云网安全运营中心
用户手册

目 录

1. 概述

1.1 初次使用说明

本文档可以帮助用户了解云网安全运营中心的主要功能和操作方式。在进行任何管理操作之前请确认已经获得操作权限。

在初次登录的时候，请使用缺省用户（root）和密码登录。

文档的具体结构如下：

1） 系统概述。介绍系统整体结构和程序的启动。

2） 业务流程配置。介绍业务流程的基本配置过程，如何快速的配置并使用本系统。

3） 资产管理功能。

4） 风险分析功能。介绍如何对事件分类规则、关联规则、防火墙设置以及预警响应策略进行配置。

5） 安全响应管理功能。介绍如何进行工单配置及处理。

6） 安全报表功能。介绍如何查看相关的报表信息。

7） 知识库功能。介绍如何管理知识库体系及其内容。

8） 系统配置功能。介绍系统各项其他配置与性能监控。

1.2 系统简介

云网安全运营中心主要分为采集层、后端分析层和前端展示层三大部分。

采集层：主要负责收集各类安全日志事件以及安全配置信息，并对这些信息进行预处理然后发送给后端分析层。

后端分析层：主要负责将采集层传送过来的各种安全事件与配置信息进行归类和关联分析，并将分析结果存储到数据库中。

前端展示层：主要负责将后端分析层分析出来的结果数据展现给用户，并提供丰富的报表供用户使用。同时也提供各种形式的操作配置，以及数据存储模式的配置使用户能更方便的使用本系统。

1.3 系统访问

云网安全运营中心是基于 B/S（Browser/Server）架构，采用 Web 作为用户

界面，用户可使用浏览器进行访问。

系统访问过程如下：

1）打开浏览器，在地址栏中输入 https://服务器 IP 地址/index.html，由于采用 SSL 技术，首次访问会出现证书错误提示，如图：1-1 所示

https://172.168.68.32 /index.html

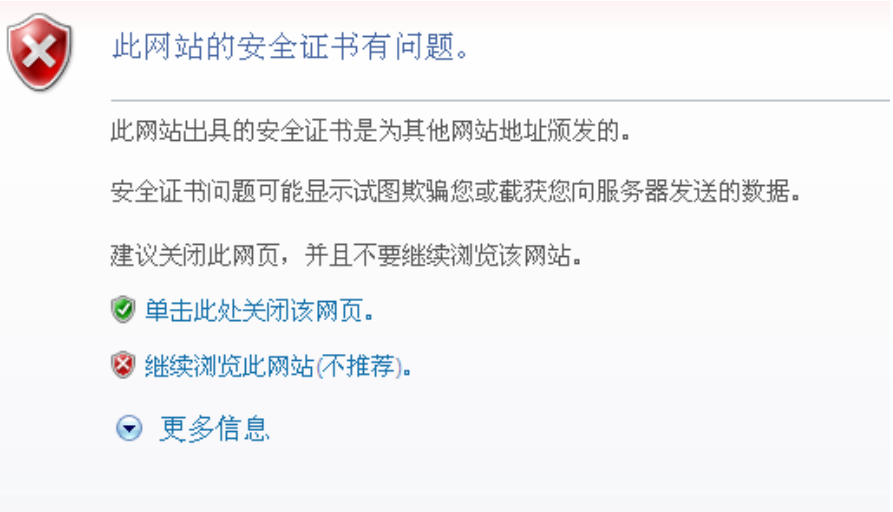


图 1-1 证书提示页面

2）此时点击“继续浏览此网站”，将出现登录页面，如图：1-2 所示

图1-2登录页

3）云网安全运营中心使用 root 账户作为默认账户，输入用户名、密码和验

证码后点击“登录”按钮即可登录。（root/123456）

2. 业务流程配置

云网安全运营中心的主要功能包括事件分析与告警、脆弱性检查与监控、安全维护作业制定与执行。要完成上述功能，用户需要对系统进行一系列的配置操作，为了方便用户使用，下面我们对这些配置操作进行详细说明。

2.1 系统配置

要收集各种设备的日志进行事件分析，首先需要完成一系列的配置，具体的事件采集配置流程如下图所示：

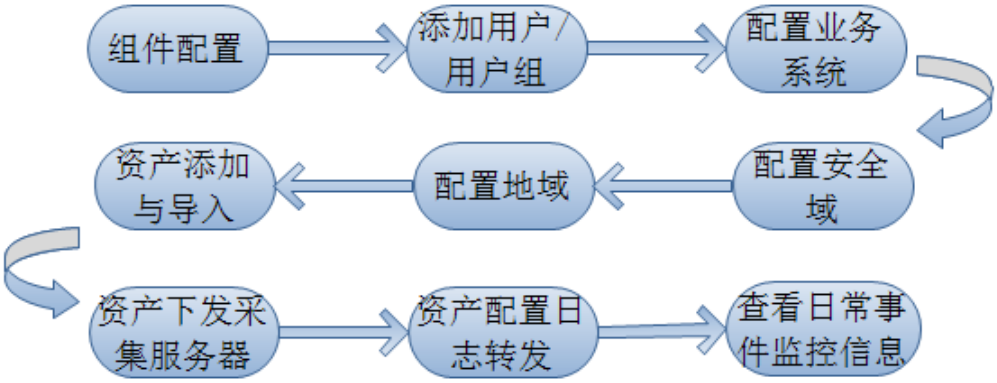


图 2-1 事件采集配置流程图

2.1.1 IP 管理

IP 管理功能用于 ip 地址库管理。

通过点击“系统配置”=>“IP 管理”，显示 IP 管理配置页面，如图：

- 点击“新增”按钮，弹出 IP 管理新增页面，*号标识为必填属性，填完

后点击“提交”按钮保存。

- 点击”导入”按钮，弹出 ip 信息导入界面，如图：

（1）点击”下载导入文件模板”，可下载 ip 导入模板，模板填写信息与 web 新增页面属性一致，如图：

（2）点击”选取文件”，在指定路径找到刚填好保存的 ip 导入模板，点击”提交”按钮，提示导入成功，点击”关闭”按钮，则 ip 未导入。

- 用户可通过在查询条件区域输入关键字，点击 查询 按钮，筛选查询结果，默认显示 4 个查询条件，点击 展开 按钮，可查看更多条件，或收起查询条件；点击 重置 按钮，可清空查询条件内容，并自动加载列表结果。

2.1.2 组件管理

组件配置主要完成云网安全运营中心自身组件服务器的配置，具体包括采集服务器、核心服务器、代理类型服务器、数据库服务器、私网远程评估代理服务器、告警服务器。

通过点击“系统配置”=>“组件管理”，显示组件服务器配置页面，如图 2-2

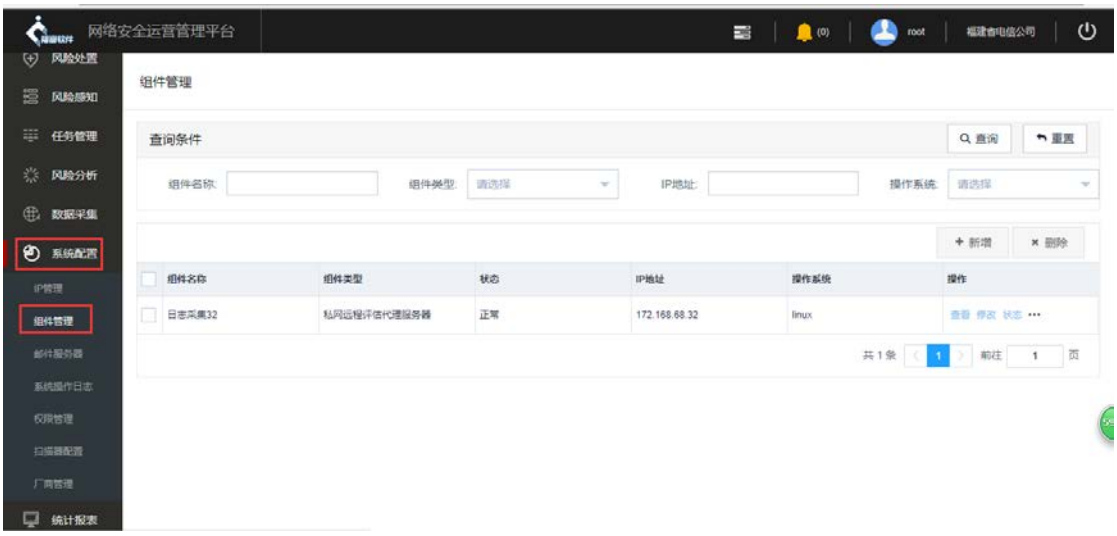


图 2-2 组件服务器配置

- 点击“新增”按钮，弹出组件新增界面，*号标识为必填，如图：

其中：

（1）组件名称：添加的组件服务器的名称。

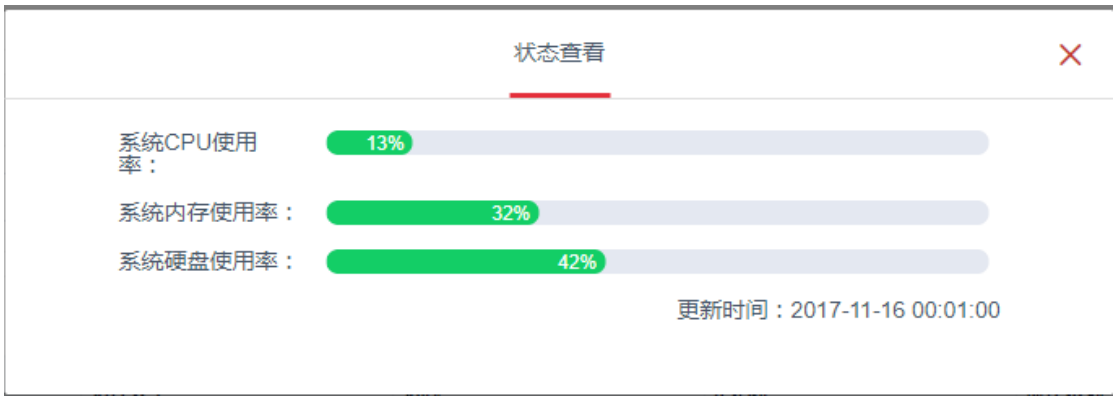
（2）组件类型：在下拉框中选择，其中采集服务器指的是本平台运行采集服务的组件，代理类型服务器指的是本平台运行采集代理服务的组件，核心服务器指的是本平台运行核心分析服务的组件。

（3）IP 地址：添加的组件服务器的 IP。

（4）操作系统：选择组件服务器操作系统类型。

填写完后点击“提交”即可。

- 用户可通过点击“查看”“修改”“删除”按钮，查看组件信息、修改组件信息、删除组件信息；
- 选中一条组件记录，点击”状态”按钮，可查看该组件服务器的状态信息，如图：



- 用户可通过查询条件区域输入条件，点击 

按钮，筛选组件服

务器，默认显示 4 个查询条件，点击 展开 按钮，可查看更多条件，或收起查询条件；点击 重置 按钮，可清空查询条件内容，并自动加载列表结果。

2.1.3 邮件服务器

- 点击”系统配置”=>”邮件服务器”菜单，显示邮件设置页面，如图：

- 点击”编辑”按钮，可设置邮件服务器信息，其中

SMTP 服务器地址：配一个邮件服务器地址。

邮件发件人地址：即配置的邮件服务器上的一个邮箱。

邮件发送帐号密码：即邮件发件人的邮箱密码。

设置完后点击 保存 按钮即可，成功的话就提示成功，失败就提示失败。点击 取消 按钮，则编辑信息未保存。

2.1.4 系统操作日志

- 点击”系统配置”=>“系统操作日志”，可查看用户操作日志，主要记录用户对系统各个模块的操作记录，如图：

- 用户可通过在查询条件区域输入关键字，点击 

按钮，筛选查询结果，默认显示 4 个查询条件，点击 

按钮，可查看更多条件，或收起查询条件；点击 

按钮，可清空查询条件内容，并自动加载列表结果。

2.1.5 扫描器配置

- 点击”系统配置”=>”扫描器配置”，显示扫描器配置界面，如图：

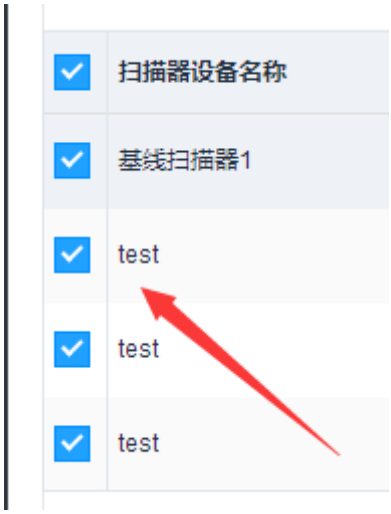
- 点击”新增”按钮，弹出扫描器新增界面，*号标识为必填属性，如图：

(1) 其中，用户名、密码属性只有设备类型为”Nessus 漏扫”时需要必填，选择其他设备类型，该属性为非必填属性；

（2）若”是否支持导入”选择是，则说明该扫描器支持策略导入，在操作栏鼠标移入悬浮标点，显示”策略导入”按钮；若选择“否”，则没有策略导入按钮，如图：

- 通过点击“查看”、“修改”、“删除”按钮，用户可查看扫描器具体属性、修改扫描器属性、删除扫描器信息；
- 勾选复选框，点击右上角  按钮，可批量删除扫描器信息，只

能批量删除当前页数据。



2.1.6 权限管理

2.1.6.1 用户管理

- 点击“系统配置”=>“权限管理”=>”用户管理”，进入用户管理配置页面，默认展示所有 soc 用户，如图：

- **添加用户**

点击“新增”按钮，弹出用户添加界面，根据页面提示填写相应的信息，*号标识的为必填属性，其中：

用户类型：选择 SOC 用户或非 SOC 用户；

用户名称：可选填，要求只能以中文开头，（长度 2-12 位）

登录名：只支持数字、字符、下划线、横杠（长度 2-12 位）

密码、确认密码：必须由字母、字符和数字任意两种类型八位个数以上组合，支持特殊字符，不支持空格；

固定电话：要求使用区号-号码格式；

角色：该用户拥有该角色的权限；

填写完信息，点击 提交 按钮，即可保存用户信息成功，若填写格式非法，则弹出错误提示；点击 重置 按钮，所填用户信息被清空，如图：

- **用户密码修改**

点击 密码修改 按钮，弹出密码修改页面，用户输入新密码，即可修改密码，如图：

- **用户授权**

点击 授权 按钮，弹出用户授权界面，角色下拉框显示所有当前登录用户所属角色包含的所有可授出角色，可为用户配置角色，并支持多角色授权，如图：

- **用户锁定/解锁**

（1）选择一个用户状态正常的用户，点击 锁定 按钮，弹出锁定用户确认弹窗，点击确定，则用户被锁定，无法登陆 SOC 平台；

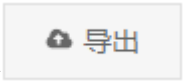
（2）选择一个锁定状态的用户，点击 解锁 按扭，弹出解锁用户

确认弹窗，点击确定，则用户被解锁，用户可重新登陆 SOC 平台；

- **用户导入/导出**

（1）点击 

按钮，弹出导入界面，点击“下载导入文件模板”，可下载模板，模板内容与 web 页面新增用户属性一致，根据提示填写信息，保存模板；点击“选取文件”按钮，选择刚保存的模板文件，点击“提交”按钮，信息填写正确，则提示导入成功，若信息填写非法，则导入失败，页面弹窗提示错误日志；点击“关闭”按钮，则关闭导入界面，如图：

（2）点击 

按钮，默认导出全部 SOC 用户，用户可根据查询条件、勾选导出指定用户数据。

- **用户查询**

用户可通过在查询条件区域输入关键字，点击 

按钮，筛选查询结果，默认显示 4 个查询条件，点击 

按钮，可查看更多条件，或收起查询条件；点击 

按钮，可清空查询条件内容，并

自动加载列表结果。

2.1.6.2 角色管理

- 点击“系统配置”=>“权限管理”=>”角色管理”，进入角色配置页面，如图：

- 角色新增、修改、删除

点击  按钮，根据提示输入信息，如图：

角色编码：只支持数字、字母、下划线，（长度 3-16 位）；

可授出角色：选择拥有该角色的用户可授出的角色，且用户只能分配这些可授出角色权限的并集；

在左侧角色列表，选择一个角色，点击 

按钮，可修改、删除角色；

- 按钮权限

在左侧角色列表，选择一个角色，点击 

，弹出按钮权限配置界面，默认用户没有所有按钮权限，如图：

- 菜单权限

在左侧角色列表，选择一个角色，点击 

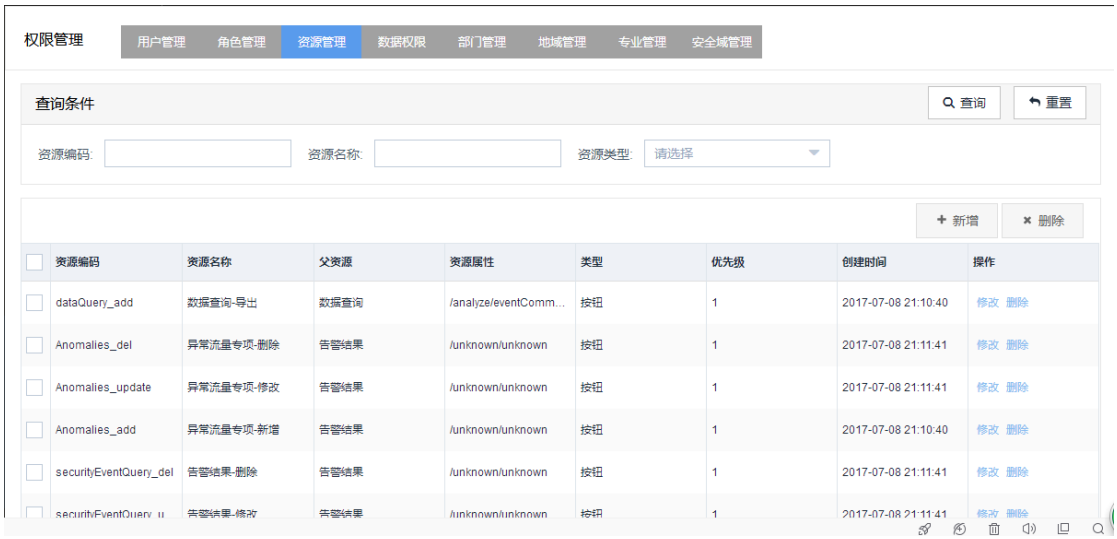
，弹出菜单权限配置界面，默认用户没有所有菜单权限，如图：

- 数据权限

在左侧角色列表，选择一个角色，点击 数据权限 ，弹出数据权限配置界面，默认用户没有所有数据权限，如图：

2.1.6.3 资源管理

- 点击“系统配置”=>“权限管理”=>”资源管理”，进入资源管理配置页面，可配置按钮、菜单、组件资源，如图：



- 点击“新增”按钮，弹出新增资源界面，*号标识为必填项，如图：

资源编码：必填，任意字符；

资源名称：根据实际输入名称；

资源类型：菜单、按钮、组件类型；

父资源：资源所在位置；

资源属性：需正确填写，否则无效，访问该资源的链接属性，可找开发提供；

填写完成，点击提交即可。

2.1.6.4 数据权限

- 点击“系统配置”=>“权限管理”=>”数据权限”，进入数据权限配置页面，如图：

- 点击“新增”按钮，弹出数据权限新增界面，*号标识为必填项，如图：

权限类型：下拉框选择要添加的数据权限类型；

权限编码：根据选择的权限类型自动关联，不可编辑；

规则名称：其中表别名需正确填写，否则规则未生效，可找开发提供；

点击提交按钮即可。

2.1.6.5 部门管理

- 点击“系统配置”=>“权限管理”=>”部门管理”，进入部门管理配置页面，用户可修改、删除部门配置，如图：

2.1.6.6 地域管理

- 点击“系统配置”=>“权限管理”=>”地域管理”，进入地域管理配置页面，用户可修改、删除地域配置，如图：

2.1.6.7 专业管理

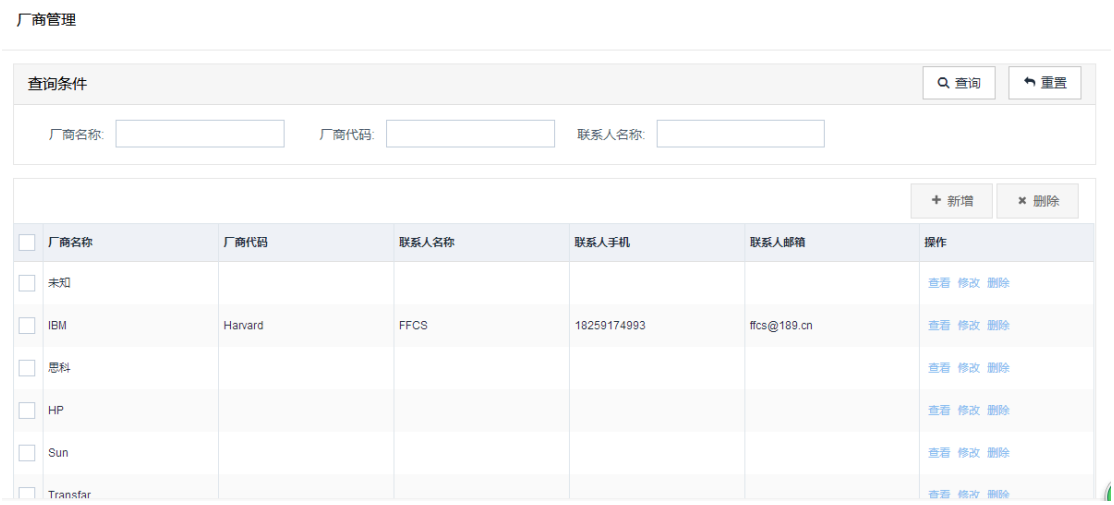
- 点击“系统配置”=>“权限管理”=>”专业管理”，进入专业管理配置页面，用户可修改、删除专业配置，如图：

2.1.6.8 安全域管理

- 点击“系统配置”=>“权限管理”=>”安全域管理”，进入安全域管理配置页面，用户可修改、删除安全域配置，如图：

2.1.7 厂商管理

- 点击”系统配置”=>”厂商管理“菜单，显示厂商管理配置页面，如图：



- 点击“新增”按钮，弹出厂商新增界面，*号标识为必填属性，如图：

信息填写完后点击”提交”即可。

- 点击“查看”、“修改”、“删除”按钮，用户可查看厂商属性信息、修改厂商属性、删除厂商；

- 通过勾选勾选框，点击右上角批量删除按钮 

，用户可批量删除当前页面数据。

2.2 统计报表

点击系统上方菜单项的“安全报表”，进入报表管理模块，如图 6-1：

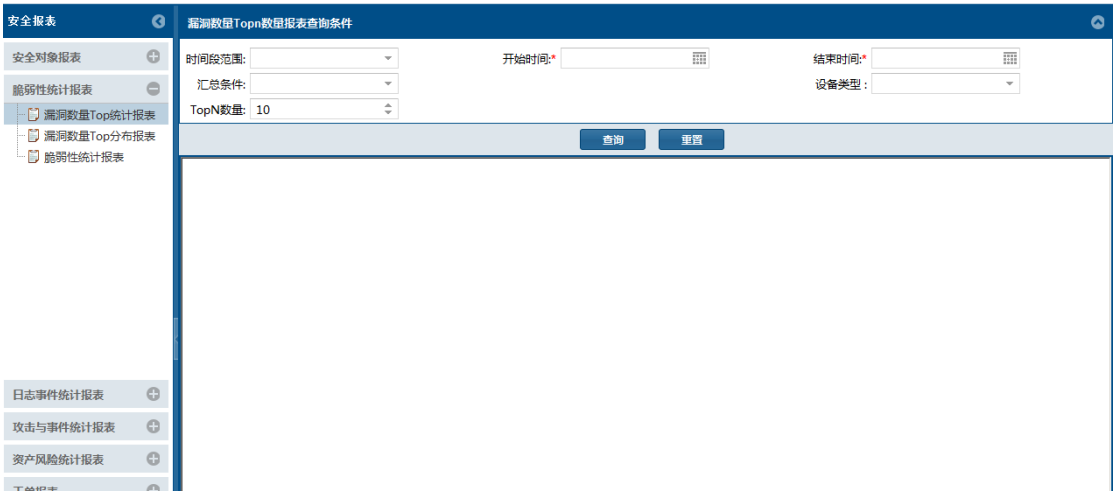


图 6-1 报表管理

报表管理分为：

- 安全对象报表

安全对象变化趋势报表

安全对象 TOPN 数量报表

安全对象详细信息报表

- 脆弱性统计报表

  漏洞数量 Top 统计报表

  漏洞数量 Top 分布报表

  脆弱性统计报表

- 日志事件统计报表

  设备事件报表

  事件分组统计统计

- 攻击与事件统计报表

  攻击来源 TopN 统计报表

  攻击目标 TopN 统计报表

  安全攻击与异常事件统计报表

  资产威胁数量变化趋势统计报表

- 资产风险统计报表

  风险值变化趋势报表

  风险等级变化趋势报表

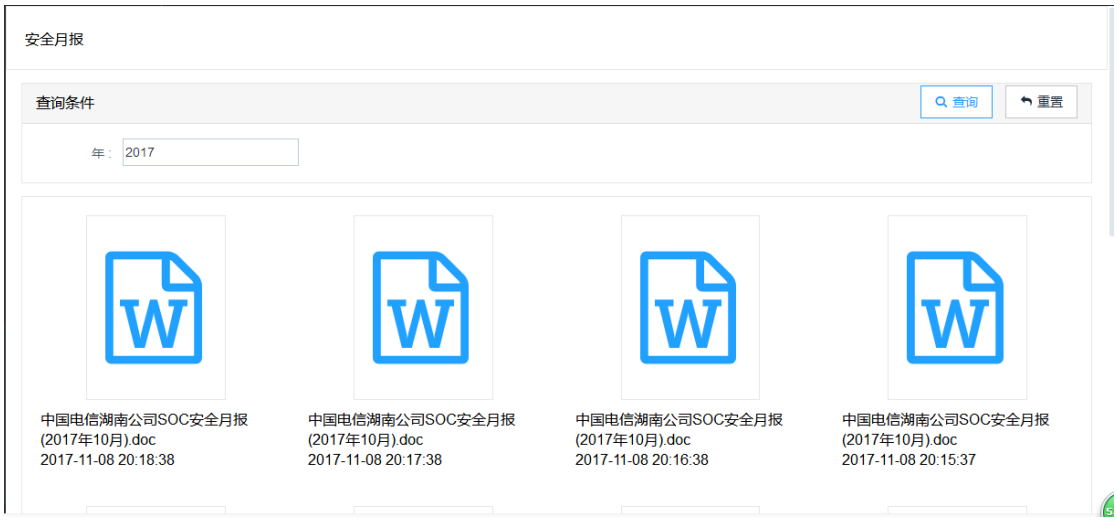
- 配置脆弱性报表

  配置脆弱性数量 TOPN 统计报表

  配置脆弱性类型数量变化趋势报表

2.2.1 安全月报

- 点击”统计报表”=>“安全月报”，进入安全月报查看页面，如图：

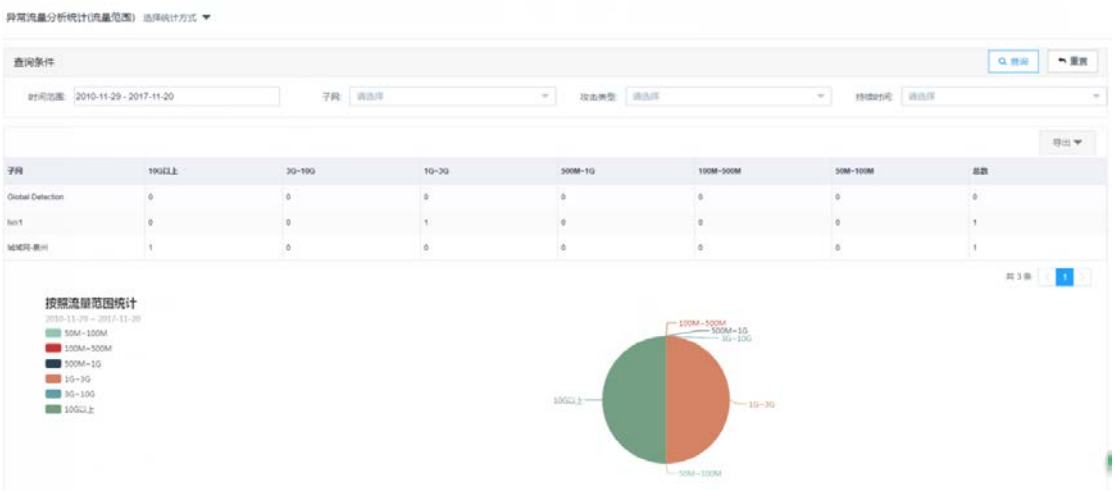


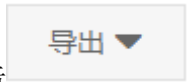
- 鼠标点击 word 文件，可下载月报；

2.2.2 异常流量分析报表

2.2.2.1 流量范围统计

- 点击“统计报表”=>“异常流量分析报表”，默认展示按流量范围统计数据，如图：

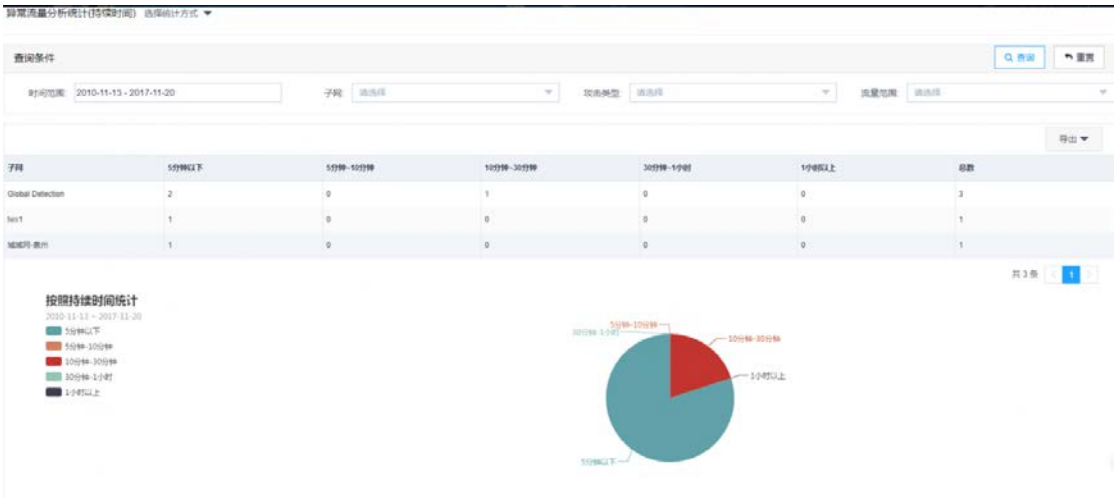


- 点击 

按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.2.2 持续时间分类统计

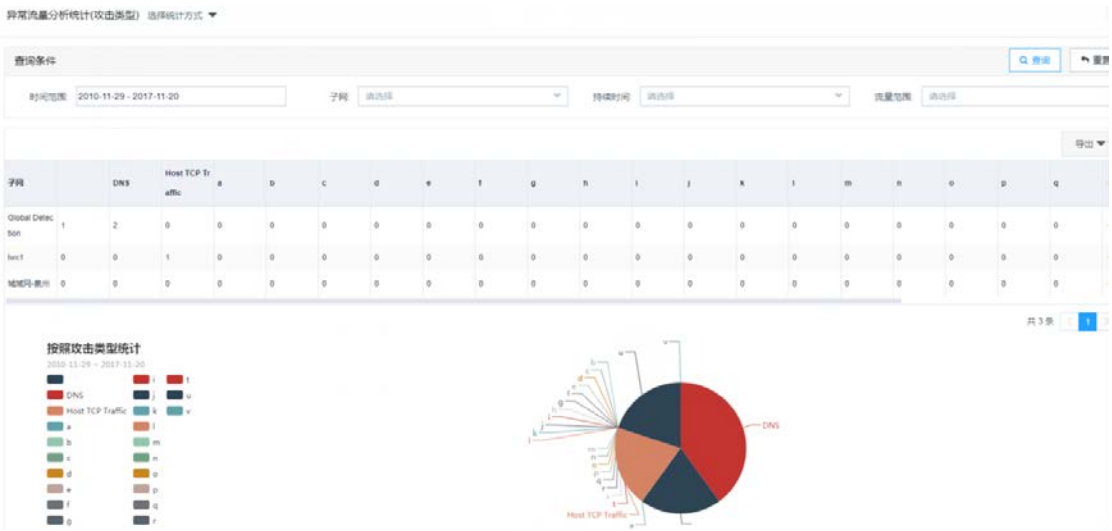
- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“持续时间”，如图：

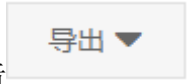


- 点击  按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.2.3 攻击类型分类统计

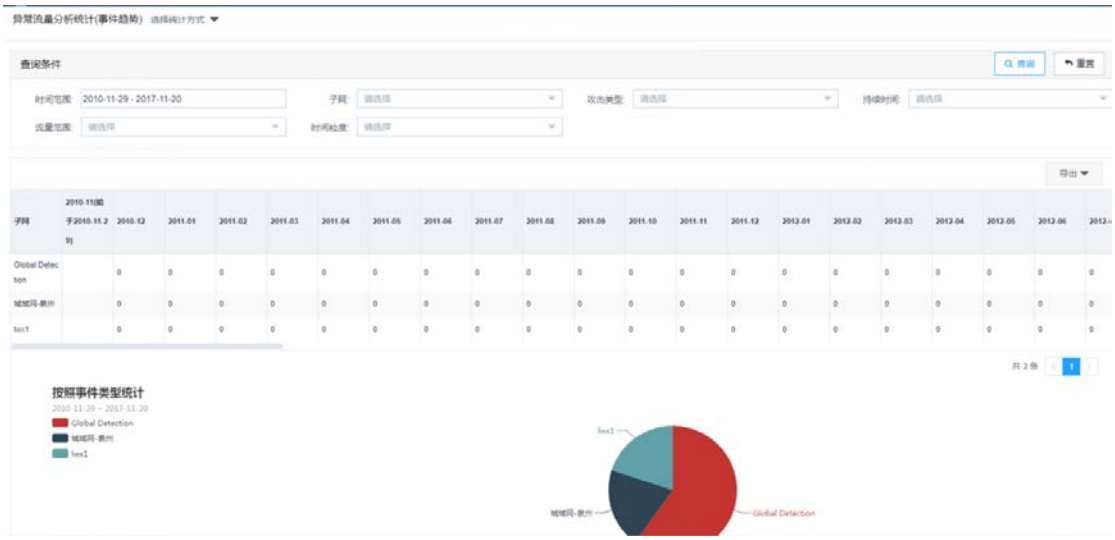
- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“攻击类型”，如图：



