云安全中心

用户使用指南

天翼云科技有限公司

修订记录

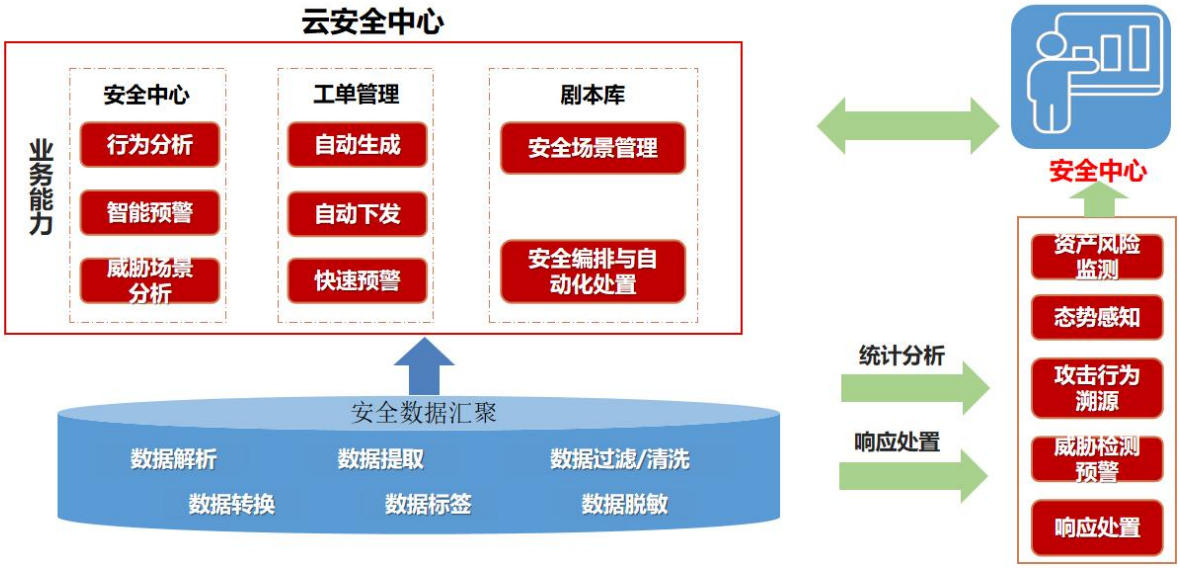
文档版本	发布日期	修改说明
01	2024/07/10	第一次正式发布。

目 录

1. 产品简介

1.1. 产品定义

云安全中心（CT-CSC，Cloud Security Center，简称云 CSC）作为用户侧的安全中心，通过对各个主机资产、安全设备告警日志等数据的采集对数据进行应用，通过安全数据的统一汇聚进行安全数据的统一融合化处理，通过平台整体整合形成数据汇聚、威胁检测、安全事件响应的业务能力，对业务进行应急处置和统计分析，满足态势感知、响应处置拦截、威胁预警和攻击行为溯源等目标，最终实现统一的前台展示，帮助用户实现威胁检测、溯源、响应的自动化安全运营闭环。



云安全中心系统主要包含应用中心、安全分析中心、安全数据汇聚以及安全响应中心四大模块。

- **应用中心**：提供各类安全数据的展示、资产以及风险管理，对各类安全指标进行统计分析，出具安全运营报告，实现安全系统数据的统一管理、统一运营。
- **安全分析中心**：实现安全分析和数据分析，构建各类威胁模型，深度检测安全威胁，智能分析辅助安全决策，感知整体安全态势。
- **安全数据汇聚**：实现各类数据源的数据收集，实现数据服务、数据存储、数据处理以及数据采集等。

- **安全响应中心**：实现工单、剧本以及插件工具的管理，安全编排与自动化响应处置，提升安全威胁检测能力和处置效率。

1.2. 产品优势

云安全中心作为用户侧的安全中心，产品优势如下：

- **安全数据全面采集**

  进行内部（资产、脆弱性）、外部（流量、日志）以及云端威胁情报接入等相关安全数据的全面采集，汇聚、分析。

- **安全威胁深度检测**

  对多源安全告警进行关联分析、规则分析、情报分析等，发现潜伏的高级持续性威胁，提升告警检出率和准确率。

- **安全态势集中监测**

  从多安全事件、攻击方向、攻击趋势、影响范围等多维度多视角进行态势呈现。

- **安全事件快速处置**

  对接联动安全防护设备，在安全事件发生时自动下发阻断策略，并在必要时下发通知预警，及时完成安全闭环。

1.3. 功能特性

云安全中心系统主要包含安全态势、资产中心、风险管理、威胁管理、分析中心、工单管理、编排响应、报表中心、集成配置以及数据源监控等功能：

- **安全态势**：依托接入云安全中心的数据，提供统一可视化界面展示网页业务的整体安全状态。
- **资产中心**：各类资产集中展示，全面汇集资产情况。
- **风险管理**：资产风险信息清晰明确，定期更新资产漏洞、弱口令等信息。
- **威胁管理**：对威胁全方位管理，提供告警概览、告警管理以及威胁检测功能，可实现各类告警灵活定制。
- **分析中心**：提供日志以及原始告警灵活查询，提供多种分析专题，为用户多角度呈现数据态势。
- **工单管理**：提供云安全中心全局工单管理能力，是各类工单进行处置的入口。

- **编排响应**：是企业内部定制或者沉淀的知识经验，也是安全应急响应通用事件处理的“模板”。不论是自动化的编排，还是人工的编排，都可以通过“安全剧本”来进行表述。
- **报表中心**：通过周期性的报表任务和可定制的报表模板承载各类个性化报表的展示和生成。
- **集成配置**：数据集成一键配置，实现所配即所得。
- **数据源监控**：为用户提供各类数据源的展示和基本信息统计。

1.4. 应用场景

场景一：安全运营场景

为中小企业提供专业的安全运营团队，为用户提供专业的安全运营支撑。为用户提高各类威胁检测率，降低误报率。在一定程度上降低用户在安全运营上的成本，提升了安全运营的灵活性。

方案优势

- 减少无效告警：通过不同安全产品之间的数据关联，减少孤立的数据点，降低无效告警信息的产生。
- 提升告警精准度：提高告警信息的精准度，使得安全团队能够专注于真正重要的安全事件，从而提升整体运维效率。
- 高效统一的安全运营工具：用户云上的安全工具互相独立，每种工具只能有限防范几种常见攻击。云安全中心提供统一的安全运营平台，帮助用户高效统一地进行安全运营。

场景示意图

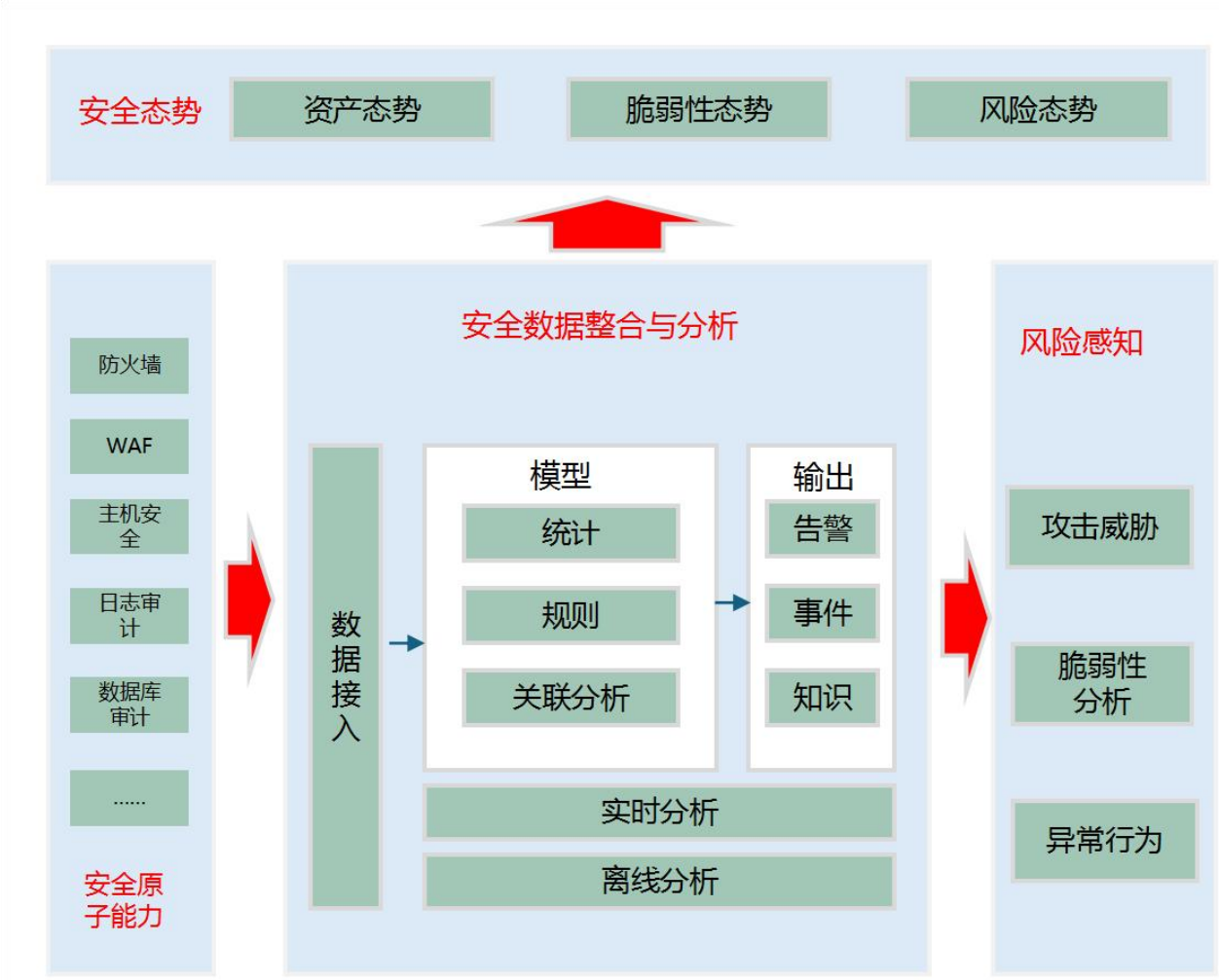
场景二：安全合规场景

满足国家行业监管要求，帮助企业业务安全合规。帮助企业明确安全目标，系统化构建信息系统安全，降低安全隐患和攻击风险，向客户及利益相关方展示安全承诺，增强客户、合作伙伴及利益相关方的信心。

方案优势

- 全局数据整合：将不同安全能力产生的数据进行整合和分析，使企业能够全面掌握安全态势。
- 全局统一视角：整合各安全措施后，企业能够从全局视角监控和管理安全状况，提高对整体安全态势的把握。
- 全局协同效应：各安全能力之间实现有效协同，形成统一的防护体系，增强整体防御能力。
- 云安全中心依托安全服务订阅模式，为企业提供个性化服务套餐订阅，事前预防，事发检测分析，事中快速响应，事后溯源。遵从合规性要求，监控预防，实时知悉系统健康情况，“御敌于城门之外”

场景示意图



场景三：攻防实战场景

随着逐步接受和了解公有云的安全性，企业用户的重点转向了公有云‘内部’的安全。根据常见的责任分担模型，云运营商主要负责云基础设施的安全，而客户则负责云中数据和应用的安全，针对云中数据和应用的攻防实战就显得尤为重要了。

方案优势

- 提升数据关联性：通过关联和整合海量数据日志，企业可以提升运维效率，实现更加精准的监控和管理。
- 实时分析：利用先进的安全算力，实时关联和分析海量信息，有效提高运维的响应速度和决策能力。
- 高级威胁的有效发现：借助全局数据的支持，企业可以更有效地检测和应对复杂的高级威胁，提升威胁发现能力。

- 实战效果好：当前网络威胁的数量、复杂性，网络安全工作负载的增加以及攻击面的增长，专业人员经常抱怨依赖手动流程和大量的点工具来进行威胁检测和响应。云安全中心具备全局视野，多年安全维护经验，帮助用户实现各类威胁的检测和响应，能满足用户的实战诉求。

场景示意图

1.5. 产品规格

云安全中心为所有用户带来的主功能是一致的，产品实例主资源目前有标准版一个版本。版本详细规格描述见“主资源规格说明”。

另外，标准版主资源支持选择购买扩展资源，用户可以通过购买额外的扩展资源，以满足更多日志分析量以及安全态势大屏等服务的需求。扩展资源详细规格说明见“扩展资源规格说明”。

