安恒信息
DAS-security 安全中国

安恒 AICSO 网络防御运营管理平台

V2.32

用户使用手册

文档版本：2.32

发布日期：2022-03-29

文档说明

产品名称		AiCSO 网络防御运营管理平台	
适用平台/版本		V2.32.0 软件版本	
拟制人	AH9997（安全运营部-杭州安全运营部）	**评审组**	AH9997（安全运营部-杭州安全运营部）
发布人	AH9997（安全运营部-杭州安全运营部）	**备注**	受控文档

修订记录

日期	修订版本	修改记录	修改人
2022-01-18	2.28	初次发布	AH9997（安全运营部-杭州安全运营部）
2022-02-14	2.28	扫描类工作流新增定时功能；原更改责任人改为更改处理人；渗透类、通告类流程新增资产责任人筛选	AH9997（安全运营部-杭州安全运营部）
2022-02-23	2.29	版本更新	AH9997（安全运营部-杭州安全运营

			部)
2022-03-07	2.30	工作流新增资产退网和资产变更优化业务准入工作流	AH9997（安全运营部-杭州安全运营部)
2022-03-14	2.31	启动台一级菜单文字修改；工作流新增资产风险自查工作流	AH9997（安全运营部-杭州安全运营部)
2022-03-29	2.32	开启管理员和 opdmin 对工作流的编辑权限	AH9997（安全运营部-杭州安全运营部

目 录

1 产品概述 1

2 WEB 概述 2

2.1 功能简介 2

2.2 WEB 登录 2

2.3 退出 WEB 登录 3

2.4 WEB 页面布局 3

3 AICSO 网络防御运营管理平台 5

3.1 权限控制 5

3.1.1 superadmin 5

3.1.2 useradmin 5

3.1.3 opadmin 6

3.1.4 generaluser 6

3.1.5 auditadmin 7

3.2 账户详情 7

3.2.1 修改账户详情 8

3.2.2 修改密码 9

3.3 设置 9

3.4 身份认证管理 10

3.4.1 角色管理 10

3.4.2 用户管理 11

3.4.3 跳转链接配置 15

3.5 编辑工作流 18

3.5.1 工作流列表 18

3.5.2 新建工作流 18

3.5.3 编辑工作流 19

3.5.4 删除工作流 19

3.6 配置启动台 20

3.6.1 功能简介 20

3.6.2 新增子平台 20

3.6.3 编辑子平台 21

3.6.4 删除子平台 22

3.6.5 新增彩虹标签 22

3.7 配置管理 23

3.8 角色管理 24

3.9 审计日志 24

3.10 授权信息 25

3.11 待办任务 25

4 工作流 28

4.1 扫描类工作流 28

4.1.1 新增扫描任务 28

4.1.2 解析方式确认 28

4.1.3 资产确认 33

4.1.4 责任人处置 34

4.1.5 项目经理评审 35

4.1.6 结果查看 36

4.2 渗透类流程 37

4.2.1 添加计划 37

4.2.2 选择资产 38

4.2.3 导入漏洞 38

4.2.4 资产确定 39

4.2.5 责任人处置 40

4.2.6 项目经理评审 40

4.2.7 结果查看 41

4.3 通告类流程 42

4.3.1 添加计划 42

4.3.2 选择资产 43

4.3.3 上传外部文件 43

4.3.4 责任人指定 44

4.3.5 责任人处置 44

4.4 云 EDR 告警工作流 45

4.5 港中旅工作流 49

4.5.1 敏感信息发现与排查 49

4.5.2 互联网资产发现与管理 52

4.5.3 钓鱼邮件测试 54

4.5.4 安全应急演练 56

4.5.5 玄武盾监测告警分析与处置 58

4.6 安全运维工作流 59

4.6.1 安全设备及平台巡检 59

4.6.2 安全设备及平台维护记录 61

4.6.3 安全设备及平台策略调优 62
4.6.4 安全设备基础信息收集 63
4.6.5 安全设备及平台故障报告 64
4.6.6 安全工作报备 65
4.7 周期计划 69
4.7.1 安全告警监控数据录入工作流 69
4.8 情报转事件工作流 70
4.8.1 AiLPHA 告警转事件 74
4.8.2 EDR 告警转事件工作流 75
4.8.3 新系统上线评估 76
4.9 安全服务工作流 84
4.9.1 渗透测试服务 84
4.9.2 WEB 漏洞扫描服务 85
4.9.3 主机漏洞扫描服务 86
4.9.4 基线核查扫描服务 87
4.9.5 弱口令扫描服务 88
4.9.6 新系统上线安全评估服务 89

4.10 运营成熟度工作流 90
4.10.1 运营雷达评估 91
4.10.2 运营风险趋势 92
4.11 资产管理工作流 93
4.11.1 资产业务准入 93
4.11.2 资产变更报备工作流 98
4.11.3 资产退网工作流 104

1 产品概述

AICSO 网络防御运营管理平台是一款为政企单位、行业用户提供安全服务运营分析与协作管理服务的产品，用户可以在平台上进行身份认证管理、配置工作流、配置启动台、配置管理等操作，通过该平台直接免登陆跳转到各个模块。

2 WEB 概述

2.1 功能简介

用户可以通过 Web 界面对 AICSO 网络防御运营管理平台进行配置和维护。

2.2 WEB 登录

以 Google Chrome 浏览器为例，在浏览器中输入 https://aicso.dbappsecurity.com.cn/网络防御运营管理平台链接，进入登录窗口。

平台支持钉钉扫描二维码登录，也可以输入手机号获取验证码登录。在扫码登录页点击右上角电脑图标按钮，输入手机号和验证码后获取短信验证码输入，点击<登录>后，进入网络防御运营管理平台。

2.3 退出 WEB 登录

在 OS 启动页面右上角，单击用户，点击<退出>，退出 WEB 登录。

2.4 WEB 页面布局

WEB 页面布局共分为：顶部彩虹导航栏，核心功能区，设置和待办任务。

核心功能为安全防护、暴露面检测、数字驾驶舱、运营管理、威胁狩猎、应急响应。


AiCSO 安全运营防御管理平台


AiCSO 安全运营防御管理平台

3 AICSO 网络防御运营管理平台

安全运营平台 OS 启动页可以配置相关的平台链接，点击跳转到相应的平台。

3.1 权限控制

平台设置 superadmin、useradmin、opadmin、auditadmin、generaluser 一共 5 种角色，可以根据需要在“角色管理”里对上述 5 种角色进行再修改。

3.1.1 superadmin

Superadmin（超级管理）拥有所有权限，包含身份认证管理、编辑工作流、角色管理、配置启动台、配置管理、审计日志、授权信息等。

3.1.2 useradmin

Useradmin（用户管理）只能管理用户，权限包含身份认证管理、查看工作流、查看授权信息等。

3.1.3 opadmin

Opadmin（运维管理）管理平台运行配置，权限包含编辑工作流、配置启动台、角色管理、配置管理、审计日志和授权信息等。

3.1.4 generaluser

Generaluser（普通用户）只有用户权限，包含查看菜单、查看工作流和查看授权信息。

3.1.5 auditadmin

auditadmin（审计管理员）

3.2 账户详情

在安全运营中心页面的右上角单击<用户>按钮有“账户详情”、“退出登录”的功能， 点击下拉的<

账户详情>按钮，页面跳转至 KEYCLOAK -编辑账户。

3.2.1 修改账户详情

页面跳转至 KEYCLOAK -编辑账户，可进行用户手机号、电子邮箱、姓名等信息的修改，点击<保存>，成功修改。

3.2.2 修改密码

页面跳转至 KEYCLOAK -编辑账户，点击<密码>，可输入新密码和确认密码，点击<保存>，成功修改。

3.3 设置

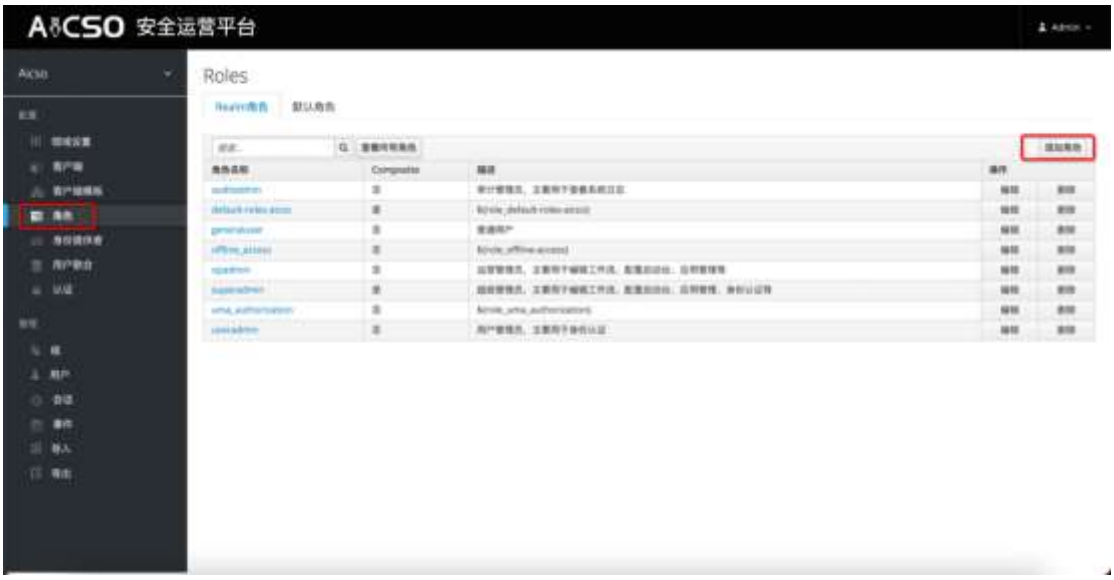
点击右上角<设置>按钮有“身份认证管理”、“编辑工作流”、“配置启动台”、“配置管理”、“授权信息”、“角色管理”的功能，分别可以进入 Keycloak 身份认证管理平台、工作流列表、启动台页面、配置管理页面、授权信息页面、角色管理页面。

3.4 身份认证管理

keycloak 身份认证管理，用来管理系统用户、模块跳转链接配置管理。Superadmin 权限的用户可以直接点击 OS 启动页的“身份认证管理”跳转到 keycloak 管理页面。或者访问 https://ip/auth/admin，使用 admin/Cq9ayCyt50elI@ub 登录

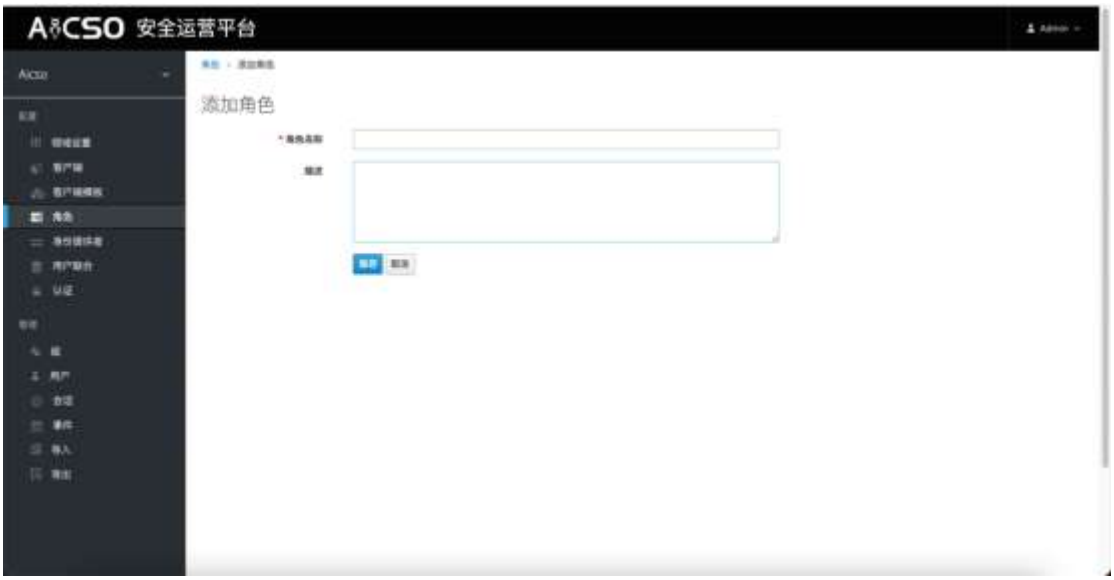
3.4.1 角色管理

登录身份认证管理系统后，点击左侧的<角色>，可以看到当前系统中设置的角色列表。



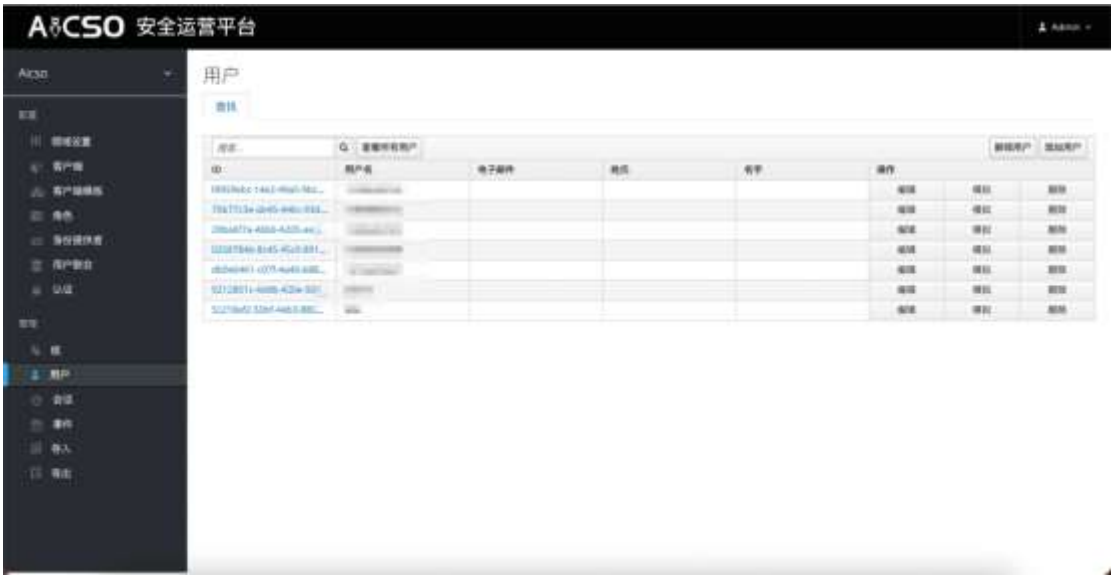
点击添加角色，输入角色名称、描述后，点击<保存>，添加角色成功。

添加角色后，需要登录网络防御运营管理平台后，superadmin 或者 opadminer 登录后，点击右上角的<角色管理>，给该角色设置访问权限。



3.4.2 用户管理

登录身份认证管理系统后，点击左侧的<用户>，可以看到当前系统中设置的用户列表。



3.4.2.1 添加用户

点击右上角<添加用户>，出现以下添加用户页面，在“用户名”处输入手机号，点击<保存>，创建用户成功。

3.4.2.2 用户属性

在属性 tab 页面中输入以下字段信息，添加后点击<保存>。

Key：fullname，value：用户姓名

Key：phone，value：手机号

3.4.2.3 用户凭据

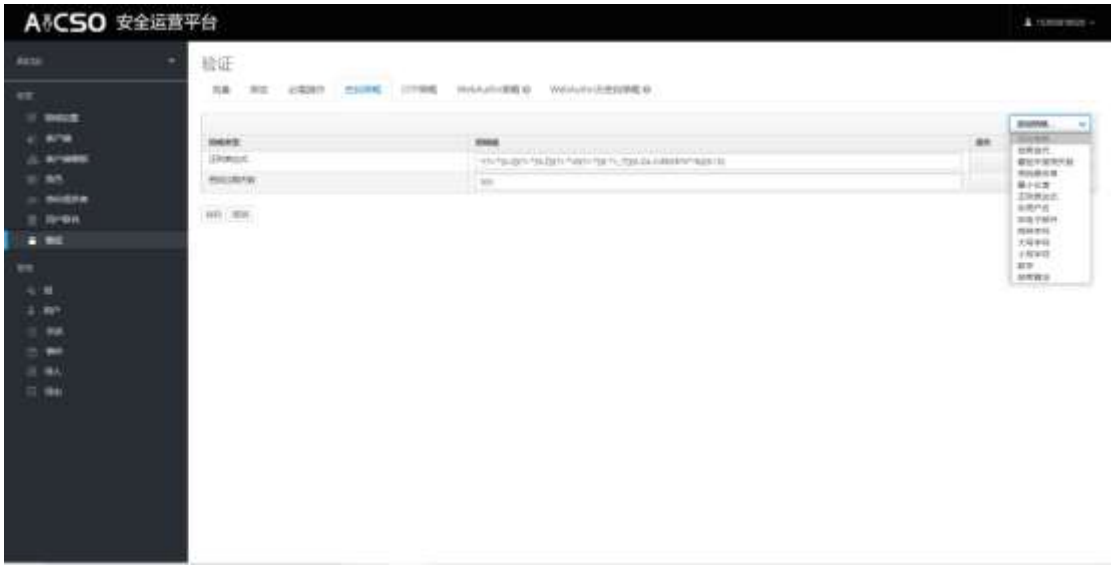
在“凭据”tab 页面设置用户密码。输入“密码”、“密码确认”，点击<设置密码>，用户密码设置成功。

密码限制：8~16 个字符，需包含大小写字母、数字和特殊字符（@.*=_!?）。

3.4.2.4 密码策略

在验证 - 密码策略中，可设置进行密码的限制条件，点击<添加策略>，选定策略后，策略列表内该策略对应消失。

添加策略后，可在“策略值”内设置相应限制条件。点击<保存>，密码策略设置完成。



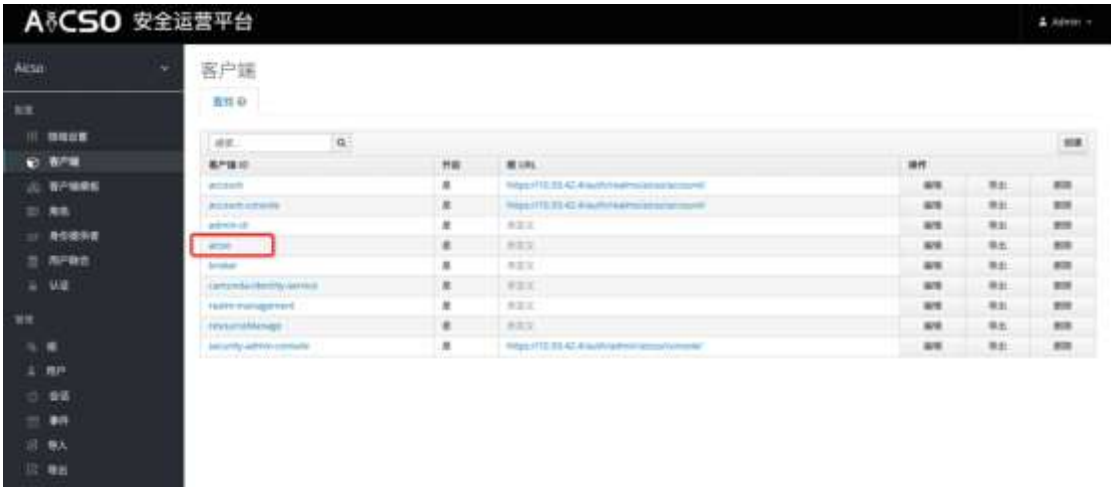
3.4.2.5 角色映射

在“角色映射”页面设置用户所属的权限组。权限控制参考 3.1 权限控制。

在“可用角色”列表选中角色权限，点击<添加选择>；在“分配的角色”列表内选中角色权限，点击<删除所选项>。

3.4.3 跳转链接配置

Aicso–左侧配置中选择“客户端”，选择“aicso”，点击进入。



进入“客户端”用户详情，页面跳转至“设置”tab 页，在“有效的重定向 URI”和“Web 起源”中输入配置的 url 信息。

在正常安装部署情况下：

（1）有效的重定向 URI 需要添加：

- https://{ip}/*
- https://{ip}:5443/*
- https://{ip}:6443/*
- https://{ip}:7443/*
- https://{ip}:40008/*

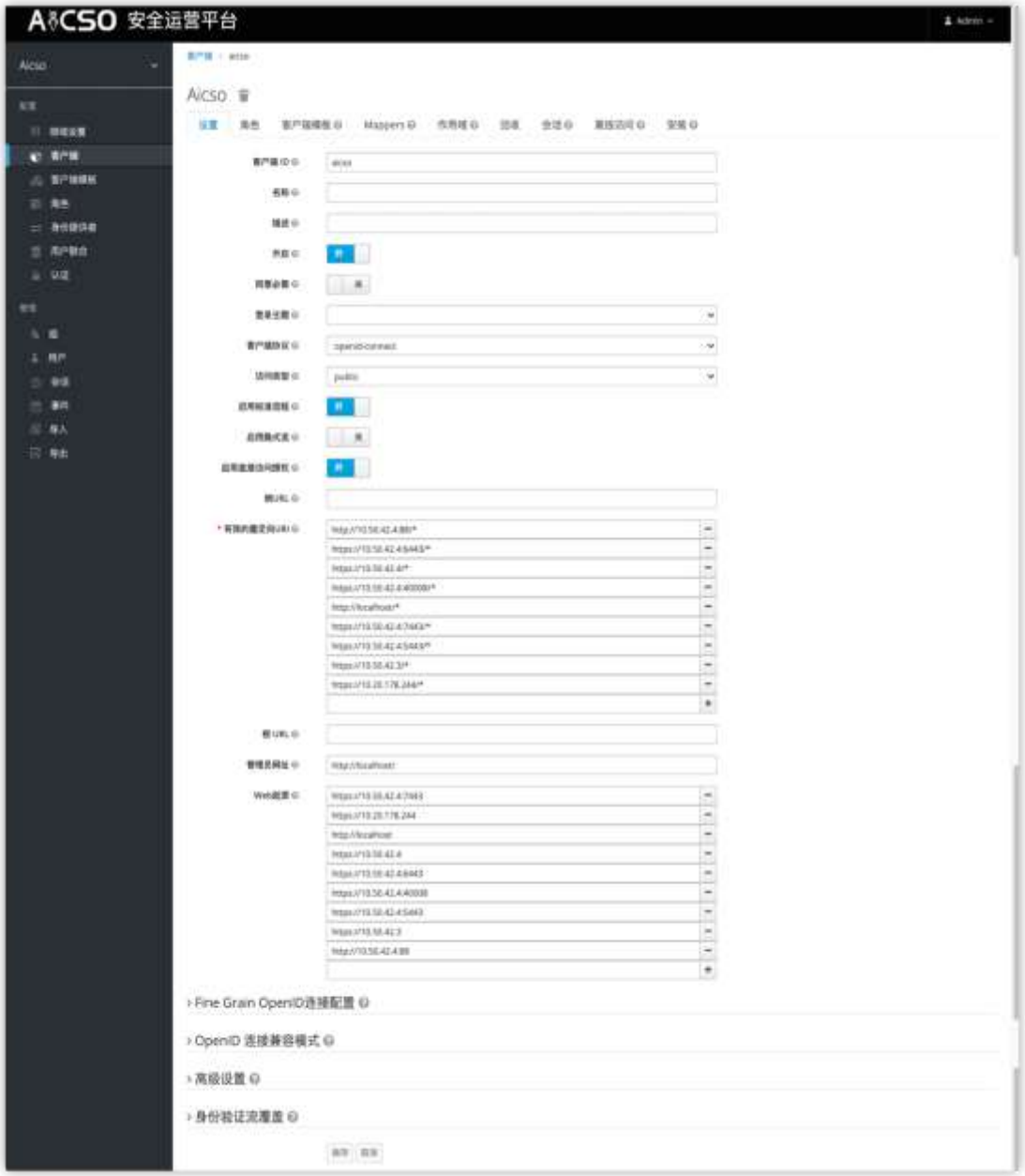
（2）管理员网址需要添加：https://{ip}

（3）Web 起源需要添加：

- https://{ip}
- https://{ip}:5443
- https://{ip}:6443
- https://{ip}:7443
- https://{ip}:40008

（4）其他情况：

- 如果需要添加其他第三方平台，也需要在有效的重定向 URI、Web 起源添加地址：https://{ip}/*
- 有效的重定向 URI：https://{ip}/*
- Web 起源：https://{ip}


AiCSO 安全运营平台
Aicso
Fine Grain OpenID连接配置
OpenID 连接兼容模式
高级设置
身份验证流覆盖

3.5 编辑工作流

3.5.1 工作流列表

工作流列表包括序号、工作流名称、KEY、部署时间和操作列下的查看、编辑、删除。

工作流列表的工作流名称取新建工作流时用户自定义的工作流名称，KEY 取用户导入的.bpmn 文件内的 ID。

3.5.2 新建工作流

点击<新建>，页面跳转至新建工作流。

输入工作流名称，点击<导入>，选择.bpmn 文件上传，点击<确定>。

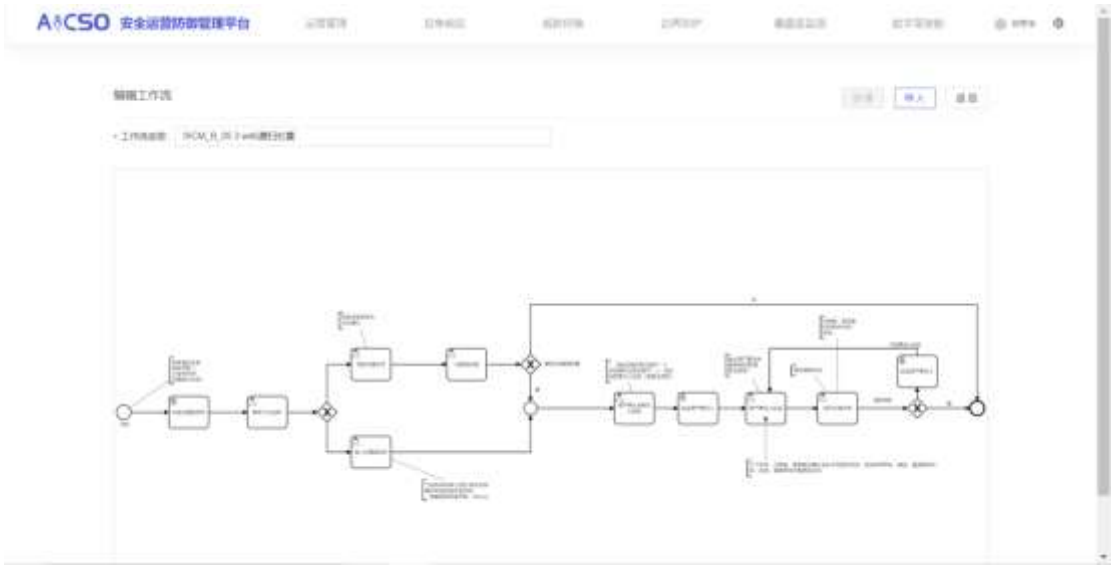
当 KEY 唯一时，点击<部署>，新建工作流成功。

当 KEY 已存在时，点击<部署>，提示失败。

3.5.3 编辑工作流

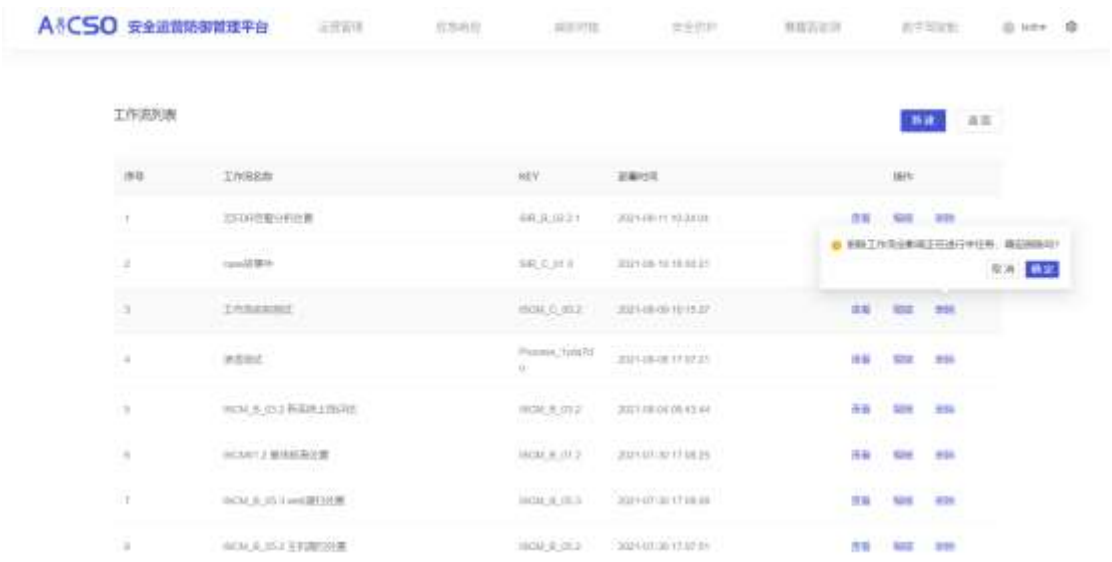
点击<编辑>，页面跳转至编辑工作流。

输入更改工作流名称，点击<导入>，导入更改后的 KEY 相同的工作流文件，点击<部署>，工作流编辑成功。



3.5.4 删除工作流

点击<删除>，二次提示删除工作流会影响进行中的任务，若删除，则任务被挂起。



3.6 配置启动台

3.6.1 功能简介

配置启动台的主要功能是对子平台进行新增、编辑和删除，实现对启动台子平台的自由配置。方便用户根据自己的需求增加平台，利于集中管理。

3.6.2 新增子平台

点击父级模块的名称，上方显示“新增子平台”，输入平台名称和域名地址，选择<是否开启>，默认<新开页面>按钮打开，点击<保存>，新增子平台成功。

上方导航栏新增该子平台，返回启动页，父级模块出现新增的子平台。

3.6.3 编辑子平台

点击子平台的名称，上方显示编辑子平台，显示历史的平台名称和域名地址，根据需求修改平台名称和域名地址，选择是否开启，点击<保存>。

若编辑了名称菜单中该子平台的名称就会改变。上方导航栏该子平台的名称也发生了变化。返回启动页，父级模块下的该子平台的名称也发生变化，若修改了域名，则点击之后跳转的页面也会发生变化。编辑页面如图所示。

3.6.4 删除子平台

点击子平台右侧的<删除>按钮，跳出提示，点击<确定>，菜单中该子平台就会被删除。上方导航栏该子平台也会被删除。返回启动页，父级模块下的该子平台也被删除了。

3.6.5 新增彩虹标签

配置子平台可以添加彩虹团队标签，添加完成后显示在启动台和导航栏的子平台菜单中。

子平台配置完成后，进入 OS 启动台，鼠标移至上方导航栏，会显示彩虹团队的名称，同时下拉框内显示对应的子平台。

3.7 配置管理

配置管理中可以配置 logo、修改平台名称和修改水印。

3.8 角色管理

在角色管理页面，选中角色后，选择右侧的菜单权限，点击<保存>。

通过该设置功能，可以给不同的用户组设置不同的平台访问权限。

3.9 审计日志

可以查看安全运营中心，安全大数据分析模块，资产弱点管理模块的相关日志信息。

安全运营中心根据平台模块分为运营支撑系统、安全事件管理系统、安全服务管理系统、情报威胁运营系统，同时可以按照操作类型、操作人和时间范围对日志进行筛选、查询。

点击<导出全部>，默认导出近 6 个月的日志文件，也可经过筛选后导出结果。

注:取用户名 keycloak 中属性的 fullname;大数据分析模块中 system 命名为系统账号;弱点模块 opadmin 命名为审计账号、openUser 命名为系统账号。