- 点击  按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.2.4 事件趋势统计

- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“事件趋势”，如图：

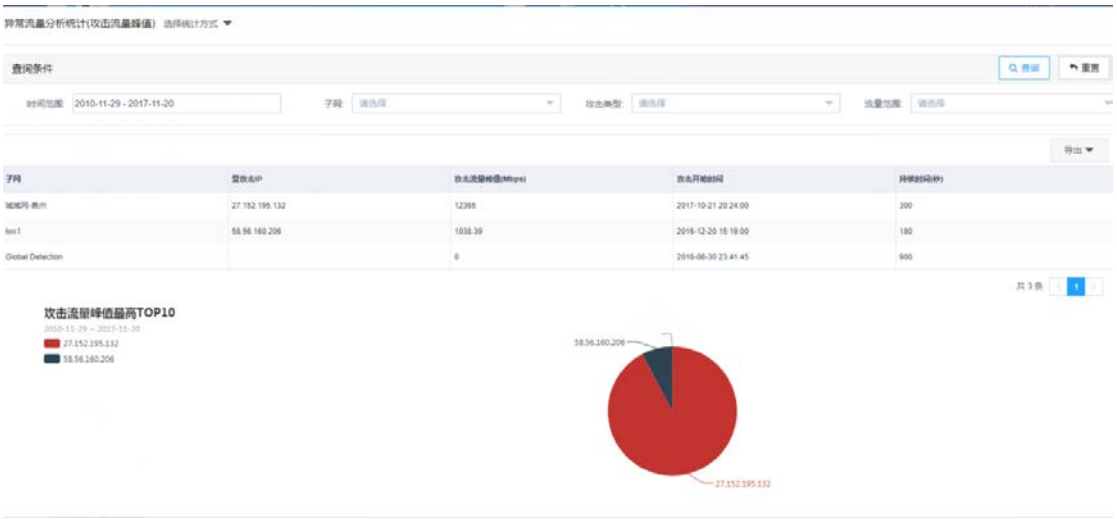


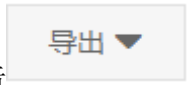
- 点击 

按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.2.5 攻击流量峰值

- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“攻击流量峰值”，如图：

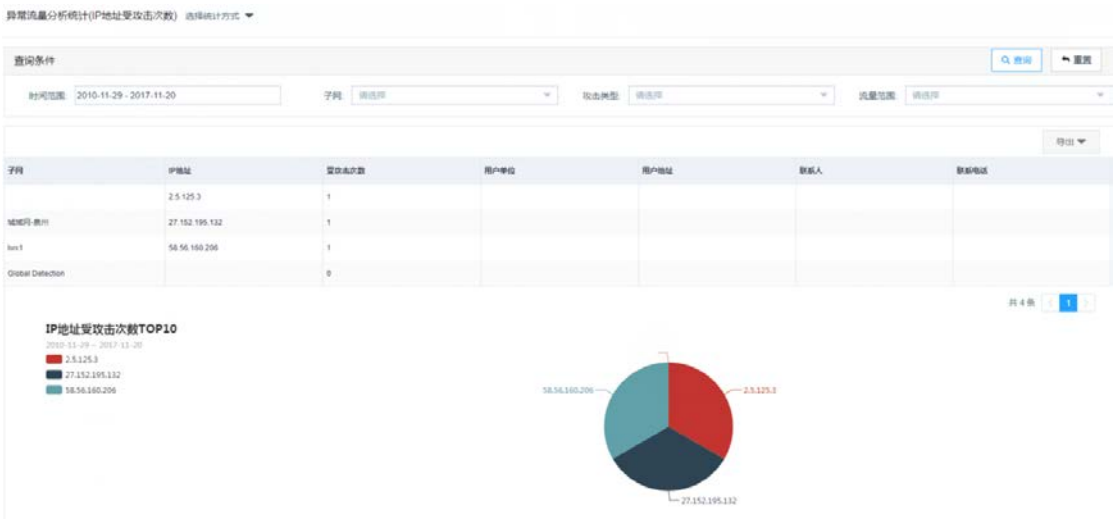


- 点击 

按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.2.6 IP 地址受攻击次数

- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“IP 地址受攻击次数”，如图：



- 点击  按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.3 漏洞统计报表

2.2.3.1 漏洞数量统计

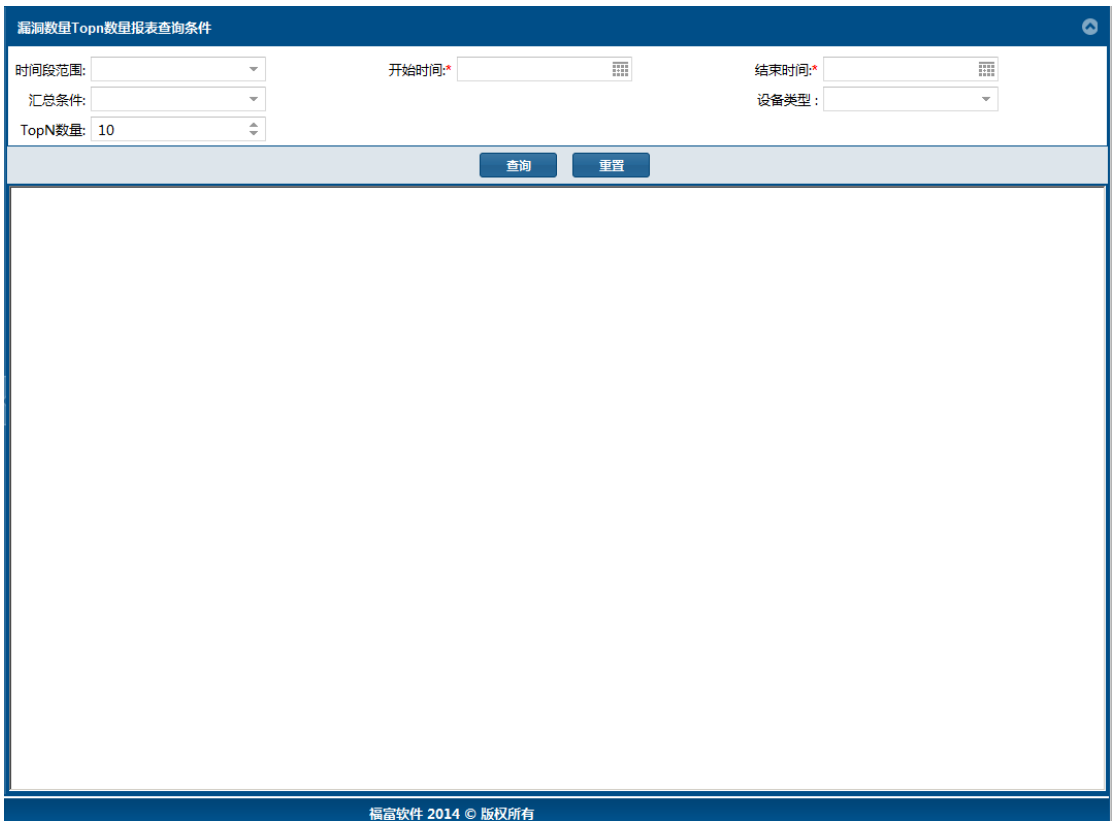


图6-9漏洞数量TOP统计报表选择

- 输入条件信息

  时间范围、汇总条件请参考 6.1.1

- 报表展示

选择好条件后点击图 6-9 

图标就会把报表显示出来，如图：6-10

图 6-10 漏洞数量Top统计报表

其它操作如导出报表等请参考 6.1.1 操作步骤。

2.2.3.2 弱口令应用类型统计

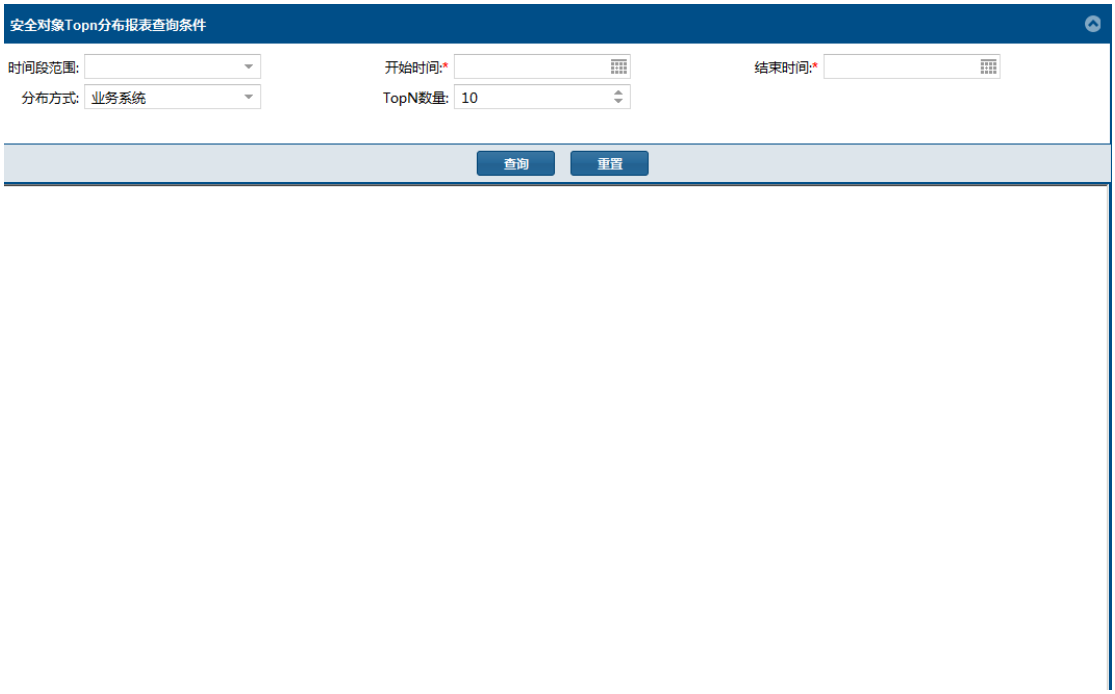
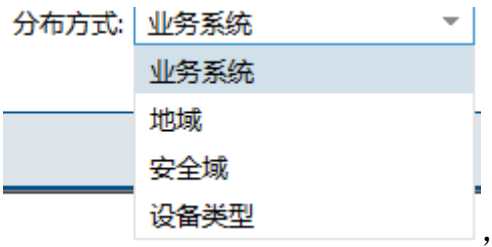


图 6-11 漏洞数量 TOP 分布报表选择

- 输入条件信息

  时间范围请参考 6.1.1

  分布方式： 

，选择希望的分布方式。

- 报表展示

选择好条件后点击图 6-11 

图标就会把报表显示出来，如图：6-12

图 6-12 漏洞数量 Top 分布报表

其它操作如导出报表等请参考 6.1.1 操作步骤。

2.2.3.3 漏洞应用类型数量统计

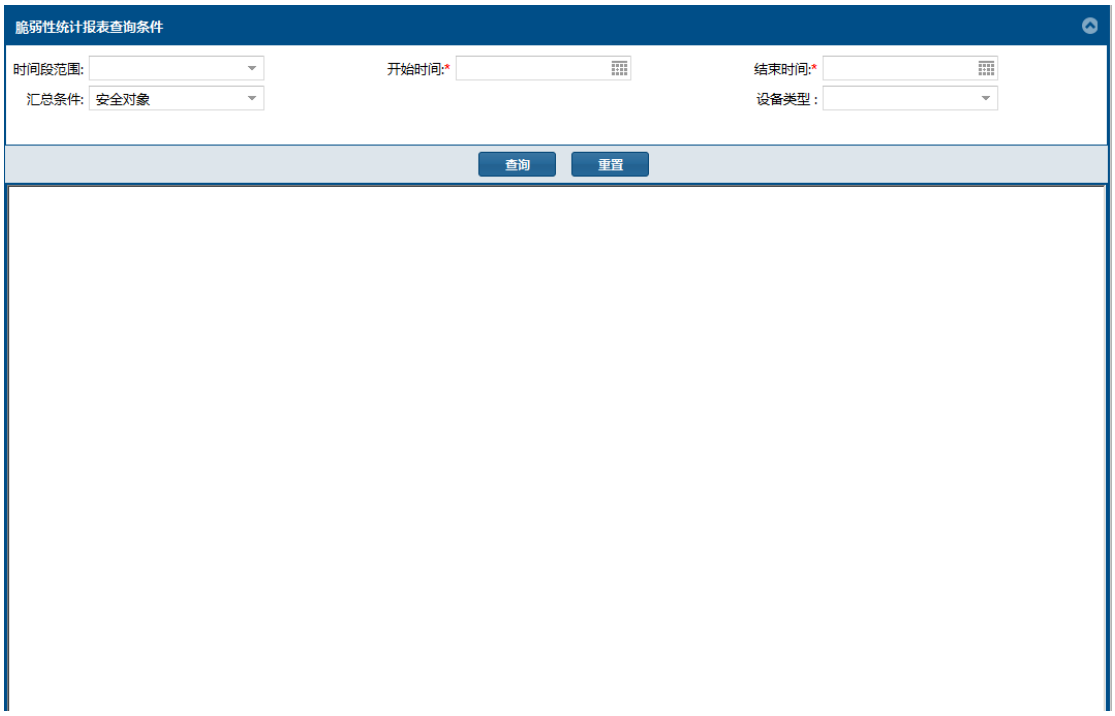


图 6-15 脆弱性统计报表选择

- 输入条件信息

  时间范围、汇总条件请参考 6.1.1 的步骤描述

- 报表展示

选择好条件后点击图 6-15 

图标就会把报表显示出来，如图：6-16

图 6-16 脆弱性统计报表

其它操作如导出报表等请参考 6.1.1 操作步骤。

2.2.4 资产统计报表

2.2.4.1 资产维度统计

2.2.4.2 Agent 维度统计

2.2.4.3 未知资产维度统计

2.2.5 漏洞处置报表

2.3 资产管理

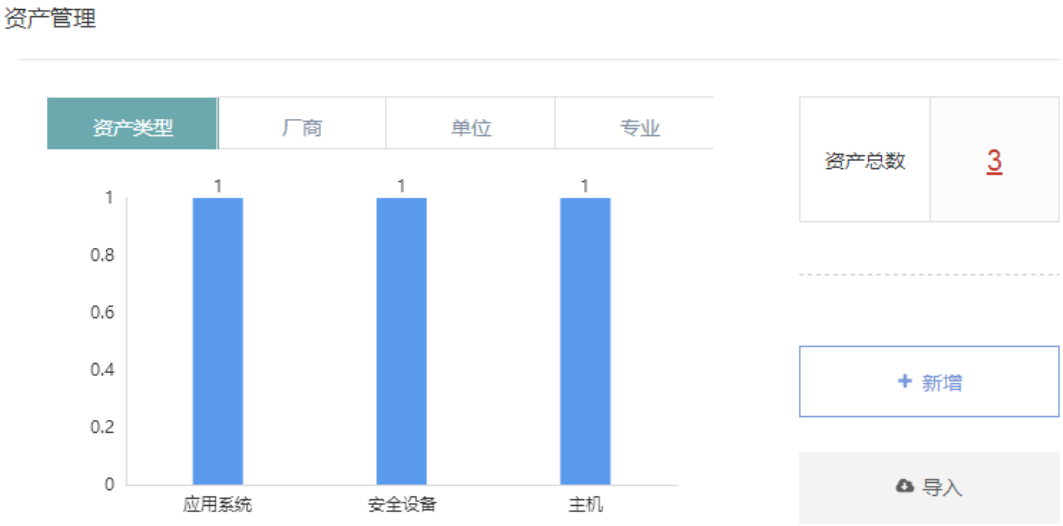
2.3.1 资产管理首页

用户登录后默认跳转至资产首页，或鼠标点击左侧一级菜单“资产管理”，进入资产首页。如图：

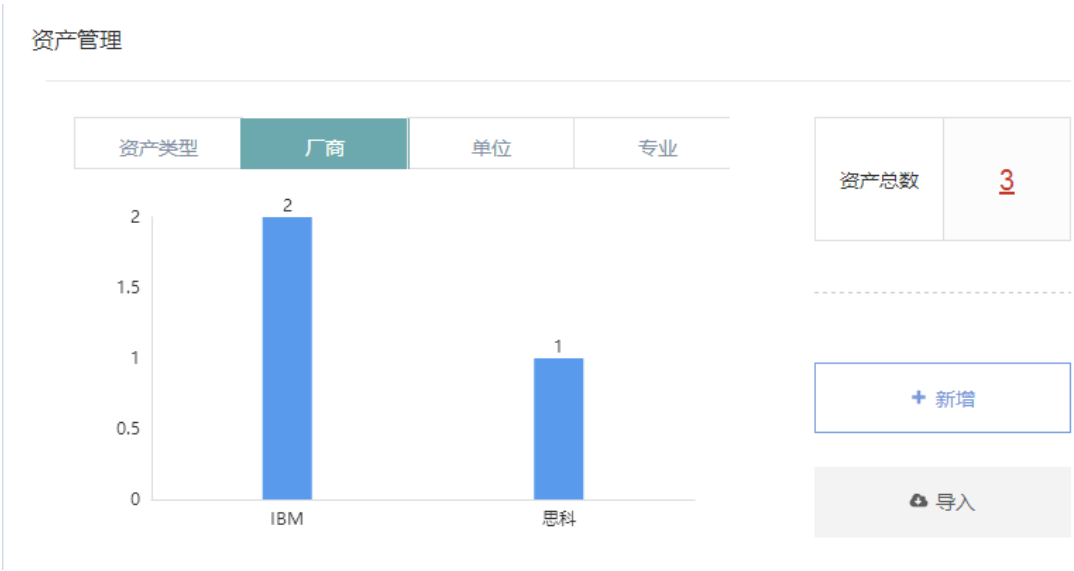
- **资产模块**

  左侧按不同维度展示资产柱形图，鼠标点击柱形图可下钻至资产详情页面；右侧统计资产总数，并提供资产新增、导入入口。

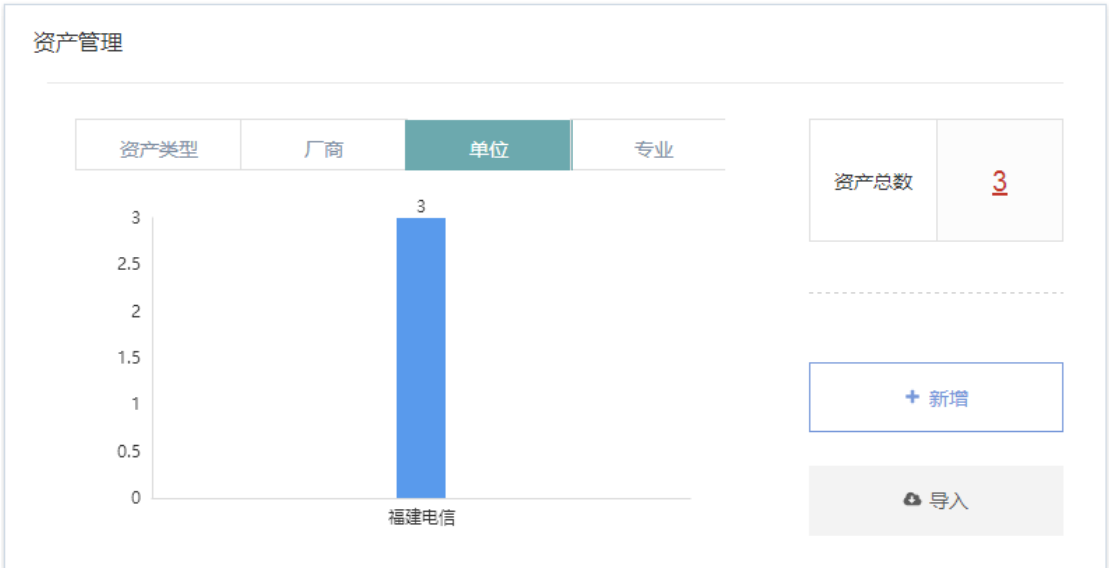
  （1）按资产类型维度统计，如图：



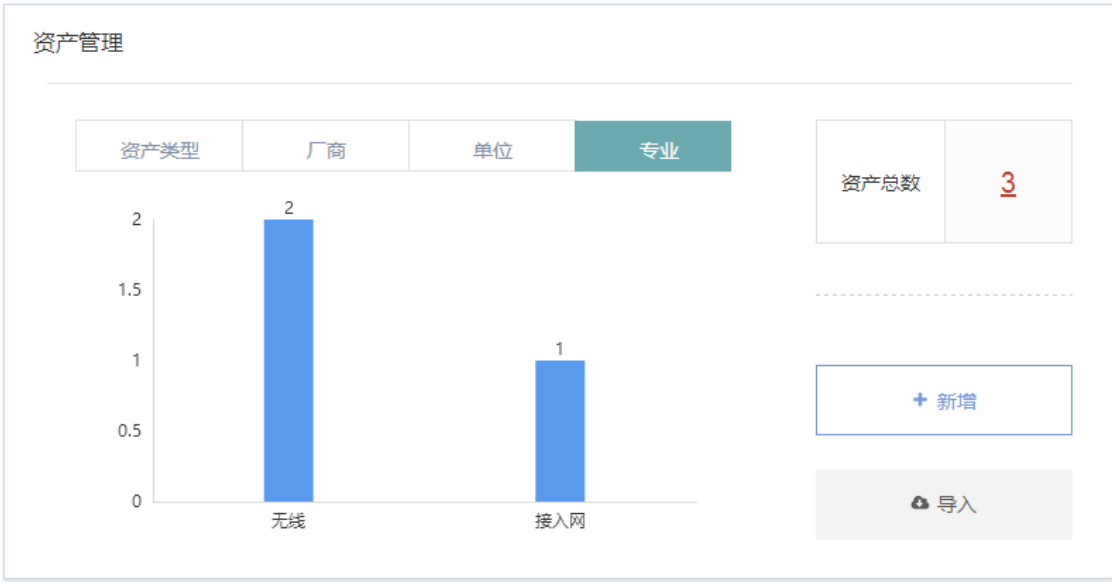
（2）按资产厂商维度统计，如图：



（3）按单位维度统计，如图：



（4）按专业维度统计，如图：



（4）点击  ，页面跳转至资产详情界面；

（5）点击  按钮，弹出资产新增界面；

（6）点击  按钮，弹出资产导入界面；

- **未知资产模块**

列表展示未知资产名称、节点状态，点击未知资产总数，页面跳转至未

知资产详情页面，点击 待处理 按钮，跳转至处理界面。

- **业务系统模块**

  按资产维度展示 TOP5 业务系统，按资产数量降序排列，展示字段为“业务系统名称”、“业务系统定级等级”、“资产数量”，如图：

- **资产发现模块**

按任务创建时间展示最新 5 条离线任务，点击“离线导入”跳转至结果文件导入界面。

- **WEB 资产模块**

按业务系统维度展示 TOP5web 资产，如图：

- **主机代理下载**

点击 

按钮，弹出主机代理下载界面，如图：

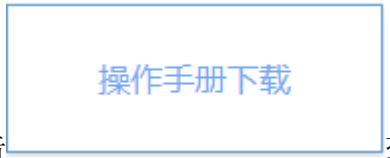
（1）置灰属性通过业务系统自动关联，不可编辑；

（2）前置机地址：中转服务器 IP；

点击 

按钮，进入 agent 版本下载页面，鼠标点击某个版本即可下载。

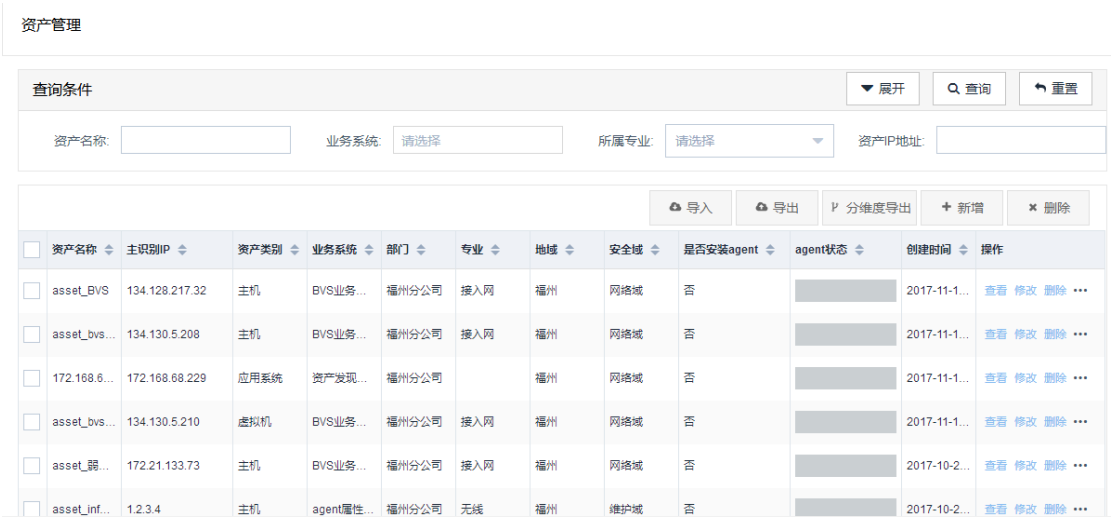
- **操作手册下载**



点击操作手册下载按钮，下载 agent 操作手册。

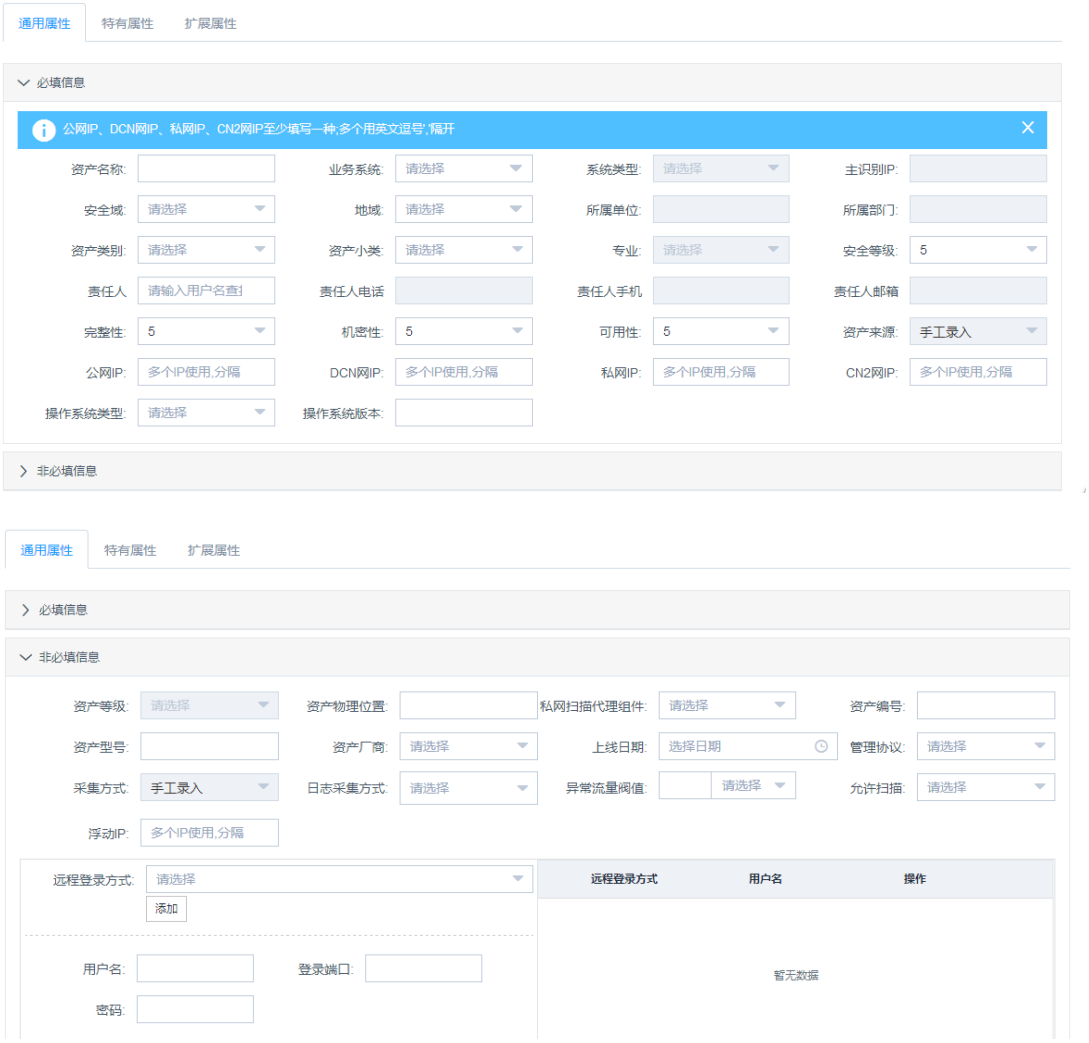
2.3.2 资产管理

- 点击”资产管理”,进入资产管理配置界面,如图:



- **资产添加**

点击”新增”按钮,弹出新增资产界面,包含通用属性（必填属性、非必填属性）、特有属性、扩展属性（前端可配置），如图：



（1）系统类型、所属单位、所属部门、专业、责任人、责任人电话、责任人手机、责任人邮箱通过业务系统自动关联，责任人支持修改，其余属性置灰不可编辑；

（2）公网 IP、DCN 网 IP、私网 IP、CN2 网 IP 至少填写一种类型，多个 ip 用“，”隔开；主识别 ip 根据五种 IP 类型优先级自动关联，公网 IP>DCN 网 IP>私网 IP>CN2 网 IP>浮动 IP，不可编辑

（3）安全等级、完整性、机密性、可用性默认显示 5，可修改；

（4）资产等级根据业务系统自动关联，为业务系统定级等级；

（5）特有属性：根据选择的资产类别显示对应的资产特有属性；

（6）扩展属性：前端可配置，用户可自行增删改属性值；

属性填写完后，点击“提交”按钮，填写合法则提示提交成功，若填写不合法，则弹窗错误提示；

- **资产变更历史**

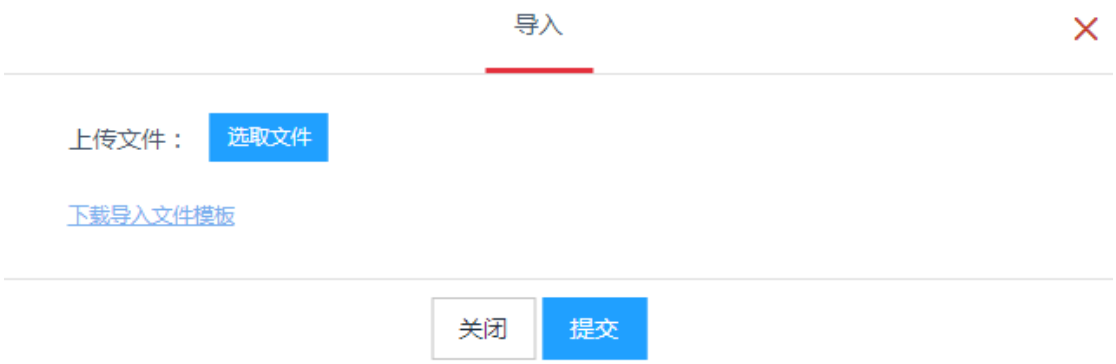
选择一条资产，点击 

按钮，进入资产变更历史查看界面，用户可查看资产的变更情况，如图：

- **资产异步导入/导出**

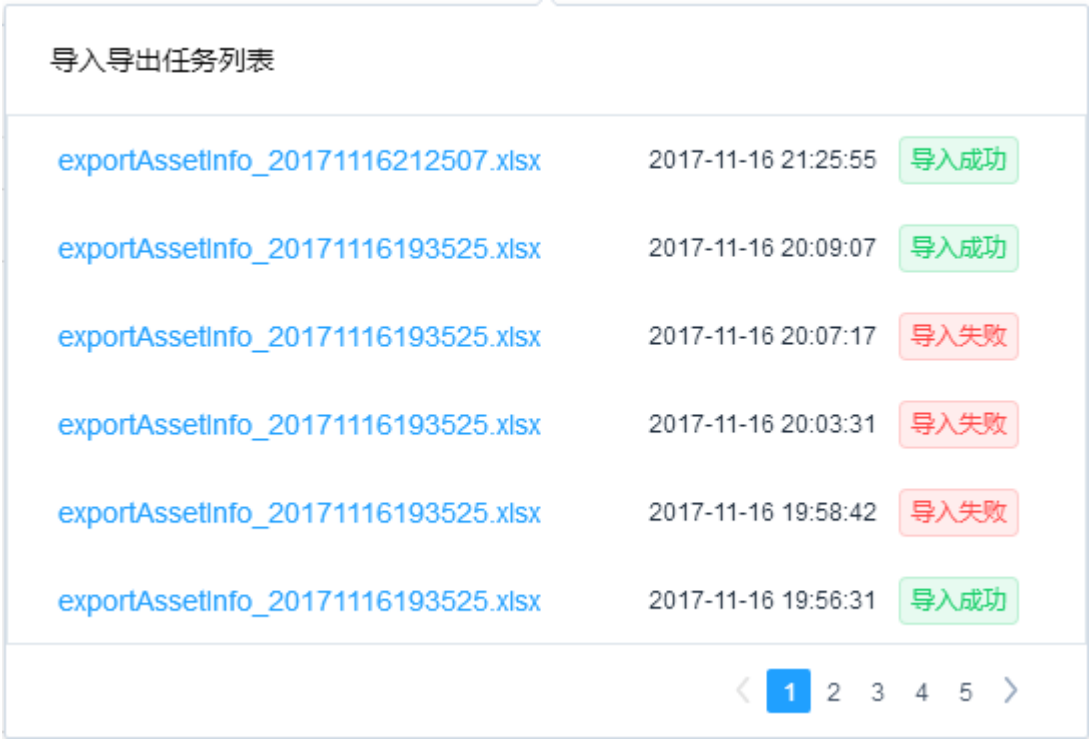
（1）点击 

按钮，弹出资产导入界面，如图：



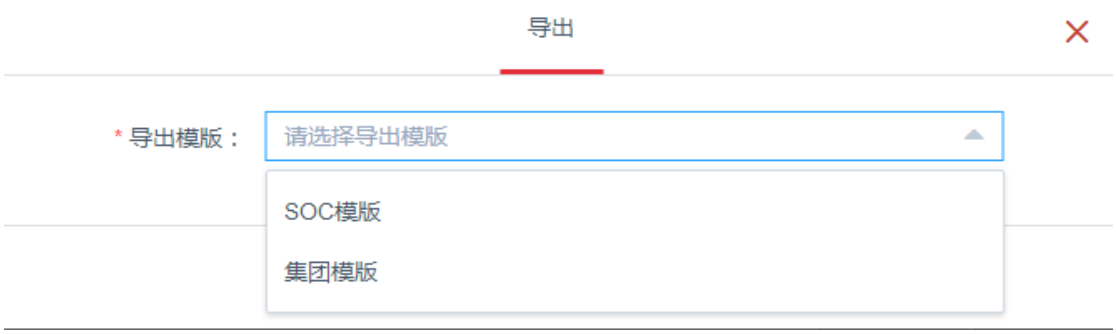
点击“下载导入文件模板”，用户可下载资产导入模板，模板字段属性与 web 资产新增界面属性一致，模板内有填写说明，如图：

点击 选取文件 按钮，选择要导入的文件，点击 提交 按钮，文件提交成功，导入情况可点击页面右上角  按钮，查看导入结果，如图：



导入模板格式填写合法，则显示 导入成功 ，用户可在资产列表查看导入的资产；若格式填写不合法，则显示 导入失败 ，鼠标点击导入失败的文件，弹出错误提示，如图：

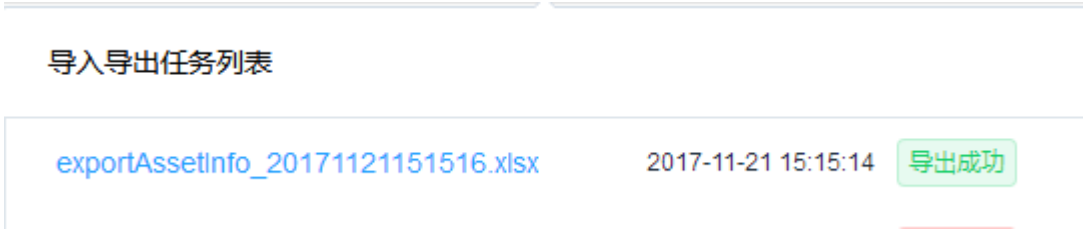
（2）点击 导出 按钮，弹出资产导出模板选择界面，如图：



① 选择“SOC 模板”，点击“提交”按钮，提示新增导出任务成功，如

图：

点击页面右上角按钮，可查看导出任务是否成功，鼠标点击导出成功文件可下载文件，如图：



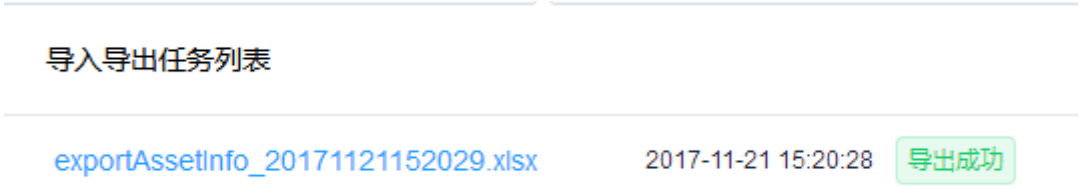
导出文件内容如图：

	A	B	C	D	E	F	G	H
1	填写说明：							
2	1、资产类别从《网络设施安全基本信息分类和属性字段参考 v2.2》中所列的7个大类中选取，不能填主机、网络设备、安全设备、应用系统、存储设备、虚拟机、其他设备之外的内容。							
3	2、主识别IP地址不能为空或无，只能填一个点分十进制IP地址。无IP地址的网络设施不在本表格统计之列。							
4	3、资产等级填所属定级网元级别，非定级网元填0。安全等级表示资产重要程度，填写1-5的数字。							
5	4、远程登录方式可填“无”，公网IP、DCN网IP、CN2网IP、私网IP必填其一，可根据实际情况填写，没有的留空，浮动IP也可以留空。							
6	5、浮动IP地址列之前的项目无论IT类或非IT类网络设施均要填写，浮动IP地址列之后的项目仅限IT类网络设施按对应情况填写。							
7								
8								
9	资产名称	业务系统	系统类型	主设备IP	安全域	地域	所属单位	所属部门
10	asset_不确定漏洞统计	外网扫描系统	电信自用系统	134.129.79.133	网络域	福州	省NOC	福州分公司
11	WIN-A46SLFS8HCI	内网扫描系统	面向公众的增值业务	172.168.68.39	维护域	福州	省NOC	信息安全部门
12	WIN-A46SLFS8HCI_oracle_1521	内网扫描系统	面向公众的增值业务	172.168.68.39	维护域	福州	省NOC	信息安全部门
13	WIN-A46SLFS8HCI_postgresql_5432	内网扫描系统	面向公众的增值业务	172.168.68.39	维护域	福州	省NOC	信息安全部门
14	WIN-A46SLFS8HCI_nginx_81	内网扫描系统	面向公众的增值业务	172.168.68.39	维护域	福州	省NOC	信息安全部门
15	189_IIS_80	内网扫描系统	面向公众的增值业务	172.168.68.189	维护域	福州	省NOC	信息安全部门
16	189_jboss_8085	内网扫描系统	面向公众的增值业务	172.168.68.189	维护域	福州	省NOC	信息安全部门
17	189_sqlserver_1434	内网扫描系统	面向公众的增值业务	172.168.68.189	维护域	福州	省NOC	信息安全部门
18	WIN-A46SLFS8HCI_apache_80	内网扫描系统	面向公众的增值业务	172.168.68.39	维护域	福州	省NOC	
19	189_weblogic_7001	内网扫描系统	面向公众的增值业务	172.168.68.189	维护域	福州	省NOC	

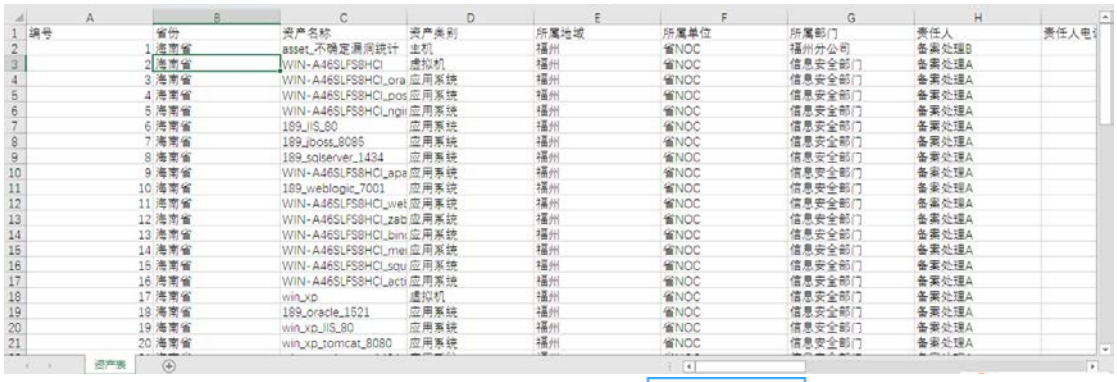
Sheet1

② 选择“集团模板”， 点击“提交”按钮，提示新增导出任务成功，如图：

点击页面右上角按钮，可查看导出任务是否成功，鼠标点击导出成功文件可下载文件，如图：



导出文件内容如图：



- 用户可通过在查询条件区域输入关键字，点击 查询 按钮，筛选查询结果，默认显示 4 个查询条件，点击 展开 按钮，可查看更多条件，或收起查询条件；点击 重置 按钮，可清空查询条件内容，并自动加载列表结果。

2.3.3 扩展属性配置

点击菜单“资产管理”=>“扩展属性配置”，进入扩展属性配置界面，如图:

- 点击“新增”按钮，弹出新增界面，*号标识为必填项，如图：

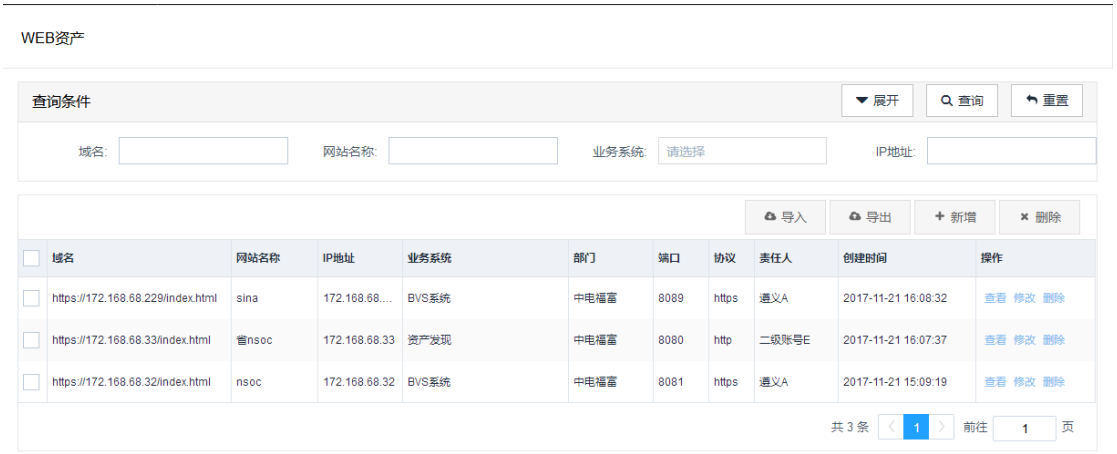
（1）扩展属性类型：自营普通资产类型即资产管理的扩展属性，WEB 资产类型；

（2）属性表单类型：文本框、下拉框、多选框；

- 用户可通过点击“查看”、“修改”“删除”按钮，对扩展属性进行操作。

2.3.4 WEB 资产

点击菜单“资产管理”=>“WEB 资产”，进入 WEB 资产配置界面，如图：



- **WEB 资产新增**

  点击“新增”按钮，弹出 WEB 资产新增界面，*号为必填标识，如图：

属性填写完后，点击提交按钮即可。

- **WEB 资产导入/导出**

（1）点击 

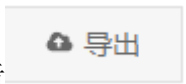
按钮，弹出 WEB 资产导入界面，如图：

点击“下载导入文件模板”，可下载模板文件，文档内有填写格式说明，如图：

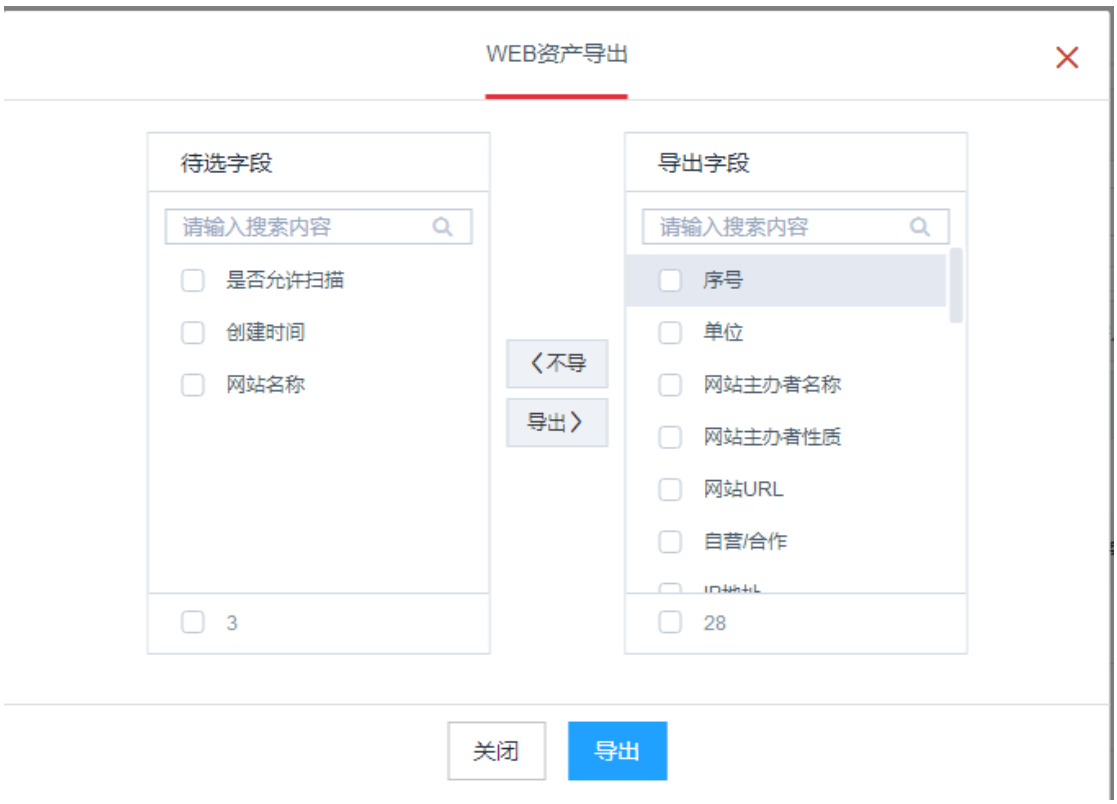
点击 

按钮，选择需要导入的文件，点击 

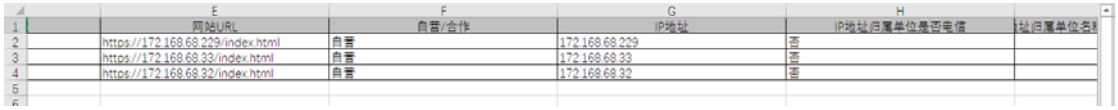
按钮，文件格式填写合法，提示导入成功，若填写不合法，则弹窗错误提示。

（2）点击 

按钮，弹出 WEB 资产导出界面，如图：



导出字段可选择，点击 导出 按钮，若导出成功，则按用户选择的导出字段展示，若导出失败则提示导出失败。



	E	F	G	H
1	网站URL	自营/合作	IP地址	IP地址归属单位是否电信
2	https://172.168.68.229/index.html	自营	172.168.68.229	否
3	https://172.168.68.33/index.html	自营	172.168.68.33	否
4	https://172.168.68.32/index.html	自营	172.168.68.32	否
5				

- 用户可通过在查询条件区域输入关键字，点击 查询 按钮，筛选查询结果，默认显示 4 个查询条件，点击 展开 按钮，可查看更多条件，或收起查询条件；点击 重置 按钮，可清空查询条件内容，并自动加载列表结果。

2.3.5 业务系统

点击菜单“资产管理”=>“业务系统”，进入业务系统配置界面，如图：

- **业务系统新增**

  点击“新增”按钮，弹出业务系统新增界面，*号标识为必填项，如图：

（1）在“管理员信息”sheet 中，责任人、安全管理员为必填，可以选择多个，但默认责任人和默认安全管理员有且只有一个；

（2）在“网络信息”sheet 中，至少填写一种 ip 类型，ip 格式要求为（1.1.1.1,2.2.2.2-2.2.2.3,3.3.3.3-8,4.4.4.4/16）。

- **业务系统导入/导出**

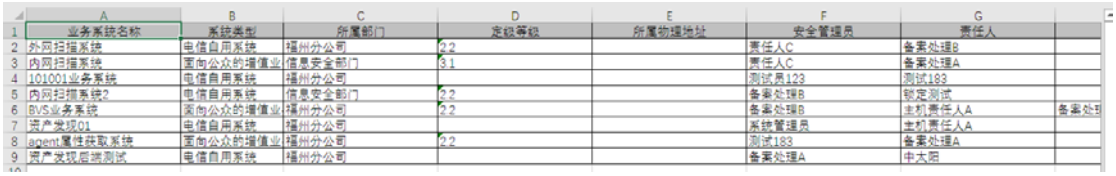
（1）点击 

按钮，弹出业务系统导入界面，如图：

点击“下载导入文件模板”，可下载导入模板，模板内有格式填写说明，如图：

点击 选取文件 按钮，选取需要导入的文件，点击 提交 按钮，格式填写正确则提示导入成功，若格式填写不合法，则弹窗错误提示；

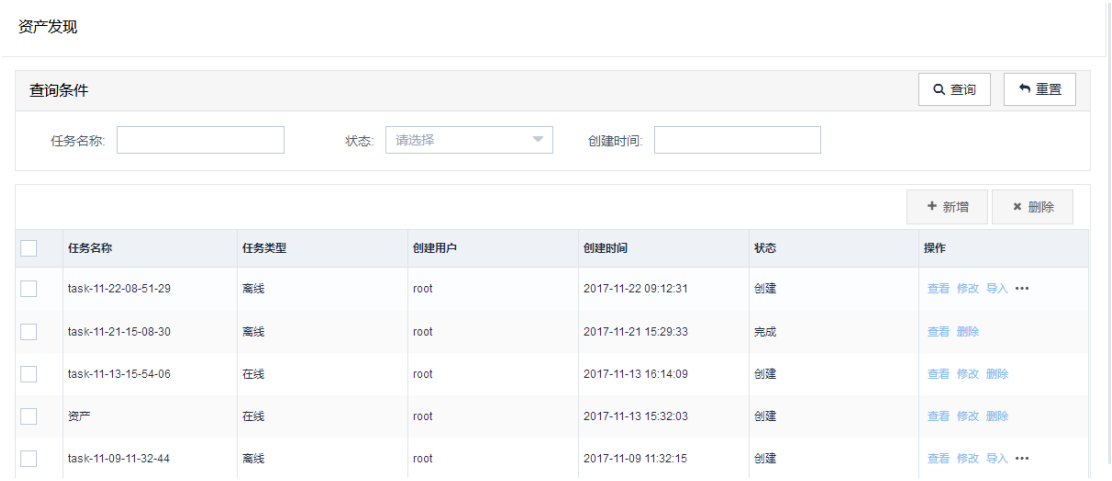
（2）点击 导出 按钮，导出业务系统列表数据，如图：



- 用户可通过在查询条件区域输入关键字，点击 查询 按钮，筛选查询结果，默认显示 4 个查询条件，点击 展开 按钮，可查看更多条件，或收起查询条件；点击 重置 按钮，可清空查询条件内容，并自动加载列表结果。

2.3.6 资产发现

点击菜单“资产管理”=>”资产发现”，进入资产发现任务配置界面，如图：



- **资产发现任务下发**

  点击“新增”按钮，弹出任务下发界面，*号标识为必填项，根据选择的不同任务类型联动展示不同属性字段，如图：

任务名称：可为空，提交时会自动生成任务名称，格式为：task-月-日-时-分-秒；

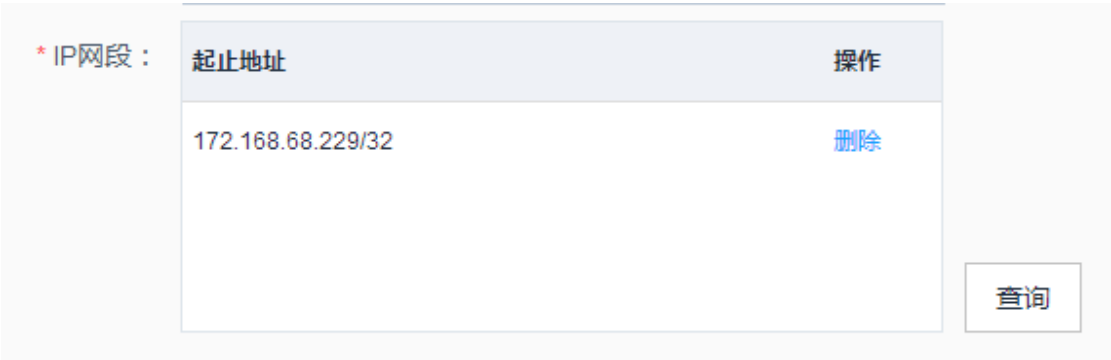
（1）在线任务

端口范围：非必填项，在线任务扫描的端口范围，格式要求为8080,8080-8089；多个用“,”隔开；

IP 网段：选择在线任务扫描的 IP 范围，点击 

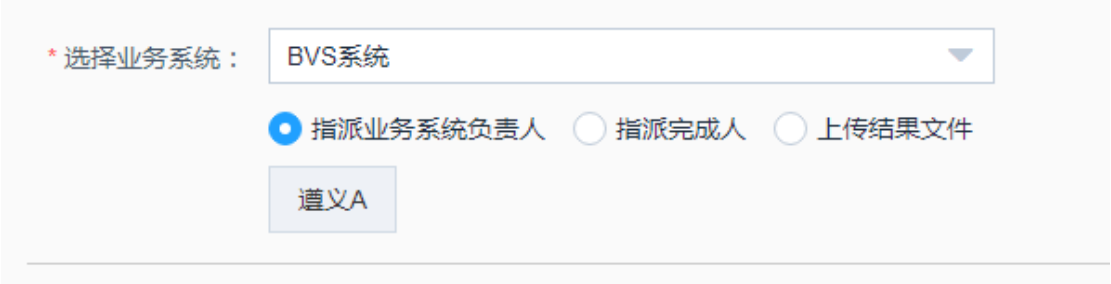
按钮，弹出 IP 网段选择界面，如图：

点击“查询”按钮，左侧展示所有待选择的业务系统名称，选中其中一个业务系统，右侧展示该业务系统的网络信息；选择 IP 范围，点击“提交”按钮，IP 网段文本框展示已选择 IP 地址范围，如图：



（2）离线任务

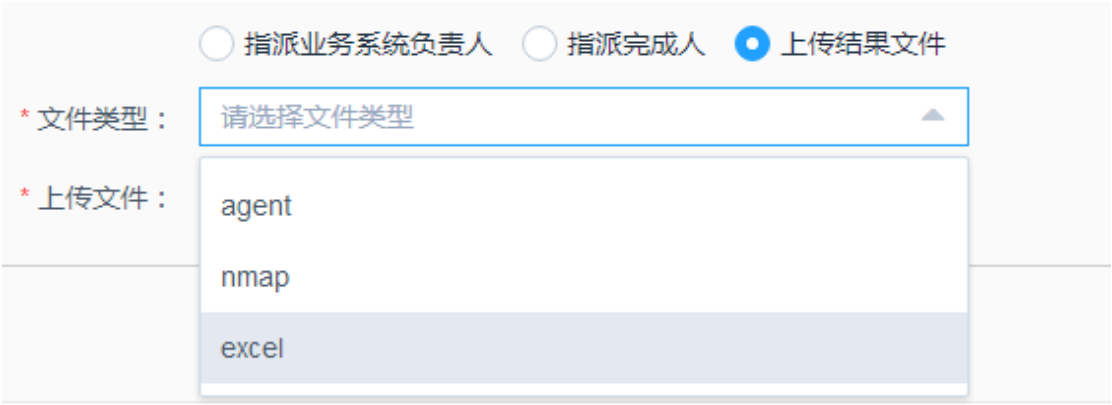
用户分别可选择业务系统责任人、指派完成人、或直接导入离线结果文件来完成任务，如图：



① 指派业务系统负责任人：该任务只能由业务系统的默认责任人来完成离线结果文件导入；

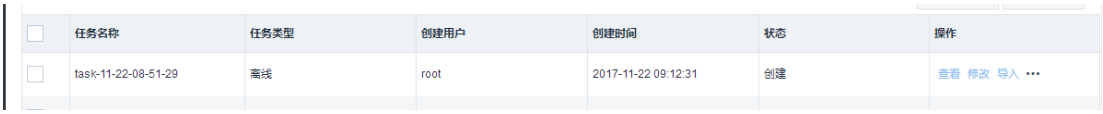
② 指派完成人：创建人可指派任一 SOC 用户来完成任务；

③ 上传结果文件：支持三种文件格式，分别为：agent、nmap、excel，如图：

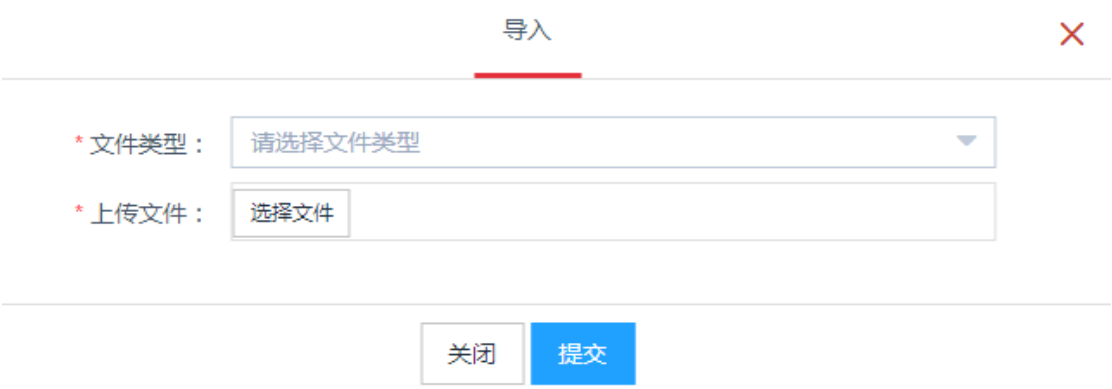


信息填写完成，点击提交按钮即可。

④ 若离线任务选择指派业务系统责任人或指派完成人，则任务列表对应任务操作按钮有个“导入”按钮，操作同③；如图：



点击“导入”按钮，弹出导入界面，如图：

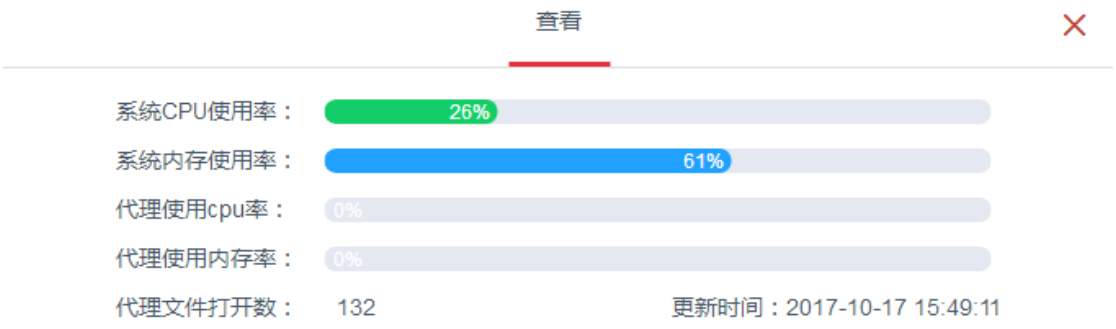


2.3.7 主机代理

点击菜单“资产发现”=>“主机代理”，进入主机代理配置界面，展示所有安装 agent 的主机资产，如图：

- **Agent 状态查看**

点击 查看 按钮，弹出 agent 状态查看界面，如图：



- **代理更新**

点击 代理更新 按钮，弹出代理更新包上传界面，如图：

根据实际需要选择操作系统类型，输入更新包版本号，点击 选取文件 按钮，点击 上传 按钮，提示上传成功。

2.3.8 未知资产

点击菜单“资产管理”=>“未知资产”，进入未知资产界面，如图：

- **未知资产来源**

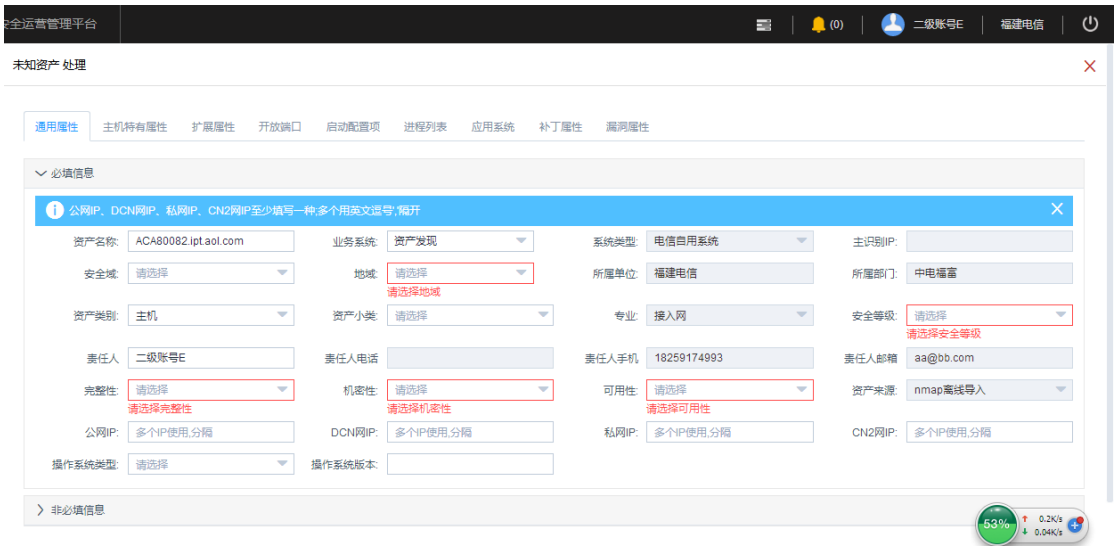
  通过资产发现任务发现未知资产，具体参看 2.3.6；

- **未知资产处理 / 指派 / 回退**

  （1）处理

  默认由业务系统的默认责任人处理未知资产，责任人登录 SOC 平台后，点击“处理”按钮，进入处理流程界面，如图：

  点击“开始处理”弹出未知资产处理界面，如图：



用户完善必填属性后，点击提交，进入未知资产审核流程。

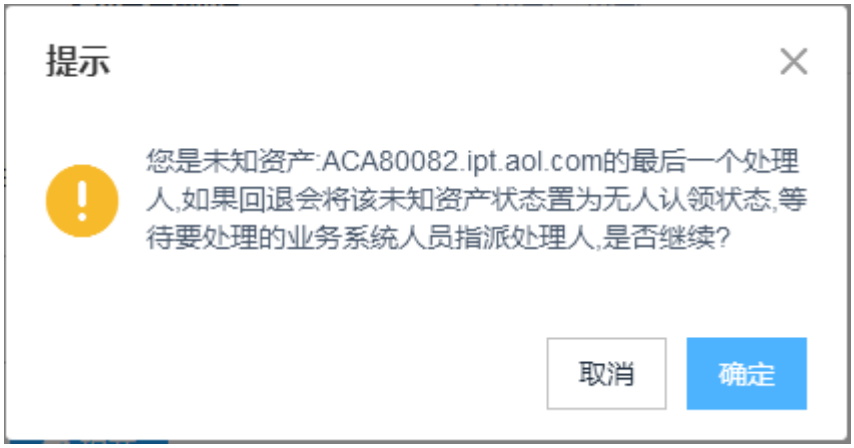
（2）指派

责任人选择指派处理用户，可指派给其他用户处理该资产，如图：

（3）回退

责任人选择回退，可将任务回退给上级管理员，如图：

注：若用户为该资产的最后一个处理人，申请回退后，该条资产则变未无人认领状态，如图：



- **未知资产批量处理**

（1）选择“待处理”状态资产，点击 

按钮，用户可在 excel 批量完善资产信息后保存文件；

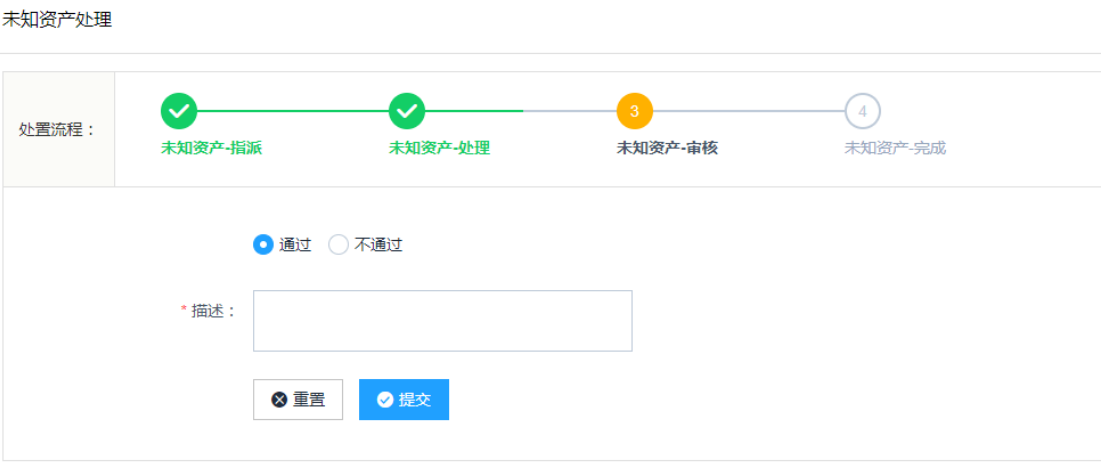
（2）点击 

按钮，弹出导入界面，如图：

点击 选取文件 按钮，选择（1）中保存的文件，点击 提交 按钮，若信息填写合法，则未知资产导入成功；若信息填写非法，则弹窗错误提示。

- **未知资产审核**

审核员登录 SOC 平台，点击“处理”按钮，进入审核界面，如图：



① 选择“通过”，则该未知资产变为已知资产；

② 选择“不通过”，则退回至“指派”流程，如图：

- **处理历史查看**

  点击“处理历史”按钮，弹出处理历史记录界面，可溯源该未知资产的操作记录，如图：

2.3.9 代理客户端

2.3.9.1 省测自建任务

2.3.9.1.1 流量监控：

（1）任务说明：进行抓包。
（2）操作说明：选择对应的任务类型、资产、周期类型、任务内容填写过滤条件。

任务内容：过滤出目的地址为 192.168.39.188，且目的端口为 22 的包

{"ipaddress":"172.168.68.142","count":20,"filter":"dst host 192.168.39.188 and dst port 22","ifupload":"true"}

（3）结果查看：

结果在客户端心跳打印，暂时没有上报入库。

2.3.9.1.2 监控文件生成、监控文件属性、监控文件属性、监控 ROOTKITS、检测隐藏进程、监控账号信息、检测隐藏文件和目录、检测.history、检测.history、登陆后门检查、检测 sniffer_logs、检测可疑的目录、监控开机自动恶意软件、检查可能的 Rootkit 文件和目录、检测可疑的端口、检测可疑文件类型、检测 Xinetd 守护进程、检测 Shared_Libs、检测 deleted_files、检测 running_procs：

（1）任务说明：进行 rkhunter 检测；

（2）操作说明：选择对应的任务类型、资产、周期类型即可；

（3）结果查看：

任务采集结束后，在结果查看里展示。

2.3.9.1.3 本地脚本、shell 脚本/C#动态脚本：

（1）任务说明：进行基线检查；

（2）操作说明：选择对应的任务类型、资产、周期类型即可；

（3）结果查看：

查看基线更新时间即可。

2.3.9.1.4 监控

暂时无用。

2.3.9.1.5 监控采集配置

暂时无用。

2.3.9.1.6 arp：

（1）任务说明：检查 arp 信息；

（2）操作说明：选择对应的任务类型、资产、周期类型即可；

（3）结果查看：

任务采集结束后，在结果查看里展示。

2.3.9.1.7 资产采集策略（暂时无用）：

（1）任务说明：采集资产信息

（2）操作说明：选择对应的任务类型、资产、周期类型、填写任务内容：

任务内容 1:,采集 tomcat 信息

```
[{
    "flag": 2,
    "type": "app_port",
    "appTypes": {
        "keyword":
"State.Name.eq=java,Args.*.eq=org.apache.catalina.startup.Bootstrap",
        "appPath": "args[-Dcatalina.home=]",
        "port": "xml[conf/server.xml|Server/Service/Connector|port]",
        "version": "shell[bin/version.sh |grep 'Server number' | awk
'{print $3}',,*]",
        "name": "tomcat",
        "categoryId": 40103
    }
}]
```

任务内容 2：重启 agent 心跳进程

```
[{
```

```
    "flag": 1,
    "type": "app_key",
    "appTypes": {
        "keyword": "",
        "appPath": "",
        "port": "",
        "version":    "shell[ps    -ef|grep    bin/CTFFAgent.jar|grep
ctff_agent_linux|grep -v grep|awk -F''{print $2}'|xargs kill -9,,*]",
        "name": "java",
        "categoryId": 40103
    }
}]
```


（3）结果查看：

暂时不上报结果

2.3.9.1.8 弱口令：

（1）任务说明：采集弱口令信息；

（2）操作说明：选择对应的任务类型、资产、周期类型：

（3）结果查看：

任务采集结束后，在结果查看里展示。

2.3.9.1.9 强制采集

（1）任务说明：采集资产和基线信息；
（2）操作说明：选择对应的任务类型、资产、周期类型：

（3）结果查看：

任务采集结束后，查看资产和基线更新时间。

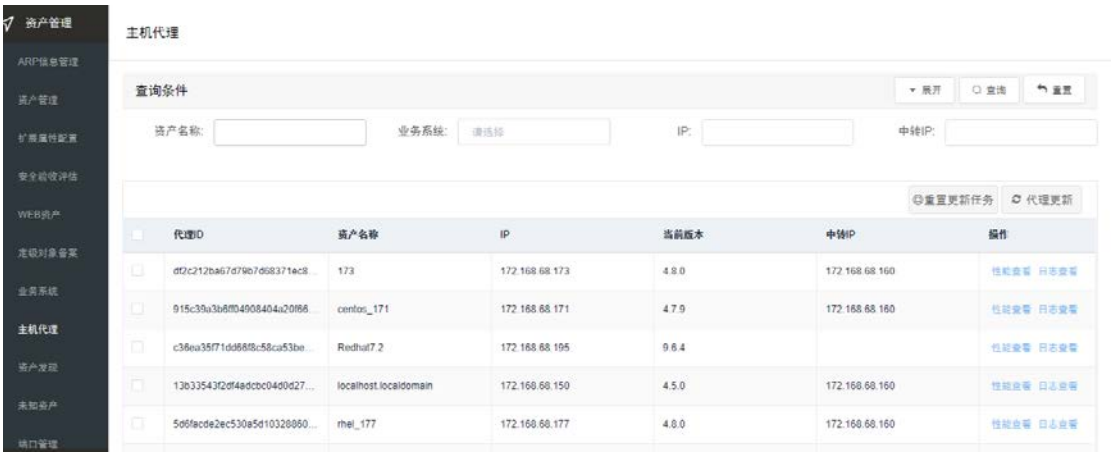
2.3.9.1.10 重新生产 agentid

（1）任务说明：采集弱口令信息；

（2）操作说明：选择对应的任务类型、资产、周期类型；

（3）、结果查看：

通过查看主机代理过滤资产信息，判断代理 id 是否发生变化；



2.3.9.1.11 更新配置文件

（1）任务说明：采集弱口令信息；
（2）操作说明：选择对应的任务类型、资产、周期类型、填写任务内容；
任务内容:将配置文件中 log.serverIp 节点原先的内容替换成 172.168.68.104，log.serverPort 节点原先的内容替换成 514，log.openHost 节点原先的内容替换成 1；

log.serverIp=172.168.68.104;log.serverPort=514;log.openHost=1;

（3）结果查看：

查看任务结果中任务状态和结果时间；

2.3.9.1.12 获取 agent 日志

（1）任务说明：获取 agent 目录 log 下的日志文件

（2）操作说明：选择对应的任务类型、资产、周期类型、填写任务内容：

任务内容 1：获取 log 目录下的 AgentClient.log 文件

AgentClient.log

任务内容 2：获取 log 目录下的 AgentClient.log 文件

CTFFAgent.log.2020-09-10

（3）结果查看：

查看任务结果任务状态和结果时间、最新结果（文件保存在 agent 服务端的路径）；

2.3.9.1.13 获取目录结构

（1）任务说明：采集弱口令信息；
（2）操作说明：选择对应的任务类型、资产、周期类型、填写任务内容；
任务内容：查看/home 目录下的结果；

ls -l /home

（3）结果查看：
查看任务结果中任务状态和结果时间、最新结果：

2.3.9.1.14 安装或更新私网代理

（1）任务说明：安装或更新私网代理；
（2）操作说明：选择对应的任务类型、资产、周期类型、填写任务内容；
任务内容：私网代理安装包的名字；

local_proxy_v20190821.tar.gz

（3）结果查看：
查看任务结果中任务状态：

2.3.9.1.15 重启私网代理

（1）任务说明：重启私网代理；

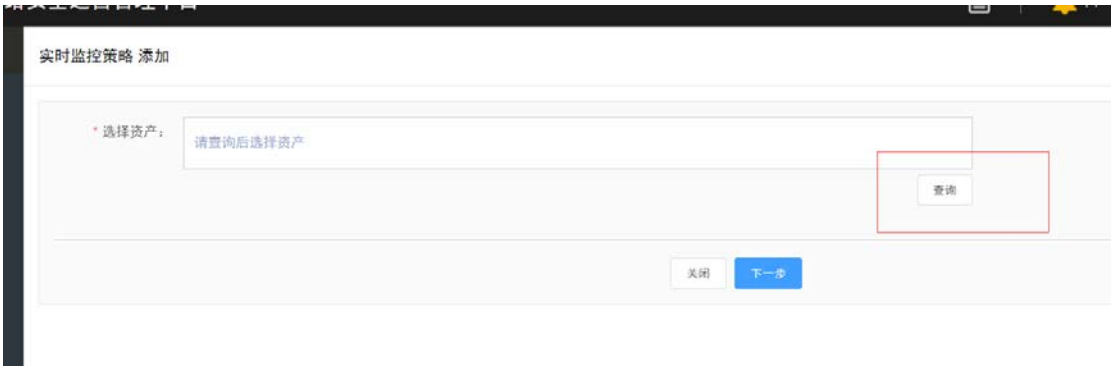
（2）操作说明：选择对应的任务类型、资产、周期类型；

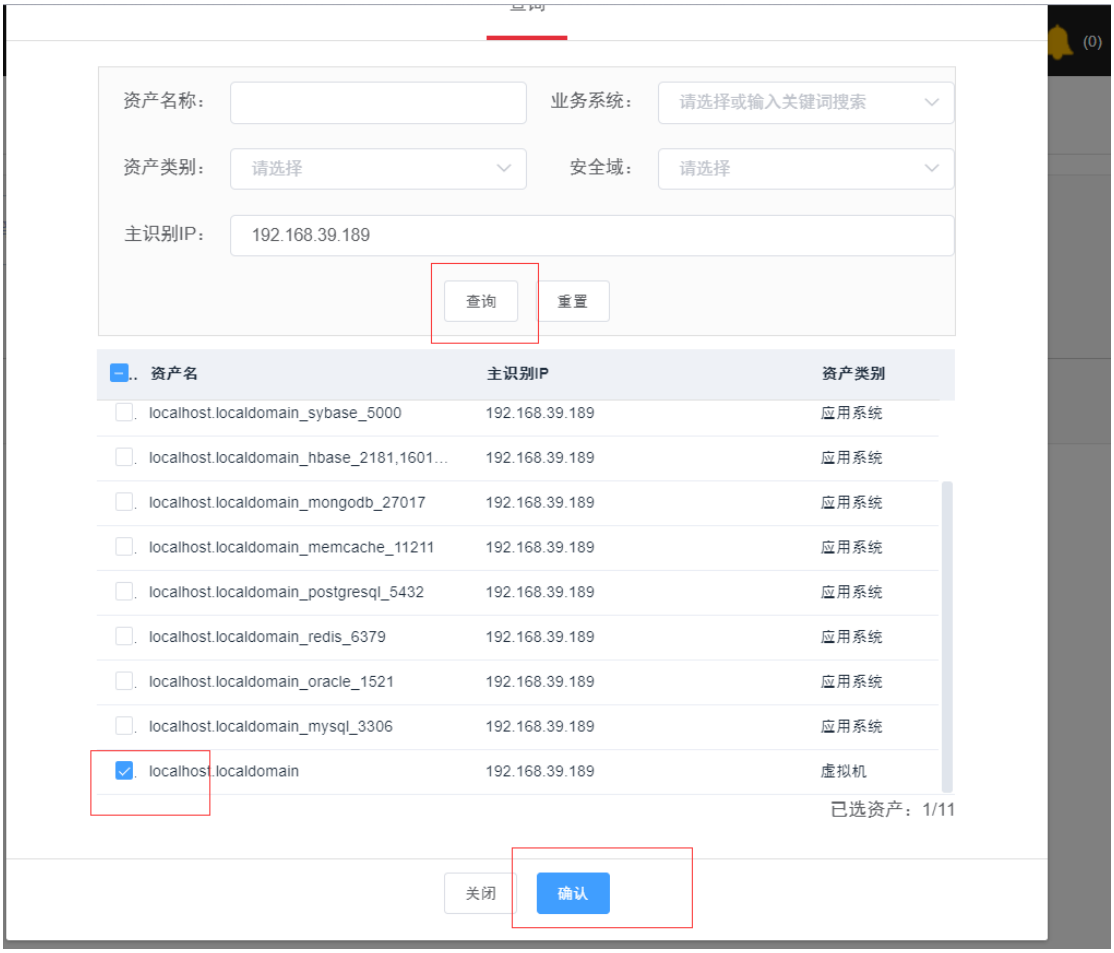
（3）结果查看：

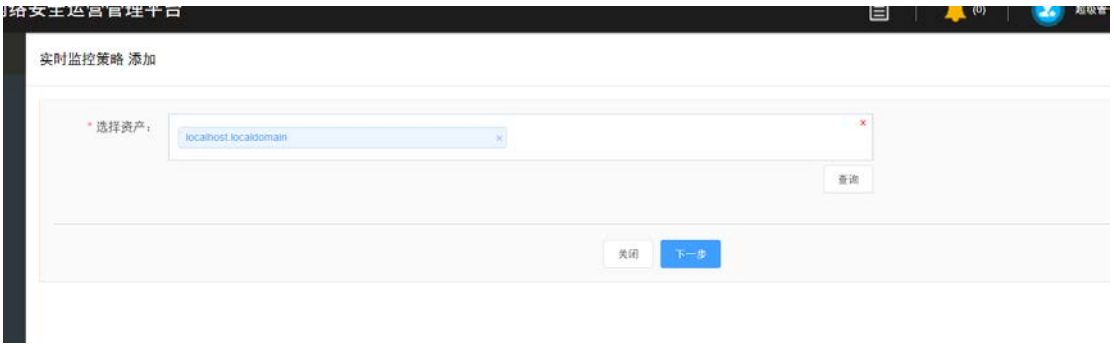
查看任务结果中任务状态：

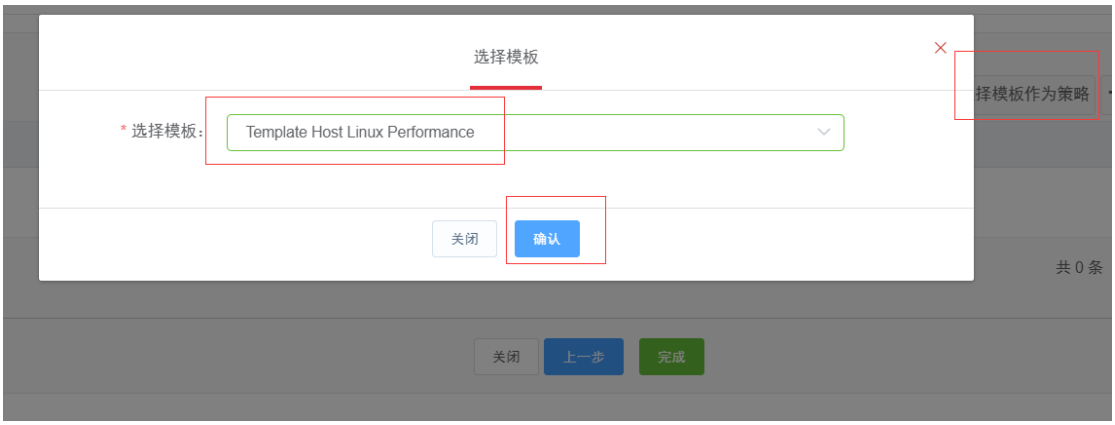
2.3.9.1.16 应用监控任务：

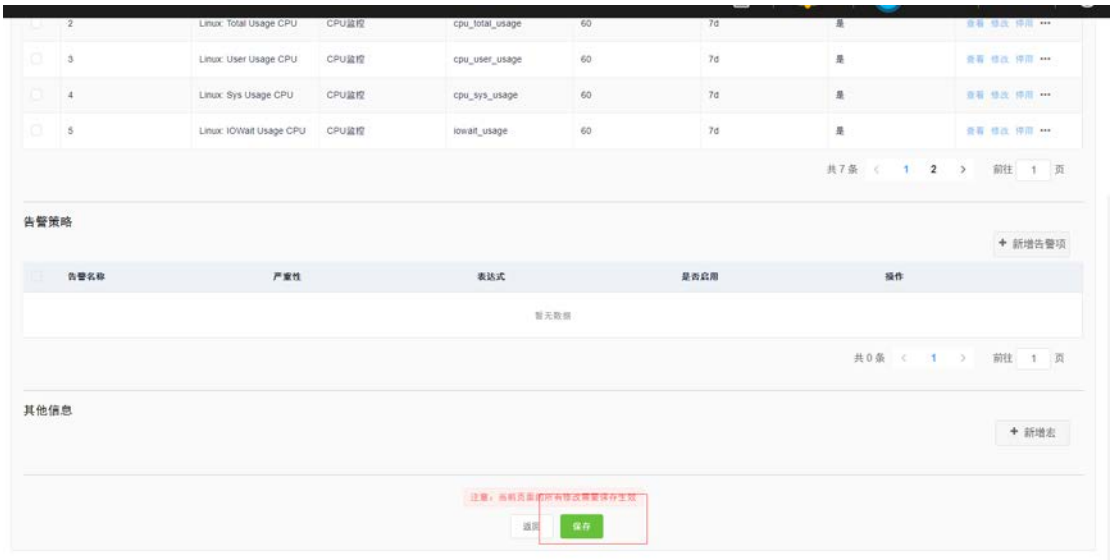
（1）新增监控策略：

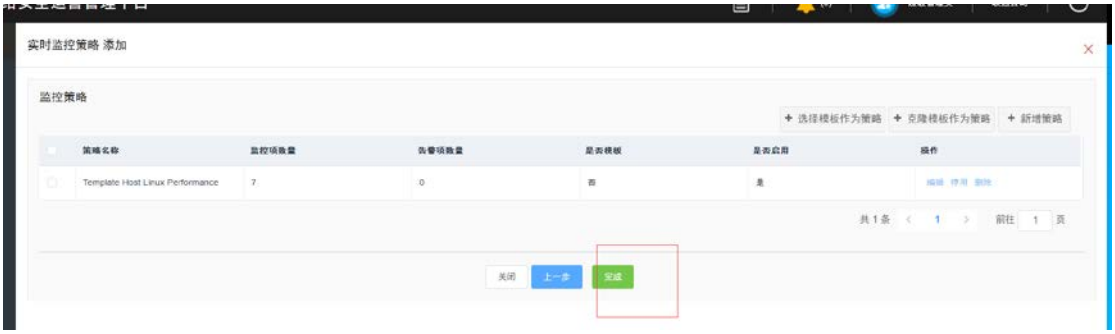



资产名称：
业务系统：
请选择或输入关键词搜索
资产类别：
请选择
安全域：
请选择
主识别IP：
192.168.39.189
查询
重置
资产名
主识别IP
资产类别
localhost.localdomain_sybase_5000 192.168.39.189 应用系统
localhost.localdomain_hbase_2181,1601... 192.168.39.189 应用系统
localhost.localdomain_mongodb_27017 192.168.39.189 应用系统
localhost.localdomain_memcache_11211 192.168.39.189 应用系统
localhost.localdomain_postgresql_5432 192.168.39.189 应用系统
localhost.localdomain_redis_6379 192.168.39.189 应用系统
localhost.localdomain_oracle_1521 192.168.39.189 应用系统
localhost.localdomain_mysql_3306 192.168.39.189 应用系统
localhost.localdomain 192.168.39.189 虚拟机
已选资产：1/11
关闭
确认