主资源规格说明

主资源目前支持标准版，版本规格说明见下表：

版本	即时通知服务	日志分析量
标准版	2000 条/月	40G/月

说明：

- 标准版包含的即时通知服务为每月 2000 条，月初余量进行重置，上月未用完的不进行转结。
- 标准版包含的日志分析量为每月 40G，月初余量进行重置，上月未用完的不进行转结。

扩展资源规格说明

扩展资源与主资源绑定，到期时间与主资源一致。

- 云安全中心日志分析量：日志分析量的起购单位为 50G，即每次购买的日志分析量为 50G 的整数倍。

  说明：

  用户日志分析量可以转结（上月余下的扩展资源部分的分析量可以累加到下个月），购买后，失效日期和主产品保持一致。

- 云安全中心态势大屏：提供态势大屏直观展示用户当前的告警态势以及安全成果态势，态势大屏只需购买一次。

2. 计费说明

2.1. 计费模式

云安全中心支持包年包月付费模式。

标准资费

云安全中心根据开通实例时选购的主资源版本、扩展资源数量、购买时长生成预付费账单。

计费项		标准价格
主资源（标准版）		1600 元/月
扩展资源	日志分析量	0.45 元/GB/月
	态势大屏	4500 元/月

说明：

一个账号仅可购买一个主资源版本和态势大屏，日志分析量可以重复购买。

扩展资源规格说明

- 云安全中心日志分析量：日志分析量的起购单位为 50G，即每次购买的日志分析量为 50G 的整数倍。
- 云安全中心态势大屏：购买后，失效日期和主产品保持一致。

说明：

- 扩展资源不支持独立购买，必须在购买主资源的基础上进行叠加购买。
- 扩展资源购买后与主资源绑定，资源到期时间与主资源一致，不支持单独退订或单独续订。
- 日志分析量转结上月未使用的余量，套餐初始赠送日志分析量每月刷新（该部分不转结）。
- 日志分析量优先使用初始赠送部分。

2.2. 升级扩容

开通了云安全中心实例后，可根据实际使用需求购买日志分析量扩展资源和态势大屏扩展资源。

前提条件

已购买云安全中心实例。

规格限制

- 态势大屏扩展资源只可购买一次。
- 日志分析量扩展资源的购买资源最小单位为 50G，即扩展资源需要购买 50G 的整数倍。

约束条件

- 同一账号在同一个区域只能开通一个云安全中心实例，对应一个服务版本。
- 云安全中心实例生效期间，支持升级购买的服务版本以及扩增扩展资源数量，但不支持降级。
- 扩展资源与主资源绑定，到期时间与主资源一致，不支持单独续订、退订。

系统影响

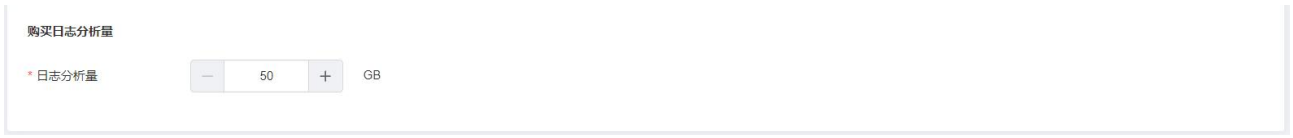
购买扩展资源时，原已启用的服务不会暂停，对业务无任何影响。

购买扩展资源

若当前实例还未购买某类扩展资源，则需单独购买。

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全>云安全中心”，进入产品服务页面。
3. 在左侧导航栏，选择“已购资源”。

4. 选择需要购买的扩展资源，“日志分析量扩展资源”、“态势大屏扩展资源”。



说明：

- “日志分析量扩展资源”可以设置购买数量，固定为 50G 的整数倍。
- “态势大屏扩展资源”为固定 1 个。

5. 设置扩展资源数量。

6. 在页面下方确认配置费用，阅读《云安全中心服务协议》并勾选“我已阅读，理解并接受《云安全中心服务协议》“，单击“立即购买”。
7. 在订单页完成订单确认并支付，付费成功后，购买扩展资源规格生效。

2.3. 续订

为避免云安全中心实例到期后，服务自动停止，需要在实例到期前进行手动续费，或设置到期自动续费。

到期说明

服务到期后，如果没有按时续费，平台会冻结服务，但用户配置信息会提供 15 天的保留期。

- 保留期内，平台会冻结云安全中心的服务，用户配置的各类数据会继续生效，但用户无法访问云安全中心。
- 保留期满，用户若仍未续费，平台会清除实例资源，用户原有的配置信息将会被删除，同时云安全中心将不再获取第三方日志、用户云上资产等信息。

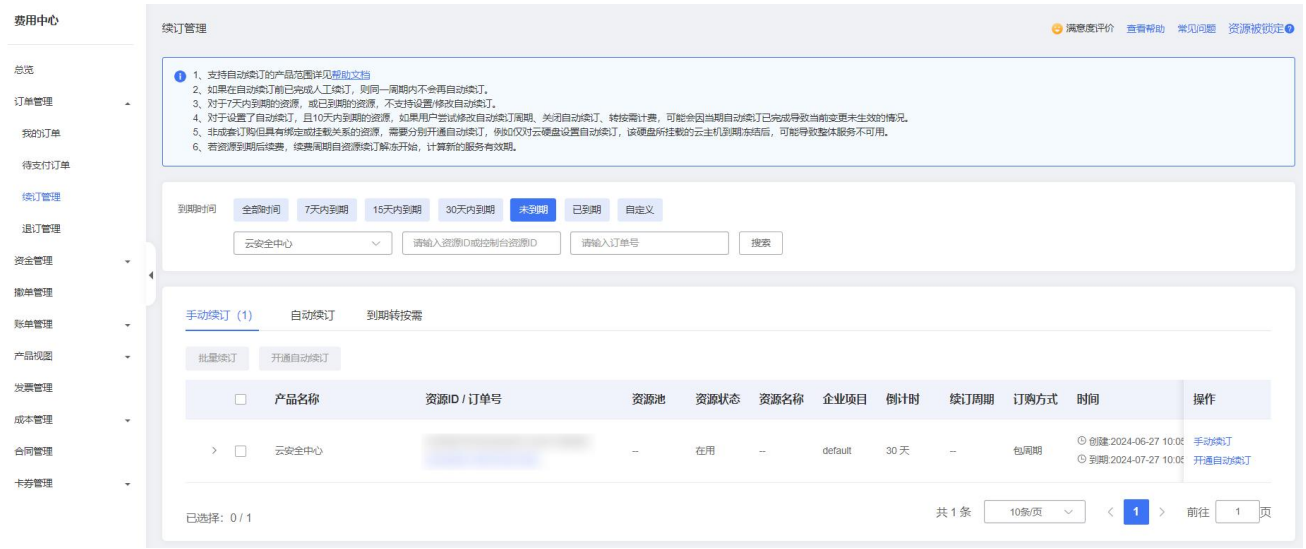
续订说明

- 在购买云安全中心时，支持勾选并同意“自动续订”，则在服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费；
- 若购买云安全中心时勾选了“自动续订”，系统将会默认设置续费周期：按月购买，自动续费周期默认为 3 个月；按年购买，自动续费周期默认为 1 年。如需要修改自动续费周期，可进入天翼云“费用中心”，进入“订单管理 > 续订管理”页面，在资源页面找到待修改自动续订的资源，单击操作列的“修改自动续订”，拖动“续订周期”可修改自动续订周期。

手动续订

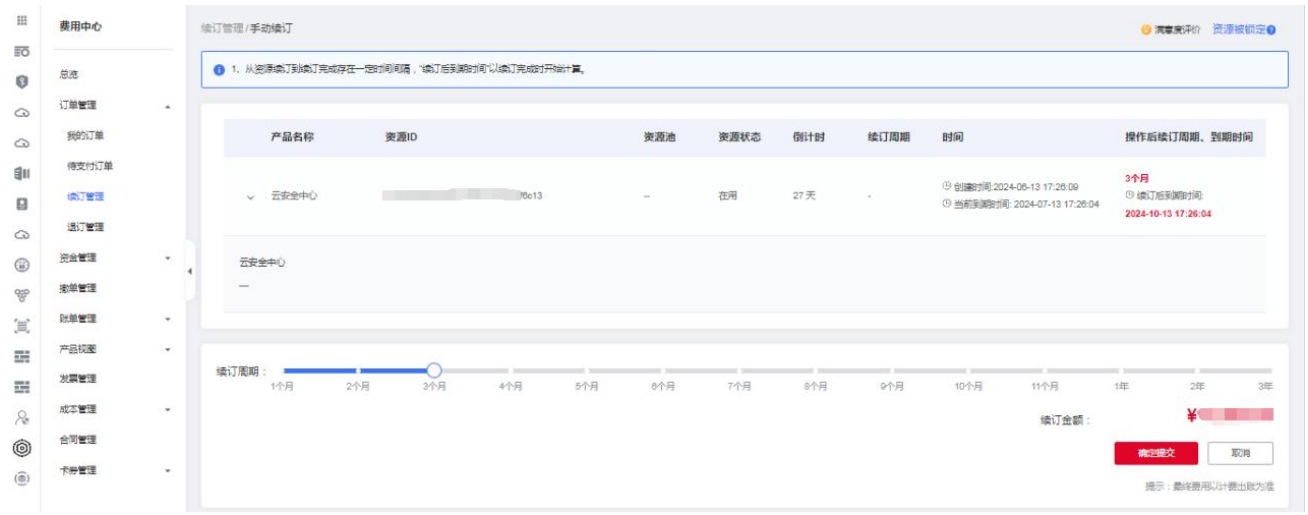
1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全>云安全中心”。
3. 进入产品服务页面，选择“已购资源”。

4. 在当前实例信息展示界面，点击“续订”。
5. 在“续订管理”操作界面，可以根据需要进行“手动续订”或者“开通自动续订”。



6. 点击“手动续订”，进入手动续订页面。

7. 选择续订时长，确认续订金额后，单击“确定提交”提交续订订单。



8. 在订单页完成订单确认并支付，付费成功后，续订生效。

自动续订

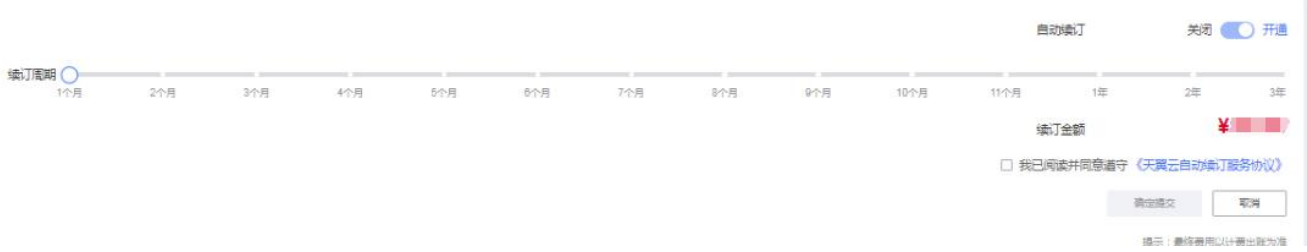
1. 云安全中心支持在购买实例时，同步开通“自动续订”。

2. 若开通实例时未开启自动续订，用户也可在开通后，通过天翼云“费用中心 > 订单管理 > 续订管理”，实现自动续订启用。

   a. 进入天翼云“费用中心 > 订单管理 > 续订管理”页面。

   b. 设置查询条件，可综合利用到期时间、产品类型、是否开通自动续订查询资源。

c. 定位到云安全中心资源订单后，点击操作列的“开通自动续订”，设置“自动续订周期”，仔细阅读《天翼云自动续订服务协议》，如果同意全部约定，则勾选“我已阅读并同意遵守《天翼云自动续订服务协议》的约定”，单击“确定提交”。

