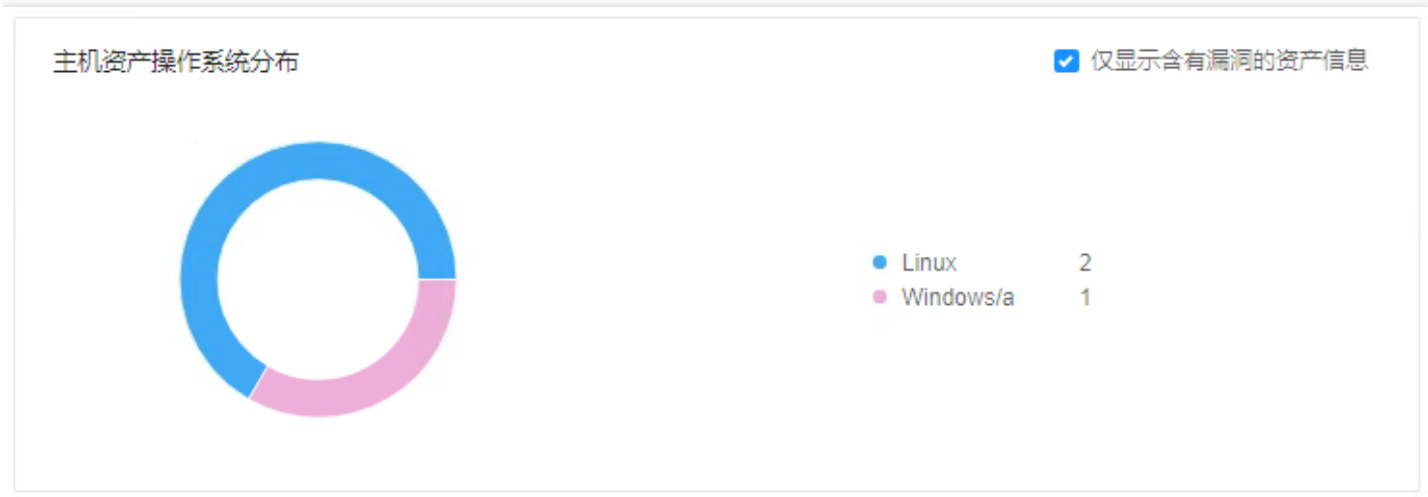
最近更新时间: 2023-01-05 16:52:26

多维度展示资产统计信息，包括各类资产数量及其变化趋势，各类资产漏洞分布及变化趋势等。

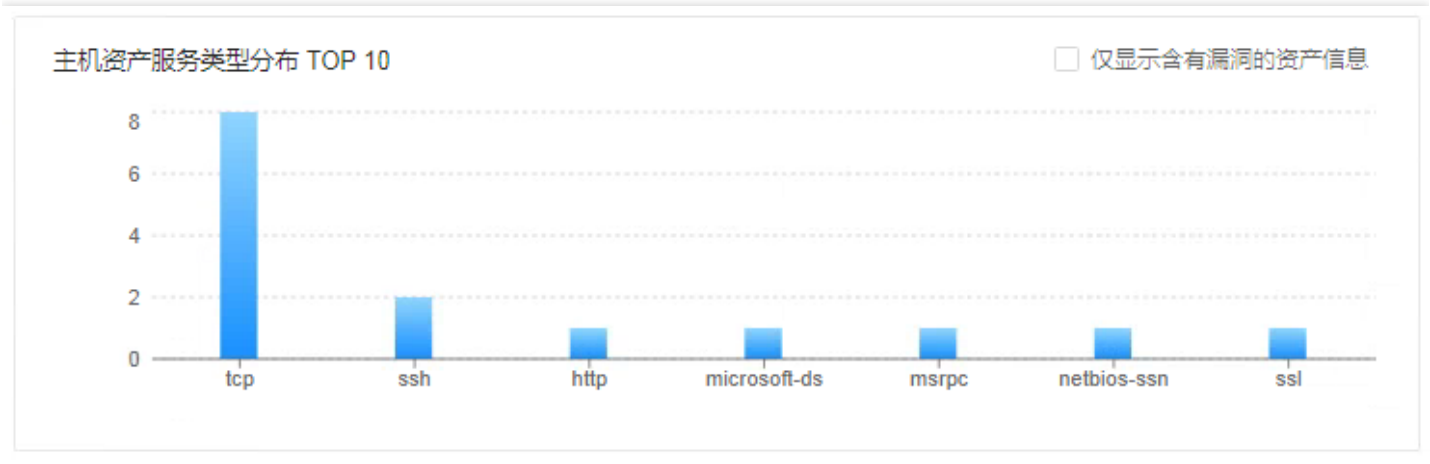
1、资产统计，显示域名总数、主机总数、服务总数、web站点总数；



2、主机资产操作系统分布，勾选仅显示含有漏洞的资产信息，可筛选仅含有漏洞的资产信息；



3、主机资产服务类型分布TOP 10 ，勾选仅显示含有漏洞的资产信息，筛选仅含有漏洞资产的信息；



4、Web资产框架分布TOP 10, 勾选“仅显示含有漏洞的资产信息”，筛选仅含有漏洞资产的信息；



5、风险最高的web资产TOP 10，显示排名、web站点地址、漏洞数量；

风险最高的 Web 资产 TOP 10

排名	Web 站点地址	漏洞数量
暂无数据		



风险资产

最近更新时间: 2023-01-05 16:52:22

风险资产，展示漏洞影响的各类资产，包括有漏洞的域名、有漏洞的主机、有漏洞的服务、有漏洞的web服务；

1、有漏洞的域名，从域名、漏洞数量、所属工作区、负责人、最后扫描时间等维度展示有漏洞的域名

风险资产

有漏洞的域名

有漏洞的主机

有漏洞的服务

有漏洞的 Web 站点

+ 添加筛选条件

域名	漏洞数量	所属工作区	负责人	最后扫描时间
----	------	-------	-----	--------

2、有漏洞的主机，从IP地址、操作系统、漏扫数量、所属工作区、负责人、最后扫描时间等维度展示存在漏洞的主机

风险资产

有漏洞的域名

有漏洞的主机

有漏洞的服务

有漏洞的 Web 站点

+ 添加筛选条件

IP 地址	操作系统	漏洞数量				所属工作区	负责人	最后扫描时间
10.1.1.0/24	Windows/a	1	0	0	0	默认工作区-125500...	-	2020-09-24 08:19:03
10.10.10.0/24	Linux	0	8	6	15	默认工作区-125500...	-	2020-09-23 22:50:01
10.10.10.1/24	Linux	0	0	1	6	默认工作区-125500...	-	2020-09-23 15:37:00