实时监控策略 添加
选择资产：
localhost.localdomain
查询
关闭
下一步


选择模板
选择模板：
Template Host Linux Performance
关闭
确认
择模板作为策略
共 0 条
关闭
上一步
完成



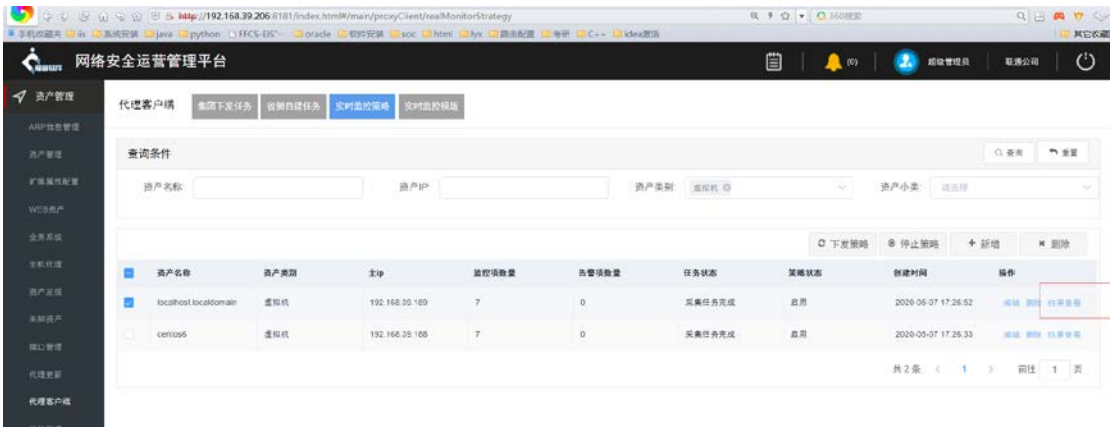


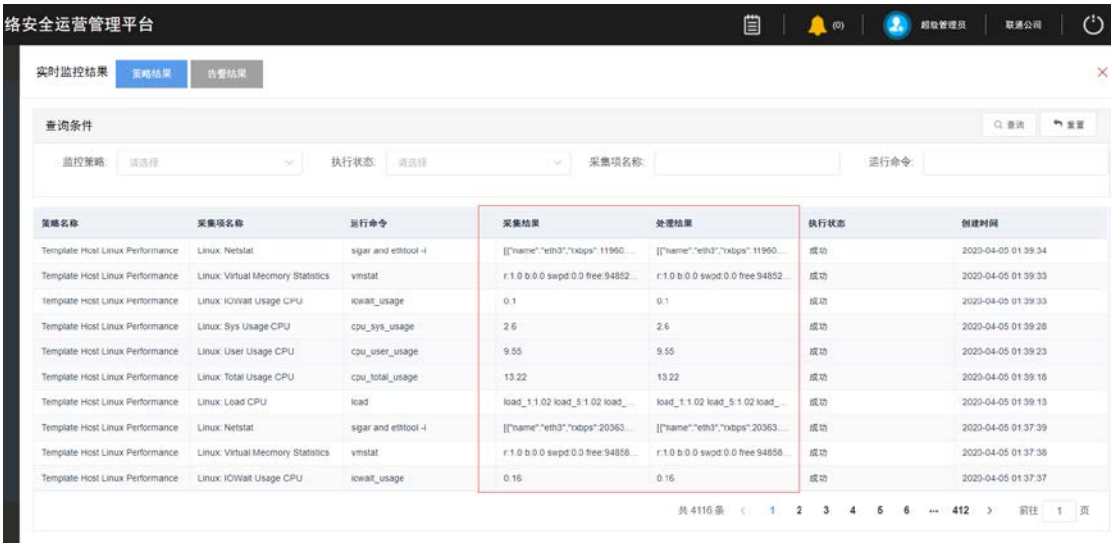
（2）下发策略；

注意事项：然后查看省侧自建任务中有生成新的应用监控任务，点击查看任务内容，有内容则创建成功。


省侧自建任务 查看
任务名称：
实时监控任务_202009101925031
* 任务类型：
应用监控任务
* 周期类型：
实时
定时
周期
* 任务对象：
按资产
按业务系统
按部门
* 选择资产：
localhost.localdomain
localhost.localdomain_mysql_3306
查询
任务内容：
[{"assetId":21795,"assetTypeList":
[50201],"httpPort":0,"jmxPort":0,"macroValueMap":{},"monitorItems":
关闭

（3）查看结果；


网络安全运营管理平台
资产管理
代理客户端
查询条件



（4）停止策略：

选中--然后点击停止策略--查看省侧任务有没有自动生成一个新的应用监控任务---点击查看任务内容---内容为空则创建成功。

2.3.9.1.17 UDP 端口探测

（1）任务说明：自动检测 agent 和 logc 的通信地址和端口；

（2）操作说明：选择对应的任务类型、资产、周期类型、填写任务内容；

任务内容：检测 agent 有部署 logc 的地址端口（172.168.68.104：514，172.168.68.158：514）是不是能正常通信；

[{"ip":"172.168.68.104","port":"514"},{"ip":"172.168.68.158","port":"514"},{"ip":"172.168.68.158","port":"514"}]

（3）结果查看：

如果检测到任务内容中的 logc 的地址和端口可以与 agent 正常通信，则会自动生成更新配置文件，将 agent 配置文件中的节点更换成任务内容中的值 log.serverIp=172.168.68.104;log.serverPort=514;log.openHost=1;

2.3.9.1.18 删除多余进程

（1）任务说明：删除 agent 重复的进程；

（2）操作说明：选择对应的任务类型、资产、周期类型；

（3）结果查看：

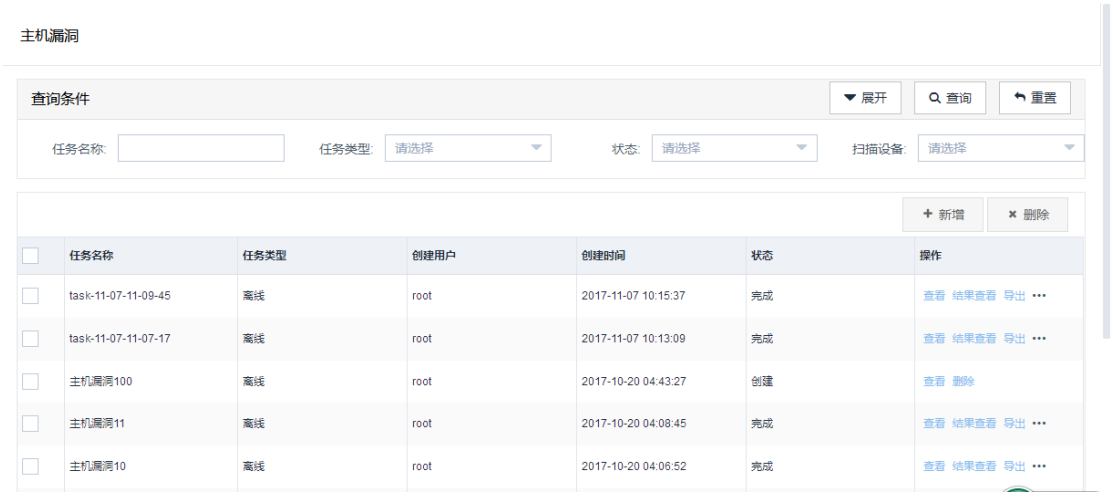
查看任务结果中任务状态：

2.4 任务管理

本模块主要功能为提供任务下发功能。

2.4.1 主机漏洞

点击菜单“任务管理”=>“主机漏洞”，进入主机漏洞任务配置界面，如图：



- **任务下发**

  点击“新增”按钮，用户可选择创建在线任务或离线任务，根据选择的不同任务类型联动展示不同字段属性，*号标识为必填字段；

  （1）在线任务，如图：

  扫描设备：下拉框展示所有漏扫设备，（基础数据可在系统配置->扫描器配置添加）；

  扫描策略：选择扫描器策略；

IP 类型：根据选择的扫描设备联动展示扫描器所支持的网段类型；

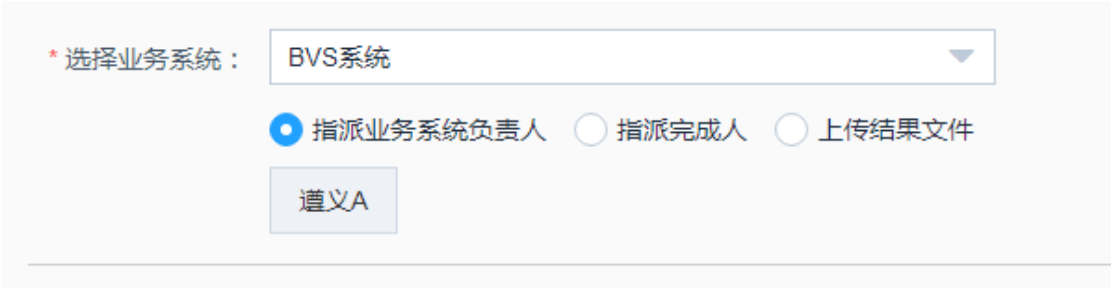
扫描目标：根据不同维度选择扫描目标；

等级选择：选择整改的漏洞等级；

信息填写完成后，点击“提交”即可。

（2）离线任务，如图：

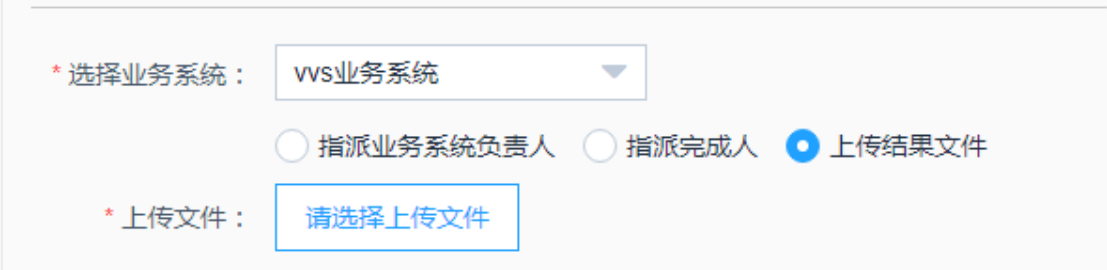
用户分别可选择业务系统责任人、指派完成人、或直接导入离线结果文件来完成任务，如图：



① 指派业务系统负责任人：该任务只能由业务系统的默认责任人来完成离线结果文件导入；

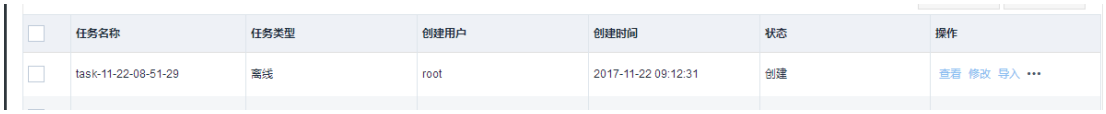
② 指派完成人：创建人可指派任一 SOC 用户来完成任务；

③ 上传结果文件：创建用户可直接导入漏扫结果文件，如图：



信息填写完成，点击提交按钮即可。

④ 若离线任务选择指派业务系统责任人或指派完成人，则任务列表对应任务操作按钮有个“导入”按钮，操作同③；如图：



点击“导入”按钮，弹出导入界面，用户可导入漏扫结果文件，如图：

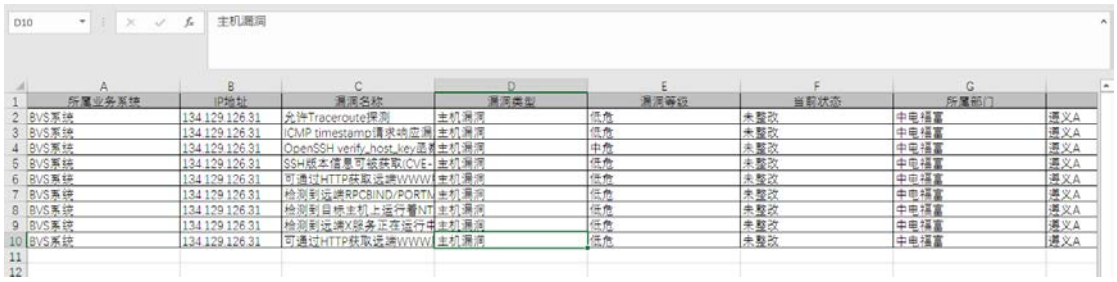
- **结果查看**

点击 结果查看 按钮，弹出漏洞结果查看详情界面，如图：

- **漏洞结果导出**

（1）在任务列表操作栏，点击 导出 按钮，导出漏洞结果详情，导出文件分别展示“漏洞扫描字段”、“漏洞扫描非资产”、“漏洞信息”，如图：

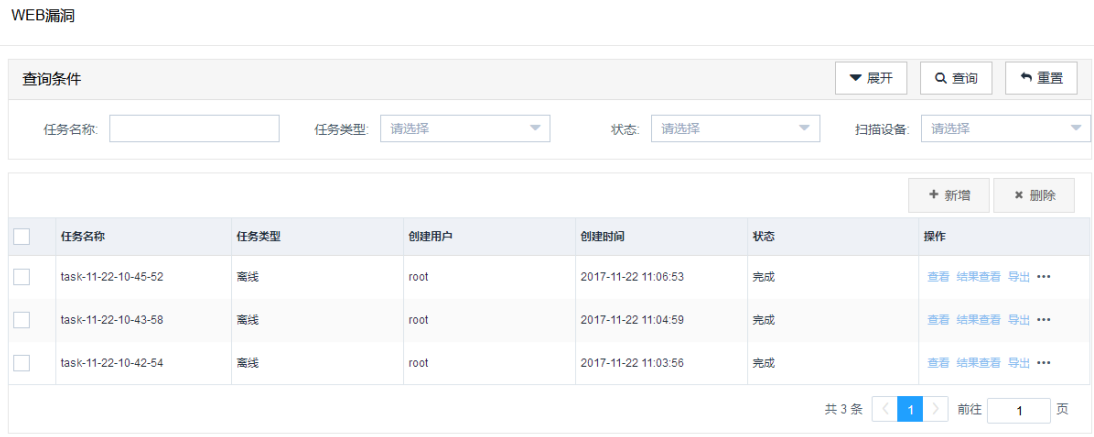
（2）在漏洞结果查看界面，点击 导出 按钮，导出漏洞详情数据，如图：



- 用户可通过在查询条件区域输入关键字，点击 查询 按钮，筛选查询结果，默认显示 4 个查询条件，点击 展开 按钮，可查看更多条件，或收起查询条件；点击 重置 按钮，可清空查询条件内容，并自动加载列表结果。

2.4.2 WEB 漏洞

点击菜单“任务管理”=>“WEB 漏洞”，进入 WEB 漏洞任务配置界面，如图：



- **任务下发**

  点击“新增”按钮，用户可选择创建在线任务或离线任务，根据选择的不同任务类型联动展示不同字段属性，*号标识为必填字段；

  （1）在线任务，如图：

  扫描设备：下拉框展示所有 WEB 漏洞扫描设备，（基础数据可在系统配置->扫描器配置添加）；

  扫描策略：选择扫描器策略；

IP 类型：根据选择的扫描设备联动展示扫描器所支持的网段类型；

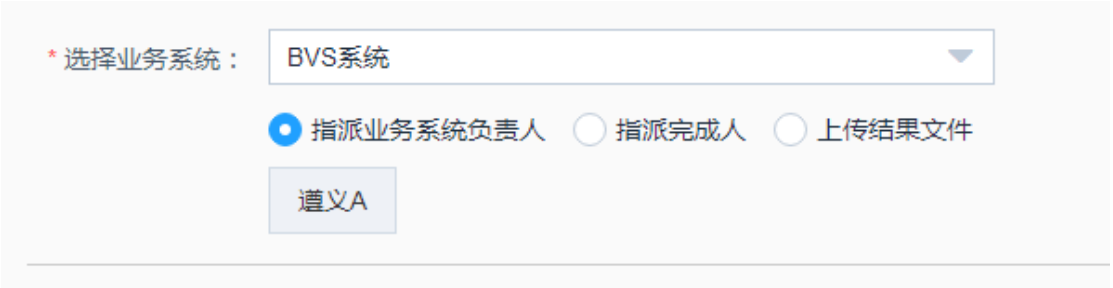
扫描目标：根据不同维度选择扫描目标；

等级选择：选择整改的漏洞等级；

信息填写完成后，点击“提交”即可。

（2）离线任务，如图：

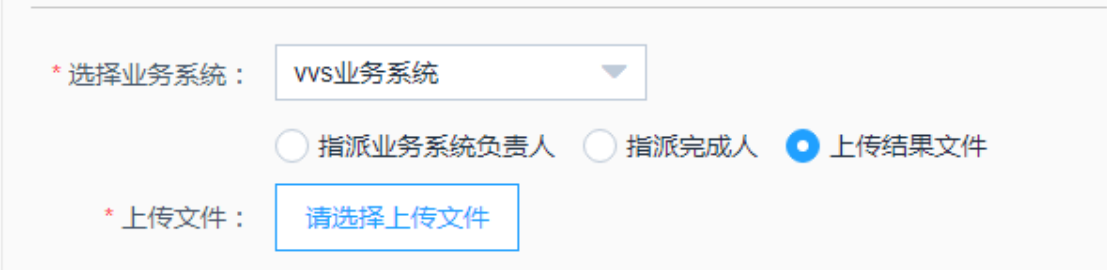
用户分别可选择业务系统责任人、指派完成人、或直接导入离线结果文件来完成任务，如图：



① 指派业务系统负责任人：该任务只能由业务系统的默认责任人来完成离线结果文件导入；

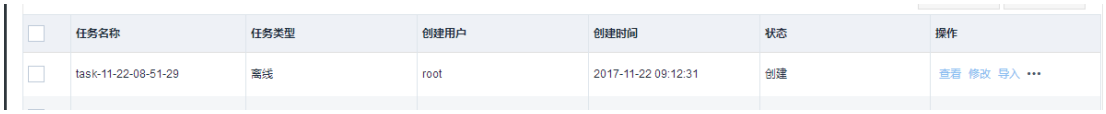
② 指派完成人：创建人可指派任一 SOC 用户来完成任务；

③ 上传结果文件：创建用户可直接导入漏扫结果文件，如图：



信息填写完成，点击提交按钮即可。

④ 若离线任务选择指派业务系统责任人或指派完成人，则任务列表对应任务操作按钮有个“导入”按钮，操作同③；如图：



点击“导入”按钮，弹出导入界面，用户可导入漏扫结果文件，如图：

- **结果查看**

点击 结果查看 按钮，弹出漏洞结果查看详情界面，如图：

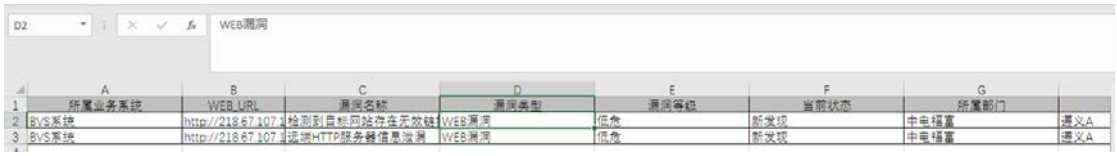
- **漏洞结果导出**

（1）在任务列表界面操作栏，点击 导出 按钮，导出漏洞结果详情，导出文件分别展示“漏洞扫描字段”、“漏洞扫描非资产”、“漏洞信息”，如图：

【task-11-22-10-45-52】 扫描结果					
web资产名称	WEB_URL	漏洞扫描			
		高危	中危	低危	总数
sina	http://218.67.107.18	0	0	2	2

漏洞扫描资产 | 漏洞扫描非资产 | 漏洞信息

（2）在漏洞结果查看界面，点击 导出 按钮，导出漏洞详情数据，如图：



所属业务系统	WEB_URL	漏洞名称	漏洞类型	漏洞等级	当前状态	所属部门	
BVS系统	http://218.67.107.1	检测到目标网站存在无效链	WEB漏洞	低危	新发现	中电福富	通义A
BVS系统	http://218.67.107.1	误报HTTP服务器信息泄漏	WEB漏洞	低危	新发现	中电福富	通义A

- 用户可通过在查询条件区域输入关键字，点击 查询 按钮，筛选查询结果，默认显示 4 个查询条件，点击 展开 按钮，可查看更多条件，或收起查询条件；点击 重置 按钮，可清空查询条件内容，并自动加载列表结果。

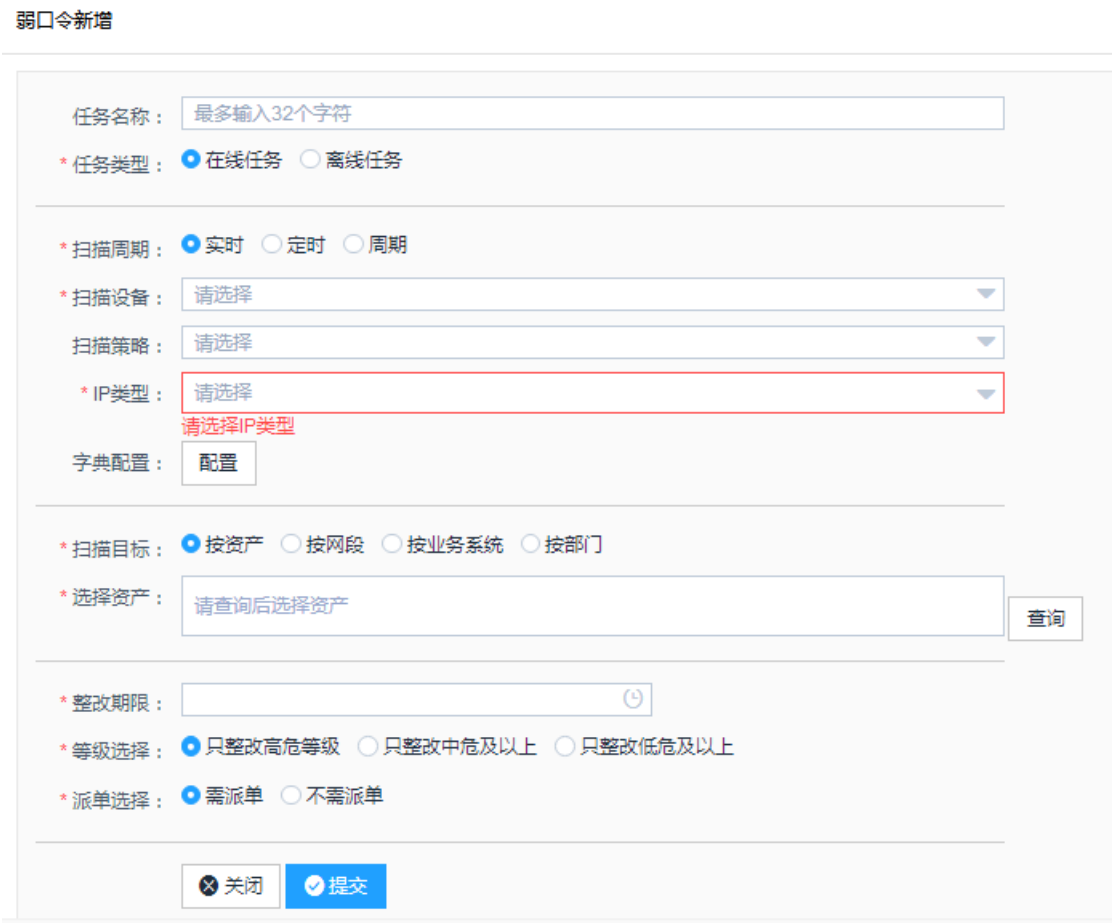
2.4.3 弱口令

点击菜单“任务管理”=>“弱口令”，进入弱口令任务配置界面，如图：

- **任务下发**

  点击“新增”按钮，用户可选择创建在线任务或离线任务，根据选择的不同任务类型联动展示不同字段属性，*号标识为必填字段；

  （1）在线任务，如图：



  扫描设备：下拉框展示所有弱口令扫描设备，（基础数据可在系统配置->扫描器配置添加）；

  扫描策略：选择扫描器策略；

  IP 类型：根据选择的扫描设备联动展示扫描器所支持的网段类型；

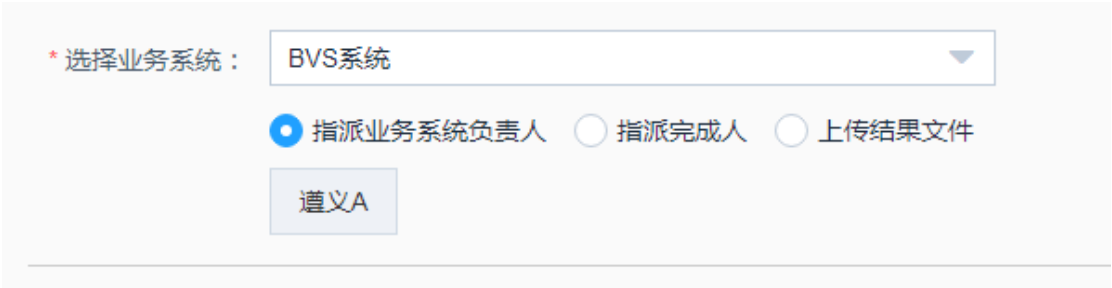
扫描目标：根据不同维度选择扫描目标；

等级选择：选择整改的漏洞等级；

信息填写完成后，点击“提交”即可。

（2）离线任务，如图：

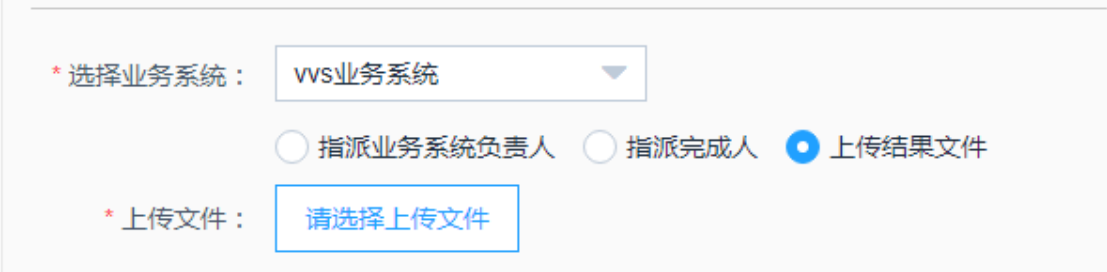
用户分别可选择业务系统责任人、指派完成人、或直接导入离线结果文件来完成任务，如图：



① 指派业务系统负责任人：该任务只能由业务系统的默认责任人来完成离线结果文件导入；

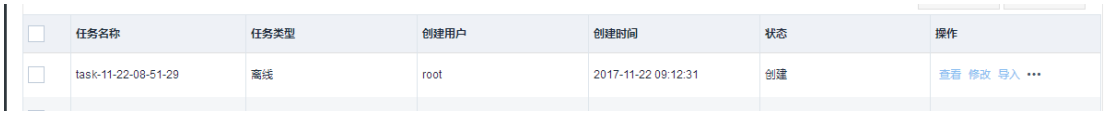
② 指派完成人：创建人可指派任一 SOC 用户来完成任务；

③ 上传结果文件：创建用户可直接导入漏扫结果文件，如图：



信息填写完成，点击提交按钮即可。

④ 若离线任务选择指派业务系统责任人或指派完成人，则任务列表对应任务操作按钮有个“导入”按钮，操作同③；如图：



点击“导入”按钮，弹出导入界面，用户可导入漏扫结果文件，如图：

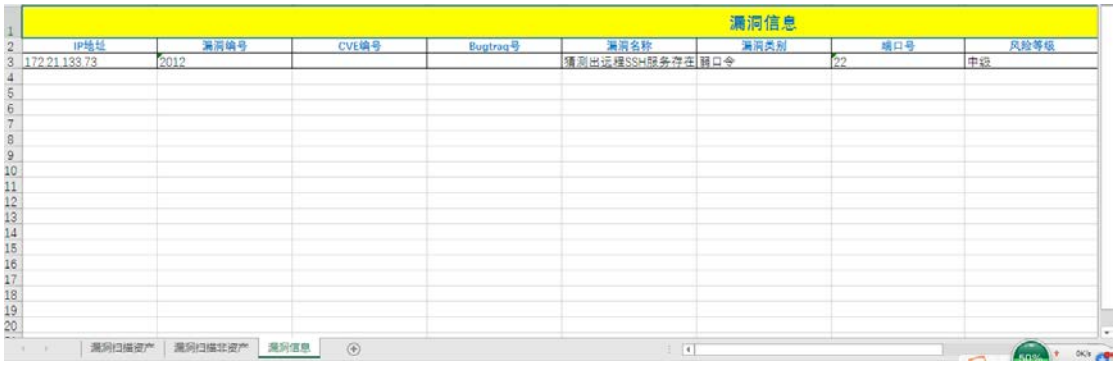
- **结果查看**

点击 结果查看 按钮，弹出弱口令结果查看详情界面，如图：

- **漏洞结果导出**

（1）在任务列表界面操作栏，点击 导出 按钮，导出漏洞结果详情，导出

文件分别展示“漏洞扫描字段”、“漏洞扫描非资产”、“漏洞信息”，如图：



（2）在漏洞结果查看界面，点击 

按钮，导出漏洞详情数据，如图：

- 用户可通过在查询条件区域输入关键字，点击 

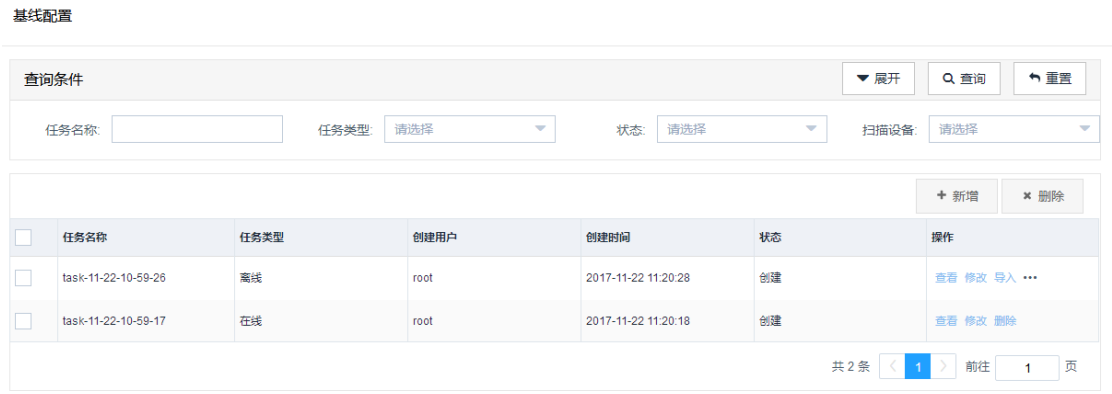
按钮，筛选查询结果，默认显示 4 个查询条件，点击 

按钮，可查看更多条件，或收起查询条件；点击 

按钮，可清空查询条件内容，并自动加载列表结果。

2.4.4 基线配置

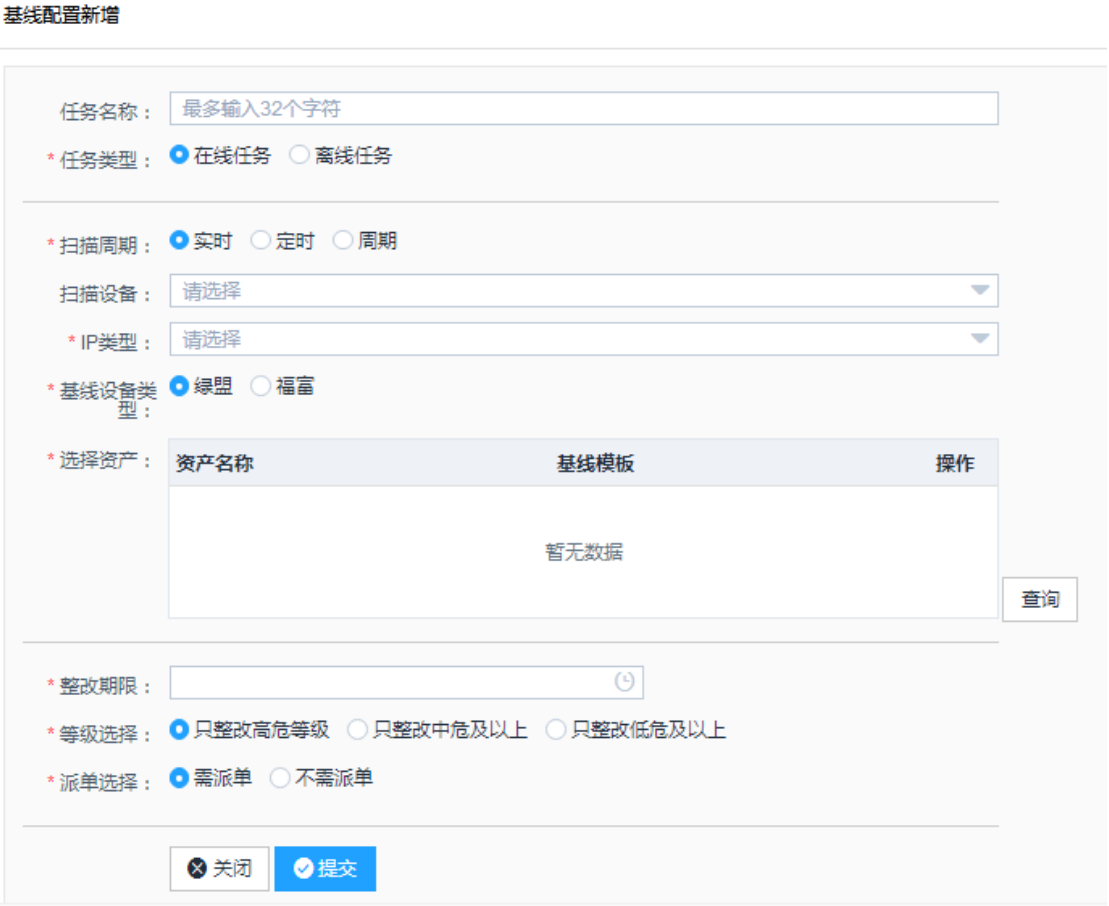
点击菜单“任务管理”=>“基线配置”，进入基线配置任务配置界面，如图：



- **任务下发**

点击“新增”按钮，用户可选择创建在线任务或离线任务，根据选择的不同任务类型联动展示不同字段属性，*号标识为必填字段；

（1）在线任务，如图：



扫描设备：下拉框展示所有弱口令扫描设备，（基础数据可在系统配置->扫描器配置添加）；

扫描策略：选择扫描器策略；

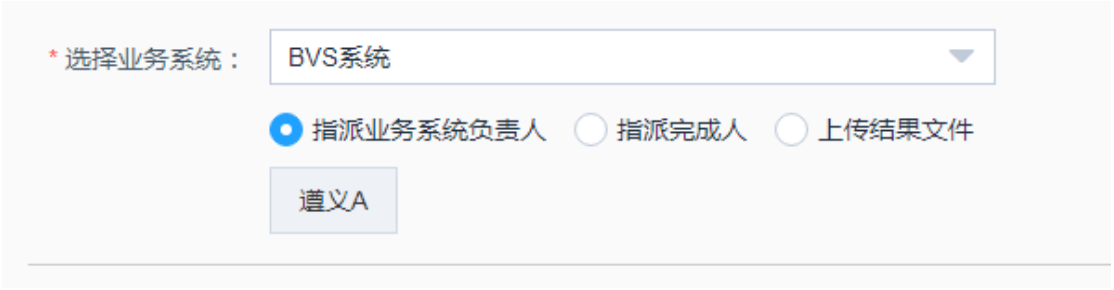
IP 类型：根据选择的扫描设备联动展示扫描器所支持的网段类型；

等级选择：选择整改的漏洞等级；

信息填写完成后，点击“提交”即可。

（2）离线任务，如图：

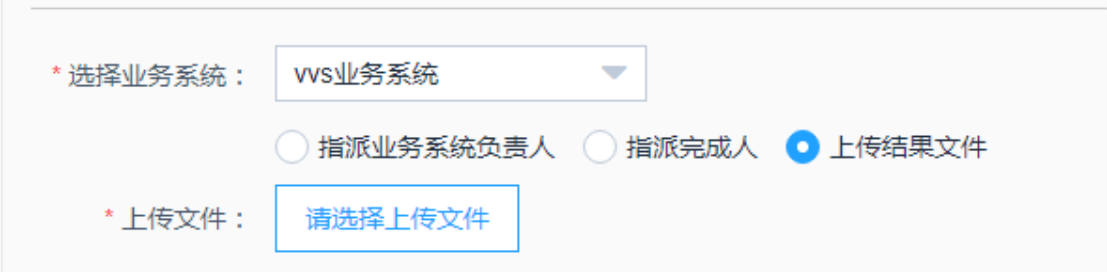
用户分别可选择业务系统责任人、指派完成人、或直接导入离线结果文件来完成任务，如图：



