

云网安全运营中心 用户手册

目 录

1. 概述.....	6
1.1 初次使用说明.....	6
1.2 系统简介.....	6
1.3 系统访问.....	6
2. 业务流程配置.....	8
2.1 系统配置.....	8
2.1.1 IP 管理.....	8
2.1.2 组件管理.....	10
2.1.3 邮件服务器.....	12
2.1.4 系统操作日志.....	13
2.1.5 扫描器配置.....	13
2.1.6 权限管理.....	16
2.1.6.1 用户管理.....	16
2.1.6.2 角色管理.....	20
2.1.6.3 资源管理.....	22
2.1.6.4 数据权限.....	24
2.1.6.5 部门管理.....	25
2.1.6.6 地域管理.....	25
2.1.6.7 专业管理.....	25
2.1.6.8 安全域管理.....	26
2.1.7 厂商管理.....	26
2.2 统计报表.....	27
2.2.1 安全月报.....	28
2.2.2 异常流量分析报表.....	29
2.2.2.1 流量范围统计.....	29
2.2.2.2 持续时间分类统计.....	29
2.2.2.3 攻击类型分类统计.....	30
2.2.2.4 事件趋势统计.....	30
2.2.2.5 攻击流量峰值.....	31
2.2.2.6 IP 地址受攻击次数.....	31

2.2.3	漏洞统计报表.....	32
2.2.3.1	漏洞数量统计.....	32
2.2.3.2	弱口令应用类型统计.....	34
2.2.3.3	漏洞应用类型数量统计.....	36
2.2.4	资产统计报表.....	37
2.2.4.1	资产维度统计.....	37
2.2.4.2	Agent 维度统计.....	37
2.2.4.3	未知资产维度统计.....	37
2.2.5	漏洞处置报表.....	37
2.3	资产管理.....	37
2.3.1	资产管理首页.....	37
2.3.2	资产管理.....	43
2.3.3	扩展属性配置.....	48
2.3.4	WEB 资产.....	49
2.3.5	业务系统.....	51
2.3.6	资产发现.....	53
2.3.7	主机代理.....	57
2.3.8	未知资产.....	59
2.3.9	代理客户端.....	63
2.3.9.1	省测自建任务.....	63
2.4	任务管理.....	85
2.4.1	主机漏洞.....	85
2.4.2	WEB 漏洞.....	89
2.4.3	弱口令.....	93
2.4.4	基线配置.....	97
2.4.5	人工渗透.....	101
2.4.6	预警任务.....	102
2.4.7	端口扫描.....	104
2.4.7.1	探测任务.....	105
2.4.7.2	验证任务.....	105

2.5	风险处置.....	106
2.5.1	风险处置首页.....	106
2.5.2	漏洞处置.....	110
2.5.2.1	主机漏洞.....	110
2.5.2.2	WEB 漏洞.....	116
2.5.2.3	弱口令.....	123
2.5.2.4	基线违背.....	130
2.5.2.5	人工渗透.....	136
2.5.3	告警处置.....	143
2.5.4	白名单管理.....	143
2.5.5	处置规则配置.....	144
2.5.6	处置通知查询.....	145
2.6	风险感知.....	145
2.7	日志审计.....	146
2.7.1	日志检索.....	146
2.7.1.1	导出.....	147
2.7.1.2	查询.....	147
2.7.2	审计分析.....	150
2.7.2.1	查询.....	151
2.7.2.2	新增.....	151
2.7.2.3	修改.....	153
2.7.2.4	执行结果.....	154
2.7.2.5	操作日志.....	155
2.7.3	报表配置.....	155
2.7.3.1	新增.....	156
2.7.3.2	操作记录.....	157
2.7.4	统计报表.....	158
2.8	风险分析.....	159
2.8.1	告警策略.....	159
2.8.1.1	脆弱性策略.....	159
2.8.1.2	关联告警策略.....	160

2.8.2	事件策略.....	163
2.8.2.1	事件分类规则.....	163
2.8.2.2	事件归并规则.....	167
2.8.2.3	事件过滤规则.....	168
2.8.3	风险评估结果.....	168
2.8.3.1	业务系统.....	169
2.8.3.2	资产.....	171
2.8.3.3	地域.....	175
2.8.3.4	安全域.....	175
2.8.4	安全事件查询.....	175
2.8.5	告警结果（新）.....	176
2.8.5.1	告警结果处置.....	177
2.8.5.2	告警结果审核.....	179
2.8.5.3	告警结果查看.....	180
2.8.5.4	告警结果导出.....	183
2.8.6	异常资产.....	185
2.8.6.1	规则配置.....	185
2.8.6.2	关联规则.....	188
2.8.6.3	白名单.....	189
2.8.6.4	告警数据查看.....	190
2.8.6.5	后端告警逻辑：.....	191
2.9	数据采集.....	192
2.9.1	数据查询.....	192
2.9.2	采集对象监控.....	193

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`

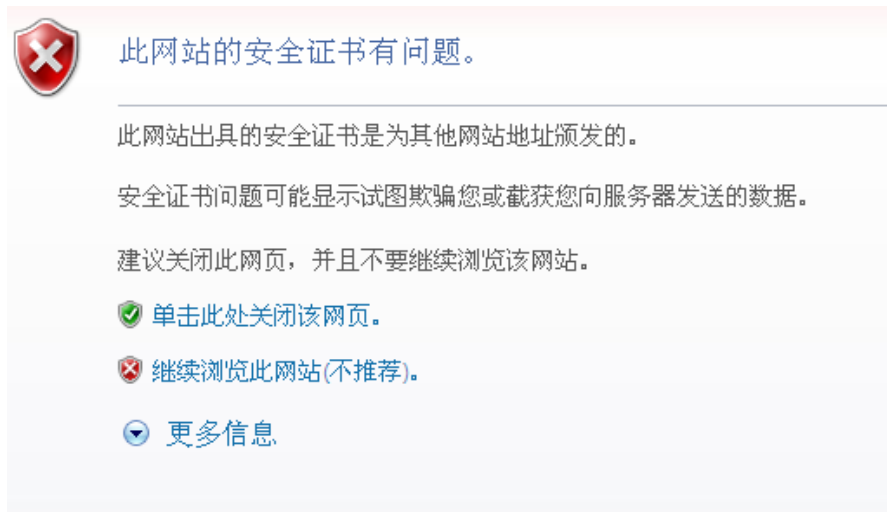


图 1-1 证书提示页面

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

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：

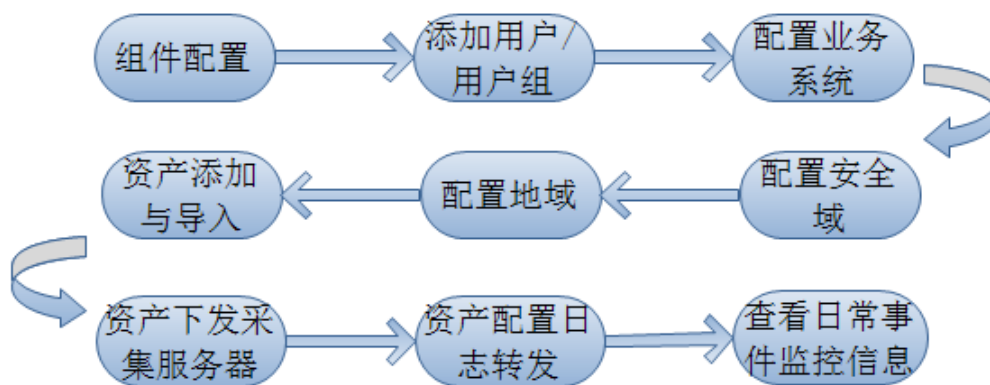


图 2-1 事件采集配置流程图

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：

起始IP	终止IP	所属地域	客户名称	IP类型	业务号	数据来源	客户地址	操作
01.189.162.135	01.189.162.153	贵阳	flca	静态	1	手工录入	福州	查看 修改 删除
3.2.3.5	3.2.3.5	安顺		静态		手工录入		查看 修改 删除
192.168.68.158	192.168.68.158	遵义		动态		手工录入		查看 修改 删除
172.168.68.141	172.168.68.141	贵阳		动态		手工录入		查看 修改 删除

- 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。

新增 ✕

起止IP填写格式为: 192.168.100.102-192.168.100.122 ✕

* 起止IP :

* IP类型 : * 所属地域 :

客户名称 : 数据来源 :

联系人 : 联系电话 :

业务号 : 电子邮件 :

客户地址 :

- 点击”导入”按钮，弹出 ip 信息导入界面，如图：

导入




上传文件 :

[下载导入文件模板](#)

(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：

IP对象导入模板						
1、起止IP格式：'1.1.1.1-1.1.1.10' 2、起止IP、IP类型、所属地域为必填项						
起止IP	IP类型	所属地域	客户名称	客户地址	联系人	联系电话
192.168.68.189-192.168.68.200	动态	贵阳				

(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  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。

2.1.2 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

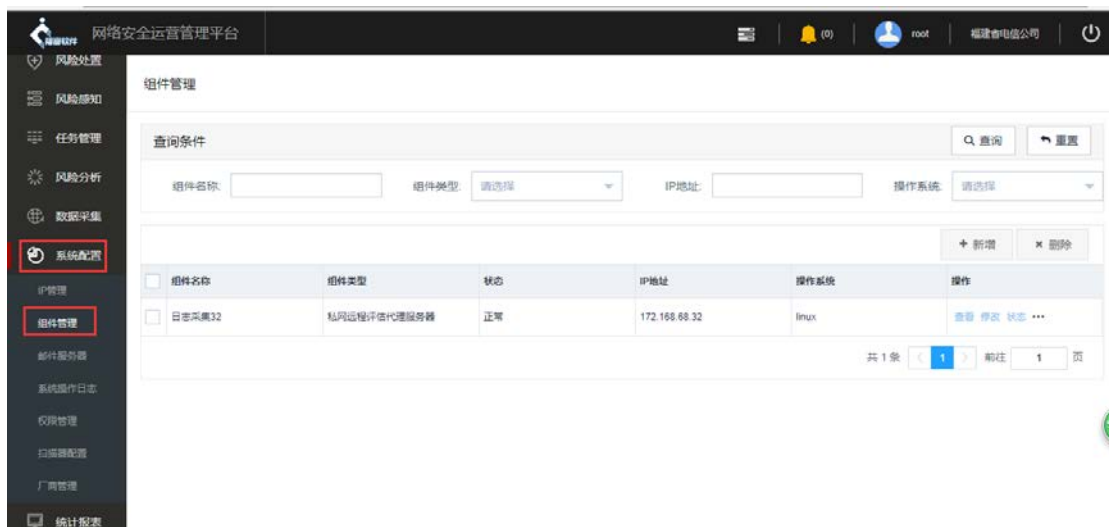


图 2-2 组件服务器配置

- 点击“新增”按钮，弹出组件新增界面，*号标识为必填，如图：

新增✕

* 组件名称：

* 组件类型：

* IP地址：

* 操作系统：

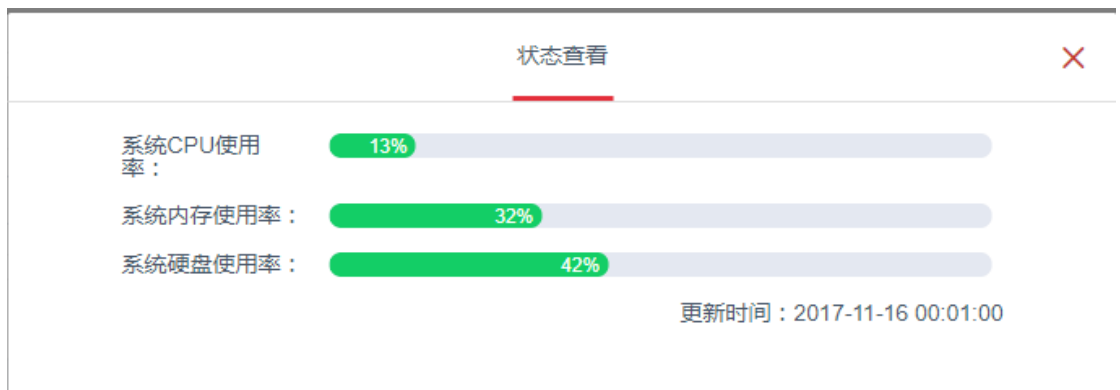
关闭提交

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 Q 查询 按钮，筛选组件服

务器，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。

组件管理



查询条件

组件名称: 32 | 组件类型: 采集服务器 X | IP地址: 172.168.68.32 | 操作系统: Linux操作系统 X

+ 新增 × 删除

组件名称	组件类型	状态	IP地址	操作系统	操作
日志采集32	私网远程评估代理服务器	正常	172.168.68.32	linux	查看 修改 状态 ...

共 1 条 < 1 > 前往 1 页

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：

邮件服务器管理



* SMTP服务器地址： smtp.189.cn

* 邮件发送账号地址： 15705988555@189.cn

* 邮件发送账号密码：


编辑

- 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  按钮即可，成功的话就提示成功，失败就提示失败。点

击  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：

系统操作日志							
查询条件							
用户名称:	<input type="text"/>	访问模块:	<input type="text"/>	开始时间:	<input type="text"/>	结束时间:	<input type="text"/>
用户名称	登录IP	访问模块	操作内容	发生时间	是否成功		
root	192.168.16.189, 127.0.0.1	邮件服务器	邮箱信息查询	2017-11-20 10:11:09	成功		
root	192.168.16.189, 127.0.0.1	邮件服务器	邮箱信息查询	2017-11-20 10:04:26	成功		
root	192.168.16.189, 127.0.0.1	邮件服务器	邮箱信息查询	2017-11-20 09:54:43	成功		
root	192.168.16.189, 127.0.0.1	邮件服务器	邮箱信息查询	2017-11-20 09:53:18	成功		
root	192.168.16.189, 127.0.0.1	IP管理	IP信息分页查询	2017-11-20 09:47:30	成功		
root	192.168.16.189, 127.0.0.1	IP管理	修改IP信息	2017-11-20 09:47:30	成功		
root	192.168.16.189, 127.0.0.1	IP管理	IP信息分页查询	2017-11-20 09:29:46	成功		
root	192.168.16.189, 127.0.0.1	IP管理	修改IP信息	2017-11-20 09:29:46	成功		

- 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：

扫描器配置							
查询条件							
扫描器设备名:	<input type="text"/>	设备类型:	<input type="text"/>	状态:	<input type="text"/>	设备IP:	<input type="text"/>
<input type="checkbox"/>	扫描器设备名称	IP地址	设备类型	管理员	状态	是否支持导入	操作
<input type="checkbox"/>	基础扫描器1	2.1.2.3	安全设备/安全扫描系统/...		正常	是	查看 修改 删除 ...
<input type="checkbox"/>	test	1.2.3.4	安全设备/安全扫描系统/安...	admin2	正常	是	查看 修改 删除 ...
<input type="checkbox"/>	test	1.2.3.4	安全设备/安全扫描系统/安...	admin	正常	是	查看 修改 删除 ...
<input type="checkbox"/>	test	1.2.3.4	安全设备/安全扫描系统/安...	admin	正常	是	查看 修改 删除 ...

- 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：

新增 ×

* 设备名称： <input style="width: 90%;" type="text"/>	
* 扫描方式： <input style="width: 45%;" type="text" value="请选择"/>	* 设备状态： <input style="width: 45%;" type="text" value="请选择"/>
* 设备类型： <input style="width: 95%;" type="text" value="请选择"/>	
* 设备IP： <input style="width: 45%;" type="text"/>	* 设备端口： <input style="width: 45%;" type="text"/>
* 并发数： <input style="width: 45%;" type="text"/>	* 权重(单位%)： <input style="width: 45%;" type="text"/>
用户名： <input style="width: 45%;" type="text"/>	密码： <input style="width: 45%;" type="text"/>
任务生存天数： <input style="width: 45%;" type="text"/>	管理员： <input style="width: 45%;" type="text"/>
* 是否支持导入： <input type="radio"/> 是 <input type="radio"/> 否	* 扫描网段类型： <input style="width: 45%;" type="text" value="请选择"/>
备注： <input style="width: 95%;" type="text"/>	

关闭提交

(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；

新增 ✕

* 设备名称：

* 扫描方式： * 设备状态：

* 设备类型：

* 设备IP： * 设备端口：

* 并发数： * 权重(单位%)：

* 用户名： * 密码：

任务生存天数： 管理员：

* 是否支持导入： 是 否 * 扫描网段类型：

备注：

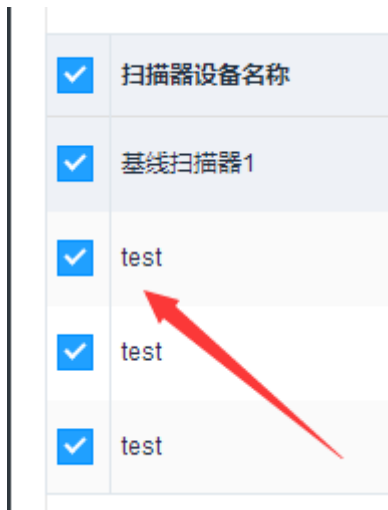
关闭 提交

(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 ✕ 删除 按钮，可批量删除扫描器信息，只

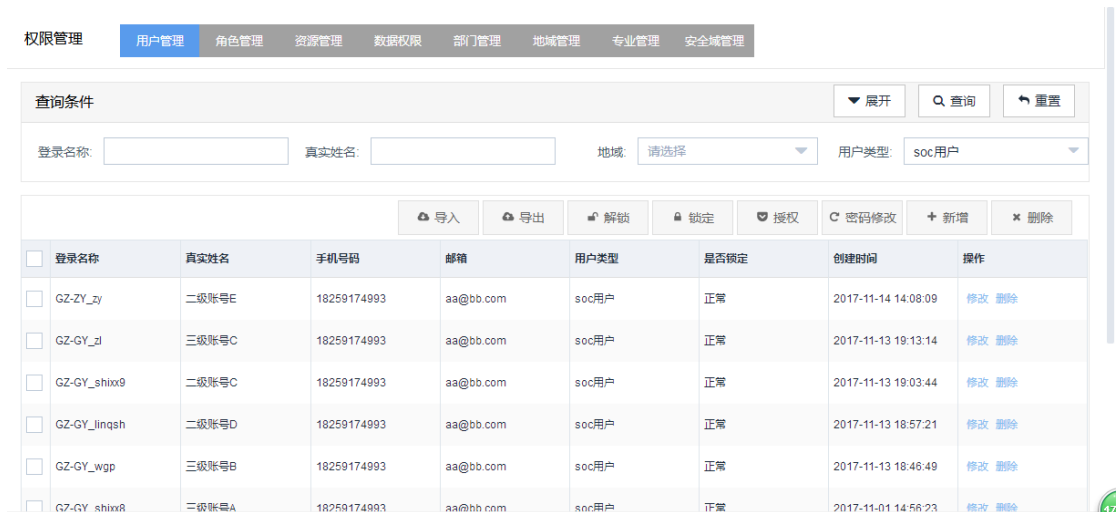
能批量删除当前页数据。



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：

The screenshot shows a user creation form with the following fields and values:

- 新增 ×
- * 用户类型：soc用户
- * 用户名称：系统管理员 * 登录名：root
- * 密码：..... 再次输入密码：.....
- * 手机号码：18259174993 固定电话：
- * 电子邮箱：ffcs@189.cn * 所属部门：福建电信
- 地域：遵义
- 安全域：维护域 ×
- 专业：接入网 ×
- 角色：超级管理员 ×
- 重置 提交

● 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：

密码修改 ×

* 密码：

再次输入密码：


● 用户授权

点击  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：

用户授权 ×

角色：

● 用户锁定/解锁

(1) 选择一个用户状态正常的用户，点击  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；

确认锁定用户？

(2) 选择一个锁定状态的用户，点击  按钮，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；

确认解锁用户？


取消

确定




● 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 **+ 新增角色** 按钮，根据提示输入信息，如图：

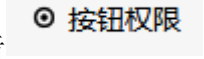
角色编码：只支持数字、字母、下划线，（长度 3-16 位）；

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：

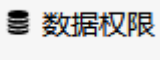


● 菜单权限

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 ，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：

权限管理

用户管理 角色管理 **资源管理** 数据权限 部门管理 地域管理 专业管理 安全域管理

查询条件

资源编码: 资源名称: 资源类型:

<input type="checkbox"/>	资源编码	资源名称	父资源	资源属性	类型	优先级	创建时间	操作
<input type="checkbox"/>	dataQuery_add	数据查询-导出	数据查询	/analyze/eventComm...	按钮	1	2017-07-08 21:10:40	修改 删除
<input type="checkbox"/>	Anomalies_del	异常流量专项-删除	告警结果	/unknown/unknown	按钮	1	2017-07-08 21:11:41	修改 删除
<input type="checkbox"/>	Anomalies_update	异常流量专项-修改	告警结果	/unknown/unknown	按钮	1	2017-07-08 21:11:41	修改 删除
<input type="checkbox"/>	Anomalies_add	异常流量专项-新增	告警结果	/unknown/unknown	按钮	1	2017-07-08 21:10:40	修改 删除
<input type="checkbox"/>	securityEventQuery_del	告警结果-删除	告警结果	/unknown/unknown	按钮	1	2017-07-08 21:11:41	修改 删除
<input type="checkbox"/>	securityEventQuery_u	告警结果-修改	告警结果	/unknown/unknown	按钮	1	2017-07-08 21:11:41	修改 删除

- 点击“新增”按钮，弹出新增资源界面，*号标识为必填项，如图：

新增 ×

* 资源编码:

* 资源名称:

* 菜单类型:

* 父资源:

* 优先级:

* 资源属性:

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：

权限编码：

* 权限名称：

* 优先级： - +

规则名称：

序号	规则编码	规则名称	表别名	运算符	操作
2	3	安全域过滤	asset_info.S...	and	删除

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：



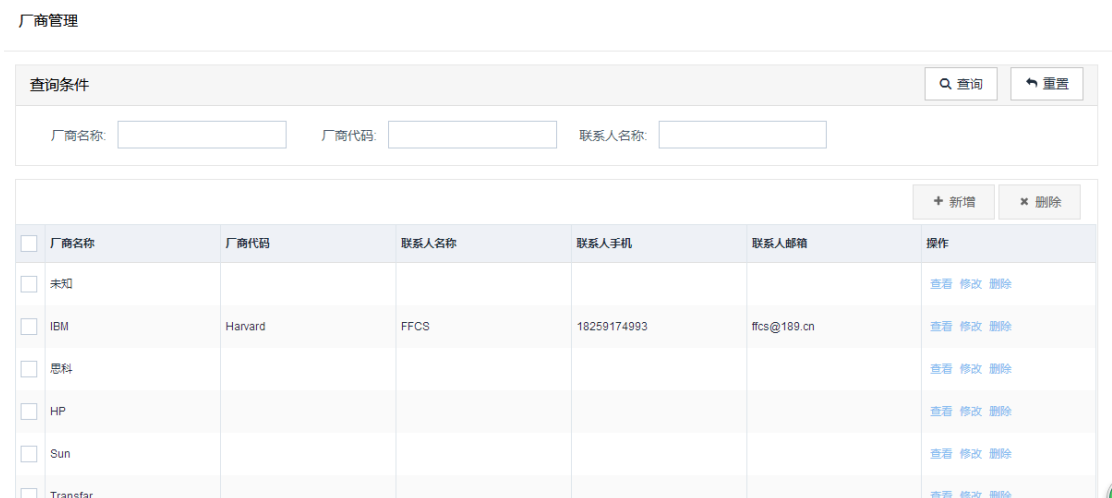
2.1.6.8 安全域管理

- 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：

新增

* 厂商名称：	<input type="text" value="IBM"/>	* 厂商代码：	<input type="text" value="Harvard"/>
* 联系人名称：	<input type="text" value="FFCS"/>	* 联系人手机：	<input type="text" value="18259174993"/>
* 联系人邮箱：	<input type="text" value="ffcs@189.cn"/>		

关闭
提交

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 ✕ 删除，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：

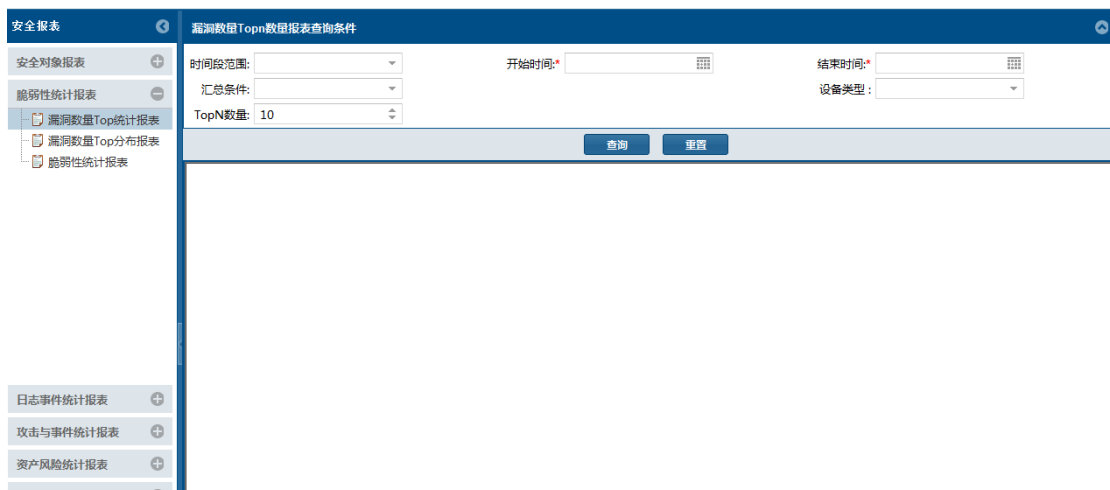


图 6-1 报表管理

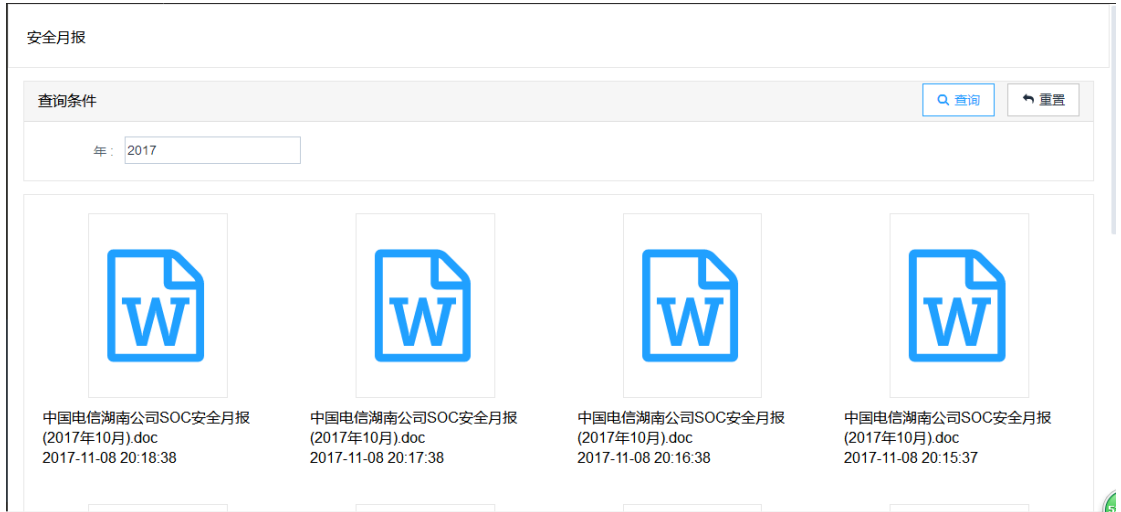
报表管理分为：

- 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：

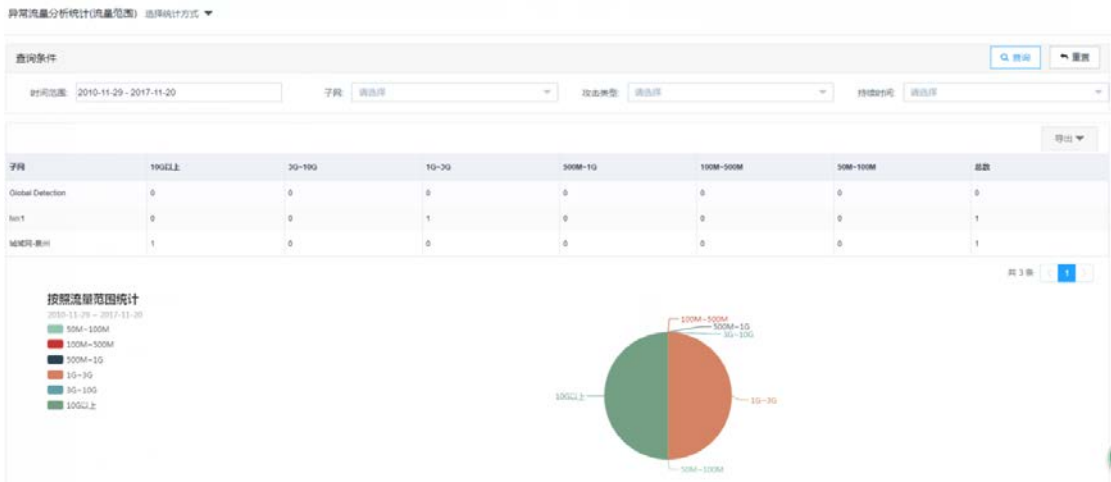


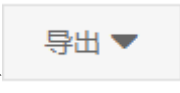
- 鼠标点击 word 文件，可下载月报；

2.2.2 异常流量分析报表

2.2.2.1 流量范围统计

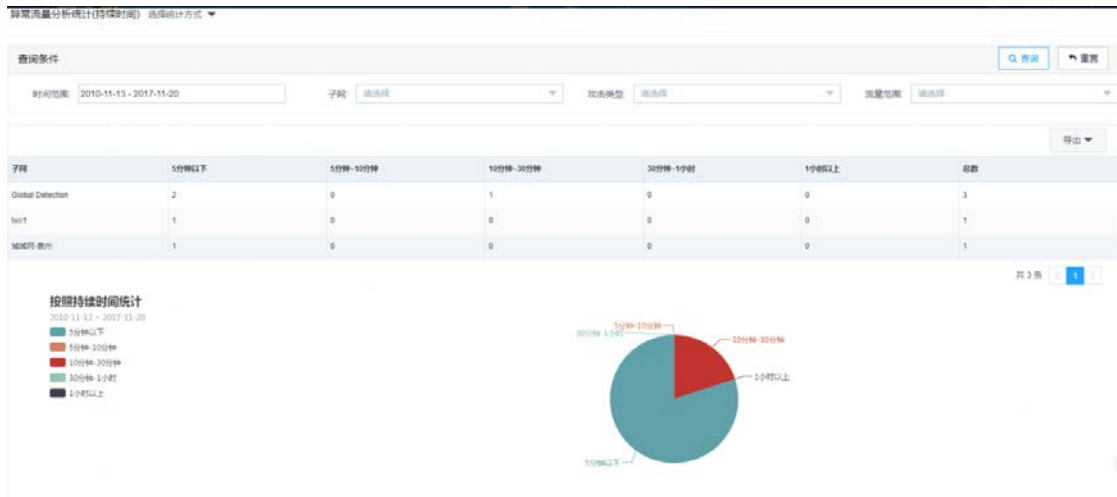
- 点击“统计报表”=>“异常流量分析报表”，默认展示按流量范围统计数据，如图：