<

1

>

10 条/页



3、有漏洞的服务，从端口、服务类型、漏洞数量、所属工作区、负责人、最后扫描的时间等维度展示

风险资产

有漏洞的域名

有漏洞的主机

有漏洞的服务

有漏洞的 Web 站点

+ 添加筛选条件

端口	服务类型	漏洞数量	所属工作区	负责人	最后扫描时间
10000-10000 TCP	ssl	<div>1</div> <div>0</div> <div>0</div> <div>0</div>	默认工作区-125500...	-	2020-09-24 08:19:03
10000-10000 CP	ssh	<div>0</div> <div>8</div> <div>6</div> <div>15</div>	默认工作区-125500...	-	2020-09-23 22:50:01
10000-10000 P/TCP	ssh	<div>0</div> <div>0</div> <div>1</div> <div>6</div>	默认工作区-125500...	-	2020-09-23 15:37:00

<

1

>

10 条/页

4、有漏洞的web站点，从web站点地址、web站点标题、漏洞数量、所属工作区、负责人、最后扫描时间等维度展示

风险资产

有漏洞的域名

有漏洞的主机

有漏洞的服务

有漏洞的 Web 站点

+ 添加筛选条件

Web 站点地址	Web 站点标题	漏洞数量	所属工作区	负责人	最后扫描时间
----------	----------	------	-------	-----	--------

暂无数据



主机资产

最近更新时间: 2023-01-05 16:52:22

1、主机列表，从IP地址、操作系统、来源、所属工作区、负责人、最后存活时间等维度显示主机资产；

主机列表

+ 添加筛选条件

已选择 0 个主机

生成主机资产报告

删除选中的主机

扫描选中的主机

导出选中的主机

+ 手动添加主机

<input type="checkbox"/>	IP 地址	操作系统	来源	所属工作区	负责人	最后存活时间
<input type="checkbox"/>	10.10.10.1	Linux	扫描发现	默认工作区-125500005...	-	2020-08-02 15:37:06