① 指派业务系统负责任人：该任务只能由业务系统的默认责任人来完成离线结果文件导入；

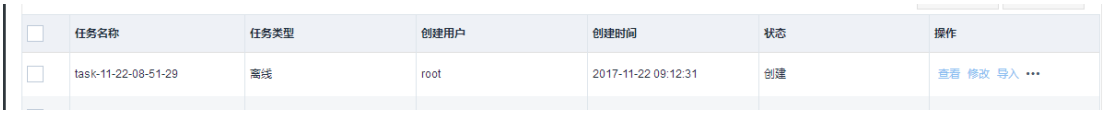
② 指派完成人：创建人可指派任一 SOC 用户来完成任务；

③ 上传结果文件：创建用户可直接导入漏扫结果文件，如图：



信息填写完成，点击提交按钮即可。

④ 若离线任务选择指派业务系统责任人或指派完成人，则任务列表对应任务操作按钮有个“导入”按钮，操作同③；如图：



点击“导入”按钮，弹出导入界面，用户可导入漏扫结果文件，如图：

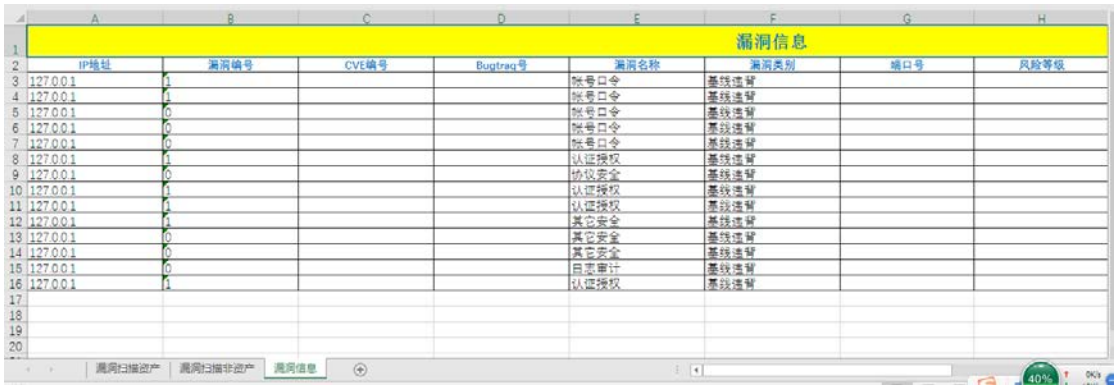
- **结果查看**

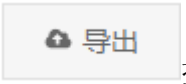
点击 结果查看 按钮，进入基线配置结果查看详情界面，如图：

- **漏洞结果导出**

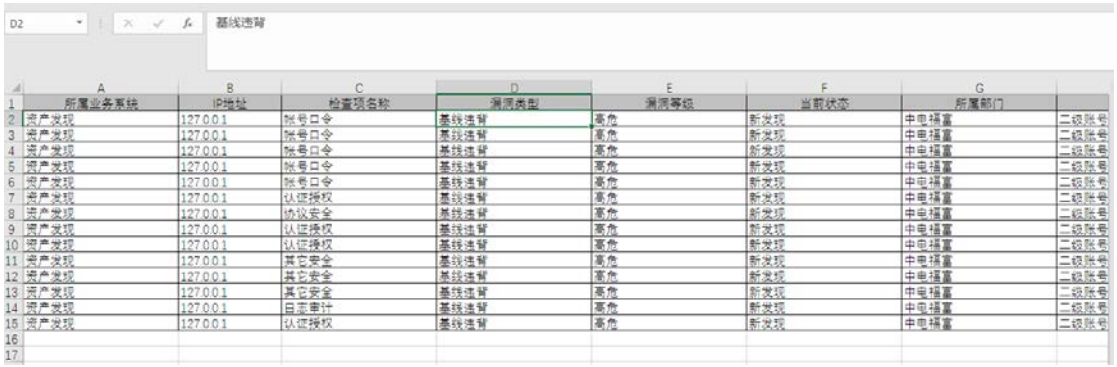
（1）在任务列表界面操作栏，点击 导出 按钮，导出漏洞结果详情，导出

文件分别展示“漏洞扫描字段”、“漏洞扫描非资产”、“漏洞信息”，如图：



（2）在漏洞结果查看界面，点击 

按钮，导出漏洞详情数据，如图：



- 用户可通过在查询条件区域输入关键字，点击 

按钮，筛选查询结果，默认显示 4 个查询条件，点击 

按钮，可查看更多条件，或收起查询条件；点击 

按钮，可清空查询条件内容，并自动加载列表结果。

2.4.5 人工渗透

点击菜单“任务管理”=>“人工渗透”，进入人工渗透任务配置界面，如图：

- 点击“新增”，弹出人工渗透新增界面，*号为必填项，如图：

信息填写完成后，点击提交按钮即可；

- 用户可通过点击“查看”、“修改”、“删除”按钮，对人工渗透数据进行操作；
- 用户可通过在查询条件区域输入关键字，点击 

按钮，筛选查询结果，默认显示 4 个查询条件，点击 

按钮，可查看更多条件，或收起查询条件；点击 

按钮，可清空查询条件内容，并自动加载列表结果。

2.4.6 预警任务

点击菜单“任务管理”=>“预警任务”，进入预警任务配置界面，如图：

- 点击“新增”按钮，弹出预警任务添加界面，如图：

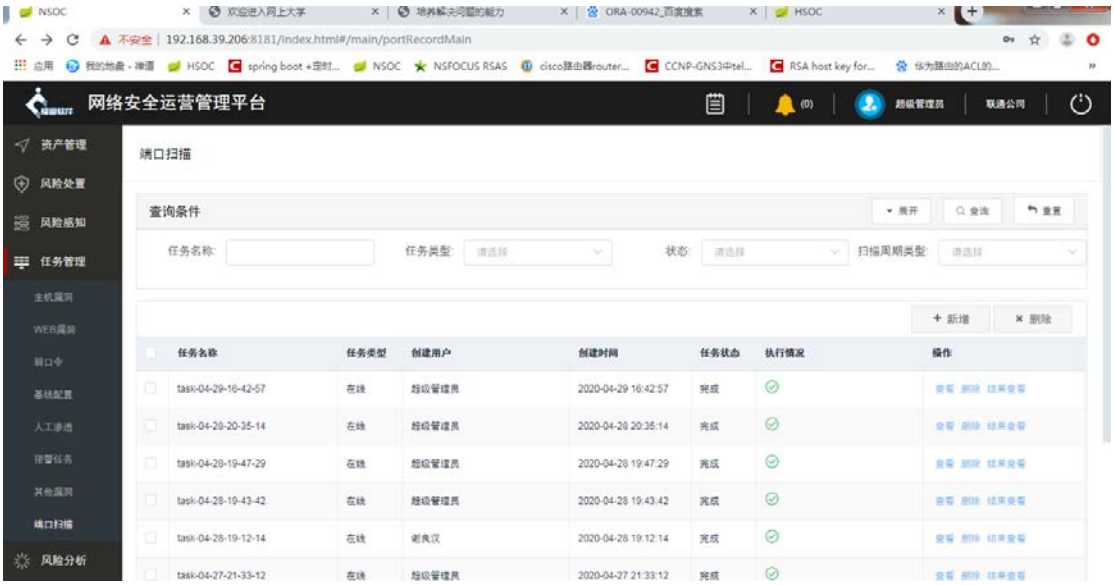
信息填写完成后，点击提交即可；

- 点击 结果查看 按钮，进入预警任务结果查看界面，如图：

- 用户可通过点击“查看”、“修改”、“删除”按钮，对预警任务进行操作；
- 用户可通过在查询条件区域输入关键字，点击 查询 按钮，筛选查询结果，默认显示 4 个查询条件，点击 展开 按钮，可查看更多条件，或收起查询条件；点击 重置 按钮，可清空查询条件内容，并自动加载列表结果。

2.4.7 端口扫描

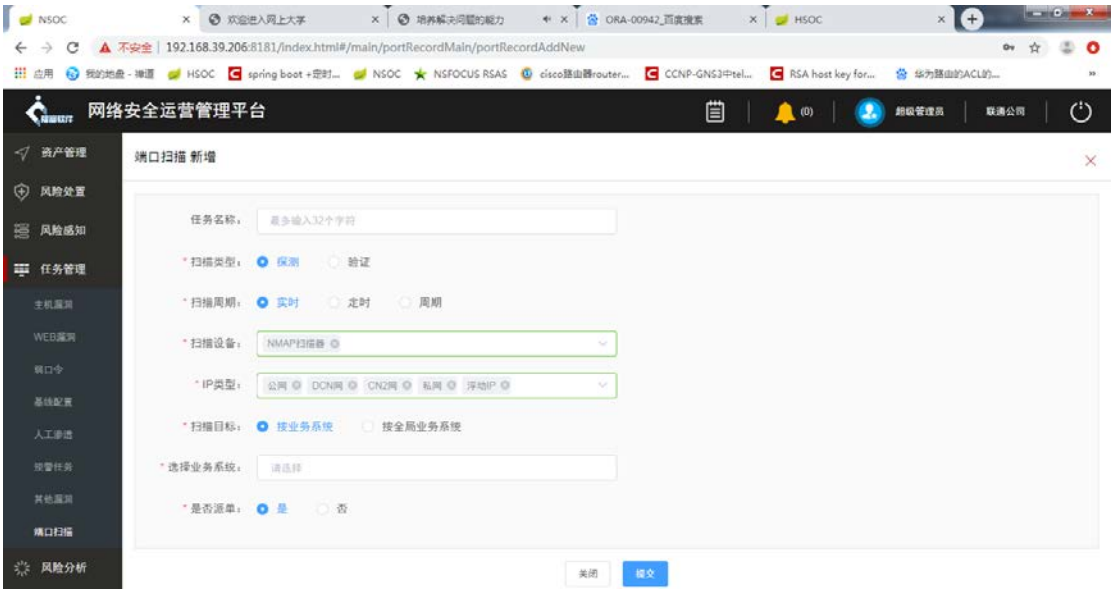
任务管理-端口扫描下，可进行端口探测或者端口验证任务的增删查与结果查看，其中探测任务借用 NMAP 扫描器进行扫描并且新增或者更新端口到端口管理，端口验证通过 TELNET 进行端口的验证并且更新端口状态到端口管理，结果查看可查看到本次涉及的扫描器所扫描出来的全量端口数据。



2.4.7.1 探测任务

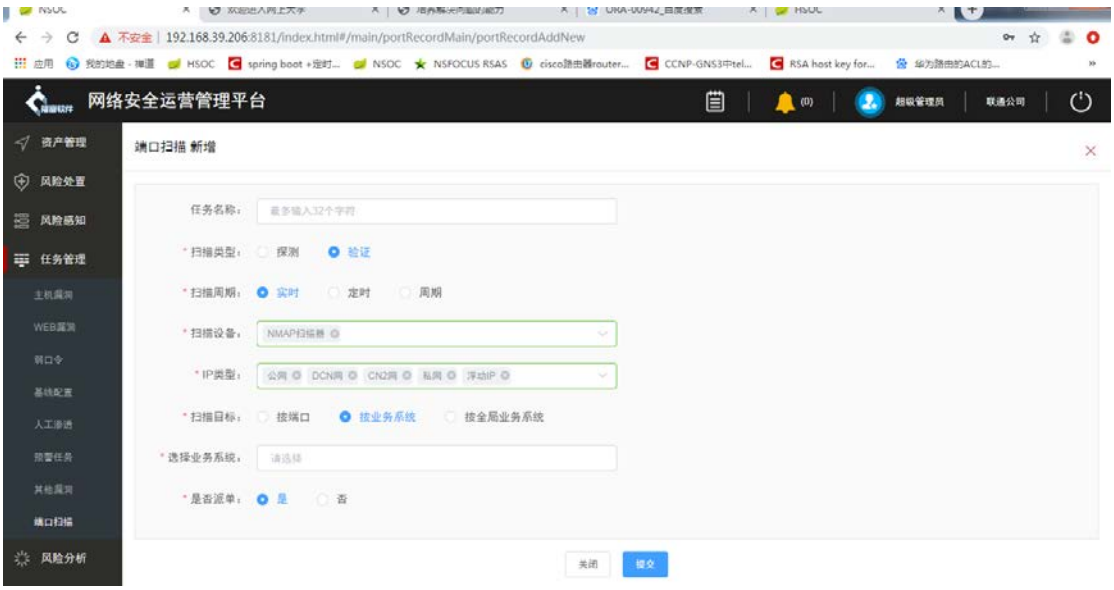
探测任务可按业务系统维度进行下发，探测该业务系统下所有资产 IP 的端口开放情况，探测任务分为两步，第一步是开放端口的探测，第二步是 BANER 信息、服务名以及版本号的采集，由于 BANNER 信息以及版本号扫描较花时间，后端会对本次扫描出来的开放端口数据进行入库的操作，再这之后再进行 BANNER 信息及版本号的扫描，扫描的数据可以在任务管理-结果查看下进行查看，展示本次探测出来的 OPEN 端口数据。

注：数据入库到端口管理，会将本次涉及 IP 所对应的未扫描到的端口状态置为 CLOSE



2.4.7.2 验证任务

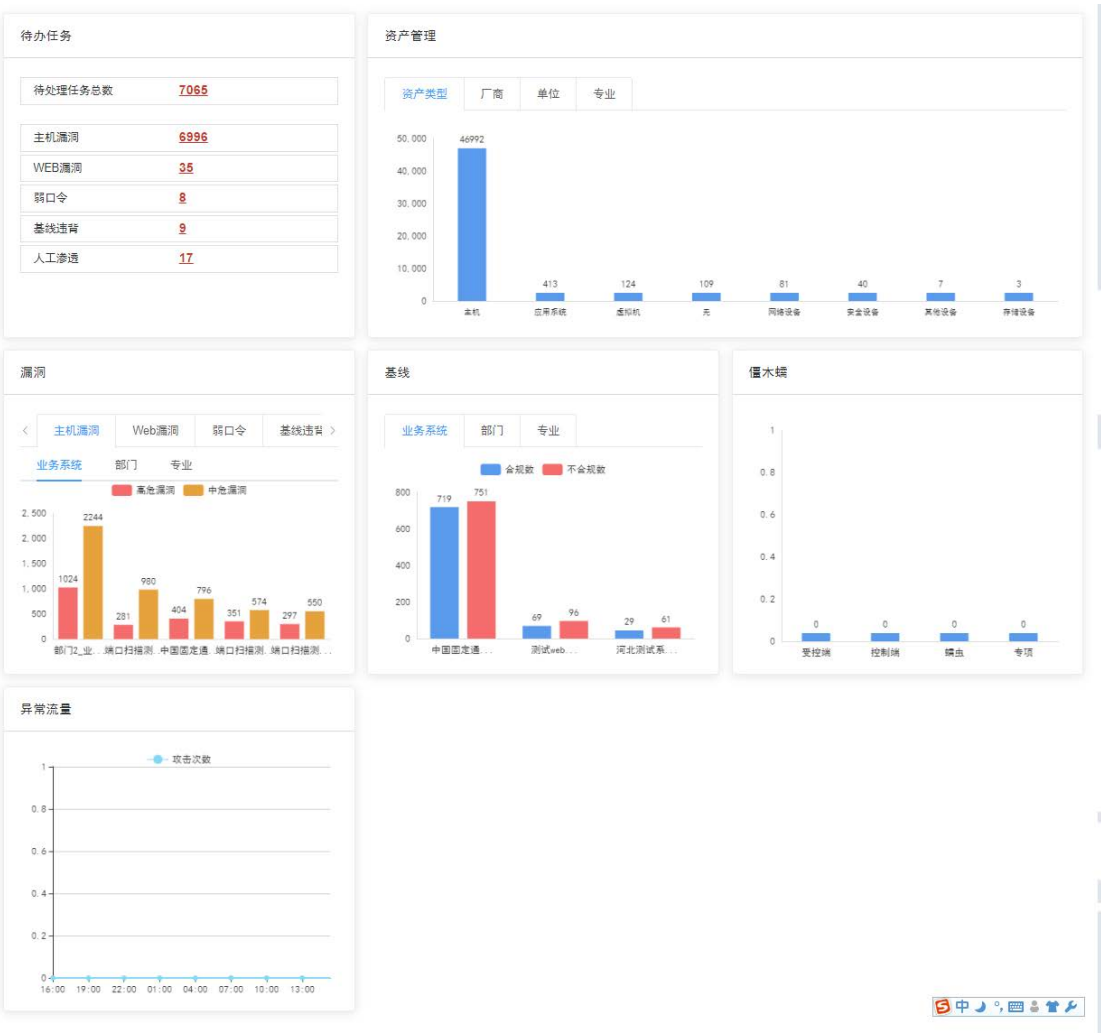
验证任务可按端口维度以及业务系统维度进行任务的下发，验证任务是通过 TELNET 对端口进行 OPEN 或者 CLOSE 的验证。



2.5 风险处置

2.5.1 风险处置首页

点击左侧一级菜单“风险处置”，进入风险处置首页，如图：



- **漏洞统计模块**

  本模块主要展示待处理状态漏洞信息，左侧统计不同漏洞类型待处理漏洞数，并按漏洞数量降序排列，右侧展示最新发现的 7 条漏洞详情，并通过不同颜色标注低、中、高危漏洞，如图：

（1）鼠标点击左上角待处理漏洞总数，页面跳转至漏洞处置详情页面，默认跳转至主机漏洞页面；

（2）鼠标分别点击不同类型漏洞数，页面跳转至对应漏洞处置详情页面；

（3）鼠标点击详情列表 处理 按钮，跳转至该条漏洞处置界面，如图：

- **告警处置模块**

本模块统计平台产生的告警数量，鼠标点击 0 ，跳转至告警处置详情界面，默认跳转至关联告警界面；点击 查看更多 按钮，页面跳转至对应告警类型详情界面，如图：

- **僵木蠕处置模块**

本模块主要统计僵木蠕信息，如图：

（1）鼠标点击图上数字区域，页面跳转至僵木蠕处置详情界面；

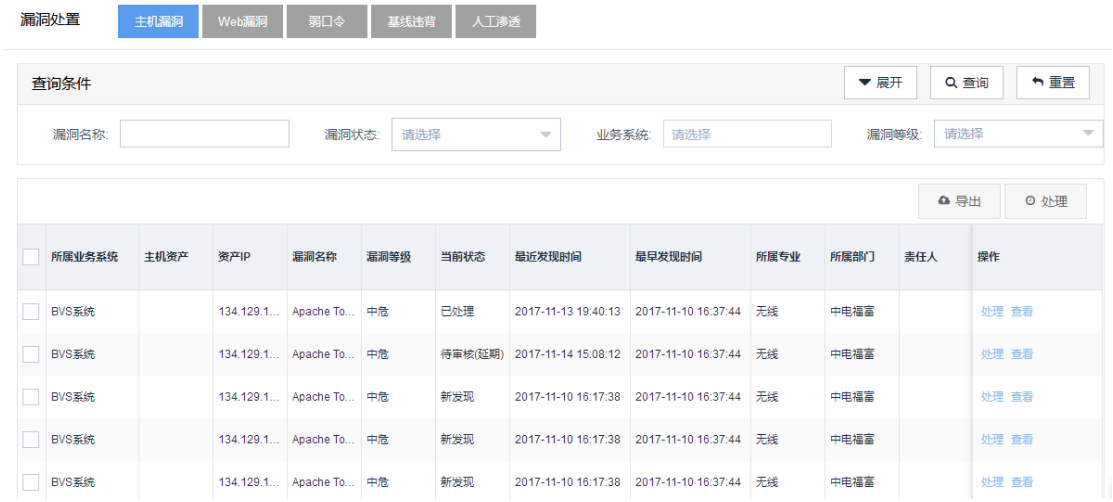
（2）点击 派发 按钮，弹出僵木儒派发界面；

（3）点击 反馈 按钮，弹出僵木儒反馈界面；

2.5.2 漏洞处置

2.5.2.1 主机漏洞

点击菜单“风险处置”=>“漏洞处置”，默认进入主机漏洞处置界面，如图：



- **主机漏洞处置**

处理用户点击 处理 按钮，进入漏洞处置界面，如图：

点击基本信息 sheet 

按钮，页面跳转至漏洞详情页面，记录漏洞详细信息，和漏洞的溯源记录；点击右上角关闭按钮，回到上

一级目录，如图：

处置流程 sheet 根据用户选择的不同处理节点联动展示：

（1）已处理，*号标识为必填项，用户根据实际选择填写信息，点击“提交”按钮即可，漏洞状态变更为“已处理”，该节点不需要审核流程，直接完成，如图：

（2）申请误报，*号为必填标识，页面含有格式说明，填写完成，点击提交，漏洞状态变更为“待审核（误报）”，进入审核流程；如图：

（3）申请延期，*号为必填项，填写完后点击提交，漏洞状态变更为“待审核（延期）”，进入审核流程，如图：

（4）申请不处理，用户填写不处理申请说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（不可关停））”进入审核流程，如图：

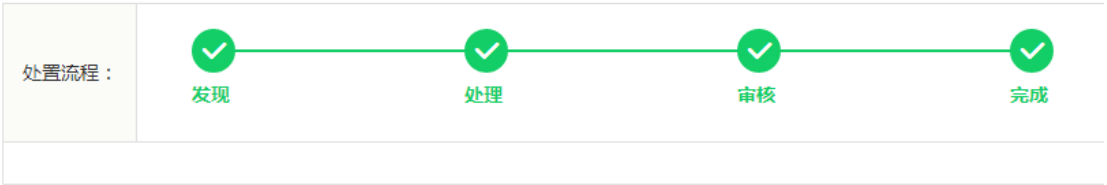
（5）申请可关停，用户填写可关停说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（可关停））”进入审核流程，如图：

- **主机漏洞审核**

审核员点击“处理”按钮，进入漏洞审核界面，如图：

（1）待审核（误报），审核员根据实际选择是否通过误报申请，点击提交即可，如图：

① 若选择“审查通过”，则该漏洞状态变更为“误报”，流程结束；



② 若选择“审查拒绝”，则该漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

③ 右侧“历史记录”，鼠标点击误报材料名称，可下载误报材料；

（2）待审核（延期），审核员根据实际选择是否通过延期申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“暂不处理”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（3）待审核（无法处理（不可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（不可关停）”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（4）待审核（无法处理（可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（可关停）”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

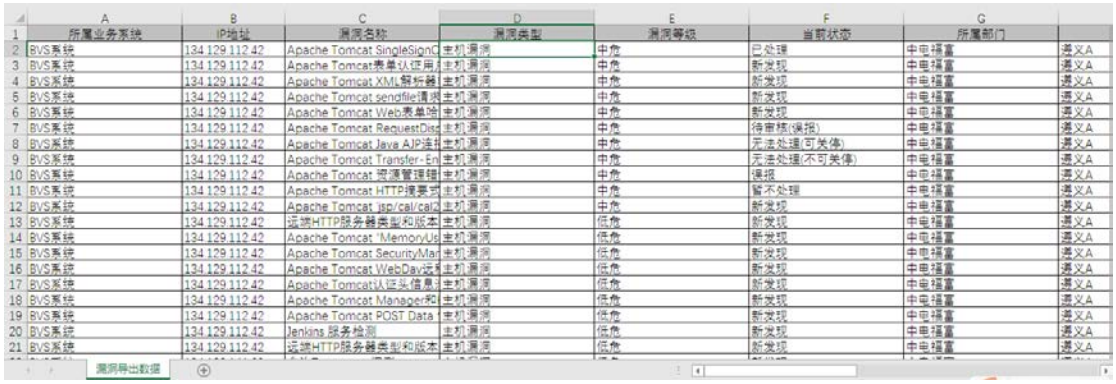
- **漏洞查看**

点击 查看 按钮，弹出漏洞详细信息界面，如图：

- **漏洞导出**

点击 

按钮，导出漏洞数据，如图：



2.5.2.2 WEB 漏洞

点击菜单“风险处置”=>“漏洞处置”=>WEB 漏洞，进入 WEB 漏洞处置界面，如图：

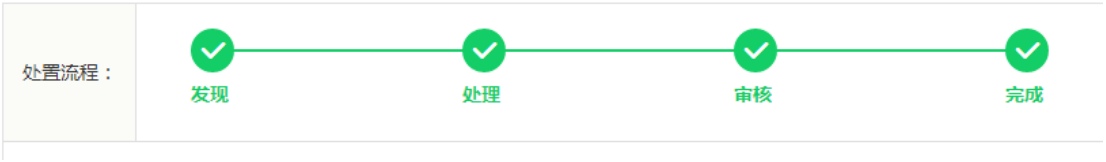
- **WEB 漏洞处置**

处理用户点击 处理 按钮，进入漏洞处置界面，如图：

点击基本信息 sheet 更多 按钮，页面跳转至漏洞详情页面，记录漏洞详细信息、受影响链接、漏洞的溯源记录；点击右上角关闭按钮，回到上一级目录，如图：

处置流程 sheet 根据用户选择的不同处理节点联动展示：

（1）已处理，*号标识为必填项，用户根据实际选择填写信息，点击“提交”按钮即可，漏洞状态变更为“已处理”，该节点不需要审核流程，直接完成，如图：



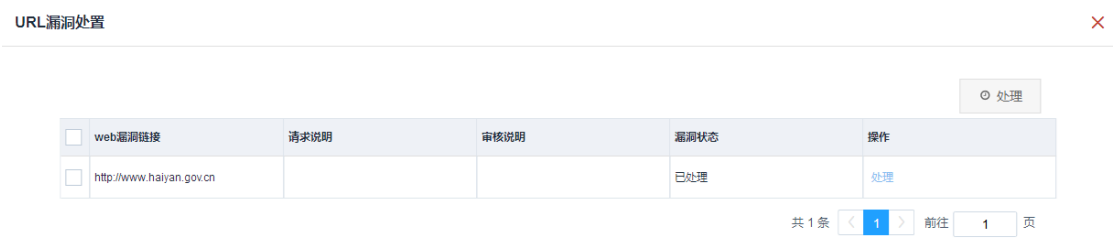
（2）申请误报，*号为必填标识，页面含有格式说明，填写完成，点击提交，漏洞状态变更为“待审核（误报）”，进入审核流程；如图：

（3）申请延期，*号为必填项，填写完后点击提交，漏洞状态变更为“待审核（延期）”，进入审核流程，如图：

（4）申请不处理，用户填写不处理申请说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（不可关停））”进入审核流程，如图：

（5）申请可关停，用户填写可关停说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（可关停））”进入审核流程，如图：

- 处理用户点击 处置子URL 按钮，弹出子 URL 链接界面，如图：



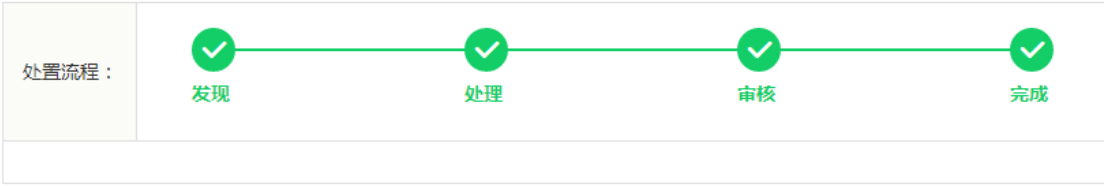
点击“处理”按钮，流程同上操作一致；

- **WEB 漏洞审核**

审核员点击“处理”按钮，进入漏洞审核界面，如图：

（1）待审核（误报），审核员根据实际选择是否通过误报申请，点击提交即可，如图：

① 若选择“审查通过”，则该漏洞状态变更为“误报”，流程结束；



② 若选择“审查拒绝”，则该漏洞状态变更为“新发现/未整改”，流程

退回至处理用户；

③ 右侧“历史记录”，鼠标点击误报材料名称，可下载误报材料。

（2）待审核（延期），审核员根据实际选择是否通过延期申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“暂不处理”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（3）待审核（无法处理（不可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（不可关停）”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（4）待审核（无法处理（可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（可关停）”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

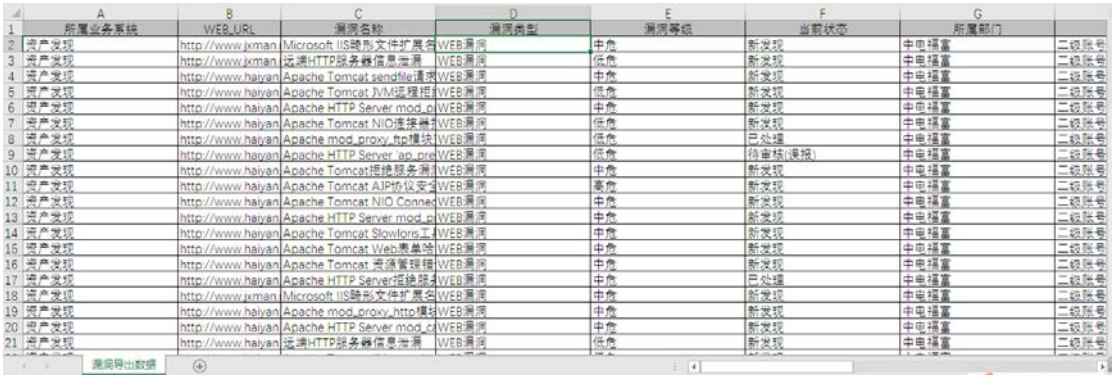
- **漏洞查看**

点击 查看 按钮，弹出漏洞详细信息界面，如图：

- **漏洞导出**

点击 

按钮，导出漏洞数据，如图：



2.5.2.3 弱口令

点击菜单“风险处置”=>“漏洞处置”=>“弱口令”，进入弱口令处置界面，如图：

- **弱口令处置**

处理用户点击 

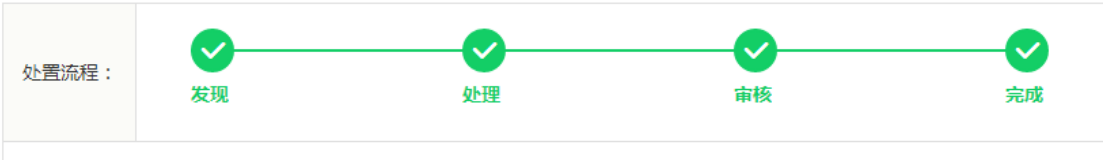
按钮，进入漏洞处置界面，如图：

点击基本信息 sheet 

按钮，页面跳转至漏洞详情页面，记录漏洞详细信息，和漏洞的溯源记录；点击右上角关闭按钮，回到上一级目录，如图:

处置流程 sheet 根据用户选择的不同处理节点联动展示：

（1）已处理，*号标识为必填项，用户根据实际选择填写信息，点击“提交”按钮即可，漏洞状态变更为“已处理”，该节点不需要审核流程，直接完成，如图：



（2）申请误报，*号为必填标识，页面含有格式说明，填写完成，点击提交，漏洞状态变更为“待审核（误报）”，进入审核流程；如图：

（3）申请延期，*号为必填项，填写完后点击提交，漏洞状态变更为“待审核（延期）”，进入审核流程，如图：

（4）申请不处理，用户填写不处理申请说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（不可关停））”进入审核流程，如图：

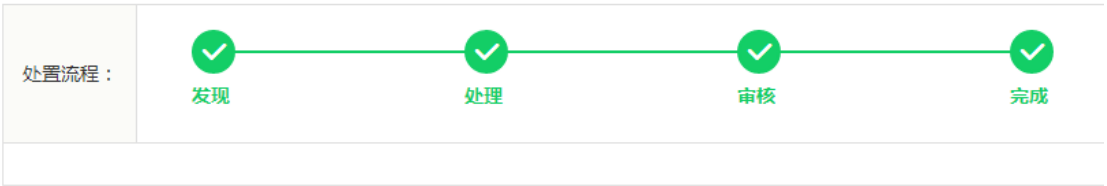
（5）申请可关停，用户填写可关停说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（可关停））”进入审核流程，如图：

- **WEB 漏洞审核**

审核员点击“处理”按钮，进入漏洞审核界面，如图：

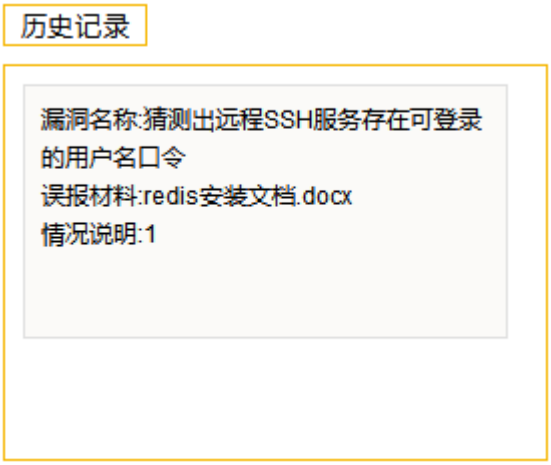
（1）待审核（误报），审核员根据实际选择是否通过误报申请，点击提交即可，如图：

① 若选择“审查通过”，则该漏洞状态变更为“误报”，流程结束；



② 若选择“审查拒绝”，则该漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

③ 右侧“历史记录”，鼠标点击误报材料名称，可下载误报材料。



（2）待审核（延期），审核员根据实际选择是否通过延期申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“暂不处理”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（3）待审核（无法处理（不可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（不可关停）”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（4）待审核（无法处理（可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（可关停）”，流程结束；

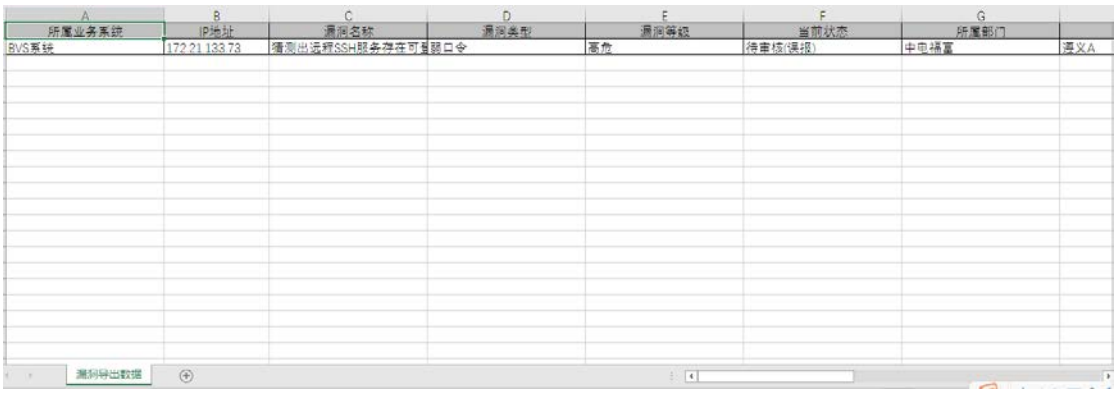
② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

- **漏洞查看**

点击 查看 按钮，弹出漏洞详细信息界面，如图：

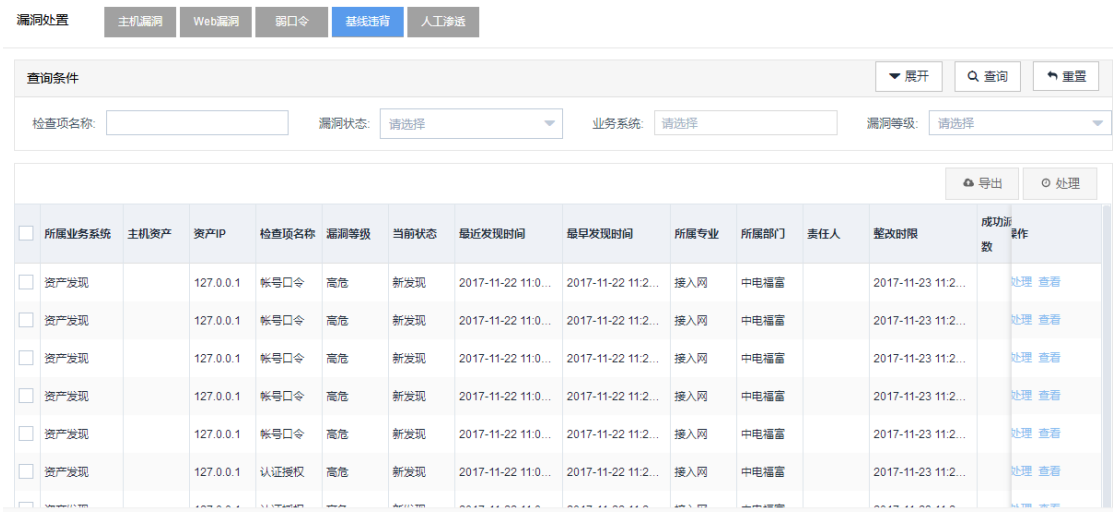
- **漏洞导出**

点击 导出 按钮，导出漏洞数据，如图：



2.5.2.4 基线违背

点击菜单“风险处置”=>“漏洞处置”=>”基线违背”，进入基线违背处置界面，如图：



- **基线违背处置**

处理用户点击 处理 按钮，进入漏洞处置界面，如图：

点击基本信息 sheet 

按钮，页面跳转至漏洞详情页面，记录漏洞详细信息，和漏洞的溯源记录；点击右上角关闭按钮，回到上一级目录，如图：

处置流程 sheet 根据用户选择的不同处理节点联动展示：

（1）已处理，*号标识为必填项，用户根据实际选择填写信息，点击“提交”按钮即可，漏洞状态变更为“已处理”，该节点不需要审核流程，直接完成，如图：

（2）申请误报，*号为必填标识，页面含有格式说明，填写完成，点击提交，漏洞状态变更为“待审核（误报）”，进入审核流程；如图：

（3）申请延期，*号为必填项，填写完后点击提交，漏洞状态变更为“待审核（延期）”，进入审核流程，如图：

（4）申请不处理，用户填写不处理申请说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（不可关停））”进入审核流程，如图：

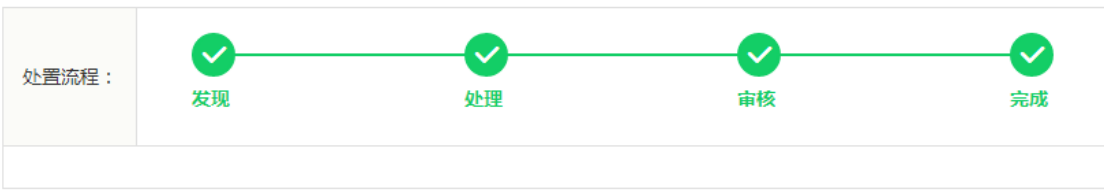
（5）申请可关停，用户填写可关停说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（可关停））”进入审核流程，如图：

- **基线违背审核**

审核员点击“处理”按钮，进入漏洞审核界面，如图：

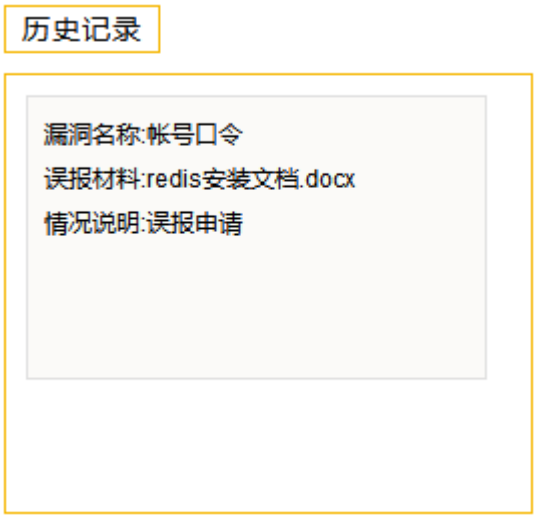
（1）待审核（误报），审核员根据实际选择是否通过误报申请，点击提交即可，如图：

① 若选择“审查通过”，则该漏洞状态变更为“误报”，流程结束；



② 若选择“审查拒绝”，则该漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

③ 右侧“历史记录”，鼠标点击误报材料名称，可下载误报材料；



（2）待审核（延期），审核员根据实际选择是否通过延期申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“暂不处理”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（3）待审核（无法处理（不可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（不可关停）”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（4）待审核（无法处理（可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（可关停）”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