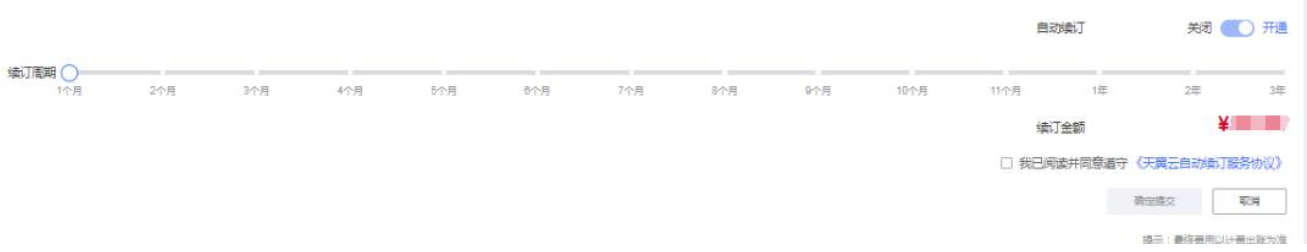


3. 修改自定义续订周期。

a. 进入天翼云“费用中心 > 订单管理 > 续订管理”页面。

b. 设置查询条件，可综合利用到期时间、产品类型、是否开通自动续订查询资源。

c. 定位到云安全中心资源订单后，点击操作列的“修改自动续订”，拖动“续订周期”可修改自动续订周期。



4. 修改自定义续订开关。

a. 进入天翼云“费用中心 > 订单管理 > 续订管理”页面。

b. 设置查询条件，可综合利用到期时间、产品类型、是否开通自动续订查询资源。

c. 定位到云安全中心资源订单后，点击操作列的“修改自动续订”，点击“自动续订”后方的关闭/开通按钮，单击“确定提交”。

2.4. 退订

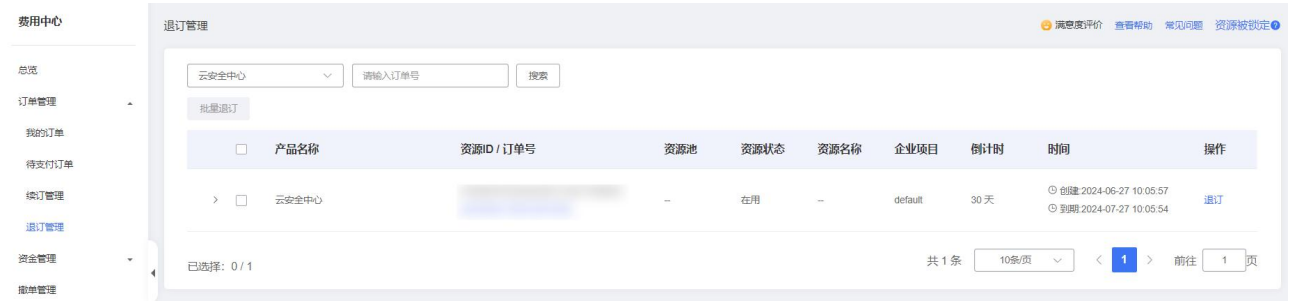
云安全中心支持退订，可通过云安全中心控制台界面、天翼云管理中心发起并完成退订操作。

退订说明

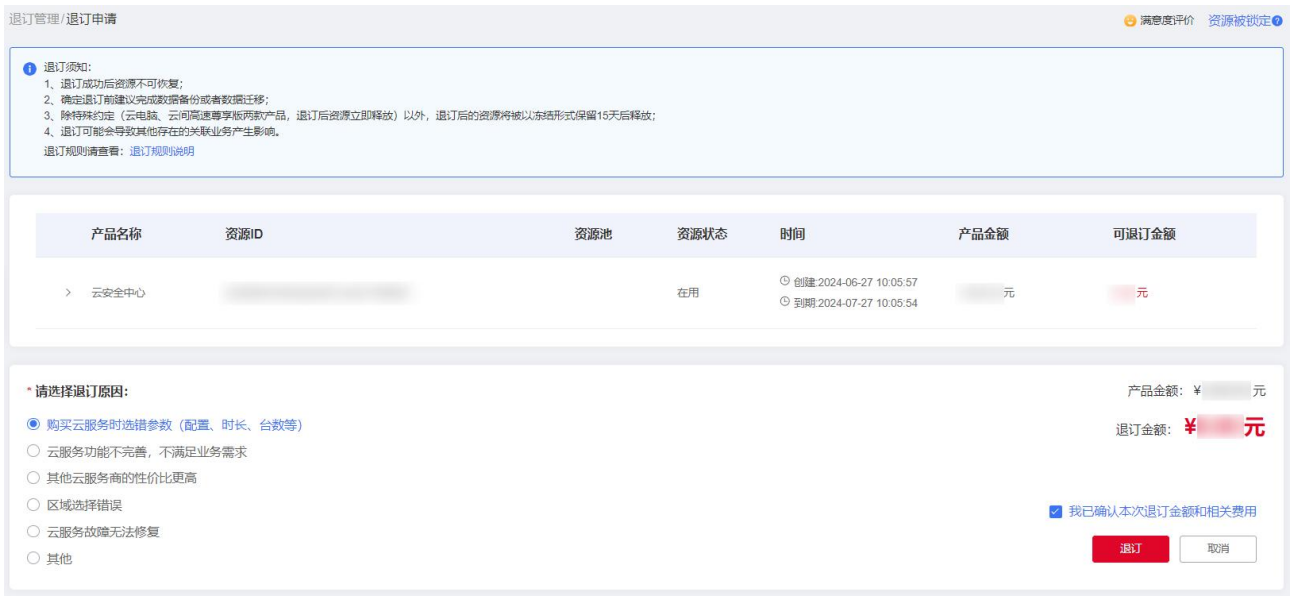
- 云安全中心退订后，主资源及扩展资源将一同退订；扩展资源不支持单独退订。
- 成功发起退订后，实例资源将转入冻结状态，冻结期 15 天。冻结期间，用户配置数据会保留 15 天， 用户配置的各类数据会继续生效，但用户无法访问云安全中心，15 天后资源被释放，释放后无法恢复。

操作步骤

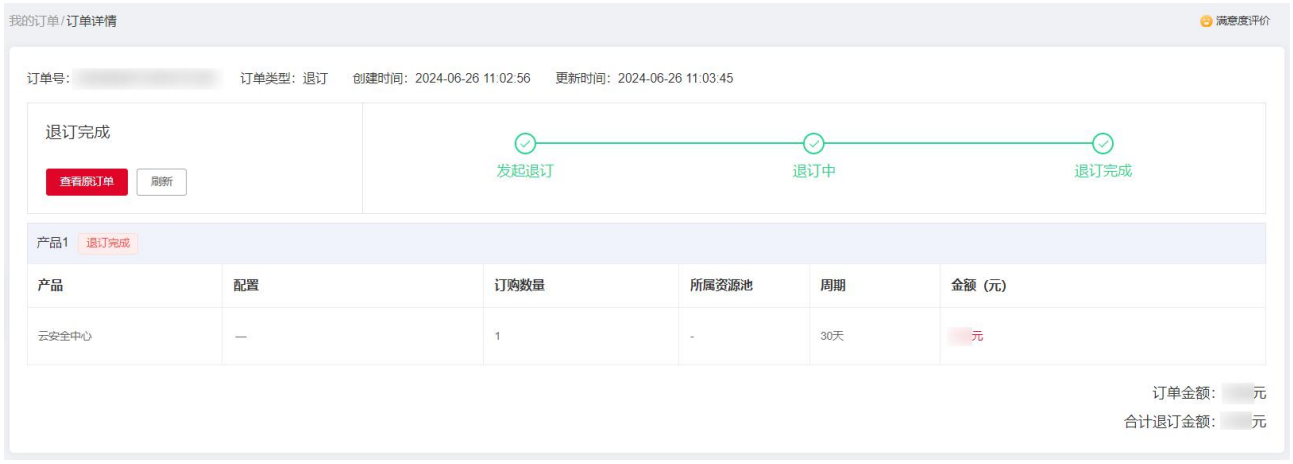
1. 进入天翼云“费用中心 > 订单管理 > 退订管理”页面，找到相应订单，点击退订。



2. 进入退订申请页面，确认退订信息，选择退订原因，信息确认无误后勾选“我已确认本次退订金额和相关费用”，点击“退订。



3. 系统提示退订申请提交成功，可前往订单详情查看退订进度。



4. 当状态变为退订完成时，订单完成退订。

2.5. 查看账单

客户可以在费用中心按月查看在天翼云的消费概况。

账单说明

云安全中心产品为包年包月计费产品，包年包月产品采用预付费模式，即先付费再使用，一般为包年包月的购买形式，支付成功后，云资源将被系统分配给用户使用，直到超过保留期后被系统回收。

说明：

- 当月最终账单将在次月 3 日生成，在次月 4 日 10 点后可查看和导出。
- 云安全中心属于按月结算的产品，当月消费可在次月 3 日查看账单。

操作步骤

1. 登录天翼云控制中心。
2. 在页面右上角用户名称处，选择“费用中心”。

3. 在左侧菜单栏选择“账单管理”， 进入“账单概览页面”，可按产品类型汇总查看产品账单。

4. 在左侧菜单栏选择“账单详情”页面，统计维度选择“产品”，统计周期选择“按账期”，计费模式选择“包周期”，账期选择需要查看的账单时间，即可查看到产品的账单详情。

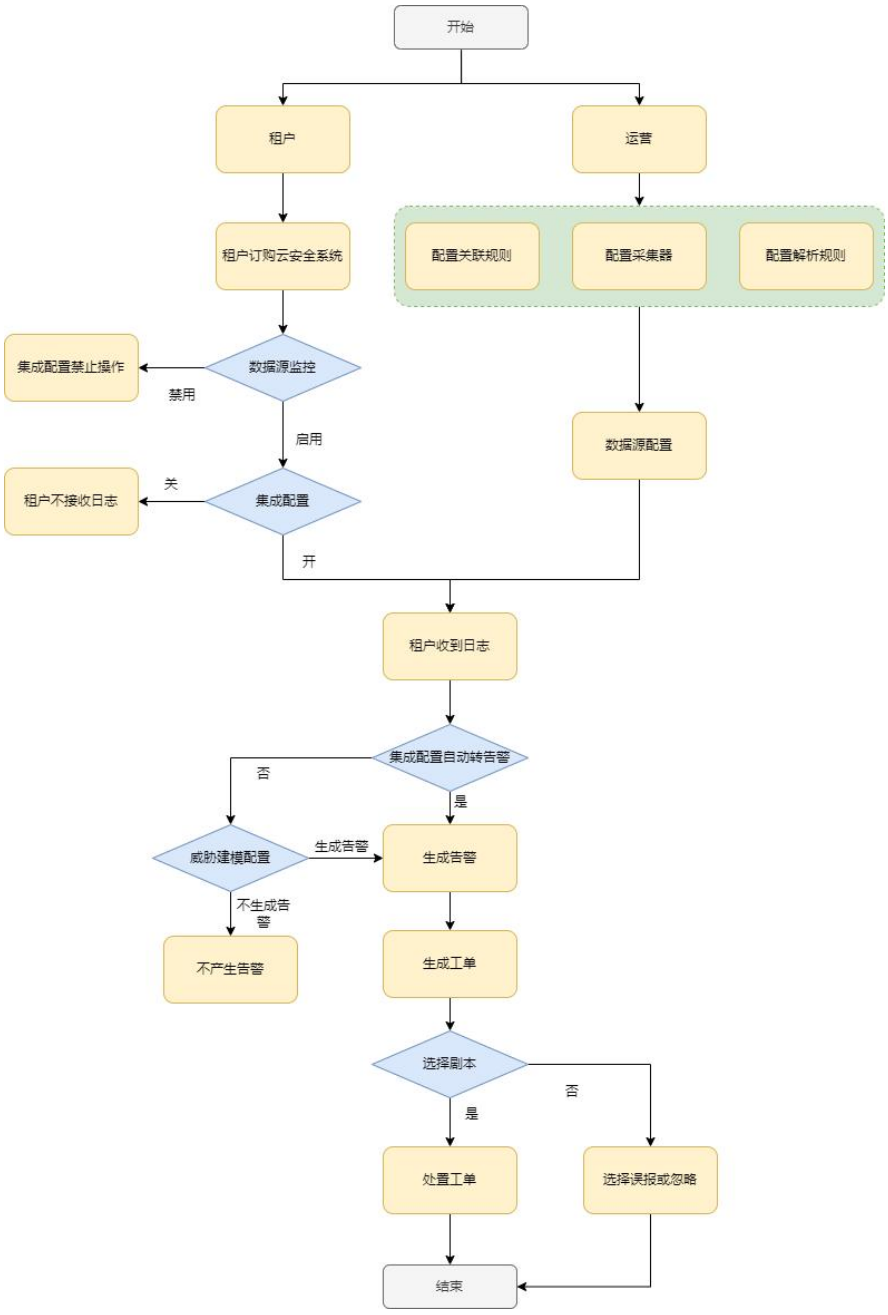

费用中心
总览
订单管理
资金管理
撤单管理
账单管理
账单概览
流水账单
账单详情
导出记录
产品视图
发票管理
总计 4,982.46 0.00 0.00 4,982.46
汇总图表和表格
收起
按产品类型汇总
按企业项目汇总
按计费模式汇总
¥ 4,982.46
云下一代防火墙 ¥60.00
弹性云主机 ¥98.93
SSL VPN ¥80.00
云硬盘 ¥10.00
导出