3.10 授权信息

授权信息里可以更新授权证书，新安装平台或者证书到期后需要在此更新网络防御运营管理平台的平台证书。授权后才能正常使用平台功能。superadmin、opadmin 可以对授权信息进行操作。

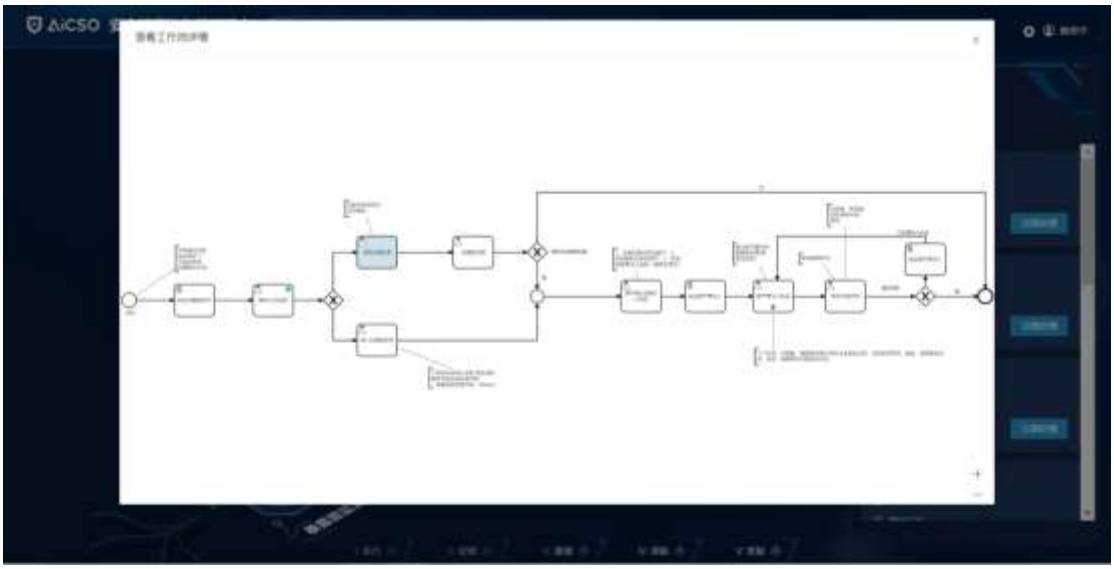
3.11 待办任务

点击右侧<待办任务>按钮，侧抽屉展示代办任务，还可以跳转到平台执行任务。

待办任务列表项可以查看工作流实例的节点数据，包含工作流名称、所属项目名称、任务类型、任务开始时间等。

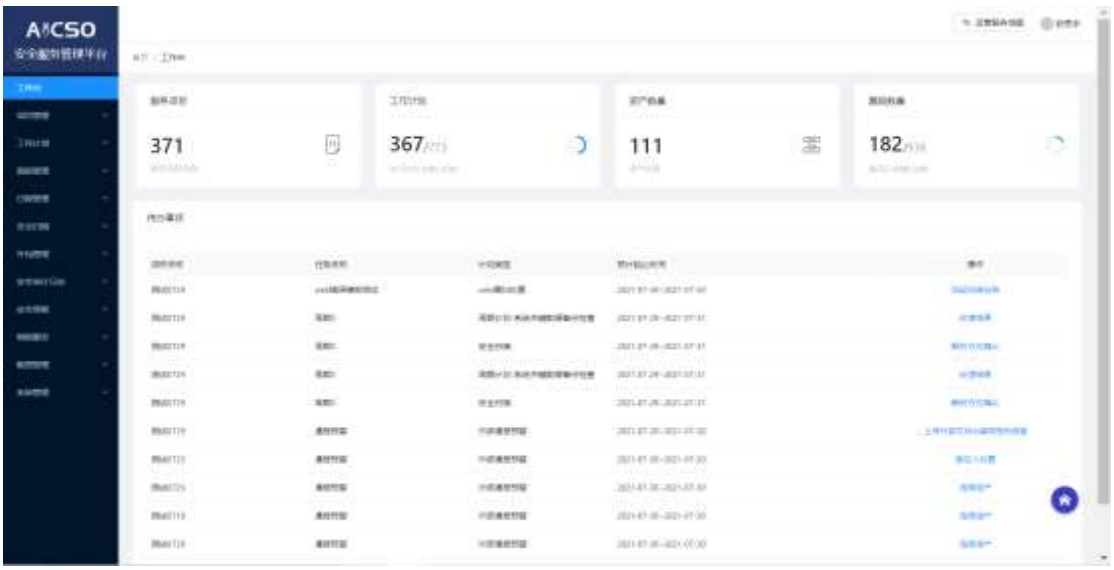
待办列表设置滑动分页，1 页 10 条。

点击<工作流名称>，弹窗展示工作流详情查看页。

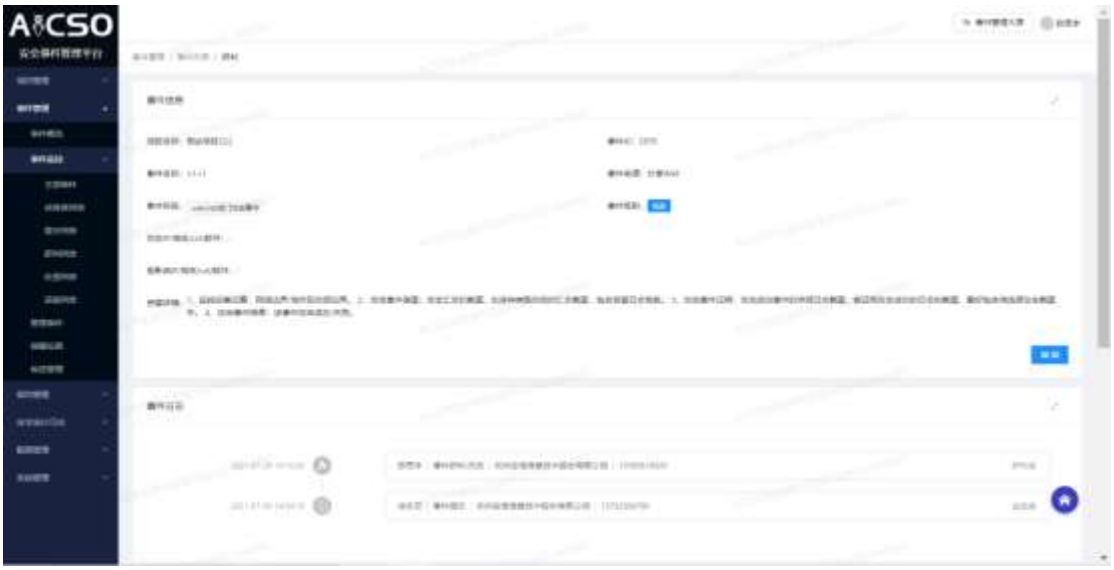


点击<立即处理>按钮：

“安全服务”任务（状态为进行中）跳转至安全服务管理模块 - 工作台；



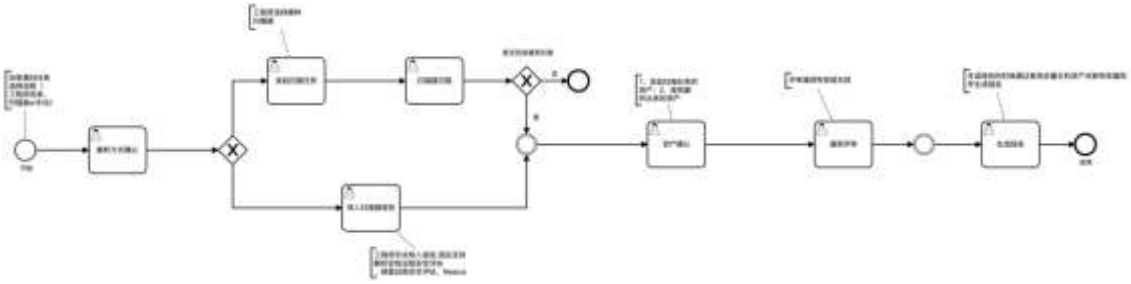
“安全事件”任务跳转至安全事件管理模块 - 事件列表 - 研判 / 处置。



4 工作流

4.1 扫描类工作流

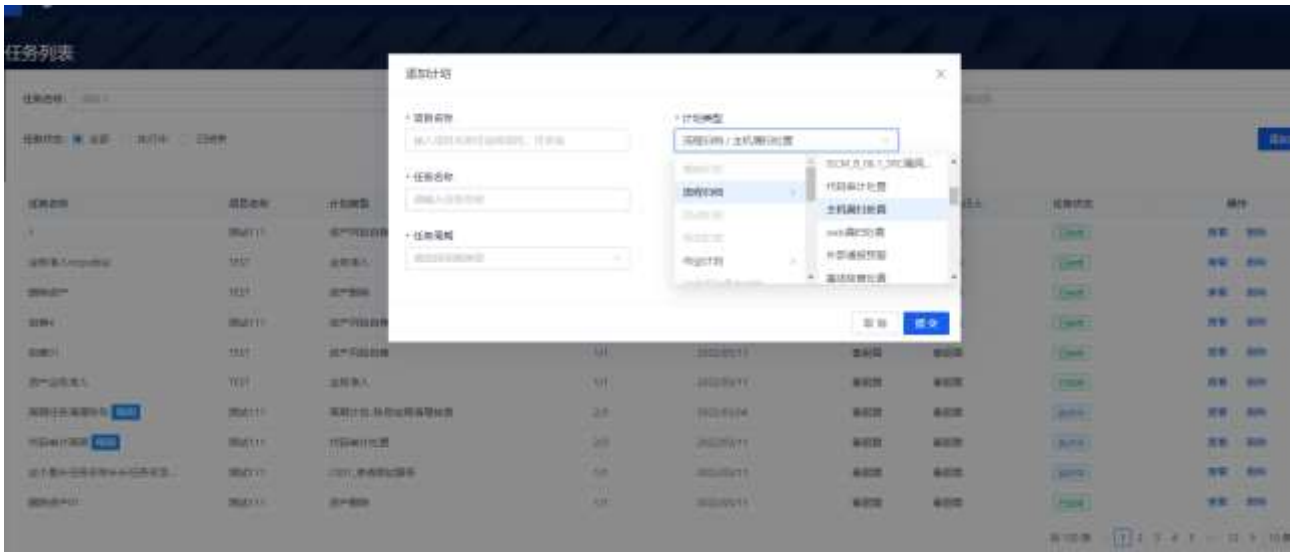
扫描类工作流主要包括主机漏扫、web 漏扫、基线核查。



4.1.1 新增扫描任务

在安全服务管理模块的项目管理中，选择项目进入到项目详情。

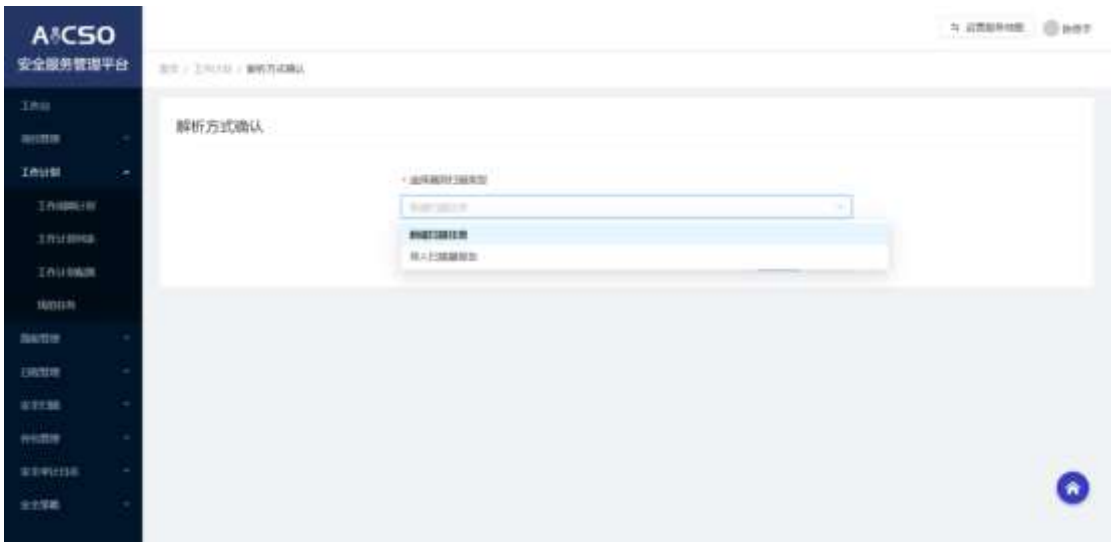
点击<工作计划>，新增“主机漏扫”任务。



4.1.2 解析方式确认

在安全服务管理模块，工作台页面的待办事项中点击<解析方式确认>。

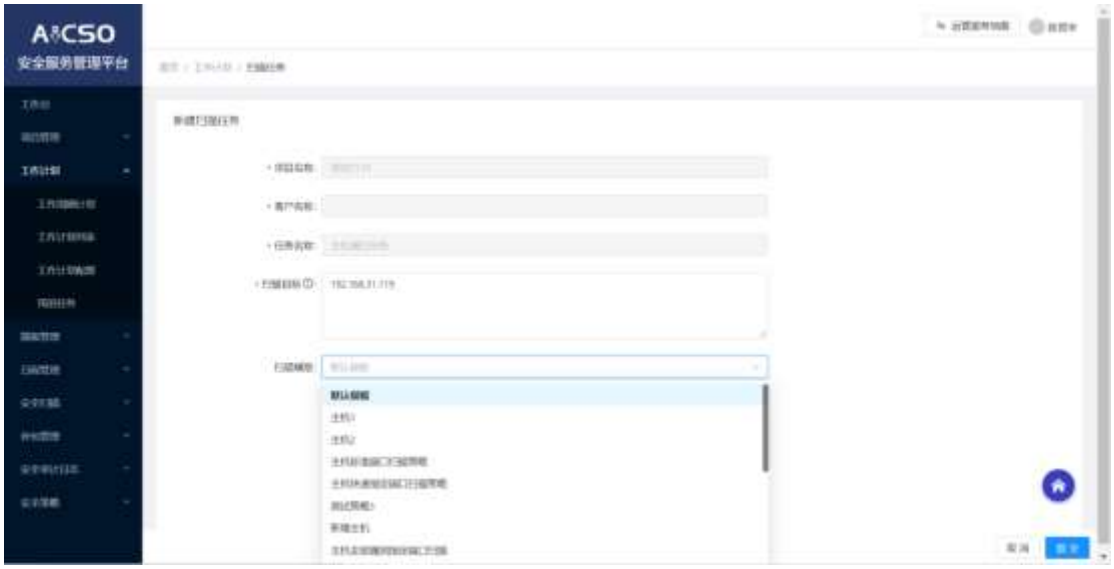
选择漏洞扫描类型时，点击<新建扫描任务>，点击<提交>。



4.1.2.1 发起扫描任务

选择<新建扫描任务>后提交，在待办事项中点击<发起扫描任务>。

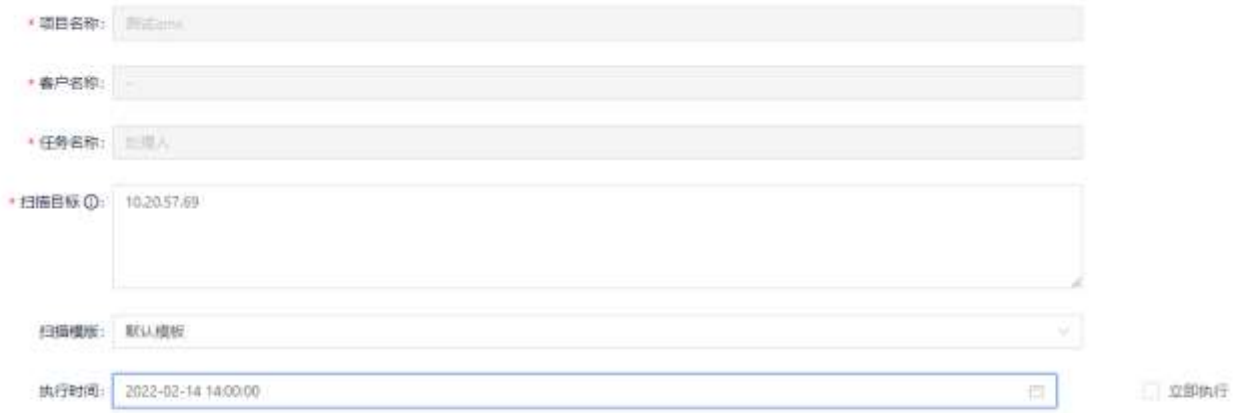
输入扫描目标，选择扫描模板（默认选中“默认模板”），系统开始扫描任务。



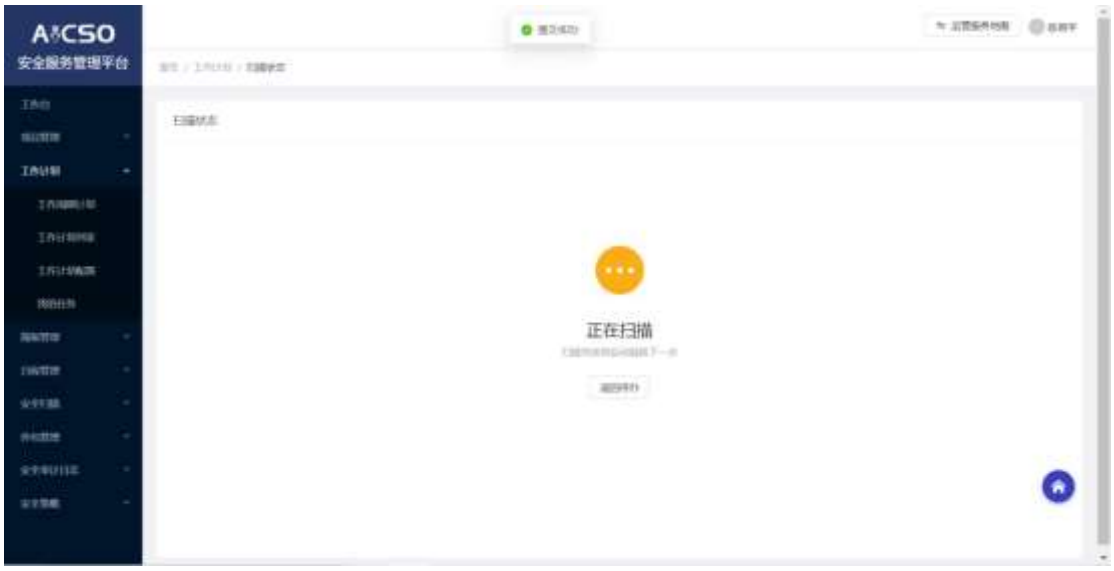
4.1.2.2 定时扫描

在<新建扫描任务>之后，用户可以选择扫描任务发起的时间，如果勾选<立即执行>则该任务将会立即执行；

若选择指定时间，则该任务仍处于扫描状态，可在工作台处查看。

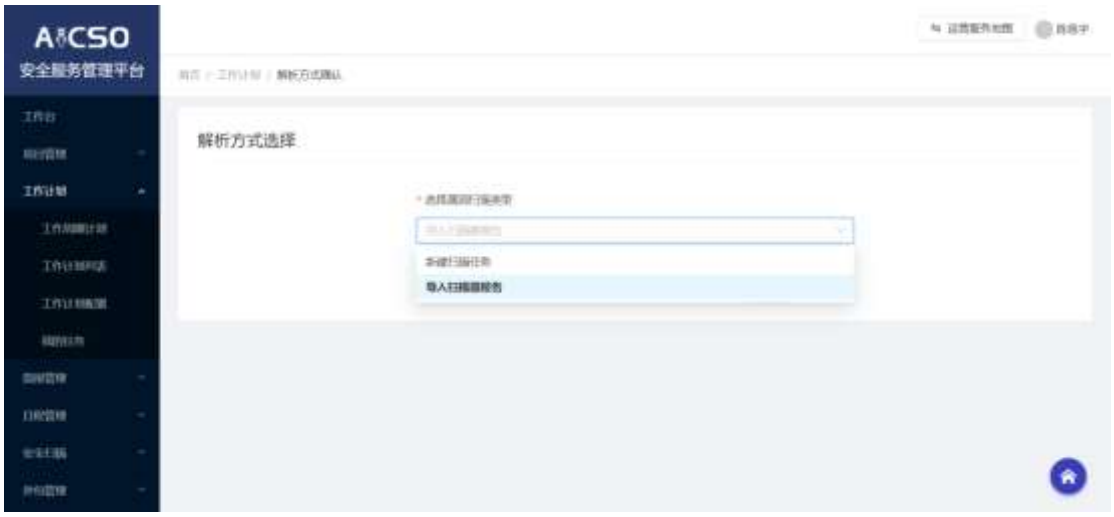


4.1.2.3 扫描器扫描



4.1.2.4 导入扫描器报告

在解析方式确认页面选择<导入扫描器报告>，点击<提交>。



在待办事项中点击<导入扫描器报告>。


待办事项
项目名称
任务名称
计划类型
预计起止时间
操作
测试0728
主机漏扫任务
主机漏扫计划
2021-08-04~2021-08-04
测试0729
主机漏扫任务
主机漏扫计划
2021-08-04~2021-08-04

根据对应文件类型上传对应的扫描报告。

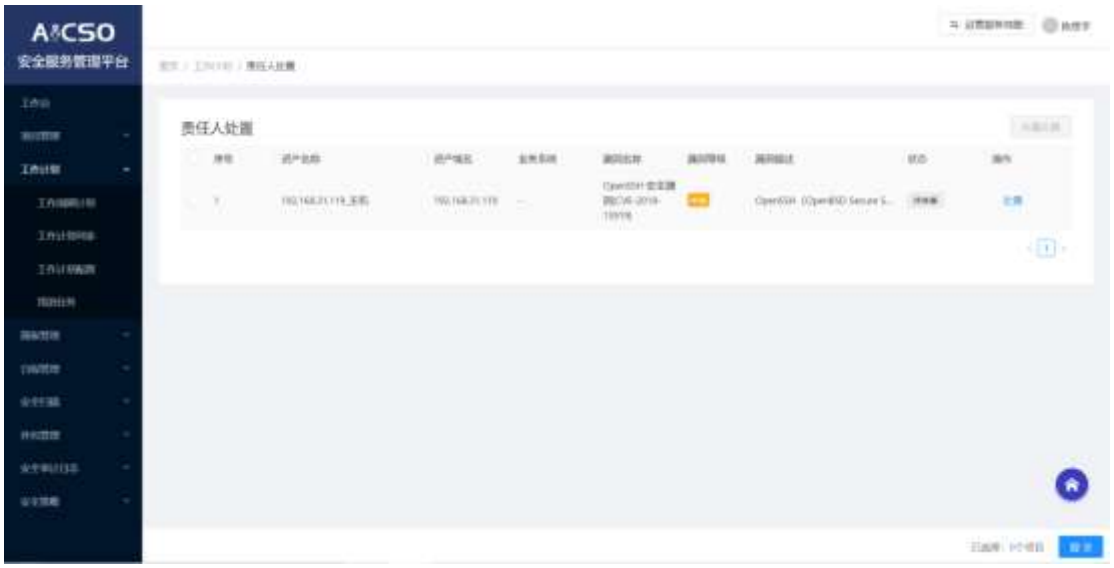
4.1.3 资产确认

点击待办任务中的<资产确认&责任人指定>，跳转页面后，展示该资产所属责任人和漏洞处理人，点击<更改处理人>，选择后点击<确定>。

选中资产，点击<提交>，完成资产确认。

4.1.4 责任人处置

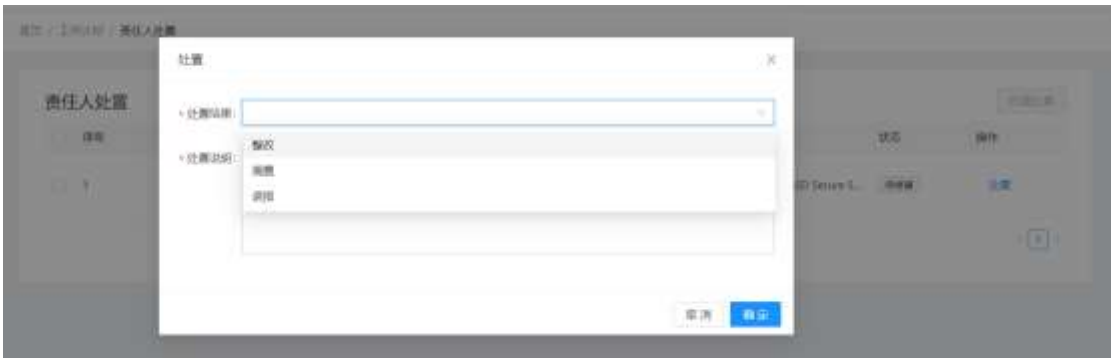
点击代办任务的<责任人处置>，进入责任人处置界面。



点击<处置>，选择处置结果<整改/搁置/误报>：

- 选择“整改”，处置状态变为“待验证”；
- 选择“搁置”或“误报”，处置状态变为“待审批”。

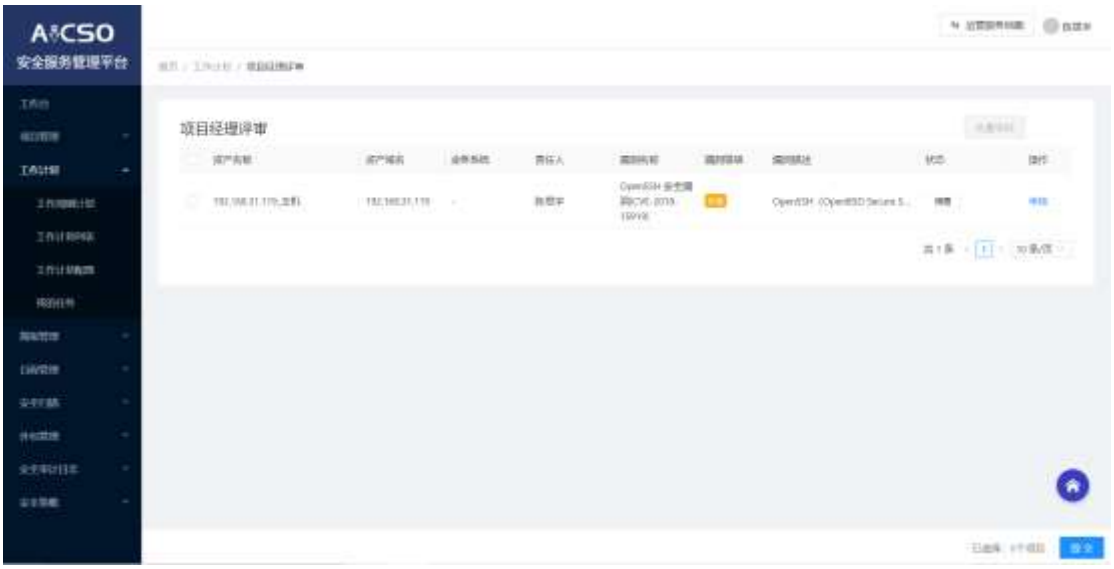
处置说明为必填项，填写的处置说明将会在项目经理评审阶段的已选漏洞列表内展现，填写相应信息后，点击<确定>。



4.1.5 项目经理评审

责任人处置提交后，进入项目经理评审阶段。

- 选择“整改”的漏洞：验证期间状态为“验证中”，验证完成后状态变更为“已修复”或“未修复”，若漏洞仍为“未修复”，则进入漏洞复测流程，回到责任人处置阶段；
- 选择“搁置”或“误报”的漏洞：处置状态变为“搁置”或“误报”。

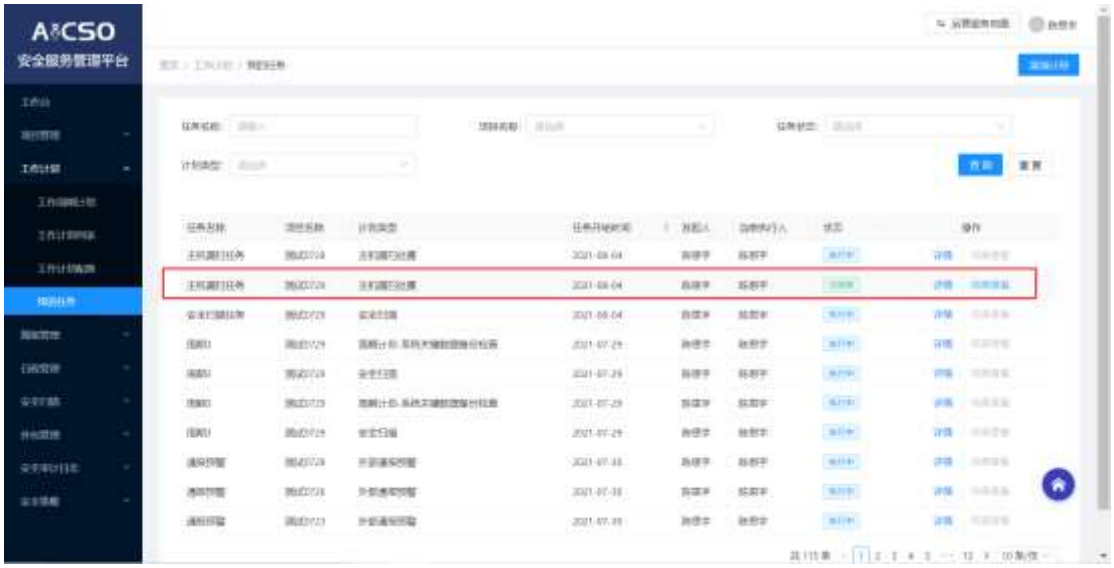


点击<审核>，选择审核结果<通过/不通过>，填写必填项处置说明。

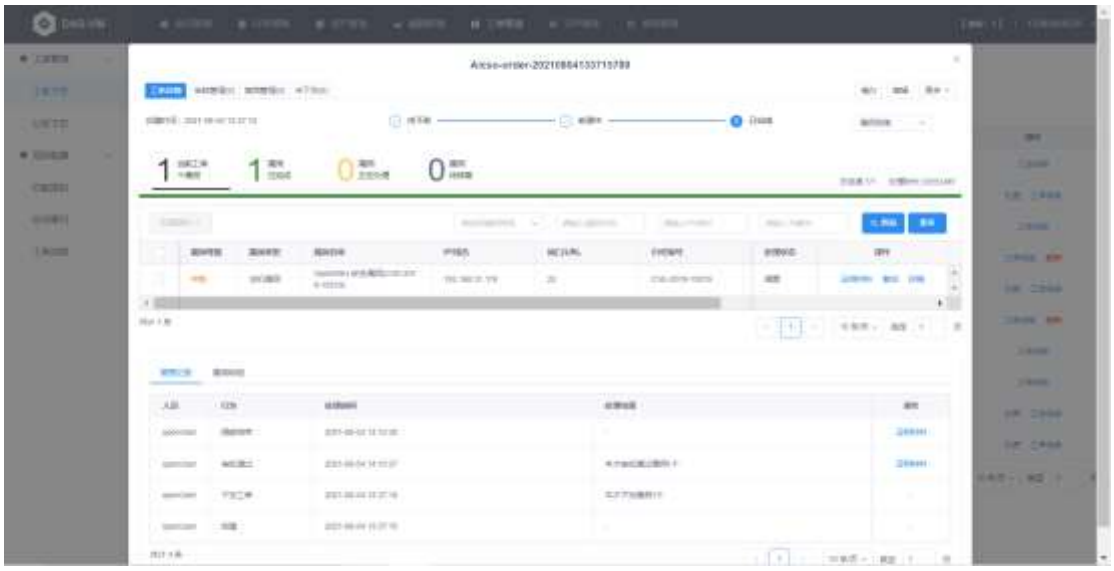
单个审核时，显示该漏洞的详细信息（漏洞名称、漏洞等级、处置结果、处置说明、责任人）；批量审核时，显示被选中的多个漏洞的详细信息。