- 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

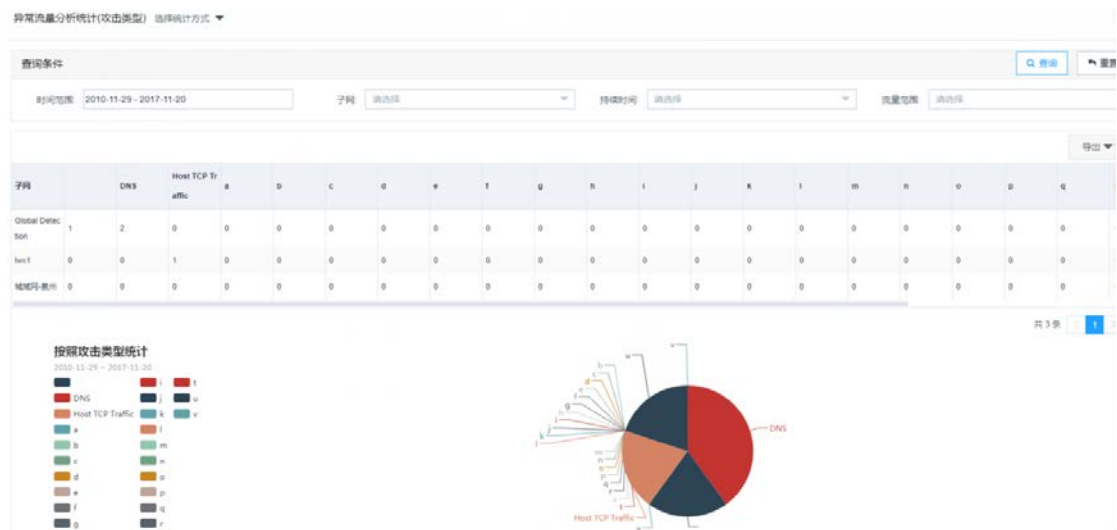
- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“持续时间”，如图：

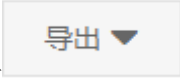


- 点击  按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.2.3 攻击类型分类统计

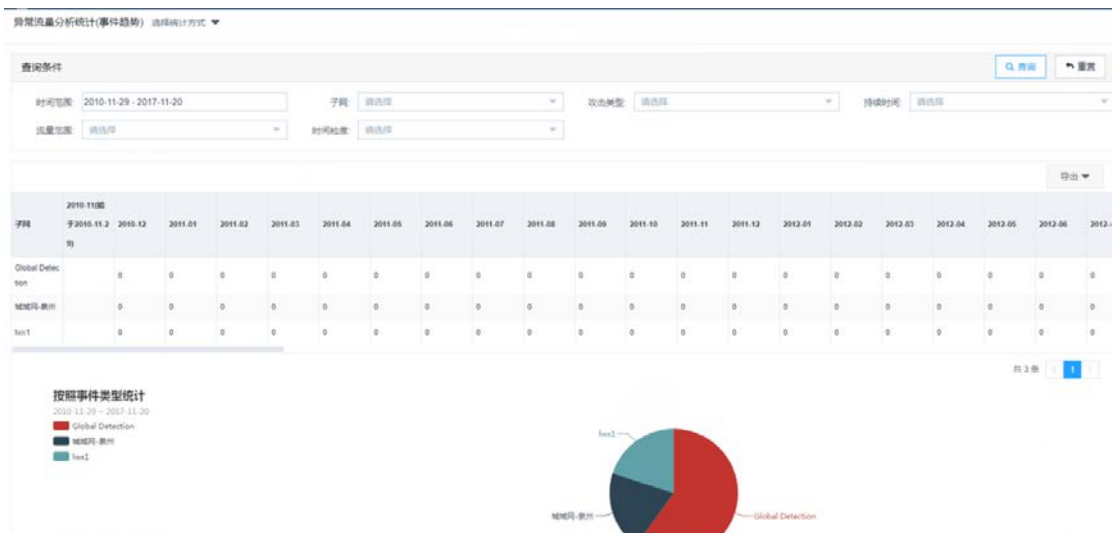
- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“攻击类型”，如图：

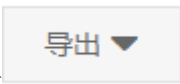


- 点击  按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.2.4 事件趋势统计

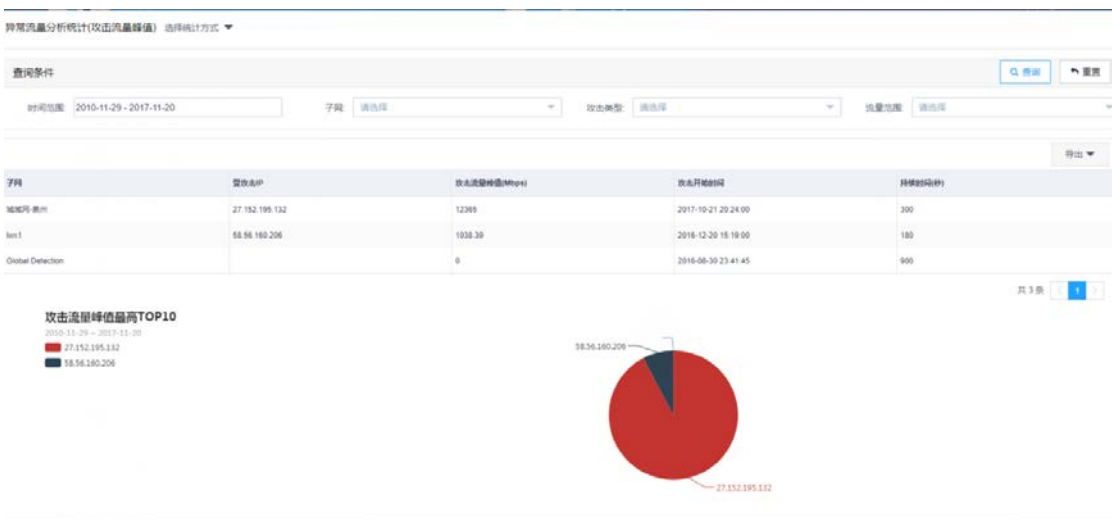
- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“事件趋势”，如图：

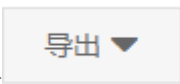


- 点击  按钮，可分别导出 word、pdf、excel 格式报表数据。

2.2.2.5 攻击流量峰值

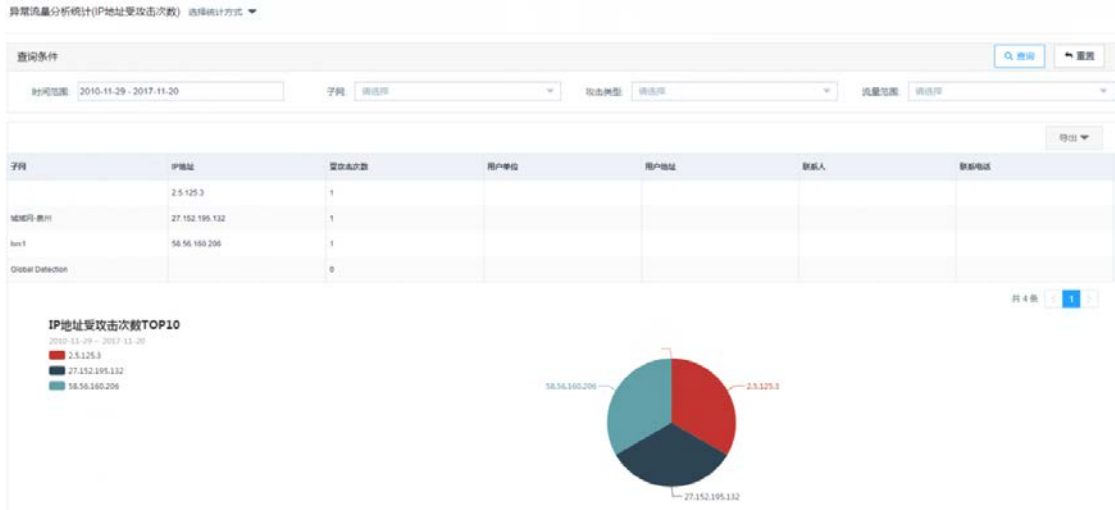
- 点击“统计报表”=>“异常流量分析报表”，统计方式选择“攻击流量峰值”，如图：




- 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

漏洞数量TopN数量报表查询条件

时间段范围: [] 开始时间*: [] 结束时间*: []

汇总条件: [] 设备类型: []

TopN数量: 10

[查询] [重置]

福富软件 2014 © 版权所有

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

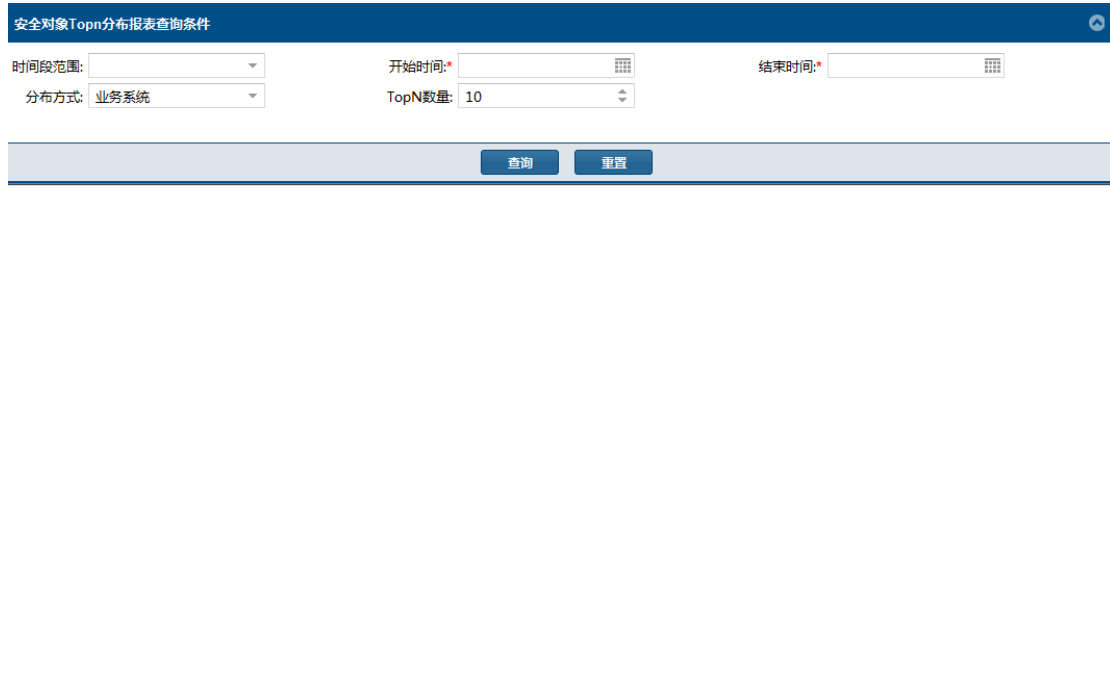
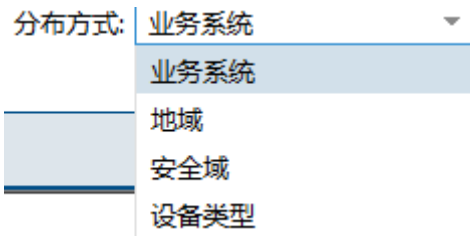


图 6-11 漏洞数量 TOP 分布报表选择

- 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

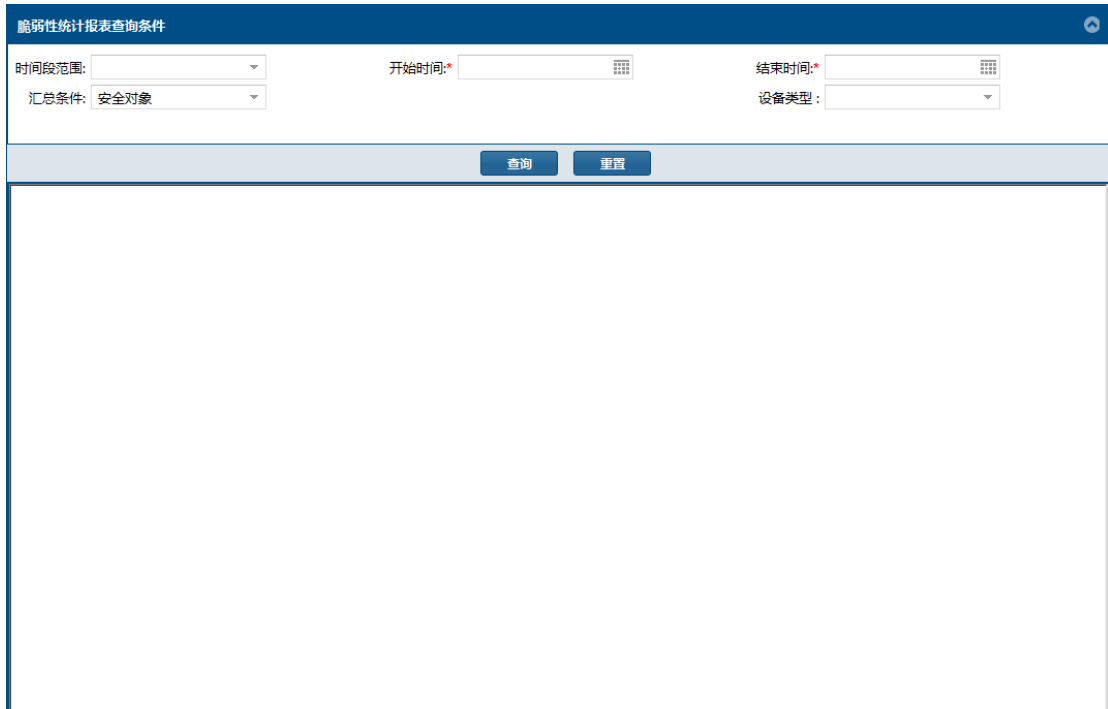


图 6-15 脆弱性统计报表选择

- 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

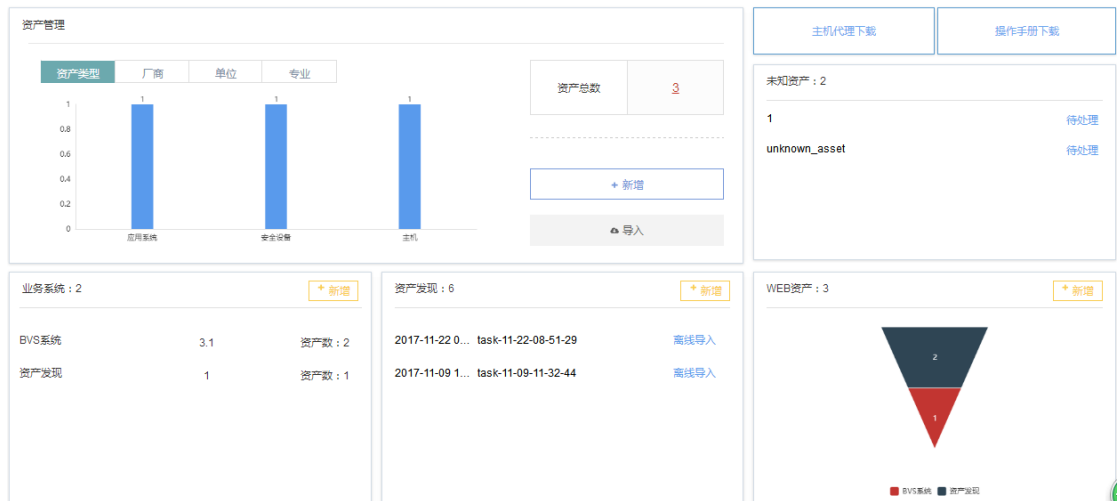
2.2.4.3 未知资产维度统计

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：

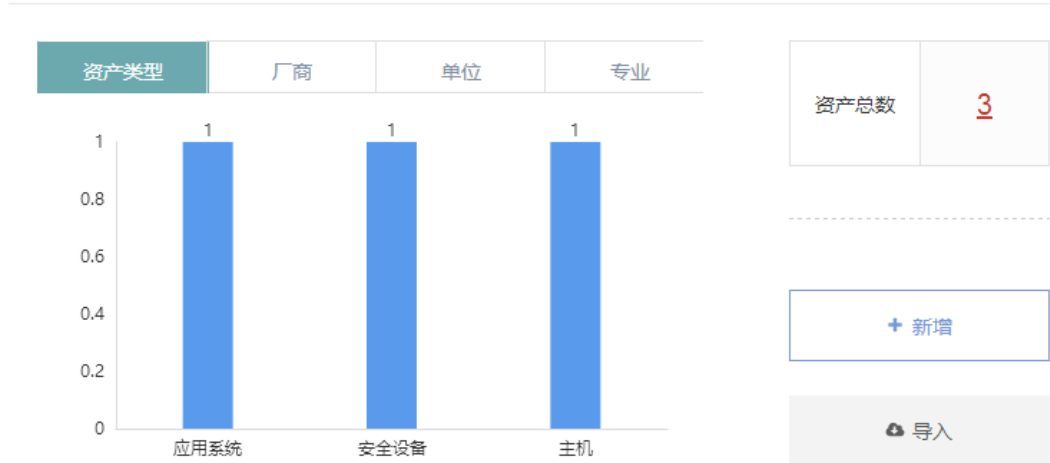


● 资产模块

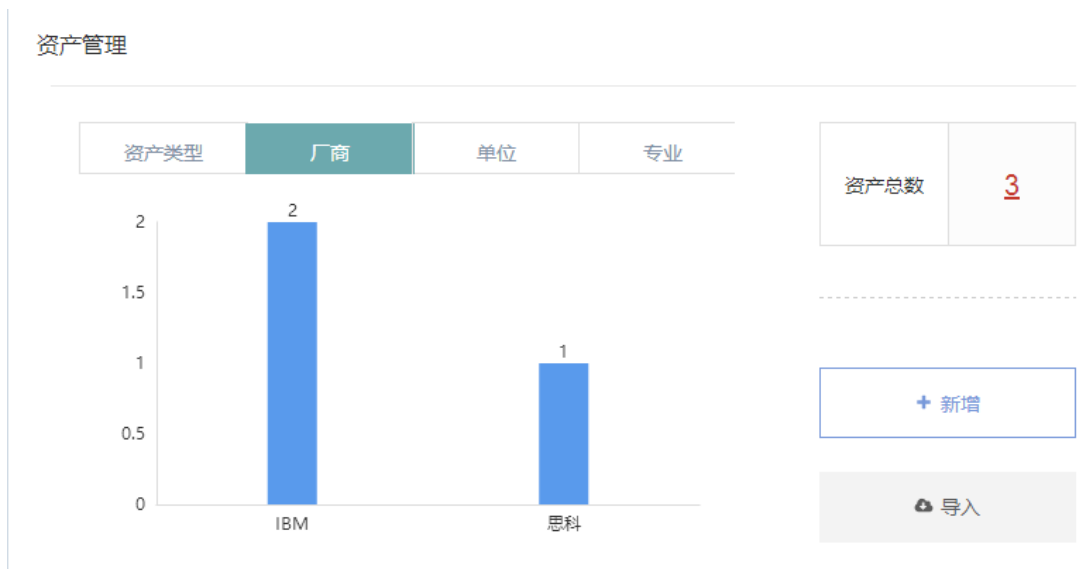
左侧按不同维度展示资产柱形图，鼠标点击柱形图可下钻至资产详情页；右侧统计资产总数，并提供资产新增、导入入口。

(1) 按资产类型维度统计，如图：

资产管理



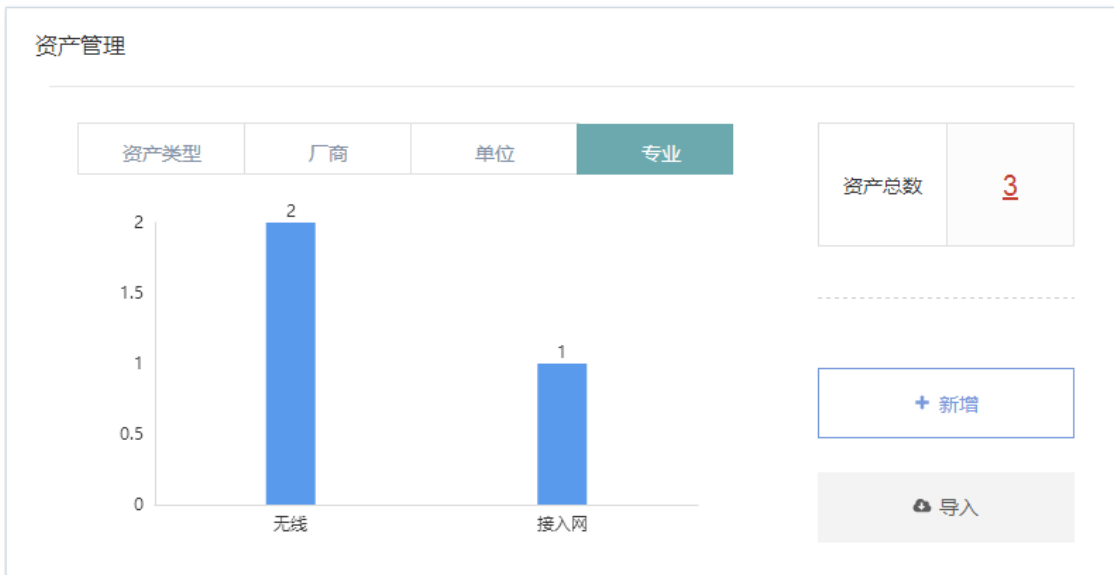
(2) 按资产厂商维度统计，如图：



(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：

The screenshot shows a card titled '业务系统 : 7' with a '+ 新增' button. Below the title is a table with 5 rows. The columns are Business System Name, Business System Rating, and Asset Count.

业务系统名称	业务系统定级等级	资产数量
内网扫描系统	3.1	资产数 : 56
BVS业务系统	2.2	资产数 : 4
agent属性获取系统	2.2	资产数 : 3
外网扫描系统	2.2	资产数 : 1
资产发现后端测试		资产数 : 1

- **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。

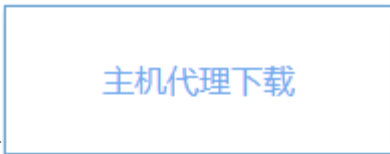


- WEB 资产模块

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：



主机代理下载

1 填写信息 2 代理下载

* 业务系统： 请选择 * 所属安全域： 请选择

* 所属地域： 请选择 资产等级： 请选择

系统类型： 请选择 所属专业： 请选择

前置机地址：


所属单位： 所属部门：

责任人： 安全管理员：

关闭 提交

(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。

主机代理下载 ✕

✓
2

填写信息
代理下载

代理软件下载：

suse-32	AIX-PPC	suse-64	solaris-32
windows-64	HP-UX-64	centos-64	AIX-PPC64
centos-32	ubuntu-64	redhat-32	solaris-64
ubuntu-32	redhat-64	windows-32	

关闭
提交

- 操作手册下载



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：

资产管理

查询条件 ▼ 展开 🔍 查询 ↺ 重置

资产名称: 业务系统: 所属专业: 资产IP地址:

📄 导入
📄 导出
📄 分维度导出
+ 新增
✕ 删除

资产名称	主识别IP	资产类别	业务系统	部门	专业	地域	安全域	是否安装agent	agent状态	创建时间	操作
asset_BVS	134.128.217.32	主机	BVS业务...	福州分公司	接入网	福州	网络域	否		2017-11-1...	查看 修改 删除 ...
asset_bvs...	134.130.5.208	主机	BVS业务...	福州分公司	接入网	福州	网络域	否		2017-11-1...	查看 修改 删除 ...
172.168.6...	172.168.68.229	应用系统	资产发现...	福州分公司		福州	网络域	否		2017-11-1...	查看 修改 删除 ...
asset_bvs...	134.130.5.210	虚拟机	BVS业务...	福州分公司	接入网	福州	网络域	否		2017-11-1...	查看 修改 删除 ...
asset_器...	172.21.133.73	主机	BVS业务...	福州分公司	接入网	福州	网络域	否		2017-10-2...	查看 修改 删除 ...
asset_inf...	1.2.3.4	主机	agent属性...	福州分公司	无线	福州	维护域	否		2017-10-2...	查看 修改 删除 ...

- 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：

通用属性
特有属性
扩展属性

必填信息
×

! 公网IP、DCN网IP、私网IP、CN2网IP至少填写一种,多个用英文逗号隔开

资产名称: <input type="text"/>	业务系统: <input type="text"/>	系统类型: <input type="text"/>	主识别IP: <input type="text"/>
安全域: <input type="text"/>	地域: <input type="text"/>	所属单位: <input type="text"/>	所属部门: <input type="text"/>
资产类别: <input type="text"/>	资产小类: <input type="text"/>	专业: <input type="text"/>	安全等级: <input type="text"/>
责任人: <input type="text"/>	责任人电话: <input type="text"/>	责任人手机: <input type="text"/>	责任人邮箱: <input type="text"/>
完整性: <input type="text"/>	机密性: <input type="text"/>	可用性: <input type="text"/>	资产来源: <input type="text"/>
公网IP: <input type="text"/>	DCN网IP: <input type="text"/>	私网IP: <input type="text"/>	CN2网IP: <input type="text"/>
操作系统类型: <input type="text"/>	操作系统版本: <input type="text"/>		

非必填信息

通用属性
特有属性
扩展属性

必填信息

非必填信息

资产等级: <input type="text"/>	资产物理位置: <input type="text"/>	私网扫描代理组件: <input type="text"/>	资产编号: <input type="text"/>
资产型号: <input type="text"/>	资产厂商: <input type="text"/>	上线日期: <input type="text"/>	管理协议: <input type="text"/>
采集方式: <input type="text"/>	日志采集方式: <input type="text"/>	异常流量阈值: <input type="text"/>	允许扫描: <input type="text"/>
浮动IP: <input type="text"/>			

远程登录方式: <input type="text"/>	远程登录方式	用户名	操作
<input type="text"/>			
<input type="text"/>			
<input type="text"/>			

(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：

导入导出任务列表		
exportAssetInfo_20171116212507.xlsx	2017-11-16 21:25:55	导入成功
exportAssetInfo_20171116193525.xlsx	2017-11-16 20:09:07	导入成功
exportAssetInfo_20171116193525.xlsx	2017-11-16 20:07:17	导入失败
exportAssetInfo_20171116193525.xlsx	2017-11-16 20:03:31	导入失败
exportAssetInfo_20171116193525.xlsx	2017-11-16 19:58:42	导入失败
exportAssetInfo_20171116193525.xlsx	2017-11-16 19:56:31	导入成功

< **1** 2 3 4 5 >

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：

! 失败原因: 第10行: 数据库存在相同的业务系统【agent业务系统】和主识别IP【2.3.4.5】和资产类别【网络设备】和资产小类【其他】

(2) 点击 **导出** 按钮，弹出资产导出模板选择界面，如图：

导出 ×

* 导出模版：


请选择导出模版

SOC模版
 集团模版

① 选择“SOC 模版”，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：

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
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
VIN-A46SLFSBHCI	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
VIN-A46SLFSBHCI_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
VIN-A46SLFSBHCI_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
VIN-A46SLFSBHCI_nslnx_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
189_11S_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
189_1boss_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
189_qlserver_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
VIN-A46SLFSBHCI_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	信息安全部门
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	信息安全部门

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：

导入导出任务列表




exportAssetInfo_20171121152029.xlsx

2017-11-21 15:20:28

导出成功

导出文件内容如图：

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
编号	省份	资产名称	资产类别	所属地域	所属单位	所属部门	责任人	责任人电话												
	1 海南省	asset_不确定漏洞统计	主机	福州	省NOC	福州分公司	鲁豪处理B													
	2 海南省	WIN-A46SLFS8HCI	虚拟机	福州	省NOC	信息安全部门	鲁豪处理A													
	3 海南省	WIN-A46SLFS8HCI.ora	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	4 海南省	WIN-A46SLFS8HCI.pos	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	5 海南省	WIN-A46SLFS8HCI.ngin	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	6 海南省	189_jis_80	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	7 海南省	189_jboss_8085	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	8 海南省	189_sqlserver_1434	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	9 海南省	WIN-A46SLFS8HCI.apa	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	10 海南省	189_weblogic_7001	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	11 海南省	WIN-A46SLFS8HCI.web	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	12 海南省	WIN-A46SLFS8HCI.zab	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	13 海南省	WIN-A46SLFS8HCI.bin	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	14 海南省	WIN-A46SLFS8HCI.mei	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	15 海南省	WIN-A46SLFS8HCI.sou	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	16 海南省	WIN-A46SLFS8HCI.acg	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	17 海南省	win_xp	虚拟机	福州	省NOC	信息安全部门	鲁豪处理A													
	18 海南省	189_oracle_1521	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	19 海南省	win_xp_jis_80	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													
	20 海南省	win_xp_tomcat_8080	应用系统	福州	省NOC	信息安全部门	鲁豪处理A													

- 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。

2.3.3 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：

扩展属性配置

<input type="checkbox"/>	属性中文名称	属性英文名称	扩展对象类型	属性表单类型	是否必填	创建时间	创建人	操作
<input type="checkbox"/>	接口状态	status	自营普通资产	文本框	是	2017-11-21 16:58:23	root	查看 修改 删除

共 1 条 < 1 > 前往 1 页

- 点击“新增”按钮，弹出新增界面，*号标识为必填项，如图：

新增 ✕

* 属性中文名称：

* 属性英文名称：

* 扩展对象类型：

* 是否必填：

* 属性表单类型：

(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

查询条件 ▼ 展开 🔍 查询 ↺ 重置

域名: 网站名称: 业务系统: IP地址:

📁 导入

<input type="checkbox"/>	域名	网站名称	IP地址	业务系统	部门	端口	协议	责任人	创建时间	操作
<input type="checkbox"/>	https://172.168.68.229/index.html	sina	172.168.68...	BVS系统	中电福雷	8089	https	遵义A	2017-11-21 16:08:32	查看 修改 删除
<input type="checkbox"/>	https://172.168.68.33/index.html	曹nsoc	172.168.68.33	资产发现	中电福雷	8080	http	二级账号E	2017-11-21 16:07:37	查看 修改 删除
<input type="checkbox"/>	https://172.168.68.32/index.html	nsoc	172.168.68.32	BVS系统	中电福雷	8081	https	遵义A	2017-11-21 15:09:19	查看 修改 删除

共 3 条 < 1 > 前往 1 页

- 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：

WEB资产新增

基础信息 管理信息 维护信息 服务信息 扩展属性

* 域名： * 网站名称：

* 是否属于产业/业务平台： 是 否 * 是否安全评估： 是 否

产品/业务名称：


* 是否允许扫描： 是 否

所属单位：

所属部门：

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：



导入 ×

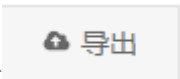
上传文件：

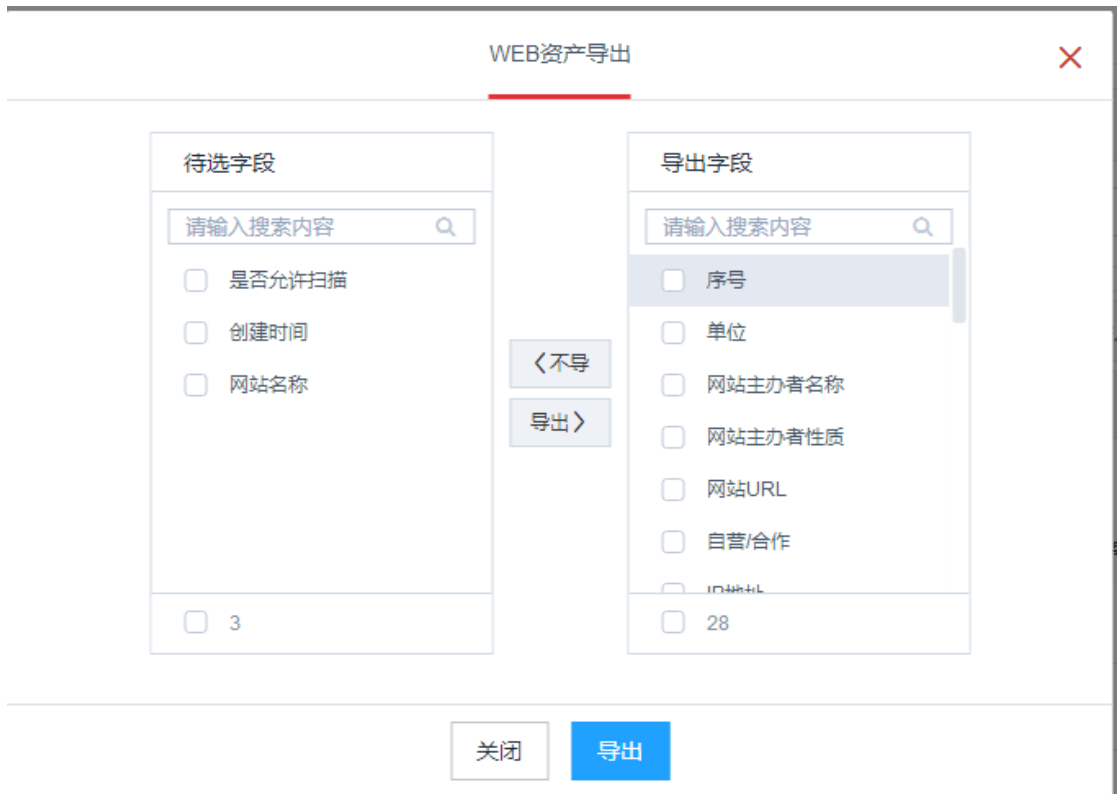
[下载导入文件模板](#)

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：

WEB资产导入模板													
【是否属于产业/业务平台选否时 产品/业务名称必填】													
端口	IP地址归属单位是否电信	IP地址归属单位名称	接入方式	是否ICP备案	备案号	网站性质	网站主办者名称	网站主办者性质	自营/合作	是否属于产业/业务平台	产品/业务名称【请填写此项不填】	是否已进行安全评估	网站

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
	网站URL	自营/合作	IP地址	IP地址归属单位是否电信
1				
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				
6				

- 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

查询条件 ▼ 展开 Q 查询 ↶ 重置

业务系统名称: 所属部门: 所属专业: 责任人:

📁 导入 📄 导出 + 新增 ✖ 删除

<input type="checkbox"/>	业务系统名称	所属部门	所属专业	系统类型	定级等级	操作
<input type="checkbox"/>	资产发现	中电福富	接入网	电信自用系统	1	查看 修改 一键评估 ...
<input type="checkbox"/>	BVS系统	中电福富	无线	电信自用系统	3.1	查看 修改 一键评估 ...