3. 快速入门

3.1. 使用流程

为全面帮助您进行安全运营，您需要购买云安全中心实例并接入安全产品日志。云安全中心获取到各类日志后，能通过日志的内容进行威胁建模，完成各类安全告警的生成，辅助您进行安全处置，实现安全运营。

云安全中心使用流程如下：



3.2. 注册天翼云账号

在购买和使用云安全中心之前，您需要先注册天翼云门户的账号。本节将介绍如何进行账号注册，如果您拥有天翼云的账号，请跳转至使用云安全中心。

1. 登录天翼云门户 http://www.ctyun.cn，点击注册。

2. 在注册页面，请填写“邮箱地址”、“登录密码”、“手机号码”，并点击同意协议并提交，如 1 分钟内手机未收到验证码，请再次点击免费获取短信验证码。

3. 注册成功后，可到邮箱激活您的账号或立即体验天翼云服务。

3.3. 购买云安全中心实例

云安全中心支持包年/包月计费方式，目前提供基础版的主资源，两种扩展资源：日志分析量、态势大屏。您可以根据业务规模选择云安全中心规格。

前提条件

已经注册天翼云账号并完成实名认证。

规格限制

- 态势大屏只可购买一次。
- 日志分析量扩展资源的购买资源最小单位为 50G，即购买时只能选择 50G 的整数倍。

约束条件

- 同一账号在同一个区域只能开通一个云安全中心实例，对应一个服务版本。
- 开通云安全中心实例，必须购买主资源，可以在主资源基础上叠加购买扩展资源，扩展资源与主资源绑定，到期时间与主资源一致，不支持单独续订、退订。

> 说明：
>
> 原则上，在任何一个区域购买的云安全中心实例支持接入所在区域的日志信息，建议在购买云安全中心实例时，根据业务所在区域选择购买云安全中心实例。

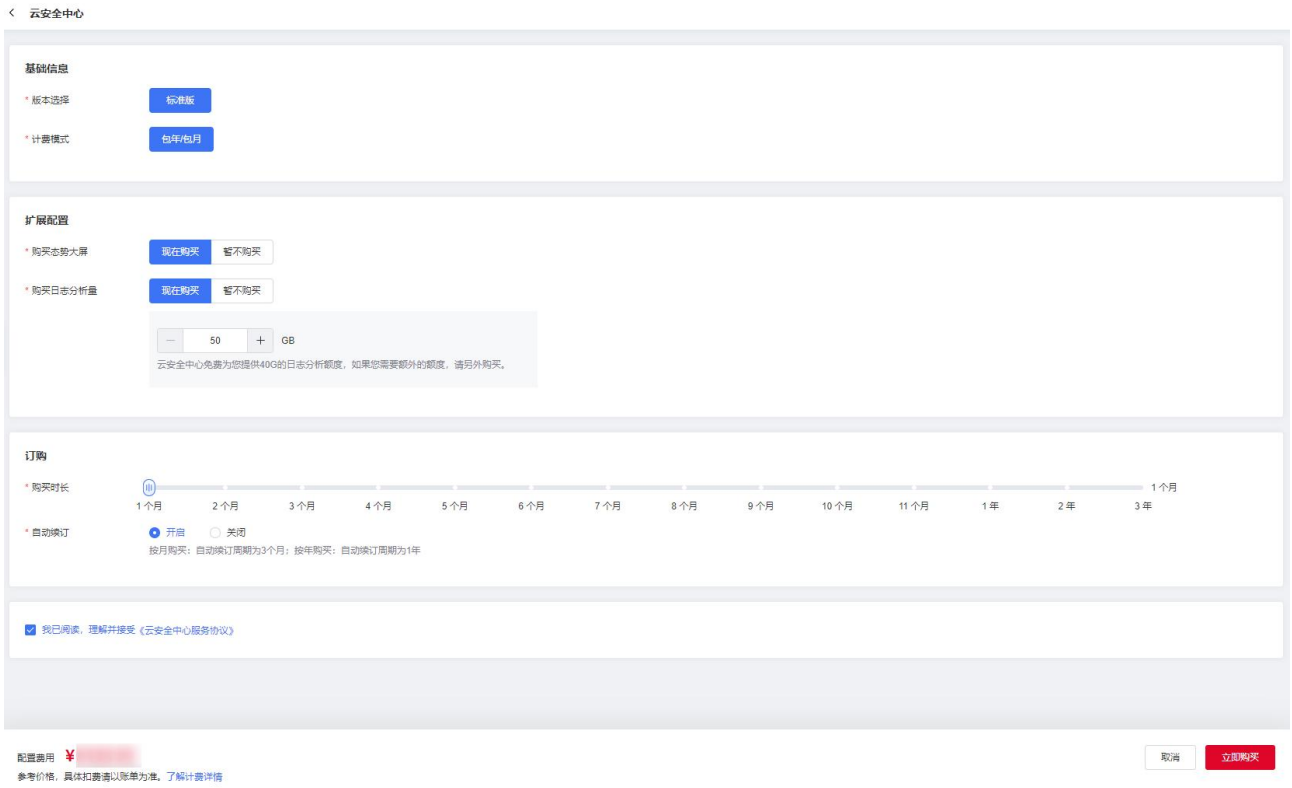
适用场景

用户购买了天翼云上的安全服务“Web 应用防火墙（原生版）、服务器安全卫士（原生版）、云等保专区等”并部署在天翼云上。

操作步骤

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全>云安全中心”，进入云安全中心控制台。

3. 单击“立即购买”，进入购买页面。



4. 选择版本信息、扩展资源、选择“购买时长”。

参数		说明
基本信息	版本选择	支持“标准版”。规格详情请参见“产品规格”。
	计费模式	支持“包年包月”。

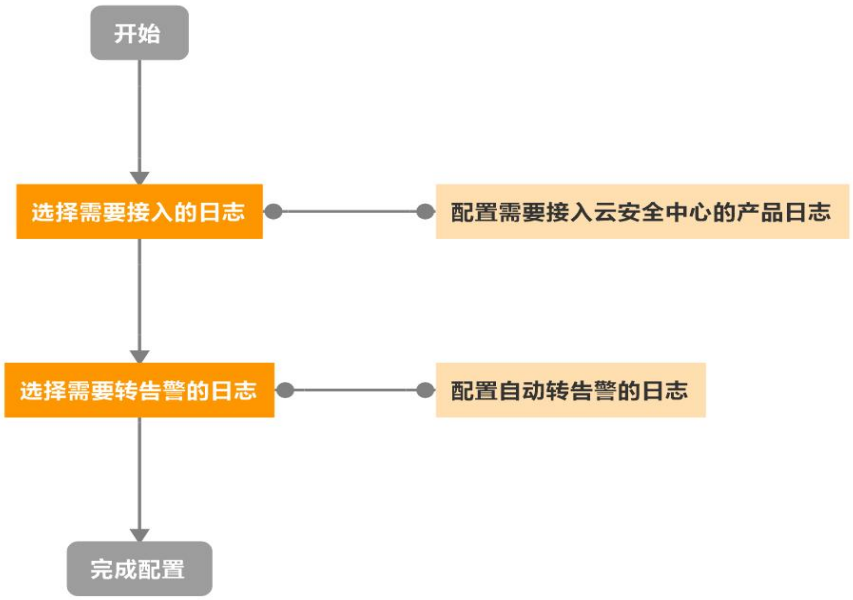
参数		说明
扩展配置	购买态势大屏	默认为“现在购买”，也可以选择“暂不购买”。 说明： 态势大屏只可购买一次。
	购买日志分析量	默认为“现在购买”，也可以选择“暂不购买”。 说明： 云安全中心标准版免费提供 40G 的日志分析额度，如果您需要额外的额度，请另外购买。 日志分析量扩展资源的购买资源最小单位为 50G，即购买时只能选择 50G 的整数倍。
订购	购买时长	拖动时间轴设置购买时长，可以选择 1 个月~3 年的时长。
	自动续订	开启“自动续订”后，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费。 ● 按月购买，自动续费周期默认为 3 个月。 ● 按年购买，自动续费周期默认为 1 年。 如需要修改自动续费周期，可进入天翼云“费用中心 > 订单管理 > 续订管理”页面，找到对应的资源进行修改。

5. 确认配置参数和配置费用，阅读《云安全中心服务协议》并勾选“我已阅读，理解并接受《云安全中心服务协议》”，单击“立即购买”。
6. 进入“付款”页面，完成付款。

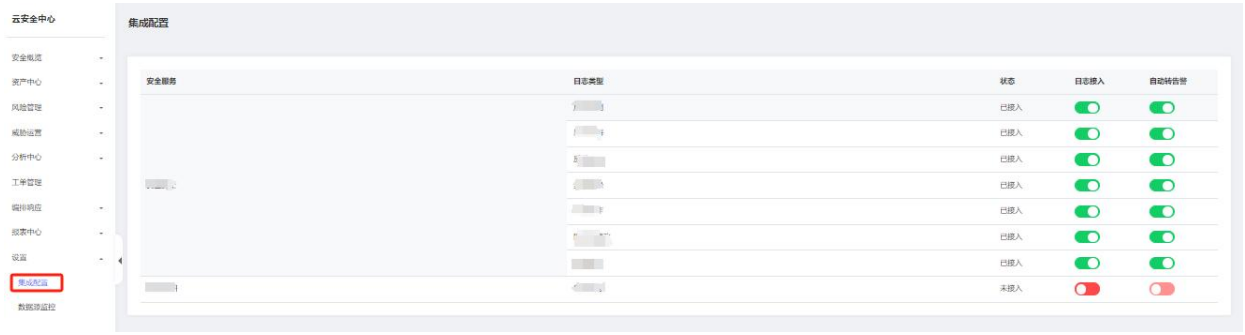
3.4. 接入日志、告警

开通云安全中心实例后，系统默认会接入部分日志数据并对用户进行初始化配置。您可以根据自己的业务特性修改初始化配置。

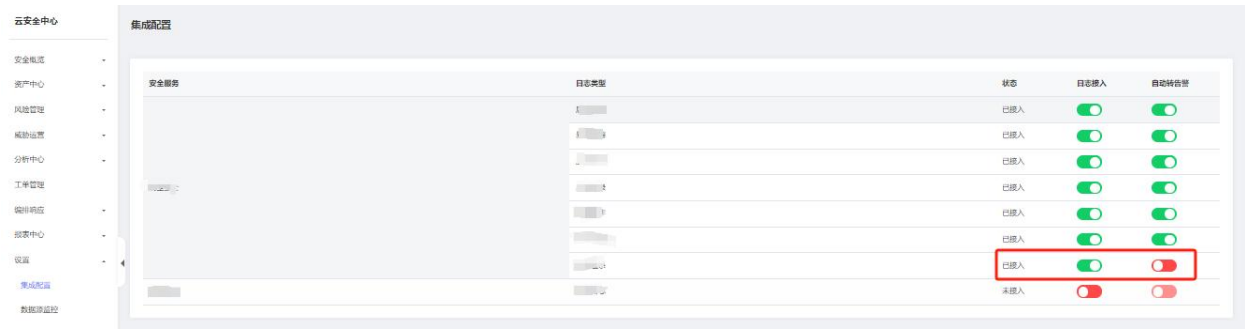
打开云安全中心的“设置 > 集成配置”，在集成配置中选择需要接入的日志类型。部分日志支持直接转告警，可以直接打开转告警开关，云安全中心会根据内置转告警规则进行转告警配置。