4.1.6 结果查看

进入工作列表-我的任务，点击<结果查看>。

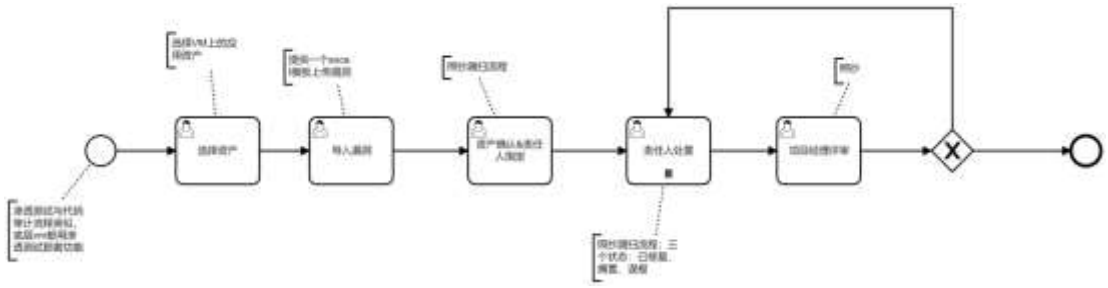


点击<结果查看>，页面跳转至 VM 弱点管理平台-工单管理-该任务的工单详情信息。



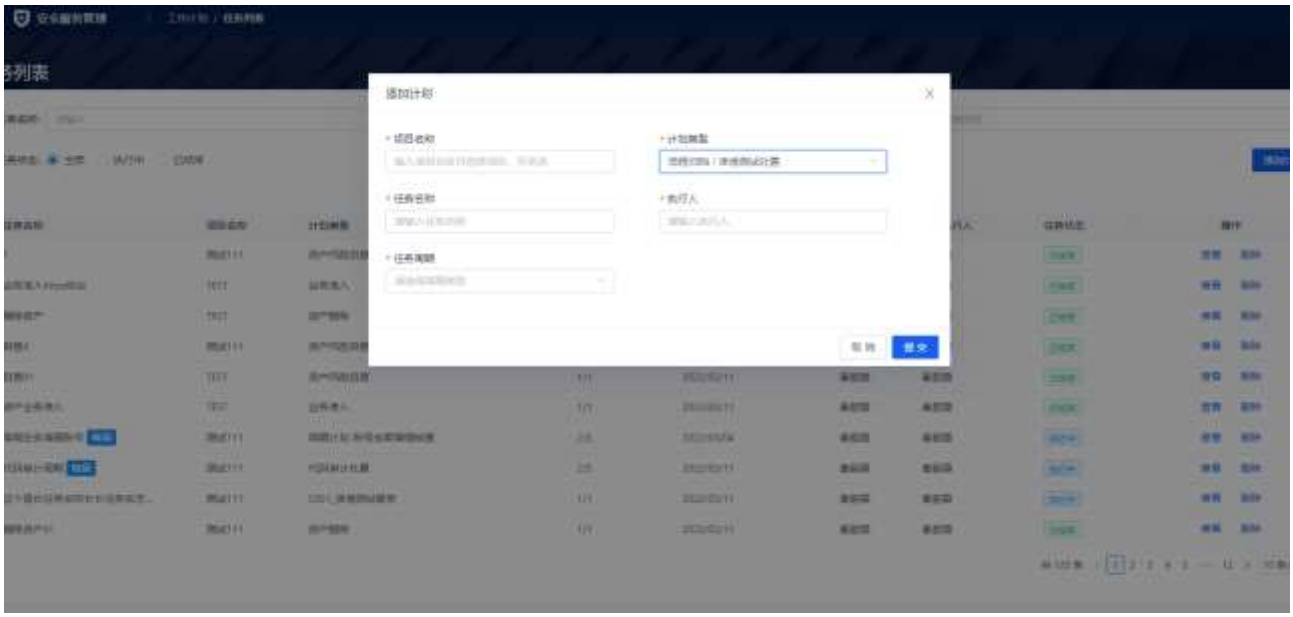
4.2 渗透类流程

渗透类流程包括渗透测试、代码审计。



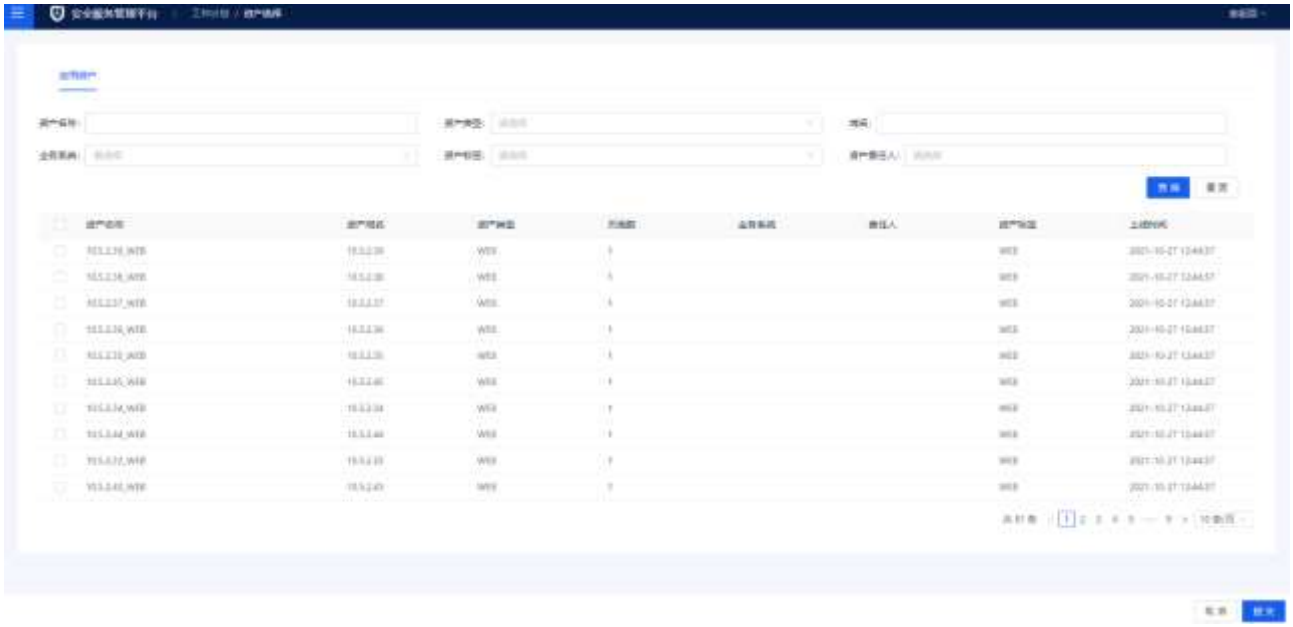
4.2.1 添加计划

选择计划类型为“渗透测试处置”。



4.2.2 选择资产

渗透类流程的资产选择为“应用资产”。可针对资产名称、类型、域名、业务系统、资产标签、资产责任人进行应用资产的筛选、查询操作，选择资产后，点击<提交>。



4.2.3 导入漏洞

漏洞详情涉及资产列表和漏洞列表，点击<导入漏洞>，进行漏洞文件上传，若无模板则点击<下载模

板>后填写上传。

点击<导入>，导入漏洞成功。

点击<导入报告>，导入报告成功。点击<提交>。

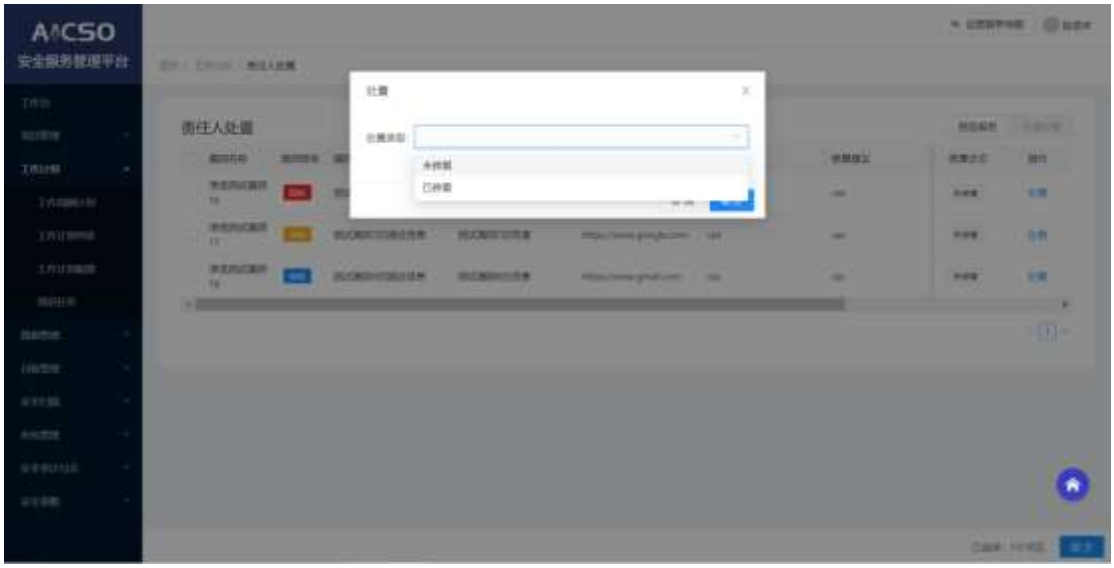
4.2.4 资产确定

点击<更改处理人>，选择后，点击<提交>。

4.2.5 责任人处置

进入责任人处置阶段，点击<处置>，选择处置类型为<已修复/未修复>。

- 选择“已修复”，状态变更为“已修复”；
- 选择“未修复”，状态变更为“未修复”；

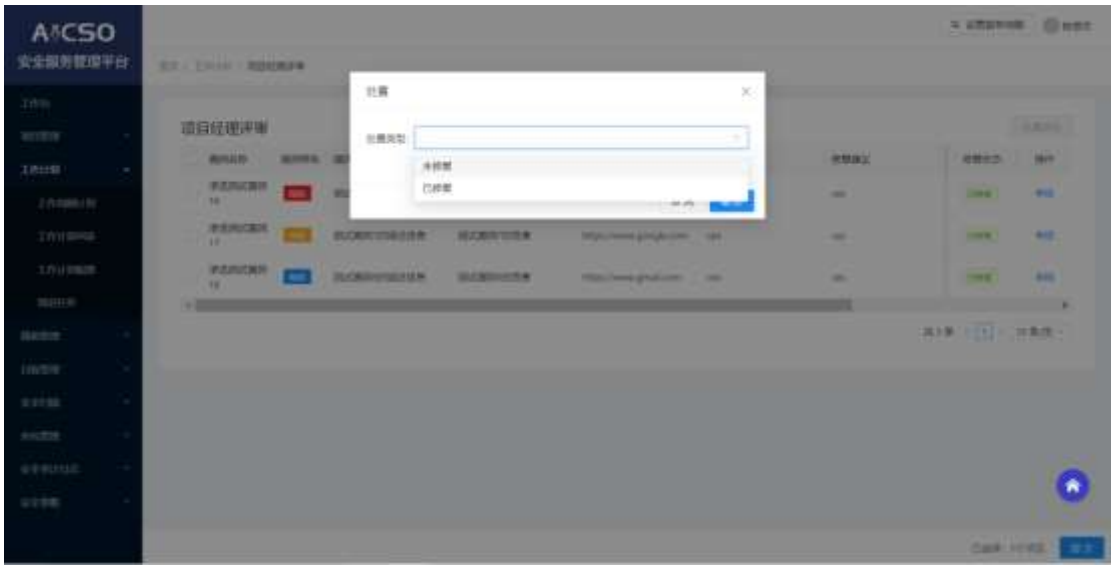


4.2.6 项目经理评审

进入项目经理评审阶段，点击<审核>，选择审核类型<未修复/已修复>

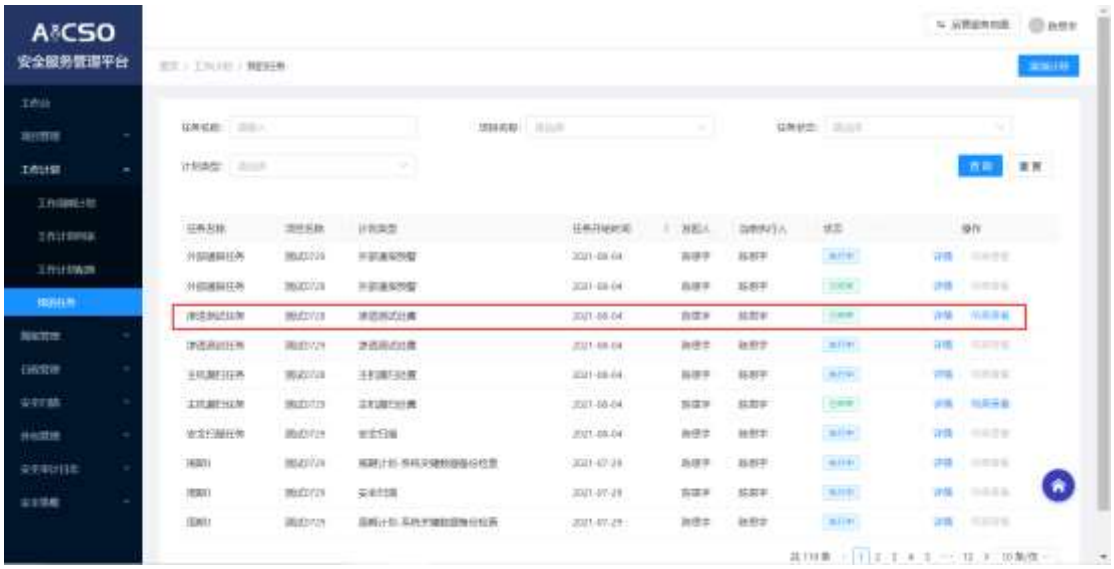
- 选择“已修复”，状态变更为“已修复”；
- 选择“未修复”，状态变更为“未修复”，该阶段若状态为“未修复”，则进入漏洞复测流程，未修

复漏洞重新进入责任人处置阶段。

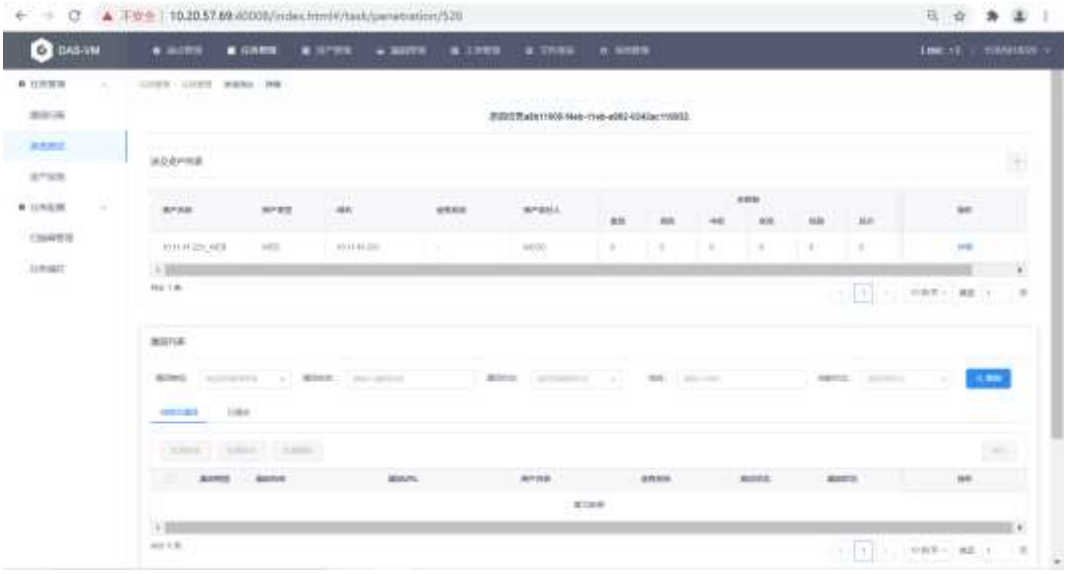


4.2.7 结果查看

流程结束后，进入工作计划-我的任务，点击操作列下的<结果查看>。

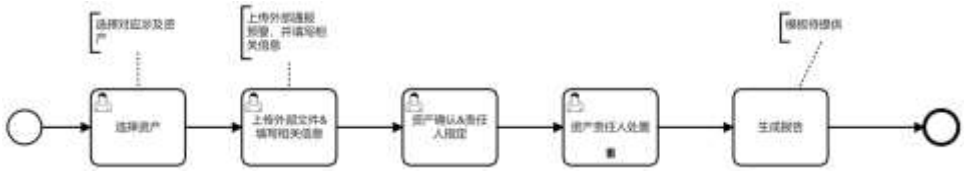


页面跳转至 VM 弱点管理平台的任务管理-渗透测试-任务详情。



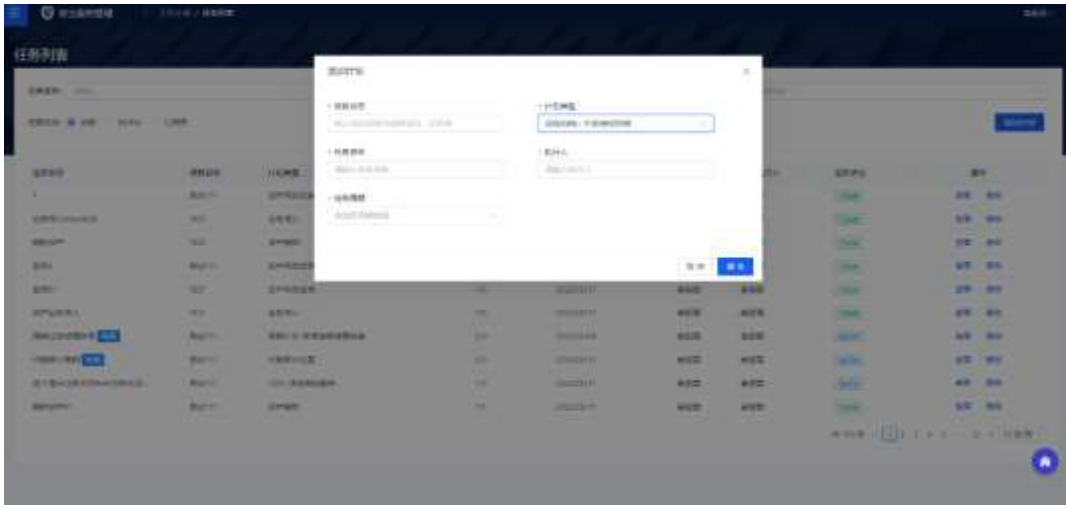
4.3 通告类流程

通报类流程包括外部通报预警。



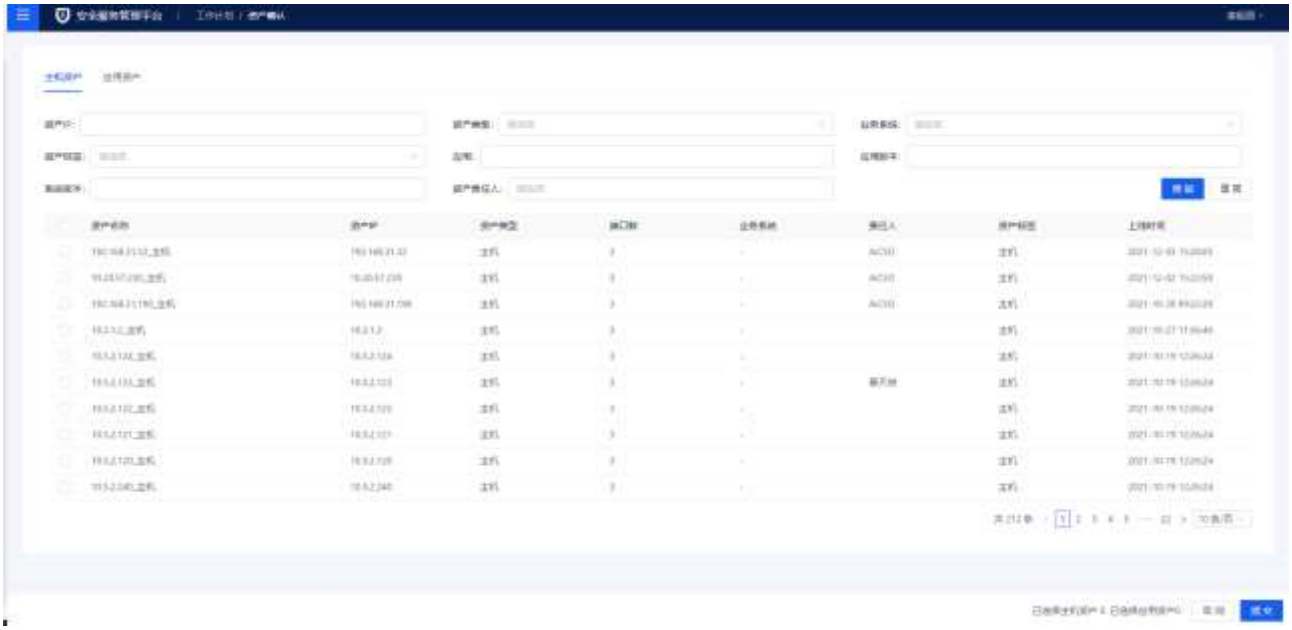
4.3.1 添加计划

选择计划类型为“外部通报预警”。



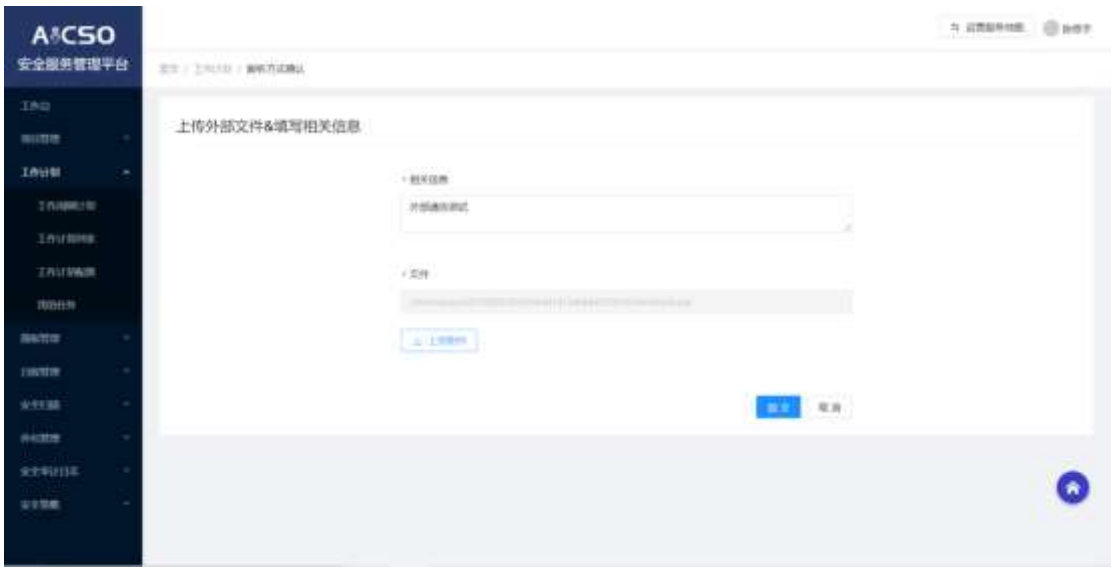
4.3.2 选择资产

外部通报预警的资产选择分为“主机资产”和“应用资产”。可根据资产 IP、类型、标签、业务系统、应用、系统版本、资产责任人等进行主机资产筛选，选择资产后，点击<提交>。



4.3.3 上传外部文件

填写相关信息，并上传附件，点击<提交>。

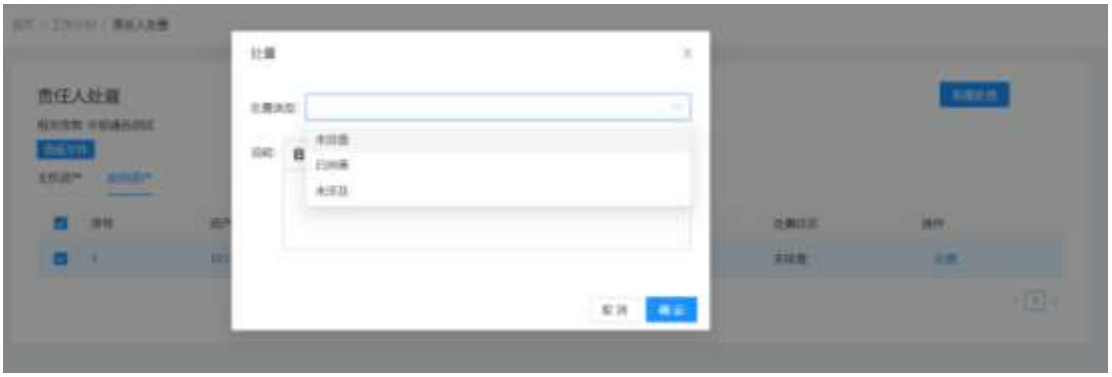


4.3.4 责任人指定

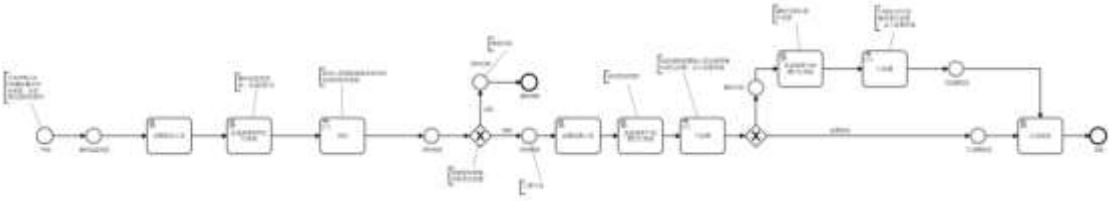
点击<更改处理人>，选择责任人后，选中资产，点击<提交>。

4.3.5 责任人处置

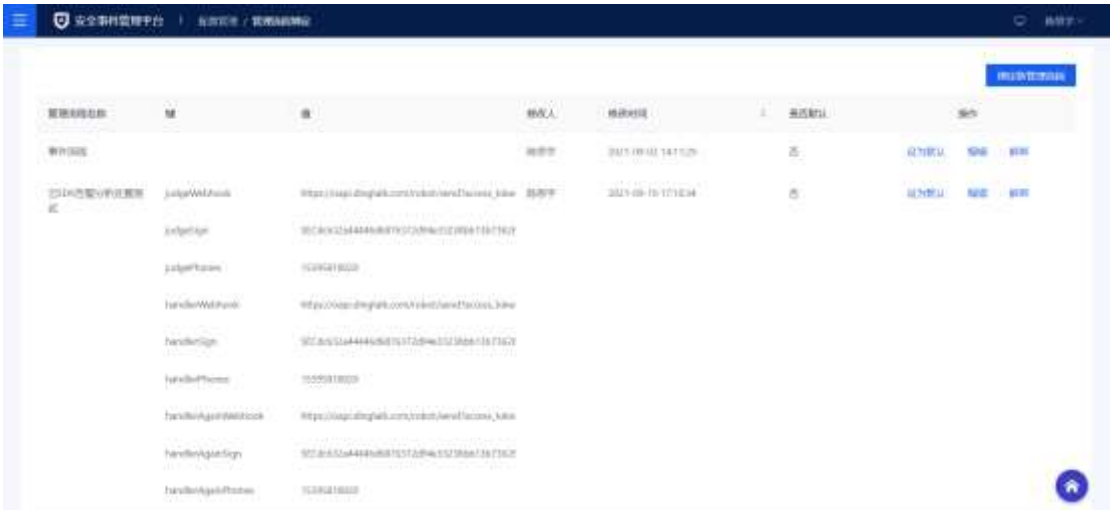
点击<处置>，选择<未排查/已排查/未涉及>，点击<提交>。



4.4 云 EDR 告警工作流

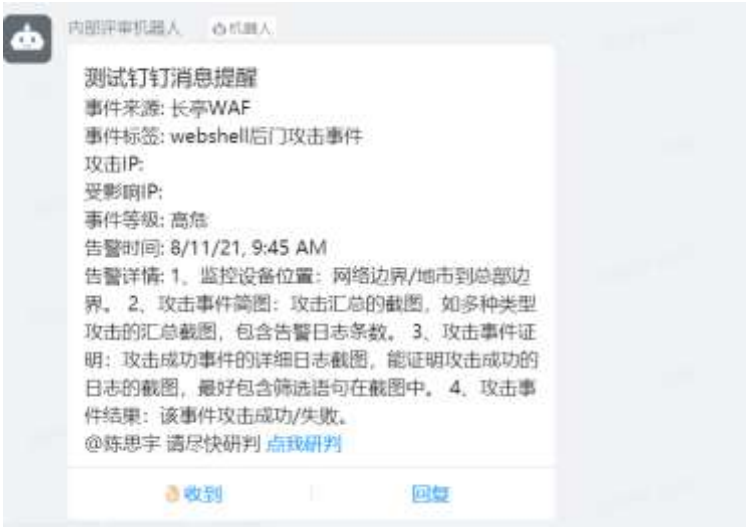


在安全事件管理模块，配置管理-管理流程绑定页面，绑定新的管理流程，依次输入研判、T1 处置和 T2 处置人员所在钉钉群的 webhook、sign 和对应人员的手机号。