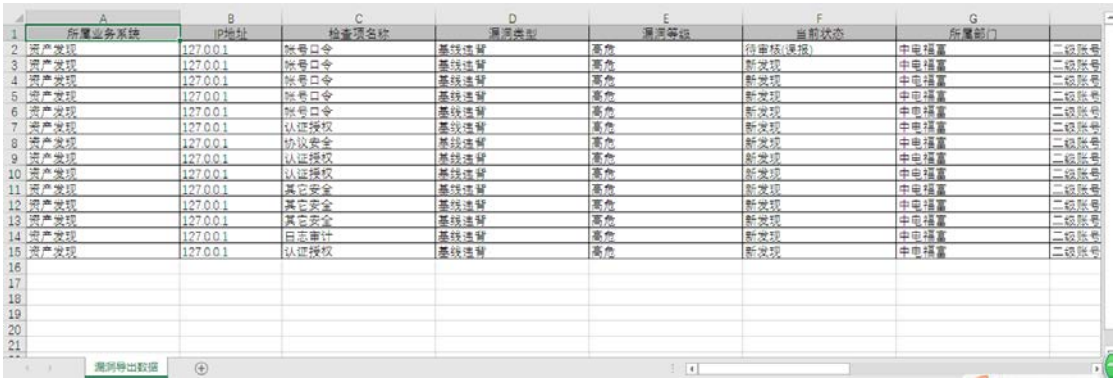
- **漏洞查看**

点击 查看 按钮，弹出漏洞详细信息界面，如图：

- **漏洞导出**

点击 

按钮，导出漏洞数据，如图：



2.5.2.5 人工渗透

点击菜单“风险处置”=>“漏洞处置”=>”人工渗透”，进入人工渗透处置界面，如图：

- **人工渗透处置**

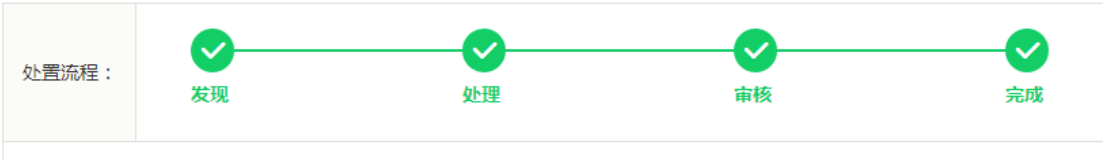
处理用户点击 处理 按钮，进入漏洞处置界面，如图：

点击基本信息 sheet 

按钮，页面跳转至漏洞详情页面，记录漏洞详细信息，和漏洞的溯源记录；点击右上角关闭按钮，回到上一级目录，如图：

处置流程 sheet 根据用户选择的不同处理节点联动展示：

（1）已处理，*号标识为必填项，用户根据实际选择填写信息，点击“提交”按钮即可，漏洞状态变更为“已处理”，该节点不需要审核流程，直接完成，如图：



（2）申请误报，*号为必填标识，页面含有格式说明，填写完成，点击提交，漏洞状态变更为“待审核（误报）”，进入审核流程；如图：

（3）申请延期，*号为必填项，填写完后点击提交，漏洞状态变更为“待审核（延期）”，进入审核流程，如图：

（4）申请不处理，用户填写不处理申请说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（不可关停））”进入审核流程，如图：

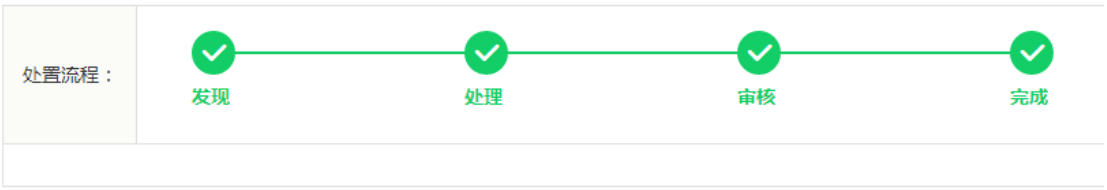
（5）申请可关停，用户填写可关停说明，点击提交按钮，漏洞状态变更为“待审核（无法处理（可关停））”进入审核流程，如图：

- **人工渗透审核**

审核员点击“处理”按钮，进入漏洞审核界面，如图：

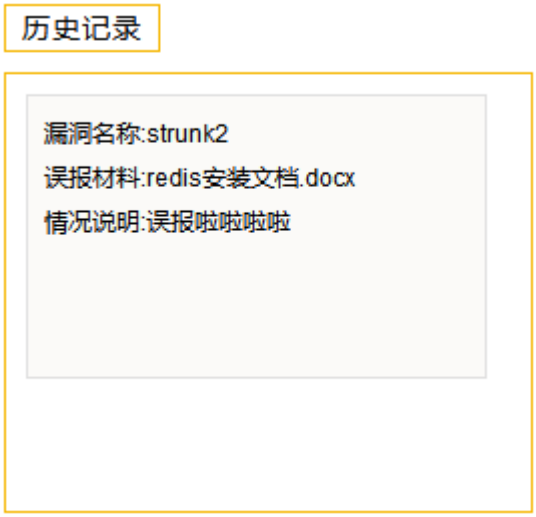
（1）待审核（误报），审核员根据实际选择是否通过误报申请，点击提交即可，如图：

① 若选择“审查通过”，则该漏洞状态变更为“误报”，流程结束；



② 若选择“审查拒绝”，则该漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

③ 右侧“历史记录”，鼠标点击误报材料名称，可下载误报材料。



（2）待审核（延期），审核员根据实际选择是否通过延期申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“暂不处理”，流程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（3）待审核（无法处理（不可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（不可关停）”，流

程结束；

② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

（4）待审核（无法处理（可关停）），审核员根据实际选择是否通过不处理申请，点击提交即可，如图：

① 若选择“审查通过”，漏洞状态变更为“无法处理（可关停）”，流程结束；

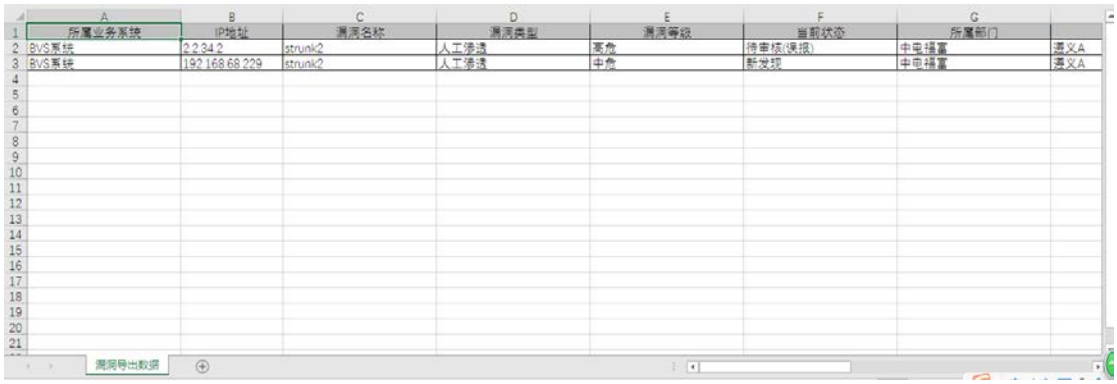
② 若选择“审查拒绝”，则漏洞状态变更为“新发现/未整改”，流程退回至处理用户；

- **漏洞查看**

点击 查看 按钮，弹出漏洞详细信息界面，如图：

- **漏洞导出**

点击 导出 按钮，导出漏洞数据，如图：



	A	B	C	D	E	F	G	
1	所属业务系统	IP地址	漏洞名称	漏洞类型	漏洞等级	当前状态	所属部门	
2	BVS系统	2.2.34.2	strunk2	人工渗透	高危	待审核(误报)	中电福富	满义A
3	BVS系统	192.168.68.229	strunk2	人工渗透	中危	新发现	中电福富	满义A

漏洞导出数据

2.5.3 告警处置

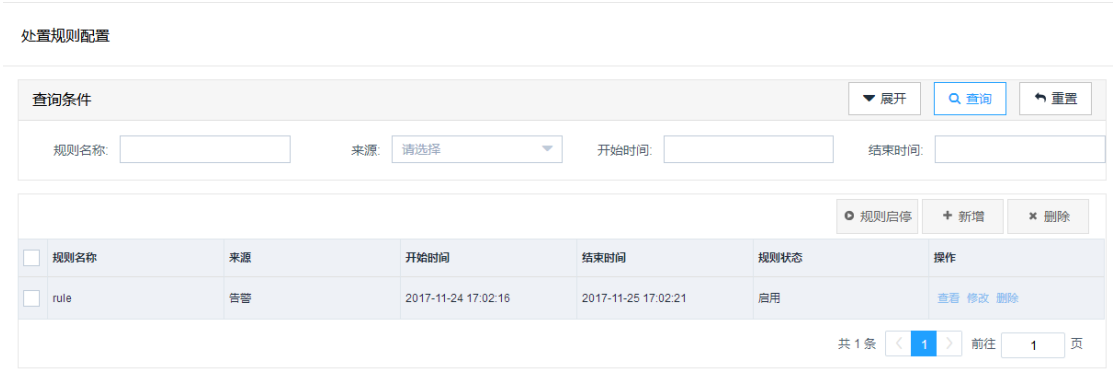
2.5.4 白名单管理

漏洞处置，处理时选择申请误报，审核通过后，这个漏洞就进入白名单

按如下操作步骤：

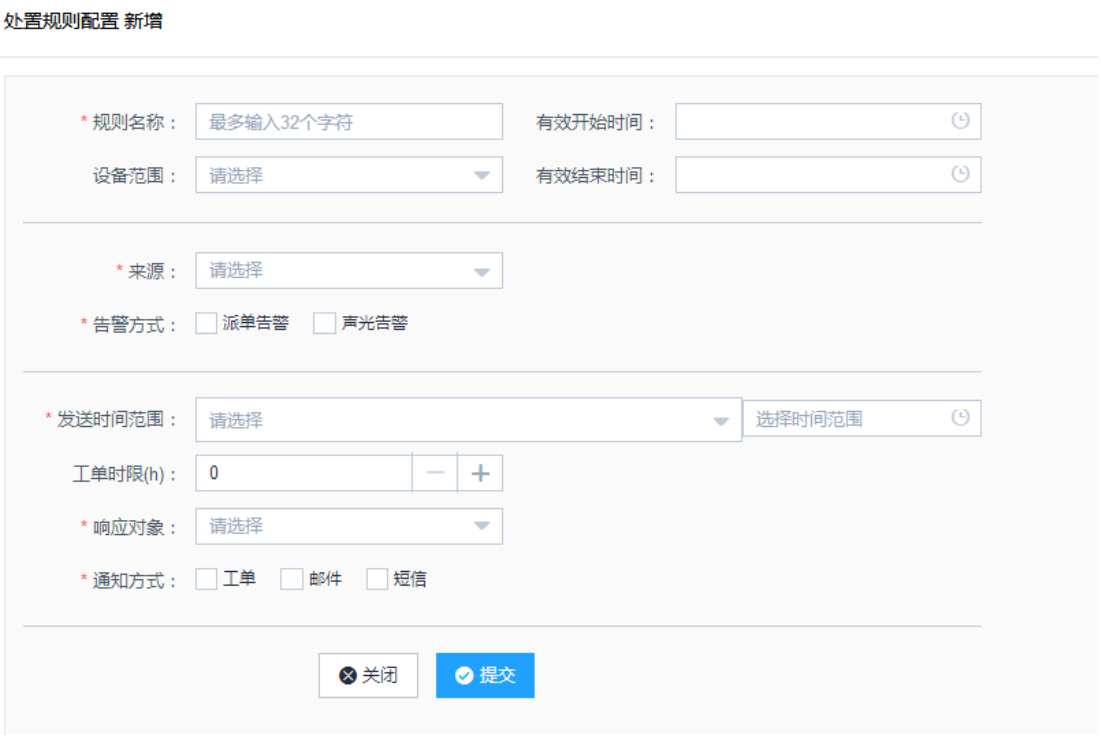
2.5.5 处置规则配置

点击菜单“风险处置”=>“处置规则配置”，进入处置规则配置界面，如图：



- **规则添加**

  点击“新增”按钮，弹出规则新增界面，*号为必填标识，根据选择的不同“来源”联动展示不懂属性；如图：



- **规则启停**

  选择需要更改启停的规则，点击 

按钮，提示规则状态更改成功，如图：

2.5.6 处置通知查询

- 后端根据前端页面设置的处置规则，触发处置规则后，即会派单通知处理人，可在这里查询派单记录。

2.6 风险感知

点击菜单“风险感知”，即进入风险感知页面，如图：

本页面主要记录平台的总体情况，其中包括漏洞统计、安全告警监控、风险评估（按不同维度）、安全预警、安全时间监控（最新 5 个小时）。

2.7 日志审计

2.7.1 日志检索

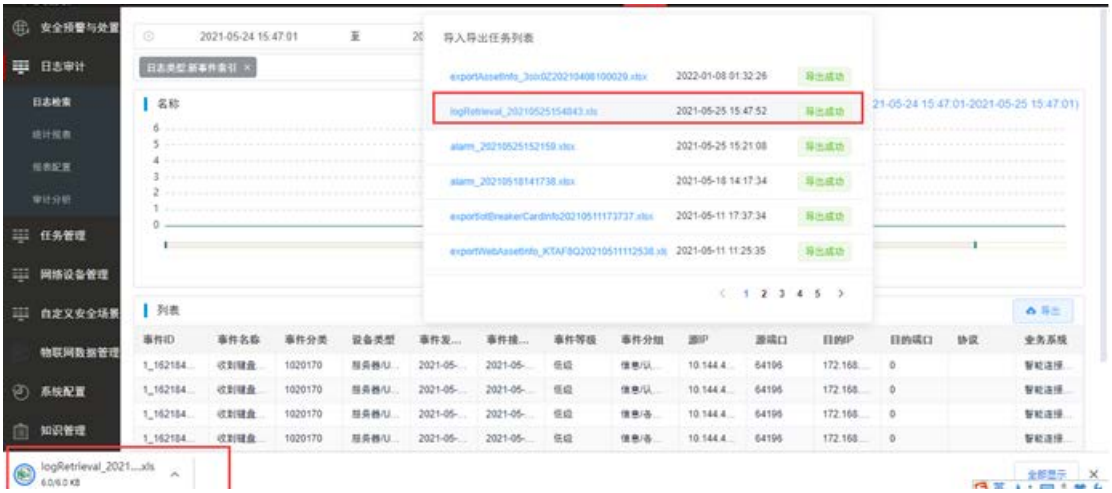
点击左侧主菜单日志审计，默认进入日志检索主界面，如图：

默认查询最近一天的是数据

单机列表某行数据，弹窗展示事件详情信息，根据字段动态加载，只展示有数据的字段。

2.7.1.1 导出

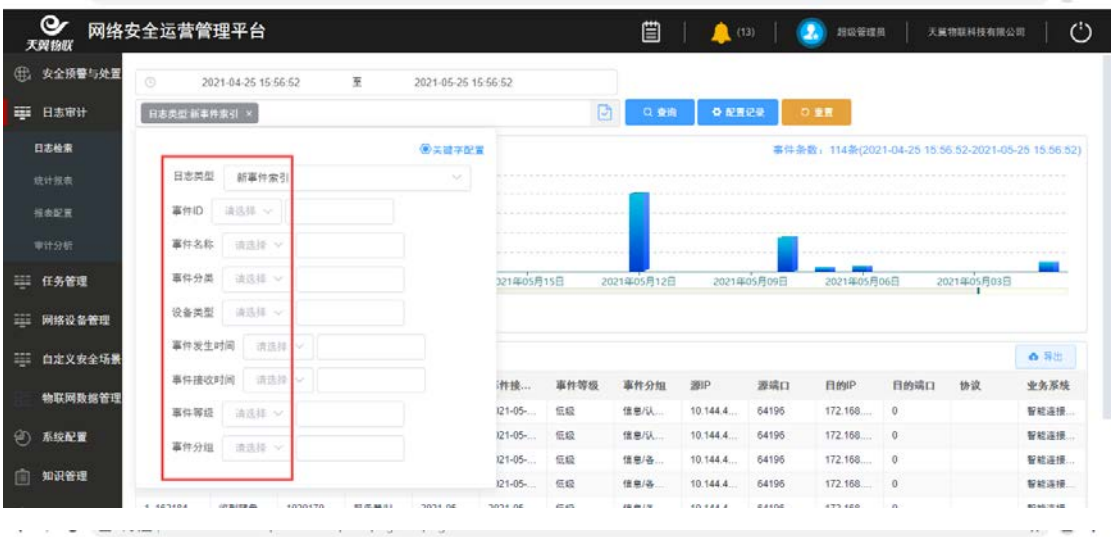
点击导出按钮，加入离线任务，鼠标移入导航栏异步任务窗口，可查看导出是否成功，点击文件名，可下载导出文件。



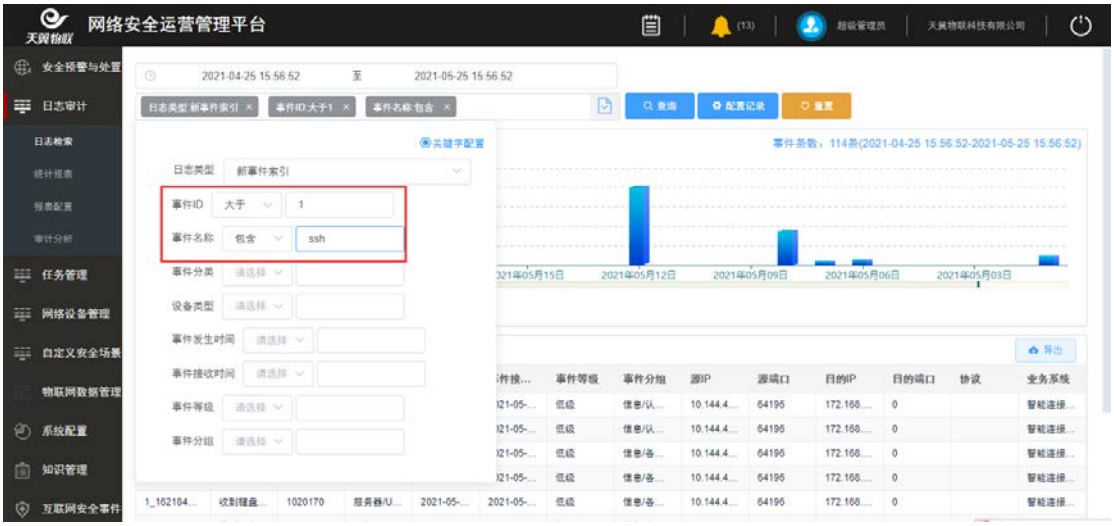
2.7.1.2 查询

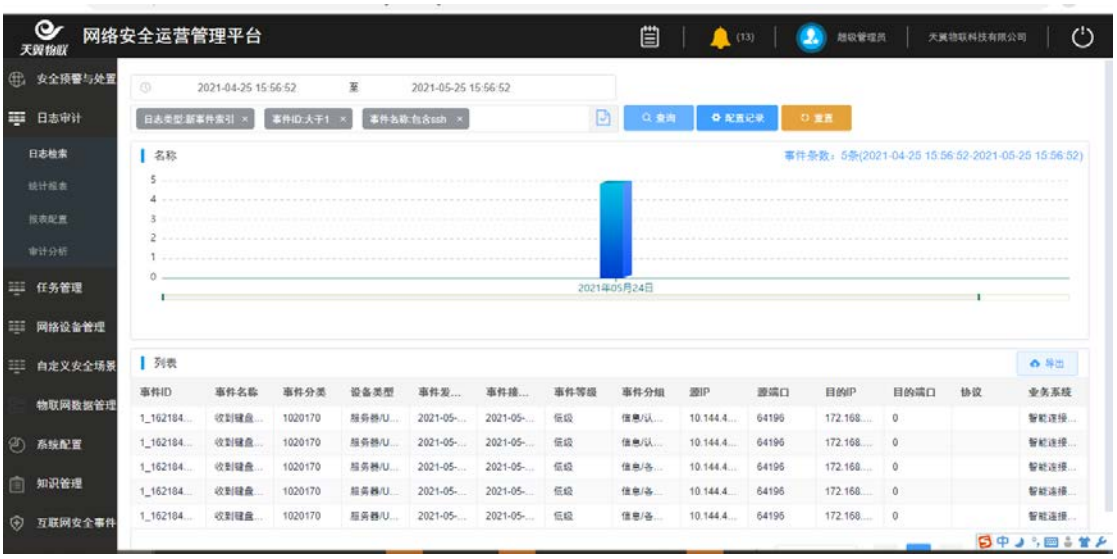
列表默认展示查询列表这些字段，可通过配置关键字调整列表展示的字段，

勾选状态的为当前展示字段，未勾选状态的不展示。

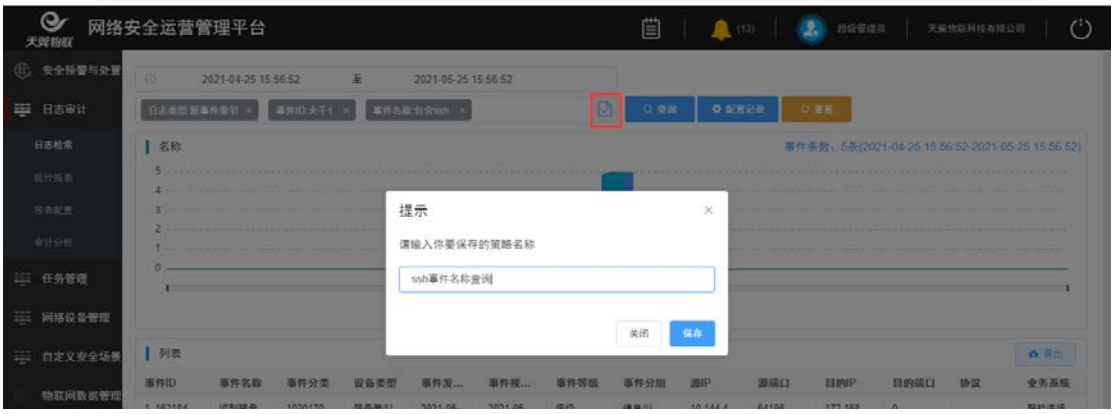


用户可根据需要配置过滤条件，点击查询，根据配置的条件筛选结果。

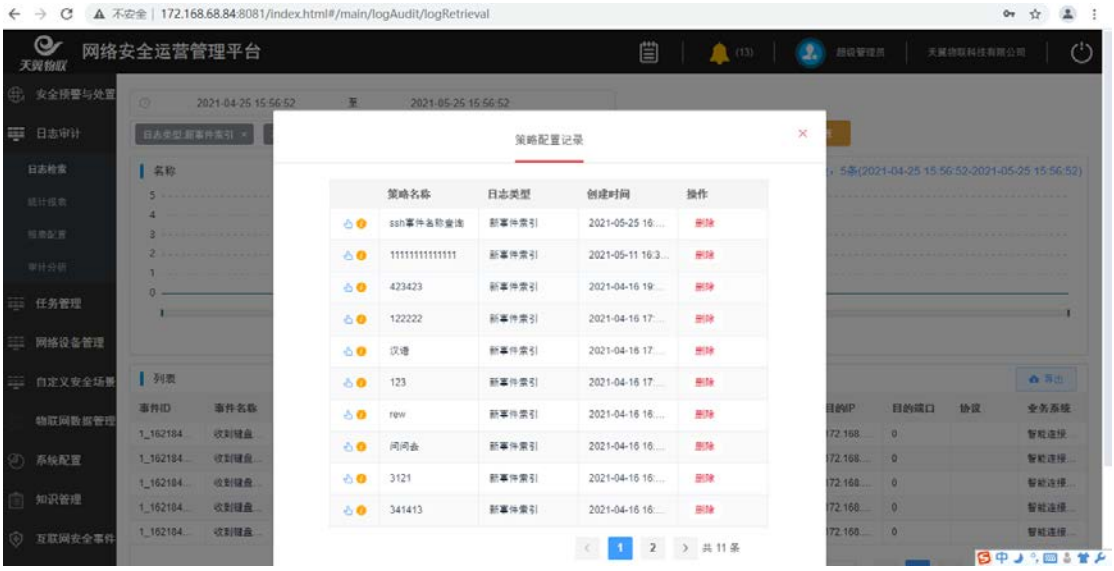




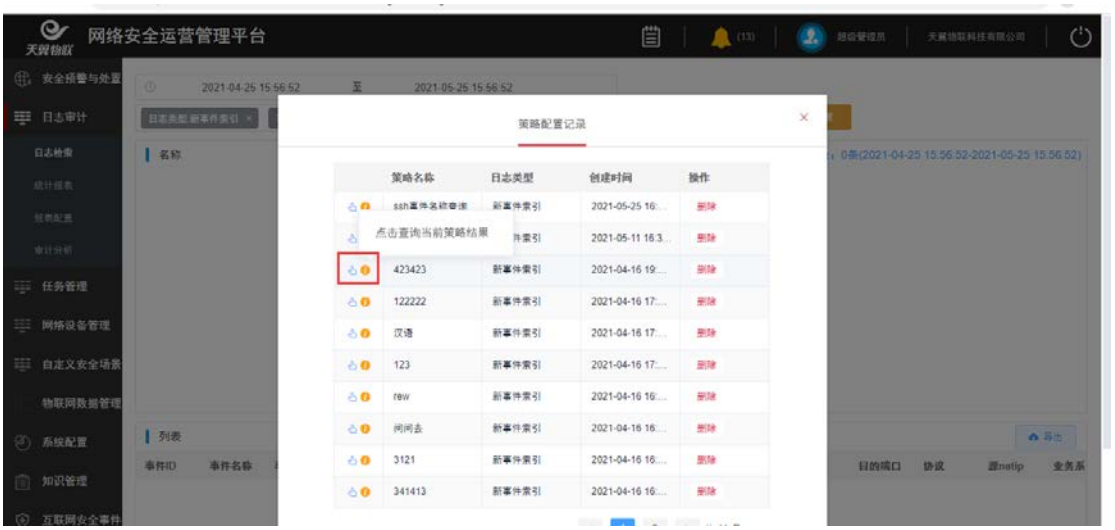
点击如图红框区域，可保存查询条件配置记录，输入名称，保存成功。



点击 配置记录 按钮，可查看配置记录。



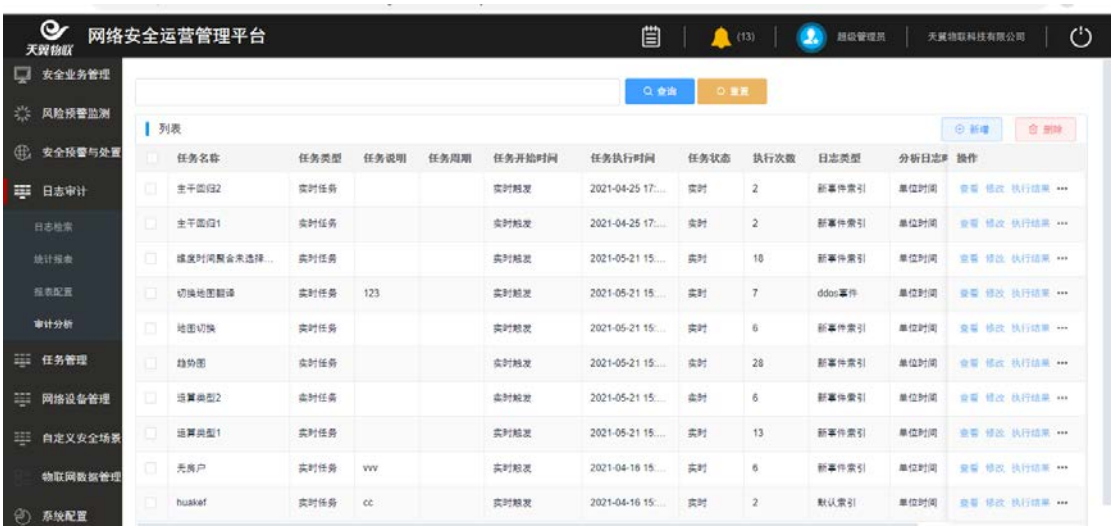
鼠标点击手指，可根据该条配置记录筛选结果。



2.7.2 审计分析

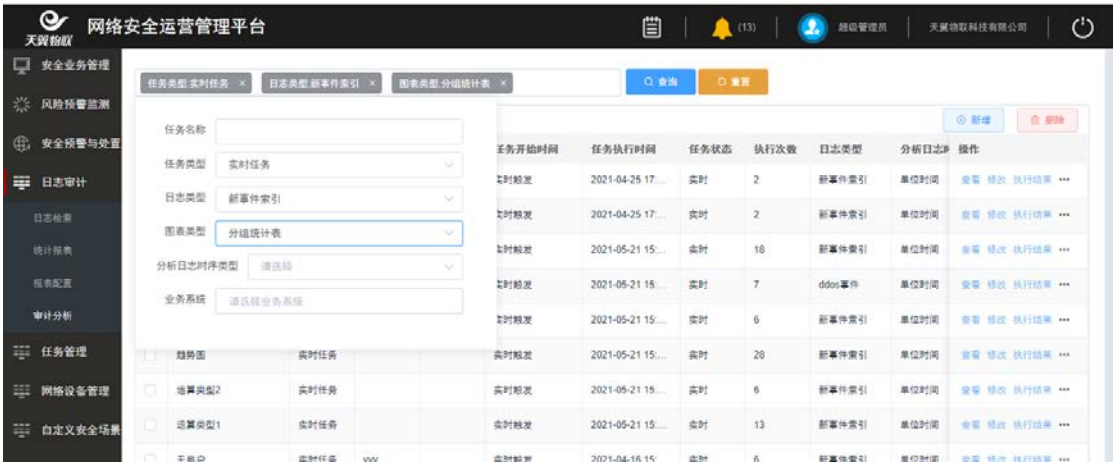
点击左侧主菜单日志审计>>审计分析，进入审计分析主界面，如图：

审计分析数据源为 es 集群上采集的相关日志。



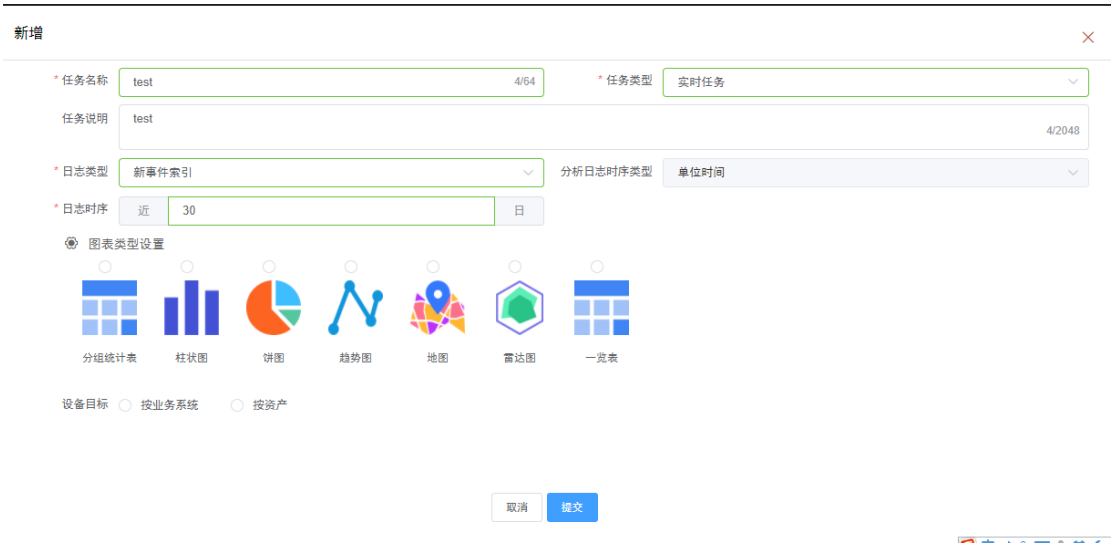
2.7.2.1 查询

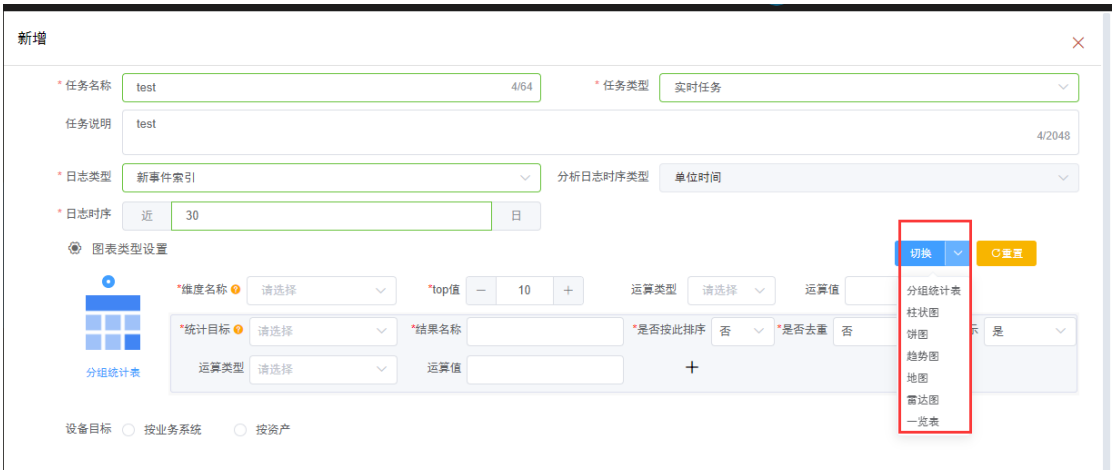
鼠标点击查询框，弹出查询条件，用户根据实际需要输入查询条件，点击查询按钮，根据查询条件筛选出正确结果，点击重置按钮，清空查询条件，并自动重新加载列表数据。

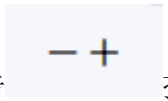


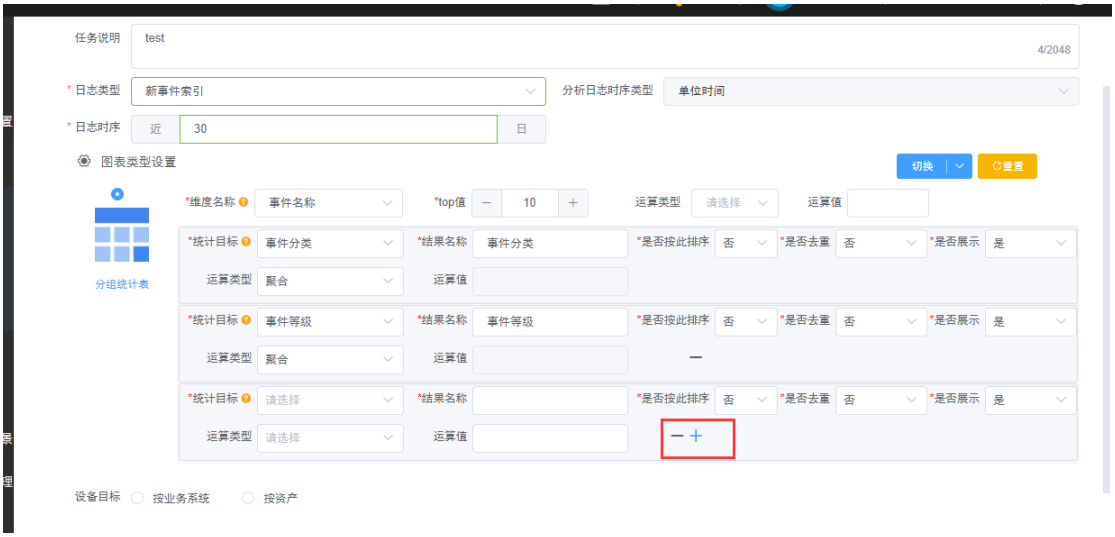
2.7.2.2 新增

点击新增按钮，弹出新增界面，可根据实际需要选择展示的图表类型，并且可进行切换。

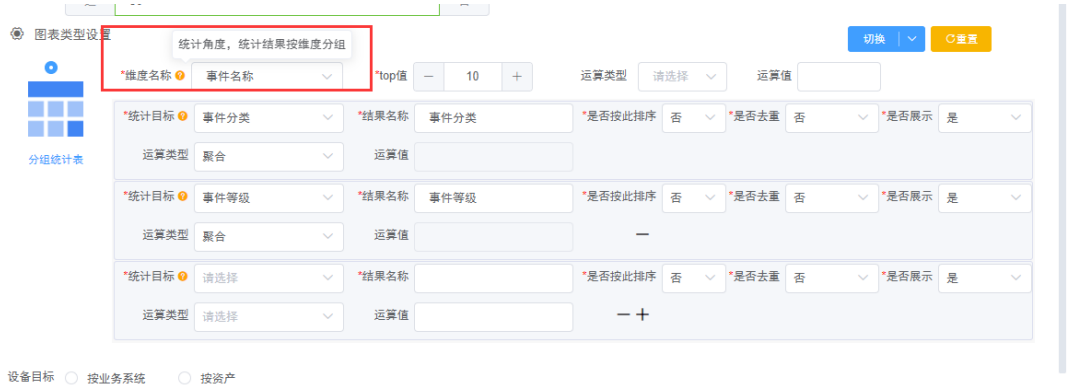




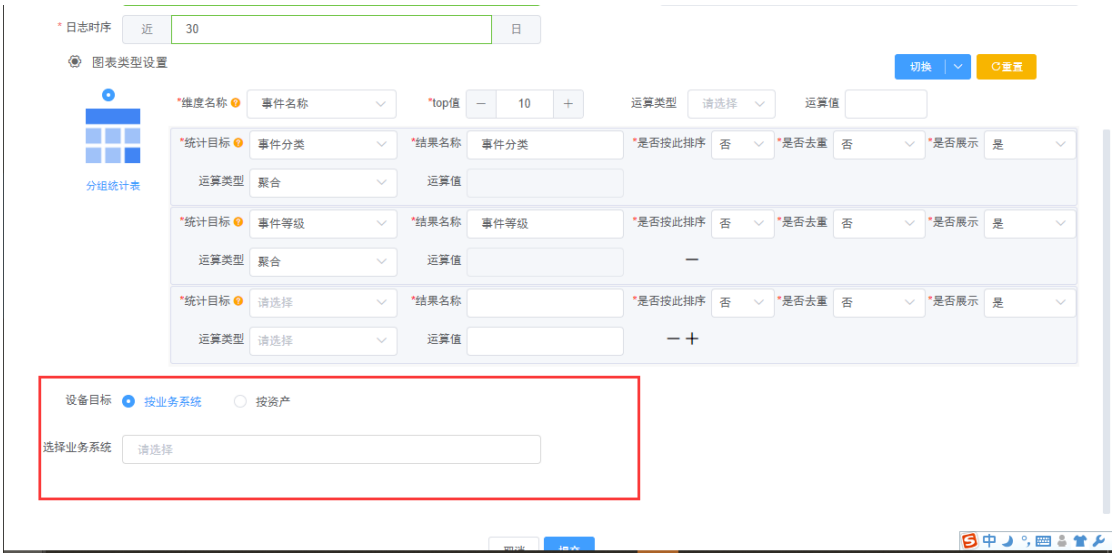
点击  按钮，可删减增加统计目标，鼠标点击某个统计目标行，可进行拖拽，移动统计目标的位置。