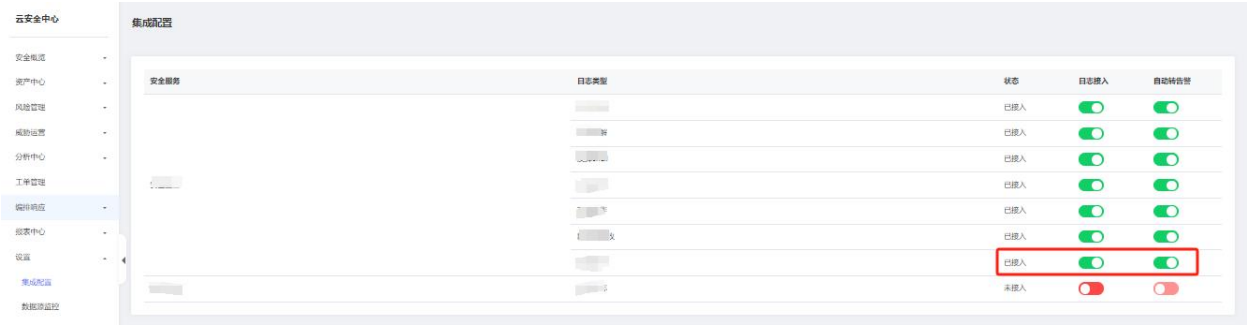
1. 选择“设置 > 集成配置”，打开数据集成配置页面。



2. 选择需要接入的日志，并打开日志接入开关。



3. 选择需要转告警的日志，并打开自动转告警的开关。

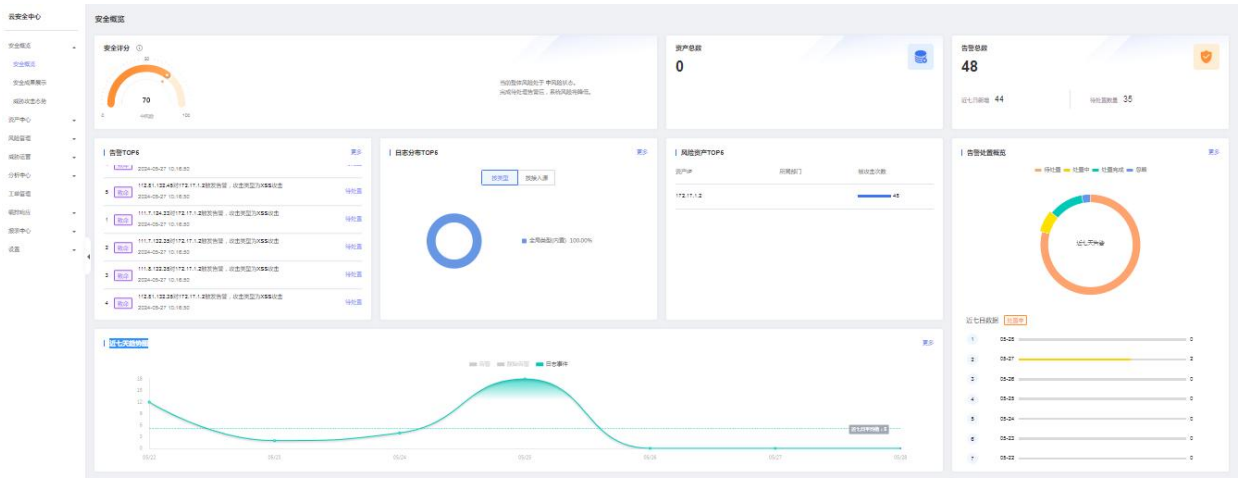


说明：

- 系统默认会接入部分日志，用户如有需要，可以自行关闭。
- 日志需要先接入才能自动转告警，只有部分类型的日志支持自动转告警。

3.5. 查看安全概览

打开云安全中心>安全概览，安全概览会通过大屏的方式展示安全评分、资产总数、告警总数、告警 TOP5、日志分布 TOP5、风险资产 TOP5、告警处置概览 TOP5、近七天趋势图。



说明：

- 安全概览的数据来源于接入系统的数据量，需要确保已完成数据接入。
- 日志、告警等维度数据展示均支持下钻点击，通过详情进行展示。
- 概览数据只展示当前情况，最新实时数据需要手动刷新页面获取。

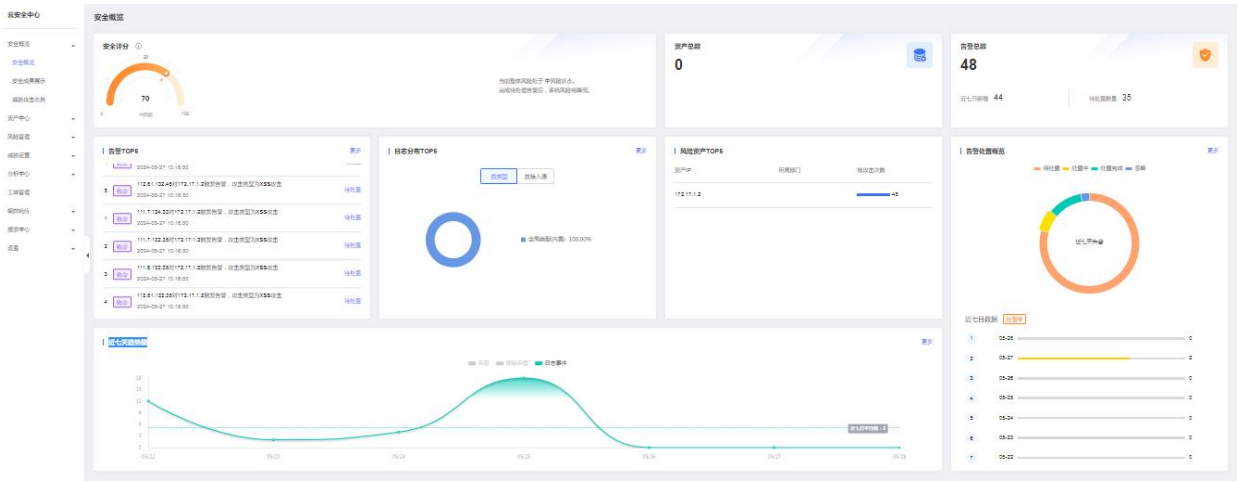
4. 用户指南

4.1. 安全态势

云安全中心安全态势页面向您展示当前云安全中心实例中已接入数据的统计信息，为了便于用户对平台数据进行整理分析，安全态势提供安全概览、安全成果展示、威胁攻击态势三个大屏进行可视化展示。

4.1.1. 安全概览

安全概览大屏：展现安全评分、资产总数、告警总数、告警 TOP5、日志分布 TOP5、风险资产 TOP5、告警处置概览 TOP5、近七天趋势图。其中告警总数、告警 TOP5、日志分布 TOP5、告警处置概览、近七天趋势图支持下钻查看详细信息。