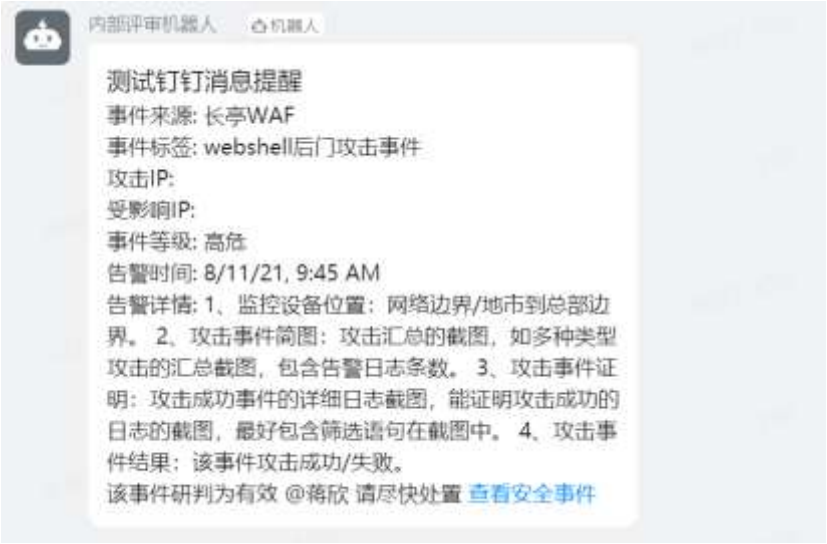
在事件管理-事件监控-提交事件页面中，选择管理流程名称为“云 EDR 告警分析处置测试”，选择项目名称、事件来源、事件标签和告警时间，填写事件名称，点击<提交>。

事件提交后，发送钉钉消息至研判群，并@对应的研判人员。



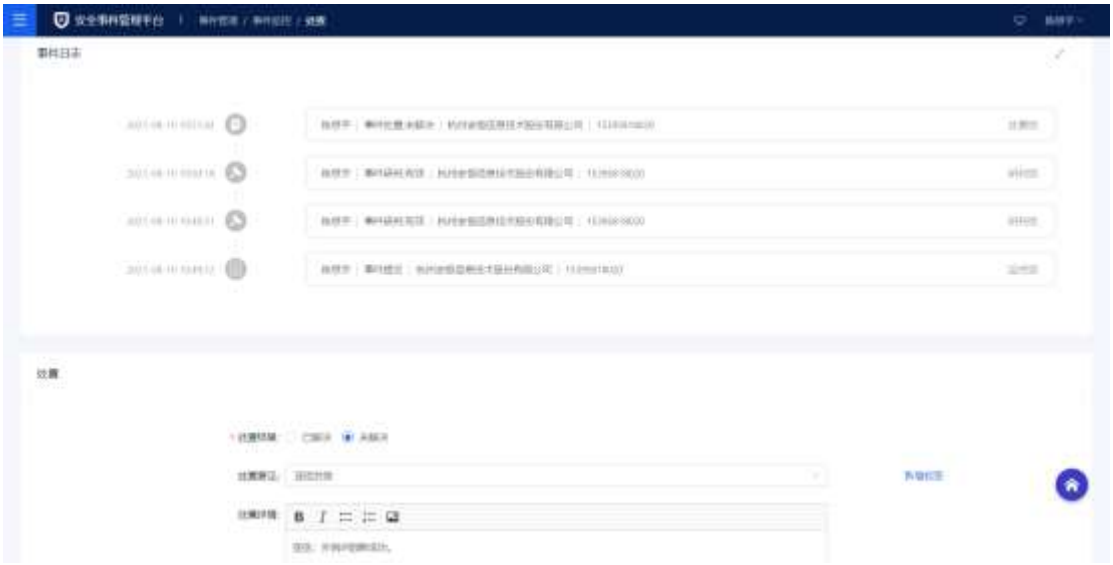
若事件研判有效，进入 T1 处置阶段；若事件研判无效，则进入误报列表。

事件研判有效后，发送钉钉消息至 T1 处置群，并@对应的 T1 处置人员。

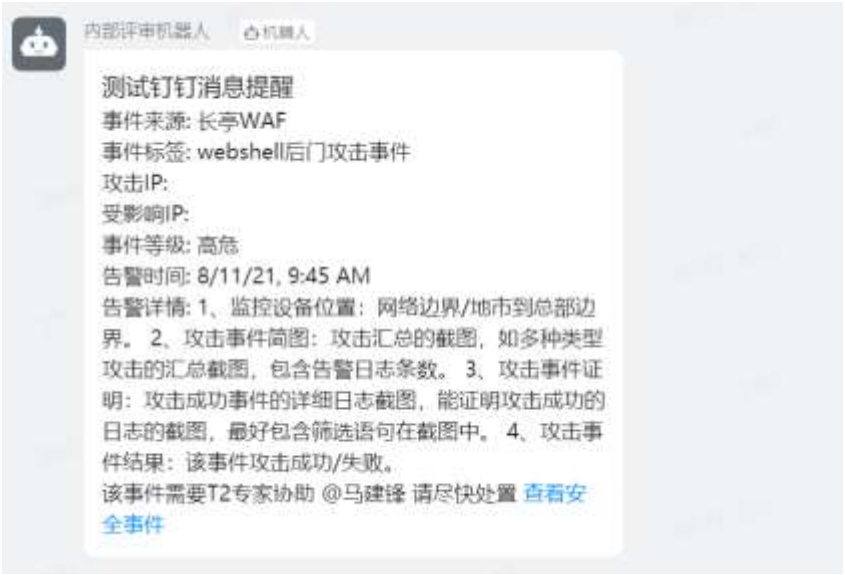


若事件 T1 处置为“已解决”，则事件归档；

若事件 T1 处置为“未解决”，则进入 T2 专家处置阶段。

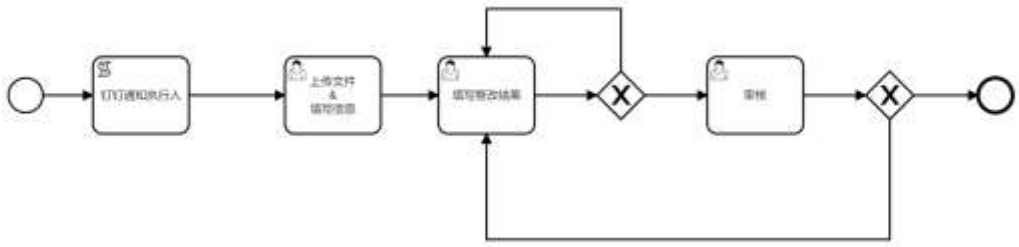


事件 T1 处置为“未解决”后，发送钉钉消息至 T2 处置群，并@对应的 T2 处置专家，由 T2 专家处置后事件归档。



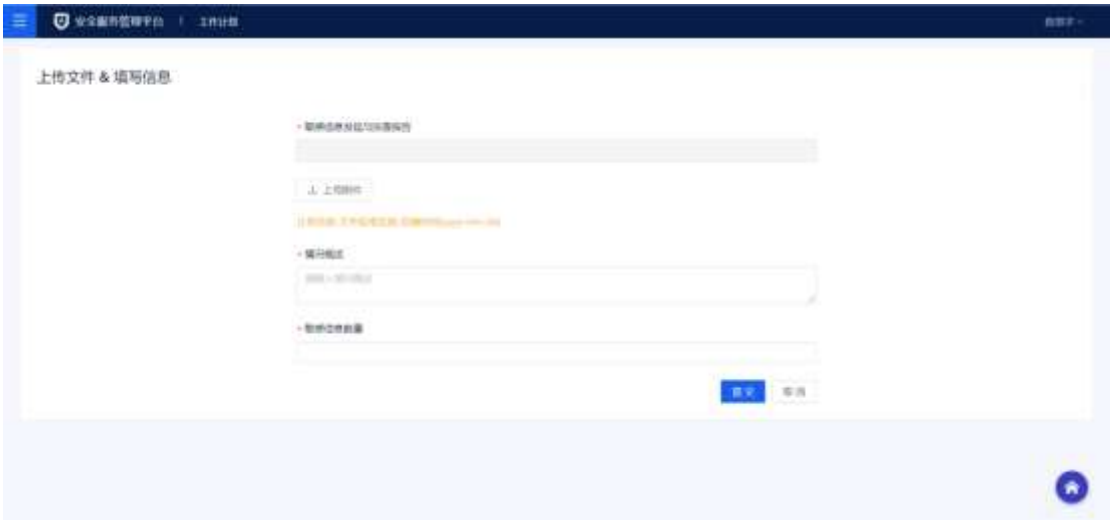
4.5 港中旅工作流

4.5.1 敏感信息发现与排查



在安全服务管理模块的工作计划-任务列表内添加计划，选择计划类型为“敏感信息发现与排查”，填写相应信息后点击<确定>。

上传文件&填写信息，上传附件、填写情况概述和敏感数量，点击<提交>。



填写处理结果时，填写无需处置数量、整改结果、整改数量，勾选是否完成：

若完成，则进入下一个节点，项目经理审核；

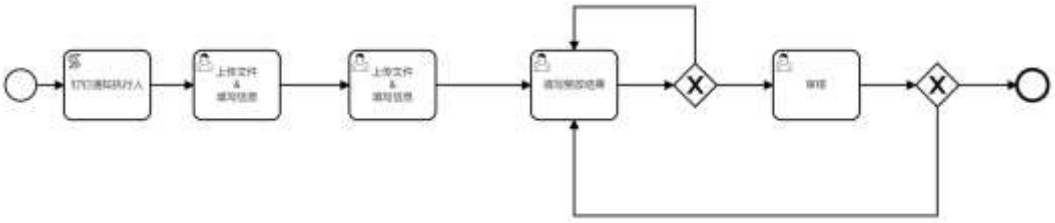
若未完成，则进入循环，重新填写处理结果至完成。

项目经理审核，不能对信息进行修改，填写审核意见后，选择是否通过：

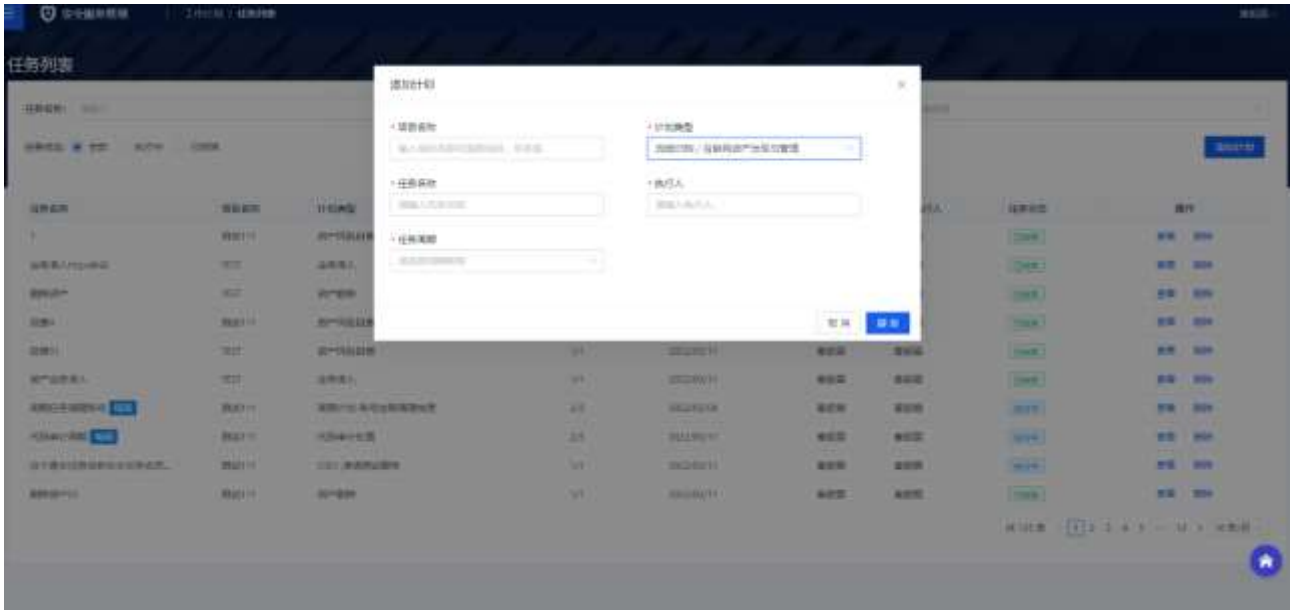
若通过，则流程结束；

若不通过，则重新回到填写处理结果的节点，直至审核通过。

4.5.2 互联网资产发现与管理



在安全服务管理模块的工作计划-工作计划列表内添加计划，选择计划类型为“互联网资产发现与管理”，填写相应信息后点击<确定>。



第一个上传文件&填写信息，上传附件、填写情况概述后，点击<提交>。

第二个上传文件&填写信息，上传附件、填写情况概述和资产数量后，点击<提交>。

填写处理结果时，填写无需处置数量、整改结果、整改数量，勾选是否完成：

若完成，则进入下一个节点，项目经理审核；

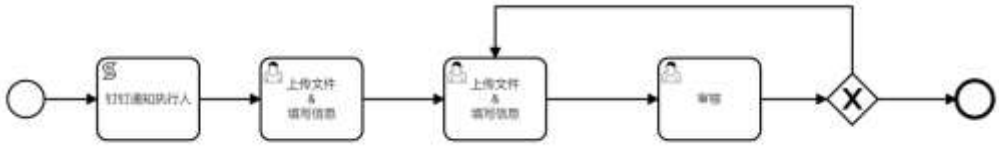
若未完成，则进入循环，重新填写处理结果至完成。

项目经理审核，不能对信息进行修改，填写审核意见后，选择是否通过：

若通过，则流程结束；

若不通过，则重新回到填写处理结果的节点，直至审核通过。

4.5.3 钓鱼邮件测试



在安全服务管理模块的工作计划-工作计划列表内添加计划，选择计划类型为“钓鱼邮件测试”，填写相应信息后点击<确定>。

第一个上传文件&填写信息，上传附件、填写情况概述后，点击<提交>。

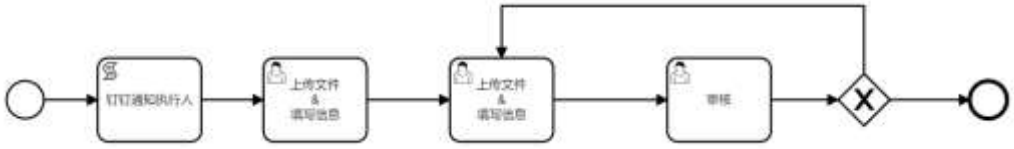
第二个上传文件&填写信息，上传附件、填写情况概述、涉及人员数量、上钩人员数量后，点击<提交>。

项目经理审核，不能对信息进行修改，填写审核意见后，选择是否通过：

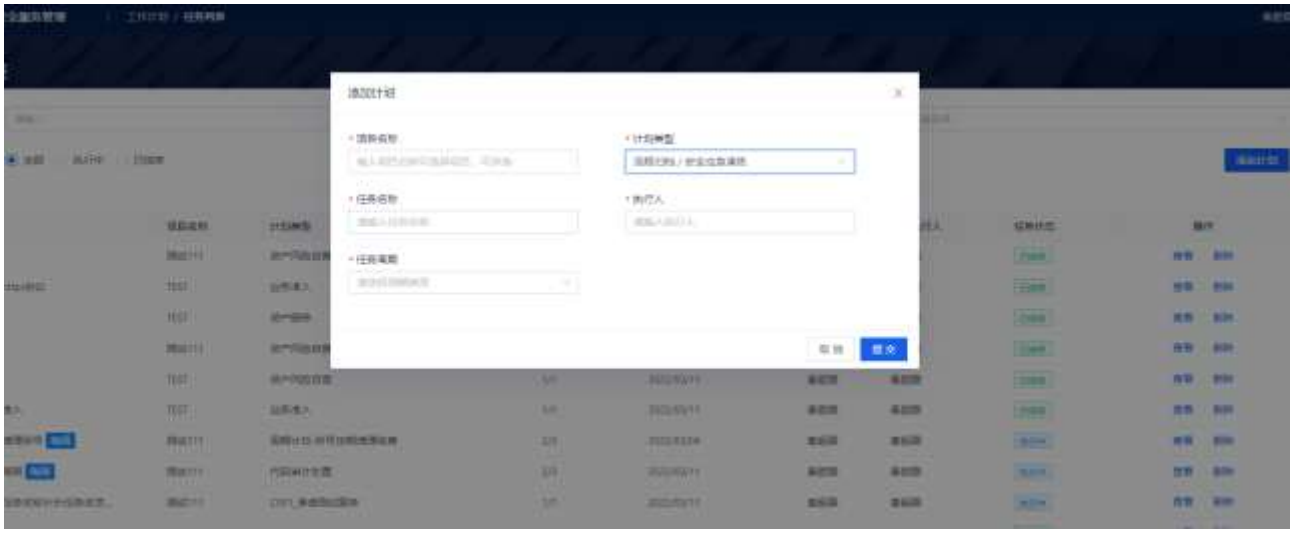
若通过，则流程结束；

若不通过，则重新回到第二个上传文件&填写信息的节点，直至审核通过。

4.5.4 安全应急演练

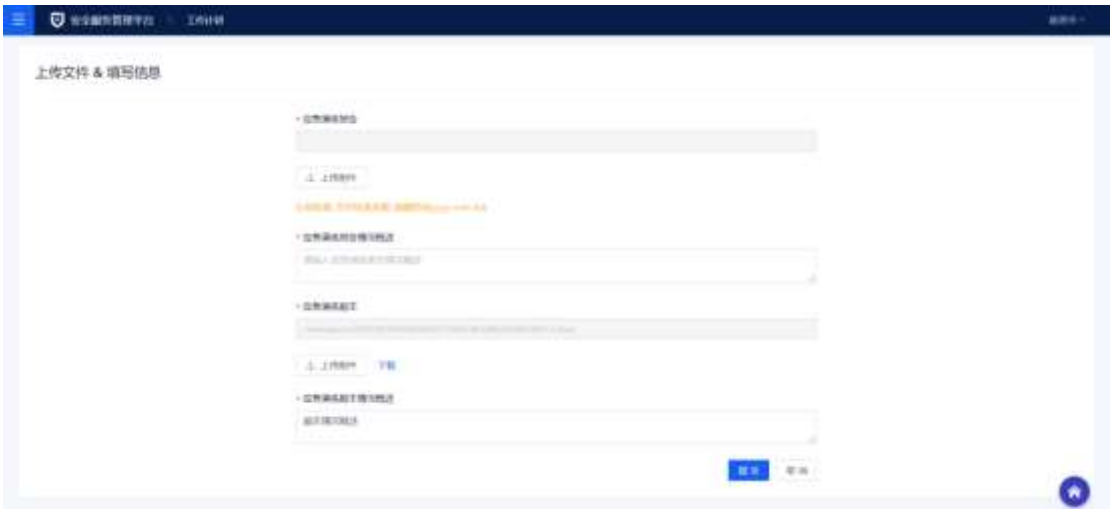


在安全服务管理模块的工作计划-工作计划列表内添加计划，选择计划类型为“安全应急演练”，填写相应信息后点击<确定>。



第一个上传文件&填写信息，上传附件、填写情况概述后，点击<提交>。

第二个上传文件&填写信息，上传附件、填写情况概述后，点击<提交>。

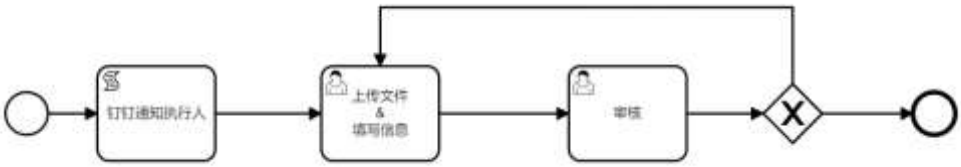


项目经理审核，不能对信息进行修改，填写审核意见后，选择是否通过：

若通过，则流程结束；

若不通过，则重新回到第二个上传文件&填写信息的节点，直至审核通过。

4.5.5 玄武盾监测告警分析与处置



在安全服务管理模块的工作计划-工作计划列表内添加计划，选择计划类型为“玄武盾监测告警分析与处置”，填写相应信息后点击<确定>。

上传文件&填写信息，上传附件、填写事件数量、处置数量、误报数量和情况概述后，点击<提交>。

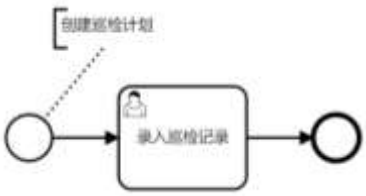
项目经理审核，不能对信息进行修改，填写审核意见后，选择是否通过：

若通过，则流程结束；

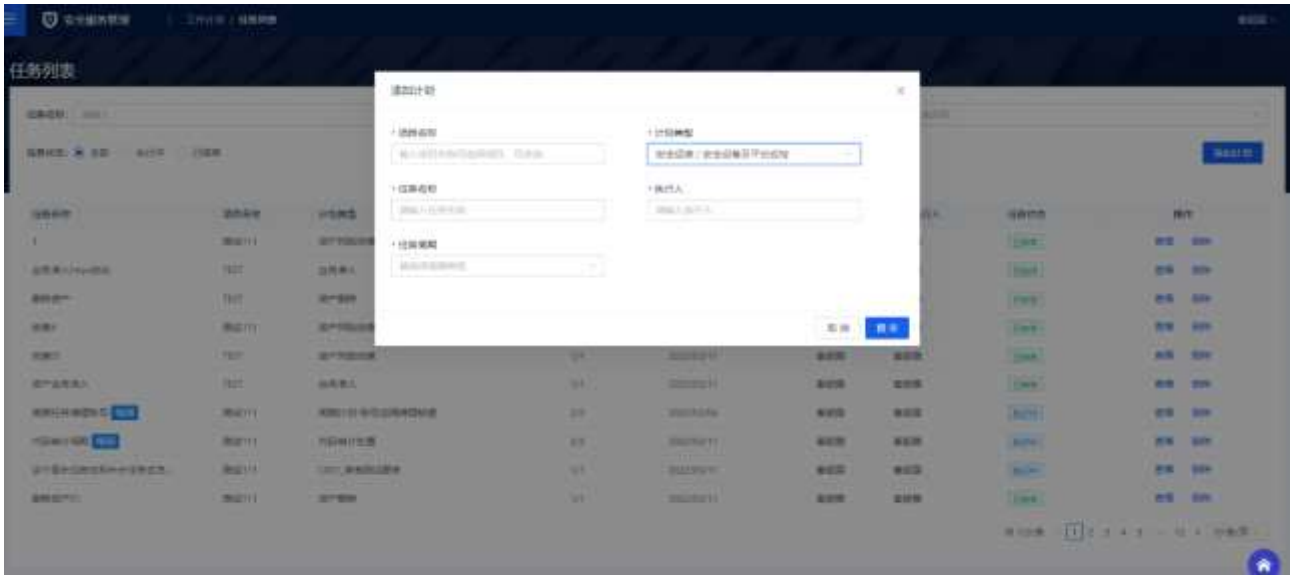
若不通过，则重新回到上传文件&填写信息的节点，直至审核通过。

4.6 安全运维工作流

4.6.1 安全设备及平台巡检

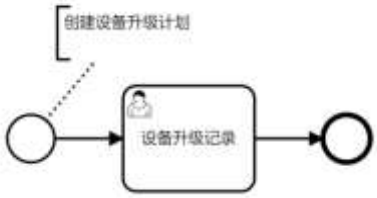


在安全服务管理模块，在安全运维阶段添加建立“安全设备及平台巡检”计划类型的计划。

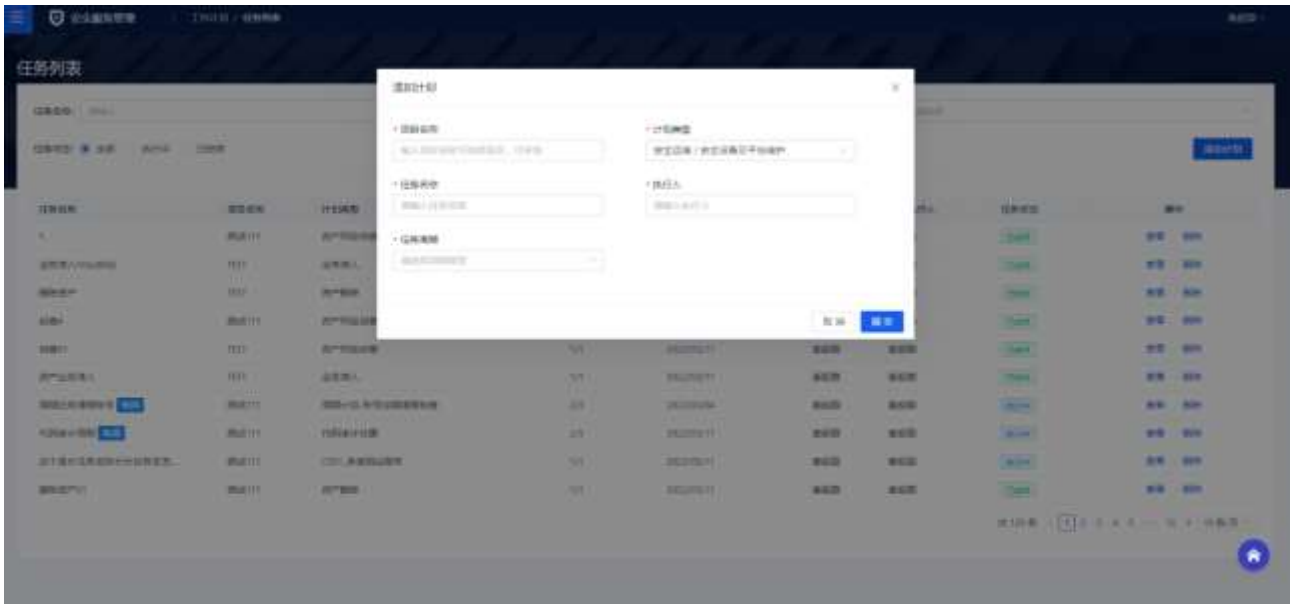


计划添加成功之后，录入巡检记录，选择设备状态为“正常”或“异常”，输入备注并上传附件，点击<提交>流程结束。

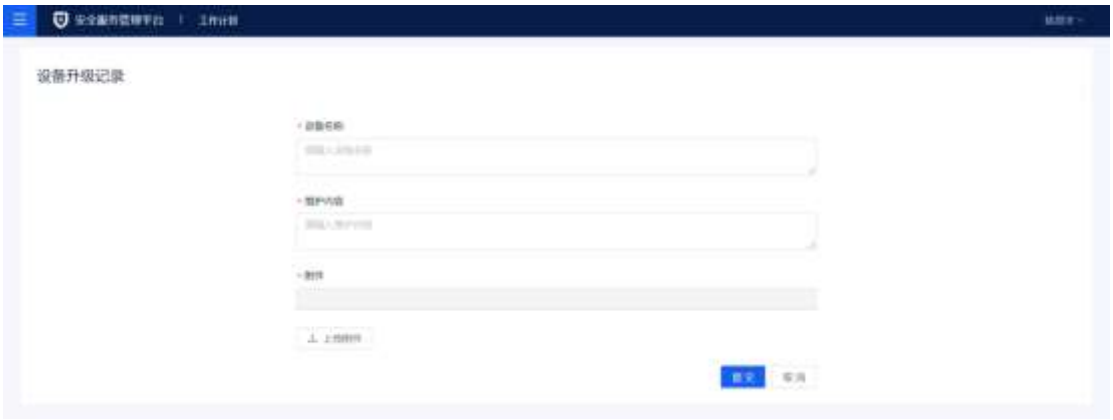
4.6.2 安全设备及平台维护记录



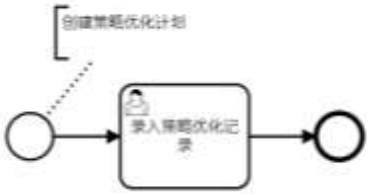
在安全服务管理模块，在安全运维阶段建立“安全设备及平台维护记录”计划类型的计划。