鼠标移入?，可查看注释。

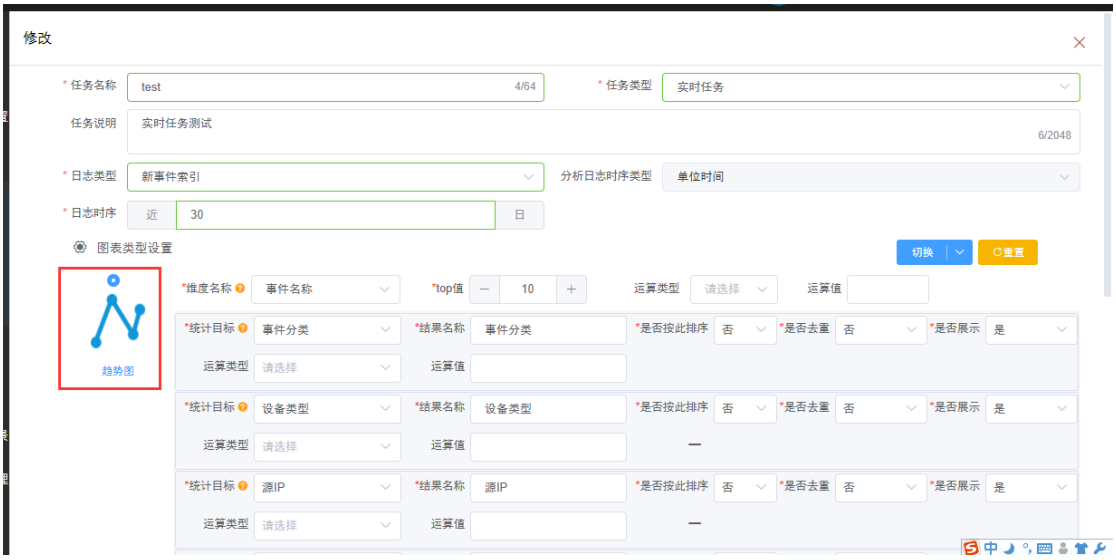


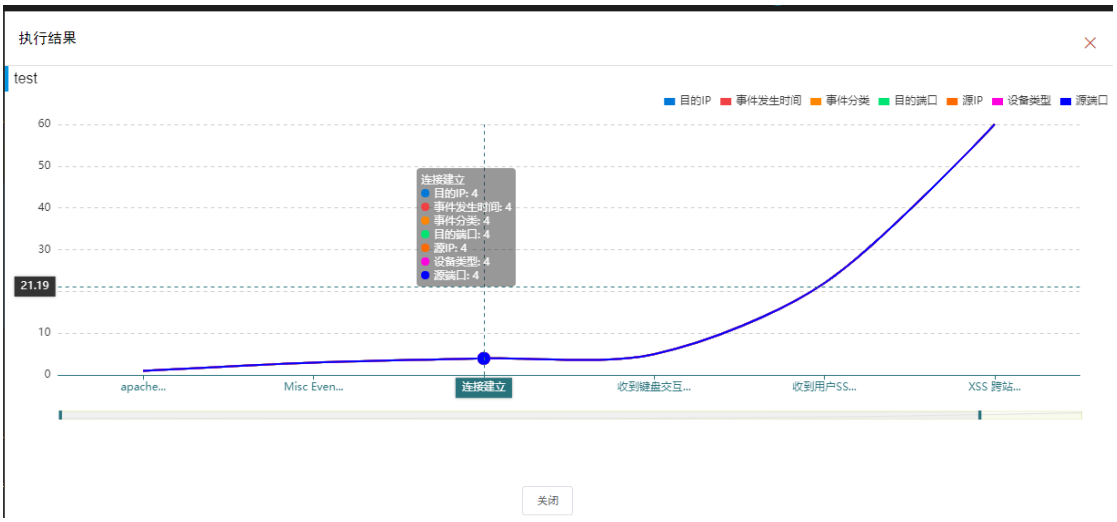
选择设备目标，可选择业务系统或资产维度，非必填，若不填，则默认针对所有资产；点击提交，任务创建成功。



2.7.2.3 修改

点击修改按钮，弹出修改界面，属性同新增界面，用户可根据需要修改内容，如修改图表类型为趋势图，提交成功，点击执行结果，如图：





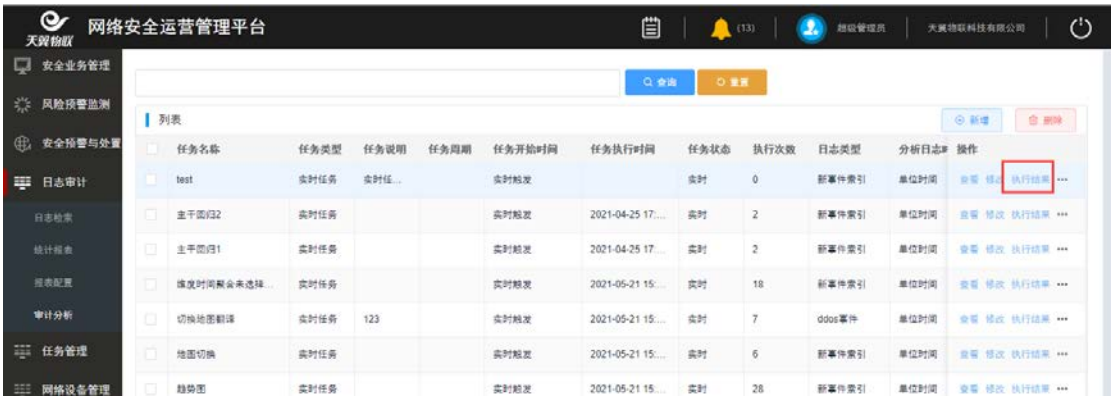
2.7.2.4 执行结果

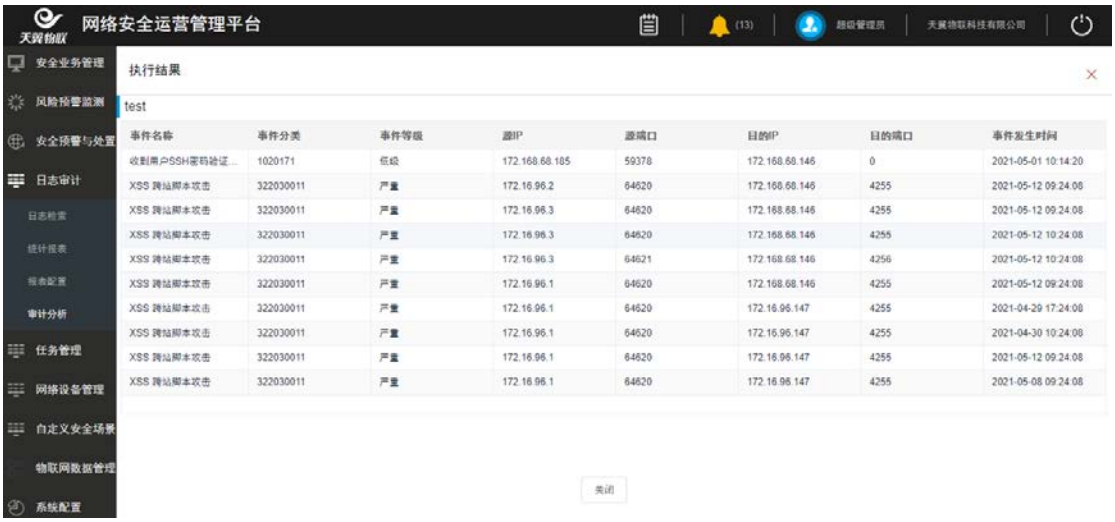
点击执行结果按钮，根据任务创建时选择的维度展示，如图：

其中，实时任务：根据点击执行结果按钮的时刻，实时加载最新结果数据，不同时刻查看的结果会发生变化；

历史任务：查看创建任务时选择的时间范围数据，执行结果不会发生变化；

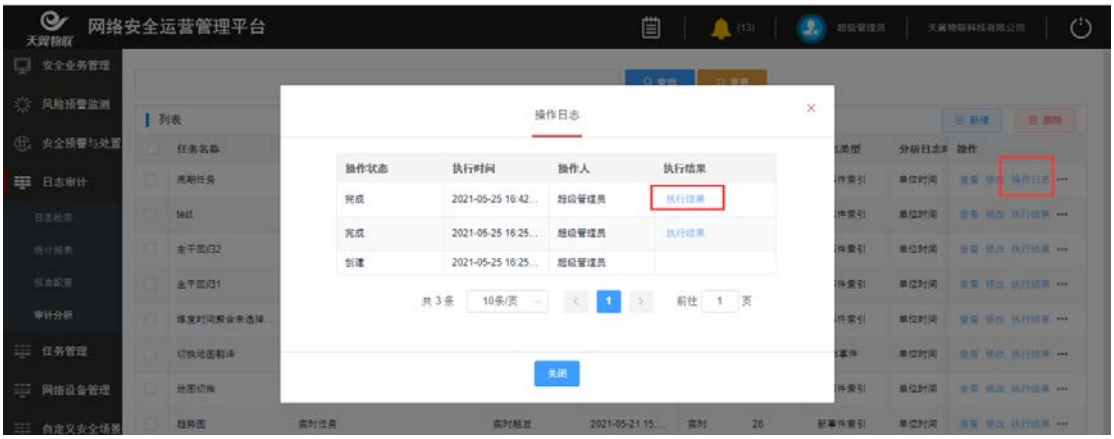
周期任务：系统按照任务周期定时统计日志时序内的的数据，执行结果根据周期变化；





2.7.2.5 操作日志

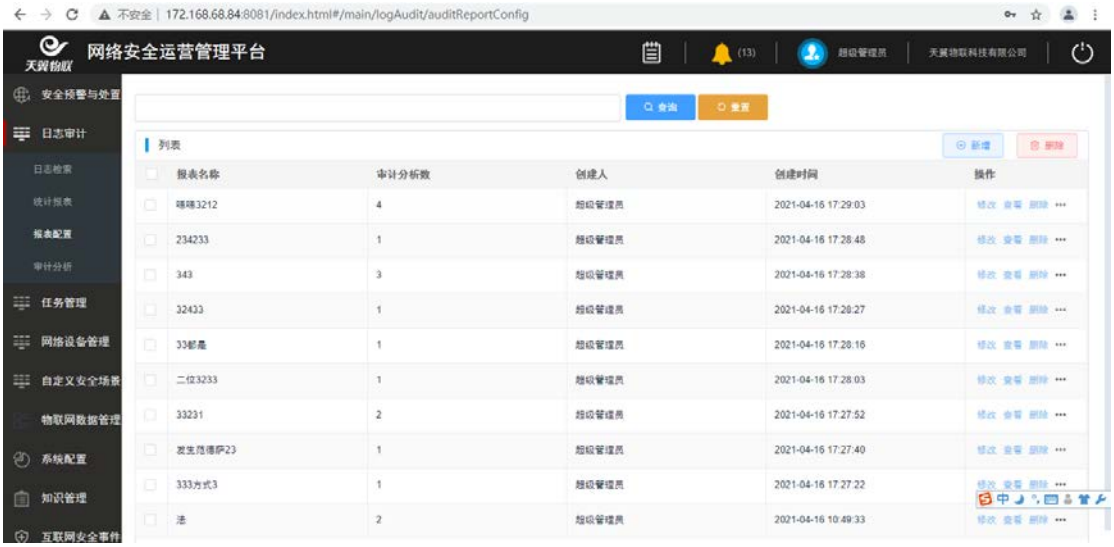
点击操作日志按钮，可查看任务创建、修改、与执行记录；操作栏的执行结果为历史统计数据。



2.7.3 报表配置

报表配置数据源为审计分析模块新建的相关任务。

列表页展示了报表名称、审计分析任务数、创建人、创建时间，提供报表名称、创建时间等查询条件。



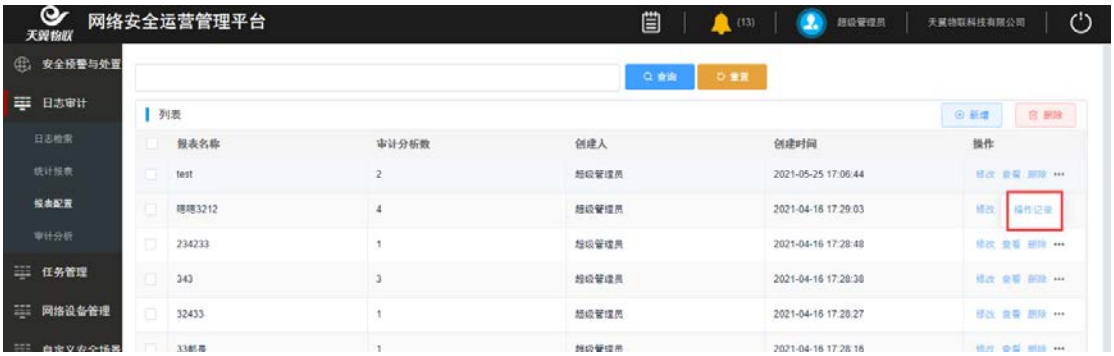
2.7.3.1 新增

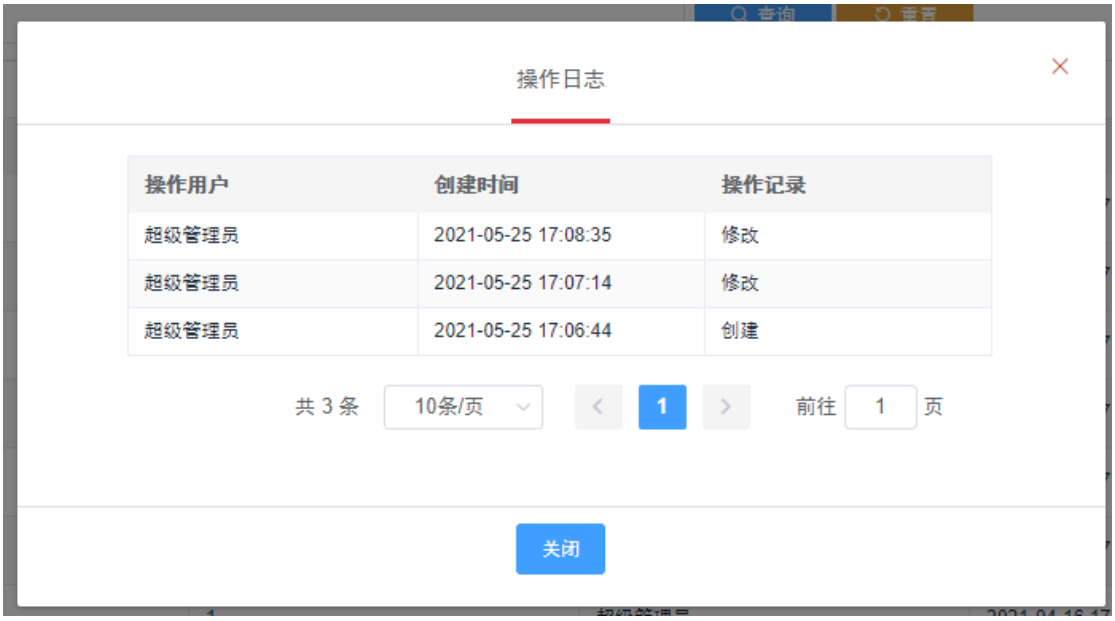
点击新增按钮，弹出报表配置界面，审计分析任务列表为审计分析创建的相关任务，可选择多个审计分析任务组合成报表，并自定义报表布局，图表位置可拖拽调整，点击生成布局，布局成功，点击提交按钮，报表配置成功。

布局所占格子数应大于等于任务数。

2.7.3.2 操作记录

点击操作栏的操作记录按钮可查看报表的操作记录。

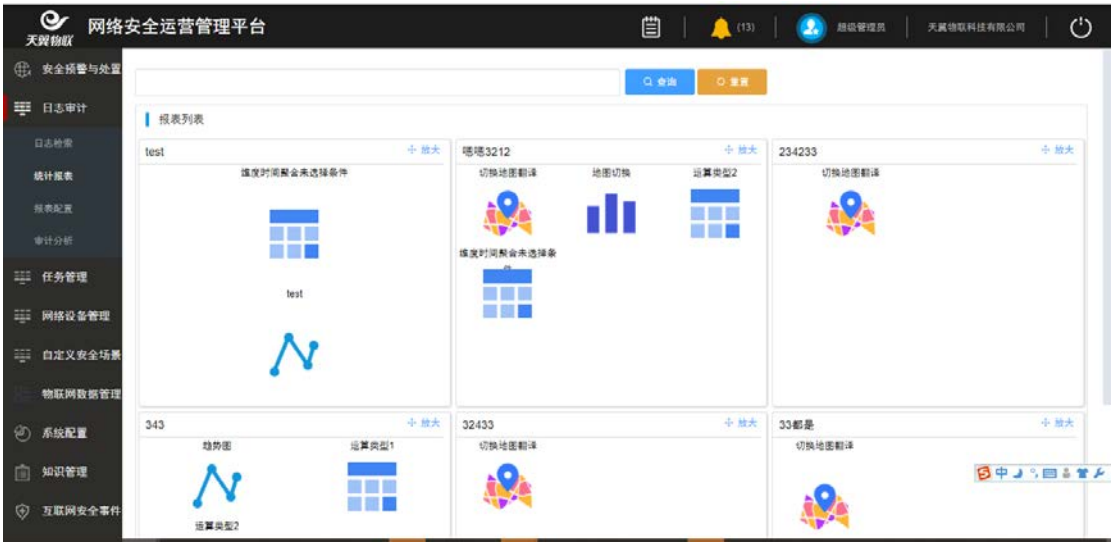




2.7.4 统计报表

统计报表为报表配置的结果展示页面。

统计报表列表页展示每个报表的缩略图，每页展示 6 个报表，可点击放大按钮查看报表详情。



2.8 风险分析

2.8.1 告警策略

2.8.1.1 脆弱性策略

点击菜单“风险分析”=>“告警策略”，默认进入脆弱性策略配置界面，如图：

- 点击“新增”按钮，弹出脆弱性告警规则新增界面，*号标识为必填项，如图：

信息填写完后，点击“提交”即可保存成功；

- 该界面还提供脆弱性告警规则的修改、查看、删除功能，如图：

2.8.1.2 关联告警策略

点击菜单“风险分析”=>“告警策略”=>“关联告警策略”，进入关联告警策略配置界面，如图：

- 点击“新增”按钮，弹出关联告警策略新增界面，分为两部分，分别为规则的基础信息 tab、补充逻辑规则 tab，*号为必填标识，如图：

填写完基础信息 tab，点击“保存”按钮，跳转至补充逻辑规则配置界面，如图：

（1）点击 

按钮，可新增逻辑节点，逻辑规则分别为 OR、AND、FB（followby），如图：

（2）点击 

按钮，弹出补充规则节点界面，如图：

鼠标分别点击左侧任意数以，右侧界面对应展示该属性值供用户选择，如上图，用户鼠标点击“安全时间对象 IP”，右侧对应展示资产信息，并提供过滤条件筛选结果；

（3）选中其中一个节点，点击 

按钮，可修改节点信息；

（4）选中其中一个节点，点击 

按钮，可删除节点信息；

最后，点击 

按钮，则一条关联告警规则添加并保存成功；

- 本配置界面还提供规则的查看、修改、删除功能；

2.8.2 事件策略

事件类策略主要提供对安全事件规则的配置。点击菜单“风险分析”=>“事件策略”，分别为事件分类规则、事件过滤规则、事件归并规则三个子 tab 界面。

2.8.2.1 事件分类规则

事件分类规则主要提供对安全事件的分类描述与配置。主要分为节点信息区和规则列表区。如图：

节点信息区主要用来配置事件规则组，规则列表区主要用来配置具体的分类规则以及规则的展示。

1）新增规则组

在节点信息区，选择其中一个节点，点击 

按钮，输入如下信息，如图：

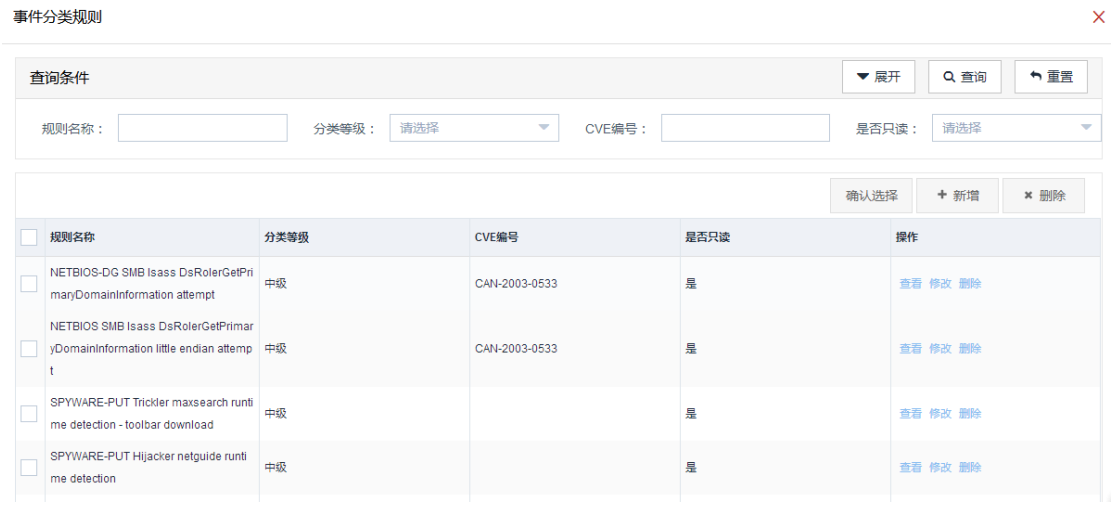
点击 新增保存 按钮，即添加了一个新的规则分组。

2）删除规则组

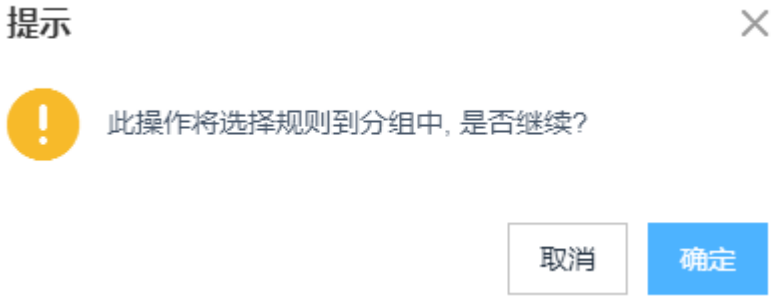
选择某个规则组，点击 删除 按钮，弹出提示信息对话框，选择是否删除该规则组。点击“确定”则该节点被删除，点击“取消”，则取消删除操作。

3）选择分类规则

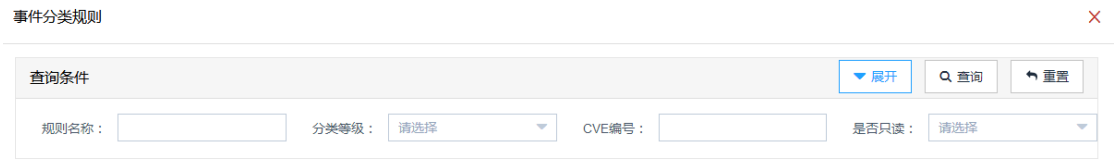
添加完规则分组之后，要对该规则分组选择相应的分类规则。点击 选择分类规则 按钮，弹出事件分类规则界面，如图：



选择需要的分类规则，点击 确认选择 按钮，弹出是否选择规则到分组确认框，点击 确定 按钮，即可完成规则分类的选择，如图：



查询表单中，可以根据规则名、分类登记、CVE 编号以及是否只读对可选的分类规则进行过滤，在输入框中输入查询条件，点击 查询 按钮，列表栏即会列出满足要求的分类规则。点击 重置 按钮，可重新设置查询条件。



4）分类规则添加、查看、编辑和删除

添加：在图事件分类规则界面点击 + 新增 按钮，弹出规则配置窗口，如图：

根据要求填入规则名称、CVE 编号、分类等级、规则描述、建议措施、误报信息、关键字、正则表达式、规则所属设备等规则基础信息，其中除规则名称和分类等级、规则所属设备为必填项外，其他项可选填。输入关键字和正则表达式，在下拉框选项中选择规则所属的设备。点击 

按钮，提交配置信息。

查看：点击分类当前行的 

按钮，可查看该规则的详细信息。

编辑：点击分类当前行的 

按钮，可对该分类规则进行重新编辑，具体步骤与添加分类规则时一致。

删除：选择某一个只读属性为否的分类规则，点击 

按钮，可删除该分类规则。

批量删除：选择多个只读属性为否的分类规则，点击 

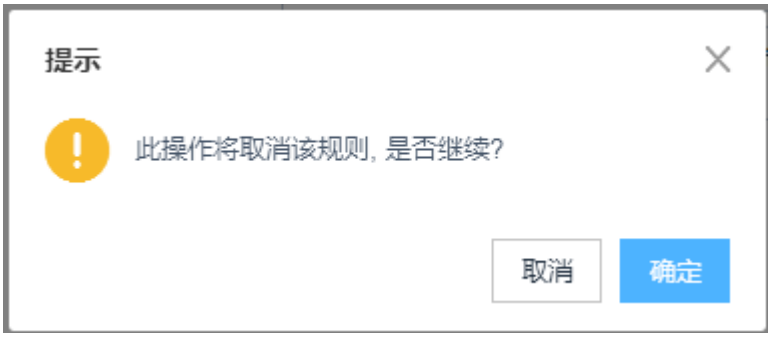
按钮，可批

量删除分类规则。

5）取消分类规则

在规则列表区，选择一个或多个分类规则，点击 

按钮，可从该分类规则组中，将这些规则取消，如图：4-8



2.8.2.2 事件归并规则

点击 

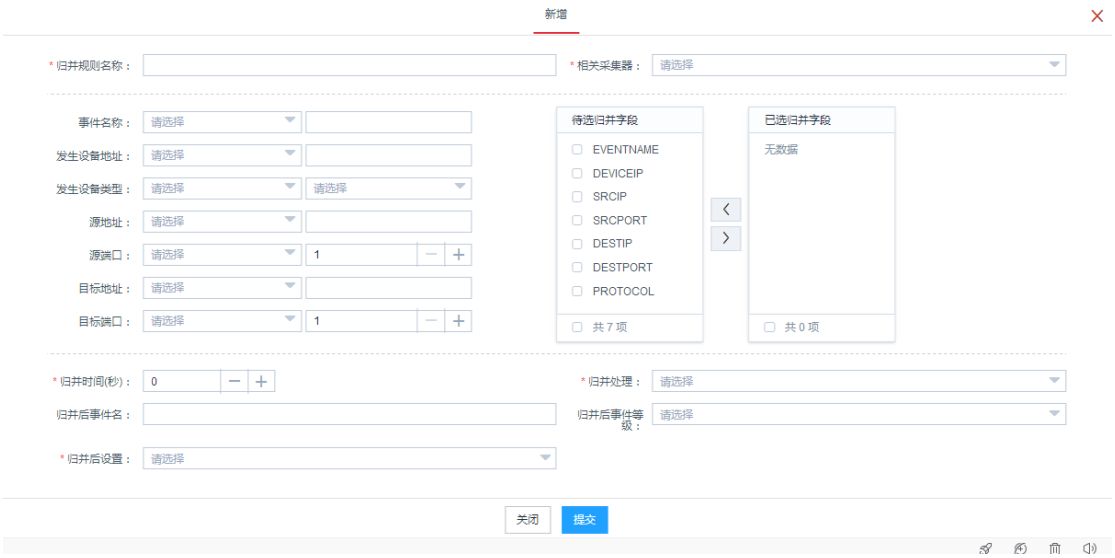
节点，可见到事件归并规则详情，如图： 4-9

在上图中查询区，可以按归并规则名称、归并时间、归并处理、归并后事件名称、归并后事件等级、归并后事件设置等字段进行查询所需要的归并规则信息。

1）**添加归并规则**

点击 

按钮，弹加新增归并规则页面并填写表单信息，如图：



填写完表单信息后点击 

保存图标，成功将提示保存成功，失败就提示失败信息。

2）**编辑归并规则**

点击 

按钮，可对该归并规则进行重新编辑，具体步骤与添加归并规则时一致。

3）**查看归并规则**

选择某个归并规则，点击 

按钮，可查看该规则的详细信息。

4）**删除归并规则**

选择某一个或者多个归并规则，点击 

按钮，可删除该归并规则。

2.8.2.3 事件过滤规则

该模块与 2.6.2.2 模块操作类似，可以参照 2.6.2.2 步骤，此处省略。

2.8.3 风险评估结果

展开**风险评估结果**菜单，在该节点下有 4 个子节点：业务系统、资产、地域、安全域。

2.8.3.1 业务系统

1）业务系统风险总体总体概览

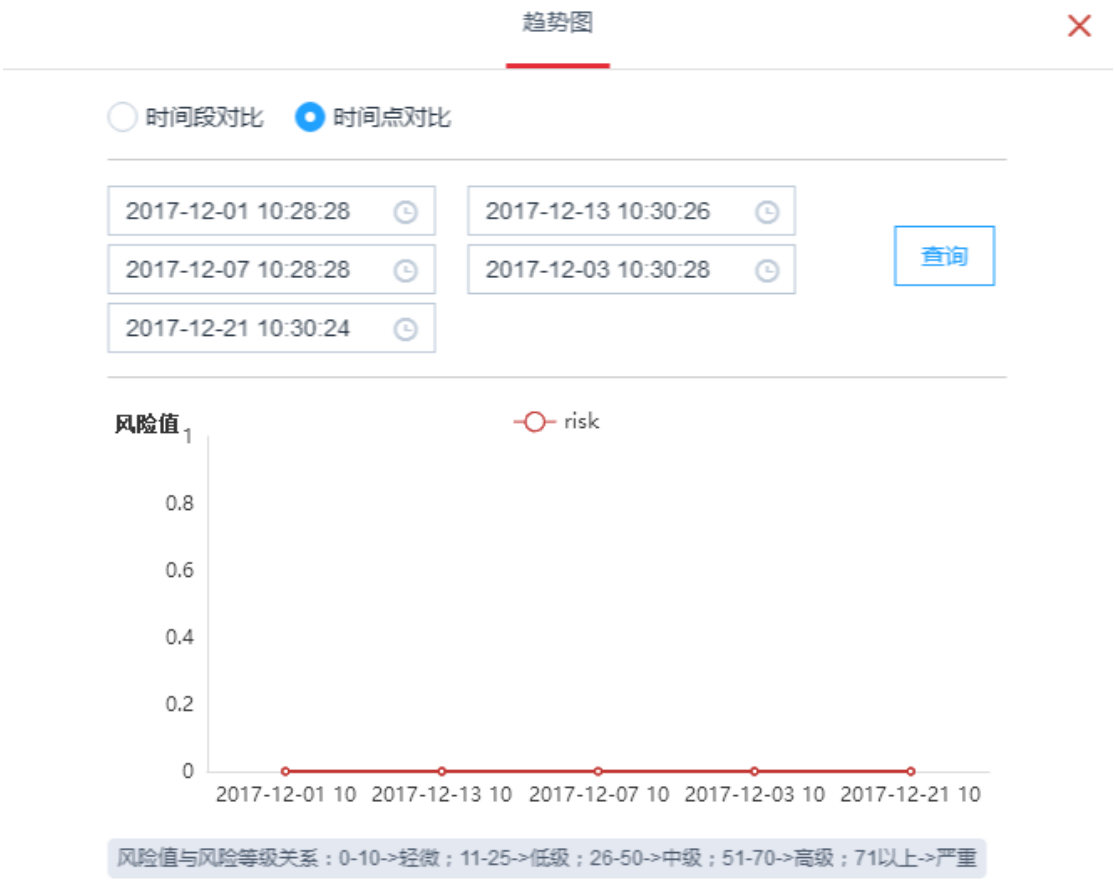
- 点击 业务系统 节点，可以看到整个业务系统的风险情况，如图：

2）查看某个子业务系统的风险情况

点击 查看 按钮，弹出该业务系统的风险趋势图：

① 时间段对比：选择两个不同日期的同一时间段，点击 查询 按钮，如图展示风险值趋势图：

② 时间点对比：选择不同时间，点击 查询 按钮，展示不同时间点的风险值趋势图，如图：



2.8.3.2 资产

- 资产风险总体总体概览

点击 资产 节点，所有的安全资产都会罗列出来，如图：

选择一个安全资产，点击 查看 按钮，显示如图：

- 时间点风险值趋势

在 风险趋势图 sheet 这个页面中，可以查看不同时间段的风险值变化趋势，或选择不同时间点查看风险值变化趋势，如图：

- 安全对象威胁

在 安全对象威胁 sheet 页面中会显示当天的安全资产威胁，如图：

- 安全对象漏洞

在 安全对象漏洞 sheet 页面中显示该安全资产已发现的安全漏洞信息，如图：

- 基本信息

在 基本信息 sheet 页面中只展示该安全资产部分信息 如图：

- 安全对象配置隐患

在 安全对象配置隐患 sheet 中只展示该资产的配置隐患信息，如图：

2.8.3.3 地域

该模块的操作和 2.6.3.1 中的操作一样，可以参考 2.6.3.1

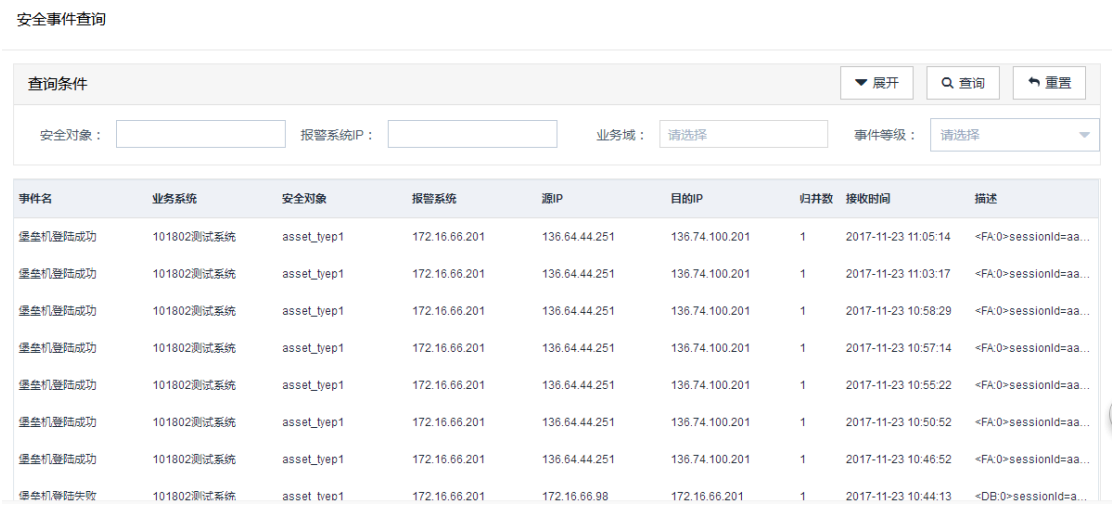
2.8.3.4 安全域

该模块的操作和 2.6.3.1 中的操作一样，可以参考 2.6.3.1

2.8.4 安全事件查询

- 点击菜单“风险分析”=>“安全事件查询”，进入安全事件查询页面，

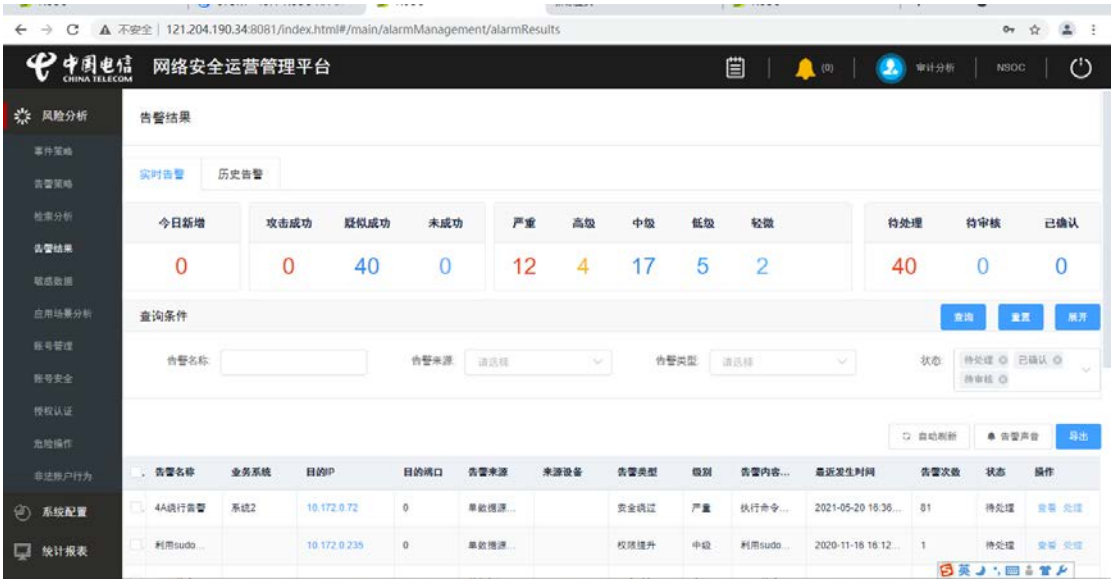
如图：



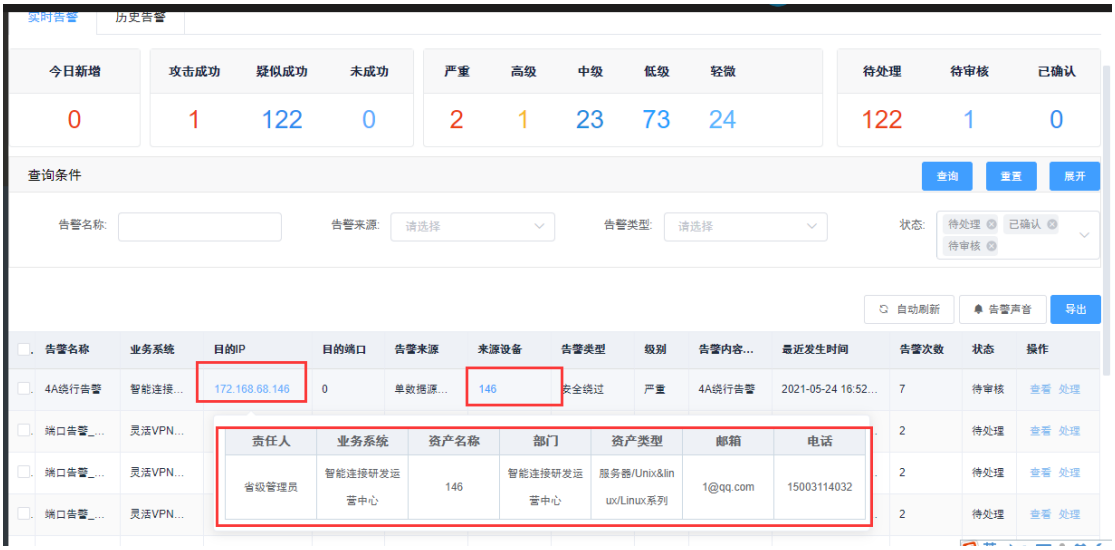
选中其中一条记录，双击可查看详情，如图：

2.8.5 告警结果（新）

点击主菜单风险分析>>告警结果，进入告警结果实时告警主界面，如图：

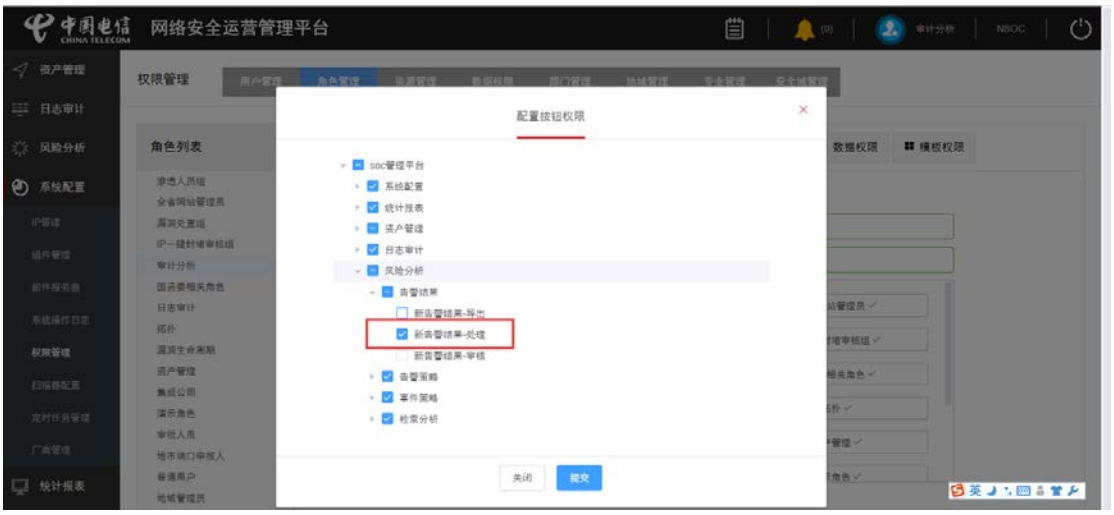


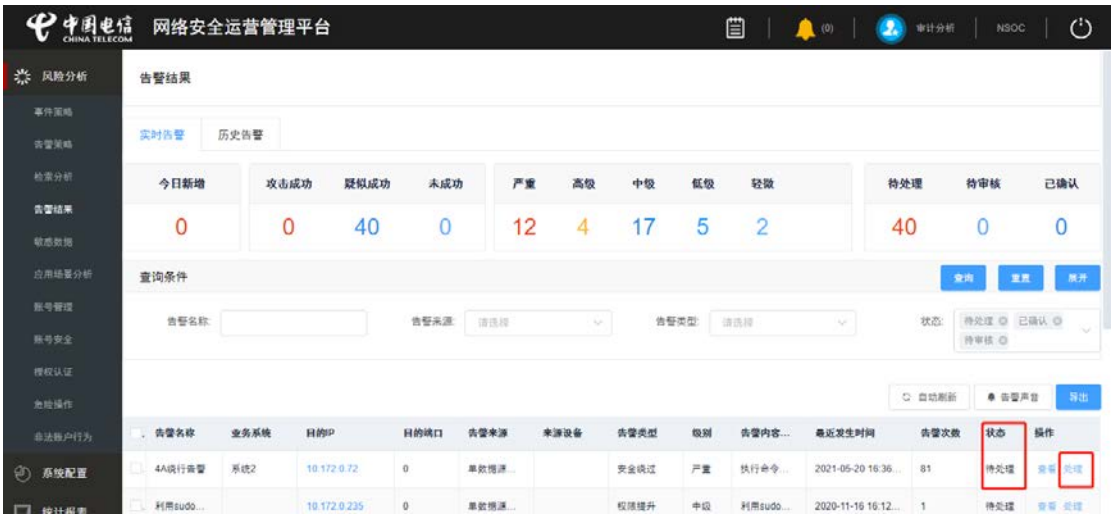
点击 ip、设备名称，关联出责任人信息。



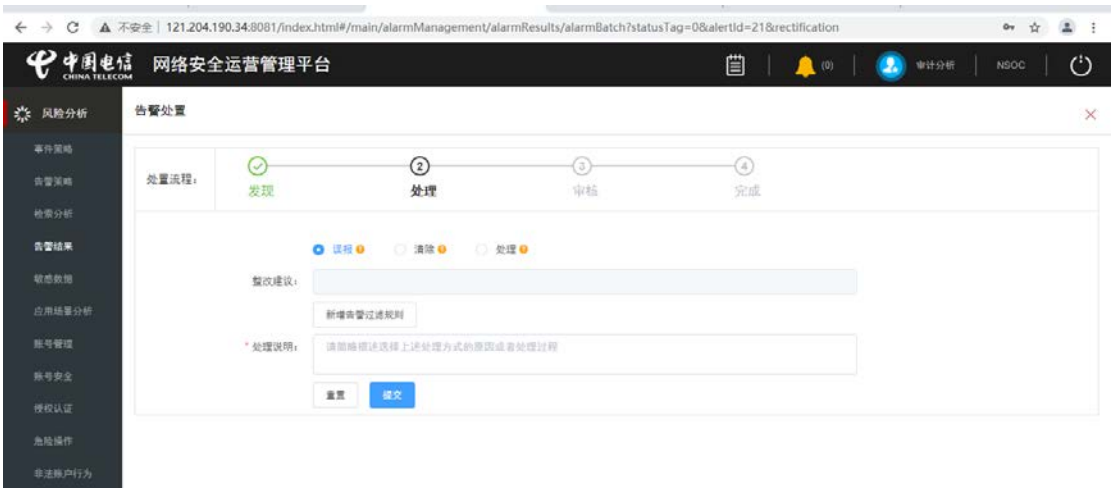
2.8.5.1 告警结果处置

具有告警结果处理权限的用户登录系统，选择待处理状态的告警数据，可进行告警处置。





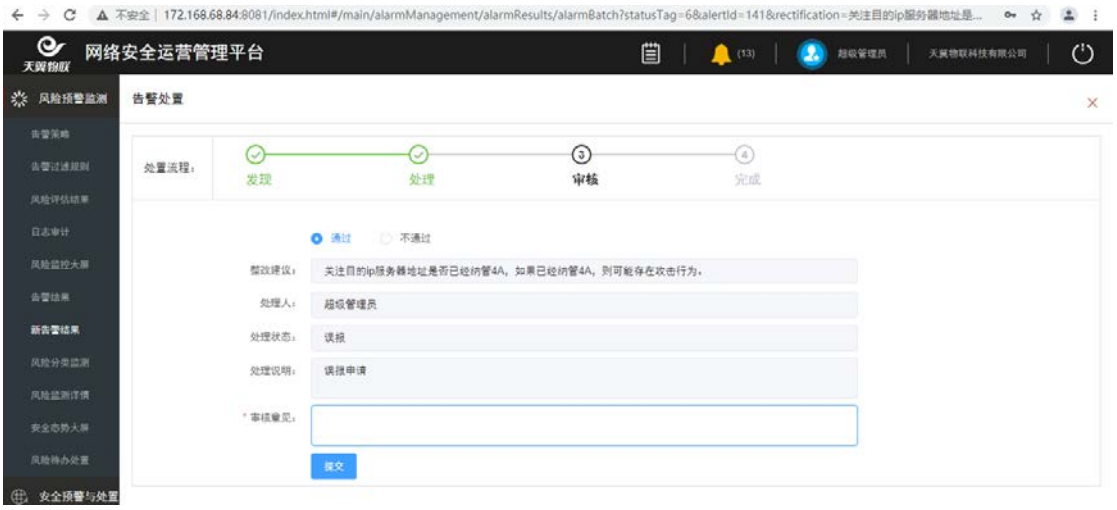
点击处理按钮，进入处置界面，用户可根据实际需要选择误报、清除、处理告警，鼠标移入每个节点后的？弹出详情解释。