< 1 >

10 条/页

2、手工添加主机，在主机列表页点击+手动添加主机，可手工添加一个或多个主机资产；

1) 添加一个IP，填写ip地址、操作系统、设备名称，备注等信息，带* 号为必填项，点击确定完成添加；

手动添加主机

* 添加方式

添加一个 IP

添加多个 IP

上传 IP 文件

* IP 地址

操作系统

设备名称

备注

取消

确定

2) 添加多个IP，按照指定格式填写主机IP地址，并填写统一备注，带* 号为必填项，点击确定完成添加；

3) 上传IP文件，首先通过点击下载文件模板下载模板文件并填写主机资产信息，修改完成后上传文件，点击确定完



成添加；

手动添加主机

X

* 添加方式

添加一个 IP

添加多个 IP

上传 IP 文件

备注

点击下载文件模板



点击或将文件拖拽到这里上传

文件大小不超过 10 M ; 文件类型 : .csv

取消

确定



Web站点资产

最近更新时间: 2023-01-05 16:52:22

1、Web站点列表，从web站点地址、web站点标题、url数量、来源、所属工作区、负责人、最后活动时间等维度显示Web站点资产；

Web 站点列表

+ 添加筛选条件

已选择 0 个 Web 站点

生成 Web 站点资产报告

删除选中的 Web 站点

扫描选中的 Web 站点

+ 手动添加站点

<input type="checkbox"/>	Web 站点地址	Web 站点标题	url 数量	来源	所属工作区	负责人	最后存活时间
<div><div></div><div>暂无数据</div></div>							

<

0

>

10 条/页

2、手动添加站点，同样支持添加一个站点、添加多个站点以及上传站点文件3种添加方式；

手动添加站点

* 添加方式

添加一个站点

添加多个站点

上传站点文件

* Web 站点地址

Web 站点标题

备注

取消

确定



服务资产

最近更新时间: 2023-01-05 16:52:22

1、服务列表，从端口、服务类型、应用、版本、来源、所属工作区、负责人、最后存活时间等维度显示服务资产；

服务列表

+ 添加筛选条件

已选择 0 个服务

删除选中的服务

扫描选中的服务

+ 手动添加服务

<input type="checkbox"/>	端口	服务类型	应用	版本	来源	所属工作区
<input type="checkbox"/>	22	ssh	OpenSSH	7.4	扫描发现	默认工作区