共 2 条 < 1 > 前往 1 页

● 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：

✖

基本信息 管理员信息 网络信息

* 业务系统名称: * 系统类型:

* 所属部门: 所属专业:

定级等级: 是否为备案系统: 是 否

物理位置: 最多输入66个字


系统描述: 最多输入100个字

关闭 提交

(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：

业务系统对象导入模板						
1: 业务系统名称,部门, 责任人, 安全管理员,系统类型为必填, 网段必须填写一种.						
所属物理地址	公网	DCN	CN2	私网	其他	安全管理员

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：

A	B	C	D	E	F	G
业务系统名称	系统类型	所属部门	定级等级	所属物理地址	安全管理员	责任人
1 外网扫描系统	电信自用系统	福州分公司	2.2		责任人C	备案处理B
3 内网扫描系统	面向公众的增值业	信息安全部门	3.1		责任人C	备案处理A
4 101001业务系统	电信自用系统	福州分公司			测试员123	测试123
5 内网扫描系统2	电信自用系统	信息安全部门	2.2		备案处理B	绑定测试
6 BUS业务系统	面向公众的增值业	福州分公司	2.2		备案处理B	主罚责任人A
7 资产发现01	电信自用系统	福州分公司			系统管理员	主罚责任人A
8 agent属性获取系统	面向公众的增值业	福州分公司	2.2		测试123	备案处理A
9 资产发现后端测试	电信自用系统	福州分公司			备案处理A	中大阳

- 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

查询条件

任务名称: 状态: 创建时间:

<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作
<input type="checkbox"/>	task-11-22-08-51-29	离线	root	2017-11-22 09:12:31	创建	查看 修改 导入 ...
<input type="checkbox"/>	task-11-21-15-08-30	离线	root	2017-11-21 15:29:33	完成	查看 删除
<input type="checkbox"/>	task-11-13-15-54-06	在线	root	2017-11-13 16:14:09	创建	查看 修改 删除
<input type="checkbox"/>	资产	在线	root	2017-11-13 15:32:03	创建	查看 修改 删除
<input type="checkbox"/>	task-11-09-11-32-44	离线	root	2017-11-09 11:32:15	创建	查看 修改 导入 ...

● 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：

资产发现新增

任务名称：

* 任务类型： 在线 离线

* 扫描周期： 实时 定时 周期

端口范围：

* IP网段：

起止地址	操作
暂无数据	

资产发现新增

任务名称：最多输入32个字符

* 任务类型： 在线 离线

* 选择业务系统：请选择

指派业务系统负责人 指派完成人 上传结果文件


请重新选择业务系统

× 关闭 提交

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：

查询 ×

业务系统名： 所属部门：

所属专业： 系统类型：

业务系统名

资产发现

BVS系统

IP范围 - 全选

172.168.68.229/32

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：

* IP网段：

起止地址	操作
172.168.68.229/32	删除

(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：

* 选择业务系统：

指派业务系统负责人
 指派完成人
 上传结果文件

① 指派业务系统负责人：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：

<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作
<input type="checkbox"/>	task-11-22-08-51-29	离线	root	2017-11-22 09:12:31	创建	查看 修改 导入 ...

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：

主机代理

查询条件 Q 查询 重置

资产名称: 业务系统: IP: 中转IP:

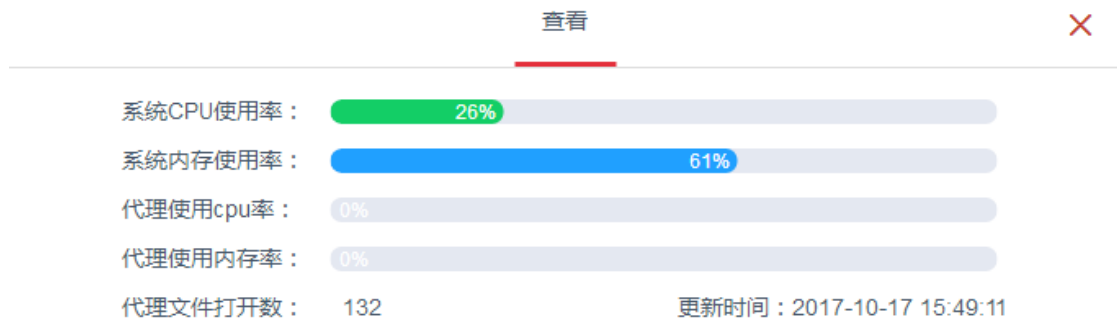
代理更新

<input type="checkbox"/>	代理ID	资产名称	IP	当前版本	中转IP	操作
<input type="checkbox"/>	DED8CAD40B5D3339175F366B1EE68FA9	WIN-A46SLFS8HCI	172.168.68.39	1.5.2	172.168.68.250	查看
<input type="checkbox"/>	007E5B3EA27CA8BD360E0757623DD080	win_xp	172.168.68.43	1.5.2	172.168.68.250	查看
<input type="checkbox"/>	ecc832cb6a55982feb6d8e6af08f6e37	189	172.168.68.174	1.5.2	172.168.68.250	查看
<input type="checkbox"/>	967f832dc76db3790d19d149e46b6a2	solaris188	172.168.68.188	1.5.2	172.168.68.250	查看

共 4 条 < 1 > 前往 1 页

● 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：

代理更新 ✕

* 操作系统： * 版本号：

安装文件： [选取文件](#)

关闭 上传

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：

未知资产处理

(3) 回退

责任人选择回退，可将任务回退给上级管理员，如图：

未知资产处理



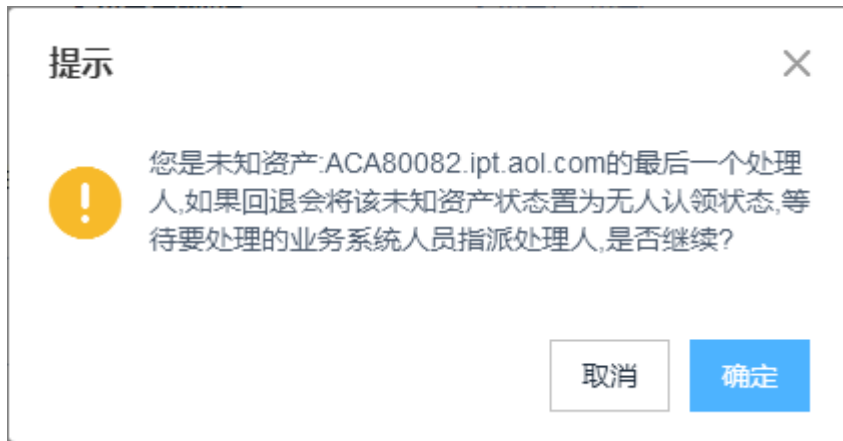
处置流程：

1 未知资产-指派 (已完成) → 2 未知资产-处理 (当前) → 3 未知资产-审核 → 4 未知资产-完成

处理 指派 回退


*描述：

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：

未知资产处理

处置流程：

● 指派

* 指派处理用户：

- 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：

处理历史 ✕

日期	状态	操作说明	下一处理人
2017-11-24 16:34:37	待处理	已指派待处理	系统管理员
2017-11-24 16:34:22	待指派 (审核未通过)	不通过	二级账号E
2017-11-24 16:34:15	已处理(待审核)	已处理待审核	二级账号E
2017-11-24 16:07:53	待处理		二级账号E

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。

The screenshot shows a task configuration form with the following fields and options:

- 任务名称: 147流量分析
- * 任务类型: 流量分析 (dropdown menu)
- * 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: WIN-41IECU79AV7 (with a red 'x' icon)
- 任务内容: {"ipaddress":"172.168.68.142","count":10,"filter":"","ifupload":"true"}

A "查询" (Query) button is located to the right of the "选择资产" field.

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；

省侧自建任务 查看

任务名称: agentTask-06-01-09-47-31

* 任务类型: 检测running_procs

* 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: centos6

任务内容:

查询

关闭

(3) 结果查看：
任务采集结束后，在结果查看里展示。

代理客户端 集团下发任务 省侧自建任务 实时监控策略 实时监控模版

查询条件 查询 重置

任务类型: 监控ROOTKITS 任务状态: 请选择 创建时间: -

任务名称	任务类型	任务状态	创建时间	操作
142监控ROOTKITS	监控ROOTKITS	已下发	2020-05-27 15:31:50	查看 重新下发 删除 ...

共 1 条 < 1 结果查看 1 页

任务结果查看

查询条件 查询 重置

资产名称: 主识别IP: 业务系统: 请选择 所属部门: 请选择

资产名称	部门名称	业务系统名称	主识别IP	任务状态	结果时间	最新结果
centos6	测试部	中国固定电话网浙江省信...	172.168.68.142	采集任务完成	2020-07-27 17:02:42	0个rootkits文件

共 1 条 < 1 前往 1 页

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；

省侧自建任务 查看

任务名称：

* 任务类型：

* 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：

任务内容：

(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。

资产名称	部门名称	业务系统名称	主机IP	任务状态	结束时间	最后结果
Redhat7.2	测试部	中国宝通集团浙江省证券类资产系统	172.168.66.195	采集任务完成	2020-06-15 10:12:53	find arp num: 4

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：

省侧自建任务 查看

任务名称: 165_175_180_185_188_资产采集

* 任务类型: 资产采集策略

* 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:

hbase180	centos_165
175_rhet4	caswl-desktop

查询

任务内容: [{"flag": 2,

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:

省侧自建任务 查看

任务名称：

* 任务类型：

* 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

* 选择部门：

系统类型：

任务内容：

(3) 结果查看：

任务采集结束后，在结果查看里展示。

查询条件

任务类型： 任务状态： 创建时间：

任务名称	任务类型	任务状态	创建时间	操作
agentTask-08-25-19-11-28	弱口令	已下发	2020-08-25 19:11:57	查看 重新下发 删除 ...
弱口令按业务系统	弱口令	审核通过	2020-04-02 17:06:28	查看 删除 结果查看
资产采集策略-test	弱口令	已下发	2020-03-13 11:43:41	查看 重新下发 删除 ...

资产名称： 主识别IP： 业务系统： 所属部门：

资产名称	部门名称	业务系统名称	主识别IP	任务状态	结果时间	最新结果
rhel_177	测试部	中国固定电话网浙江省信...	172.168.68.177	待下发	2020-06-30 15:52:16	存在弱口令账号：root
centos_171	测试部	中国固定电话网浙江省信...	172.168.68.171	待下发	2020-06-30 15:52:12	不存在弱口令账号
rhel_179	测试部	中国固定电话网浙江省信...	172.168.0.179	待下发	2020-06-30 15:52:05	不存在弱口令账号
182	测试部	中国固定电话网浙江省信...	172.168.68.182	待下发	2020-06-30 15:51:11	不存在弱口令账号
server	测试部	中国固定电话网浙江省信...	172.168.68.178	待下发	2020-06-30 15:50:39	存在弱口令账号：root
master	测试部	中国固定电话网浙江省信...	172.168.68.192	待下发	2020-06-30 15:50:32	不存在弱口令账号
173	测试部	中国固定电话网浙江省信...	172.168.68.173	待下发	2020-06-30 15:49:54	不存在弱口令账号
CentOS7	测试部	中国固定电话网浙江省信...	172.17.0.1	待下发	2020-06-30 15:49:34	不存在弱口令账号
centos167	测试部	中国固定电话网浙江省信...	123.168.68.167	待下发	2020-06-30 15:48:58	不存在弱口令账号
#181	测试部	中国固定电话网浙江省信...	172.168.68.181	待下发	2020-06-30 15:47:52	不存在弱口令账号

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：

The screenshot shows a web-based configuration form for a '强制采集' (Forced Collection) task. The form is organized into several sections:

- Task Name:** A text input field containing '强制采集test'.
- Task Type:** A dropdown menu with '强制采集' selected.
- Cycle Type:** Three radio buttons: '实时' (Real-time, selected), '定时' (Scheduled), and '周期' (Periodic).
- Task Object:** Three radio buttons: '按资产' (By Asset, selected), '按业务系统' (By Business System), and '按部门' (By Department).
- Select Assets:** A search box containing two asset tags: 'centos_165' and '#linux'. A '查询' (Search) button is located to the right of the search box.
- Task Content:** A large text area for entering task details.

- (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；

资产管理 主机代理

查询条件

资产名称: 业务系统: IP: 中转IP:

代理ID	资产名称	IP	当前版本	中转IP	操作
d0c212ba67d79b7d58371ac8...	173	172.168.68.173	4.8.0	172.168.68.160	性能查看 日志查看
915c35a3b80d4908404a20f68...	centos_171	172.168.68.171	4.7.9	172.168.68.160	性能查看 日志查看
c38ea35f71d9585bc58ca53be...	Redhat7.2	172.168.68.195	9.6.4		性能查看 日志查看
13b33543f2f44dc0c04d0d27...	localhost.localdomain	172.168.68.150	4.5.0	172.168.68.160	性能查看 日志查看
505f8cde2ec530a5d103280950...	rhel_177	172.168.68.177	4.8.0	172.168.68.160	性能查看 日志查看

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;

省侧自建任务 查看

任务名称:

* 任务类型:

* 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:

任务内容:

(3) 结果查看：

查看任务结果中任务状态和结果时间；

任务结果查看

资产名称	部门名称	业务系统名称	主识别IP	任务状态	结果时间	最新结果
centos_165	测试部	中国固定电话网浙江省信...	172.168.88.165	采集任务完成	2020-09-10 15:12:18	

共 1 条 < 1 > 前往 1 页

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

省侧自建任务 查看

任务名称：	agentTask-09-14-11-16-19
* 任务类型：	获取agent日志
* 周期类型：	<input checked="" type="radio"/> 实时 <input type="radio"/> 定时 <input type="radio"/> 周期
* 任务对象：	<input checked="" type="radio"/> 按资产 <input type="radio"/> 按业务系统 <input type="radio"/> 按部门
* 选择资产：	localhost.localdomain localhost.localdomain_mysql_3306
任务内容：	CTFFAgent.log.2020-09-10

查询

(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：

任务结果查看 ✕

查询条件 🔍 查询 ↶ 重置

资产名称: 主识别IP: 业务系统: 所属部门:

资产名称	部门名称	业务系统名称	主识别IP	任务状态	结果时间	最新结果
hadoop2	测试部	中国固定电话网浙江省信...	172.168.68.172	采集任务完成		
170	测试部	中国固定电话网浙江省信...	172.168.68.170	采集任务完成		
server	测试部	中国固定电话网浙江省信...	172.168.68.178	采集任务完成		
hbase180	测试部	中国固定电话网浙江省信...	172.168.68.180	采集任务完成		

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；

省侧自建任务 查看

任务名称:

* 任务类型:

* 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:

hbase180

server

centos_165

RHEL176

169

caswl-virtual-machine

170

182

hadoop2

- (3) 结果查看：
查看任务结果中任务状态：

任务结果查看

查询条件

资产名称: 主识别IP: 业务系统: 所属部门:

资产名称	部门名称	业务系统名称	主识别IP	任务状态	结果时间	最新结果
hadoop2	测试部	中国固定电话网浙江省信...	172.168.68.172	采集任务完成		
170	测试部	中国固定电话网浙江省信...	172.168.68.170	采集任务完成		
server	测试部	中国固定电话网浙江省信...	172.168.68.178	采集任务完成		
hbase180	测试部	中国固定电话网浙江省信...	172.168.68.180	采集任务完成		

2.3.9.1.16 应用监控任务:

(1) 新增监控策略:

资产管理

代理客户端 集团下发任务 自制自研任务 **实时监控策略** 实时监控策略

查询条件

资产名称: 资产IP: 资产类别: 资产小类:

下批策略 停止策略 **+ 新增** X 删除

ID	资产名称	资产类型	主ip	监控项数量	告警项数量	任务状态	策略状态	创建时间	操作
<input type="checkbox"/>	hadoop2	虚拟机	192.168.39.109	7	0	采集任务完成	启用	2020-05-07 17:20:52	编辑 删除 查看详情
<input type="checkbox"/>	server5	虚拟机	192.168.39.100	7	0	采集任务完成	启用	2020-05-07 17:20:33	编辑 删除 查看详情

共 2 条 < 1 > 前往 1 页

代理更新

代理客户端

策略管理

web网站发现

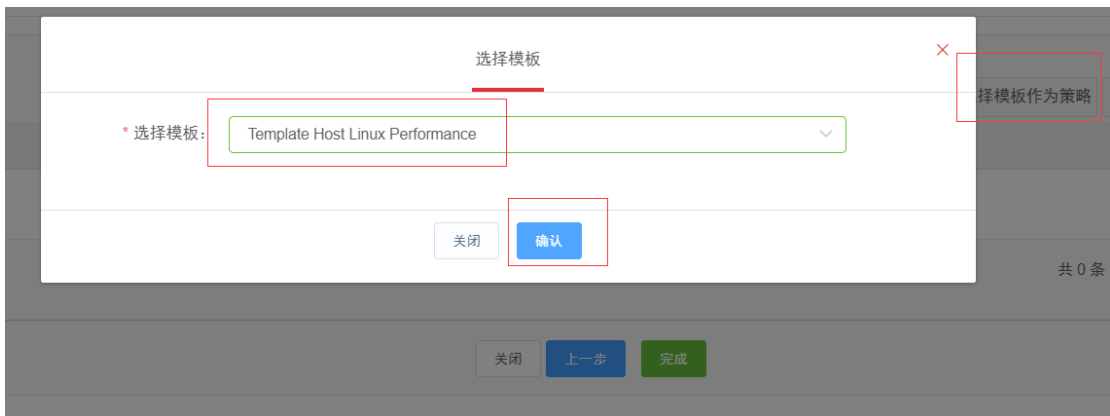
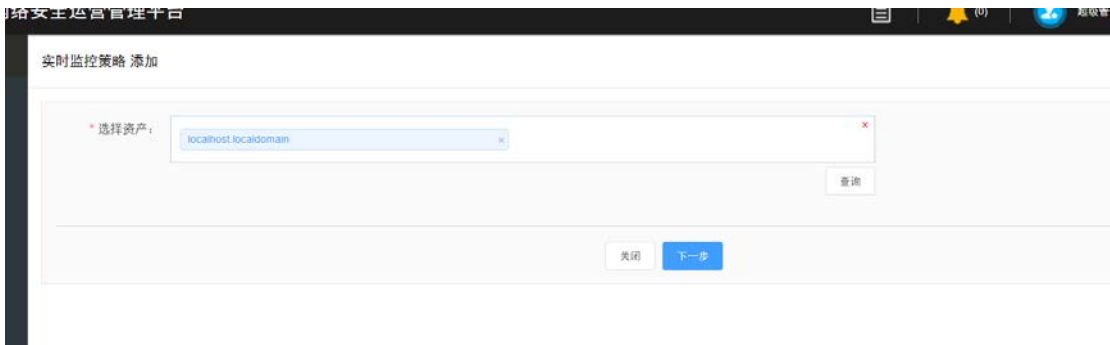
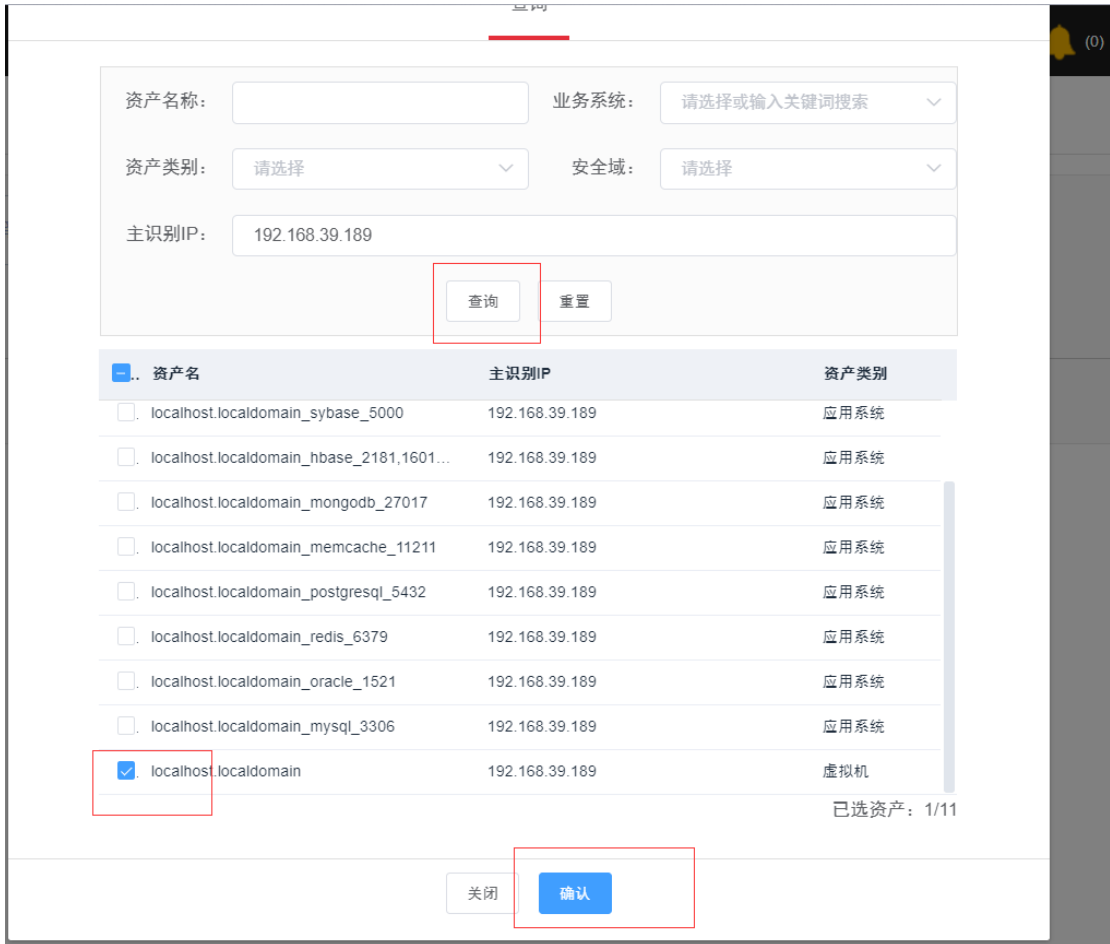
漏洞配置管理

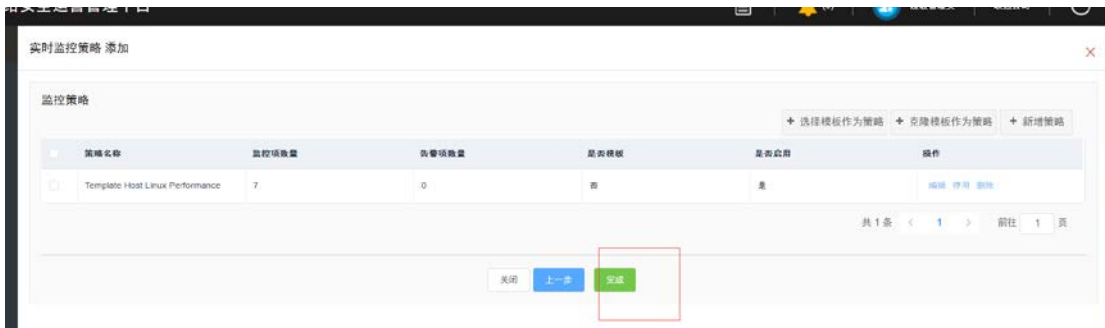
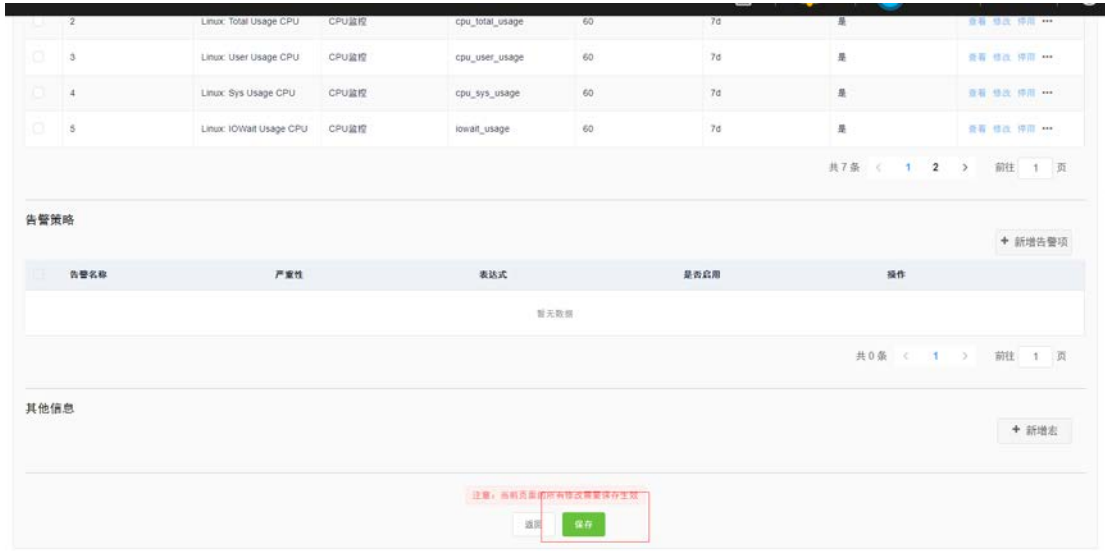
实时监控策略 添加

* 选择资产:

查询

关闭 下一步





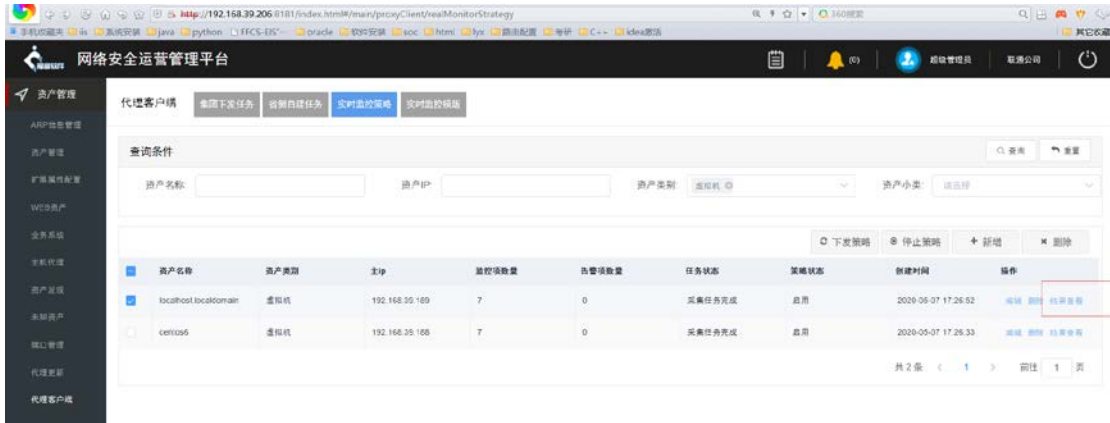
(2) 下发策略；

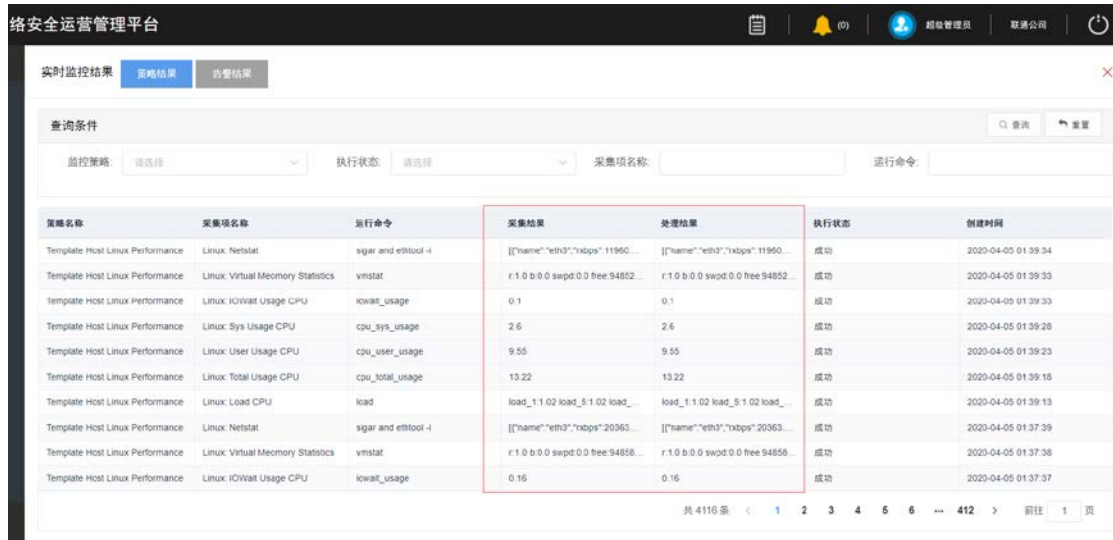


注意事项：然后查看省侧自建任务中有生成新的应用监控任务，点击查看任务内容，有内容则创建成功。



(3) 查看结果:





(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。

省侧自建任务 查看

任务名称：

* 任务类型：

* 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：

任务内容：

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"}]
```

省侧自建任务 查看

任务名称: 142udp检测104-158

* 任务类型: UDP端口探测

* 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: centos6 ✕

查询

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

关闭

(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;

省侧自建任务 查看

任务名称：

* 任务类型：

* 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：

任务内容：

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；

省侧自建任务 查看

任务名称：

* 任务类型：

* 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：

任务内容：

(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：

主机漏洞

查询条件							展开	查询	重置
任务名称:	<input type="text"/>	任务类型:	请选择	状态:	请选择	扫描设备:	请选择		
							+ 新增	x 删除	
<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作			
<input type="checkbox"/>	task-11-07-11-09-45	离线	root	2017-11-07 10:15:37	完成	查看 结果查看 导出 ...			
<input type="checkbox"/>	task-11-07-11-07-17	离线	root	2017-11-07 10:13:09	完成	查看 结果查看 导出 ...			
<input type="checkbox"/>	主机漏洞100	离线	root	2017-10-20 04:43:27	创建	查看 删除			
<input type="checkbox"/>	主机漏洞11	离线	root	2017-10-20 04:08:45	完成	查看 结果查看 导出 ...			
<input type="checkbox"/>	主机漏洞10	离线	root	2017-10-20 04:06:52	完成	查看 结果查看 导出 ...			

● 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：

主机漏洞新增

任务名称：	<input type="text" value="最多输入32个字符"/>
* 任务类型：	<input checked="" type="radio"/> 在线任务 <input type="radio"/> 离线任务
* 端口扫描方式：	<input checked="" type="radio"/> 实时 <input type="radio"/> 定时 <input type="radio"/> 周期
* 扫描设备：	<input type="text" value="请选择"/>
扫描策略：	<input type="text" value="请选择"/>
* IP类型：	<input type="text" value="请选择"/>
* 扫描目标：	<input checked="" type="radio"/> 按资产 <input type="radio"/> 按网段 <input type="radio"/> 按业务系统 <input type="radio"/> 按部门
* 选择资产：	<input type="text" value="请查询后选择资产"/> <input type="button" value="查询"/>
* 整改期限：	<input type="text" value=""/> <input type="button" value="🕒"/>
* 等级选择：	<input checked="" type="radio"/> 只整改高危等级 <input type="radio"/> 只整改中危及以上 <input type="radio"/> 只整改低危及以上
* 派单选择：	<input checked="" type="radio"/> 需派单 <input type="radio"/> 不需派单
<input type="button" value="关闭"/> <input type="button" value="提交"/>	

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：

主机漏洞新增

The screenshot shows a web form for adding a host vulnerability task. The form is titled "主机漏洞新增" (Host Vulnerability Addition). It contains the following fields and options:

- 任务名称:** A text input field with a placeholder "最多输入32个字符" (Maximum 32 characters).
- * 任务类型:** Radio buttons for "在线任务" (Online Task) and "离线任务" (Offline Task). "离线任务" is selected.
- * 选择业务系统:** A dropdown menu showing "vvs业务系统" (vvs Business System).
- 指派业务系统负责人:** A radio button that is selected, with a text input field below it containing "主机责任人A" (Host Responsible Person A).
- 指派完成人:** A radio button that is not selected.
- 上传结果文件:** A radio button that is not selected.
- * 整改期限:** A date/time picker field.
- * 等级选择:** Radio buttons for "只整改高危等级" (Only High Risk), "只整改中危及以上" (Only Medium Risk and Above), and "只整改低危及以上" (Only Low Risk and Above). "只整改高危等级" is selected.
- * 派单选择:** Radio buttons for "需派单" (Need Ticket) and "不需派单" (No Ticket). "需派单" is selected.
- Buttons:** "关闭" (Close) and "提交" (Submit).

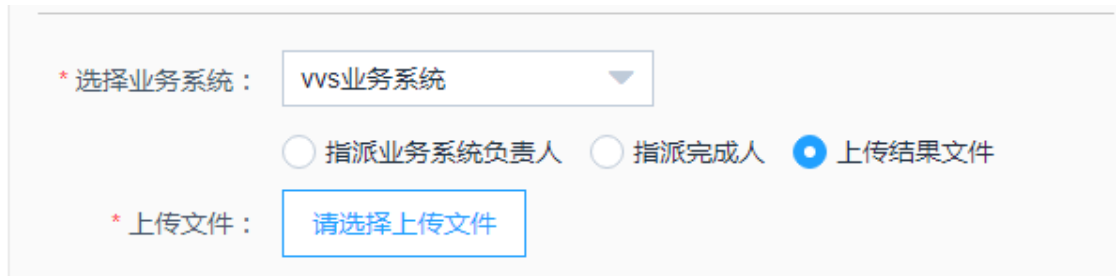
用户分别可选择业务系统责任人、指派完成人、或直接导入离线结果文件来完成的任务，如图：

The screenshot shows a web form for adding a host vulnerability task. The form is titled "主机漏洞新增" (Host Vulnerability Addition). It contains the following fields and options:

- * 选择业务系统:** A dropdown menu showing "BVS系统" (BVS System).
- 指派业务系统负责人:** A radio button that is selected, with a text input field below it containing "道义A" (Dao Yi A).
- 指派完成人:** A radio button that is not selected.
- 上传结果文件:** A radio button that is not selected.

① 指派业务系统负责人：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：


<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作
<input type="checkbox"/>	task-11-22-08-51-29	离线	root	2017-11-22 09:12:31	创建	查看 修改 导入 ...

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

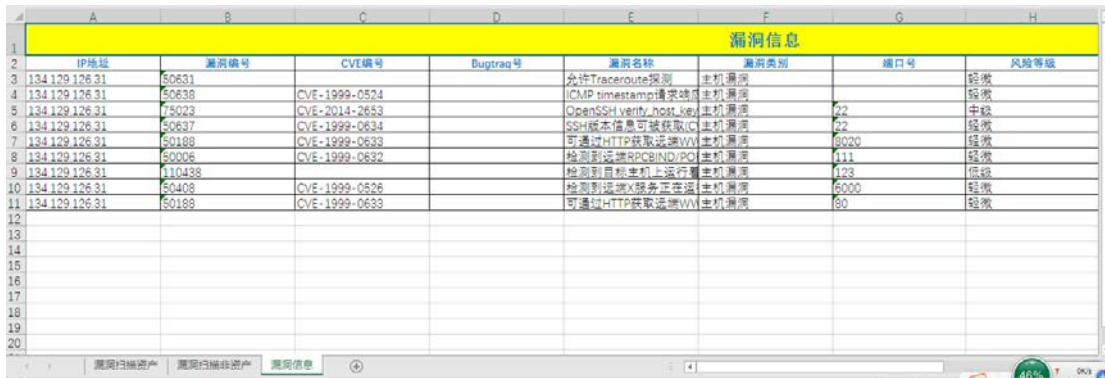
点击 **结果查看** 按钮，弹出漏洞结果查看详情界面，如图：




<input type="checkbox"/>	主任务名	业务系统	所属部门	IP地址	漏洞名称	漏洞等级	漏洞状态	最近发现时间	整改时限
<input type="checkbox"/>	task-11-22-10-22-52	BVS系统	中电福雷	134.129.126.31	允许Traceroute探测	低危	未整改		2017-11-24 10:44:07
<input type="checkbox"/>	task-11-22-10-22-52	BVS系统	中电福雷	134.129.126.31	ICMP timestamp...	低危	未整改		2017-11-24 10:44:07
<input type="checkbox"/>	task-11-22-10-22-52	BVS系统	中电福雷	134.129.126.31	OpenSSH verify_h...	中危	未整改		2017-11-24 10:44:07
<input type="checkbox"/>	task-11-22-10-22-52	BVS系统	中电福雷	134.129.126.31	SSH版本信息可被...	低危	未整改		2017-11-24 10:44:07
<input type="checkbox"/>	task-11-22-10-22-52	BVS系统	中电福雷	134.129.126.31	可通过HTTP获取...	低危	未整改		2017-11-24 10:44:07

● 漏洞结果导出

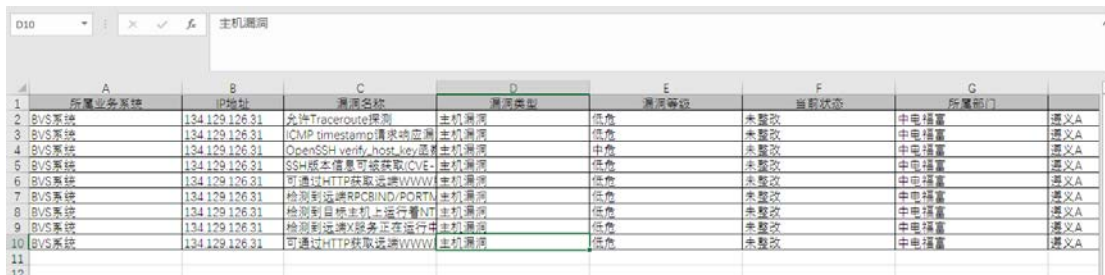
(1) 在任务列表操作栏，点击  按钮，导出漏洞结果详情，导出文件分别展示“漏洞扫描字段”、“漏洞扫描非资产”、“漏洞信息”，如图：




漏洞信息							
IP地址	漏洞编号	CVE编号	Bugtraq号	漏洞名称	漏洞类别	端口号	风险等级
134.129.126.31	50631			允许Traceroute探测	主机漏洞		轻微
134.129.126.31	50638			ICMP timestamp请求漏洞	主机漏洞		轻微
134.129.126.31	75023	CVE-2014-2653		OpenSSH verify_host_key漏洞	主机漏洞	22	中危
134.129.126.31	50637	CVE-1999-0634		SSH版本信息可被获取(CVE-)	主机漏洞	22	轻微
134.129.126.31	50188	CVE-1999-0633		可通过HTTP获取远端WWW	主机漏洞	8020	轻微
134.129.126.31	50006	CVE-1999-0632		检测到远端RPCBIND/PORTN	主机漏洞	411	轻微
134.129.126.31	110438			检测到目标主机上运行着NT	主机漏洞	413	低危
134.129.126.31	50408	CVE-1999-0526		检测到远端X服务正在运行	主机漏洞	6000	轻微
134.129.126.31	50189	CVE-1999-0633		可通过HTTP获取远端WWW	主机漏洞	80	轻微


(2) 在漏洞结果查看界面，点击  按钮，导出漏洞详情数据，

如图：



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	建议
BVS系统	134.129.126.31	允许Traceroute探测	主机漏洞	低危	未整改	中电运营	建议A
BVS系统	134.129.126.31	ICMP timestamp请求漏洞	主机漏洞	低危	未整改	中电运营	建议A
BVS系统	134.129.126.31	OpenSSH verify_host_key漏洞	主机漏洞	中危	未整改	中电运营	建议A
BVS系统	134.129.126.31	SSH版本信息可被获取(CVE-)	主机漏洞	低危	未整改	中电运营	建议A
BVS系统	134.129.126.31	可通过HTTP获取远端WWW	主机漏洞	低危	未整改	中电运营	建议A
BVS系统	134.129.126.31	检测到远端RPCBIND/PORTN	主机漏洞	低危	未整改	中电运营	建议A
BVS系统	134.129.126.31	检测到目标主机上运行着NT	主机漏洞	低危	未整改	中电运营	建议A
BVS系统	134.129.126.31	检测到远端X服务正在运行	主机漏洞	低危	未整改	中电运营	建议A
BVS系统	134.129.126.31	可通过HTTP获取远端WWW	主机漏洞	低危	未整改	中电运营	建议A

● 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。

2.4.2 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：

WEB漏洞

查询条件 展开 查询 重置

任务名称: 任务类型: 状态: 扫描设备:

新增 删除

<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作
<input type="checkbox"/>	task-11-22-10-45-52	离线	root	2017-11-22 11:06:53	完成	查看 结果查看 导出 ...
<input type="checkbox"/>	task-11-22-10-43-58	离线	root	2017-11-22 11:04:59	完成	查看 结果查看 导出 ...
<input type="checkbox"/>	task-11-22-10-42-54	离线	root	2017-11-22 11:03:56	完成	查看 结果查看 导出 ...

共 3 条 < 1 > 前往 1 页

● 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：

WEB漏洞新增

任务名称： 最多输入32个字符

* 任务类型： 在线任务 离线任务

* 扫描周期： 实时 定时 周期

* 扫描设备： 请选择

扫描策略： 请选择

* IP类型： 请选择
请选择IP类型

* 扫描目标： 按业务系统 按URL

* 选择业务系统： 请选择

* 整改期限：

* 等级选择： 只整改高危等级 只整改中危及以上 只整改低危及以上

* 派单选择： 需派单 不需派单

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：

WEB漏洞新增

任务名称：

* 任务类型： 在线任务 离线任务

* 选择业务系统：

指派业务系统负责人 指派完成人 上传结果文件

* 整改期限：

* 等级选择： 只整改高危等级 只整改中危及以上 只整改低危及以上

* 派单选择： 需派单 不需派单

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：

* 选择业务系统：

指派业务系统负责人 指派完成人 上传结果文件

① 指派业务系统负责人：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：

任务名称	任务类型	创建用户	创建时间	状态	操作
task-11-22-08-51-29	离线	root	2017-11-22 09:12:31	创建	查看 修改 导入 ...

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：

WEB漏洞结果查看


主任务名	业务系统	所属部门	IP地址	漏洞名称	漏洞等级	漏洞状态	最近发现时间	整改时限
task-11-22-10-45-52	BVS系统	中电福雷	http://218.67.107.18	检测到目标网站存...	低危	新发现		2017-11-23 11:07:06
task-11-22-10-45-52	BVS系统	中电福雷	http://218.67.107.18	远端HTTP服务器...	低危	新发现		2017-11-23 11:07:06

共 2 条 < 1 > 前往 1 页




● 漏洞结果导出

(1) 在任务列表界面操作栏，点击  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			总数	
		高危	中危	低危		
sina	http://218.67.107.18	0	0	2	2	

(2) 在漏洞结果查看界面，点击  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://218.67.107.18	检测到目标网站存在无授权	WEB漏洞	低危	新发现	中电组
BVS系统	http://218.67.107.18	或源HTTP服务器信息泄漏	WEB漏洞	低危	新发现	中电组

- 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。

2.4.3 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：

弱口令

查询条件						展开	查询	重置
任务名称:	<input type="text"/>	任务类型:	请选择	状态:	请选择	扫描设备:	请选择	
							+ 新增	* 删除
<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作		
<input type="checkbox"/>	task-11-22-10-53-14	离线	root	2017-11-22 11:14:16	完成	查看 结果查看 导出 ...		
						共 1 条	< 1 >	前往 1 页

● 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：

弱口令新增

任务名称：	<input type="text" value="最多输入32个字符"/>
* 任务类型：	<input checked="" type="radio"/> 在线任务 <input type="radio"/> 离线任务
* 扫描周期：	<input checked="" type="radio"/> 实时 <input type="radio"/> 定时 <input type="radio"/> 周期
* 扫描设备：	<input type="text" value="请选择"/>
扫描策略：	<input type="text" value="请选择"/>
* IP类型：	<input type="text" value="请选择"/> <small>请选择IP类型</small>
字典配置：	<input type="button" value="配置"/>
* 扫描目标：	<input checked="" type="radio"/> 按资产 <input type="radio"/> 按网段 <input type="radio"/> 按业务系统 <input type="radio"/> 按部门
* 选择资产：	<input type="text" value="请查询后选择资产"/> <input type="button" value="查询"/>
* 整改期限：	<input type="text" value=""/> <input type="button" value="🕒"/>
* 等级选择：	<input checked="" type="radio"/> 只整改高危等级 <input type="radio"/> 只整改中危及以上 <input type="radio"/> 只整改低危及以上
* 派单选择：	<input checked="" type="radio"/> 需派单 <input type="radio"/> 不需派单
<input type="button" value="✕ 关闭"/> <input type="button" value="✔ 提交"/>	

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：

弱口令新增