安全评分

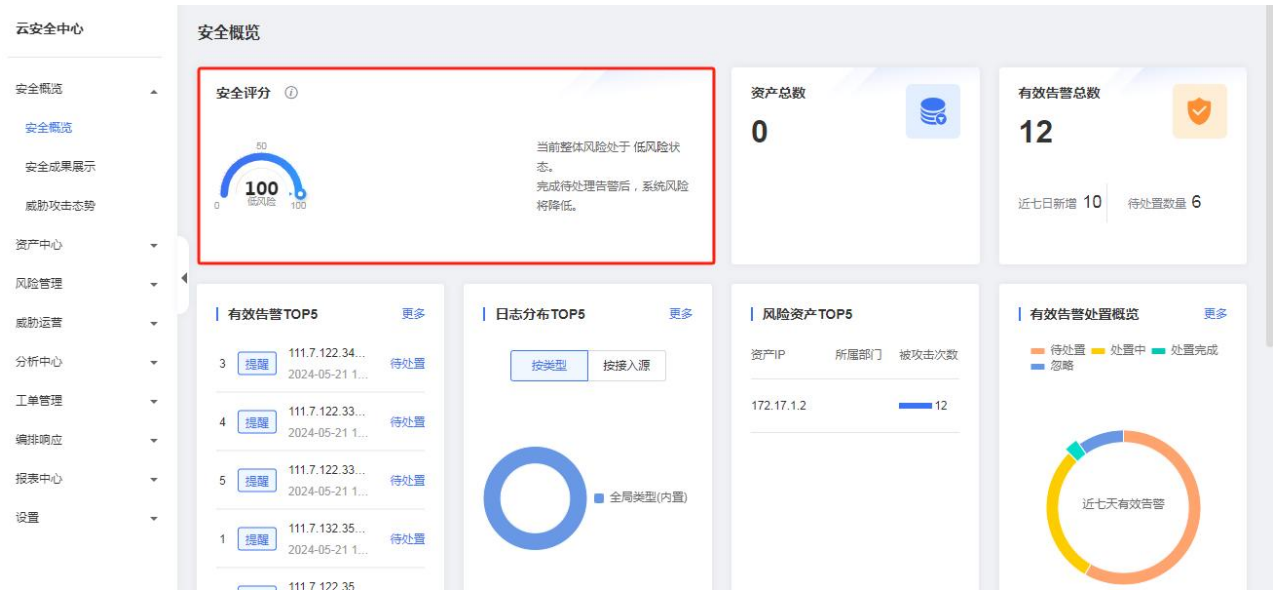
评分系统根据弱口令、漏洞和告警扣分，各占 40%、30%、30%。

扣分规则：【弱口令】10 分/项；【漏洞】高危 5 分/项，中危 2 分/项；【告警】致命 5 分/项，严重 3 分/项，警告 1 分/项。

风险等级实时更新，低风险（80-100 分）、中风险（60-80 分）、高风险（0-60 分）。

说明：

安全评分是依据用户的弱口令、漏洞、告警进行综合计算，不同项目其分数配额相互独立。



资产总数

统计已经接入云安全中心的资产总数。

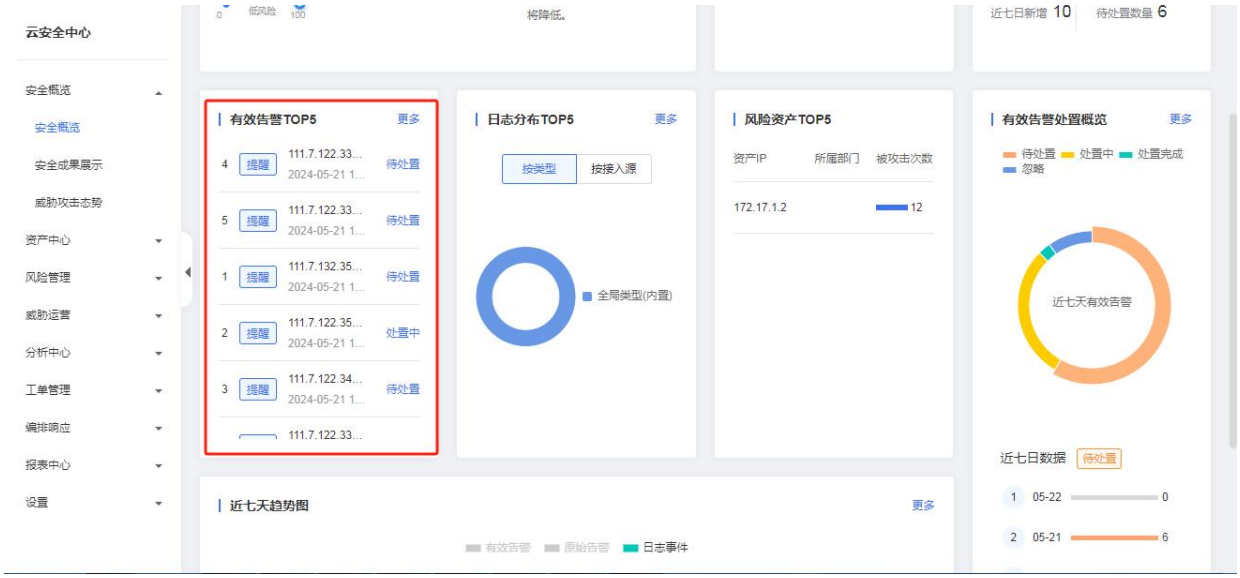
告警总数

统计您当前产生的所有有效告警数量，同时展示最近七日的新增数量以及待处置的有效告警数量。

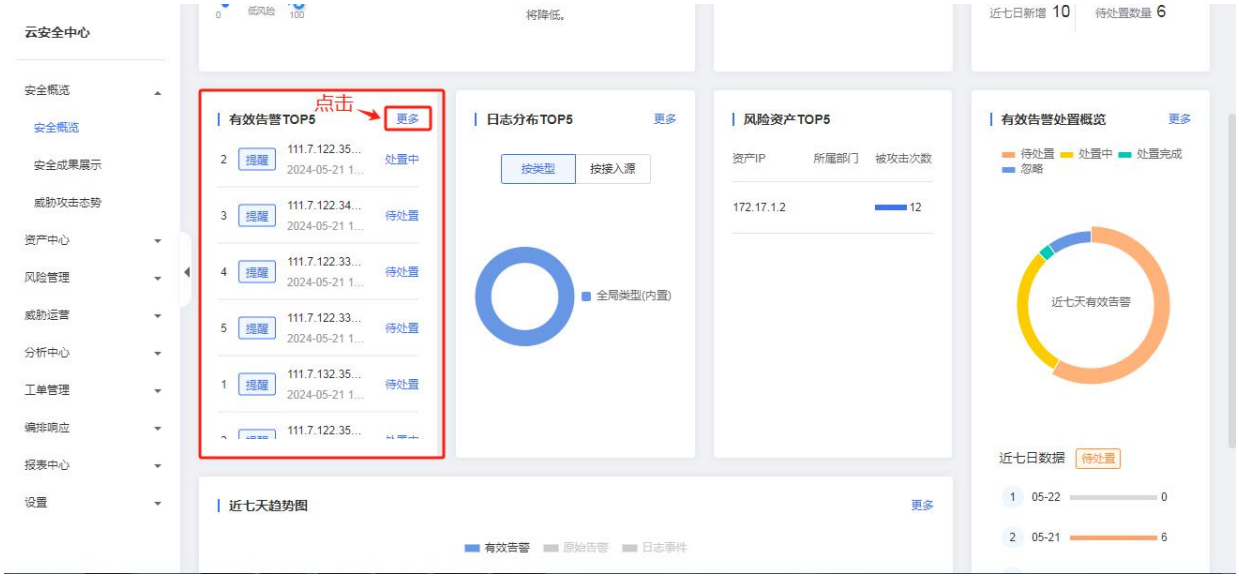
近 7 日新增，支持下钻至告警管理页面。

告警 TOP5

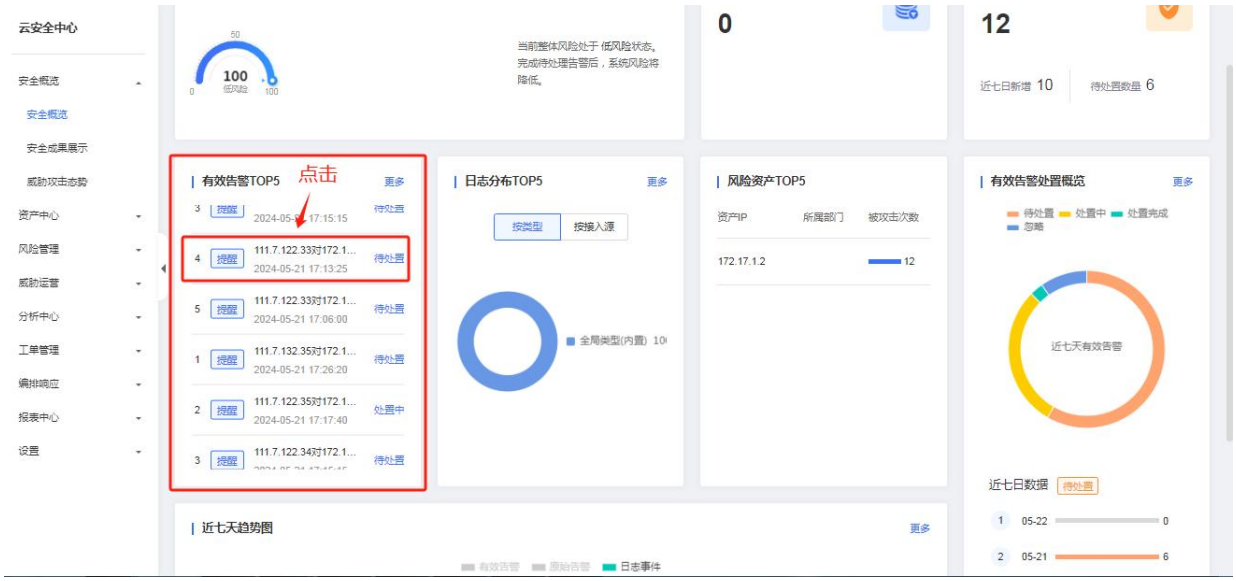
提供有效告警 TOP5 的滚动展示。



点击更多，支持下钻至告警管理页面。



点击告警消息，支持下钻至告警消息详情页面。



日志分布 TOP5

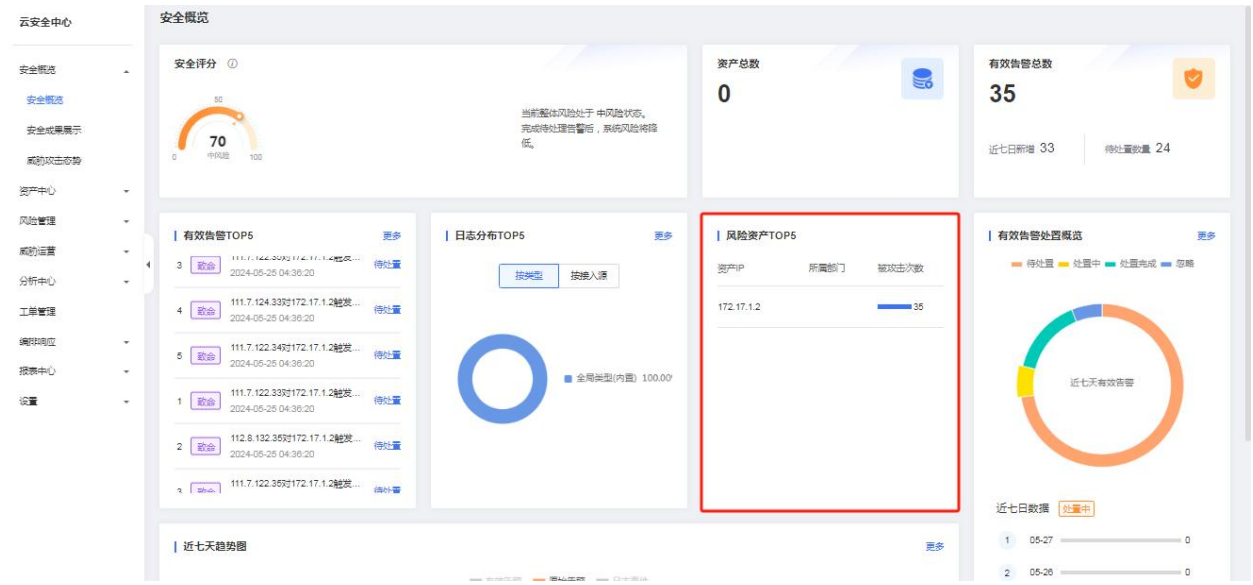
提供日志分布 TOP5 的展示。

支持按类型或按接入源查看日志分布 TOP5。

点击更多，支持下钻至日志查询页面