<

1

>

10 条/页

2、手动添加服务，同样支持添加一个服务、添加多个服务以及上传服务文件3种添加方式；

手动添加服务

* 添加方式

添加一个服务

添加多个服务

上传服务文件

* 主机 IP 地址

* 端口

TCP

1

服务类型

备注

取消

确定



域名资产

最近更新时间: 2023-01-05 16:52:22

1、域名列表中，从域名、来源、所属工作区、负责人、最后存活时间等维度显示域名资产；

域名列表

+ 添加筛选条件

已选择 0 个域名

删除选中的域名

扫描选中的域名

导出选中的域名

+ 手动添加域名

<input type="checkbox"/> 域名	来源	所属工作区	负责人	最后存活时间
<div><div></div>暂无数据</div>				

<

0

>

10 条/页

2、手动添加域名，同样支持添加一个域名、添加多个域名以及上传域名文件3种添加方式，如下图：

手动添加域名

X

* 添加方式

添加一个域名

添加多个域名

上传域名文件

* 域名

备注

取消

确定

版权所有：

第46 页 共73页

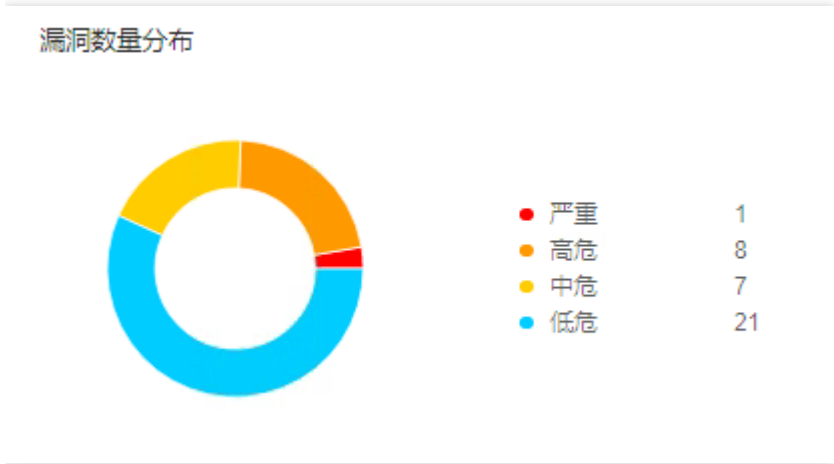


漏洞管理

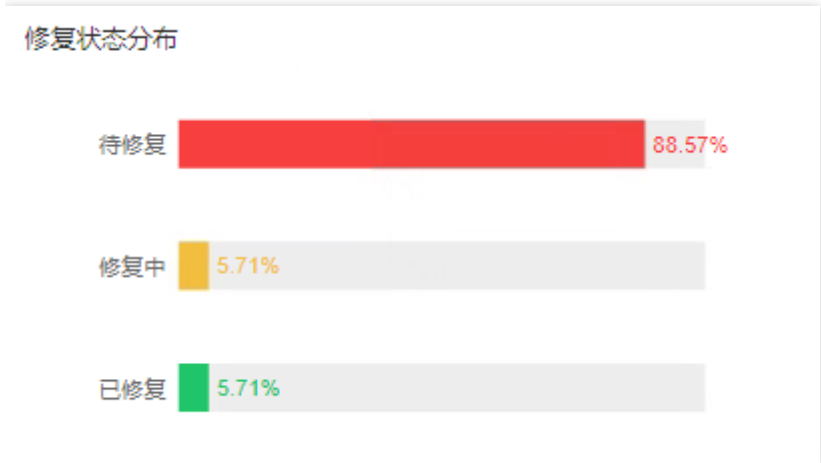
漏洞统计

最近更新时间: 2023-01-05 16:52:21

1、漏洞数量分布，饼图展示不同风险等级的漏洞分布情况，鼠标悬浮在饼图上会显示漏洞总数、所选部分标识的漏洞风险等级及其漏洞数量和占比，数据展示不同风险程度的漏洞数量（严重、高危、中危、低危）；



2、修复状态分布，展示漏洞修复三种状态（待修复、修复中、已修复）的占比，鼠标悬浮在图形上，会显示当前状态下的漏洞数量；

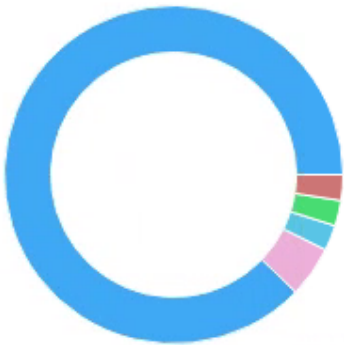


3、漏洞类型占比，分别展示各类型漏洞数量及占比；



漏洞类型占比

其他	36
不安全的配置	2
代码注入	1
信息泄露	1
未授权访问	1



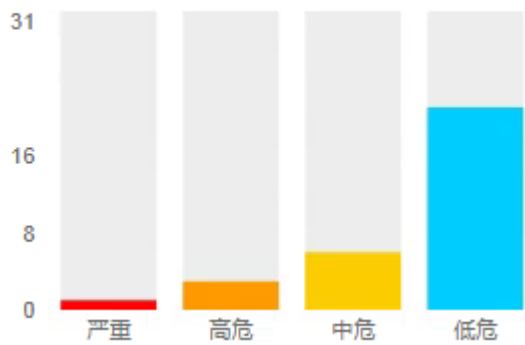
4、修复漏洞耗费时间分布，修复漏洞耗费时间分布，主要展示修复不同风险程度的漏洞时，所耗费时间的分布情况；

修复漏洞耗费时间分布

30 天内	0	2	0	0
30 - 60 天	0	0	0	0
60 - 90 天	0	0	0	0
90 天以上	0	0	0	0
	严重	高危	中危	低危

5、未修复的漏洞数量，主要展示处于待修复状态下不同风险程度的漏洞数量，鼠标悬浮在柱形图上时，将显示所选风险等级的未修复漏洞数量；

未修复的漏洞数量





漏洞列表

最近更新时间: 2023-01-05 16:52:21

1、漏洞列表，从漏洞风险等级、确信程度、漏洞名称、存在漏洞的位置、漏洞状态等维度显示被扫描发现的漏洞；

漏洞列表

+ 添加筛选条件

已选择 0 个漏洞

生成漏洞报告

删除选中的漏洞

<input type="checkbox"/> ▼	风险等级	确信程度	漏洞名称漏洞的位置	所属工作区	负责人	漏洞状态处理
<input type="checkbox"/>	严重	确信	10.10.10.10/22/TCP	默认工作区-125500...	-	待修复 ▼
<input type="checkbox"/>	高危	疑似	10.10.10.10/22/TCP	默认工作区-125500...	-	待修复 ▼

2、筛选漏洞，在列表页可对漏洞进行筛选操作，可根据漏洞名称、漏洞风险等级、漏洞确信程度、相关资产、漏洞状态、发现时间、相关扫描任务，自由添加一个或多个条件进行筛选；