计划添加成功之后，录入升级记录，填写设备名称、维护内容并上传附件，点击<提交>后流程结束。

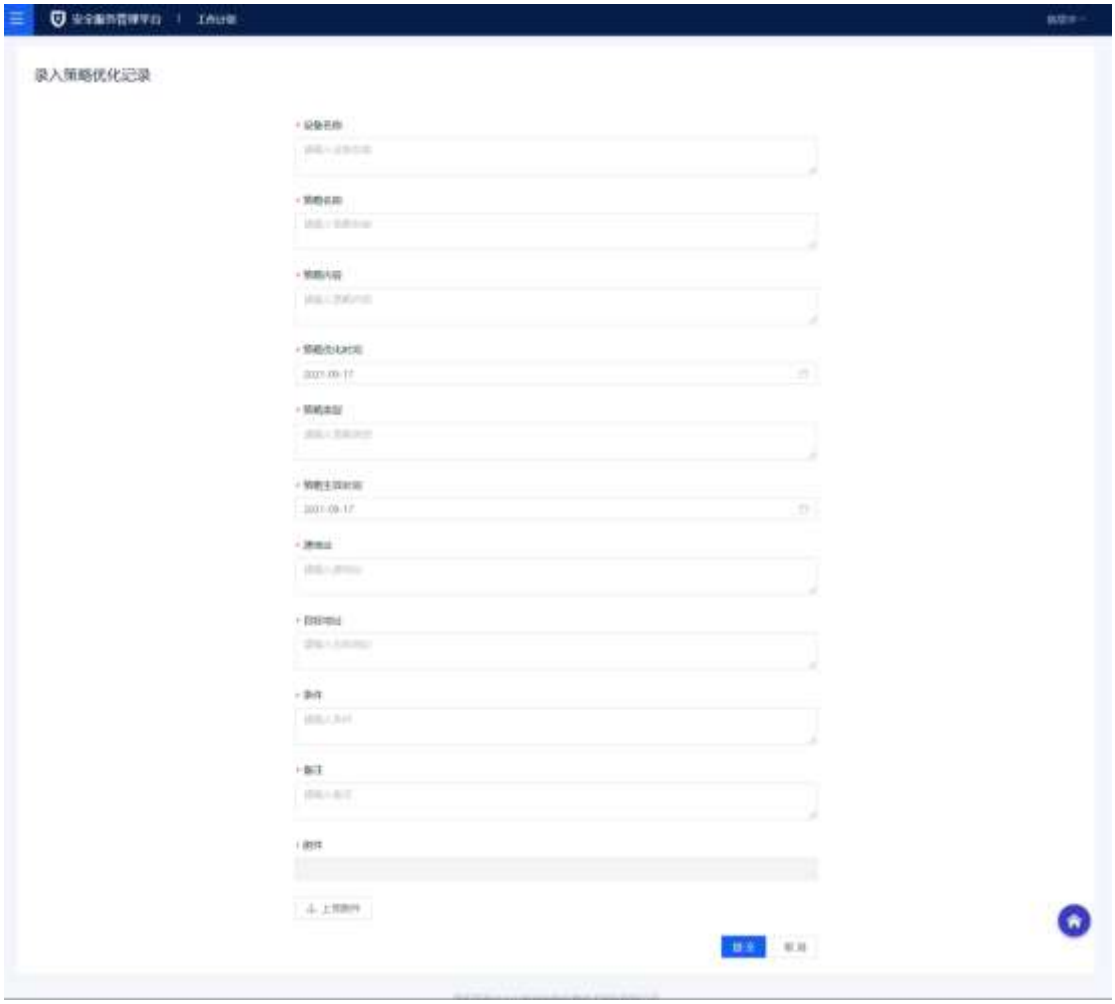


4.6.3 安全设备及平台策略调优

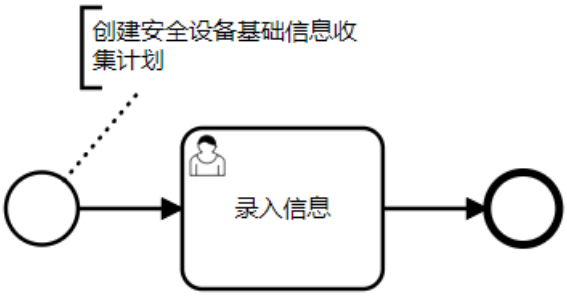


在安全服务管理模块，在安全运维阶段建立“安全设备及平台策略调优”计划类型的计划。

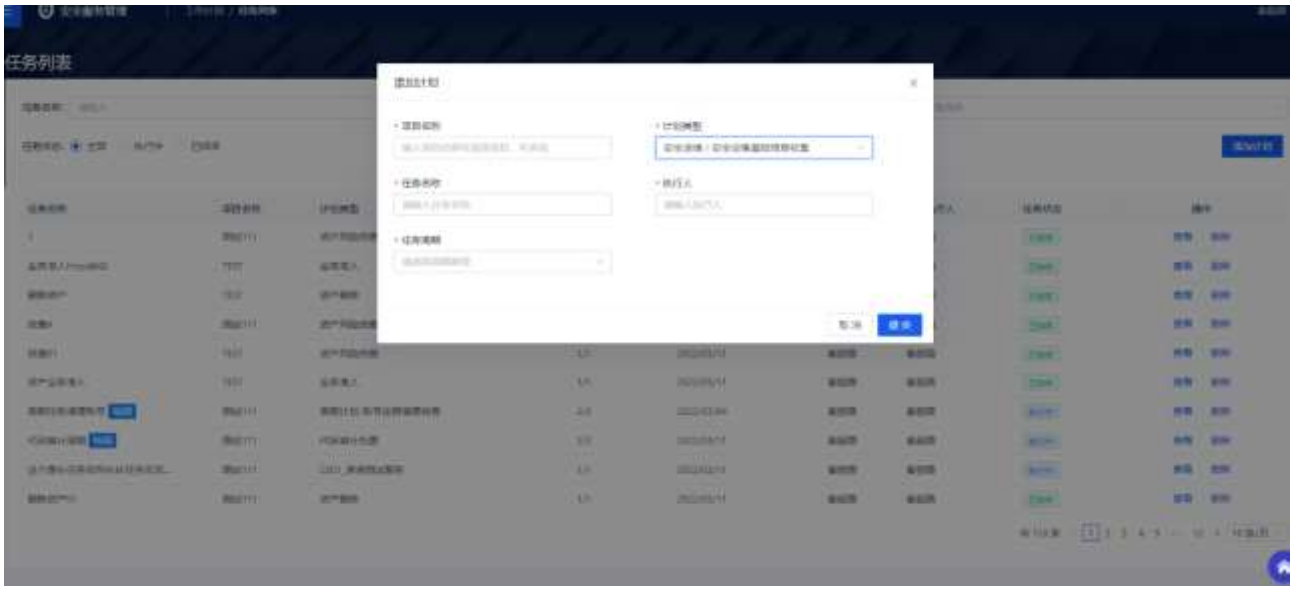
计划添加成功之后，录入策略优化记录，填写设备名称、策略名称、策略内容、源地址、目标地址、条件、备注和上传附件，策略优化时间和策略生效时间默认为当日，可重新选择，点击<提交>后流程结束。



4.6.4 安全设备基础信息收集

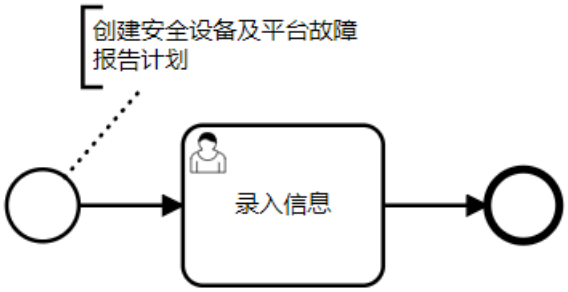


在安全服务管理模块，在安全运维阶段建立“安全设备基础信息收集”计划类型的计划。

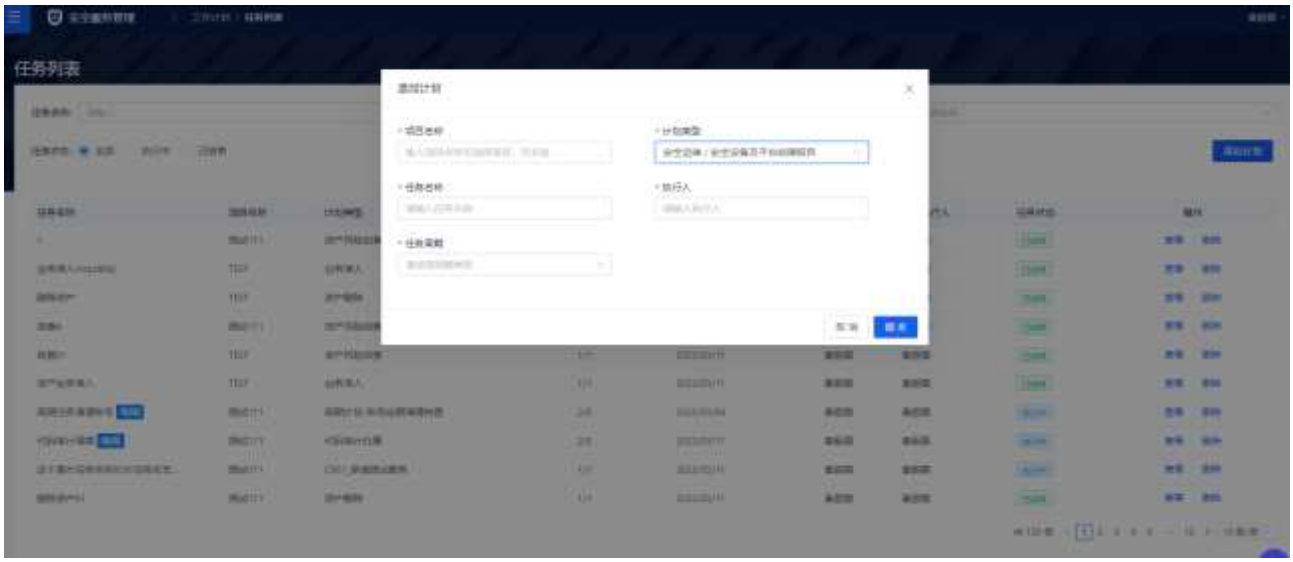


计划添加成功之后，录入信息，录入设备名称、设备访问地址、设备型号、设备安装日期（默认当日）客户信息，输入备注，上传附件，点击<提交> 后流程结束

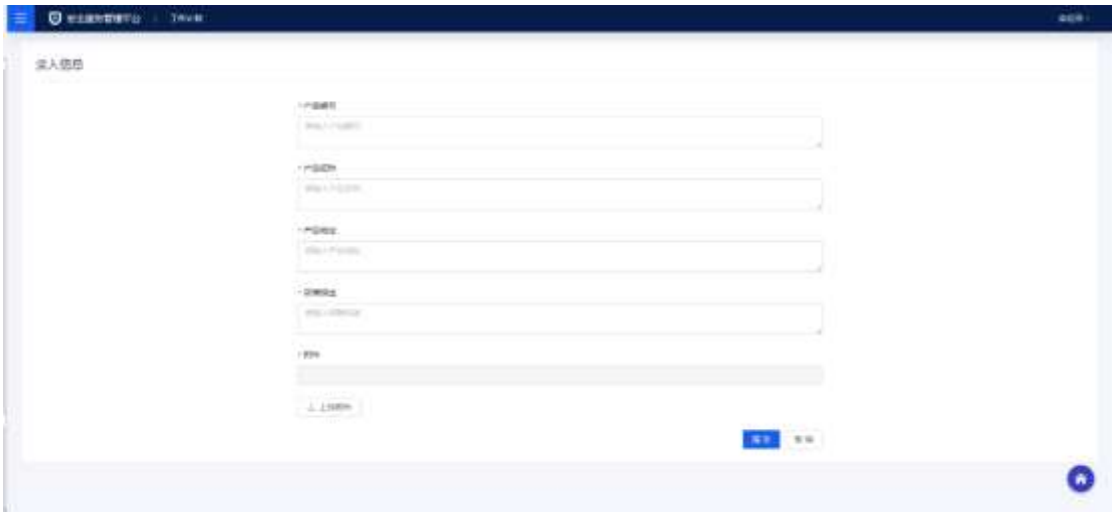
4.6.5 安全设备及平台故障报告



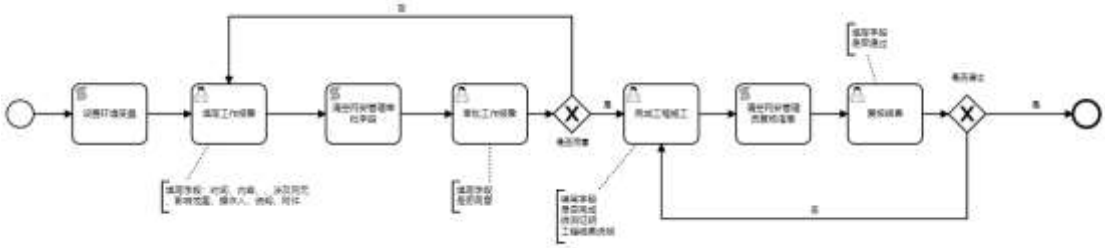
在安全服务管理模块，在安全运维阶段建立“安全设备及平台故障报告”计划类型的计划。



录入信息，录入产品编号、产品名称、产品地址、故障描述，上传附件，点击<提交>后流程结束。



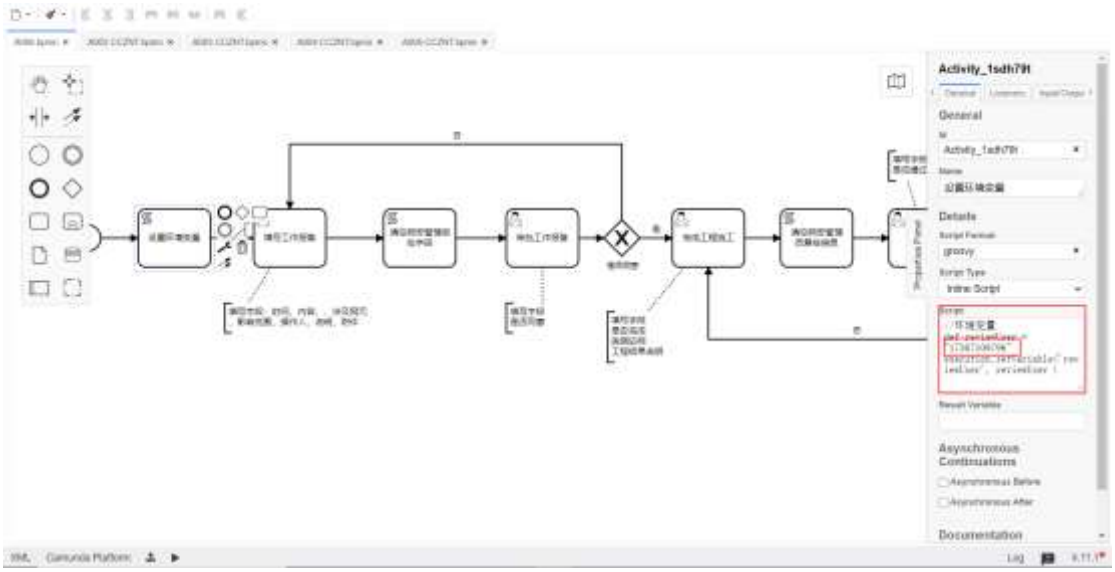
4.6.6 安全工作报备



管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流，进入工作流页面。选择 A006_安全工作报备流程的.bpmn，点击编辑，点击工作流的第一步，设置//环境变量

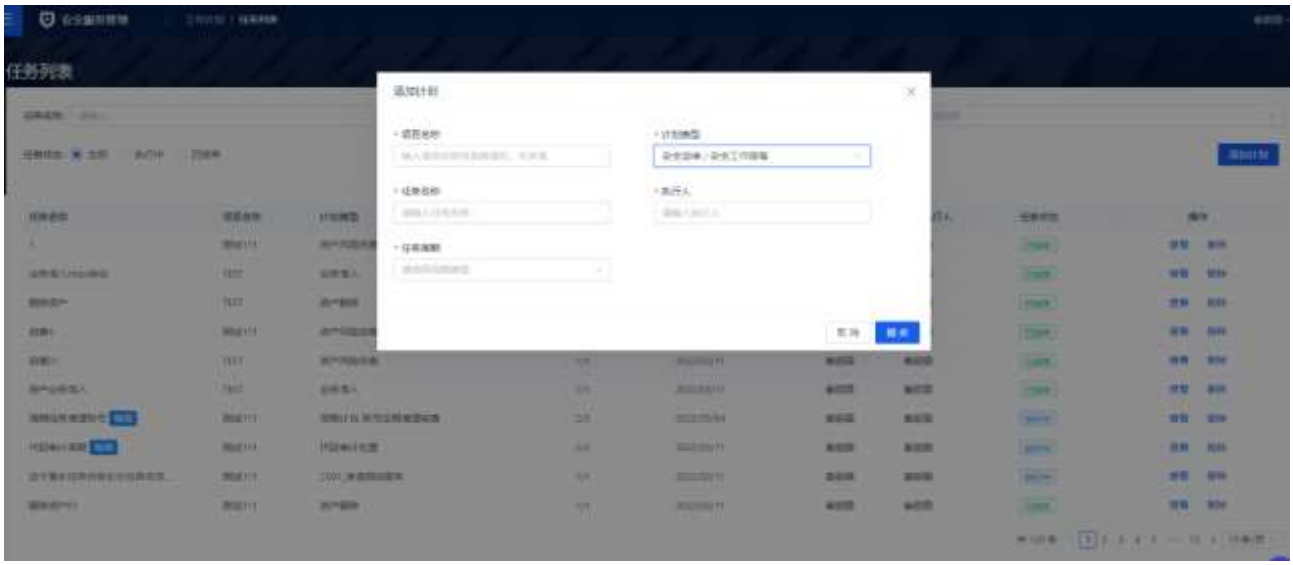
def reviewUser = "计划添加人的手机号"

execution.setVariable('reviewUser', reviewUser)后保存。

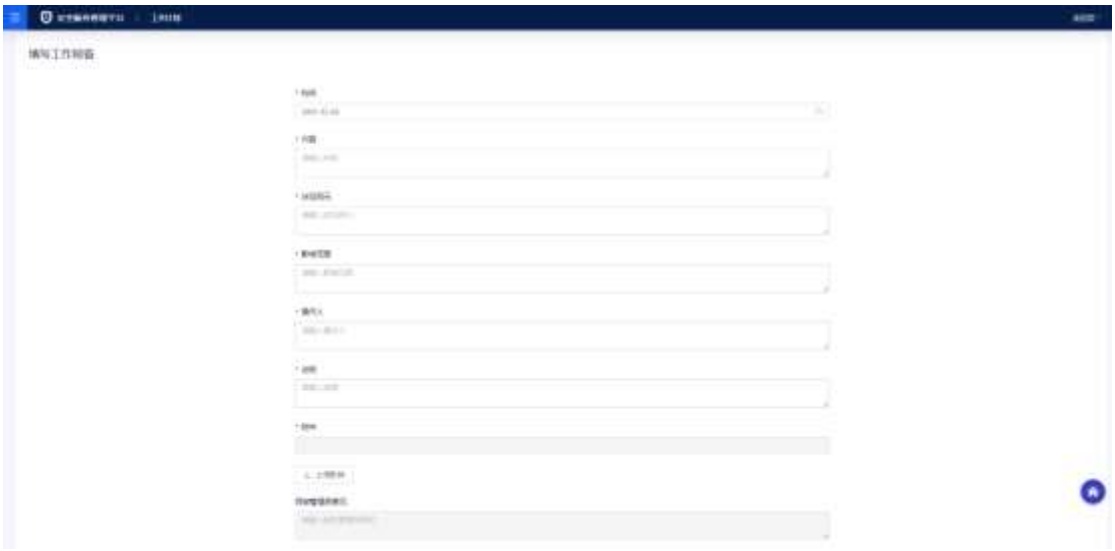


编辑完成之后点击<部署>，点击二次确认部署弹窗<确定>。

在安全服务管理模块，在安全运维阶段建立“安全工作报备”计划类型的计划。



填写工作报备，时间默认当天可自行修改，输入内容、涉及网元、影响范围、操作人姓名、添加说明，上传附件之后点击<提交>



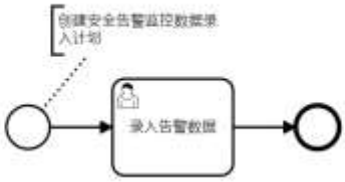
流程进入审批工作报备，勾选是否同意，填写审批意见后，点击<提交>；若审批不同意将重新填写工作报备直至审批同意。

审批同意之后，完成工程施工。勾选是否完成，上传“拨测证明”附件后点击<提交>；

工程施工完成之后由项目经理复核结果。勾选是否复核通过，填写复核意见之后点击<提交>；若复核不通过将在工程施工出处重新上传拨测证明完成工程施工直至复核通过。复核通过之后流程结束。

4.7 周期计划

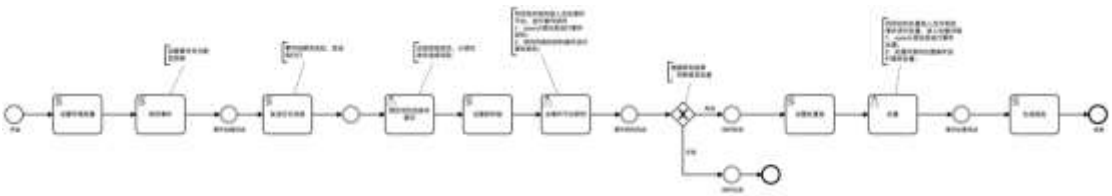
4.7.1 安全告警监控数据录入工作流



在安全服务管理模块，建立“安全告警监控数据录入”计划类型的周期计划。

录入告警数据时，填写设备名称，告警数量和备注，其中记录时间默认值为当日，可重新选择时间，点击<提交>后流程结束

4.8 情报转事件工作流

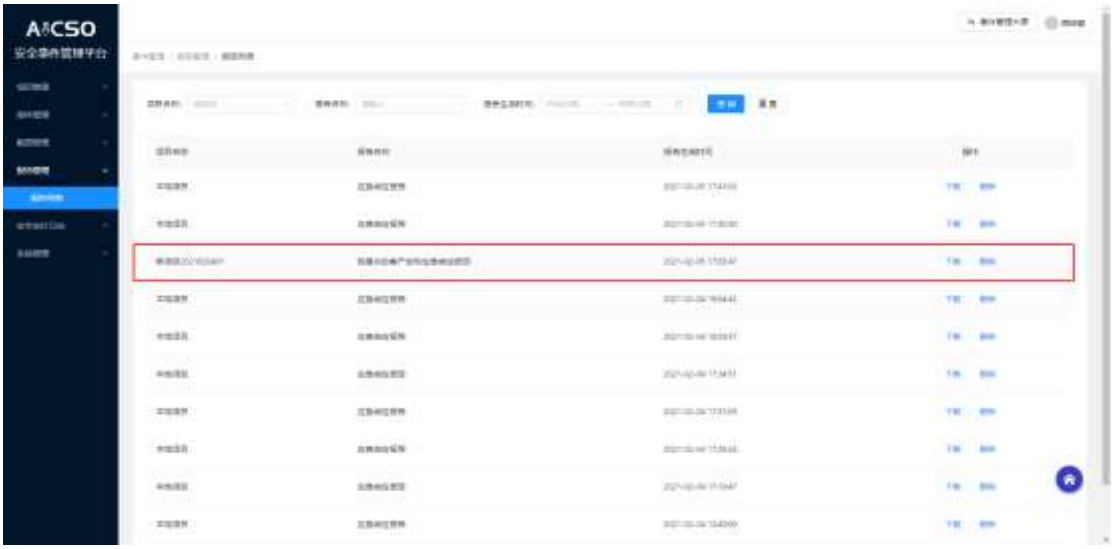


在威胁信息共享模块，情报管理-情报列表页面中，选择一条情报，点击<转事件排查>，安全事件管理模块的监控组成员在“待排查列表”中，选择该条事件进行排查，选择项目后，输入其他字段信息，点击<提交>，事件创建完成，进入待研判状态。如果点击<误报>，则该事件进入到误报列表，工作流结束。

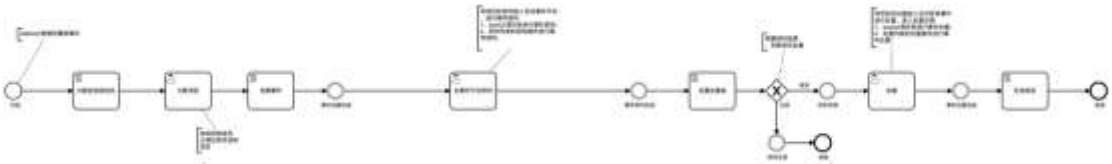
研判组成员在待办任务的待认领列表新增研判任务，或者直接在事件管理平台的研判列表中选择该事

件，点击<研判>，进入事件平台进行研判操作，研判完成后待处置列表新增事件。

处置组成员在待办任务的待认领列表新增处置任务，或者直接在事件管理平台的处置列表中选择该事件，点击<处置>，进入事件平台进行处置操作。处置完成后已处置列表新增事件，工作流结束，结束后事件平台生成报告。



4.8.1 AiLPHA 告警转事件



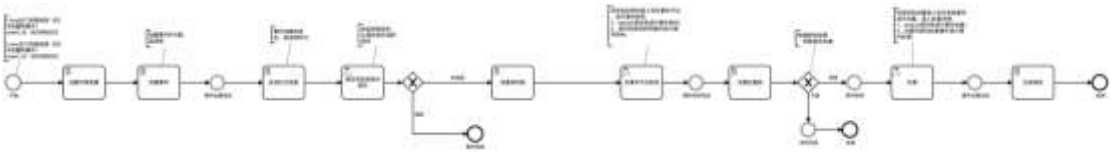
AiLPHA 告警转事件工作流

AiLPHA 推送数据到安全运营平台后，事件管理平台监控组用户在“待排查列表”中，选择该条事件进行排查，选择项目后，输入其他字段信息，点击提交，事件创建完成，进入待研判状态。如果点击误报，则该事件进入到误报列表，工作流结束。

事件平台研判者角色的用户在待办任务的待认领中选择“AILPHA 指派了【网络防御运营管理平台】的去事件平台研判的任务”，并在事件平台进行研判。

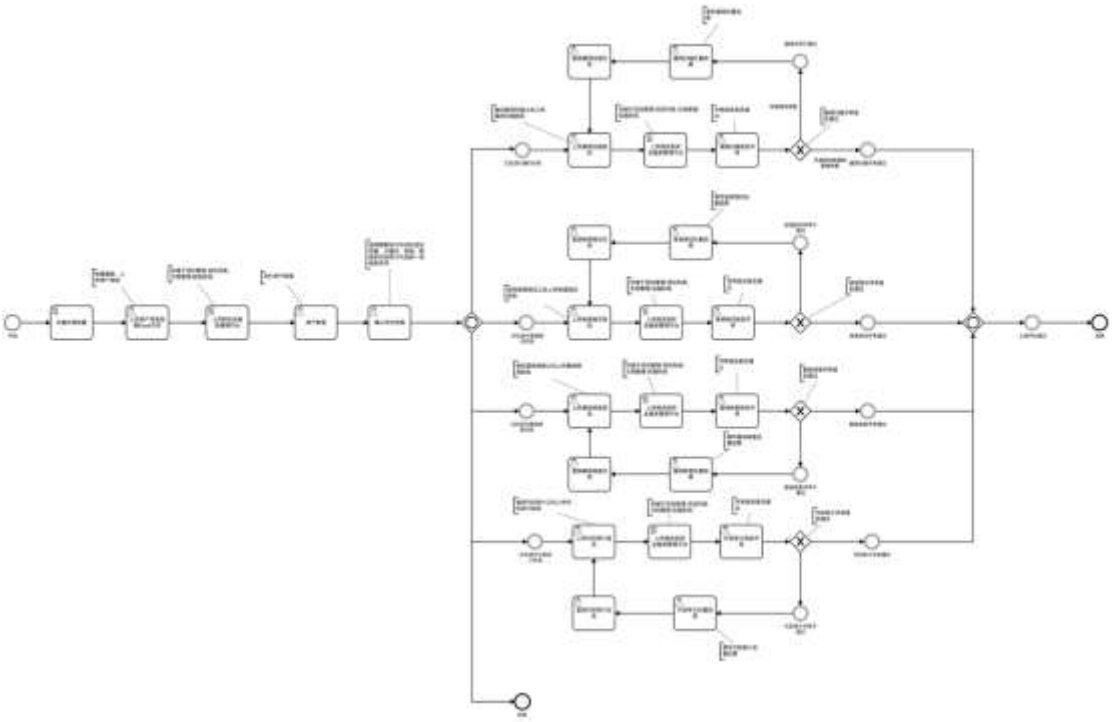
事件平台处置者角色的用户在待办任务的待认领中选择“AILPHA 指派了【网络防御运营管理平台】的去事件平台处置的任务”，并在事件平台进行处置。

4.8.2 EDR 告警转事件工作流



EDR 推送告警后，事件平台监控组成员直接在“待排查列表”中，选择该条事件进行排查，选择项目后，输入其他字段信息，点击提交，事件创建完成，进入待研判状态。如果点击误报，则该事件进入到误报列表，工作流结束。研判和处置流程与“情报转事件”和“AILPHA 告警转事件”相似。

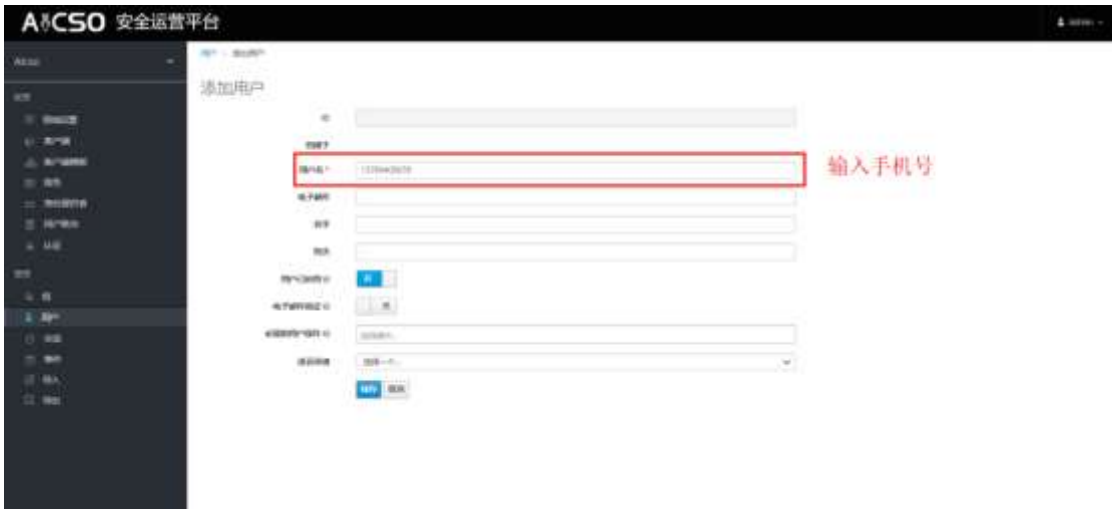
4.8.3 新系统上线评估



在 keyclock 平台进行用户配置。

注：需要新增三个用户：项目负责人、客户 B、工程师;

添加用户，输入用户手机号；



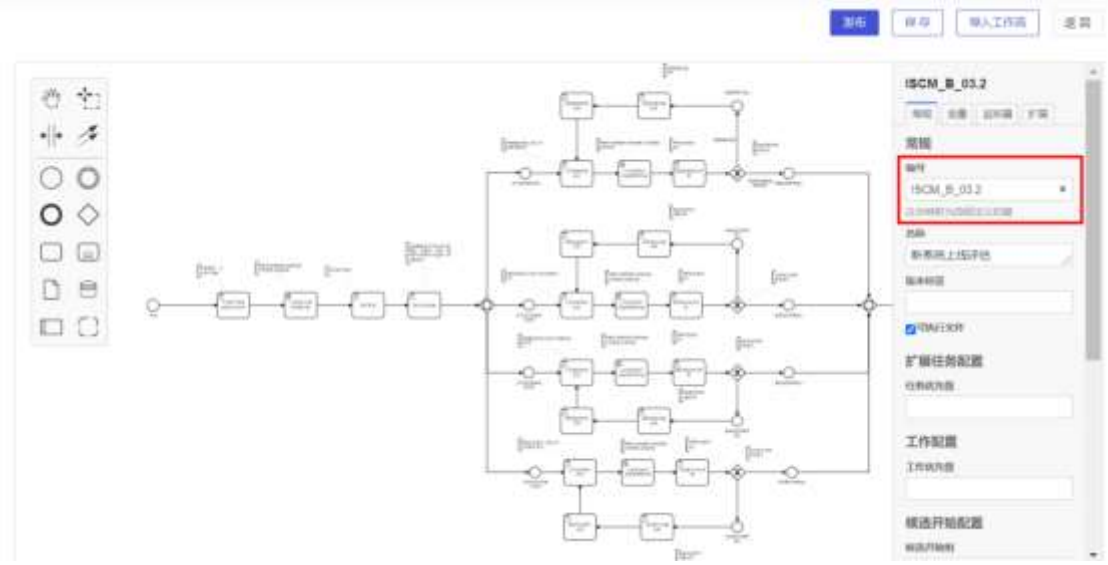
用户添加后，需要配置 2 个属性：fullname 与 phone；

fullname：项目负责人、工程师、客户 B；

phone:手机号码；

管理员在安全服务管理模块的工作计划配置模块，在实施阶段与规划阶段，新增“系统上线评估”任务类型；

注：工作流编号来自“网络防御运营管理平台-编辑工作流-工作流列表-查看单条工作流-编号”；



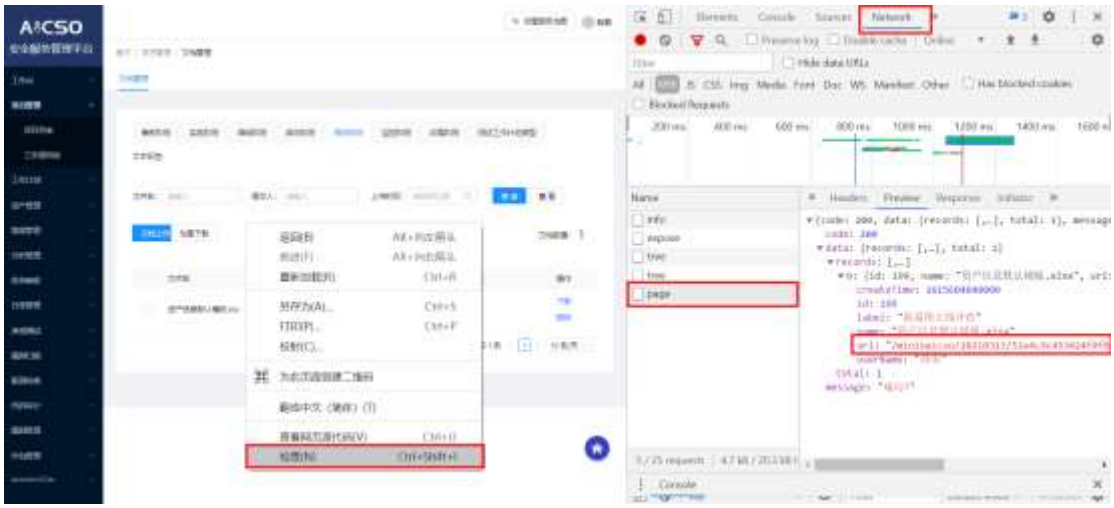
由项目负责人在安全服务管理模块，新建项目，并且新建项目后，需要添加成员工程师与客户 B；