The screenshot shows a web form for adding a weak password task. It includes a task name input field (max 32 characters), a task type selection (radio buttons for 'Online Task' and 'Offline Task', with 'Offline Task' selected), a business system selection dropdown (currently 'Please Select'), and three options for assigning responsibility: 'Assign Business System Responsible' (selected), 'Assign Completion Person', and 'Upload Result File'. Below these are fields for 'Rectification Period' (with a clock icon), 'Level Selection' (radio buttons for 'Only High Risk', 'Only Medium and Above', and 'Only Low and Above', with 'Only High Risk' selected), and 'Ticket Selection' (radio buttons for 'Need Ticket' and 'No Ticket', with 'Need Ticket' selected). At the bottom are 'Close' and 'Submit' buttons.

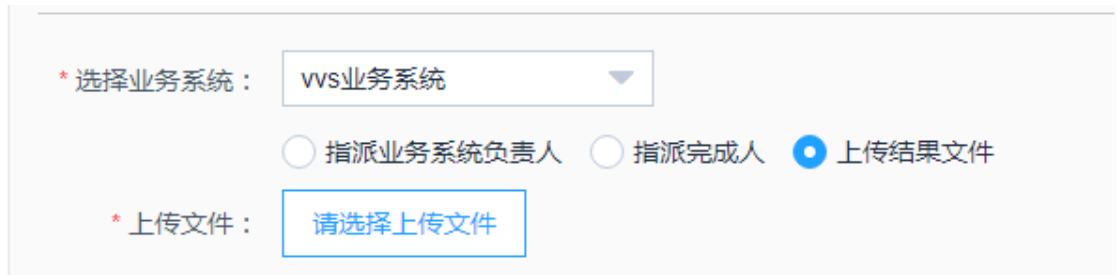
用户分别可选择业务系统责任人、指派完成人、或直接导入离线结果文件来完成的任务，如图：

This screenshot shows the same form as above, but with 'BVS系统' selected in the business system dropdown. The 'Assign Business System Responsible' radio button is selected, and a button labeled '遵义A' is visible below the options.

① 指派业务系统负责人：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 用户来完成的任务；

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：

<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作
<input type="checkbox"/>	task-11-22-08-51-29	离线	root	2017-11-22 09:12:31	创建	查看 修改 导入 ...

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：



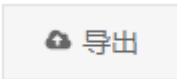
主任姓名	业务系统	所属部门	IP地址	漏洞名称	漏洞等级	漏洞状态	最近发现时间	整改时限
task-11-22-10-53-14	BVS系统	中电福富	172.21.133.73	猜测出远程SSH服...	高危	新发现	2017-11-22 10:53:14	2017-11-23 11:14:29

● 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：

漏洞信息							
IP地址	漏洞编号	CVE编号	Bugtraq号	漏洞名称	漏洞类别	端口号	风险等级
172.21.133.73	2012			猜测出远端SSH服务存在弱口令		22	中低

(2) 在漏洞结果查看界面，点击  按钮，导出漏洞详情数据，

如图：

	A	B	C	D	E	F	G	
	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	
1	BVS系统	172.21.133.73	猜测出远端SSH服务存在弱口令	高危	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  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：

基线配置

查询条件				展开	查询	重置	
任务名称:	<input type="text"/>	任务类型:	请选择	状态:	请选择	扫描设备:	请选择
						+ 新增	* 删除
<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作	
<input type="checkbox"/>	task-11-22-10-59-26	基线	root	2017-11-22 11:20:28	创建	查看 修改 导入 ...	
<input type="checkbox"/>	task-11-22-10-59-17	在线	root	2017-11-22 11:20:18	创建	查看 修改 删除	
						共 2 条	1 / 1 页

● 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：

基线配置新增

任务名称：

* 任务类型： 在线任务 离线任务

* 扫描周期： 实时 定时 周期

扫描设备：

* IP类型：

* 基线设备类型： 绿盟 福富

* 选择资产：

资产名称	基线模板	操作
暂无数据		

* 整改期限：

* 等级选择： 只整改高危等级 只整改中危及以上 只整改低危及以上

* 派单选择： 需派单 不需派单

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：

基线配置新增

任务名称：最多输入32个字符

* 任务类型： 在线任务 离线任务

* 选择业务系统：请选择

指派业务系统负责人 指派完成人 上传结果文件

请重新选择业务系统

* 整改期限：

* 等级选择： 只整改高危等级 只整改中危及以上 只整改低危及以上

* 派单选择： 需派单 不需派单

✕ 关闭 提交

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：

* 选择业务系统：BVS系统

指派业务系统负责人 指派完成人 上传结果文件

道义A

- ① 指派业务系统负责人：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：

* 选择业务系统：

指派业务系统负责人 指派完成人 上传结果文件

* 上传文件：

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：

<input type="checkbox"/>	任务名称	任务类型	创建用户	创建时间	状态	操作
<input type="checkbox"/>	task-11-22-08-51-29	离线	root	2017-11-22 09:12:31	创建	查看 修改 导入 ...

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：

导入 ✕

上传文件：

● 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：

基线配置结果查看 ✕

查询条件 ▼ 展开 🔍 查询 ↺ 重置

业务系统: 所属部门: 漏洞名称: 漏洞等级:

<input type="checkbox"/>	主任务名	业务系统	所属部门	IP地址	漏洞名称	漏洞等级	漏洞状态	最近发现时间	整改时限
<input type="checkbox"/>	task-11-22-10-59-26	资产发现	中电福富	127.0.0.1	帐号口令	高危	新发现		2017-11-23 11:20:42
<input type="checkbox"/>	task-11-22-10-59-26	资产发现	中电福富	127.0.0.1	帐号口令	高危	新发现		2017-11-23 11:20:42
<input type="checkbox"/>	task-11-22-10-59-26	资产发现	中电福富	127.0.0.1	帐号口令	高危	新发现		2017-11-23 11:20:42
<input type="checkbox"/>	task-11-22-10-59-26	资产发现	中电福富	127.0.0.1	帐号口令	高危	新发现		2017-11-23 11:20:42
<input type="checkbox"/>	task-11-22-10-59-26	资产发现	中电福富	127.0.0.1	帐号口令	高危	新发现		2017-11-23 11:20:42
<input type="checkbox"/>	task-11-22-10-59-26	资产发现	中电福富	127.0.0.1	认证授权	高危	新发现		2017-11-23 11:20:42

● 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：

漏洞信息								
IP地址	漏洞编号	CVE编号	Bugtraq号	漏洞名称	漏洞类别	端口号	风险等级	
127.0.0.1	1			帐号口令	基线漏洞			
127.0.0.1	1			帐号口令	基线漏洞			
127.0.0.1	0			帐号口令	基线漏洞			
127.0.0.1	0			帐号口令	基线漏洞			
127.0.0.1	0			帐号口令	基线漏洞			
127.0.0.1	1			认证授权	基线漏洞			
127.0.0.1	0			协议安全	基线漏洞			
127.0.0.1	1			认证授权	基线漏洞			
127.0.0.1	1			认证授权	基线漏洞			
127.0.0.1	1			认证授权	基线漏洞			
127.0.0.1	0			其它安全	基线漏洞			
127.0.0.1	0			其它安全	基线漏洞			
127.0.0.1	0			其它安全	基线漏洞			
127.0.0.1	0			其它安全	基线漏洞			
127.0.0.1	1			认证授权	基线漏洞			



(2) 在漏洞结果查看界面，点击

如图：

所属业务系统	IP地址	检查项名称	漏洞类型	漏洞等级	当前状态	所属部门	
资产发现	127.0.0.1	帐号口令	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	帐号口令	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	帐号口令	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	帐号口令	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	帐号口令	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	认证授权	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	协议安全	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	认证授权	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	认证授权	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	其它安全	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	其它安全	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	其它安全	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	其它安全	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	其它安全	基线漏洞	高危	新发现	中电博富	二级账号
资产发现	127.0.0.1	认证授权	基线漏洞	高危	新发现	中电博富	二级账号



● 用户可通过在查询条件区域输入关键字，点击



查询结果，默认显示 4 个查询条件，点击



按钮，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：

人工渗透

查询条件
▼ 展开
🔍 查询
↺ 重置

漏洞名称:

目标IP:

业务系统: 请选择

漏洞等级: 请选择

+ 新增
✕ 删除

<input type="checkbox"/>	漏洞名称	业务系统	目标IP	漏洞等级	创建时间	描述	操作
<input type="checkbox"/>	strunk2	BVS系统	192.168.68.229	中危	2017-11-22 11:06:00		查看 删除

共 1 条
< 1 >
前往 1 页

- 点击“新增”，弹出人工渗透新增界面，*号为必填项，如图：

新增 ✕

* 目标IP:

* 业务系统: 请选择

* 漏洞名称:

* 风险等级: 请选择

告警描述:

渗透报告:

关闭
✔ 提交

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 🔍 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。

2.4.6 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：

预警任务

查询条件 展开 查询 重置

预警名称: 预警信息来源: 预警等级: 发布人:

+ 新增 ✕ 删除

<input type="checkbox"/>	预警名称	预警信息来源	预警等级	发布人	状态	发布时间	创建时间	操作
<input type="checkbox"/>	alarm		二级	通义A	创建	2017-11-22 12:30:30	2017-11-22 11:09:51	查看 修改 结果查看 ...

共 1 条 < 1 > 前往 页

- 点击“新增”按钮，弹出预警任务添加界面，如图：

新增 ✕

预警名称: * 预警类型:

* 预警发布人: * 预警等级:

* 发布时间:

* 失效时间:

系统类型: 系统版本: 添加

受影响的操作系统:

系统类型	系统版本	操作
暂无数据		

关闭 提交

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：

预警任务结果查看

查询条件
Q 查询
↶ 重置

资产名称: ip地址:

主任务名	资产名称	ip地址
alarm	asset_info	2.2.34.2
alarm	asset_test	2.3.1.2

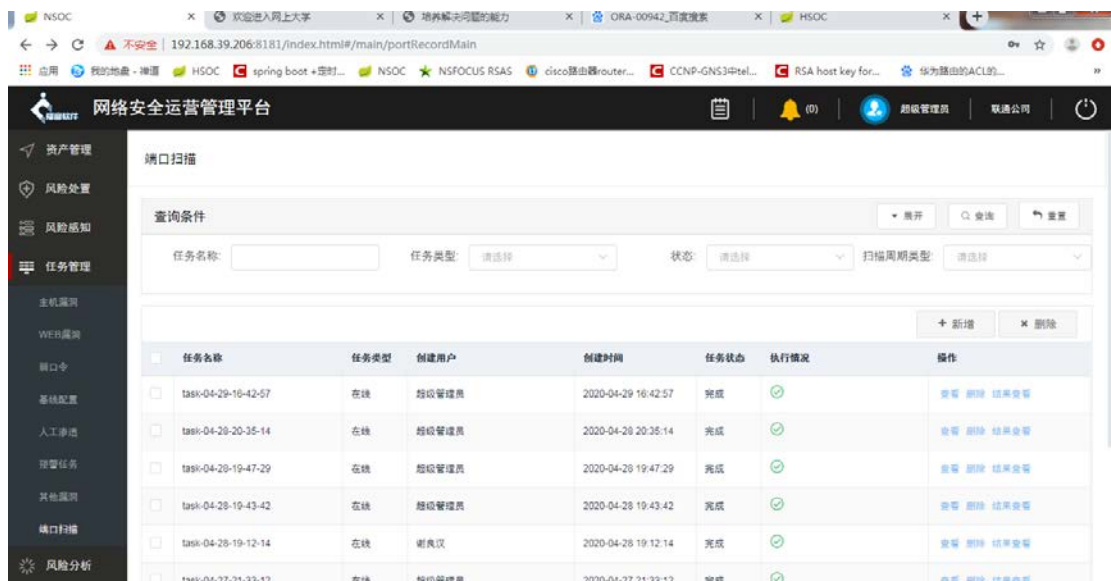
共 2 条
< 1 >
前往

页

- 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  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。

2.4.7 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。



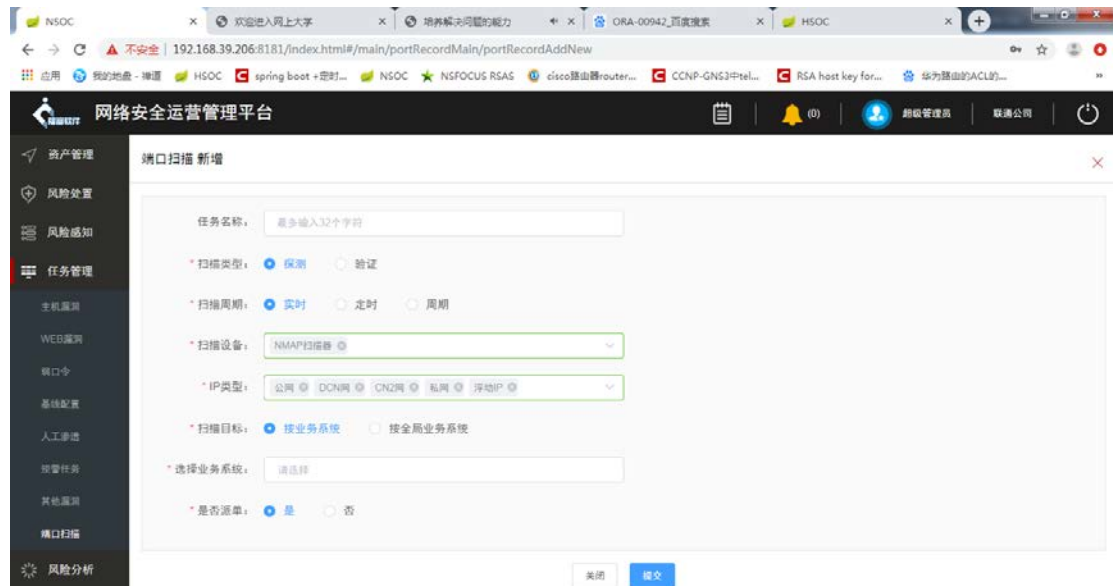
The screenshot shows the '端口扫描' (Port Scanning) section of the '网络安全运营管理平台' (Network Security Operation Management Platform). The interface includes a search bar with '展开' (Expand), 'Q 查询' (Search), and '重置' (Reset) buttons. Below the search bar, there are dropdown menus for '任务名称' (Task Name), '任务类型' (Task Type), '状态' (Status), and '扫描周期类型' (Scanning Cycle Type). A table lists the tasks with columns for '任务名称' (Task Name), '任务类型' (Task Type), '创建用户' (Created User), '创建时间' (Created Time), '任务状态' (Task Status), '执行情况' (Execution Status), and '操作' (Action). The table contains six rows of task data.

任务名称	任务类型	创建用户	创建时间	任务状态	执行情况	操作
task-04-29-16-42-57	在线	超级管理员	2020-04-29 16:42:57	完成	✓	查看 删除 结果查看
task-04-28-20-35-14	在线	超级管理员	2020-04-28 20:35:14	完成	✓	查看 删除 结果查看
task-04-28-19-47-29	在线	超级管理员	2020-04-28 19:47:29	完成	✓	查看 删除 结果查看
task-04-28-19-43-42	在线	超级管理员	2020-04-28 19:43:42	完成	✓	查看 删除 结果查看
task-04-28-19-12-14	在线	谢良汉	2020-04-28 19:12:14	完成	✓	查看 删除 结果查看
task-04-27-21-33-12	在线	超级管理员	2020-04-27 21:33:12	完成	✓	查看 删除 结果查看

2.4.7.1 探测任务

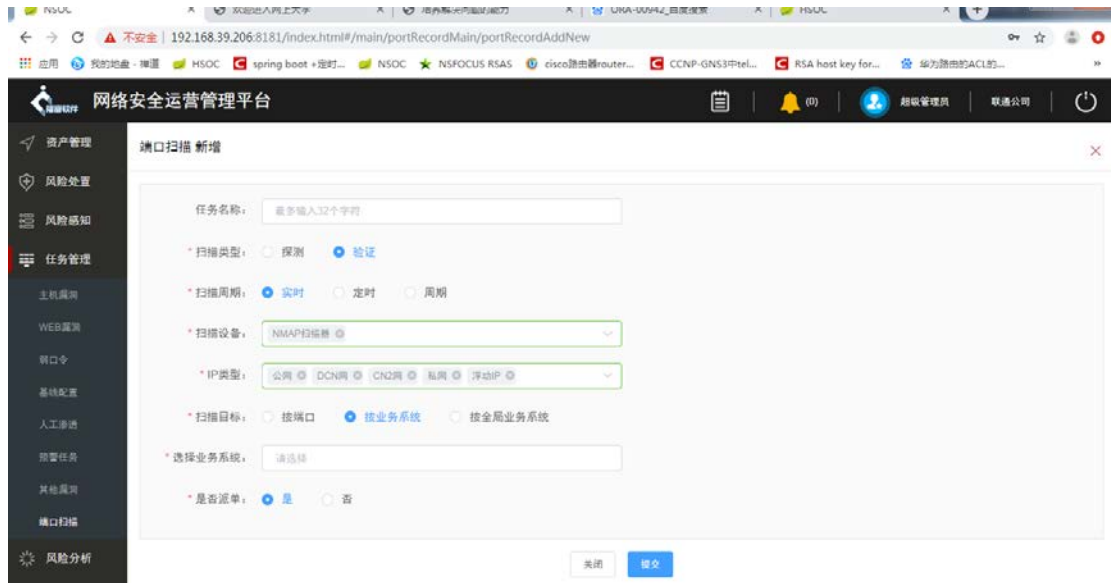
探测任务可按业务系统维度进行下发，探测该业务系统下所有资产 IP 的端口开放情况，探测任务分为两步，第一步是开放端口的探测，第二步是 BANNER 信息、服务名以及版本号的采集，由于 BANNER 信息以及版本号扫描较花时间，后端会对本次扫描出来的开放端口数据进行入库的操作，再这之后再继续进行 BANNER 信息及版本号的扫描，扫描的数据可以在任务管理-结果查看下进行查看，展示本次探测出来的 OPEN 端口数据。

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

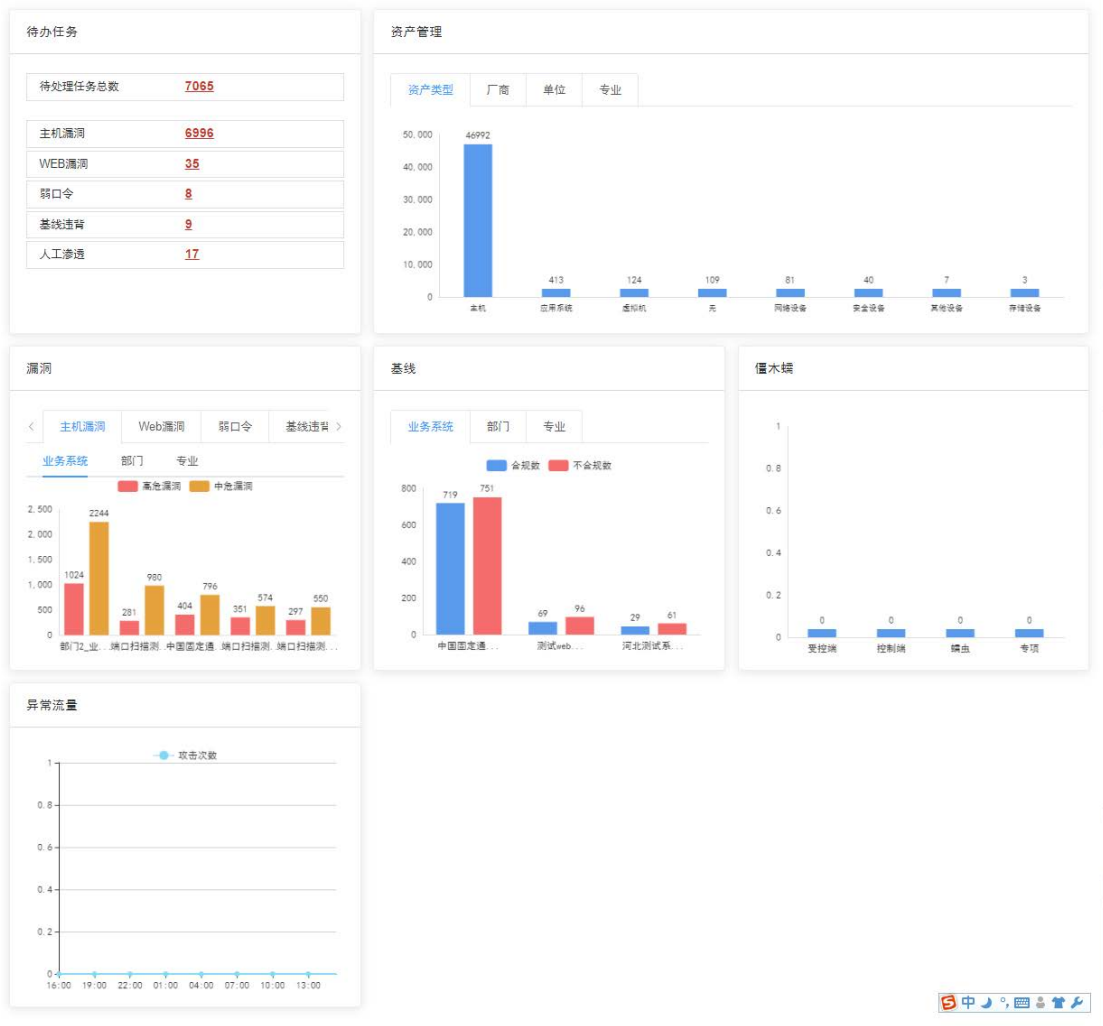
验证任务可按端口维度以及业务系统维度进行任务的下发，验证任务是通过 TELNET 对端口进行 OPEN 或者 CLOSE 的验证。



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  ，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；

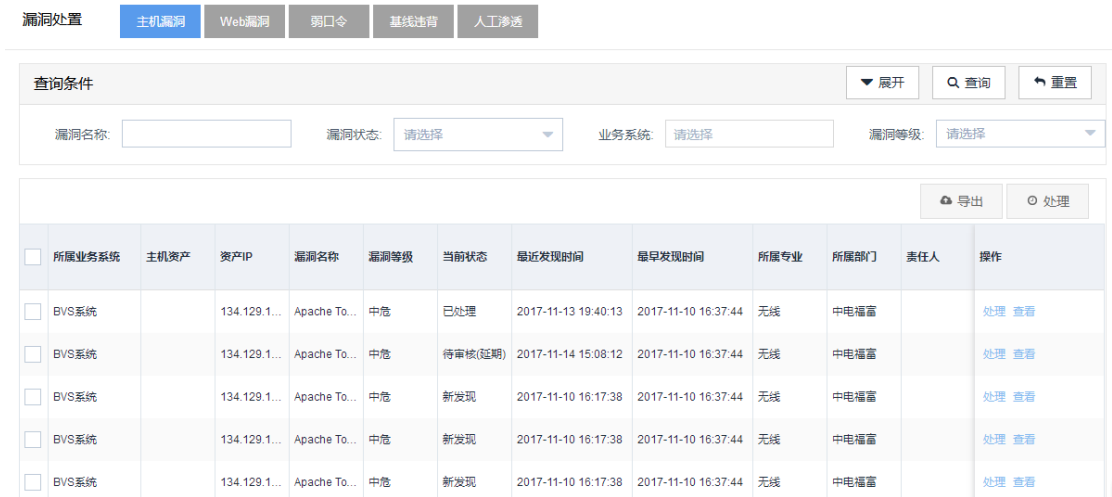
(2) 点击 **派发** 按钮，弹出僵木儒派发界面；

(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 **更多** 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：

漏洞详情 ×

漏洞信息	漏洞编号：71733	漏洞名称：Apache Tomcat 资源管理错误漏洞	漏洞等级：中危
	漏洞状态：新发现	业务系统：BVS系统	IP地址：134.129.112.42
	端口号：7080	端口类型：应用端口	CVE编号：CVE-2011-4858
	Bugtraq号：	所属专业：无线	所属部门：中电福富
	责任人：	最早发现时间：2017-11-10 16:37:44	最近发现时间：2017-11-10 16:17:38
	整改时间：2017-11-24 16:38:30		

描述：Apache Tomcat是一个流行的开放源码的JSP应用服务器程序。Apache Tomcat 5.5.35 之前版本，6.0.35之前的6.x，7.0.23前的7.x版本存在一个漏洞。该漏洞源于在没有限制触发预测异常的情况下为形式参数计算哈希值。远程攻击者可以通过发送多个特制参数导致拒绝服务。

解决方案：厂商补丁：Apache Group ----- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：<http://jakarta.apache.org/tomcat/index.html>

溯源记录	处理时间	漏洞状态	处理来源	处理操作
>	2017-11-10 16:37:44	新发现	漏洞处理结果(root)	导入

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：

处置流程：

发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 处理方式1：

处理方式2：

* 整改时间：

* 整改情况：

处置流程：

发现 处理 审核 完成

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 材料证明： [点击上传](#)
仅支持.doc和.docx文件

* 申请误报说明：

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 预计完成时间：

* 说明：

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 说明：

(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：

处置流程：

发现 处理 审核 完成

审查通过 审查拒绝

* 审核情况说明：

- 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“审核通过”，漏洞状态变更为“无法处理（不可关停）”，流程结束；

② 若选择“审核拒绝”，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“审核通过”，漏洞状态变更为“无法处理（可关停）”，流程结束；

② 若选择“审核拒绝”，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

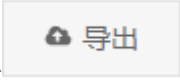
点击 [查看](#) 按钮，弹出漏洞详细信息界面，如图：