添加筛选条件

漏洞名称 ▼

请输入要筛选的内容

模糊匹配 ✓

+ 添加筛选条件

取消

保存

3、漏洞详情，漏洞列表点击漏洞所在行进入漏洞详情页；



Microsoft 远程桌面服务远程代码执行

技术细节

漏洞描述	漏洞描述
漏洞危害	Microsoft Windows 操作系统是目前使用最广泛的操作系统之一，其远程桌面协议（Remote Desktop Protocol）被广泛用于用户远程管理计算机。远程桌面协议被设计用于允许用户和其远程计算机建立虚拟会话，从而允许用户在本地计算机上处理远程计算机上的数据和应用。
CVSS 风险评分	
漏洞利用方式	
漏洞验证方式	远程桌面协议是一个多通道（multi-channel）的协议，让使用者（所在计算机称为客户端或“本地计算机”）连上提供微软终端机服务的计算机（称为服务端或“远程计算机”）。大部分的 Windows 版本都有客户端所需软件，有些其他操作系统也有这些客户端软件，例如 Linux、Free BSD、MacOSX。服务端计算机方面，则默认听取送到 TCP 3389 端口的数据。
漏洞修复方式	Microsoft 远程桌面服务远程代码执行漏洞（漏洞编号：CVE-2019-0708）指的是攻击者在未经身份校验的情况下，通过 RDP 连接目标系统并向其发送精心构造的请求，即可直接导致远程代码执行，整个过程不需要用户交互。攻击者一旦利用成功即可在目标系统上安装程序，查看、更改或者删除数据，创建具有完整用户权限的新账户，危害极大。
	2019 年 5 月 14 日，微软官方通过更正远程桌面服务处理连接请求的

基础信息

漏洞名称	Microsoft 远程桌面服务 远程代码执行
漏洞类型	代码注入
风险等级	严重
确信程度	确信
漏洞编号	CVE-2019-0708
相关资产	
扫描任务	扫描任务
发现时间	2020-09-23 14:30:13
所属工作区	默认工作区-1255000...
负责人	-
漏洞状态处理	待修复

漏洞详情页包括漏洞描述、漏洞危害、CVSS风险评分、漏洞利用方式、漏洞验证方式、漏洞修复方式等信息，可详细了解漏洞信息，并在修复漏洞时可作为参考。



报告管理

报告列表

最近更新时间: 2023-01-05 16:52:21

1、报告列表页展示生成的所有报告，从报告名称、使用的报告模板以及报告生成时间等维度展示，有生成报告、下载报告和删除报告等选项，如下图；

报告列表

+ 添加筛选条件

已选择 0 个报告

下载选中的报告

删除选中的报告

+ 生成报告

<input type="checkbox"/>	报告名称	报告模板	所属工作区	报告生成时间	操作
<input type="checkbox"/>	【2020-09-25_10:50:42】RW0...	漏洞扫描任务报告	默认工作区-125500...	2020-09-25 10:52:38	查看 删除

< 1 >

10 条/页

2、生成报告，在报告列表页点击 +生成报告，可手工生成扫描报告，详情见3.4.2节

3、下载扫描报告

1) 在报告列表页选择报告（可多选），点击 下载选中报告；

报告列表

+ 添加筛选条件

已选择 2 个报告

下载选中的报告

删除选中的报告

+ 生成报告

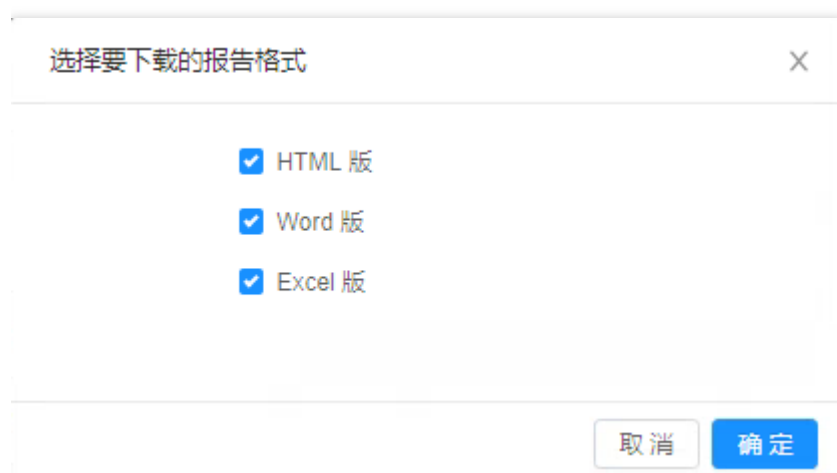
<input checked="" type="checkbox"/>	报告名称	报告模板	所属工作区	报告生成时间	操作
<input checked="" type="checkbox"/>	【2020-09-25_11:03:37】RW10...	漏洞扫描任务报告	默认工作区-125500...	2020-09-25 11:04:48	查看 删除
<input checked="" type="checkbox"/>	【2020-09-25_10:50:42】RW0...	漏洞扫描任务报告	默认工作区-125500...	2020-09-25 10:52:38	查看 删除