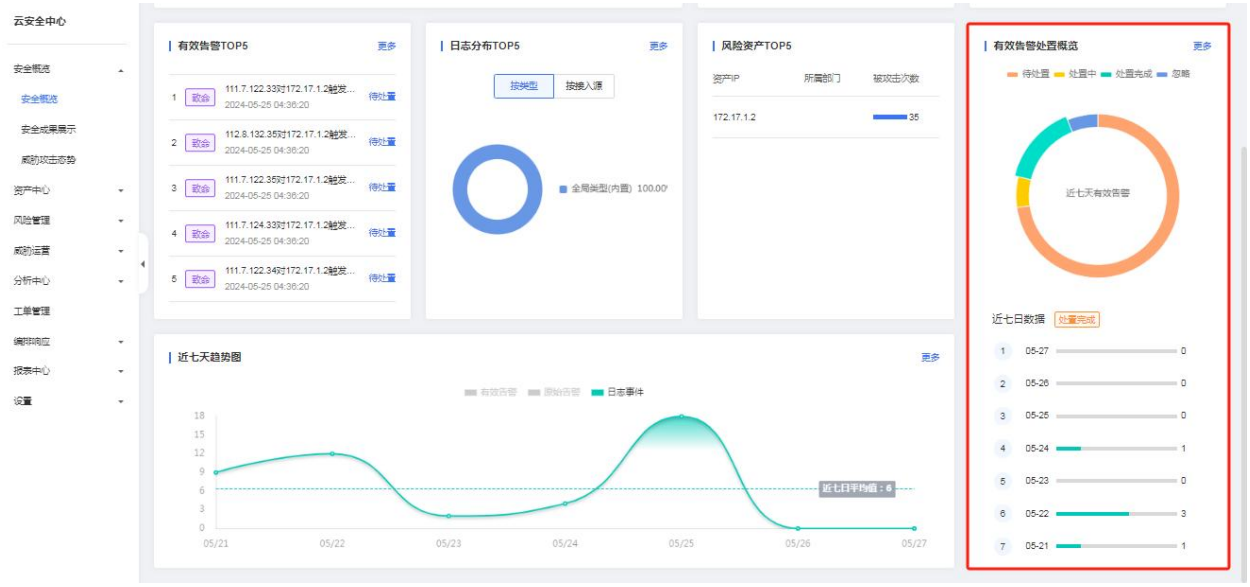
风险资产 TOP5

展示您当前系统中风险最多的 5 个资产信息

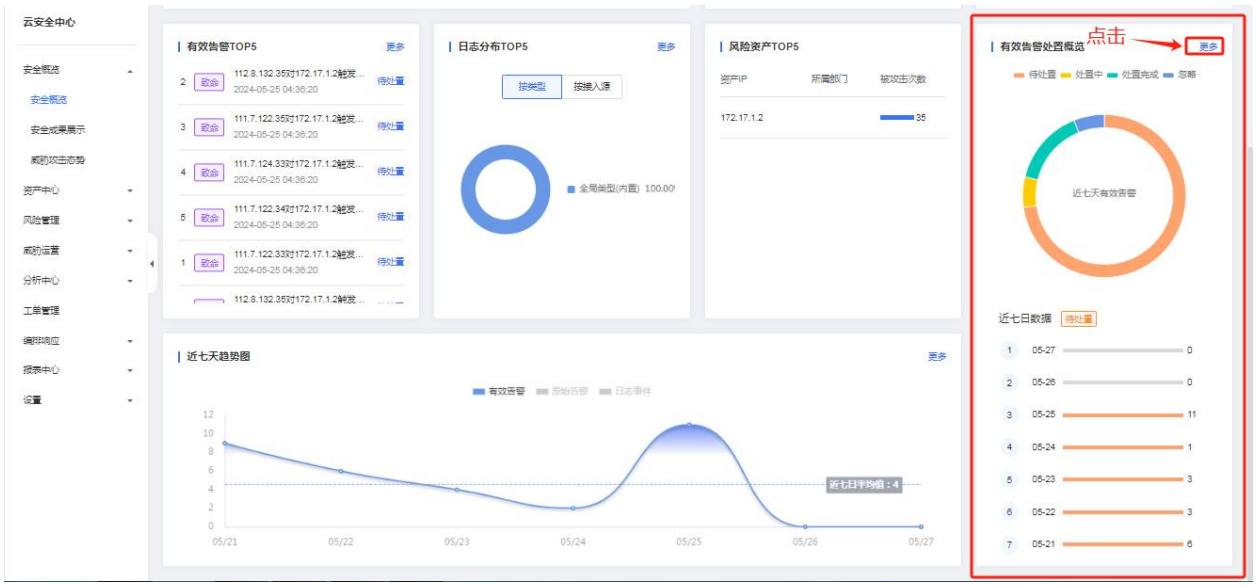


告警处置概览

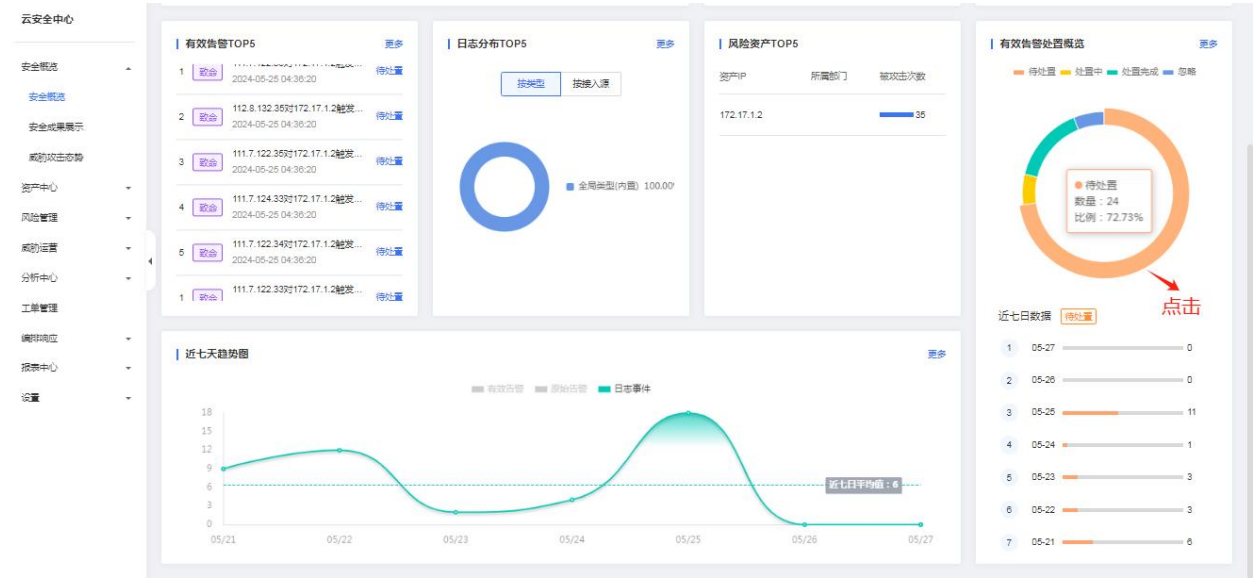
展示近七天的告警处置情况。



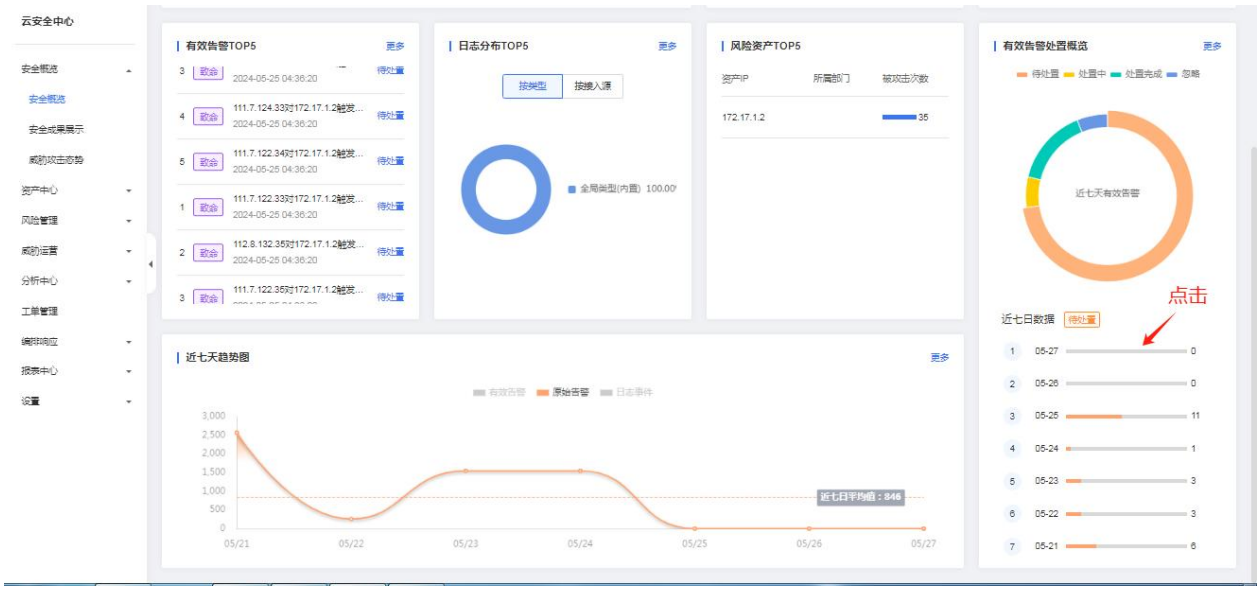
点击更多，支持下钻至告警管理页面



点击饼图，下钻至告警管理并查询对应条件的数据

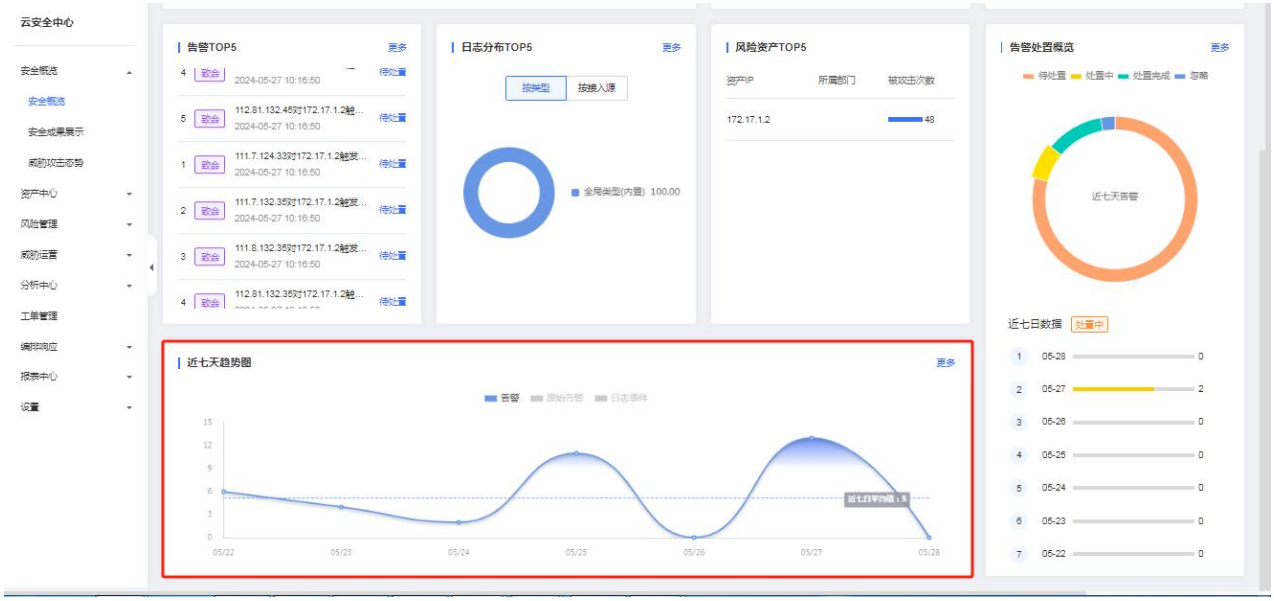


点击 7 日数据中的其中一天，下钻至告警管理，并查询当天的数据

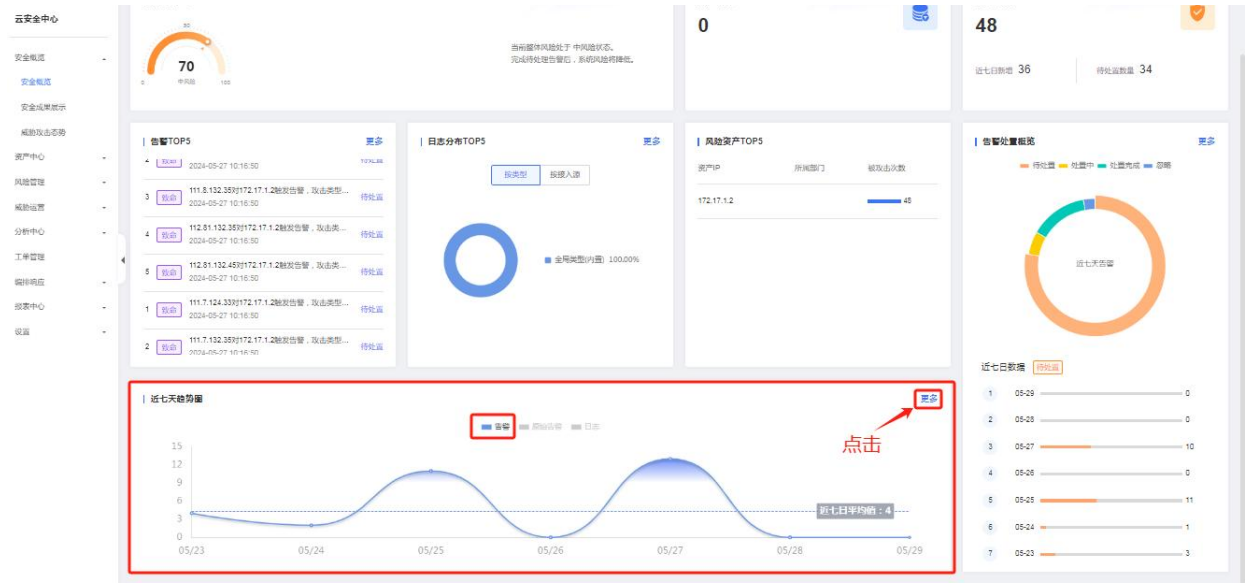


近七天趋势图

展示最近七天告警、原始告警以及日志的发生数量以及趋势，进行轮播。



点击更多，下钻至对应的告警管理、告警查询、日志查询页面



4.1.2. 安全成果展示

用户从日志接收解析到最终形成告警过程全流程的过程重要的数据统计。

4.1.3. 威胁攻击态势

用户可以查看不同级别的告警的数量统计、异常资产、高危待处理等态势

4.2. 资产中心

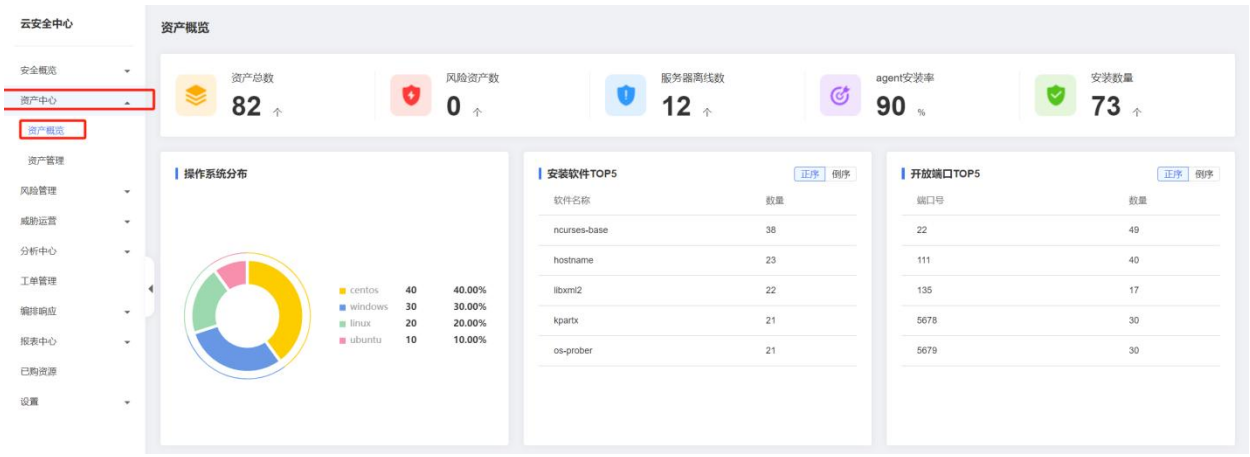
为了便于租户对平台资产数据进行整理分析与管理，资产中心提供资产概览、资产管理两个便于管理资产的功能。