漏洞信息	漏洞编号：71419	漏洞名称：Apache Tomcat HTTP摘要式身份验证多个安全漏洞	漏洞等级：中危
	漏洞状态：暂不处理	业务系统：BVS系统	IP地址：134.129.112.42
	端口号：7080	端口类型：应用端口	CVE编号：CVE-2011-1184
	Bugtraq号：49762	所属专业：无线	所属部门：中电福富
	责任人：	最早发现时间：2017-11-10 16:37:44	最近发现时间：2017-11-10 16:17:38
	整改时间：2017-11-24 16:38:30	描述：Tomcat是由Apache软件基金会下层的Jakarta项目开发的一个Servlet容器，按照Sun Microsystems提供的技术规范，实现了对Servlet和JavaServer Page (JSP) 的支持，并提供了作为Web服务器的一些特有功能。Tomcat进行HTTP摘要式身份验证时在实现上存在多个安全漏洞，远程攻击者可利用这些漏洞绕过安全限制并执行非法攻击。<“来源：vendor”>	

解决方案：厂商补丁：Apache Group ----- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://jakarta.apache.org/tomcat/index.html

处理时间	漏洞状态	处理来源	处理操作
> 2017-11-22 16:17:47	暂不处理	漏洞处理结果(root)	漏洞处理
> 2017-11-14 15:07:07	待审核(延期)	漏洞处理结果(root)	漏洞处理
> 2017-11-10 16:37:44	新发现	漏洞处理结果(root)	导入

● 漏洞导出

点击  按钮，导出漏洞数据，如图：

1	A 所属业务系统	B IP地址	C 漏洞名称	D 漏洞类型	E 漏洞等级	F 当前状态	G 所属部门
2	BVS系统	134.129.112.42	Apache Tomcat SingleSignOn	主机漏洞	中危	已处理	中电福富
3	BVS系统	134.129.112.42	Apache Tomcat 表单认证漏洞	主机漏洞	中危	新发现	中电福富
4	BVS系统	134.129.112.42	Apache Tomcat XML 解析器	主机漏洞	中危	新发现	中电福富
5	BVS系统	134.129.112.42	Apache Tomcat sendfile漏洞	主机漏洞	中危	新发现	中电福富
6	BVS系统	134.129.112.42	Apache Tomcat Web类漏洞	主机漏洞	中危	新发现	中电福富
7	BVS系统	134.129.112.42	Apache Tomcat RequestDir	主机漏洞	中危	待审核(续报)	中电福富
8	BVS系统	134.129.112.42	Apache Tomcat Java ALP漏洞	主机漏洞	中危	无法处理(可关修)	中电福富
9	BVS系统	134.129.112.42	Apache Tomcat Transfer-En	主机漏洞	中危	无法处理(不可关修)	中电福富
10	BVS系统	134.129.112.42	Apache Tomcat 资源管理漏洞	主机漏洞	中危	续报	中电福富
11	BVS系统	134.129.112.42	Apache Tomcat HTTP摘要式	主机漏洞	中危	暂不处理	中电福富
12	BVS系统	134.129.112.42	Apache Tomcat jsp/cal/cal	主机漏洞	中危	新发现	中电福富
13	BVS系统	134.129.112.42	远端HTTP服务类型和版本	主机漏洞	低危	新发现	中电福富
14	BVS系统	134.129.112.42	Apache Tomcat 'MemoryU	主机漏洞	低危	新发现	中电福富
15	BVS系统	134.129.112.42	Apache Tomcat SecurityMar	主机漏洞	低危	新发现	中电福富
16	BVS系统	134.129.112.42	Apache Tomcat WebDav远	主机漏洞	低危	新发现	中电福富
17	BVS系统	134.129.112.42	Apache Tomcat认证信息	主机漏洞	低危	新发现	中电福富
18	BVS系统	134.129.112.42	Apache Tomcat Manager和	主机漏洞	低危	新发现	中电福富
19	BVS系统	134.129.112.42	Apache Tomcat POST Data	主机漏洞	低危	新发现	中电福富
20	BVS系统	134.129.112.42	Jenkins 服务检测	主机漏洞	低危	新发现	中电福富
21	BVS系统	134.129.112.42	远端HTTP服务类型和版本	主机漏洞	低危	新发现	中电福富

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：

漏洞处置 主机漏洞 Web漏洞 弱口令 基线违背 人工渗透

查询条件 ▼ 展开 Q 查询 ↶ 重置

漏洞名称: 漏洞状态: 业务系统: 漏洞等级:

 导出 ○ 处理

<input type="checkbox"/>	所属业务系统	网站名称	网站域名	漏洞名称	漏洞等级	当前状态	最近发现时间	最早发现时间	所属专业	所属部门	责任人	操作
<input type="checkbox"/>	BVS系统	sina	http://218...	检测到目...	低危	新发现	2017-11-22 10:45:55	2017-11-22 11:06:57	无线	中电福富	逄义A	处理 查看 处置子URL
<input type="checkbox"/>	BVS系统	sina	http://218...	远端HTTP...	低危	新发现	2017-11-22 10:45:55	2017-11-22 11:06:56	无线	中电福富	逄义A	处理 查看 处置子URL

共 2 条 < 1 > 前往 1 页

● 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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 处理方式1： 处理方式1

处理方式2： 处理方式2

* 整改时间： 选择日期时间

* 整改情况：

重置 提交

处置流程：
发现 处理 审核 完成

(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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 材料证明： 点击上传

仅支持.doc和.docx文件

* 申请误报说明：

重置 提交

(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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 预计完成时间：选择日期时间

* 说明：

(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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 说明：

(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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 说明：

- 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“审核通过”，漏洞状态变更为“暂不处理”，流程结束；

② 若选择“审核拒绝”，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：



处置流程： 发现 处理 审核 完成

审核通过 审核拒绝

* 审核情况说明：

① 若选择“审核通过”，漏洞状态变更为“无法处理（不可关停）”，流程结束；

② 若选择“审核拒绝”，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：



处置流程： 发现 处理 审核 完成

审核通过 审核拒绝

* 审核情况说明：

① 若选择“审核通过”，漏洞状态变更为“无法处理（可关停）”，流程结束；

② 若选择“审核拒绝”，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：

漏洞详情

漏洞编号： 漏洞状态：已处理 漏洞号： Bugtraq号： 责任人：三级账号E 整改时间：2017-11-24 16:41:55	漏洞名称：Apache HTTP Server拒绝服务漏洞 业务系统：资产发现 漏洞类型： 所属专业：接入网 最早发现时间：2017-11-22 16:41:45	漏洞等级：中危 网站域名：http://www.haiyan.gov.cn CVE编号：CVE-2007-6750 所属部门：中电福富 最近发现时间：2017-11-22 16:20:43
---	---	--

描述：Apache HTTP Server是Apache软件基金会的一个开放源代码的网页服务器，可以在大多数计算机系统运行。 Apache HTTP Server 1.x和2.x版本中存在漏洞，允许远程攻击者部分HTTP请求导致拒绝服务攻击。
解决方案：厂商补丁：Apache Group ----- 目前厂商已经发布了升级补丁以修复这个问题，请到厂商的主页下载：http://httpd.apache.org/

URL地址	问题参数	整改状态	首次发现时间	最近发现时间	整改时间
http://www.haiyan.gov.cn		已处理	2017-11-22 16:41:45	2017-11-22 16:21:24	

共 1 条 < 1 > 前往 1 页

处理时间	漏洞状态	处理来源	处理操作
> 2017-11-22 16:42:25	已处理	漏洞处理结果(root)	漏洞处理
> 2017-11-22 16:41:45	新发现	漏洞处理结果(root)	导入

● 漏洞导出

点击 按钮，导出漏洞数据，如图：

A	B	C	D	E	F	G
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
资产发现	http://www.jkman	Microsoft IIS畸形文件扩展名	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.jkman	远端HTTP服务器信息泄漏	WEB漏洞	低危	新发现	中电福富
资产发现	http://www.haiyan	Apache Tomcat sendfile请求	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache Tomcat JvM连接请求	WEB漏洞	低危	新发现	中电福富
资产发现	http://www.haiyan	Apache HTTP Server mod_g	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache Tomcat NIO连接请求	WEB漏洞	低危	新发现	中电福富
资产发现	http://www.haiyan	Apache mod_proxy_http	WEB漏洞	低危	已处理	中电福富
资产发现	http://www.haiyan	Apache HTTP Server ap_pre	WEB漏洞	低危	待审核(通报)	中电福富
资产发现	http://www.haiyan	Apache Tomcat拒绝服务漏洞	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache Tomcat AJP协议交互	WEB漏洞	高危	新发现	中电福富
资产发现	http://www.haiyan	Apache Tomcat NIO Connec	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache HTTP Server mod_g	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache Tomcat Slowloris工	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache Tomcat Web管理端	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache Tomcat 资源管理端	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache HTTP Server拒绝服	WEB漏洞	中危	已处理	中电福富
资产发现	http://www.haiyan	Microsoft IIS畸形文件扩展名	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache mod_proxy_http	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	Apache HTTP Server mod_g	WEB漏洞	中危	新发现	中电福富
资产发现	http://www.haiyan	远端HTTP服务器信息泄漏	WEB漏洞	低危	新发现	中电福富

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：

漏洞处置

主机漏洞
Web漏洞
弱口令
基线违背
人工渗透

▼ 展开
🔍 查询
↺ 重置

漏洞名称:
 漏洞状态: 请选择
 业务系统: 请选择
 漏洞等级: 请选择

<input type="checkbox"/>	所属业务系统	主机资产	资产IP	漏洞名称	漏洞等级	当前状态	最近发现时间	最早发现时间	所属专业	所属部门	责任人	整改	操作
<input type="checkbox"/>	BVS系统		172.21.13...	猜测出远...	高危	新发现	2017-11-22 10:53:14	2017-11-22 11:14:16	无线	中电福富		2017	处理 查看

共 1 条 < 1 > 前往 1 页

● 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 更多 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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 处理方式1： 处理方式1

处理方式2： 处理方式2

* 整改时间： 选择日期时间

* 整改情况：

重置 提交

处置流程：
发现 处理 审核 完成

(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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 材料证明： 点击上传

仅支持.doc和.docx文件

* 申请误报说明：

重置 提交

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 预计完成时间：

* 说明：

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 说明：

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 说明：

● WEB 漏洞审核

审核员点击“处理”按钮，进入漏洞审核界面，如图：

漏洞处置 ✕

基本信息	漏洞编号：2012	漏洞名称：猜测出远程SSH服务存在可登录的用户名口令	漏洞等级：高危
	漏洞状态：待审核(误报)	业务系统：BVS系统	IP地址：172.21.133.73
	端口号：22	CVE编号：	Bugtraq号：
	所属专业：无线	所属部门：中电福富	责任人：
	最早发现时间：2017-11-22 11:14:16	最近发现时间：2017-11-22 10:53:14	更多

处置流程：
✔ 发现 — ✔ 处理 — ③ 审核 — ④ 完成

审查通过 审查拒绝

* 审核情况说明：

历史记录

漏洞名称 猜测出远程SSH服务存在可登录的用户名口令
 误报材料 redis安装文档.docx
 情况说明.1

(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：

漏洞处置 ✕

基本信息	漏洞编号：2012	漏洞名称：猜测出远程SSH服务存在可登录的用户名口令	漏洞等级：高危
	漏洞状态：待审核(误报)	业务系统：BVS系统	IP地址：172.21.133.73
	端口号：22	CVE编号：	Bugtraq号：
	所属专业：无线	所属部门：中电福富	责任人：
	最早发现时间：2017-11-22 11:14:16	最近发现时间：2017-11-22 10:53:14	更多

处置流程：
✔ 发现 — ✔ 处理 — ③ 审核 — ④ 完成

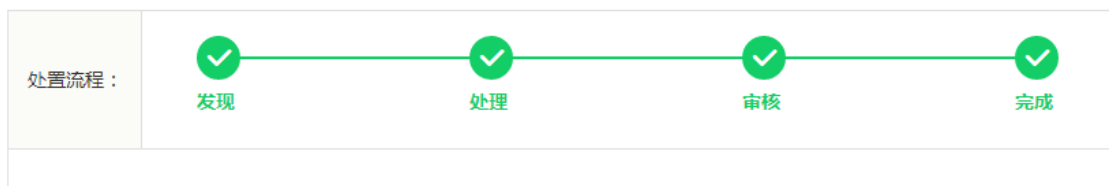
审查通过 审查拒绝

* 审核情况说明：

历史记录

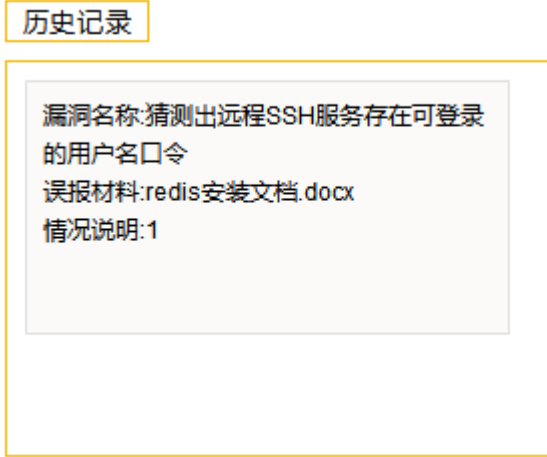
漏洞名称 猜测出远程SSH服务存在可登录的用户名口令
 误报材料 redis安装文档.docx
 情况说明.1

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“审核通过”，漏洞状态变更为“暂不处理”，流程结束；
- ② 若选择“审核拒绝”，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“审核通过”，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：

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：

漏洞详情 ×

漏洞信息	漏洞编号：1	漏洞名称：帐号口令	漏洞等级：高危
	漏洞状态：新发现	业务系统：资产发现	IP地址：127.0.0.1
	端口号：	端口类型：	CVE编号：
	Bugtraq号：	所属专业：接入网	所属部门：中电福富
	责任人：	最早发现时间：2017-11-22 11:22:41	最近发现时间：2017-11-22 11:01:39
	整改时间：2017-11-23 11:20:42		
	描述：检查是否设置口令生存周期		
	解决方案：检查是否设置口令生存周期		

溯源记录	处理时间	漏洞状态	处理来源	处理操作
	> 2017-11-22 11:22:41	新发现	漏洞处理结果(root)	导入

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：

处置流程：

发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 处理方式1：

处理方式2：

* 整改时间：

* 整改情况：

处置流程：

发现 处理 审核 完成

(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：

处置流程： 1 **发现** 2 3 4
发现 处理 审核 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 材料证明： [点击上传](#)
仅支持.doc和.docx文件

* 申请误报说明：

(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：

处置流程： 1 2 3 4
发现 处理 审核 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 预计完成时间：

* 说明：

(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：

处置流程： 1 2 3 4
发现 处理 审核 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 说明：

(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：

处置流程： 发现 处理 审核 完成

审核通过 审核拒绝

* 审核情况说明：

① 若选择“审核通过”，漏洞状态变更为“无法处理（不可关停）”，流程结束；

② 若选择“审核拒绝”，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：

处置流程： 发现 处理 审核 完成

审核通过 审核拒绝

* 审核情况说明：

① 若选择“审核通过”，漏洞状态变更为“无法处理（可关停）”，流程结束；

② 若选择“审核拒绝”，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：

漏洞详情 ✕

漏洞信息	漏洞编号：1	漏洞名称：帐号口令	漏洞等级：高危
	漏洞状态：待审核(误报)	业务系统：资产发现	IP地址：127.0.0.1
	端口号：	端口类型：	CVE编号：
	Bugtraq号：	所属专业：接入网	所属部门：中电福富
	责任人：	最早发现时间：2017-11-22 11:22:41	最近发现时间：2017-11-22 11:01:39
	整改时间：2017-11-23 11:20:42		
	描述：检查是否设置口令生存周期	解决方案：检查是否设置口令生存周期	

溯源记录	处理时间	漏洞状态	处理来源	处理操作
>	2017-11-22 17:14:31	待审核(误报)	漏洞处理结果(root)	漏洞处理
>	2017-11-22 11:22:41	新发现	漏洞处理结果(root)	导入

● 漏洞导出

点击 按钮，导出漏洞数据，如图：

	A	B	C	D	E	F	G
	所属业务系统	IP地址	检查项名称	漏洞类型	漏洞等级	当前状态	所属部门
1	资产发现	127.0.0.1	帐号口令	基础漏洞	高危	待审核(误报)	中电福富
2	资产发现	127.0.0.1	帐号口令	基础漏洞	高危	新发现	中电福富
3	资产发现	127.0.0.1	帐号口令	基础漏洞	高危	新发现	中电福富