< 1 >

10 条/页



2) 选择报告输出格式，支持Word，Excel、HTML三种格式，点击 确定 后输入文件名保存到本地；



4、删除选中的报告，在报告列表页选择报告（可多选），点击 删除选中的报告 ，所有选中的报告信息均将被删除。



生成报告

最近更新时间: 2023-01-05 16:52:21

1、生成报告，输入报告名称、默认工作区和报告模板，带* 号为必填项，支持多种维度的模板供导出报告，包括主机资产报告、Web站点资产报告、漏洞报告、漏洞扫描任务报告等。选择主机资产报告为例；

生成新的报告

* 报告名称

手工生成报告

* 所属工作区

默认工作区-125F000050 wpc_0f6d1c106

* 报告模板

主机资产报告

Web 站点资产报告

漏洞报告

漏洞扫描任务报告


基线检查任务报告

2、从列表选择需要导出报告的项目（资产、漏洞、扫描任务），以下为从列表选择主机资产，点击 **从资产列表导入**；



生成新的报告

* 报告名称 主机资产报告

* 所属工作区 默认工作区-

* 报告模板 主机资产报告

* 目标主机资产

IP 地址

操作系统

所属工作区

操作

从资产列表导入


暂无数据☒ 导出与目标主机资产相关的服务信息☒ 导出与目标主机资产相关的漏洞信息

3、筛选并选择导入的项目后，点 确定；



选择需要导入的主机资产

IP 地址:

操作系统:

备注:

所属工作区

默认工作区-125500...

<input checked="" type="checkbox"/> IP 地址	操作系统	所属工作区	备注
<input checked="" type="checkbox"/> 10.10.10.10	Linux	默认工作区-125500...	
<input checked="" type="checkbox"/> 10.10.10.11	Windows	默认工作区-125500...	
<input checked="" type="checkbox"/> 10.10.10.12	Linux	默认工作区-125500...	

<

1

>

10 条/页

取消

确定

4、可勾选 导出与目标主机资产相关的服务信息和 导出目标主机资产相关的漏洞信息，点击生成报告，完成操作；



生成新的报告

* 报告名称 主机资产报告

* 所属工作区 默认工作区-1

* 报告模板 主机资产报告

* 目标主机资产

IP 地址	操作系统	所属工作区	操作
192.168.1.1	Linux	默认工作区-125500...	删除
192.168.1.2	Windows	默认工作区-125500...	删除
192.168.1.3	Linux	默认工作区-125500...	删除

从资产列表导入

- ☒ 导出与目标主机资产相关的服务信息
- ☒ 导出与目标主机资产相关的漏洞信息

生成报告

5、在报告列表页查看到生成的报告。



系统信息

系统状态

最近更新时间: 2023-01-05 16:52:21

系统状态，显示系统运行状态，系统运行时长，引擎节点详细信息，管理节点的负载状态、网络状态、磁盘状态等信息；

系统信息 / 系统状态

系统状态

系统运行状态

正常

系统运行时长

1周 3天 20小时 7分钟

引擎节点

负载状态

网络状态

磁盘状态

1、引擎节点选项卡

1) 显示引擎节点信息，包括引擎节点IP、运行状态、引擎权限、CPU/内存、系统版本、所属工作区、运行时长、备注等信息；

引擎节点

负载状态

网络状态

磁盘状态

节点状态

● 工作 0

● 空闲 1

● 异常 0

● 更新中 0

引擎节点 IP	运行状态	引擎权限	CPU / 内存	系统版本	所属工作区
192.168.1.1	空闲	自定义权限	0.10%; 463.81MB/3.84GB_r12	默认工作区-1255000058...	