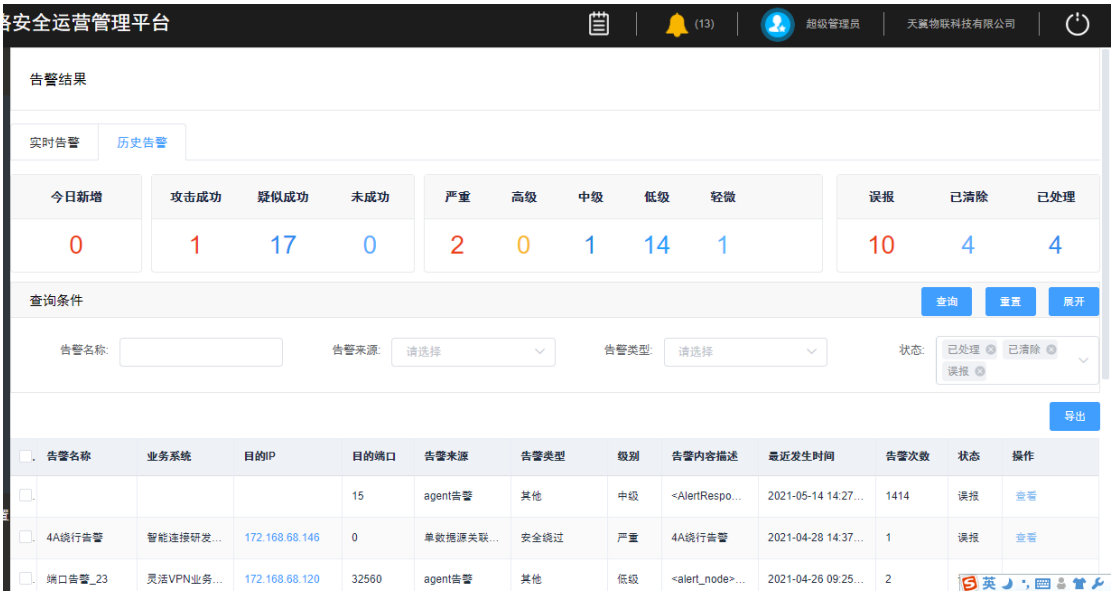
点击提交，处理成功，告警状态变更为待审核。

2.8.5.2 告警结果审核

具有告警结果审核按钮权限的用户登录系统，选择待审核状态的告警数据，点击处理按钮，填写审核意见。



点击提交，审核通过，则告警状态变更为：误报申请>>误报，清除申请>>已清除，处理申请>>已处理，数据录入到历史告警 tab，不再体现在实时告警界面；审核不通过，则状态变更为待处理；

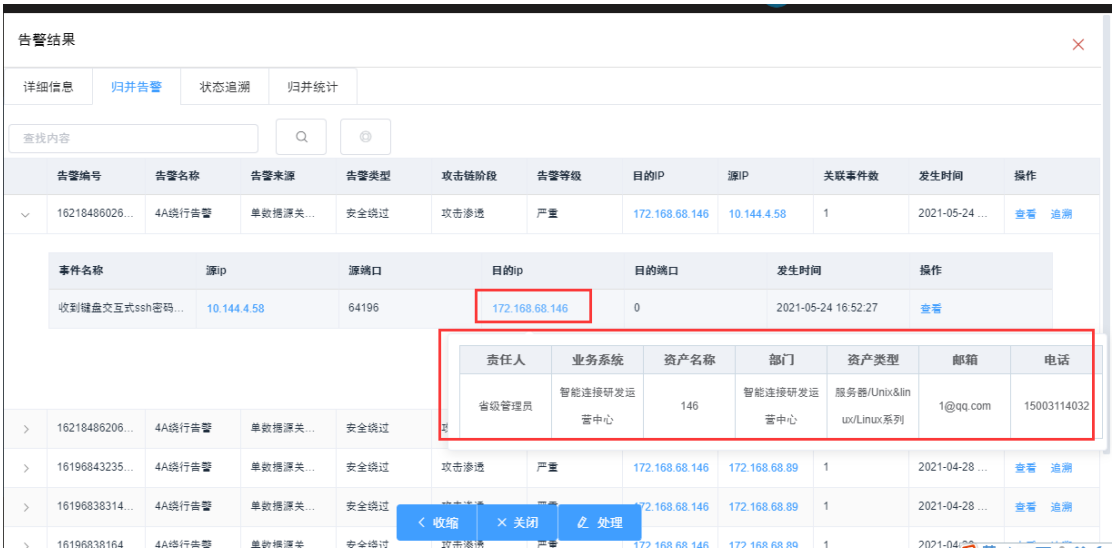


2.8.5.3 告警结果查看

点击查看，可查看告警结果详情信息，点击 ip、名称等弹出关联的资产、责任人、电话等信息。

归并信息：

点击 ip，弹出责任人、资产、电话等信息。。

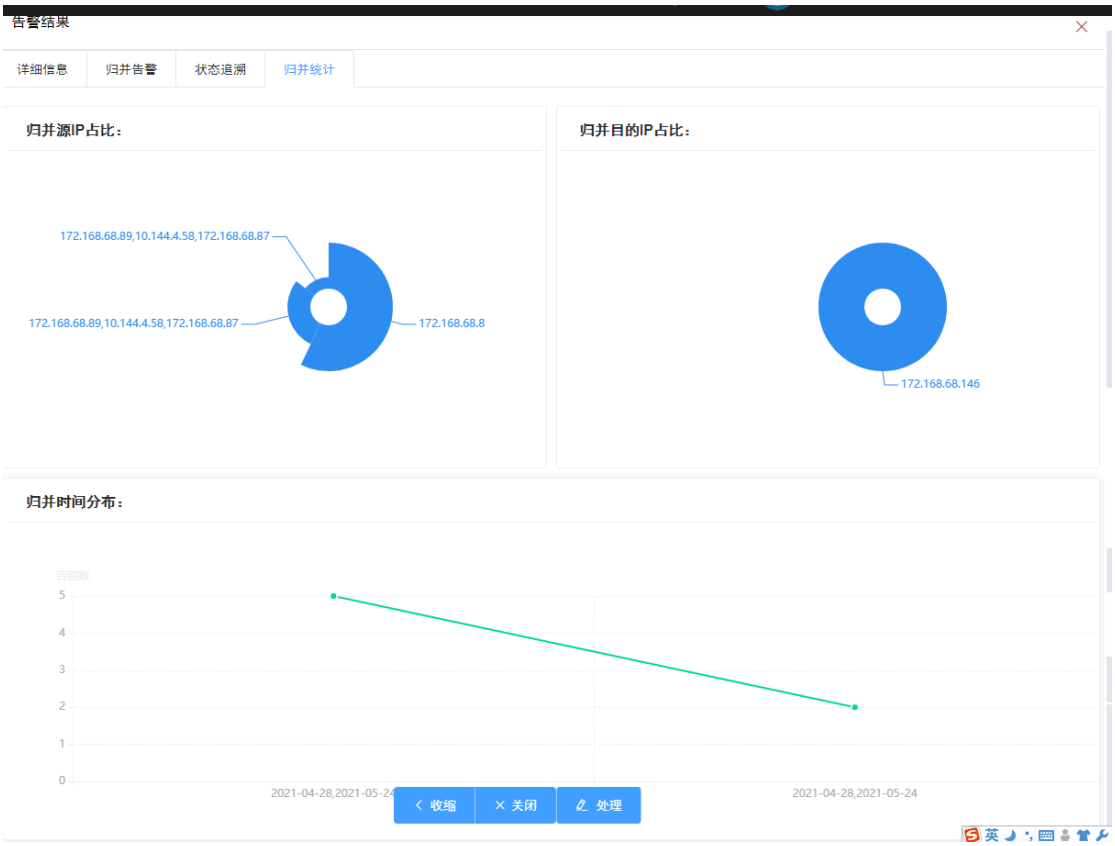


点击查看，弹出被归并告警的详情信息。

点击事件信息查看按钮，弹出事件详情信息。

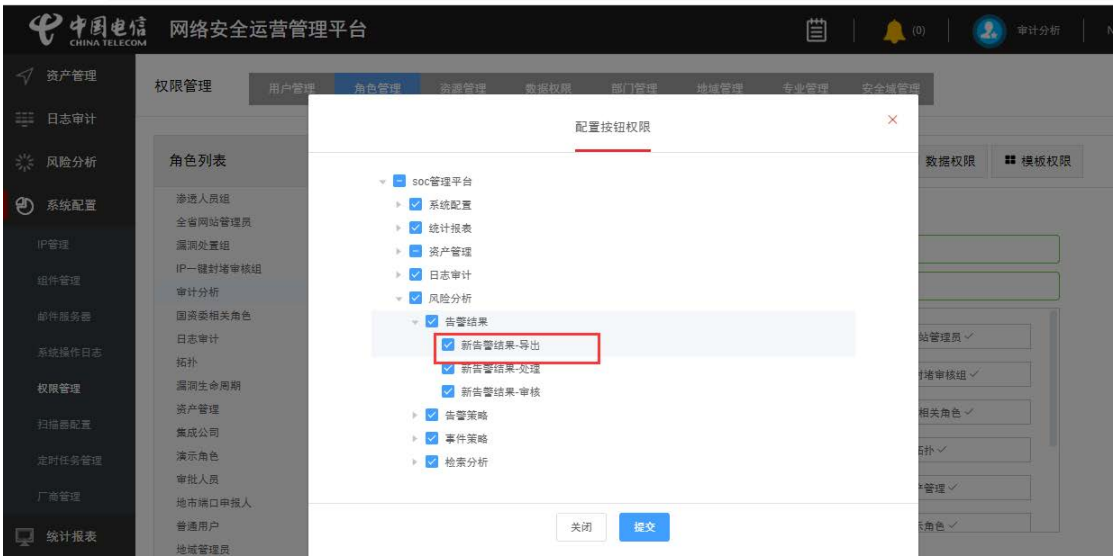
状态追溯，记录告警数据状态变更历史。

归并统计，以归并源 ip、归并目的 ip 维度统计。

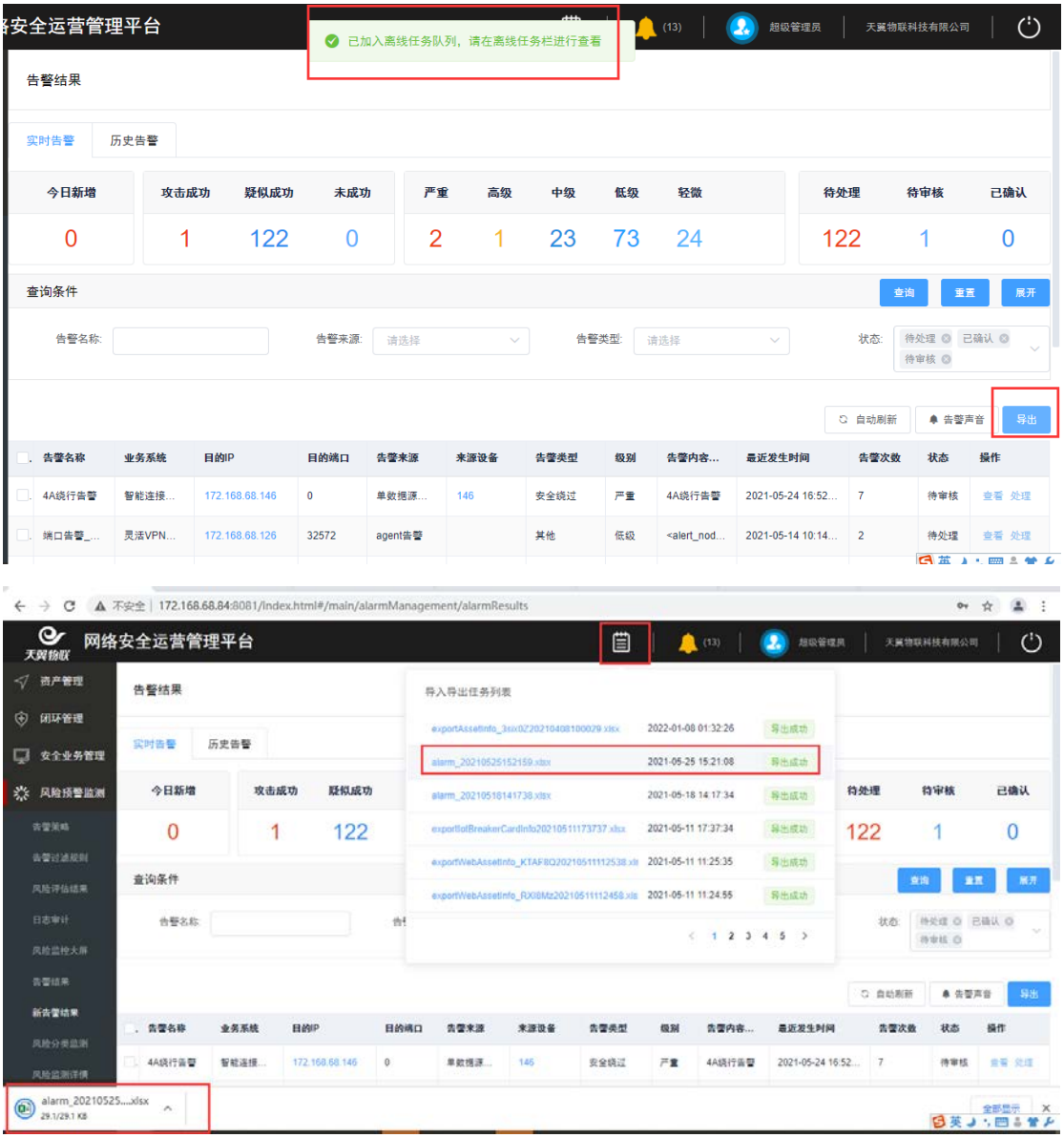


2.8.5.4 告警结果导出

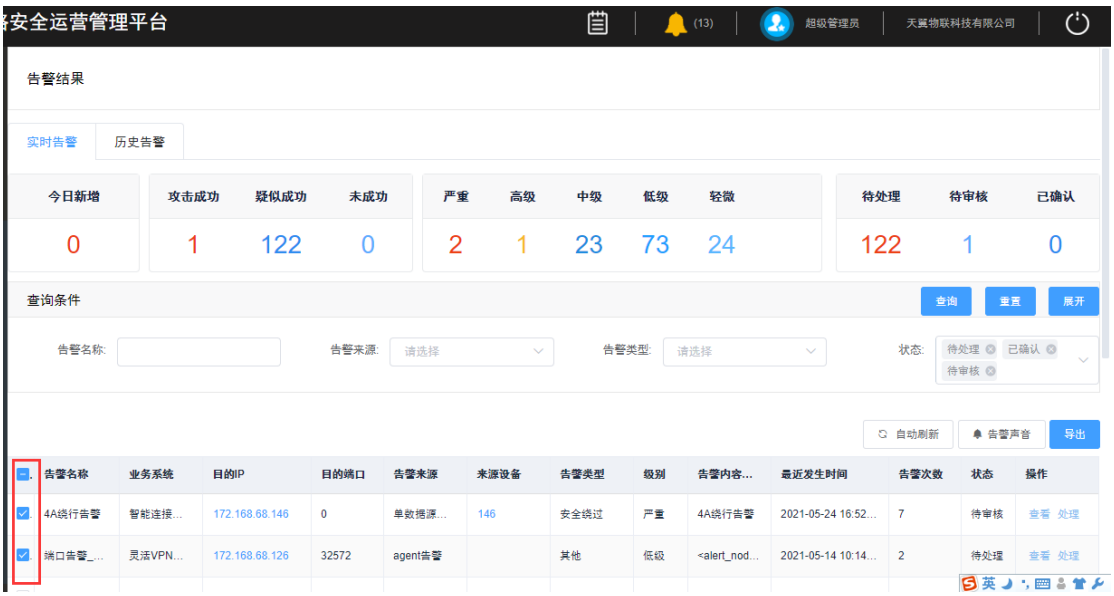
具有导出按钮权限的用户登录系统，可选择导出告警数据。



导出为异步任务，点击导出按钮，提示加入离线任务，在异步任务栏可查看导出是否成功，点击文件名，可下载导出文件。



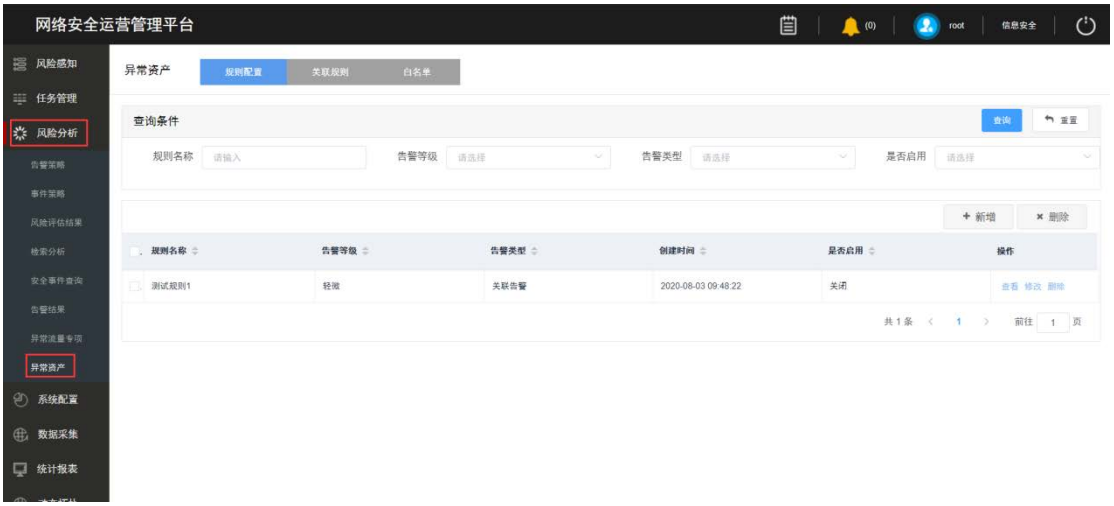
默认不勾选为导出全部数据，也可根据查询条件筛选结果导出，或勾选告警复选框，导出指定数据。



2.8.6 异常资产

2.8.6.1 规则配置

进入“风险分析”=>“异常资产”界面，新增基础规则，每个系统根据自身需求关联对应的规则。



- 新增

点击“ + 新增 ”按钮，进入规则配置界面，填写相关信息，点击新增即可

当规则类型为：异常进程或异常端口时，规则内容必填。

当规则类型为“异常端口”或“新增端口”时，端口类型可选“TCP、UDP”。

当所有数据读不填写时，点击“提交”按钮，提示：

- 查看

点击操作栏的“查看”按钮，可查看相关信息。

- 修改

点击操作栏的“修改”按钮，可修改相关信息，当规则类型由其他类型修改为“异常端口”，端口类型可选“TCP/UDP”。

- 删除

选择要删除的数据，点击删除按钮，可删除相关数据。

2.8.6.2 关联规则

- 新增

点击“ + 新增 ”按钮，进入规则配置界面，填写相关信息，点击新增即可

规则名称自动关联规则配置界面的基础规则，业务系统按当前登录用户业务系统数据权限过滤。

例如：当前用户的业务系统权限-按部门过滤，则新增时只可选择该用户所属部

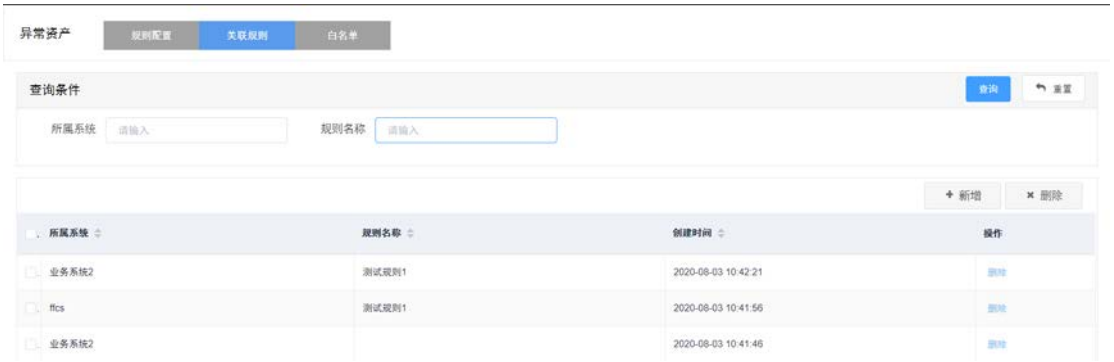
门下的业务系统。

- 删除

  选择要删除的数据，点击删除按钮，可删除相关数据。

- 查询

所属系统及规则名称支持模糊查询。



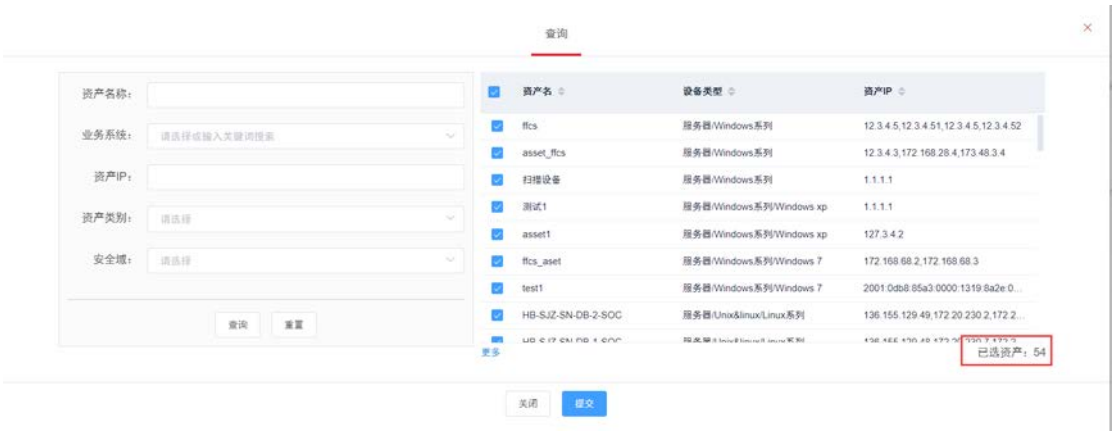
2.8.6.3 白名单

- 新增

点击“ ✚ 新增 ”按钮，进入规则配置界面，填写相关信息，点击新增即可。

规则名称自动关联规则配置界面的基础规则，资产数据按当前登录用户资产数据权限过滤。

例如：当前用户的资产数据权限-按部门过滤，则新增时只可选择该用户所属部门下的资产。



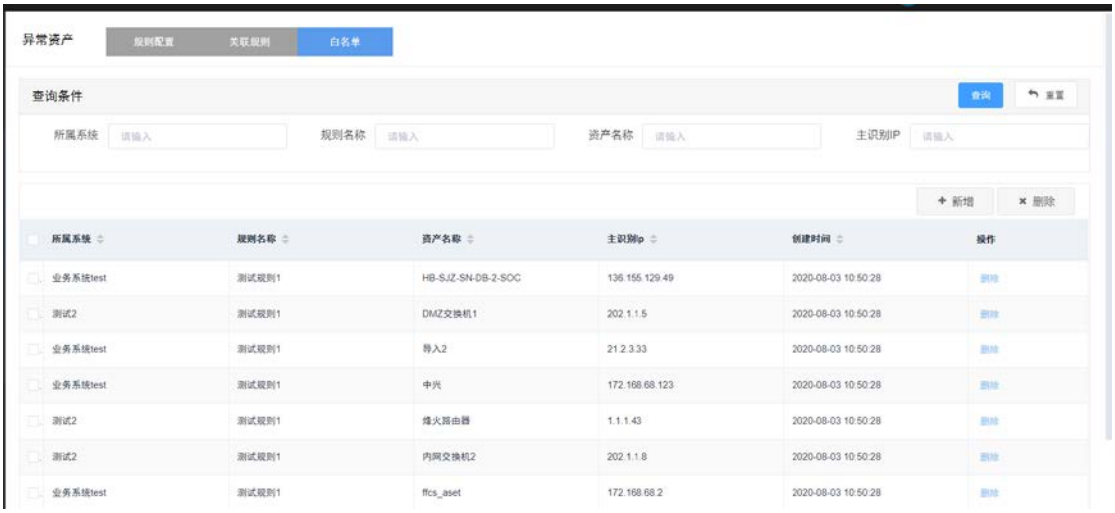
若选择多 50 条资产，则对应新增 50 条白名单。

- 删除

  选择要删除的数据，点击删除按钮，可删除相关数据。

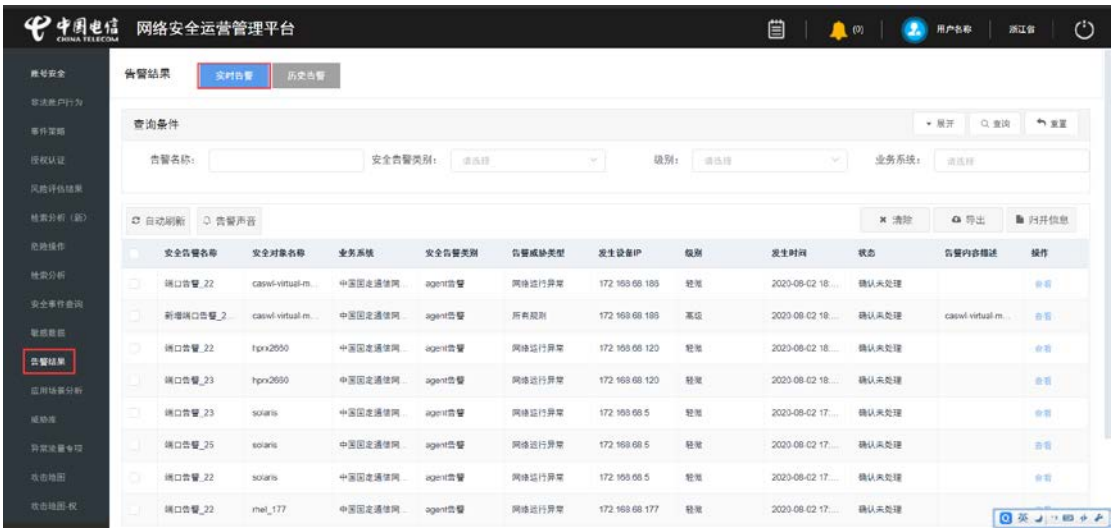
- 查询

所属系统及规则名称支持模糊查询。



2.8.6.4 告警数据查看

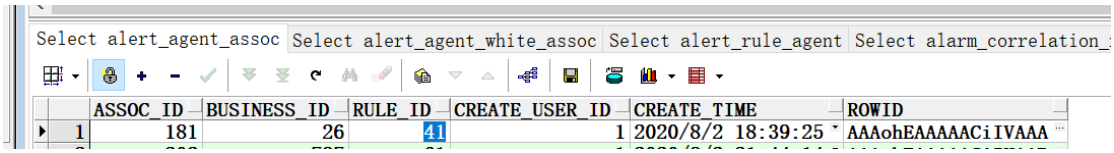
进入“风险分析”=>“告警结果”界面，可查看异常资产告警结果。



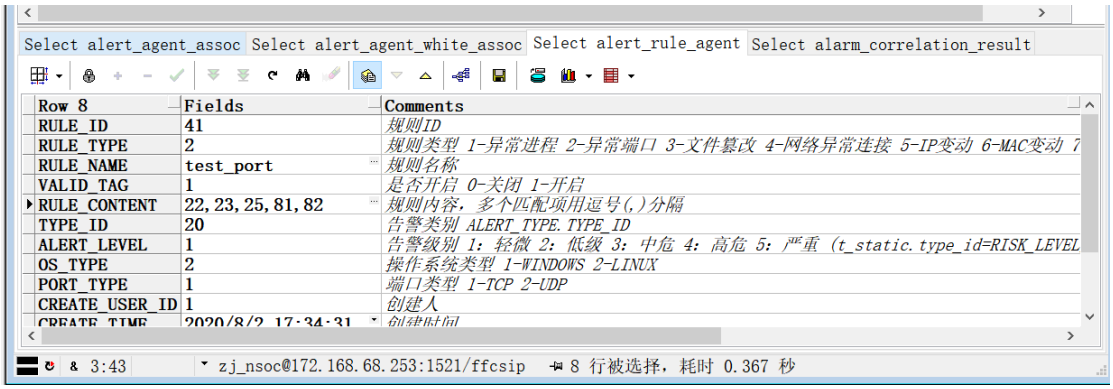
2.8.6.5 后端告警逻辑：

2.8.6.5.1 端口和进程告警：

查看 ALERT_AGENT_ASSOC 关联表绑定的业务系统 id（business_id）和规则 id(rule_id)。



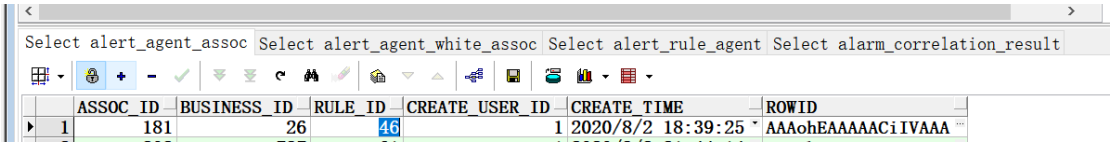
根据 rule_id 去 ALERT_RULE_AGENT 规则表取出规则内容（rule_content）和规则类型（rule_type）、端口类型（port_type）、操作系统类型（os_type）。



上报的资产在这个业务系统下并且存在规则配置的端口或进程就会产生告警。

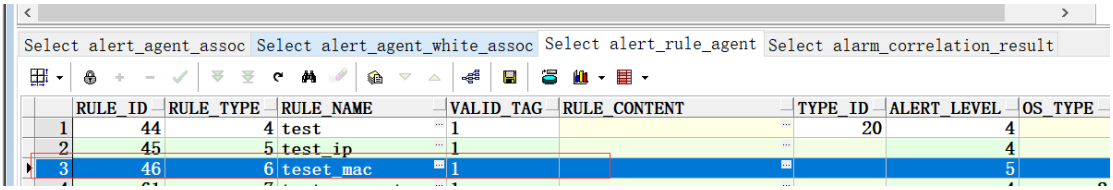
2.8.6.5.2 其他告警：

查看 ALERT_AGENT_ASSOC 关联表绑定的业务系统 id（business_id）和规则 id(rule_id)。



	ASSOC_ID	BUSINESS_ID	RULE_ID	CREATE_USER_ID	CREATE_TIME	ROWID
1	181	26	46	1	2020/8/2 18:39:25	AAAohEAAAAACiIVAAA

根据 rule_id 去 ALERT_RULE_AGENT 规则表取出规则类型（rule_type）。

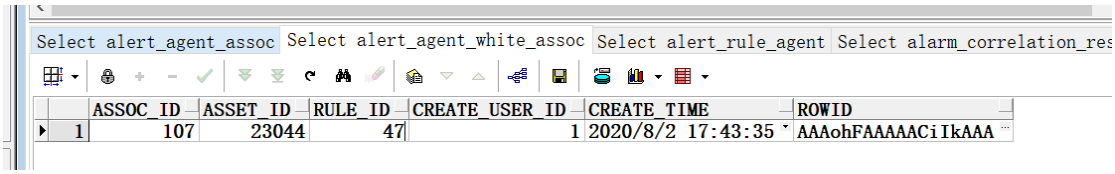


	RULE_ID	RULE_TYPE	RULE_NAME	VALID_TAG	RULE_CONTENT	TYPE_ID	ALERT_LEVEL	OS_TYPE
1	44	4	test	1		20	4	
2	45	5	test_ip	1			4	
3	46	6	teset_mac	1			5	

上报的资产在这个业务系统下并且与之前入库的信息有变动就会产生告警。

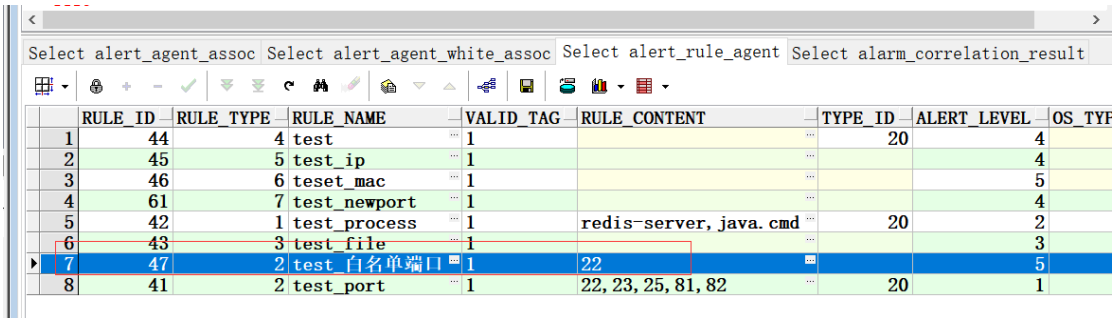
2.8.6.5.3 白名单

根据 ALERT_AGENT_WHITE_ASSOC 取出绑定的资产 id 和规则 id，



	ASSOC_ID	ASSET_ID	RULE_ID	CREATE_USER_ID	CREATE_TIME	ROWID
1	107	23044	47	1	2020/8/2 17:43:35	AAAohFAAAAACiIkAAA

对这个资产的规则 id 配置的端口、进程不进行告警。



	RULE_ID	RULE_TYPE	RULE_NAME	VALID_TAG	RULE_CONTENT	TYPE_ID	ALERT_LEVEL	OS_TYP
1	44	4	test	1		20	4	
2	45	5	test_ip	1			4	
3	46	6	teset_mac	1			5	
4	61	7	test_newport	1			4	
5	42	1	test_process	1	redis-server, java. cmd	20	2	
6	43	3	test_file	1			3	
7	47	2	test_白名单端口	1	22		5	
8	41	2	test_port	1	22, 23, 25, 81, 82	20	1	

2.9 数据采集

2.9.1 数据查询

点击菜单“数据采集”=>“数据查询”，进入数据查询界面，记录三个月内的原始日志信息，如图：

2.9.2 采集对象监控

点击菜单“数据采集”=>“采集对象监控”，进入采集对象监控界面，记录采集对象信息, 如图：