4	资产发现	127.0.0.1	帐号口令	基础漏洞	高危	新发现	中电福富
5	资产发现	127.0.0.1	帐号口令	基础漏洞	高危	新发现	中电福富
6	资产发现	127.0.0.1	帐号口令	基础漏洞	高危	新发现	中电福富
7	资产发现	127.0.0.1	认证授权	基础漏洞	高危	新发现	中电福富
8	资产发现	127.0.0.1	协议安全	基础漏洞	高危	新发现	中电福富
9	资产发现	127.0.0.1	认证授权	基础漏洞	高危	新发现	中电福富
10	资产发现	127.0.0.1	认证授权	基础漏洞	高危	新发现	中电福富
11	资产发现	127.0.0.1	其它安全	基础漏洞	高危	新发现	中电福富
12	资产发现	127.0.0.1	其它安全	基础漏洞	高危	新发现	中电福富
13	资产发现	127.0.0.1	其它安全	基础漏洞	高危	新发现	中电福富
14	资产发现	127.0.0.1	日志审计	基础漏洞	高危	新发现	中电福富
15	资产发现	127.0.0.1	认证授权	基础漏洞	高危	新发现	中电福富

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：

漏洞处置 主机漏洞 Web漏洞 弱口令 基线违背 人工渗透

查询条件 ▼ 展开 🔍 查询 🔄 重置

漏洞名称: 漏洞状态: 请选择 业务系统: 请选择 漏洞等级: 请选择

<input type="checkbox"/>	所属业务系统	主机资产	资产IP	漏洞名称	漏洞等级	当前状态	最近发现时间	最早发现时间	所属专业	所属部门	责任人	操作
<input type="checkbox"/>	BVS系统	asset_info	2.2.34.2	strunk2	高危	新发现	2017-11-22 16:58:10	2017-11-22 17:19:11	无线	中电福富	遵义A	2 处理 查看
<input type="checkbox"/>	BVS系统		192.168.0...	strunk2	中危	新发现	2017-11-22 11:06:00	2017-11-22 11:27:02	无线	中电福富		2 处理 查看

共 2 条 < 1 > 前往 1 页

● 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 **更多** 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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 处理方式1： 处理方式1

处理方式2： 处理方式2

* 整改时间： 选择日期时间

* 整改情况：

重置 提交

处置流程：
发现 处理 审核 完成

(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：

处置流程：
发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 材料证明： 点击上传

仅支持.doc和.docx文件

* 申请误报说明：

重置 提交

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 预计完成时间：

* 说明：

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 说明：

(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：

处置流程： 1 发现 2 处理 3 审核 4 完成

已处理 申请误报 申请延期 申请不处理 申请可关停

* 说明：

● 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：

漏洞处置 ×

基本信息	漏洞编号：	漏洞名称：strunk2	漏洞等级：高危
	漏洞状态：待审核(误报)	业务系统：BVS系统	IP地址：2.2.34.2
	端口号：	CVE编号：	Bugtraq号：
	所属专业：无线	所属部门：中电福富	责任人：遵义A
	最早发现时间：2017-11-22 17:19:11	最近发现时间：2017-11-22 16:58:10	更多

处置流程：
✔ 发现 — ✔ 处理 — 3 审核 — 4 完成

审查通过 审查拒绝

* 审核情况说明：

重置

历史记录

漏洞名称: strunk2
 误报材料: redis安装文档.docx
 情况说明: 误报啦啦啦啦

(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：

处置流程：
✔ 发现 — ✔ 处理 — 3 审核 — 4 完成

审查通过 审查拒绝

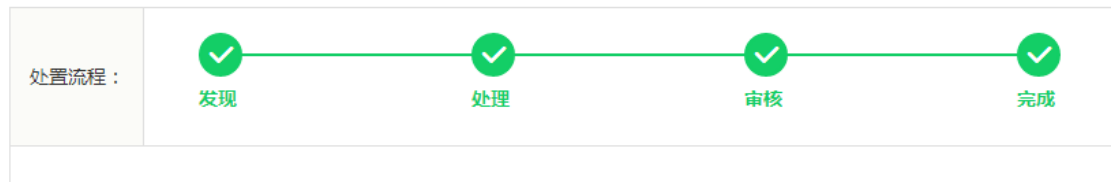
* 审核情况说明：

重置

历史记录

漏洞名称: strunk2
 误报材料: redis安装文档.docx
 情况说明: 误报啦啦啦啦

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。

历史记录

漏洞名称:strunk2
误报材料:redis安装文档.docx
情况说明:误报啦啦啦啦

(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：

处置流程： 发现 处理 3 审核 4 完成

审查通过 审查拒绝

* 审核情况说明：

- 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：

处置流程： 发现 处理 3 审核 4 完成

审查通过 审查拒绝

* 审核情况说明：

- 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

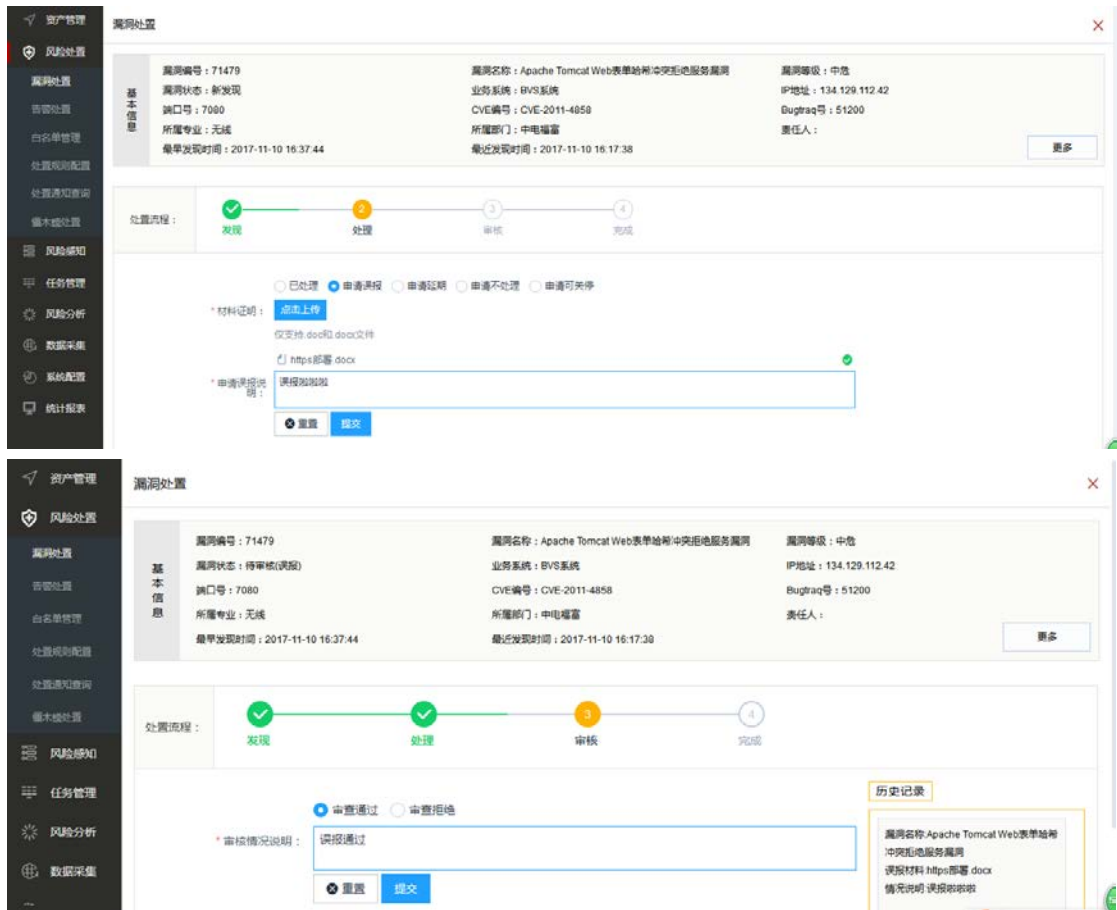
点击 **导出** 按钮，导出漏洞数据，如图：

	A	B	C	D	E	F	G	
	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	凌义A
3	BVS系统	192.168.68.229	strunk2	人工渗透	中危	新发现	中电福富	凌义A
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								

2.5.3 告警处置

2.5.4 白名单管理

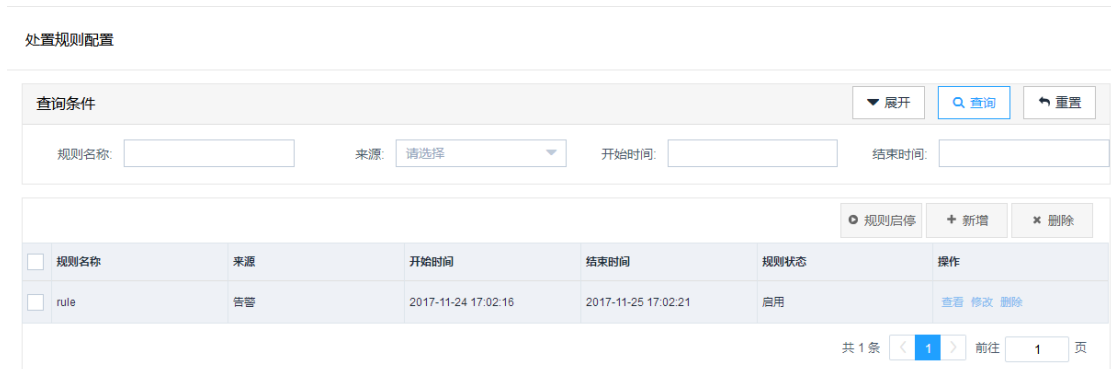
漏洞处置，处理时选择申请误报，审核通过后，这个漏洞就进入白名单
按如下操作步骤：





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”联动展示不同属性；如图：

处置规则配置 新增

* 规则名称：最多输入32个字符

有效开始时间：[选择时间范围]

设备范围：请选择

有效结束时间：[选择时间范围]

* 来源：请选择

* 告警方式： 派单告警 声光告警

* 发送时间范围：[选择] [选择时间范围]


工单时限(h)：0 [-] [+]

* 响应对象：请选择

* 通知方式： 工单 邮件 短信

[关闭] [提交]

- 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

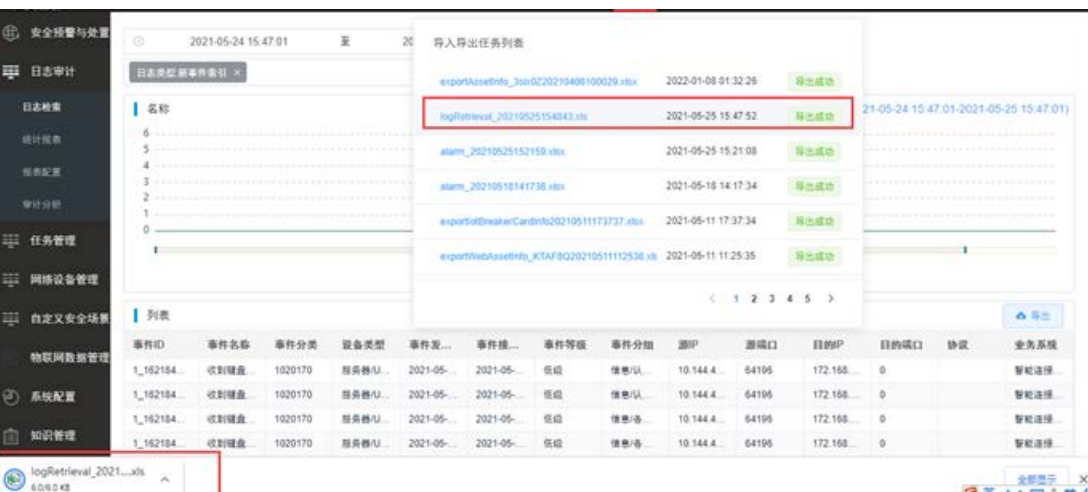
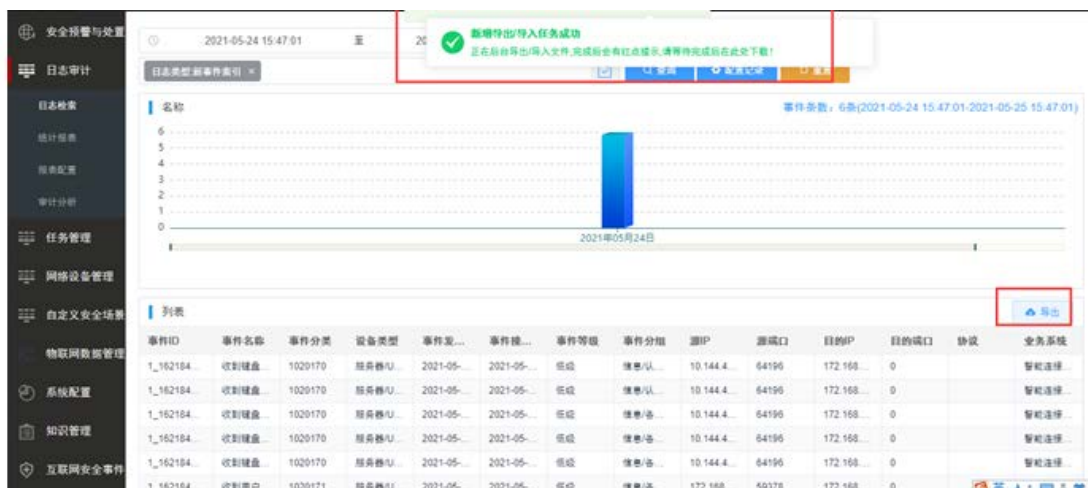


单机列表某行数据，弹窗展示事件详情信息，根据字段动态加载，只展示有数据的字段。



2.7.1.1 导出

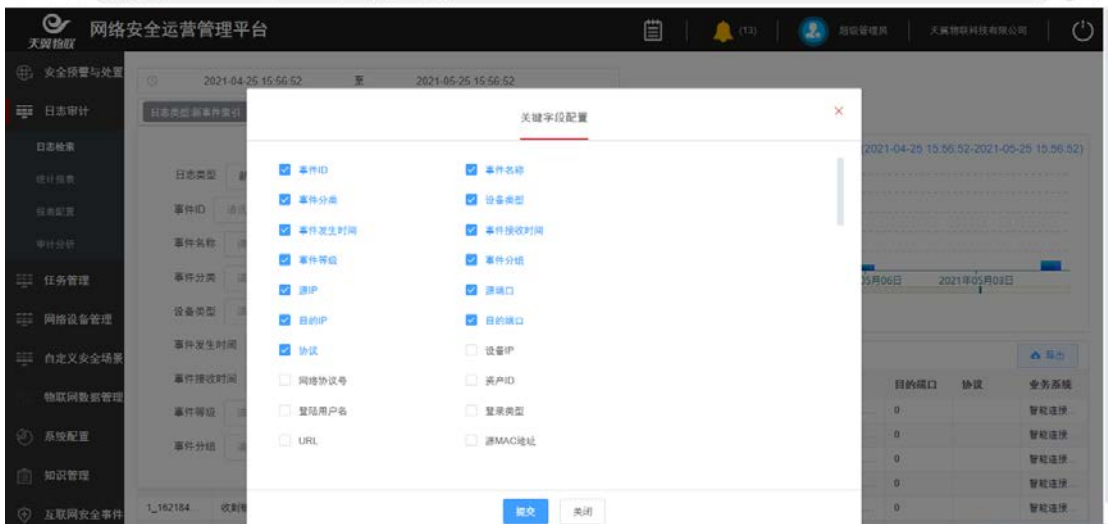
点击导出按钮，加入离线任务，鼠标移入导航栏异步任务窗口，可查看导出是否成功，点击文件名，可下载导出文件。



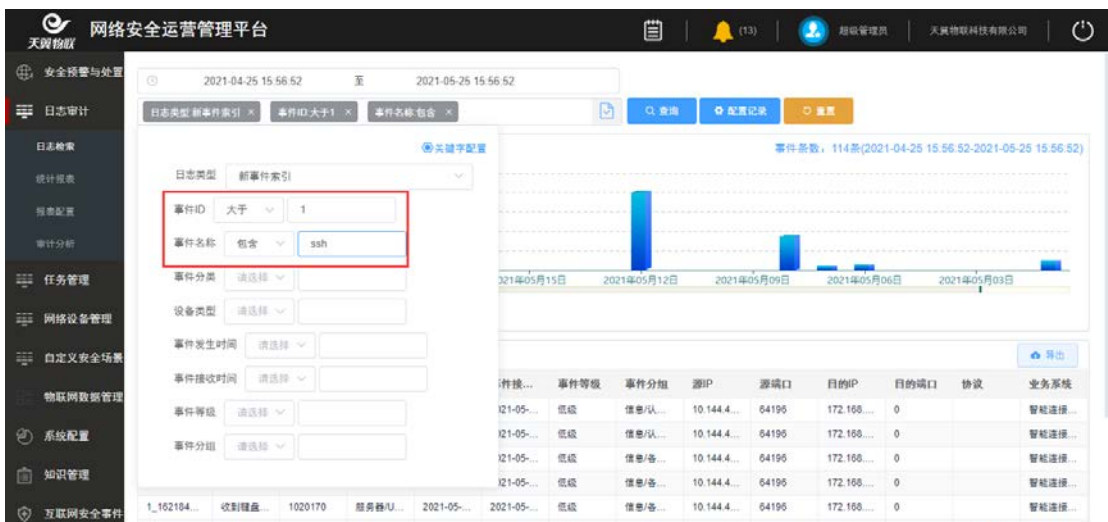
2.7.1.2 查询

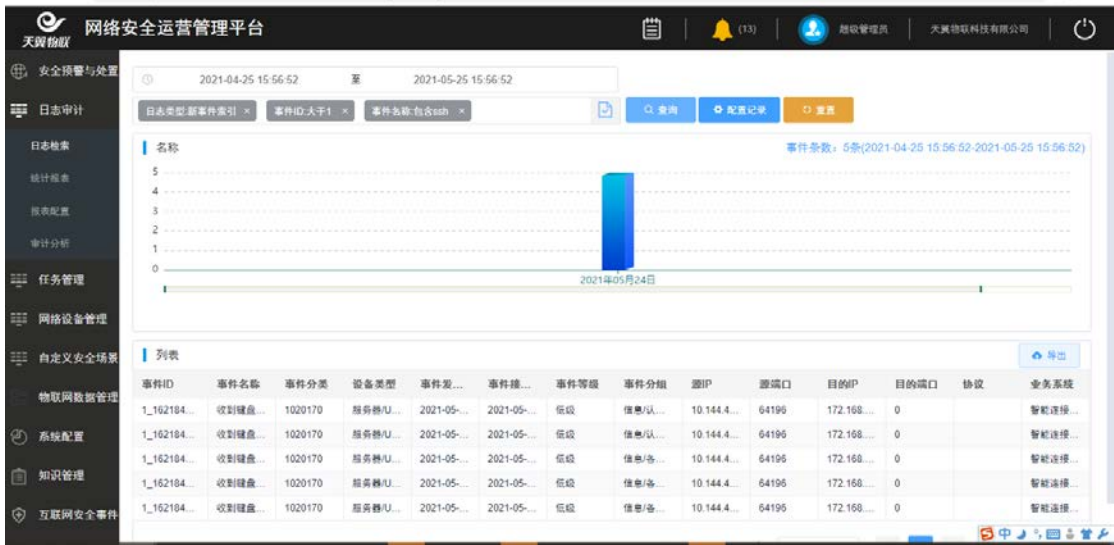
列表默认展示查询列表这些字段，可通过配置关键字调整列表展示的字段，

勾选状态的为当前展示字段，未勾选状态的不展示。

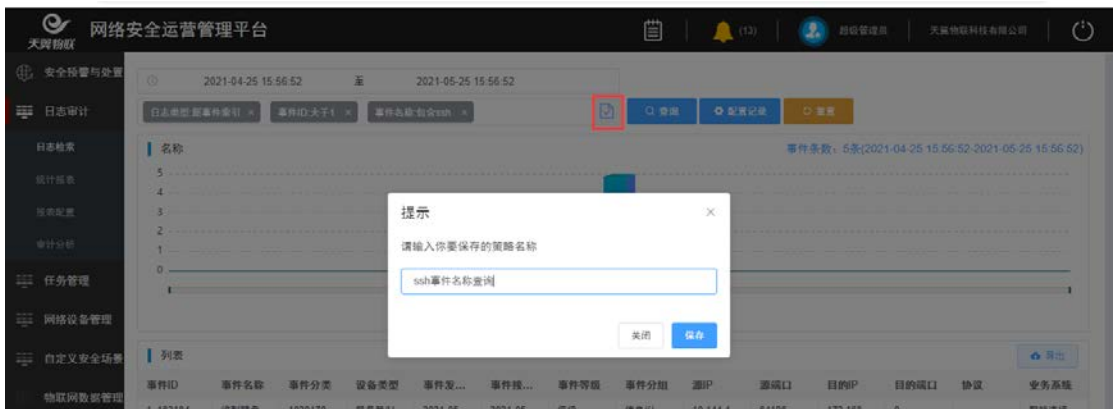


用户可根据需要配置过滤条件，点击查询，根据配置的条件筛选结果。

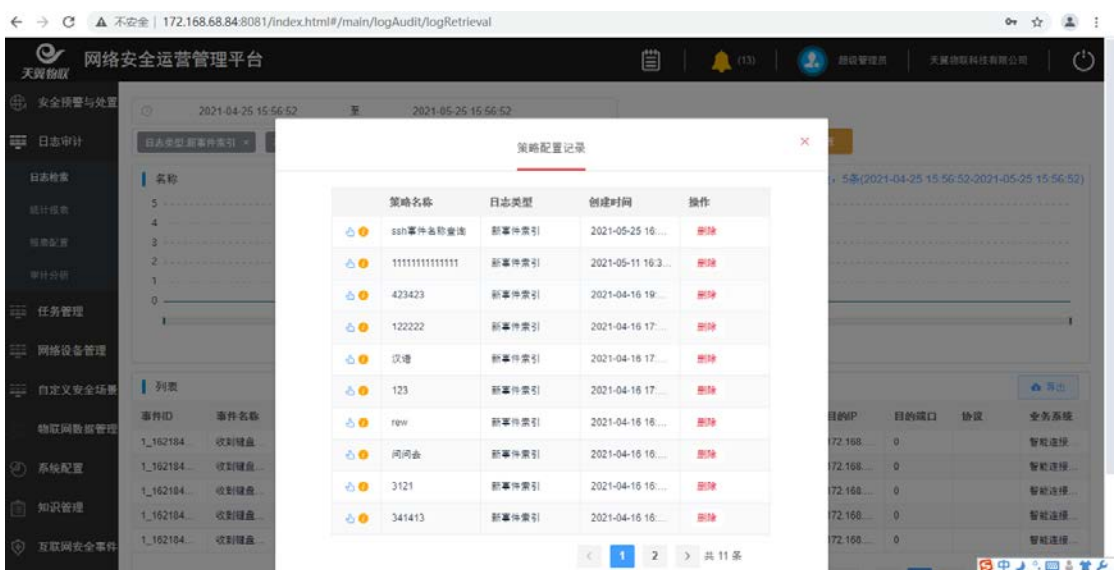




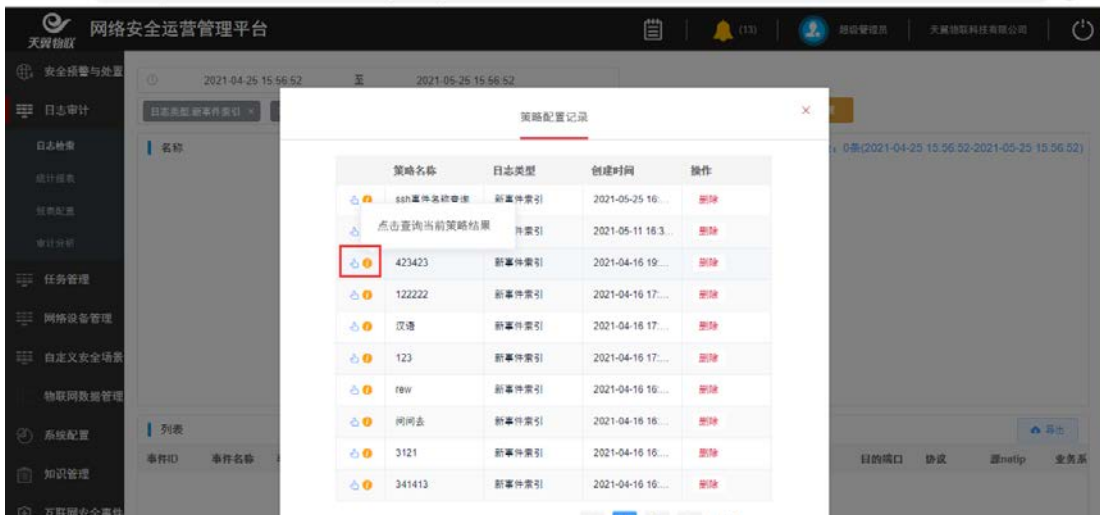
点击如图红框区域，可保存查询条件配置记录，输入名称，保存成功。



点击 **配置记录** 按钮，可查看配置记录。



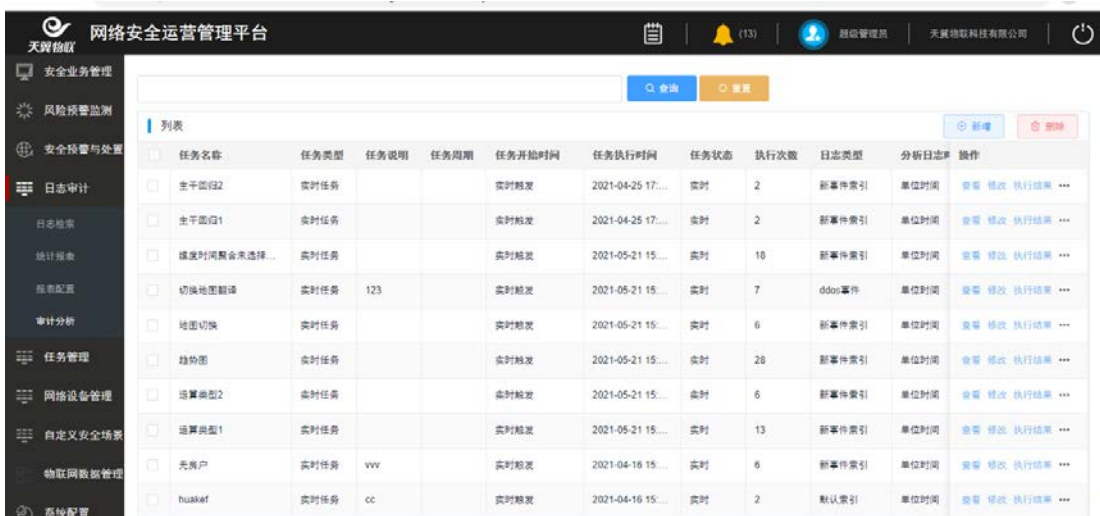
鼠标点击手指，可根据该条配置记录筛选结果。



2.7.2 审计分析

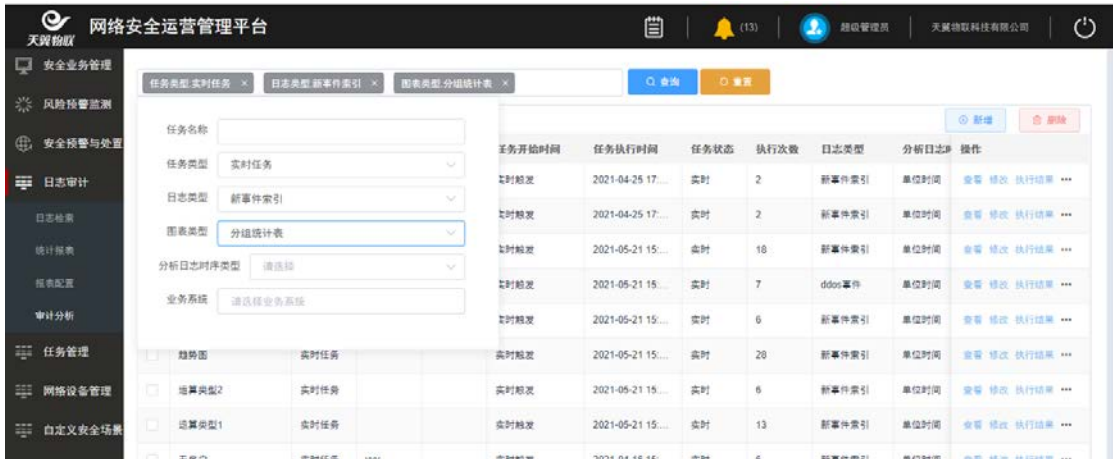
点击左侧主菜单日志审计>>审计分析，进入审计分析主界面，如图：

审计分析数据源为 es 集群上采集的相关日志。



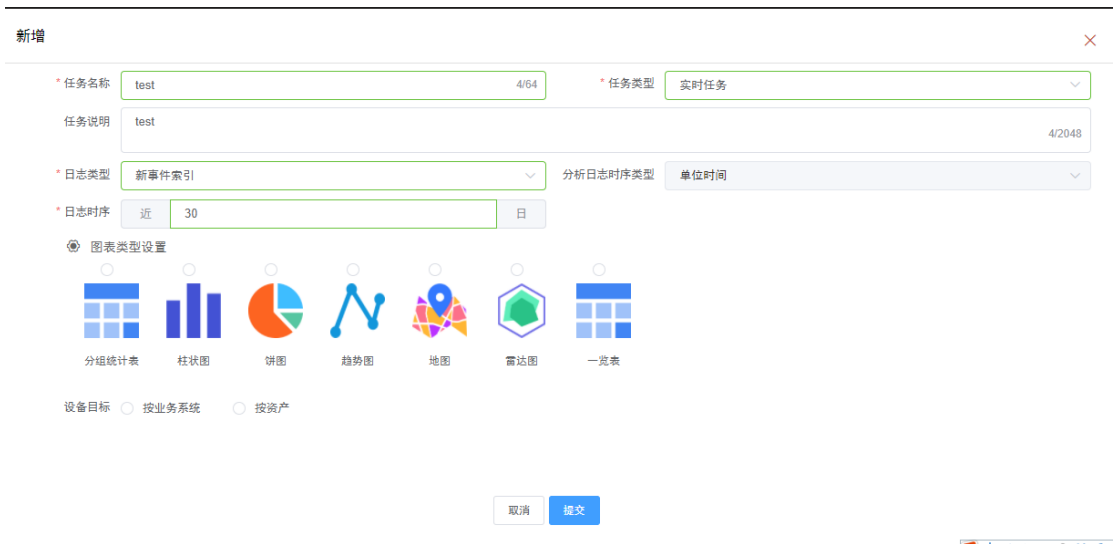
2.7.2.1 查询

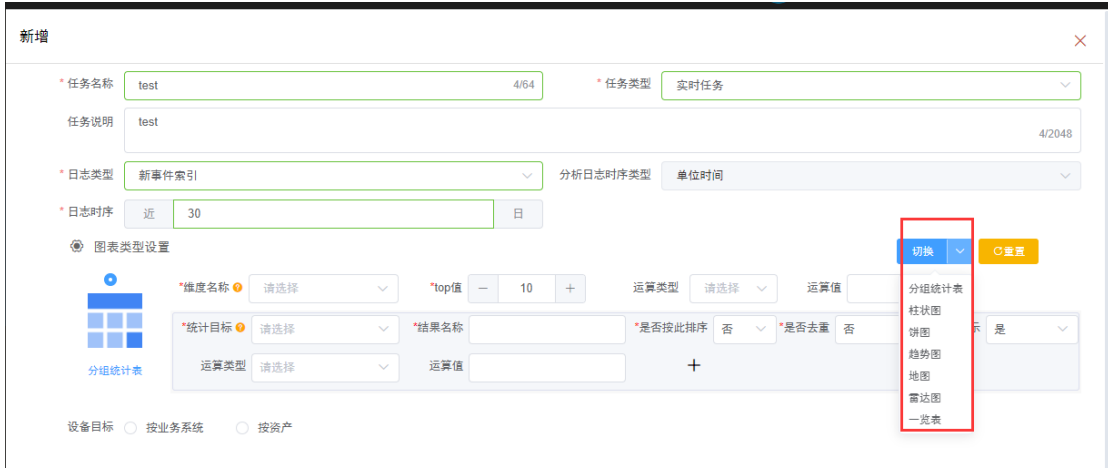
鼠标点击查询框，弹出查询条件，用户根据实际需要输入查询条件，点击查询按钮，根据查询条件筛选出正确结果，点击重置按钮，清空查询条件，并自动重新加载列表数据。

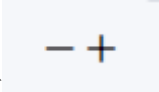


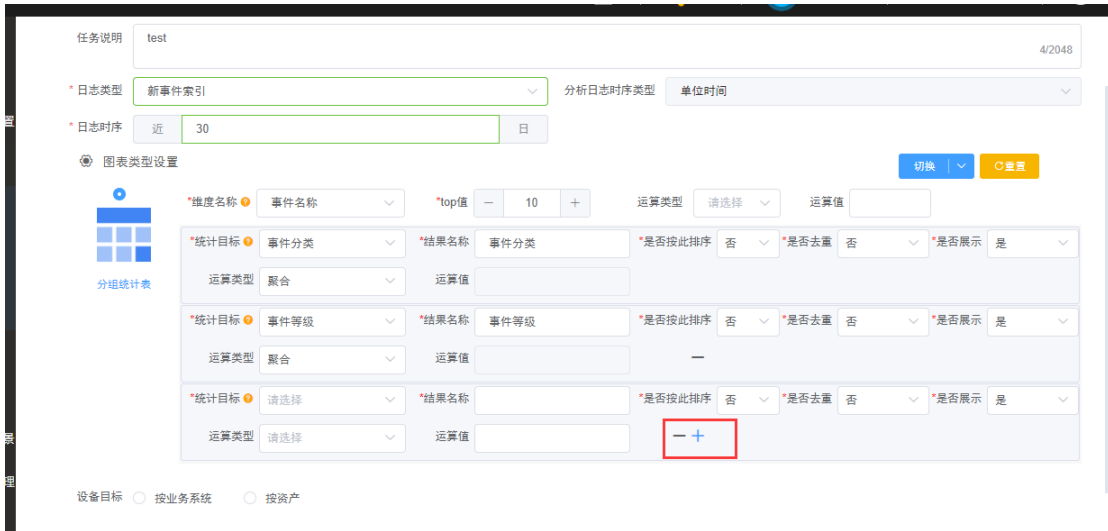
2.7.2.2 新增

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。

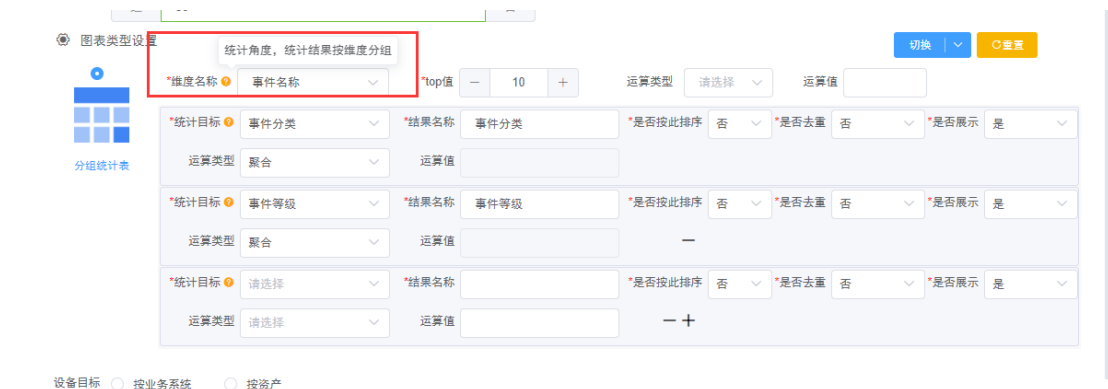




点击  按钮，可删减增加统计目标，鼠标点击某个统计目标行，可进行拖拽，移动统计目标的位置。

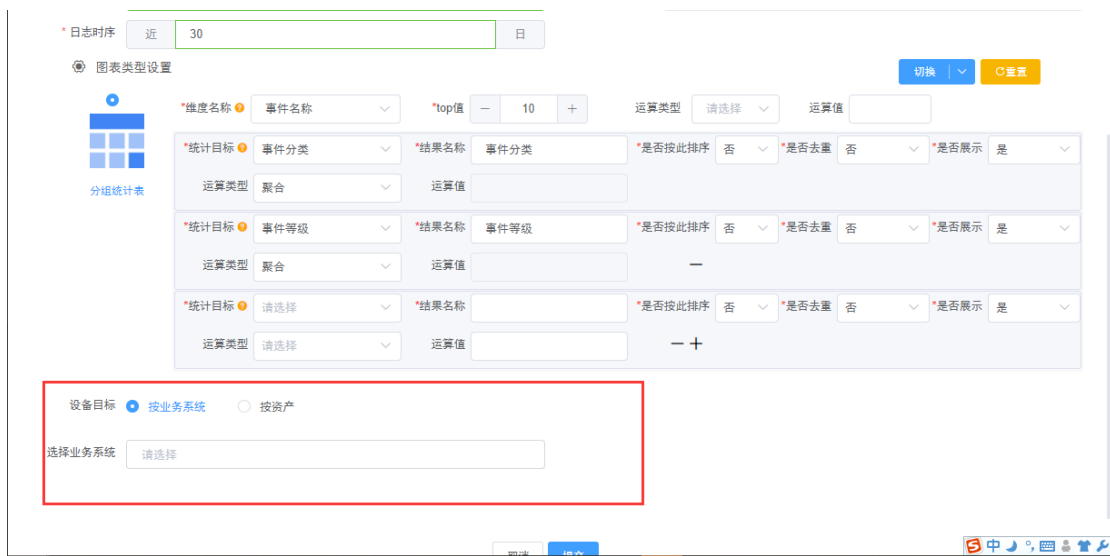


鼠标移入?，可查看注释。



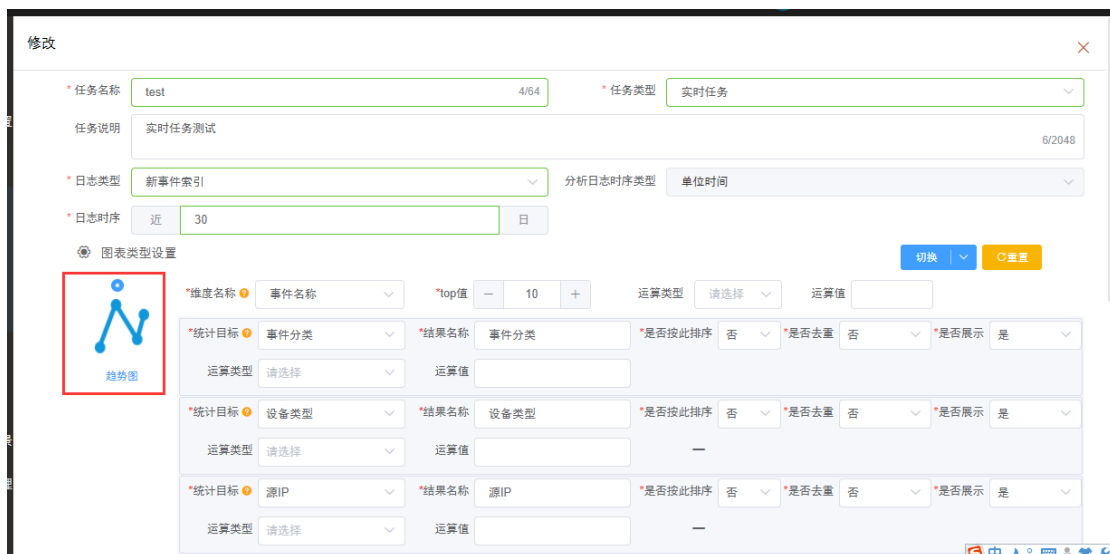


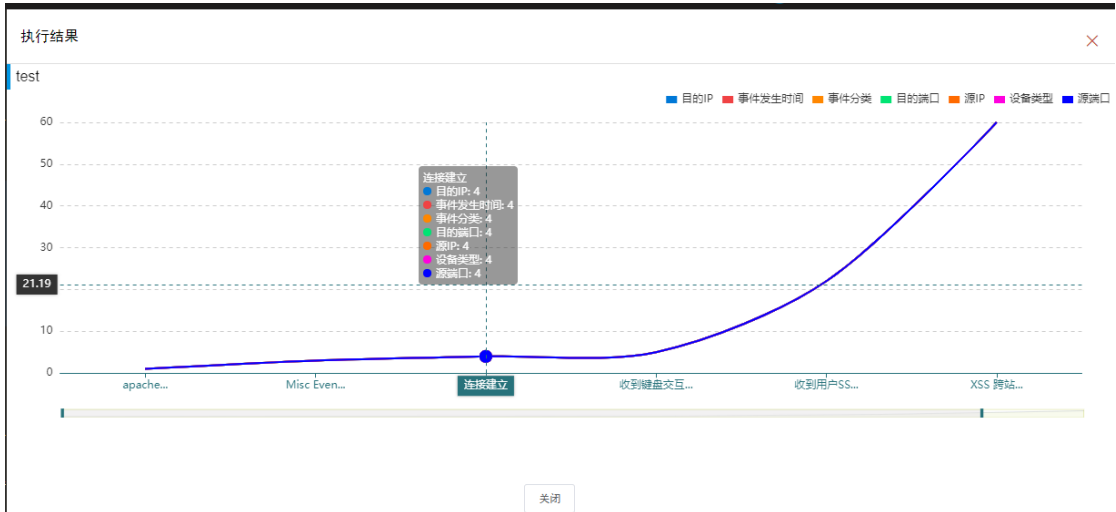
选择设备目标，可选择业务系统或资产维度，非必填，若不填，则默认针对所有资产；点击提交，任务创建成功。



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

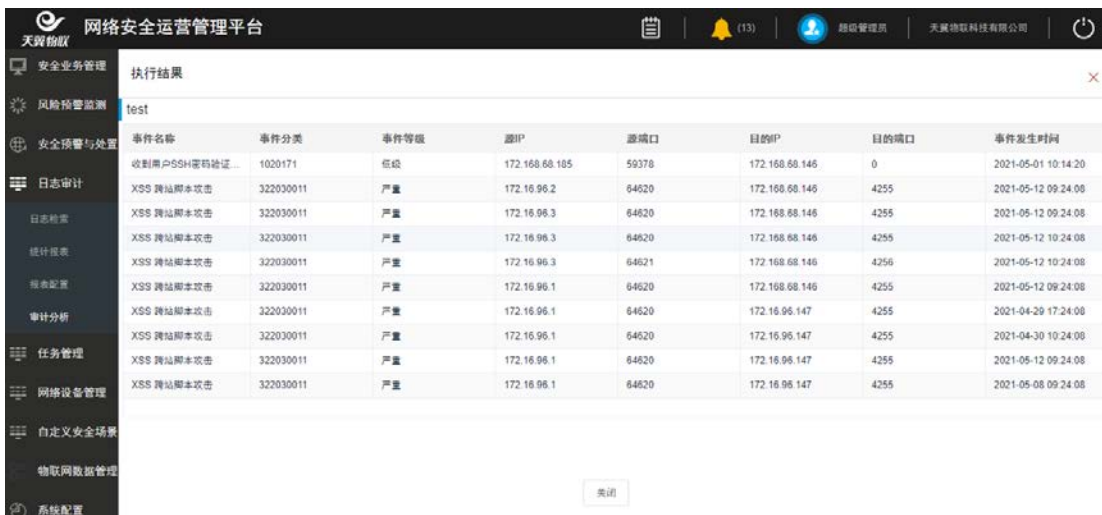
点击执行结果按钮，根据任务创建时选择的维度展示，如图：

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；

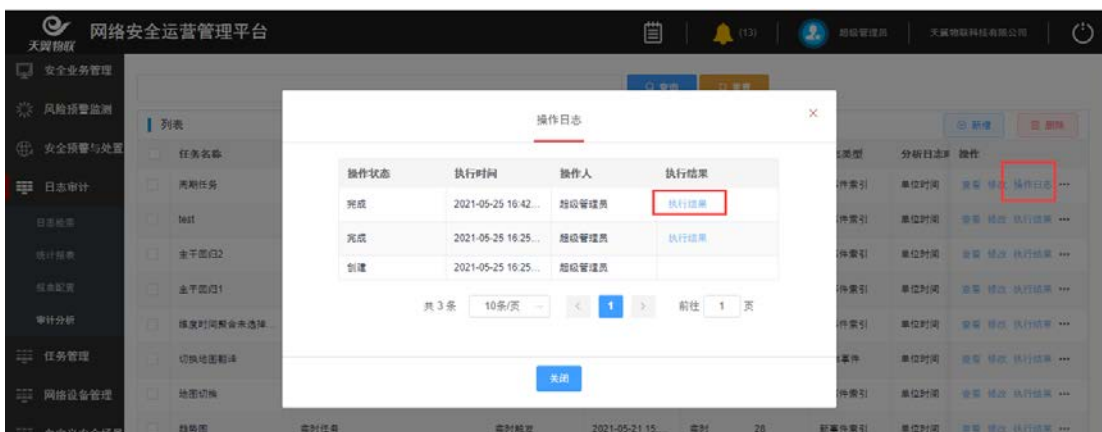
周期任务：系统按照任务周期定时统计日志时序内的的数据，执行结果根据周期变化；

任务名称	任务类型	任务说明	任务周期	任务开始时间	任务执行时间	任务状态	执行次数	日志类型	分析日志#	操作
test	实时任务	实时任...	实时触发			实时	0	新事件索引	单位时间	查看 修改 执行结果
金平西02	实时任务		实时触发	2021-04-25 17:...		实时	2	新事件索引	单位时间	查看 修改 执行结果
生平西01	实时任务		实时触发	2021-04-25 17:...		实时	2	新事件索引	单位时间	查看 修改 执行结果
维度时间剩余未选择...	实时任务		实时触发	2021-05-21 15:...		实时	18	新事件索引	单位时间	查看 修改 执行结果
切换地图翻译	实时任务	123	实时触发	2021-05-21 15:...		实时	7	ddos事件	单位时间	查看 修改 执行结果
地图切换	实时任务		实时触发	2021-05-21 15:...		实时	6	新事件索引	单位时间	查看 修改 执行结果
魏秀图	实时任务		实时触发	2021-05-21 15:...		实时	28	新事件索引	单位时间	查看 修改 执行结果



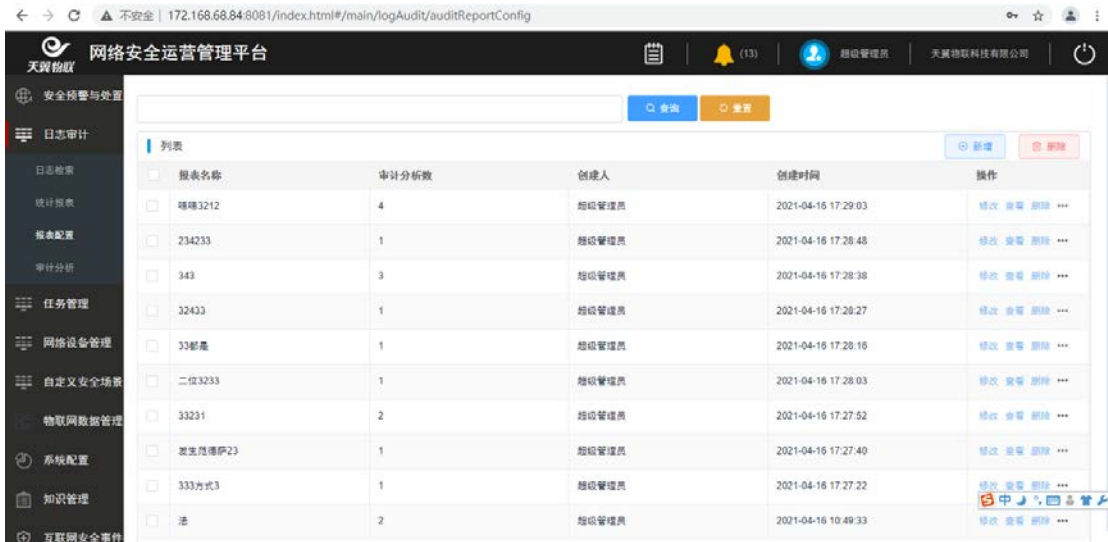
2.7.2.5 操作日志

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

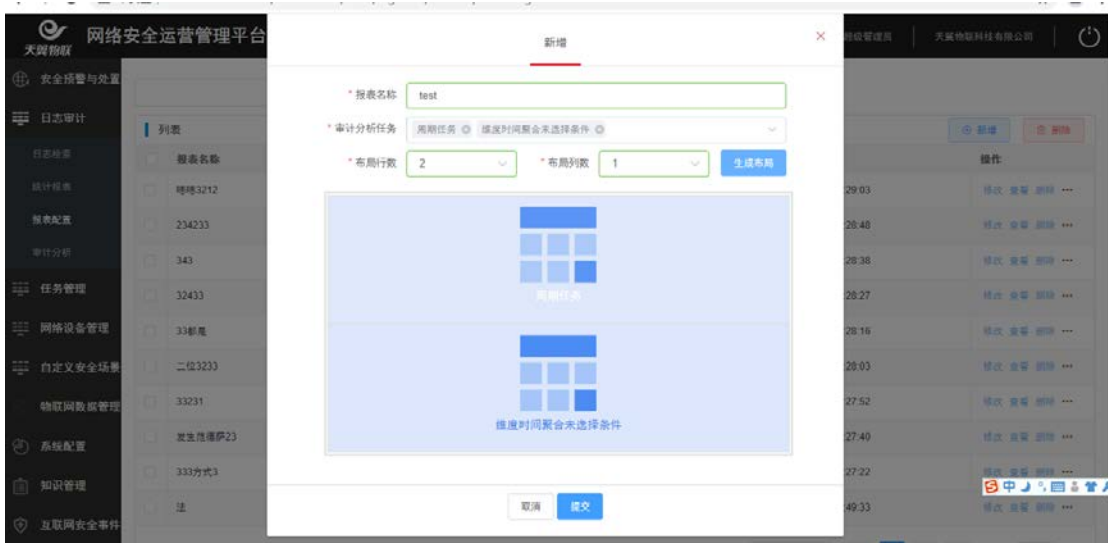
报表配置数据源为审计分析模块新建的相关任务。
列表页展示了报表名称、审计分析任务数、创建人、创建时间，提供报表名称、创建时间等查询条件。



列表	报表名称	审计分析数	创建人	创建时间	操作
<input type="checkbox"/>	瑞瑞3212	4	超级管理员	2021-04-16 17:29:03	修改 查看 删除 ...
<input type="checkbox"/>	234233	1	超级管理员	2021-04-16 17:28:48	修改 查看 删除 ...
<input type="checkbox"/>	343	3	超级管理员	2021-04-16 17:28:38	修改 查看 删除 ...
<input type="checkbox"/>	32433	1	超级管理员	2021-04-16 17:28:27	修改 查看 删除 ...
<input type="checkbox"/>	33邮箱	1	超级管理员	2021-04-16 17:28:16	修改 查看 删除 ...
<input type="checkbox"/>	二位3233	1	超级管理员	2021-04-16 17:28:03	修改 查看 删除 ...
<input type="checkbox"/>	33231	2	超级管理员	2021-04-16 17:27:52	修改 查看 删除 ...
<input type="checkbox"/>	发生地IP23	1	超级管理员	2021-04-16 17:27:40	修改 查看 删除 ...
<input type="checkbox"/>	333方式3	1	超级管理员	2021-04-16 17:27:22	修改 查看 删除 ...
<input type="checkbox"/>	法	2	超级管理员	2021-04-16 10:49:33	修改 查看 删除 ...

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。

修改

! 任务个数超出布局行列数,请重新设置

* 报表名称

* 审计分析任务 周期任务 维度时间聚合未选择条件 test

* 布局行数 * 布局列数 生成布局

取消 修改

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。

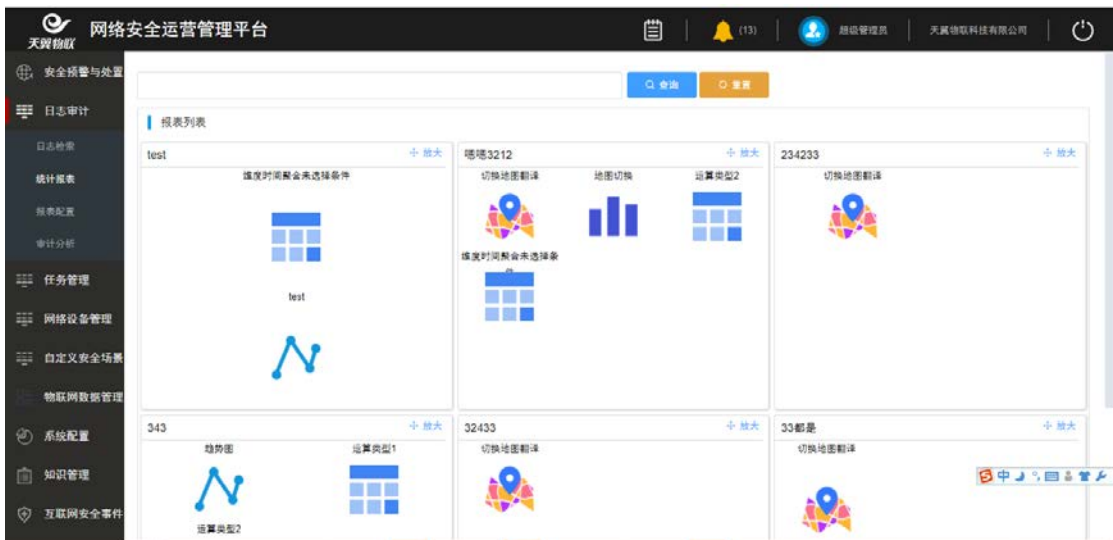
报表名称	审计分析数	创建人	创建时间	操作
test	2	超级管理员	2021-05-25 17:06:44	修改 查看 删除 ...
腾讯3212	4	超级管理员	2021-04-16 17:29:03	修改 查看 删除 ...
234233	1	超级管理员	2021-04-16 17:28:48	修改 查看 删除 ...
343	3	超级管理员	2021-04-16 17:28:38	修改 查看 删除 ...
32433	1	超级管理员	2021-04-16 17:28:27	修改 查看 删除 ...
33888	1	超级管理员	2021-04-16 17:28:16	修改 查看 删除 ...



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：

新增 ✕

* 漏洞告警规则名称：

* 漏洞告警等级：

漏洞名称：

* 漏洞等级：

* 是否进行关联分析： 是 否

漏洞告警归并条件： 告警名称 告警规则

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：

+ 新增 ✕ 删除					
<input type="checkbox"/>	漏洞告警名称	漏洞规则等级	漏洞名称	漏洞等级	操作
<input type="checkbox"/>	漏洞告警规则test2	严重	openssl	严重	查看 修改 删除
<input type="checkbox"/>	漏洞告警规则1	高级	openssh	高级	查看 修改 删除

共 2 条 < 1 > 前往 1 页

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：

告警策略 脆弱性策略 关联告警策略

查询条件 🔍 查询 🔄 重置

规则名称： 规则类型： 循环次数： - 可靠性：

+ 新增

规则名称	规则类型	循环次数	可靠性	事件等级	创建时间	创建者	是否只读	操作
关联alarm	用户自定义	3	4	严重	2017-11-27 13:58:36	root	否	查看 修改 删除

共 1 条 < 1 > 前往 1 页


- 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：



鼠标分别点击左侧任意数，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“安全事件对象 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；

规则名称	规则类型	循环次数	可靠性	事件等级	创建时间	创建者	是否只读	操作
关联alarm	用户自定义	3	4	严重	2017-11-27 13:58:36	root	否	查看 修改 删除

共 1 条 < 1 > 前往 1 页

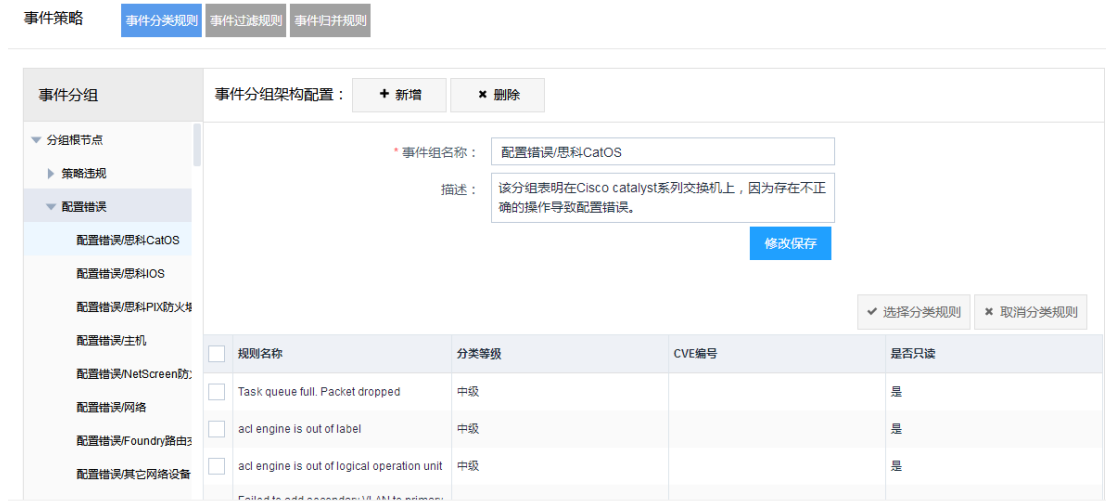
2.8.2 事件策略

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：

事件分组架构配置：

[+ 新增](#) [× 删除](#)

* 事件组名称：

描述：

父节点：

[新增保存](#)

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：

事件分类规则 ×

查询条件 ▼ 展开 🔍 查询 ↺ 重置

规则名称： 分类等级： CVE编号： 是否只读：

[确认选择](#) [+ 新增](#) [× 删除](#)

<input type="checkbox"/>	规则名称	分类等级	CVE编号	是否只读	操作
<input type="checkbox"/>	NETBIOS-DG SMB Isass DsRolerGetPrimaryDomainInformation attempt	中级	CAN-2003-0533	是	查看 修改 删除
<input type="checkbox"/>	NETBIOS SMB Isass DsRolerGetPrimaryDomainInformation little endian attempt	中级	CAN-2003-0533	是	查看 修改 删除
<input type="checkbox"/>	SPYWARE-PUT Trickler maxsearch runtime detection - toolbar download	中级		是	查看 修改 删除
<input type="checkbox"/>	SPYWARE-PUT Hijacker netguide runtime detection	中级		是	查看 修改 删除

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：

提示

此操作将选择规则到分组中, 是否继续?

取消


确定

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  按钮, 列表栏即会列出满足要求的分类规则。点击  按钮, 可重新设置查询条件。

事件分类规则 ×

查询条件				展开	查询	重置	
规则名称:	<input type="text"/>	分类等级:	请选择	CVE编号:	<input type="text"/>	是否只读:	请选择

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  按钮, 弹出规则配置窗口, 如图:

新增 ✕

添加关键字的格式为-SU:((关键字1))-SU:((关键字2))等多个中间用逗号隔开;添加正则表达式的格式为-RU:((您的正则式)) ✕

* 规则名：	<input type="text"/>
CVE编码：	<input type="text"/>
* 分类等级：	<input type="text" value="请选择"/>
规则描述：	<input type="text"/>
建议措施：	<input type="text"/>
误报信息：	<input type="text"/>
关键字：	<input type="text"/>
正则表达式：	<input type="text"/>
* 规则所属设备：	<input type="text" value="请选择"/>

关闭 提交

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 提交 按钮，提交配置信息。

查看： 点击分类当前行的 查看 按钮，可查看该规则的详细信息。


编辑： 点击分类当前行的 修改 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。

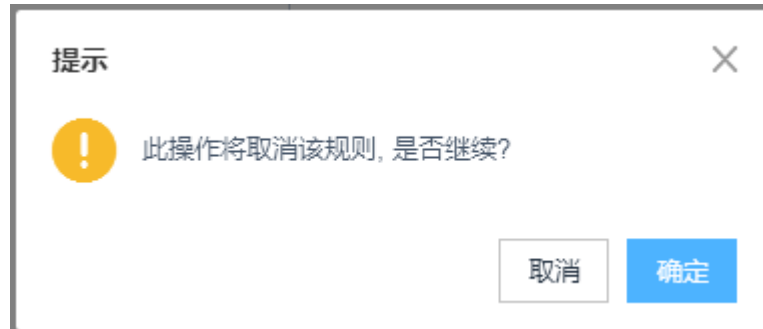
删除： 选择某一个只读属性为否的分类规则，点击 删除 按钮，可删除该分类规则。

批量删除： 选择多个只读属性为否的分类规则，点击 ✕ 删除 按钮，可批

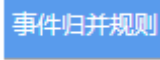
量删除分类规则。

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

事件策略 事件分类规则 事件过滤规则 事件归并规则