注：在添加用户前，工程师与客户 B 需要登录过安全服务管理模块

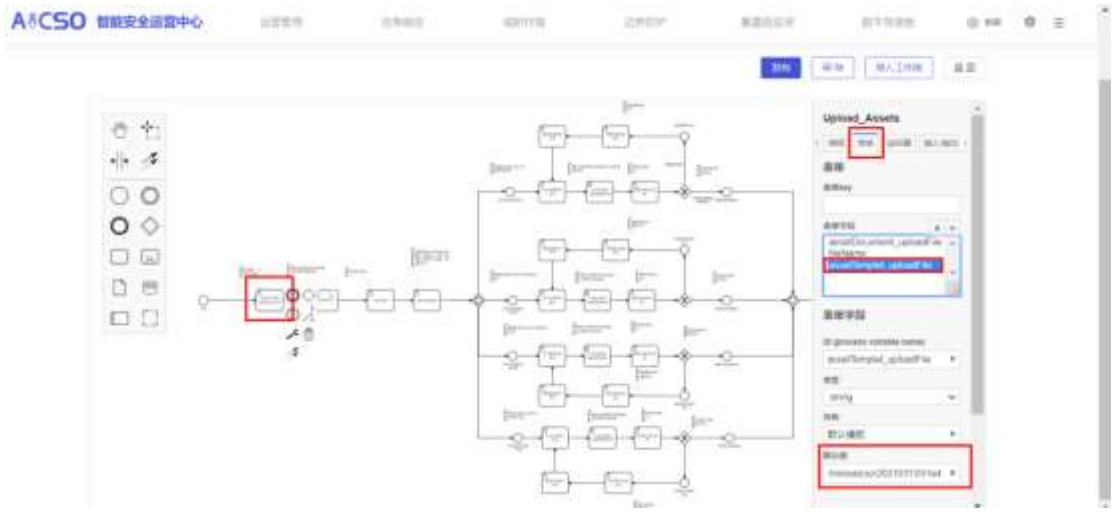
由项目负责人在项目管理-项目列表-文档管理-规划阶段-新系统上线评估，上传默认资产信息模板；

文档上传成功后，右键“检查”，点击 Network，刷新（ctrl+R）界面，点击 page 查看 url 中的值“/minioaicso/..../xlsx”；

注:此值复制后，删除此文档;



由项目负责人将 url 的值，复制到工作流第一步“上传资产信息收集 Excel 文件-表单-assetTemplet_uploadFile”中的默认值；

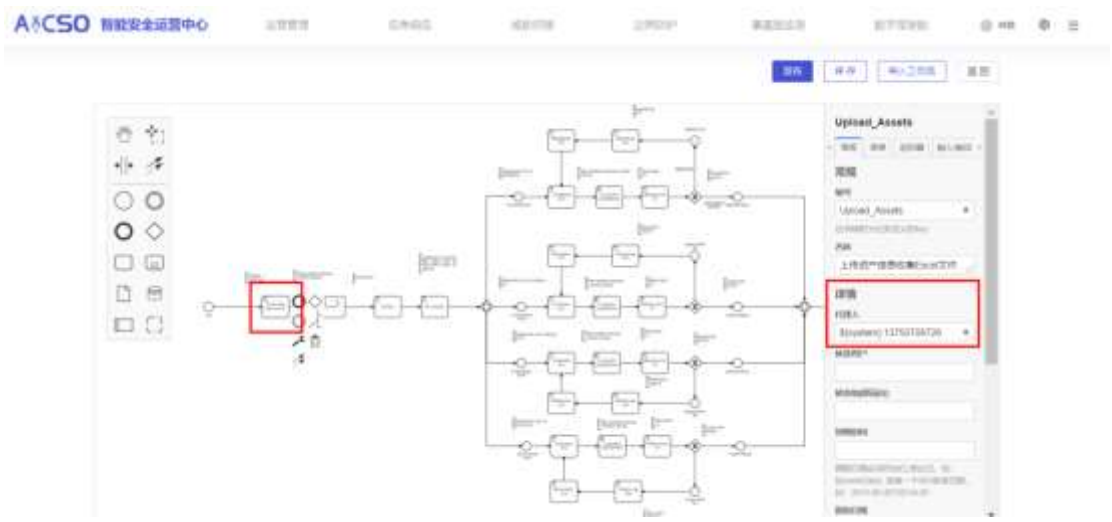


工作流用户任务的详情-代理人处，进行用户配置；

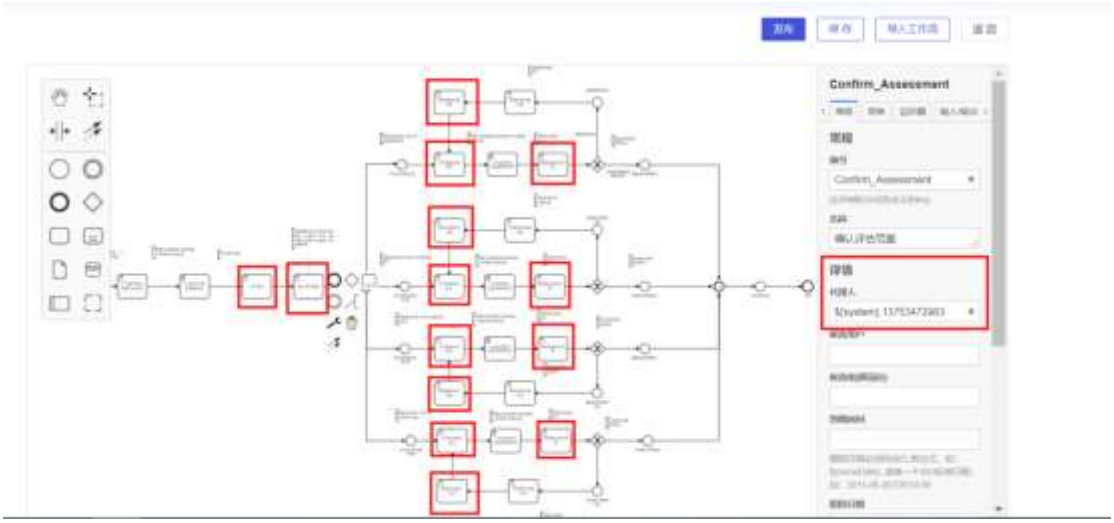
每个用户任务现在分配人是写死的,根据实际情况配置,本流程有 3 个角色,修改截图中的手机号即可；

输入${system}:处理任务者的手机号码，如下图所示，每一个用户任务处都需要添加；

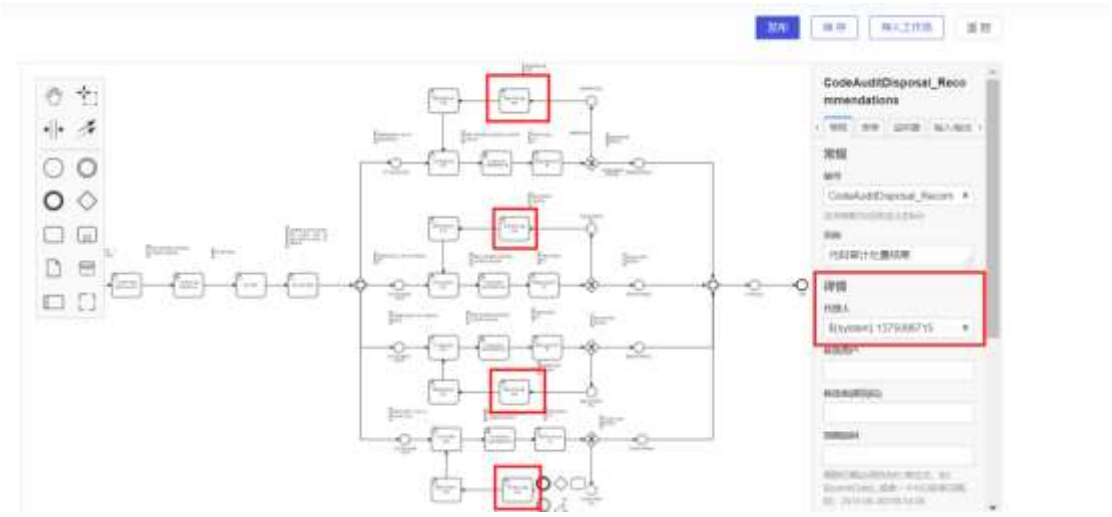
(1) 项目负责人:



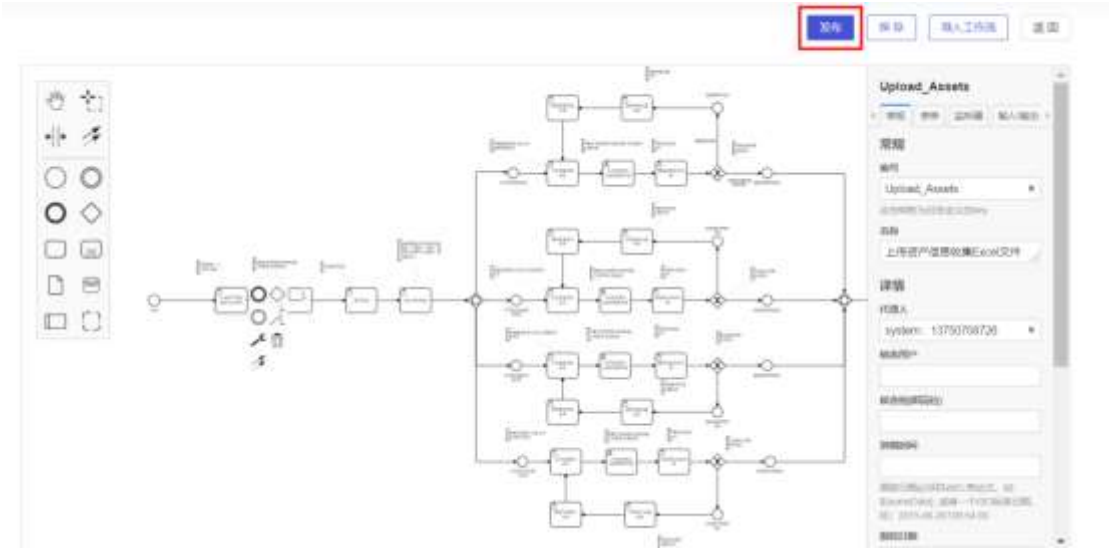
(2) 工程师:



(3) 客户 B:



用户添加成功后，点击发布；

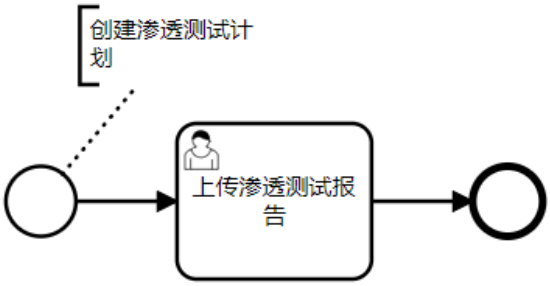


工作流发布后，在工作计划列表，选择此具体项目与任务类型，并填写相关内容后，点击<确认>，(也可以在项目管理-项目列表-工作计划-添加计划，选择任务类型“新系统上线评估”，并且填写相关信息，点击<确认>后)，则触发此工作流；

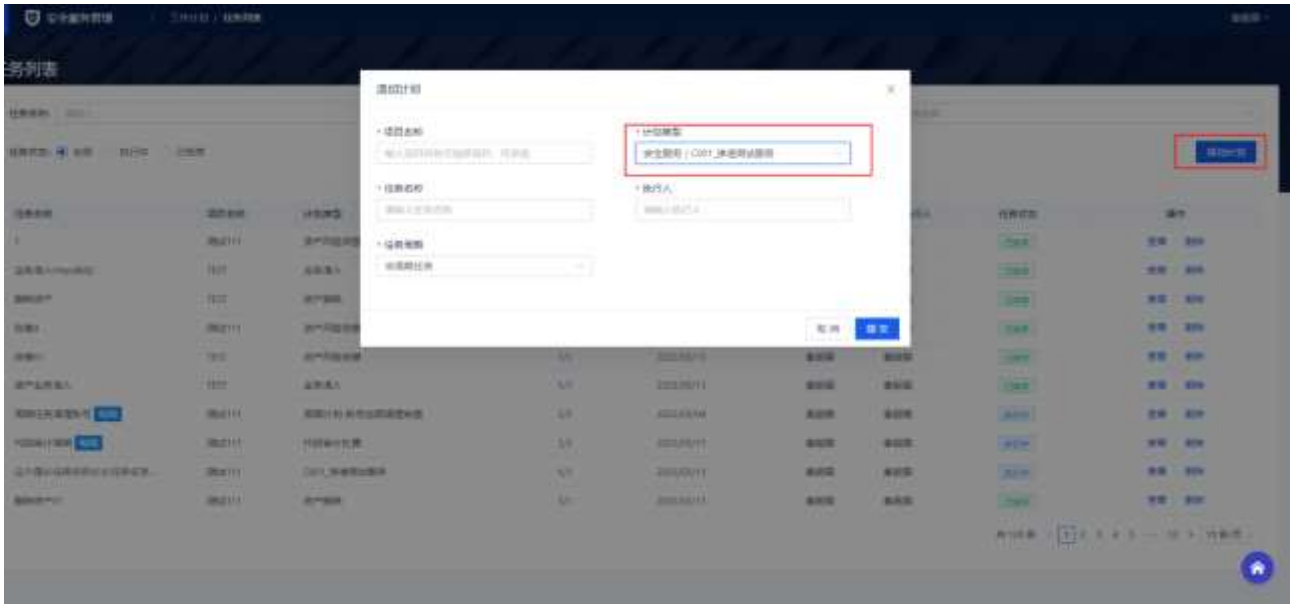
指派到的具体用户，当此任务之间的任务完成时，就会在待办任务处接收到待办任务；

4.9 安全服务工作流

4.9.1 渗透测试服务

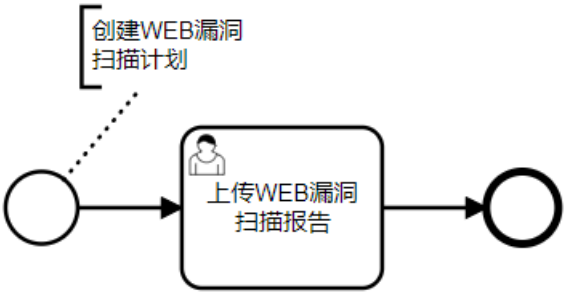


在安全服务管理模块，在安全服务阶段添加建立“渗透测试服务”计划类型的计划。

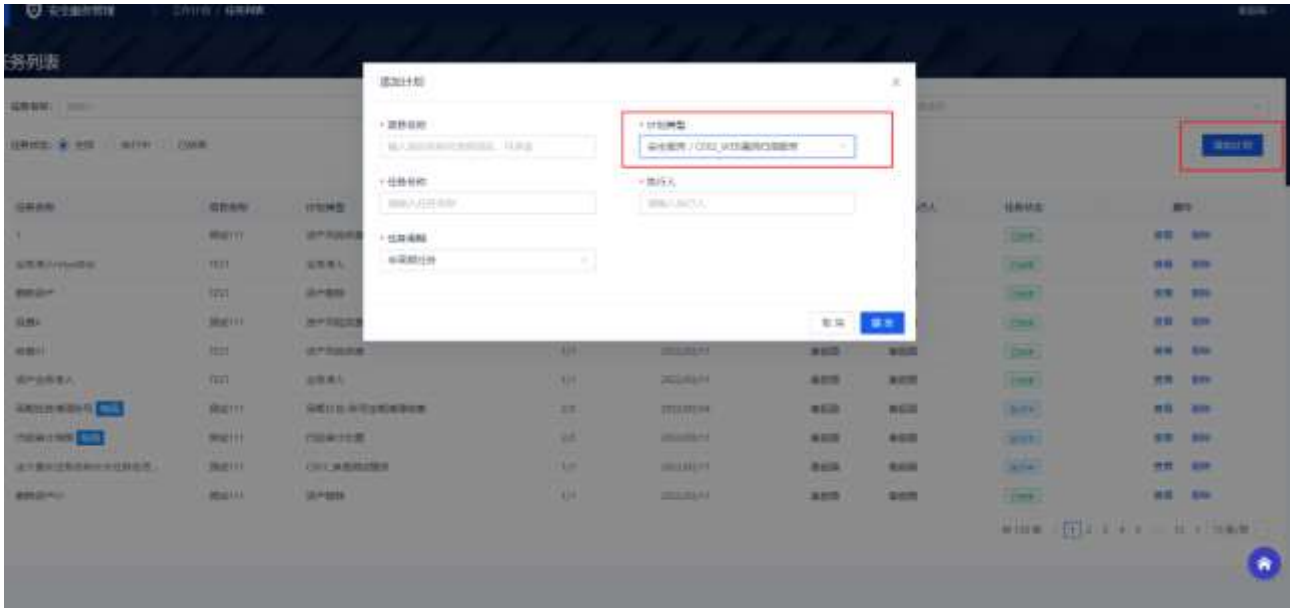


计划添加成功之后，在工作台待办事项中上传渗透测试报告的附件，输入备注，点击<提交>，提交成功之后流程结束。

4.9.2 WEB 漏洞扫描服务

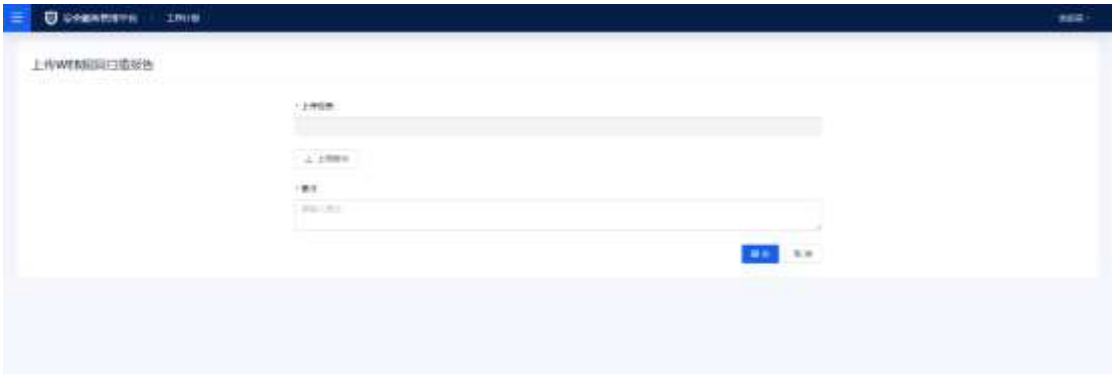


在安全服务管理模块，在安全服务阶段添加建立“WEB 漏洞扫描服务”计划类型的计划。

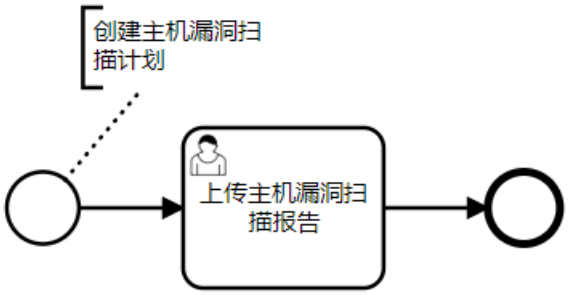


计划添加成功之后，在工作台待办事项中上传 web 漏洞扫描报告的附件，输入备注，点击<提交>，

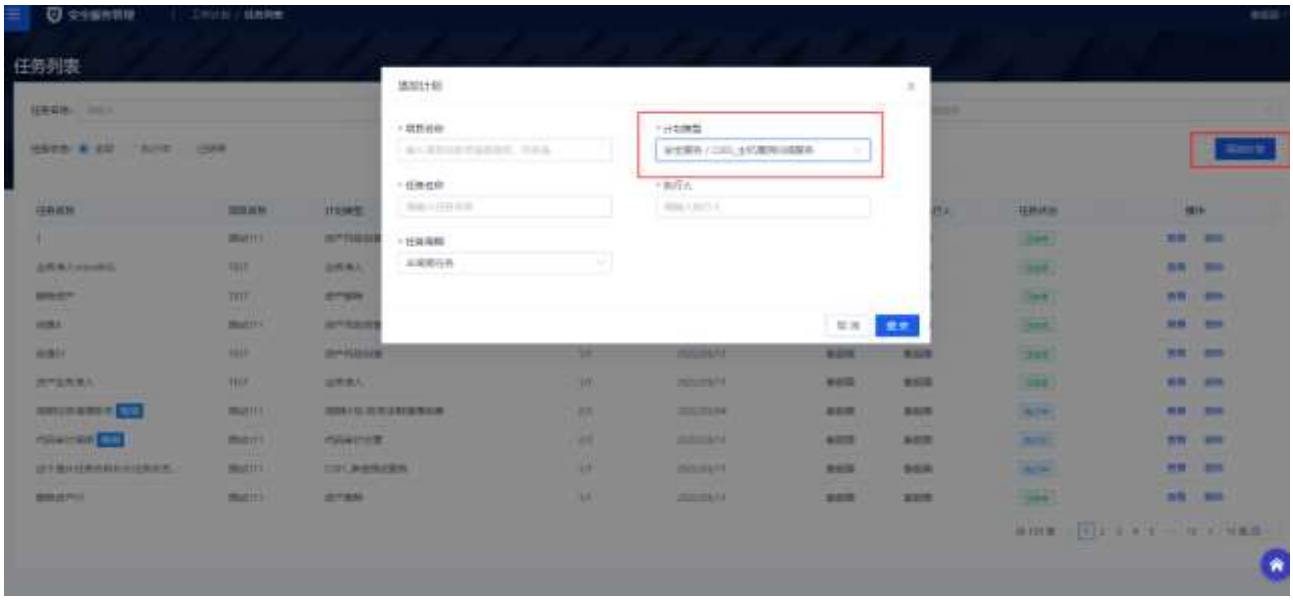
提交成功之后流程结束。



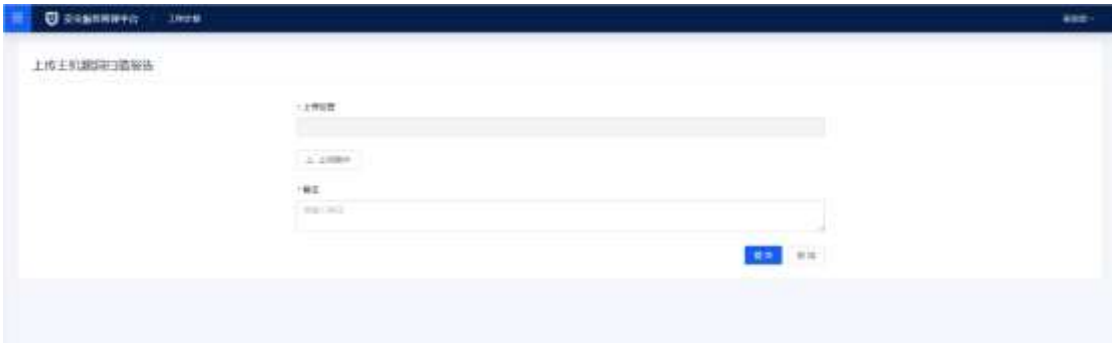
4.9.3 主机漏洞扫描服务



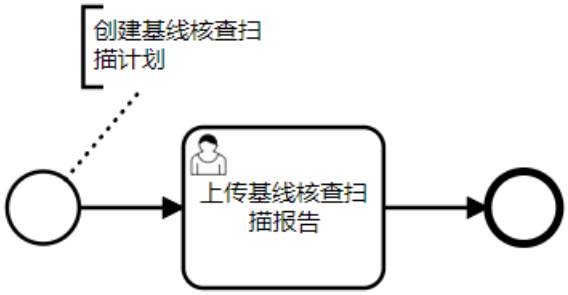
在安全服务管理模块，在安全服务阶段添加建立“主机漏洞扫描服务”计划类型的计划。



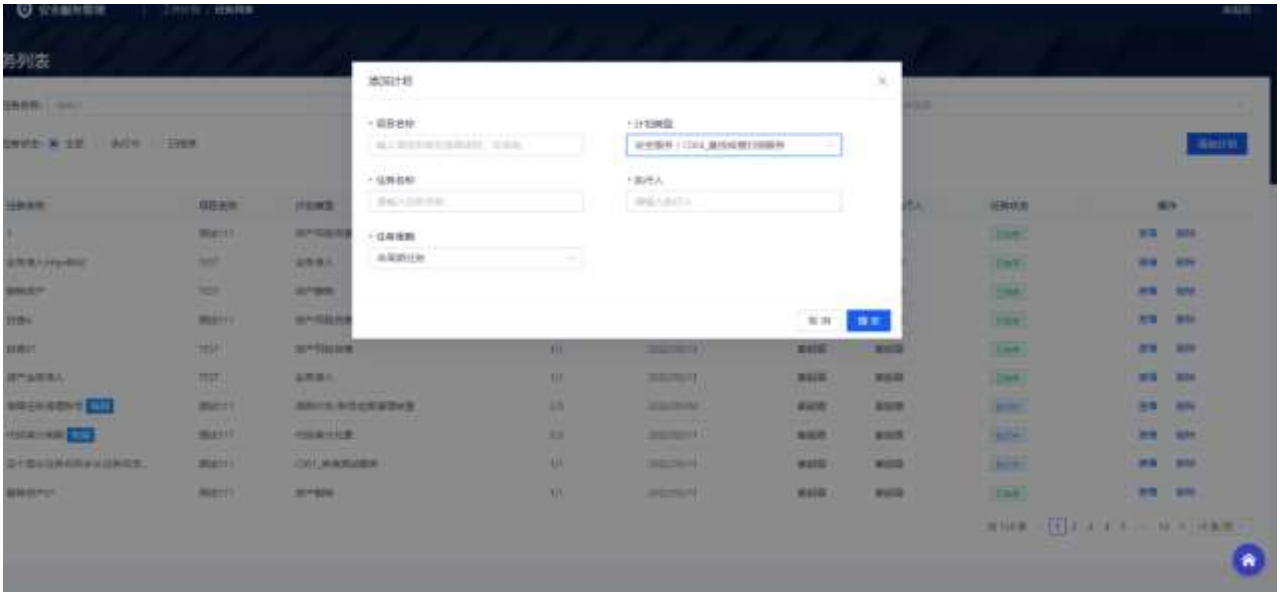
计划添加成功之后，在工作台待办事项中上传主机漏洞扫描报告的附件，输入备注，点击<提交>，提交成功之后流程结束。