2) 引擎节点系统状态，点击引擎节点所在行可进入引擎节点系统状态页，显示引擎节点的详细信息；



引擎节点系统状态

引擎节点 IP



运行状态

空闲

版本号

4.4.1_r12

运行时长

8周 5天 21小时 53分钟

备注

- 

最后升级时间

2020-09-23 14:11:57

引擎权限

自定义权限 

默认工作区-

负载状态

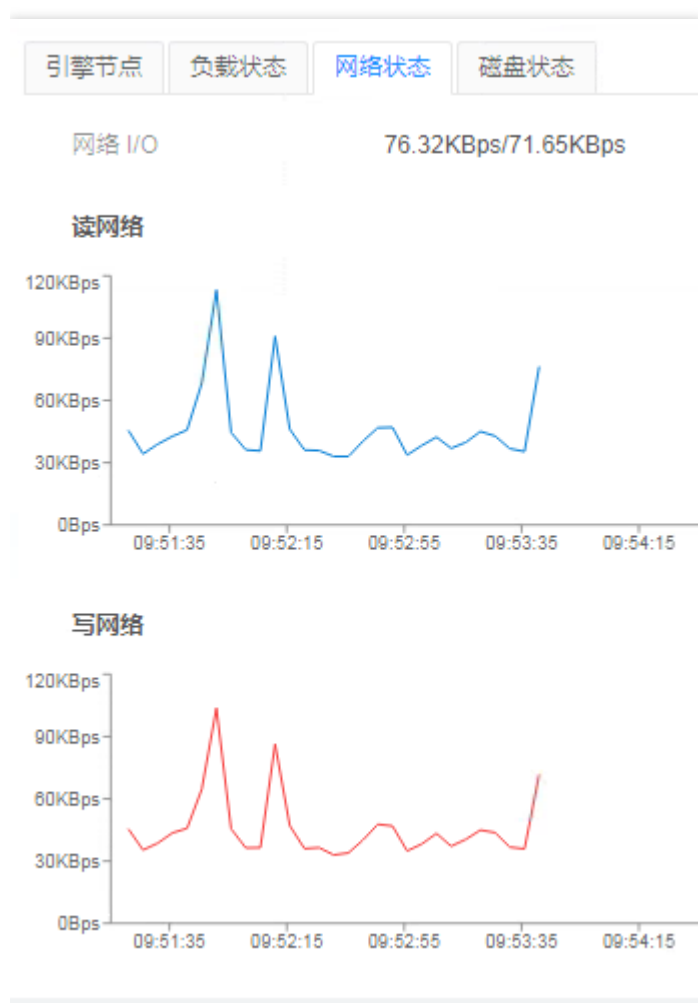
网络状态

磁盘状态

2、负载状态选项卡，展示管理节点CPU和内存资源使用情况；



3、网络状态选项卡，展示管理节点网络流量信息；





4、磁盘状态选项卡，展示管理节点磁盘情况；





常见问题

部署龙巡准备工作

最近更新时间: 2021-10-09 14:22:49

部署龙巡前首先确认内容：

1. 主账号是否存在VPC，若不存在VPC则不需要部署龙巡并且进行报备；
2. 确保主机CPU、内存、磁盘容量充足，1个VPC需要2C、4G、50G。
3. 部署龙巡需要使用主账号，建议先清除浏览器缓存后再进行部署。



漏洞扫描原理

最近更新时间: 2021-10-09 14:22:34

扫描设备会对扫描对象进行发包探测，根据响应情况得出扫描结果。主要包括了版本扫描和原理扫描两种类型。其中版本扫描根据扫描对象反馈的版本信息进行版本漏洞比对分析；原理扫描会模拟相关漏洞的利用方式，发包探测以确认是否存在漏洞。



扫描的影响

最近更新时间: 2021-10-09 14:22:34

两种扫描方式原则上都不会对扫描对象造成功能或性能上的影响，但是为确保生产稳定运行，务必在扫描前和扫描资产的管理员或项目组确认相关扫描信息。



扫描前确认信息

最近更新时间: 2021-10-09 14:22:34

创建扫描任务前务必要和扫描对象的系统（资产）管理员（运维人员）或项目组等相关负责人确认：可扫描时间、扫描服务器IP、扫描服务器是否存在端口转发情况。



扫描时间选择

最近更新时间: 2021-10-09 14:22:34

建议在非业务高峰时间段进行漏洞扫描，为保障业务稳定持续运行和降低不确定性因素的影响，原则上不在被扫描对象的变更窗口期内进行扫描。



什么是转发端口

最近更新时间: 2021-10-09 14:22:34

转发端口是指服务器可能安装了Nginx、Squid、Apache等服务并开启了端口转发模块，或部署其他具有转发功能的软件程序等，会将收到的请求包转发至其他服务器。假设某次扫描任务计划对A系统的服务器a进行扫描，但由于a存在转发端口，将来自漏洞扫描引擎的探测包转发至服务器b，服务器b可能属于某外部系统或外联单位的系统B，B在未收到报备或通知的情况下，会收到其相关安全产品的告警等，把扫描请求误判为攻击事件，进行引发封禁IP等其他可能的应急处置，从而造成无法预知的业务影响。



转发端口的处理

最近更新时间: 2021-10-09 14:22:34

1. 端口转发会导致扫描目标发生转移，造成无法预知的业务影响。扫描器无法感知扫描的对象是否有转发行为，从根本上避免此类情况发生，需要存在转发端口的服务器做好请求包过滤限制。对于扫描器的请求拒接转发（龙巡扫描引擎可配置UA或者referer字段，服务器可根据自定义的特征丢掉龙巡的扫描请求，从而避免无脑转发行为）
2. 短期内无法实现过滤的系统，在扫描前务必做好报备，确保被转发的系统或单位知晓扫描时间和扫描引擎IP，或暂时通过添加白名单的方式，不做扫描。