查询条件 Q 查询 重置

规则名称： 归并时间(秒)： 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：

+ 新增 * 删除


<input type="checkbox"/>	规则名称	归并时间(秒)	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	操作
暂无数据							

共 0 条 < > 前往 页


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。

风险评估

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：

风险评估

业务系统 资产 地域 安全域

查询条件 Q 查询 ↶ 重置

风险区间: - 业务系统:

业务系统名称	风险等级	风险值	风险生成时间	操作
外网扫描系统	严重	3		查看
内网扫描系统	轻微	5		查看
101001业务系统	中级	2		查看
found4	中级	2		查看
内网扫描系统2	严重			查看
BVS业务系统				查看
agent属性获取系统				查看
found3				查看

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：



2.8.3.2 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：

风险评估 业务系统 资产 地域 安全域

查询条件 🔍 查询 ↶ 重置

风险区间： - 业务系统：

安全对象名	业务系统	设备类型	风险等级	风险值	风险生成时间	事件数	最近接收时间	操作
asset_yingyong1	ws业务系统	应用系统/web服务/...	严重	5	2017-12-01 11:00:00	6	2017-12-01 00:10:00	查看
hbase172_redis_6...	内网扫描系统	应用系统/数据库/redis						查看
189_zookeeper_21...	内网扫描系统	应用系统/web服务/...						查看
hbase172_zookeep...	内网扫描系统	应用系统/web服务/...						查看
asset—导入test2	ws业务系统	应用系统/web服务/...						查看
asset—导入test2	ws业务系统	应用系统/web服务/...						查看
asset shouye3	ws业务系统	应用系统/web服务/...						查看

选择一个安全资产，点击 查看 按钮，显示如图：

基本信息	风险趋势图	安全对象威胁	安全对象漏洞	安全对象配置隐患	✕
安全对象名称:	asset_yingyong1				
采集方式:	手工录入				
所属业务系统:	ws业务系统				
安全对象类别:	应用系统/web服务/jboss				
安全对象编号:					
可用性:					
完整性:					
保密性:					

- 时间点风险值趋势

风险趋势图

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：

基本信息 风险趋势图 **安全对象威胁** 安全对象漏洞 安全对象配置隐患



ID	威胁名称	威胁等级	可靠性	发现时间
暂无数据				

- 安全对象漏洞

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 风险趋势图 安全对象威胁 **安全对象漏洞** 安全对象配置隐患



ID	漏洞名称	端口	严重级别	扫描时间
21588	OpenSSH默认服务器配置拒绝服务漏洞(CVE-2010-5107)	22	中级	
21588	SSH版本信息可被获取	22	轻微	
21588	检测到远端RPCBIND/PORTMAP正在运行中	111	轻微	
21588	目标主机rpcinfo -p 信息泄露	111	低级	
21588	检测到远端RPCBIND/PORTMAP正在运行中	111	轻微	

共 9 条 < 1 > 前往 1 页

- 基本信息

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：

基本信息 风险趋势图 安全对象威胁 安全对象漏洞 安全对象配置隐患



安全对象名称:	asset_yingyong1
采集方式:	手工录入
所属业务系统:	ws业务系统
安全对象类别:	应用系统/web服务/jboss
安全对象编号:	
可用性:	
完整性:	
保密性:	

● 安全对象配置隐患

安全对象配置隐患

在 sheet 中只展示该资产的配置隐患信息，如图：

基本信息 风险趋势图 安全对象威胁 安全对象漏洞 安全对象配置隐患



ID	隐患名称	异常状态	严重级别
暂无数据			

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：

安全事件查询

查询条件 展开 查询 重置

安全对象： 报警系统IP： 业务域： 事件等级：

事件名	业务系统	安全对象	报警系统	源IP	目的IP	归并数	接收时间	描述
堡垒机登陆成功	101802测试系统	asset_tyep1	172.16.66.201	136.64.44.251	136.74.100.201	1	2017-11-23 11:05:14	<FA:0>sessionId=aa...
堡垒机登陆成功	101802测试系统	asset_tyep1	172.16.66.201	136.64.44.251	136.74.100.201	1	2017-11-23 11:03:17	<FA:0>sessionId=aa...
堡垒机登陆成功	101802测试系统	asset_tyep1	172.16.66.201	136.64.44.251	136.74.100.201	1	2017-11-23 10:58:29	<FA:0>sessionId=aa...
堡垒机登陆成功	101802测试系统	asset_tyep1	172.16.66.201	136.64.44.251	136.74.100.201	1	2017-11-23 10:57:14	<FA:0>sessionId=aa...
堡垒机登陆成功	101802测试系统	asset_tyep1	172.16.66.201	136.64.44.251	136.74.100.201	1	2017-11-23 10:55:22	<FA:0>sessionId=aa...
堡垒机登陆成功	101802测试系统	asset_tyep1	172.16.66.201	136.64.44.251	136.74.100.201	1	2017-11-23 10:50:52	<FA:0>sessionId=aa...
堡垒机登陆成功	101802测试系统	asset_tyep1	172.16.66.201	136.64.44.251	136.74.100.201	1	2017-11-23 10:46:52	<FA:0>sessionId=aa...
堡垒机登陆失败	101802测试系统	asset_tyep1	172.16.66.201	172.16.66.98	172.16.66.201	1	2017-11-23 10:44:13	<DB:0>sessionId=a...

选中其中一条记录，双击可查看详情，如图：

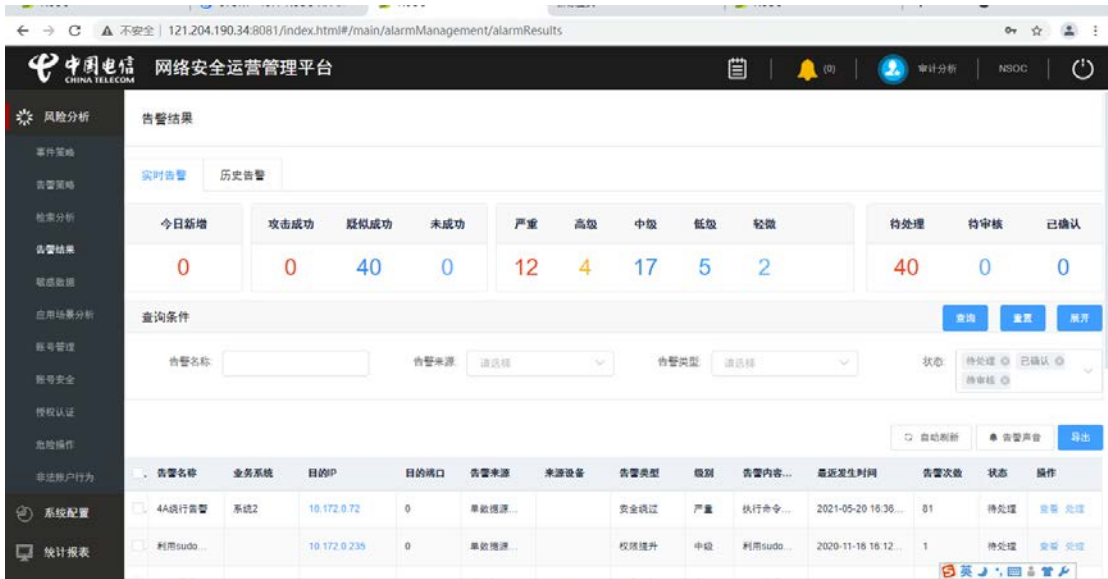
安全事件查询详情 ×

事件信息 病毒信息 流量信息 设备信息

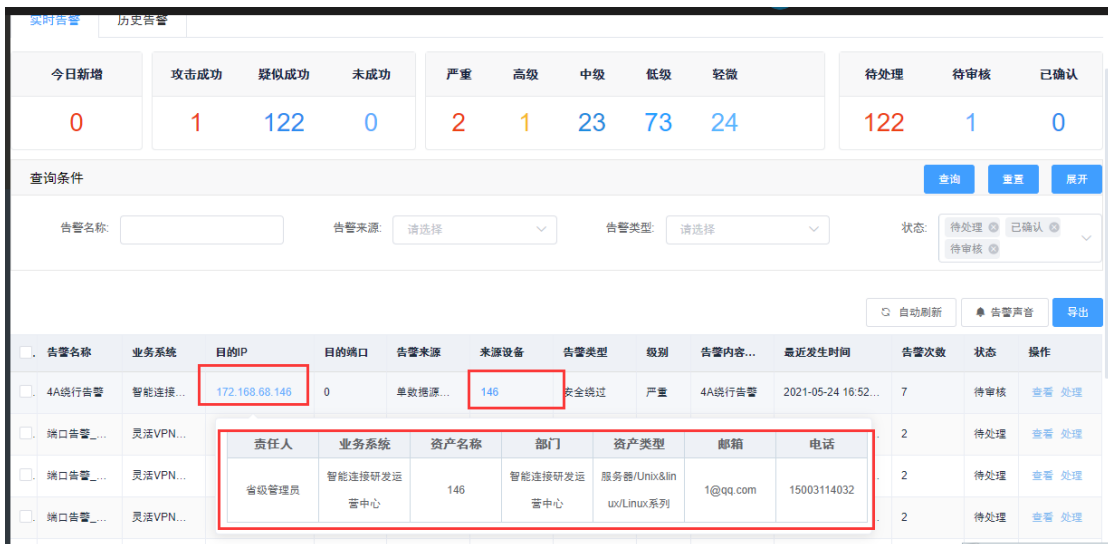
事件编号:	19	事件名称:	堡垒机登陆成功
事件分组ID:	1041514	详细事件类型ID:	1043091001
事件分组类型:	信息/成功登录/网络设备	详细事件类型:	
报警系统:	172.16.66.201	漏洞编号:	
协议类型:		特征串:	
匹配字符:		源IP:	136.64.44.251
源端口:	0	目的IP:	136.74.100.201
目的端口:	0	事件接收时间:	2017-11-23 11:05:14
事件发生时间:	2017-11-23 11:05:14	事件等级:	低级

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：

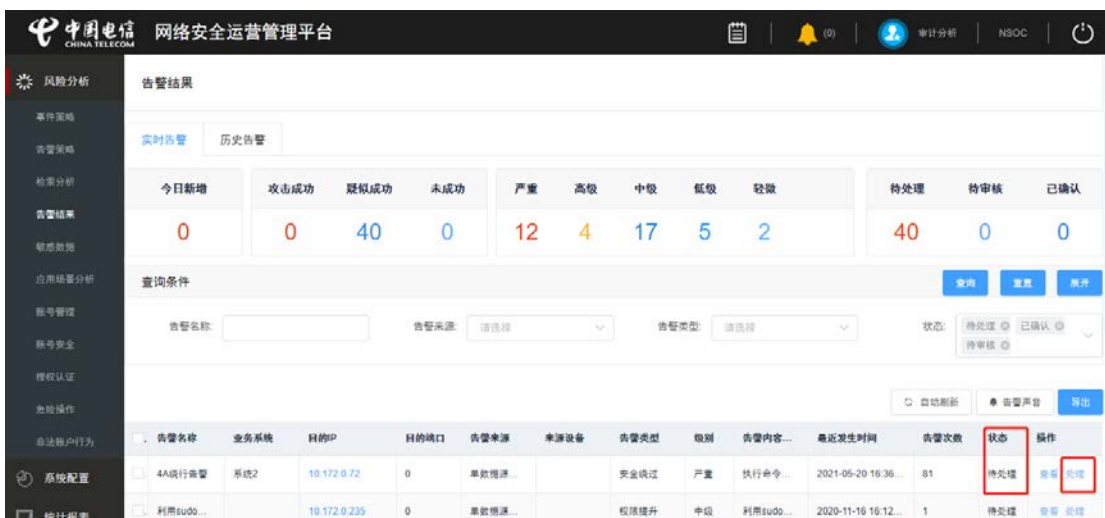
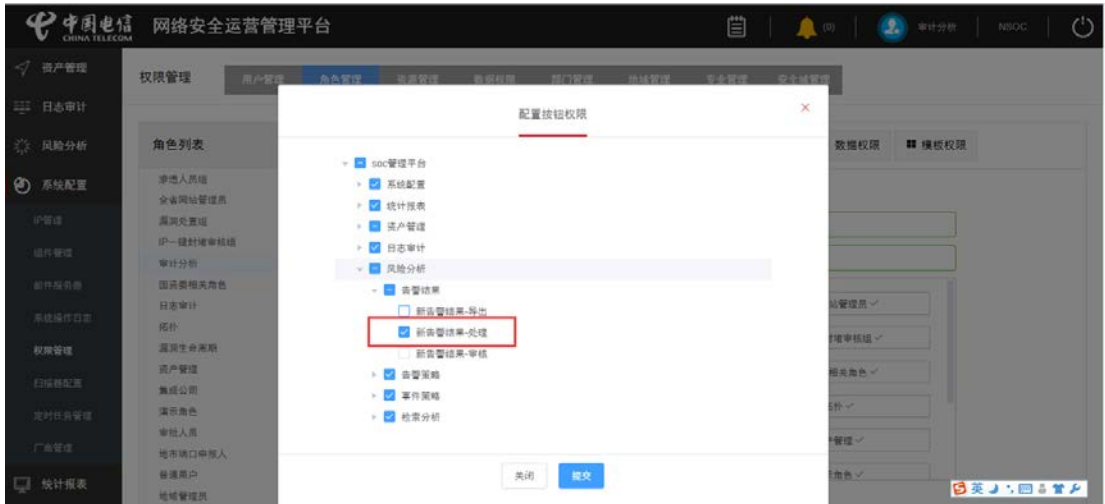


点击 ip、设备名称，关联出责任人信息。

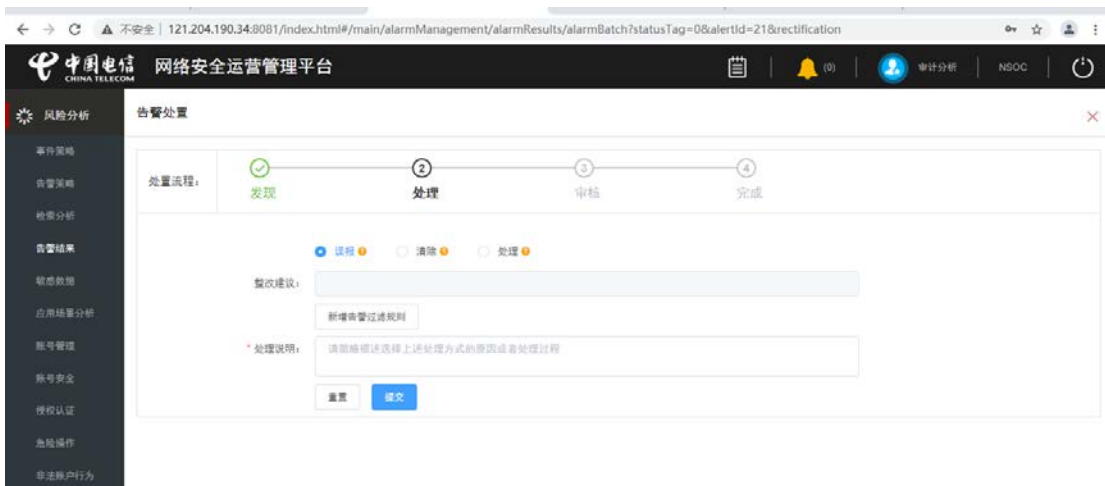


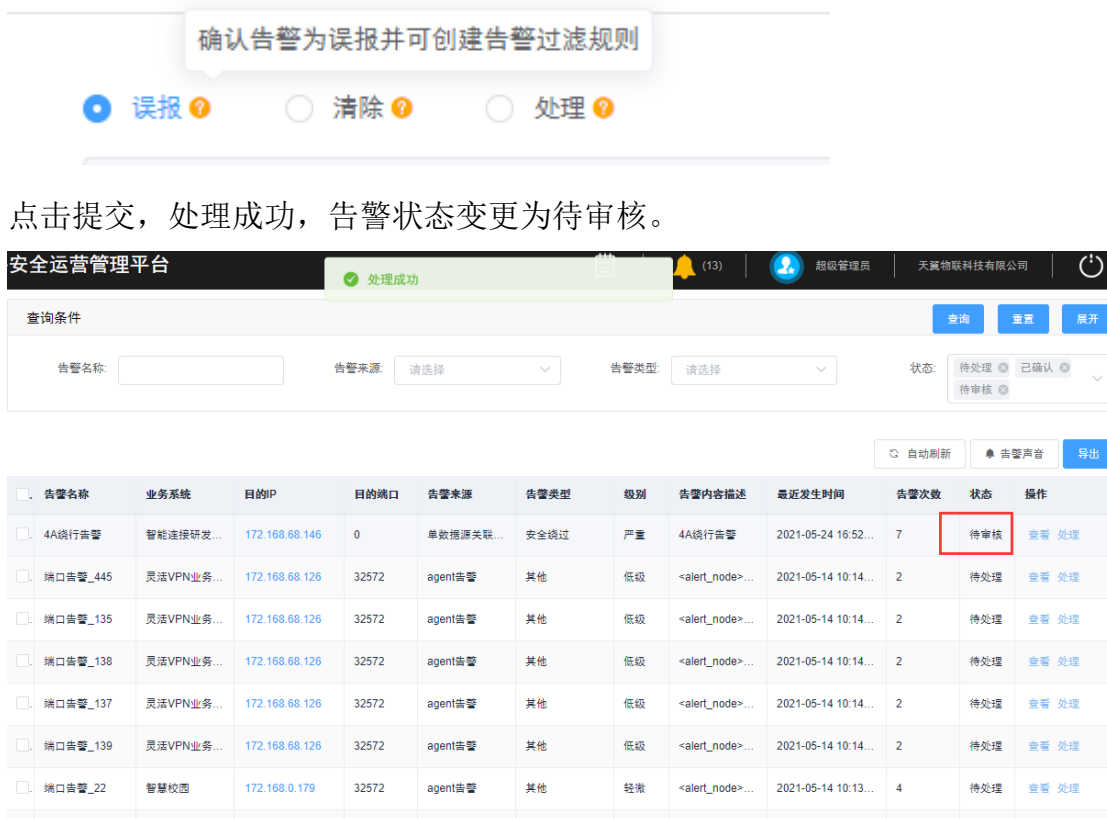
2.8.5.1 告警结果处置

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。





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；

告警结果

实时告警 | 历史告警

今日新增	攻击成功	疑似成功	未成功	严重	高级	中级	低级	轻微	误报	已清除	已处理
0	1	17	0	2	0	1	14	1	10	4	4

查询条件: 告警名称: [] 告警来源: [请选择] 告警类型: [请选择] 状态: [已处理] [已清除] [误报]

告警名称	业务系统	目的IP	目的端口	告警来源	告警类型	级别	告警内容描述	最近发生时间	告警次数	状态	操作
4A绕行告警	智能连接研发...	172.168.68.146	0	单数据源关联...	安全绕过	严重	4A绕行告警	2021-04-28 14:37...	1	误报	查看
端口告警_23	灵活VPN业务...	172.168.68.120	32560	agent告警	其他	低级	<alert_node>...	2021-04-26 09:25...	2		

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。

告警结果

详细信息 | 归并告警 | 状态追溯 | 归并统计

基本信息

告警名称: 4A绕行告警

告警类型: 安全绕过

告警来源: 单数据源关联分析告警

告警等级: 严重

状态: 待审核

最近发生时间: 2021-05-24 16:52:27

攻击阶段分布

侦察 → 投递 → 攻击渗透 → 安装工具 → 命令控制 → 恶意活动 → 工具制作 → 侦察

IP信息

源IP: 10.144.4.58 源端口: 64196 目的IP: 172.168.68.146 目的端口: []

[收缩] [关闭] [处理]

告警等级: 严重

状态: 待审核

最近发生时间: 2021-05-24 16:52:27

IP信息

源IP: 10.144.4.58 源端口: 64196 目的IP: 172.168.68.146 目的端口: 0

来源设备

设备名称: 146 设备IP:

责任人	业务系统	资产名称	部门	资产类型	邮箱	电话
省级管理员	智能连接研发中心	146	智能连接研发中心	服务器/Unix&linux/Linux系列	1@qq.com	15003114032

告警描述

4A绕行告警

整改建议

< 收缩 × 关闭 处理

归并信息：

点击 ip，弹出责任人、资产、电话等信息。。

告警结果

详细信息 归并告警 状态追溯 归并统计

查找内容

告警编号	告警名称	告警来源	告警类型	攻击链阶段	告警等级	目的IP	源IP	关联事件数	发生时间	操作
16218486026...	4A绕行告警	单数据源关...	安全绕过	攻击渗透	严重	172.168.68.146	10.144.4.58	1	2021-05-24 ...	查看 追溯

事件名称	源ip	源端口	目的ip	目的端口	发生时间	操作
收到键盘交互式ssh密码...	10.144.4.58	64196	172.168.68.146	0	2021-05-24 16:52:27	查看

责任人	业务系统	资产名称	部门	资产类型	邮箱	电话
省级管理员	智能连接研发中心	146	智能连接研发中心	服务器/Unix&linux/Linux系列	1@qq.com	15003114032

< 收缩 × 关闭 处理

点击查看，弹出被归并告警的详情信息。



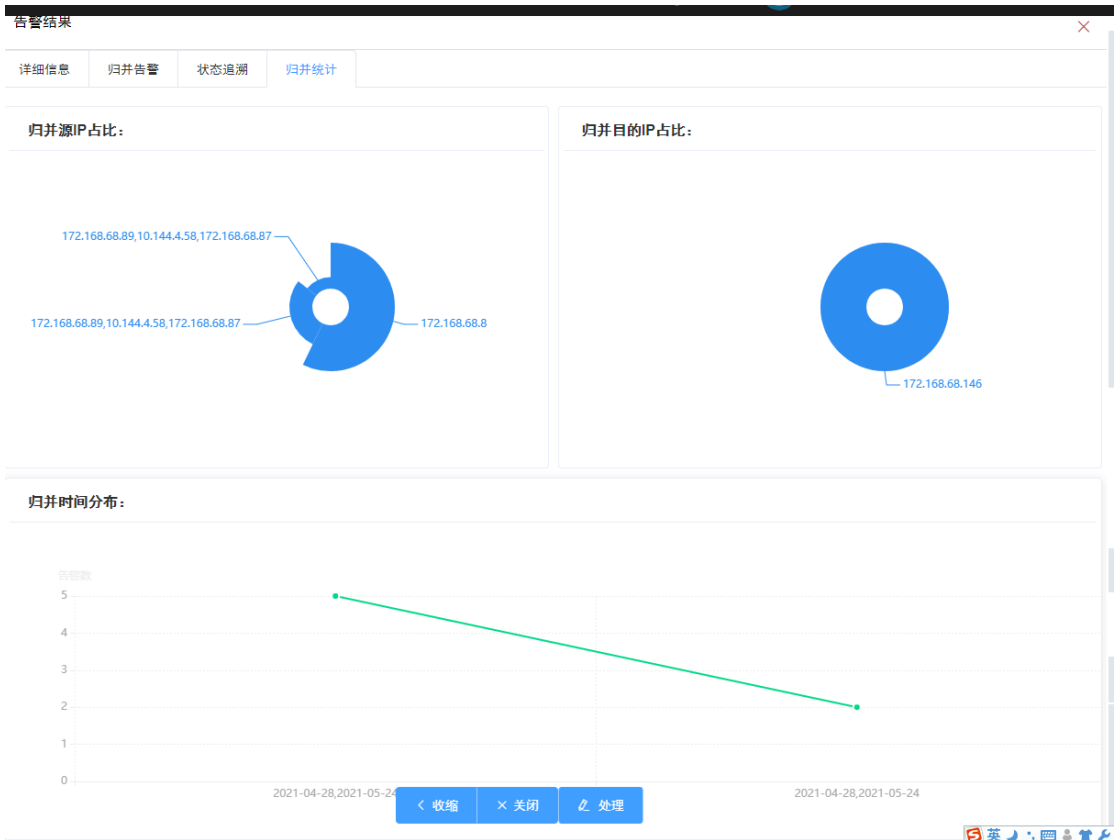
点击事件信息查看按钮，弹出事件详情信息。



状态追溯，记录告警数据状态变更历史。

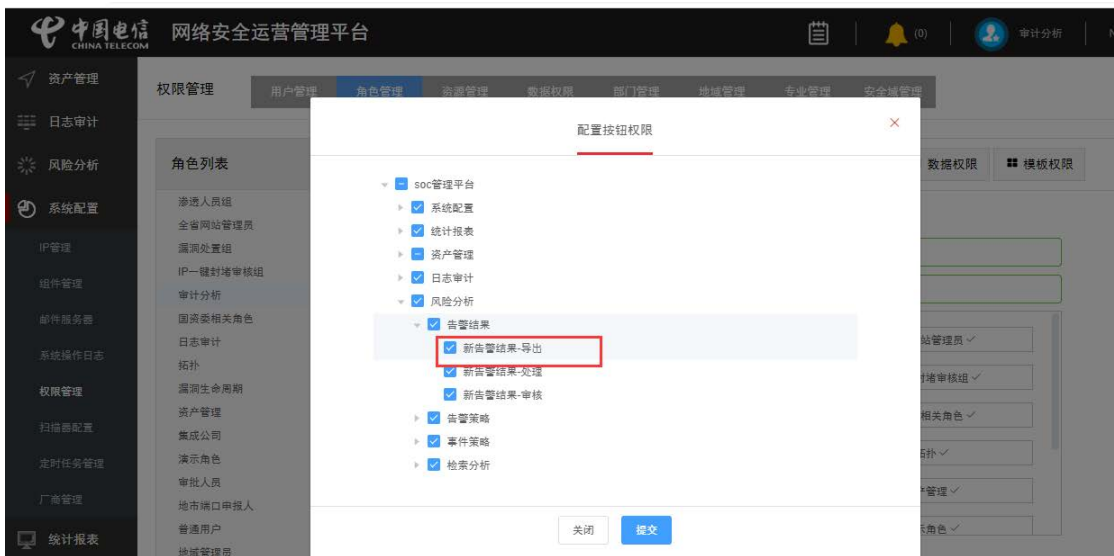


归并统计，以归并源 ip、归并目的 ip 维度统计。

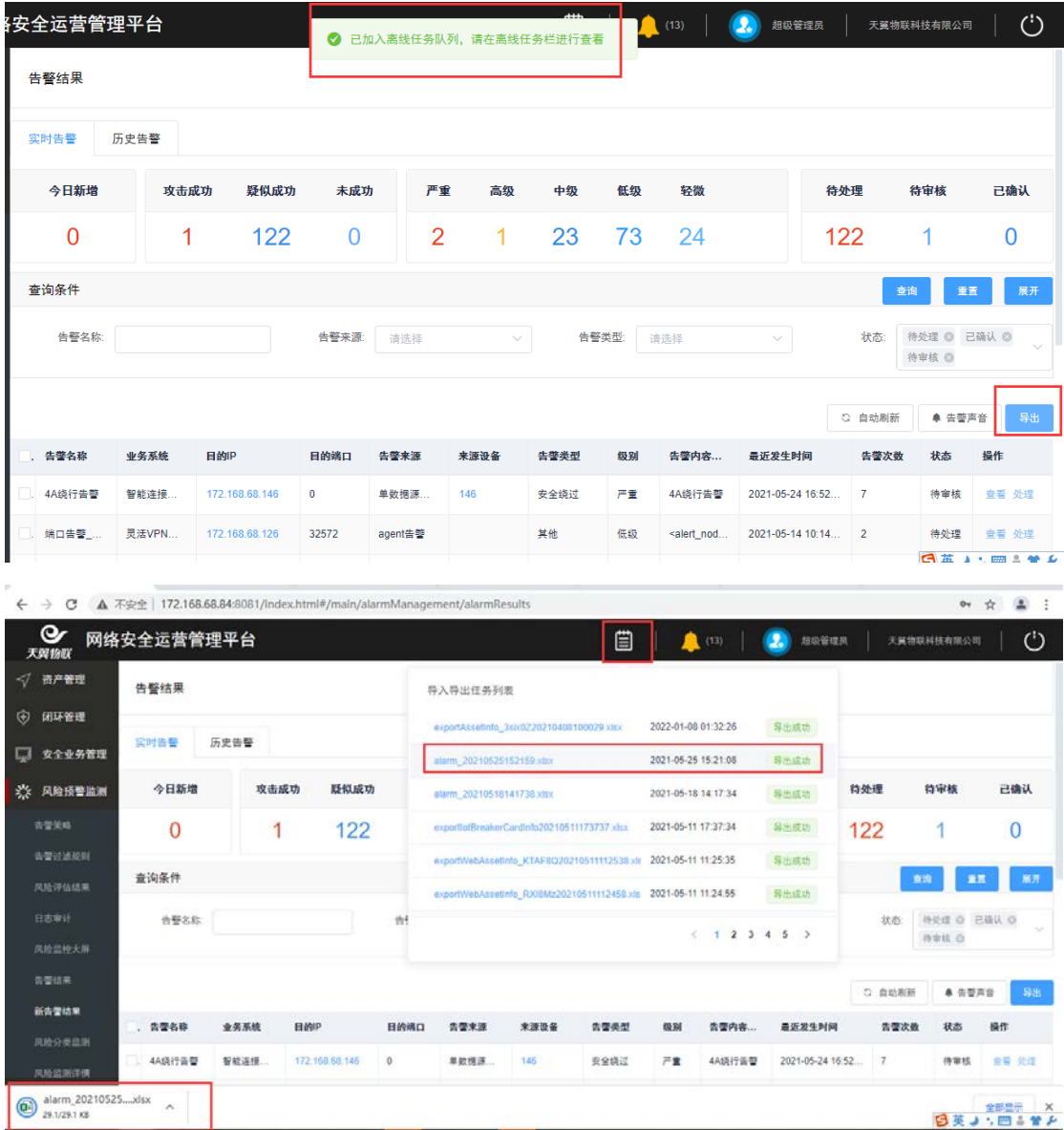


2.8.5.4 告警结果导出

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。

今日新增	攻击成功	疑似成功	未成功	严重	高级	中级	低级	轻微	待处理	待审核	已确认
0	1	122	0	2	1	23	73	24	122	1	0

告警名称	业务系统	目的IP	目的端口	告警来源	来源设备	告警类型	级别	告警内容...	最近发生时间	告警次数	状态	操作
4A绕行告警	智能连接...	172.168.68.146	0	单数据源...	146	安全绕过	严重	4A绕行告警	2021-05-24 16:52...	7	待审核	查看 处理
端口告警...	灵活VPN...	172.168.68.126	32572	agent告警		其他	低级	<aler_t_nod...	2021-05-14 10:14...	2	待处理	查看 处理


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。

规则名称	告警等级	告警类型	创建时间	是否启用	操作
测试规则1	轻微	关联告警	2020-08-03 09:48:22	关闭	查看 修改 删除

- 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。

新增✕

规则名称:	<input type="text" value="请输入"/>	规则类型:	<input type="text" value="请选择"/>
是否启用:	<input type="text" value="请选择"/>	告警级别:	<input type="text" value="请选择"/>
告警类型:	<input type="text" value="请选择"/>	操作系统类型:	<input type="text" value="请选择"/>
规则内容:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"><p style="font-size: small; color: #ccc;">多个匹配项请用逗号(,)分隔</p></div> <p style="font-size: x-small; color: #f00; margin-top: 5px;">多个匹配项请用逗号(,)分隔</p>		

当规则类型为“异常端口”或“新增端口”时，端口类型可选“TCP、UDP”。

修改✕

规则名称:	<input type="text" value="请输入"/>	规则类型:	<input type="text" value="新增端口"/>
是否启用:	<input type="text" value="请选择"/>	告警级别:	<input type="text" value="请选择"/>
告警类型:	<input type="text" value="请选择"/>	操作系统类型:	<input type="text" value="请选择"/>
规则内容:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;"><p>111</p></div> <p style="font-size: x-small; color: #f00; margin-top: 5px;">多个匹配项请用逗号(,)分隔</p>		

当所有数据读不填写时，点击“提交”按钮，提示：

✘ 不能都为空

关联规则白名单

新增 ✘

规则名称： <input type="text" value="请输入"/>	规则类型： <input type="text" value="请选择"/>
是否启用： <input type="text" value="请选择"/>	告警级别： <input type="text" value="请选择"/>
告警类型： <input type="text" value="请选择"/>	操作系统类型： <input type="text" value="请选择"/>
* 规则内容： <input style="height: 50px;" type="text" value="多个匹配项请用逗号(,)分隔"/>	

多个匹配项请用逗号(,)分隔

- 查看

点击操作栏的“查看”按钮，可查看相关信息。

查看 ✘

规则名称： <input type="text" value="111"/>	规则类型： <input type="text" value="异常进程"/>
是否启用： <input type="text" value="关闭"/>	告警级别： <input type="text" value="轻微"/>
告警类型： <input type="text" value="关联告警"/>	操作系统类型： <input type="text" value="WINDOWS"/>
* 规则内容： <input style="height: 50px;" type="text" value="111"/>	

多个匹配项请用逗号(,)分隔

- 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”。

修改 ×

规则名称: <input style="width: 150px;" type="text" value="111"/>	规则类型: <input style="width: 150px;" type="text" value="异常端口"/>
是否启用: <input style="width: 150px;" type="text" value="关闭"/>	告警级别: <input style="width: 150px;" type="text" value="轻微"/>
告警类型: <input style="width: 150px;" type="text" value="关联告警"/>	操作系统类型: <input style="width: 150px;" type="text" value="WINDOWS"/>
* 规则内容: <div style="border: 1px solid green; padding: 5px; min-height: 50px;">111</div>	* 端口类型: <input style="width: 150px;" type="text" value="TCP"/>

多个匹配项请用逗号(,)分隔

- 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。

新增 ×

* 规则名称: <input style="width: 150px;" type="text" value="请选择"/>	* 业务系统: <input style="width: 150px;" type="text" value="请选择或输入关键词搜索"/>
--	--

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。

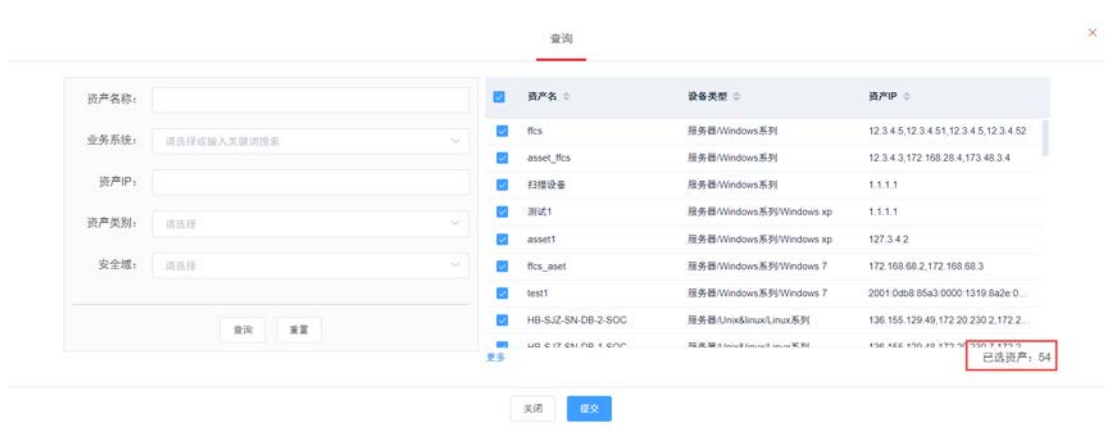
规则名称自动关联规则配置界面的基础规则，资产数据按当前登录用户资产数据权限过滤。

新增
×

* 规则名称:

* 选择资产:

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。



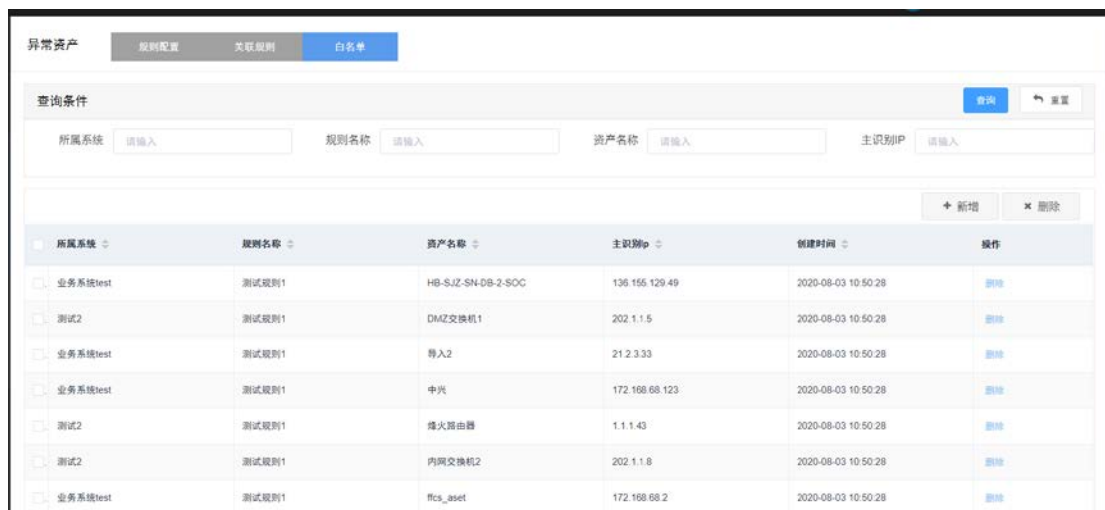
若选择多 50 条资产，则对应新增 50 条白名单。

- 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

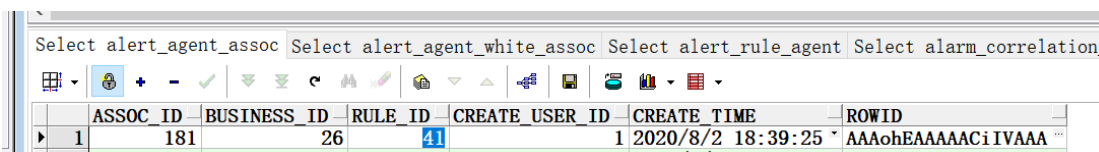
进入“风险分析”=>“告警结果”界面，可查看异常资产告警结果。



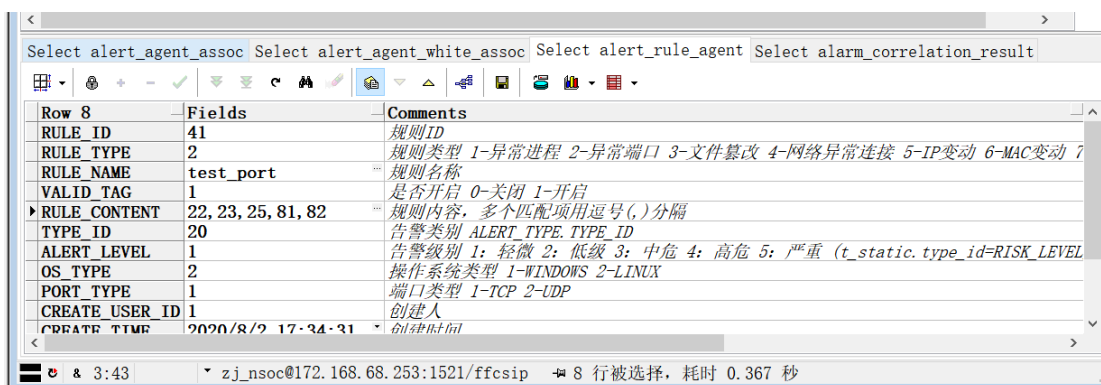
2.8.6.5 后端告警逻辑：

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_TYF
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：

数据查询

查询条件 🔍 查询 ↶ 重置

关键字:

📄 导出 🔄 同步

暂无数据

共 0 条 < > 前往 1 页

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：

采集对象监控

查询条件 🔍 查询 ↶ 重置

采集对象: IP地址: 所属部门: 业务系统:

IP地址	采集对象名	所属业务系统	最近接收日志时间	日志数	部门
43.23.4.5	asset_shouye3	ws业务系统			信息安全部门
43.23.4.5	asset_shouye3	ws业务系统			信息安全部门
31.4.5.63	asset—导入test2	ws业务系统			信息安全部门
3.4.5.63	asset—导入test2	ws业务系统			信息安全部门
3.4.5.63	asset—导入test2	ws业务系统			信息安全部门
3.4.5.63	asset—导入test2	ws业务系统			信息安全部门
3.4.5.63	asset—导入test2	ws业务系统			信息安全部门
3.4.5.63	asset—导入test2	ws业务系统			信息安全部门
3.4.5.63	asset—导入test2	ws业务系统			信息安全部门
3.4.5.63	asset—导入test2	ws业务系统			信息安全部门