4.9.4 基线核查扫描服务

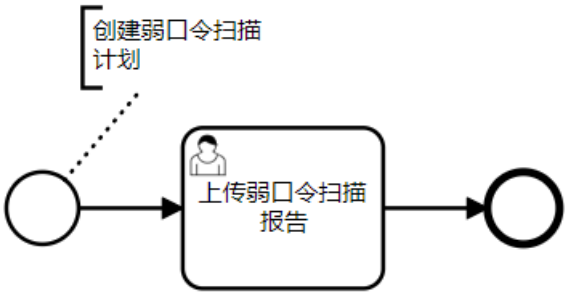


在安全服务管理模块，在安全服务阶段添加建立“基线核查扫描服务”计划类型的计划。

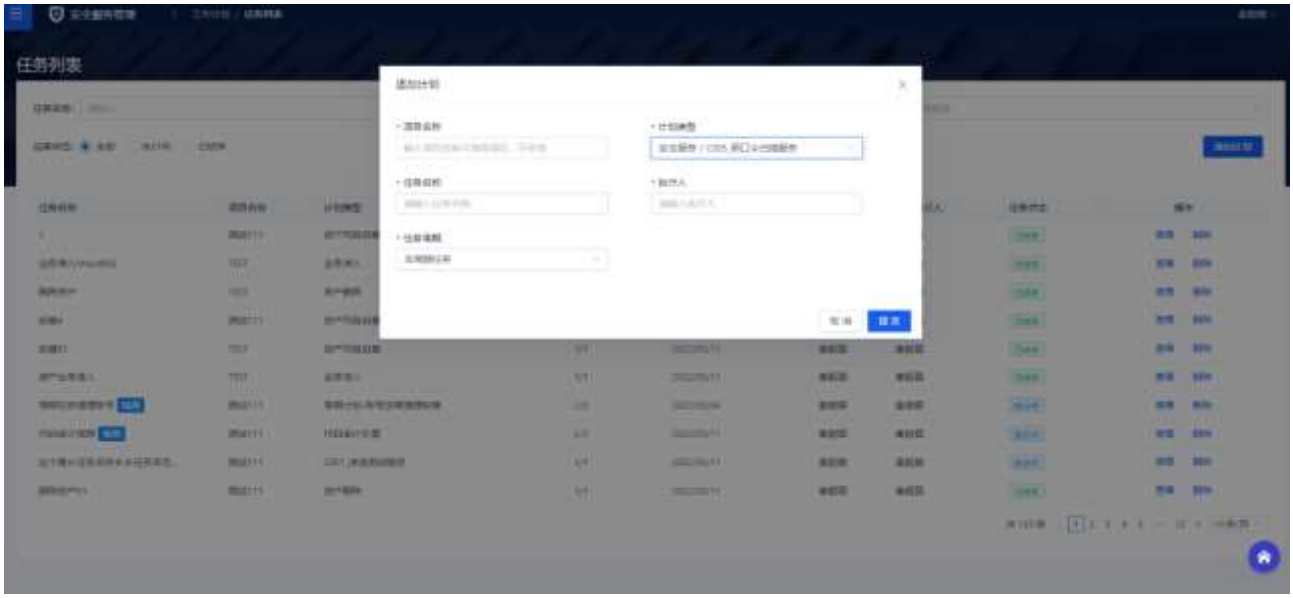


计划添加成功之后，在工作台待办事项中上传基线核查扫描报告的附件，输入备注，点击<提交>，提交成功之后流程结束。

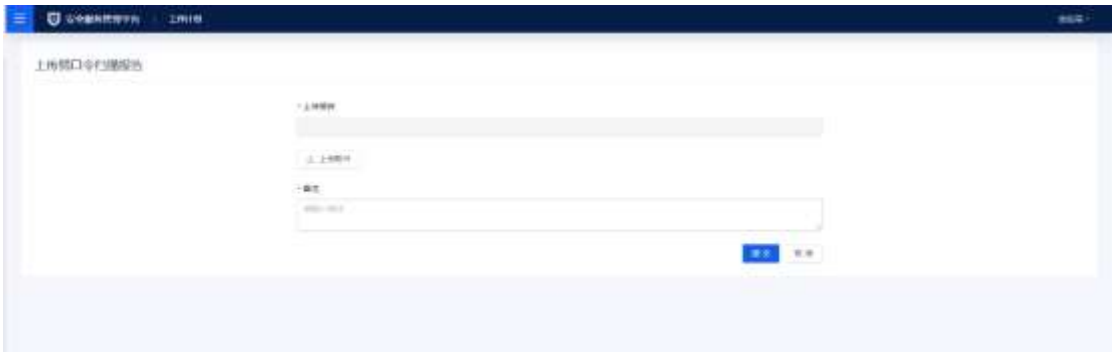
4.9.5 弱口令扫描服务



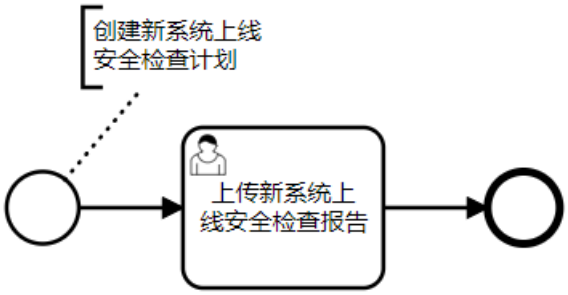
在安全服务管理模块，在安全服务阶段添加建立“弱口令扫描服务”计划类型的计划。



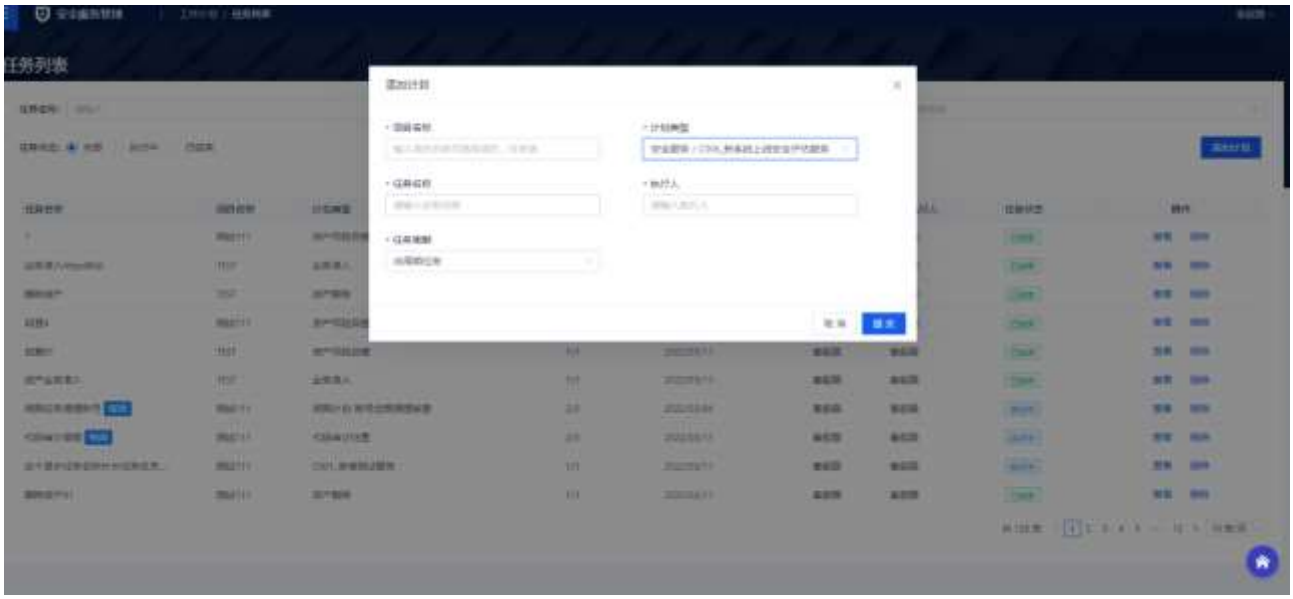
计划添加成功之后，在工作台待办事项中上传弱口令扫描报告的附件，输入备注，点击<提交>，提交成功之后流程结束。



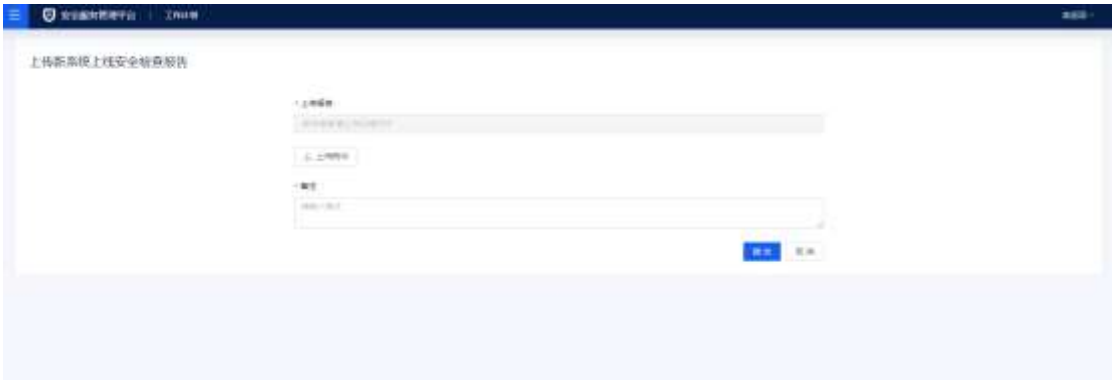
4.9.6 新系统上线安全评估服务



在安全服务管理模块，在安全服务阶段添加建立“新系统上线安全评估服务”计划类型的计划。

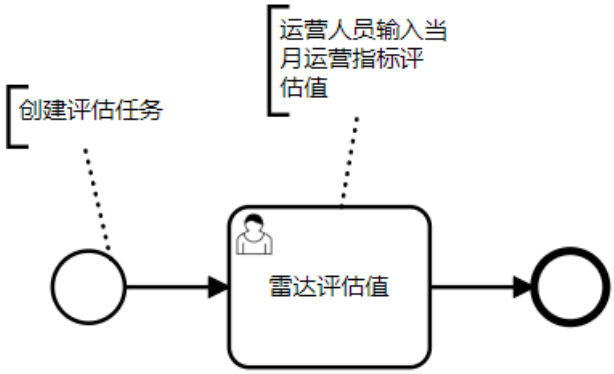


计划添加成功之后上传新系统上线安全检查报告的附件，添加备注之后点击<提交>，提交成功之后流程结束。

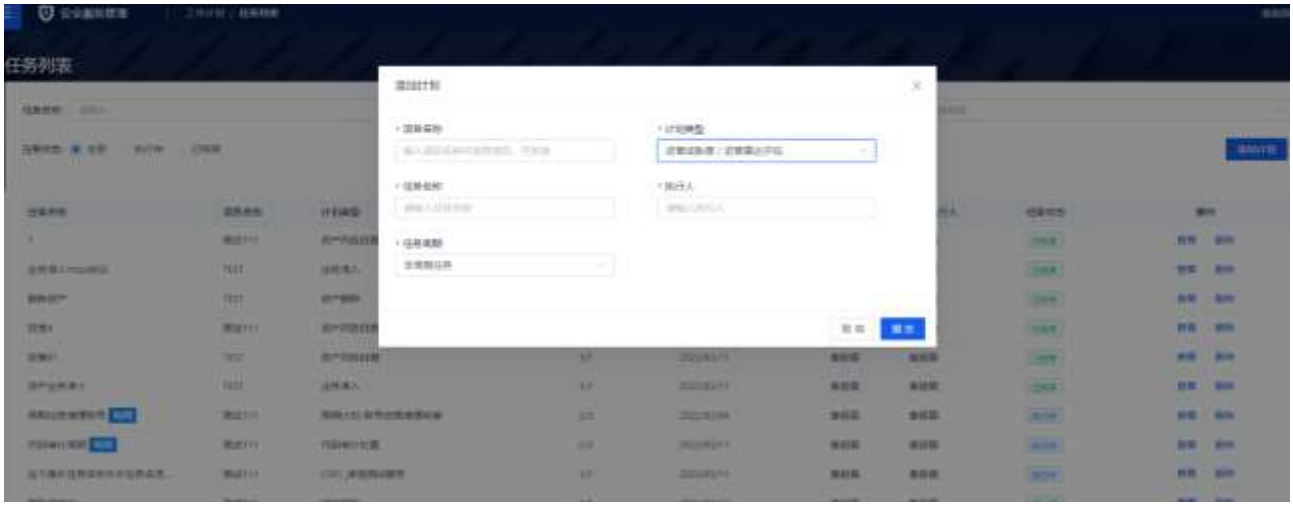


4.10 运营成熟度工作流

4.10.1 运营雷达评估



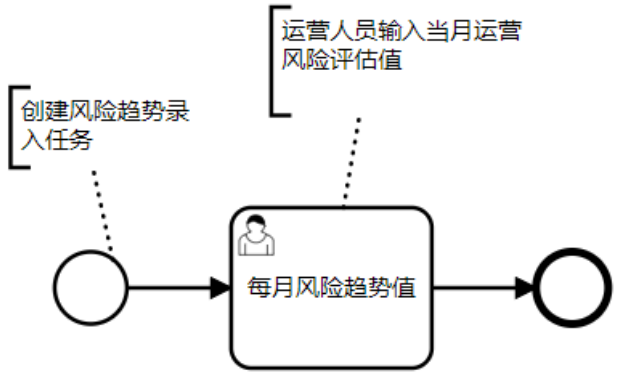
在安全服务管理模块，在运营成熟阶段添加建立“运营雷达评估”计划类型的计划。



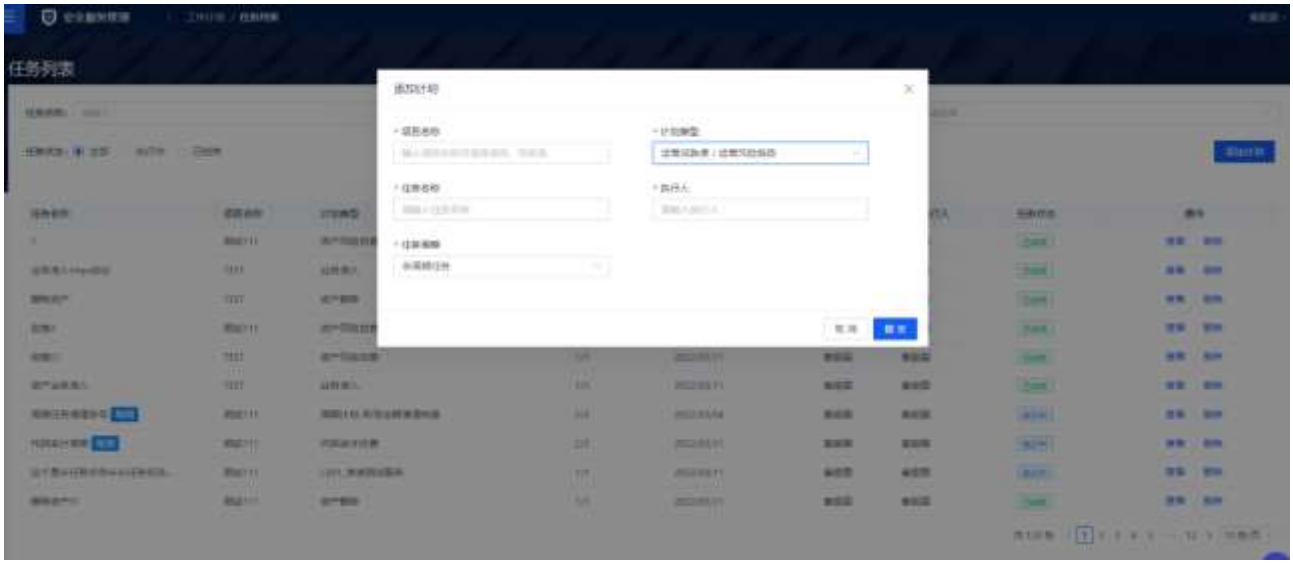
计划添加成功之后，输入雷达评估值，评估日期默认当天可自行修改，对安全运营、安全防护、暴露面监测、威胁狩猎、应急响应进行评估。评估完成之后点击<提交>，流程结束。

注意：以上填数字：高级（9～10）中级（7～8）基础（5～6）无效（0～4）。高级：满足所有关键运营服务工作，能输出交付物；中级：满足最关键、中等关键的运营服务工作，能输出交付物；基础：只满足最关键的运营服务工作，能输出交付物；无效：运营服务工作不能正常开展。

4.10.2 运营风险趋势



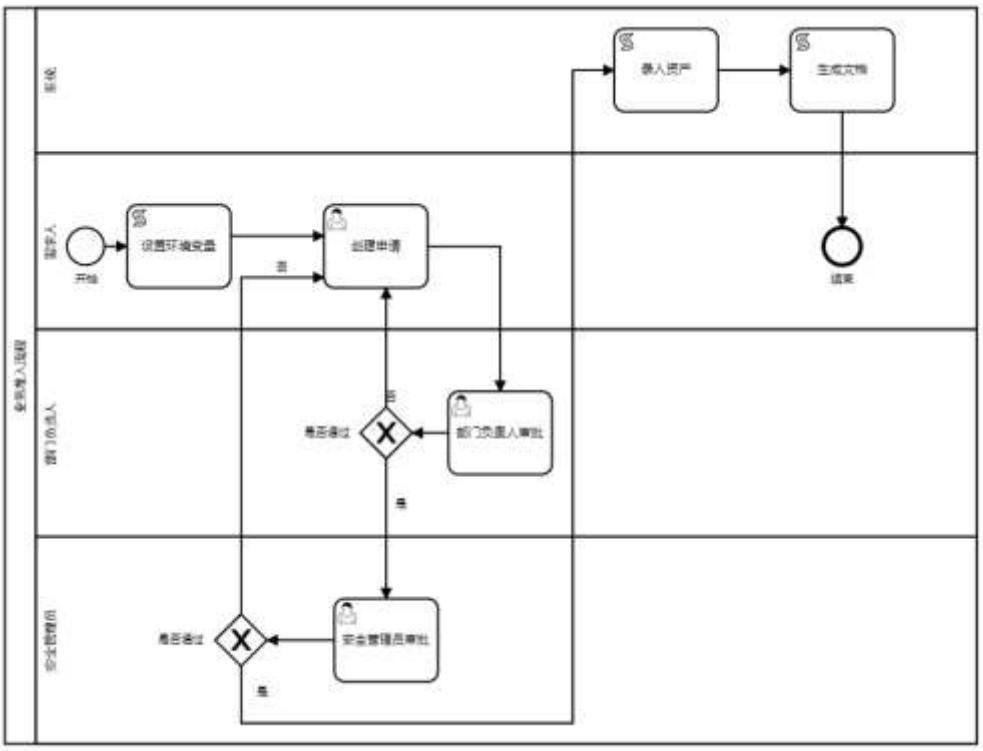
在安全服务管理模块，在运营成熟阶段添加建立“运营风险趋势”计划类型的计划。



计划添加成功之后，填写每月风险趋势值。填写完成之后点击<提交>，流程结束。

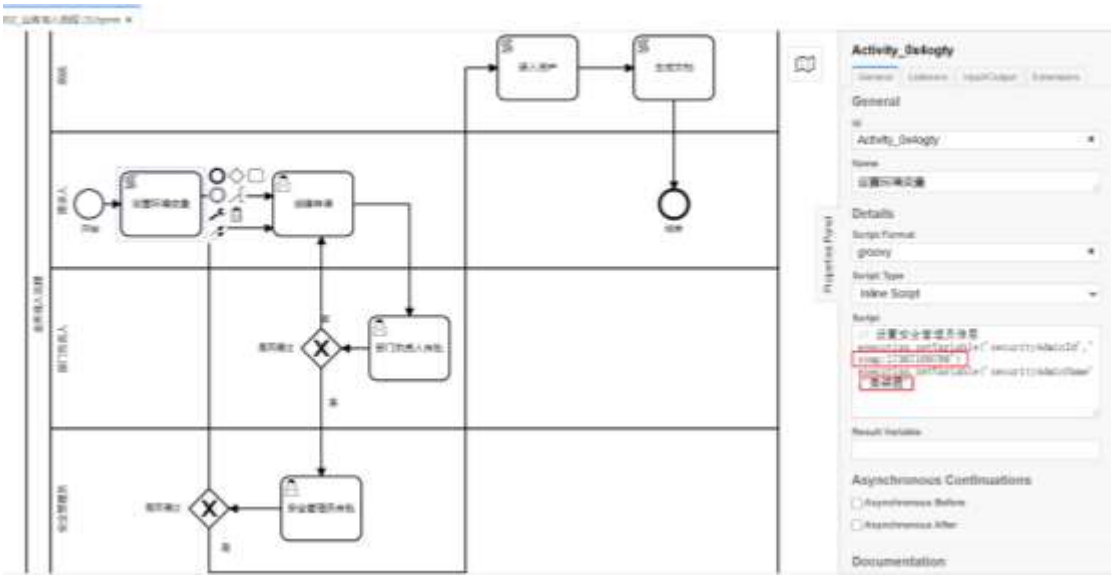
4.11 资产管理工作流

4.11.1 资产业务准入

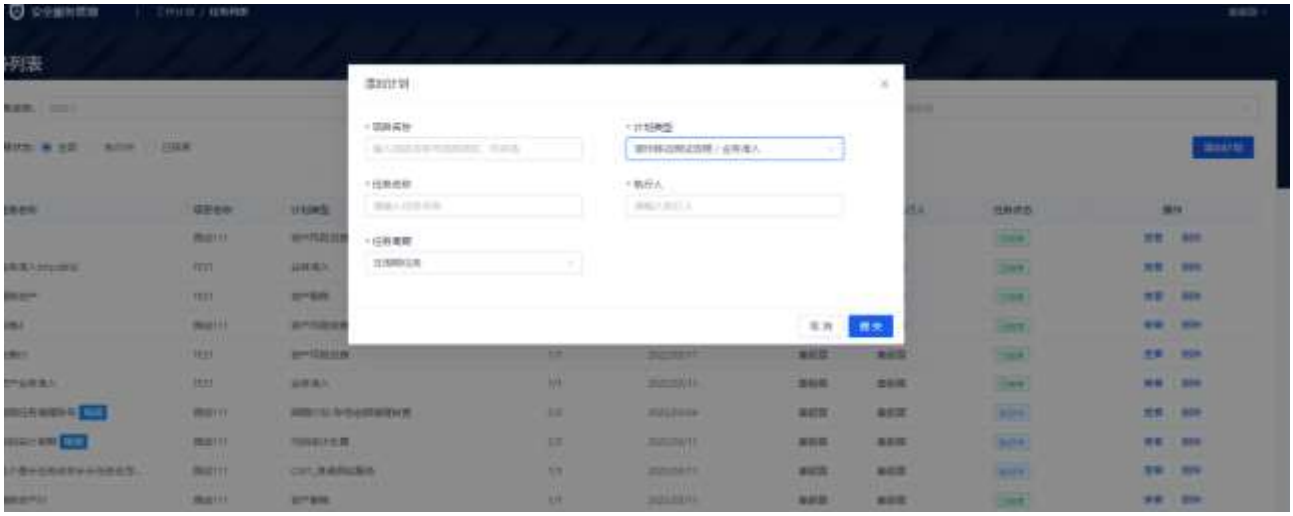


管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流，进入工作流页面。选择业务准入流程的.bpmn，点击编辑，点击工作流的第一步，设置//环境变量，//设置安全管理员信息

设置'securityAdminId','ssmp:安全管理员的手机号，'securityAdminName','安全管理员姓名'，点击部署，二次弹窗确认之后，流程部署完成。



部署完成之后，点击安全服务管理模块，由需求人在任务列表中建立“业务准入”计划类型的计划。



在工作台中的待办事项点击<创建申请>，进入申请新增资产页面。点击左侧列表右上角<+新增>，可选择新增主机资产或新增应用资产。选择需要新增的资产类型，填写相关资产的信息，点击<确定>。


申请新增资产
资产列表

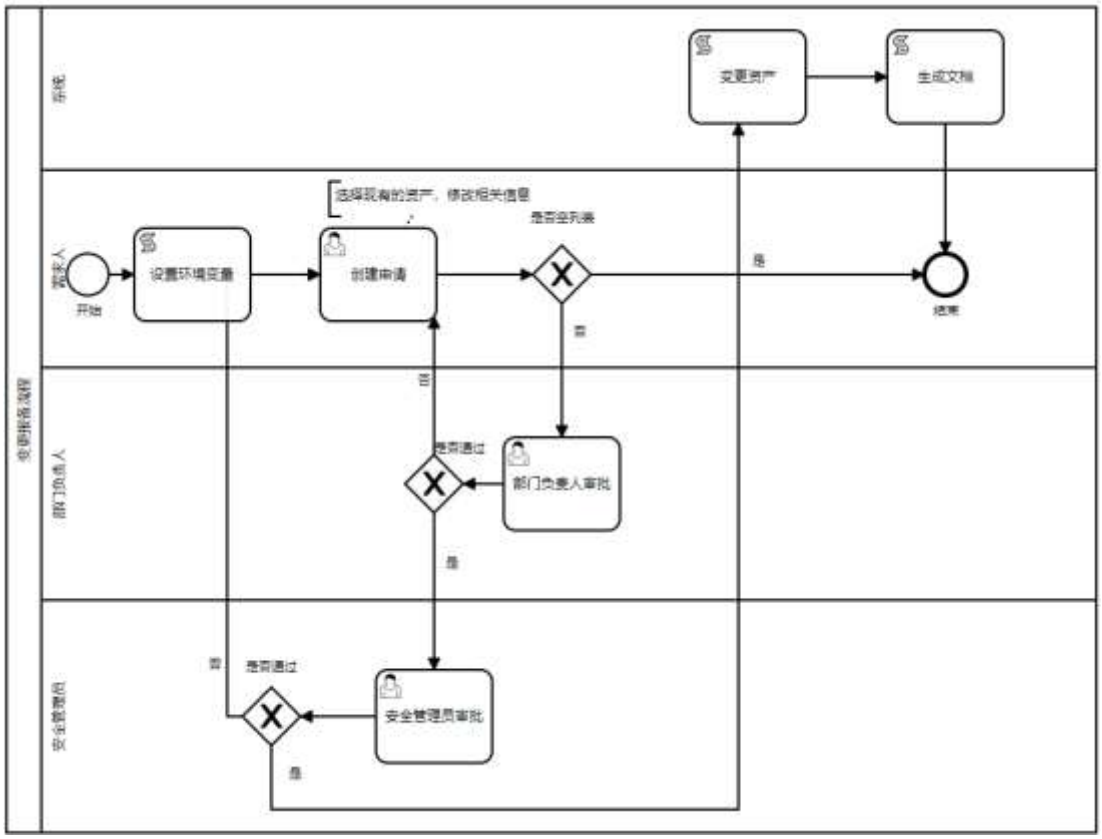

新增主机资产
* 资产名称:
* 资产责任人:
* 业务系统名称:
* 业务系统类型:
* IP地址:
* 端口:
* 设备类型:
* 设备型号:
* 操作系统:
* 设备厂商:
* 是否存在访问控制:
是
否
* 是否在线:
是
否
* 备注:
取消
确定

填写完相应资产信息之后，左侧列表展示新增的资产数据。再填写申请详情，搜索选择部门负责人，输入备注点击<提交>，弹出资产提交成功的提示。

资产提交成功之后，由部门负责人进入工作台审批报备的资产，可以查看所申请的资产列表数据。选择审批意见<通过>或<不通过>，输入备注，点击<确定>。若部门负责人审批通过，则进入下一阶段由安全管理员审批；若部门负责人审批不通过，则退回到申请阶段，由申请人重新填写并提交。

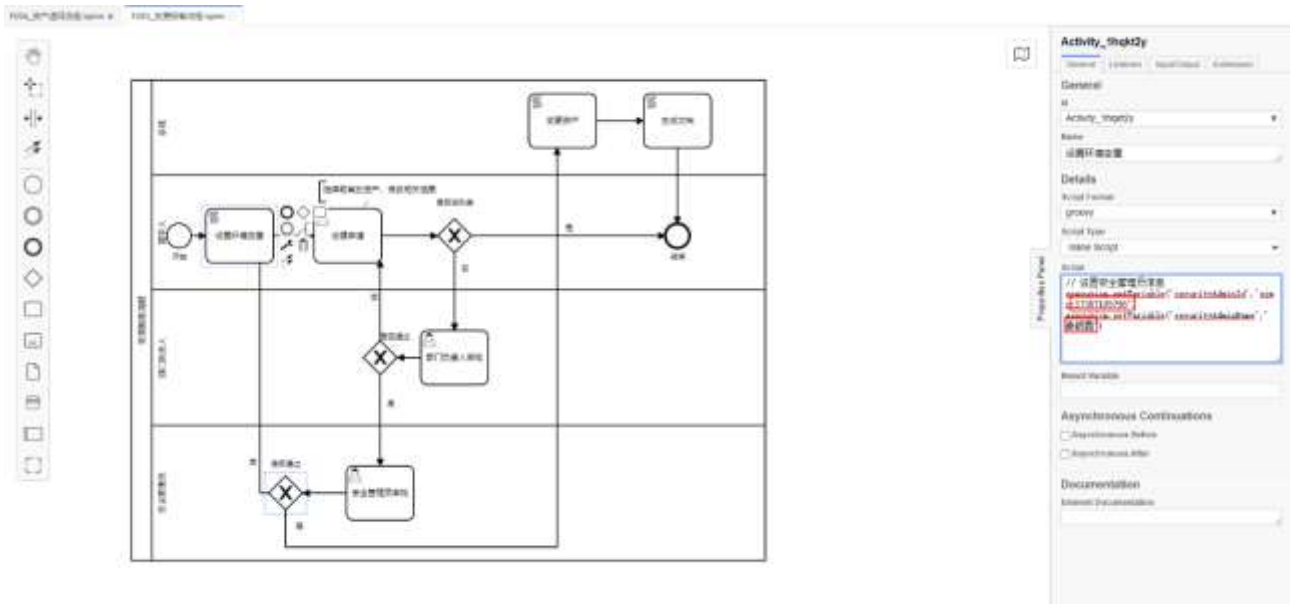
部门负责人审批通过之后，由安全管理员审批，可查看申请资产的详情。选择审批意见<通过>或<不通过>，输入备注，点击<确定>。若安全管理员审批通过，则申请的资产会录入 DAS-VM 弱点管理平台中，并生成文档，该文档需要进入我的任务中查看任务详情处下载，流程结束；若安全管理员审批不通过，则退回到申请阶段，由申请人重新填写并提交，部门负责人重新审批。

4.11.2 资产变更报备工作流



管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流，进入工作流页面。选择资产变更报备流程的.bpmn，点击编辑，点击工作流的第一步，设置//环境变量，//设置安全管理员信息

设置'securityAdminId','ssmp:安全管理员的手机号，'securityAdminName','安全管理员姓名'后保存。



部署完成之后，点击安全服务管理模块，由需求人在任务列表中建立“资产变更”计划类型的计划。

计划创建成功之后，在工作台的待办事项处，点击<创建申请>。进入申请资产变更报备流程处，资产列表分为主机资产和应用资产两个 tab 页，展示申请人名下的资产信息，分别为资产序号、资产名称、资产类型标签、资产责任人、IP/字段、是否在线、是否存在访问控制、操作项下的<变更>和<查

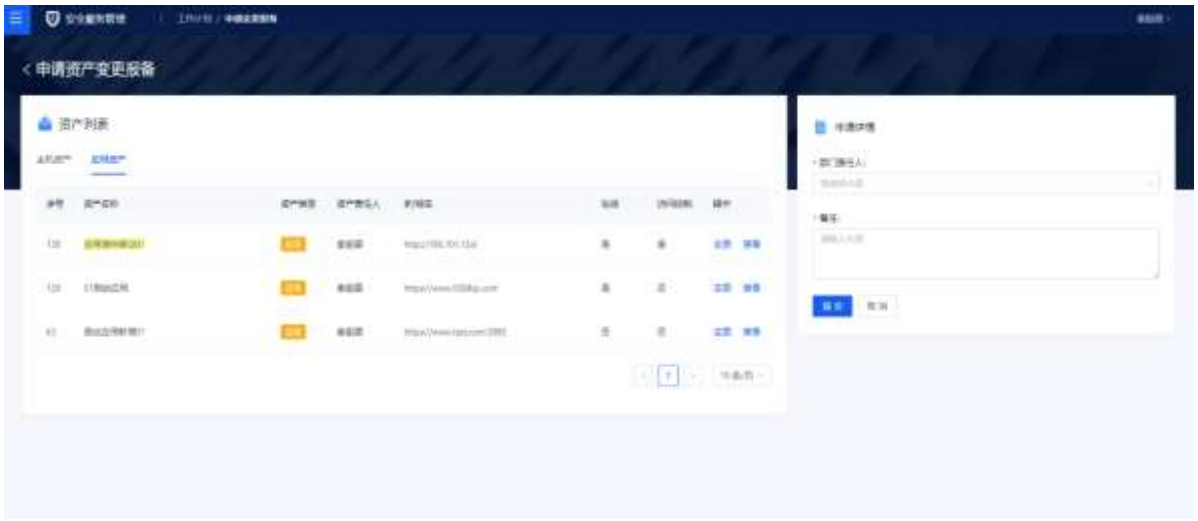
看>icon。

（1）变更主机资产

点击需要变更信息的主机资产后的<变更>icon，进入变更主机资产详情页，修改需要变更的信息。点击确定之后，在列表处该条被修改的资产名称被高亮显示，点击<查看>，可查看具体被变更的信息，且被修改的字段会高亮显示。