配置UA或添加Referer字段

最近更新时间: 2021-10-09 14:22:34

1. 对转发服务器进行Web扫描时，需要使用【基础Web漏洞扫描】策略。
2. 修改UA必须修改两个地方的配置 1) 在【信息收集参数】-【HTTP请求配置】中对User-Agent进行配置，如下图：

扫描管理 / 任务列表 / 添加扫描任务

添加扫描任务

基本信息 任务控制 信息收集参数 漏洞探测参数

HTTP 请求配置

* User-Agent

longxun

Cookie ⓘ

uid_example=12345; Finger=abc; session=ABC

> 高级选项

其他自定义 HTTP 请求头 ⓘ

+ 增加一个新的自定义 HTTP 请求头

HTTP 代理 ⓘ

http://1.2.3.4:1080/



扫描管理 / 任务列表 / 添加扫描任务

添加扫描任务

基本信息

任务控制

信息收集参数

漏洞探测参数

HTTP 请求配置

* User-Agent longxun

Cookie ② uid_example=12345; Finger=abc; session=ABC

> 高级选项

其他自定义 HTTP 请求头 ② + 增加一个新的自定义 HTTP 请求头

HTTP 代理 ② http://1.2.3.4:1080/

2) 并且在【漏洞探测参数】-【HTTP请求配置】中对User-Agent进行配置，如下图：

扫描管理 / 任务列表 / 添加扫描任务

添加扫描任务

基本信息

任务控制

信息收集参数

漏洞探测参数

HTTP 请求配置

* User-Agent longxun

Cookie ② uid_example=12345; Finger=abc; session=ABC

> 高级选项

其他自定义 HTTP 请求头 ② + 增加一个新的自定义 HTTP 请求头

HTTP 代理 ② http://1.2.3.4:1080/

3. 修改Referer字段也必须修改两个地方的配置：1) 在【信息收集参数】-【HTTP请求配置】中【增加一个新的自定义2) 并且在【漏洞探测参数】-【HTTP请求配置】中【增加一个新的自定义HTTP请求头】进行配置，如下图：



扫描管理 / 任务列表 / 添加扫描任务

添加扫描任务

- 基本信息
- 任务控制
- 信息收集参数
- 漏洞探测参数

HTTP 请求配置

* User-Agent longxun

Cookie ② uid_example=12345; Finger=abc; session=ABC

> 高级选项

其他自定义 HTTP 请求头 ②

referer

:

longxun

✖

+ 增加一个新的自定义 HTTP 请求头

HTTP 代理 ② http://1.2.3.4:1080/

2) 并且在【漏洞探测参数】 - 【HTTP请求配置】中【增加一个新的自定义HTTP请求头】进行配置，如下图：

扫描管理 / 任务列表 / 添加扫描任务

添加扫描任务

- 基本信息
- 任务控制
- 信息收集参数
- 漏洞探测参数

HTTP 请求配置

* User-Agent longxun

Cookie ② uid_example=12345; Finger=abc; session=ABC

> 高级选项

其他自定义 HTTP 请求头 ②

referer

:

longxun

✖

+ 增加一个新的自定义 HTTP 请求头

HTTP 代理 ② http://1.2.3.4:1080/



扫描特殊端口的配置

最近更新時間: 2021-10-09 14:22:34

如果被扫描目标存在转发端口等特殊端口时，需要和主机管理员再三确认除该端口外没有其他端口被用于转发等特殊服务后，想要检测该主机除特殊服务外是否存在其他漏洞时，使用【基础服务漏洞扫描】，在【信息收集参数】-【TCP协议扫描】-【端口列表】中将特殊服务的端口排除，即不要将特殊端口写入其中，例如80为转发服务使用端口，则不要将80端口写入其中，如下图所示：

TCP 协议扫描

启用

* 端口列表 ②

1-79,81-65535

+ 导入端口组

* 扫描方式 ②

SYN

* 扫描强度

快速探测

常规探测

精准探测

自定义探测

超时等待时长

1

秒

最小重试次数

2

次

最大重试次数

14

次



扫描出现告警如何处理

最近更新时间: 2021-10-09 14:22:34

如果前期信息确认充分，对可能引发异常的端口或软件等信息及时有效同步，在扫描过程中基本不会出现因扫描引发的告警。若出现异常告警，请立刻停止扫描或联系87815199-9-27886提供技术支持。