（2）变更应用资产

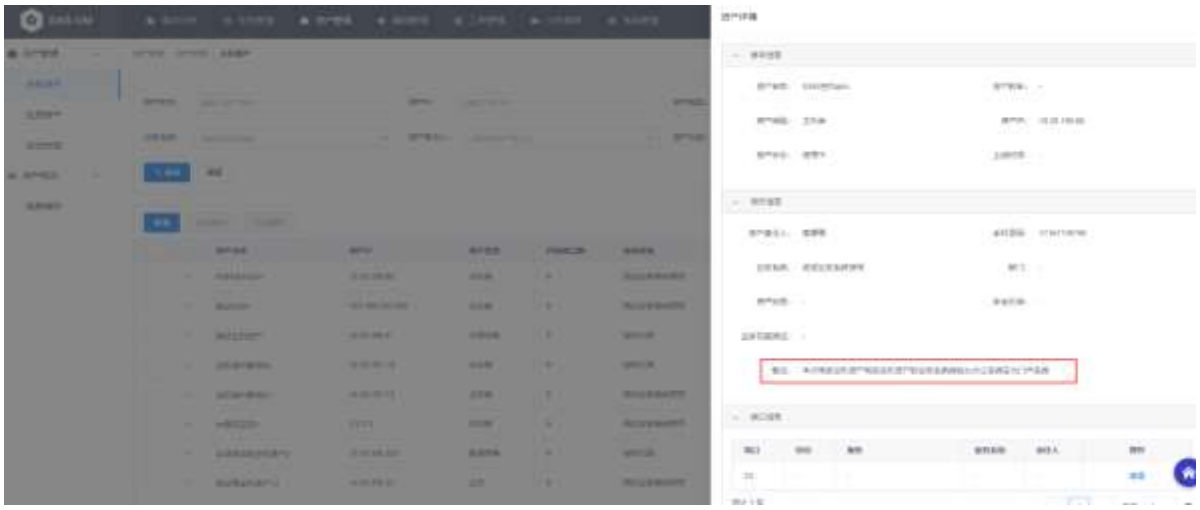
点击需要变更信息的应用资产后的<变更>icon，进入变更应用资产详情页，修改需要变更的信息。点击确定之后，在列表处该条被修改的资产名称被高亮显示，点击<查看>，可查看具体被变更的信息，且被修改的字段会高亮显示。

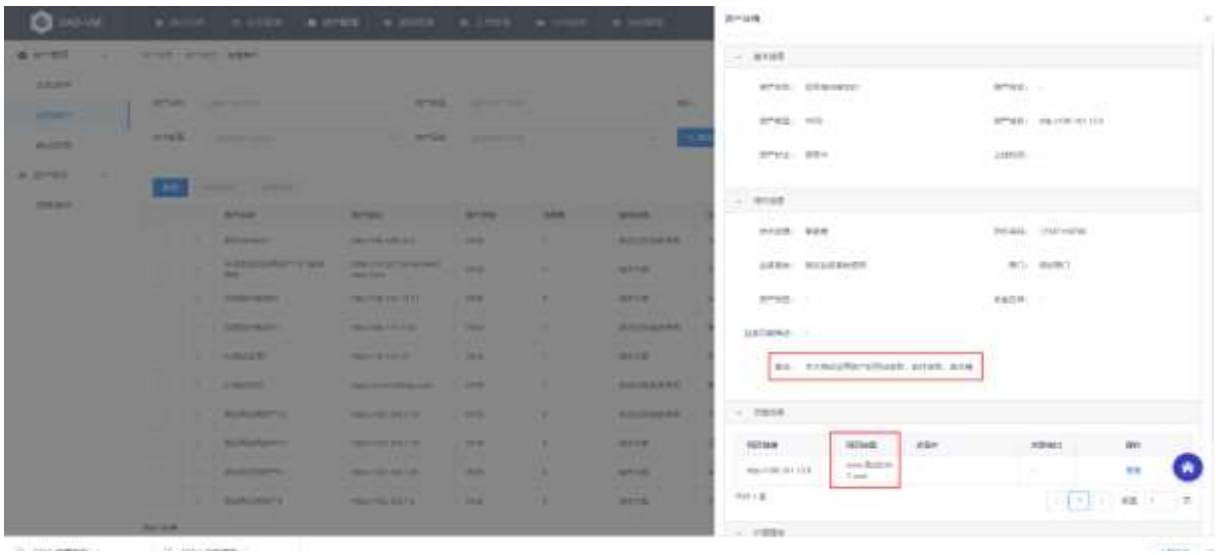


变更资产信息完成之后，填写申请详情，搜索选择部门负责人和输入备注，点击提交之后确认二次弹窗，提示资产变更报备提交成功。

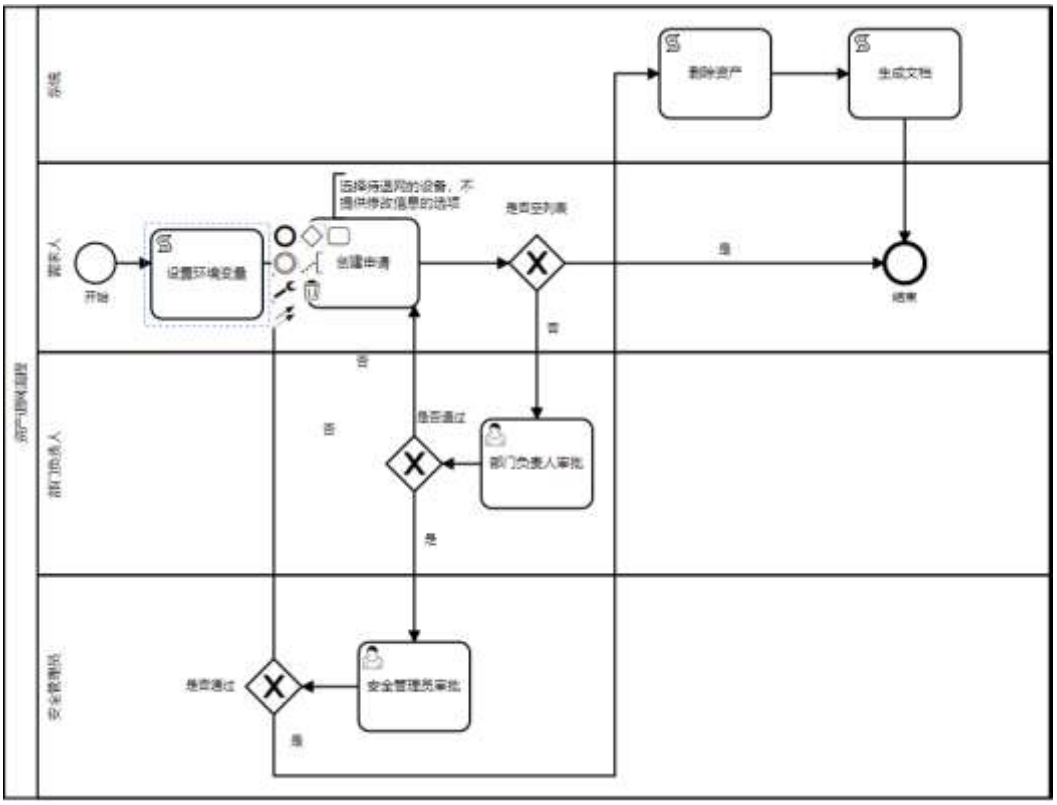
提交成功之后，进入资产变更报备审批流程，列表展示被变更过的资产详情，由部门负责人选择审批意见<通过>和<不通过>，输入备注，点击<确定>。若部门负责人审批通过，则进入下一阶段由安全管理员审批；若部门负责人审批不通过，则退回到资产变更报备阶段，被变更的资产不保存，由申请人重新填写并提交。

部门负责人审批通过之后，由安全管理员审批，可查看被变更资产的详情。选择审批意见<通过>或<不通过>，输入备注，点击<确定>。若安全管理员审批通过，则变更的资产会在 DAS-VM 弱点管理平台上同步修改，并生成文档，该文档需要进入我的任务中查看任务详情处下载，流程结束；若安全管理员审批不通过，则退回到变更申请阶段，被变更的资产不保存，由申请人重新填写并提交，部门负责人重新审批。



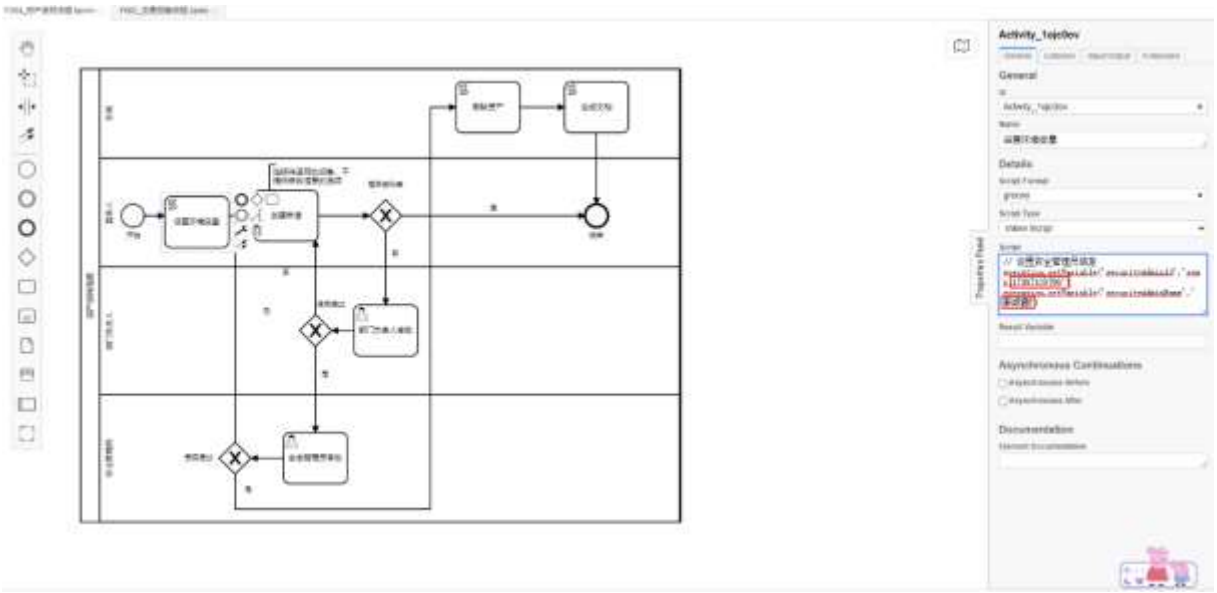


4.11.3 资产退网工作流



管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流，进入工作流页面。选择资产退网流程的.bpmn，点击编辑，点击工作流的第一步，设置//环境变量，//设置安全管理员信息

设置'securityAdminId','ssmp:安全管理员的手机号，'securityAdminName','安全管理员姓名'后保存。



部署完成之后，点击安全服务管理模块，由需求人在任务列表中建立“资产删除”计划类型的计划。

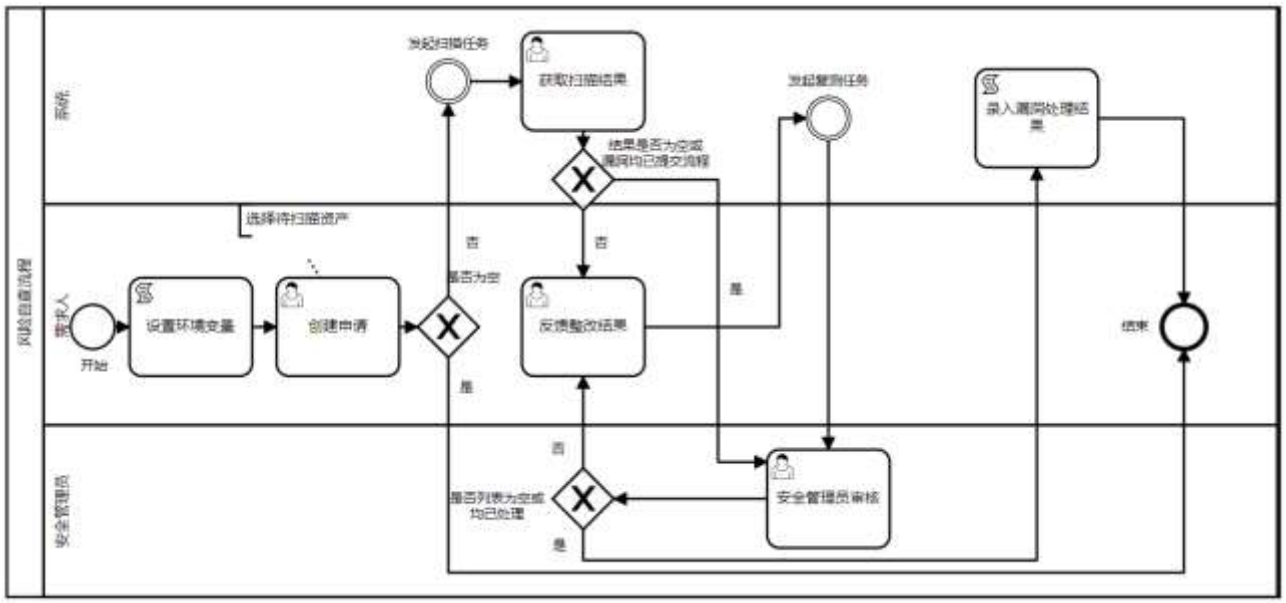
计划添加成功之后，工作台处点击<创建申请>，进入申请资产退网流程处。资产列表分为主机资产和应用资产两个 tab 页，展示申请人名下的资产信息，分别为资产序号、资产名称、资产类型标签、资产责任人、IP/字段、是否在线、是否存在访问控制、操作项下的<查看>icon。

选中要删除的资产，主机资产和应用资产需要分别选择，请不要遗漏。选择完成之后填写申请详情，搜索选择部门责任人，输入备注，点击提交，二次弹窗确认之后，弹出提示资产退网提交成功。

提交成功之后，进入资产退网审批流程，列表展示提交退网的资产详情，由部门负责人选择审批意见<通过>和<不通过>，输入备注，点击<确定>。若部门负责人审批通过，则进入下一阶段由安全管理员审批；若部门负责人审批不通过，则退回到资产退网申请阶段，由申请人重新填写并提交。

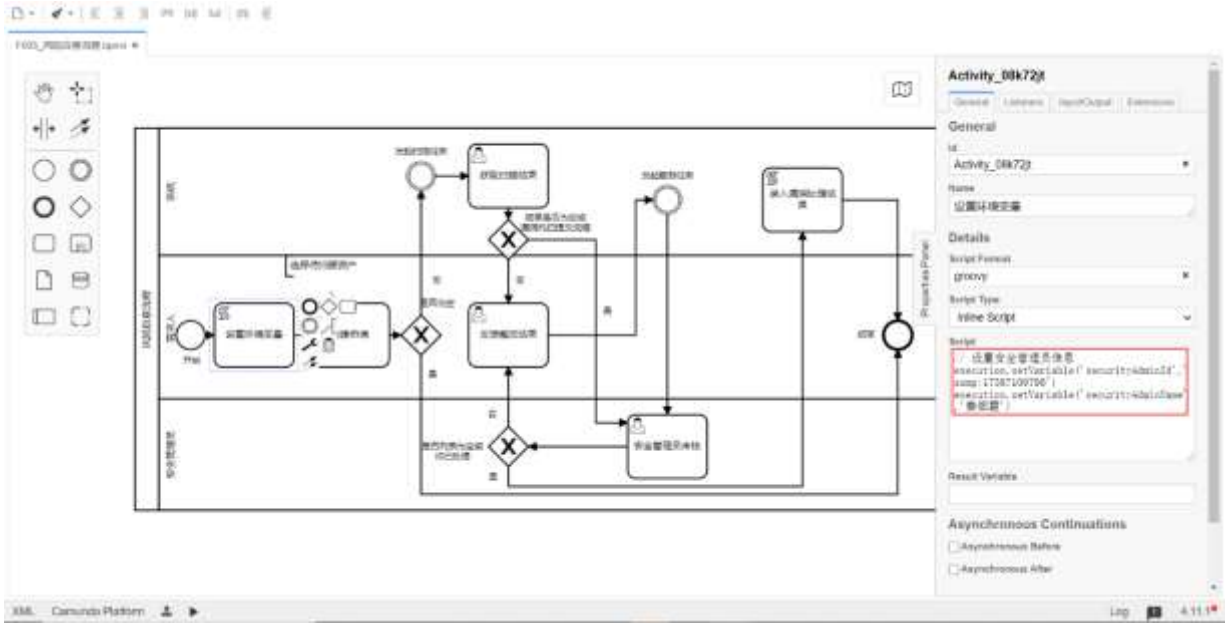
部门负责人审批通过之后，由安全管理员审批，可查看提交退网的资产详情。选择审批意见<通过>或<不通过>，输入备注，点击<确定>。若安全管理员审批通过，则提交退网的资产会在 DAS-VM 弱点管理平台上同步删除，并生成文档，该文档需要进入我的任务中查看任务详情处下载，流程结束；若安全管理员审批不通过，则退回到退网申请阶段，由申请人重新填写并提交，部门负责人重新审批。

4.11.4 资产风险自查工作流



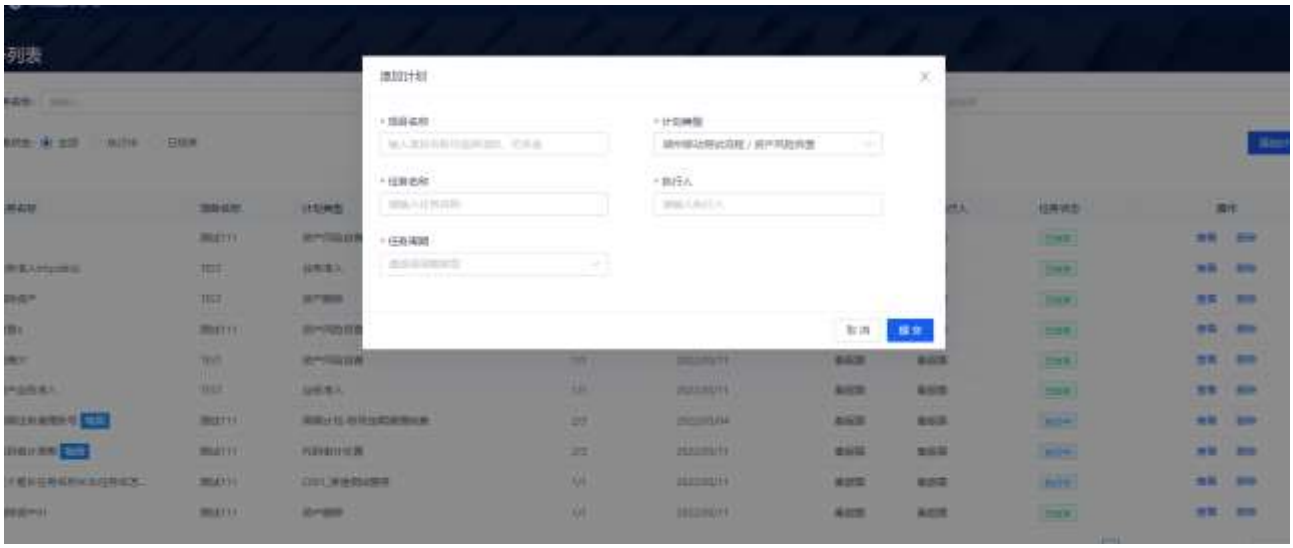
管理员和 OPadmin 进入 os 启动页,点击右上角编辑工作流，进入工作流页面。选择风险自查流程的.bpmn，点击编辑，点击工作流的第一步，设置//环境变量，//设置安全管理员信息

设置'securityAdminId','ssmp:安全管理员的手机号，'securityAdminName','安全管理员姓名'后保存。



部署完成之后，点击安全服务管理模块，由需求人在任务列表中建立“资产风险自查”计划类型的

计划。

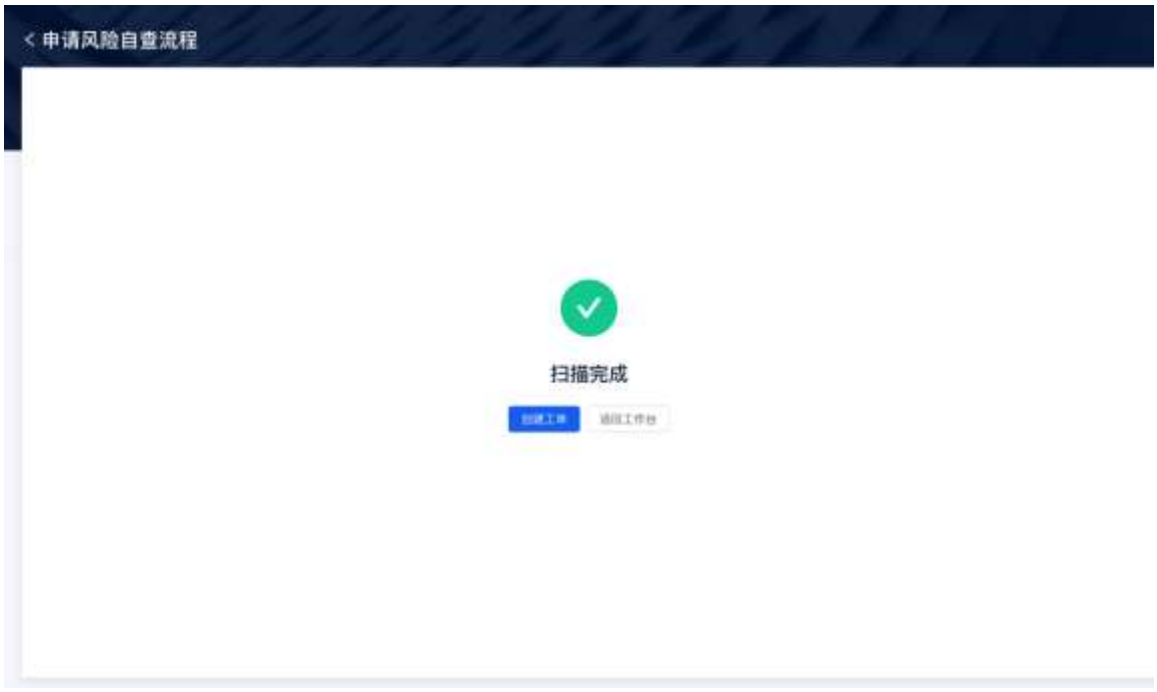


计划添加成功之后，工作台处点击<创建申请>，进入申请风险自查流程处。资产列表分为主机资产和应用资产两个 tab 页，展示申请人名下的资产信息，分别为资产名称、资产类型标签、资产责任人、IP/字段、是否在线、是否存在访问控制、操作项下的<查看>icon。

选中需要扫描的资产，输入备注，点击<提交>。二次弹窗确认之后，进入扫描页面，可返回工作台等待扫描完成。

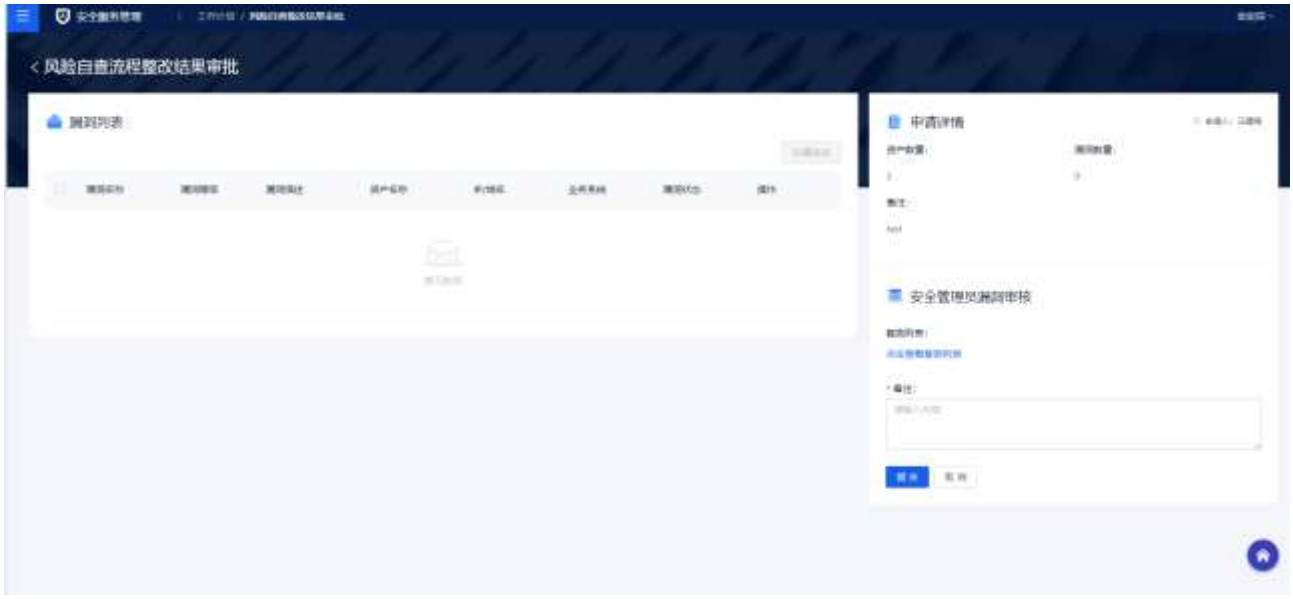
在工作台处点击<获取扫描结果>，若扫描失败，则流程直接结束。

若扫描完成，则可以点击创建工单，继续流程。

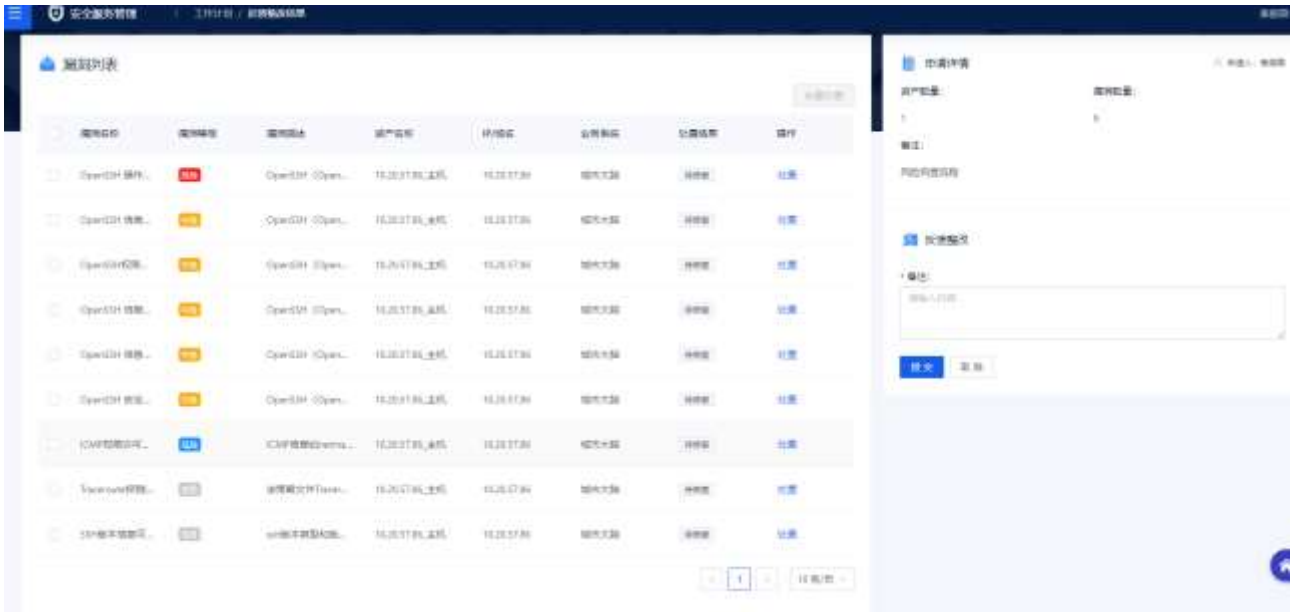


点击<创建工单>，若被扫描的资产不存在漏洞，则提示“工单创建失败，无漏洞生成”进入安全管理员审核流程。左侧展示漏洞列表，右侧展示申请详情的被扫描资产数和漏洞数。

安全管理员输入备注，点击<提交>，则流程结束，任务已完成。



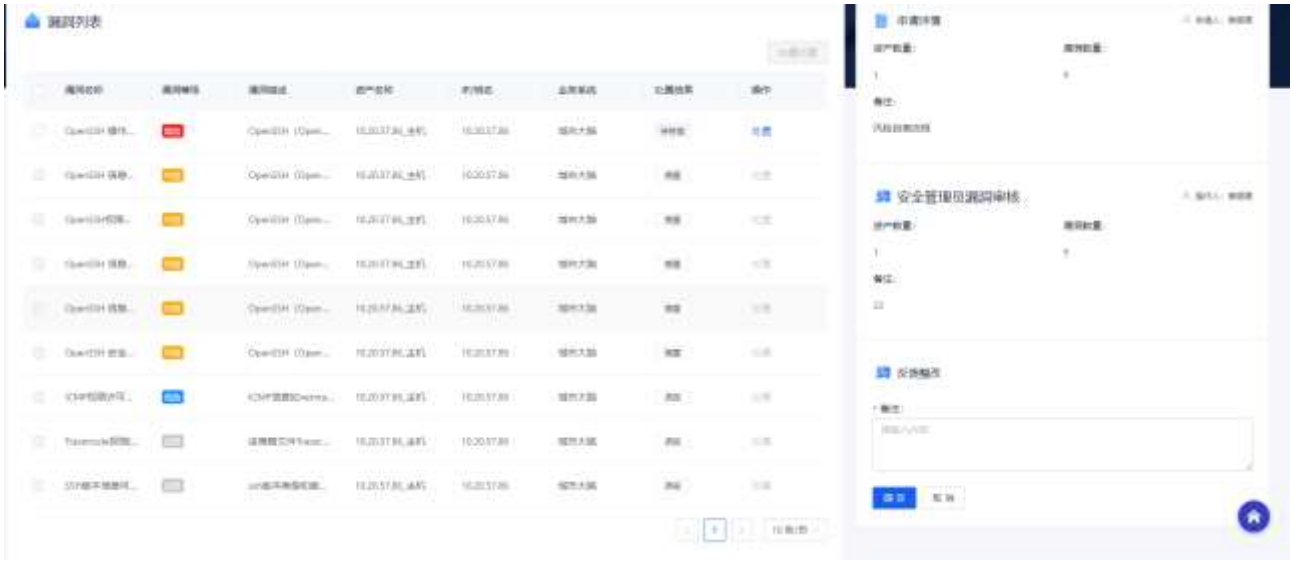
若被扫描的资产存在未修复的漏洞，提示“创建并下发工单成功”，则进入反馈整改结果流程。左侧漏洞列表展示漏洞名称、漏洞等级、漏洞描述、资产名称、IP/域名、业务系统、处置结果、操作列的处置icon，表头上方有批量处置功能。右侧展示右申请详情的被扫描资产数和漏洞数。



对漏洞进行处置，选择处置结果“整改”“搁置”“误报”，填写处置建议。当处置结果为“整改”时，漏洞状态变为待验证，当处置结果为“搁置”和“误报”，漏洞状态变为搁置和误报。填写备注，点击<提

交>。进入安全管理员漏洞审核流程，对整改的待验证的漏洞进行复测，点击复测列表可以查看任务状态。若漏洞已修复，漏洞状态从待验证变为已修复，则审核提交后流程结束；若复测该漏洞未修复，漏洞状态从待验证变为待修复，则审核提交后回退至反馈结果整改处，重新处置待修复的漏洞。

对搁置和误报的漏洞进行审核，选择审核结果“通过”和“不通过”，通过的处置结果则提交后流程结束。若未通过则回退至反馈结果整改处，重新处置漏洞。



所有漏洞都处置审核完成之后，输入备注，点击<提交>，风险自查流程结束。若存在复测未完成或未处置完成的漏洞将无法提交。