前提条件

- 已开通云安全中心实例。
- 具有云上资产数据。

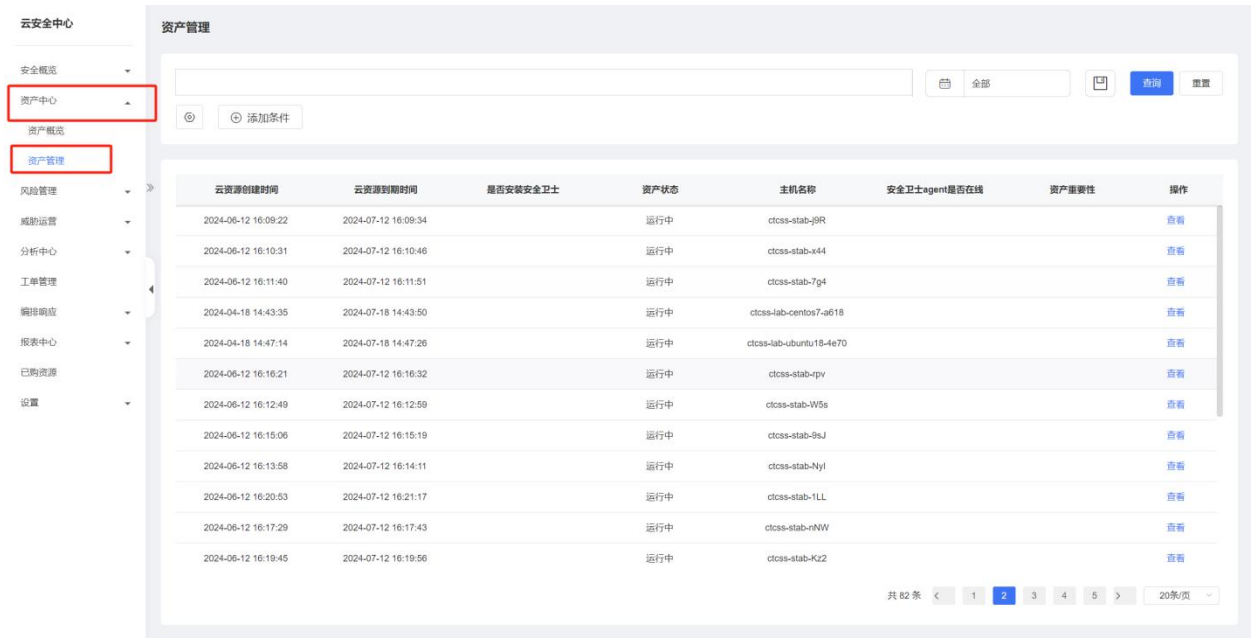
4.2.1. 资产概览

资产概览显示资产总数、风险资产数、服务器离线数量、Agent 安装率和安装数量，安装软件 TOP 排行（支持倒序和正序），操作系统分布，开放端口号 TOP 排行（支持倒序和正序）。

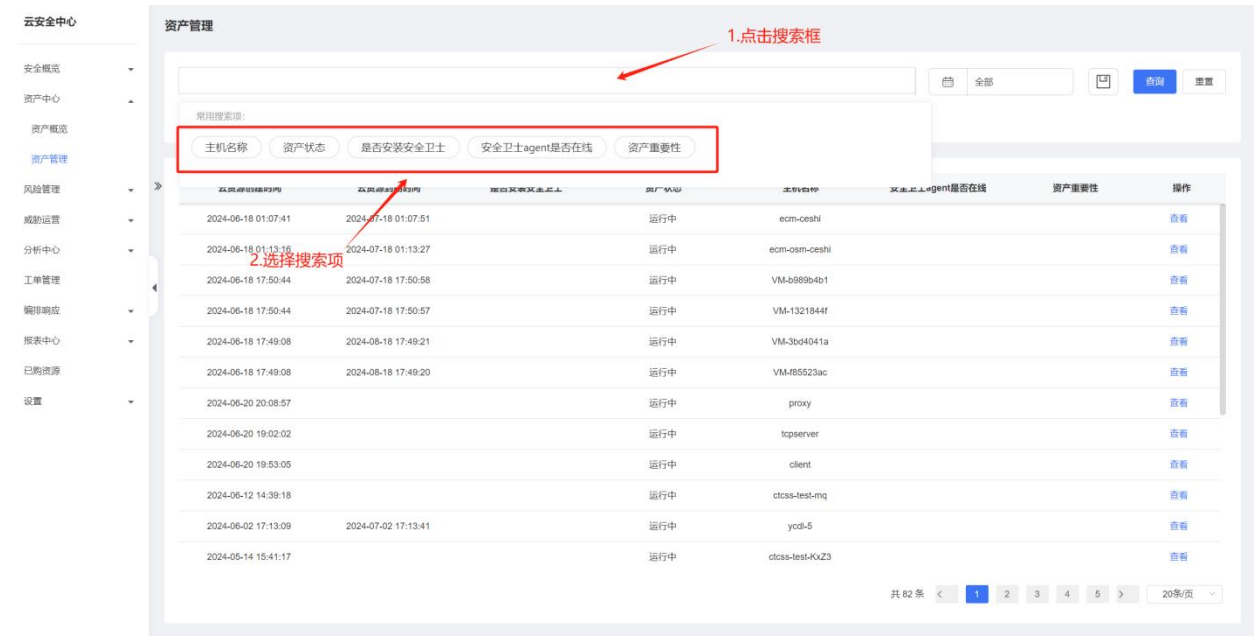


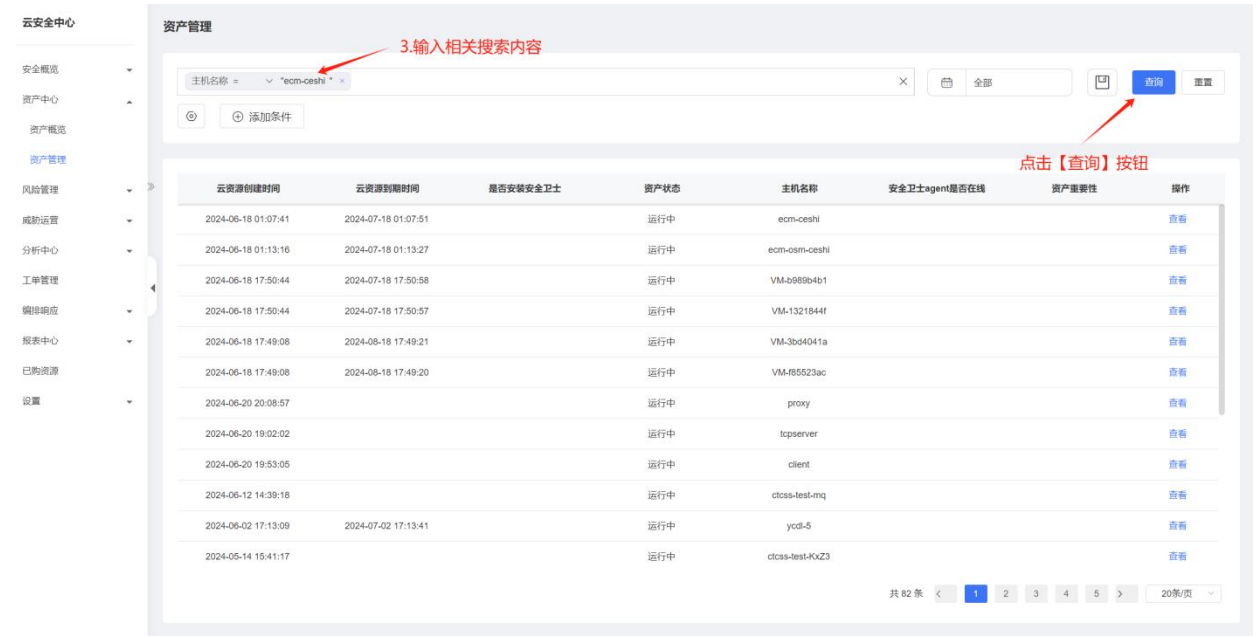
4.2.2. 资产管理

为租户提供资产及资产属性的查询功能。

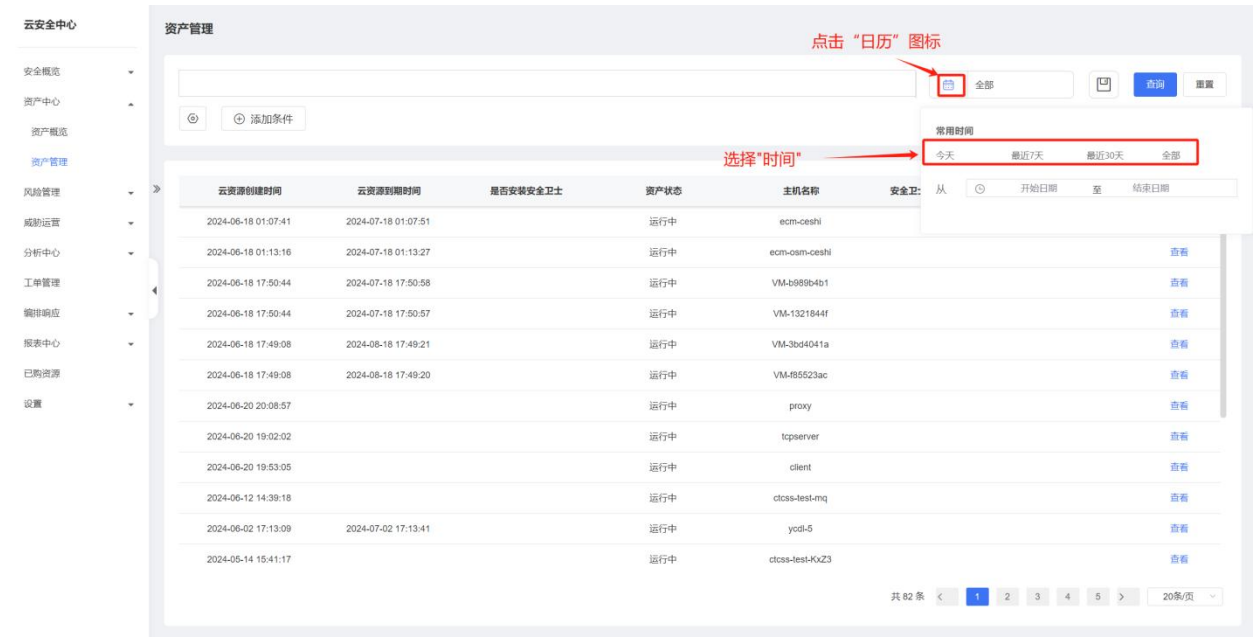


选择常用搜索项查询。

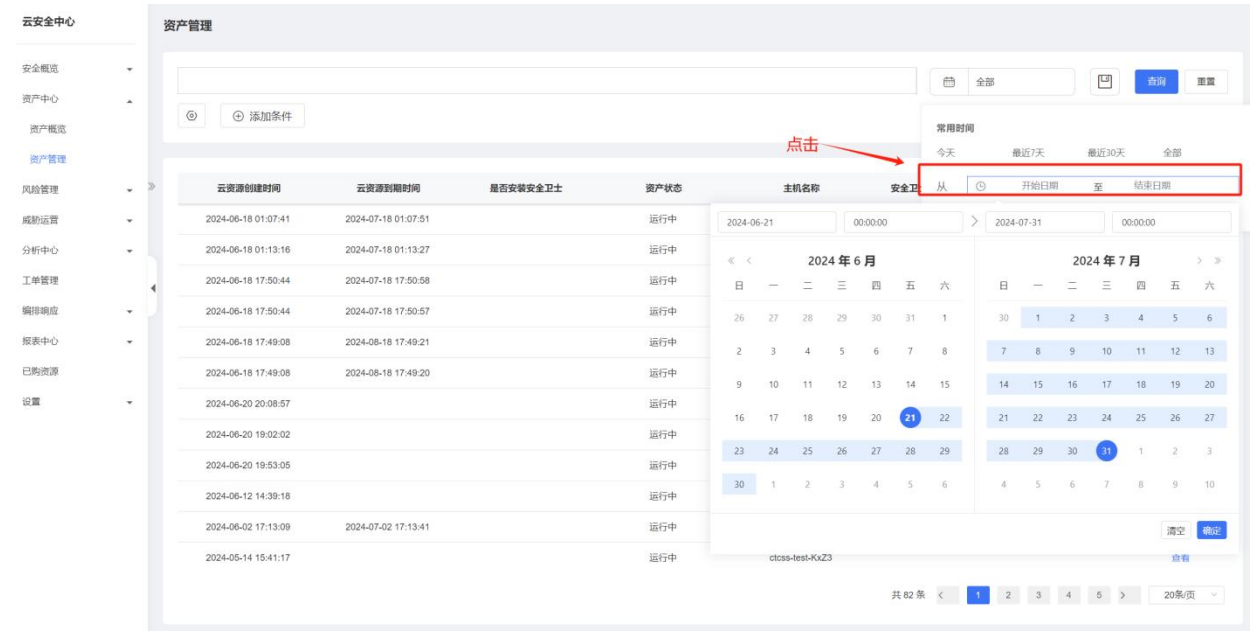

云安全中心
资产管理
1.点击搜索框
主机名称
资产状态
是否安装安全卫士
安全卫士agent是否在线
资产重要性
2.选择搜索项


云安全中心
资产管理
3.输入相关搜索内容
点击【查询】按钮

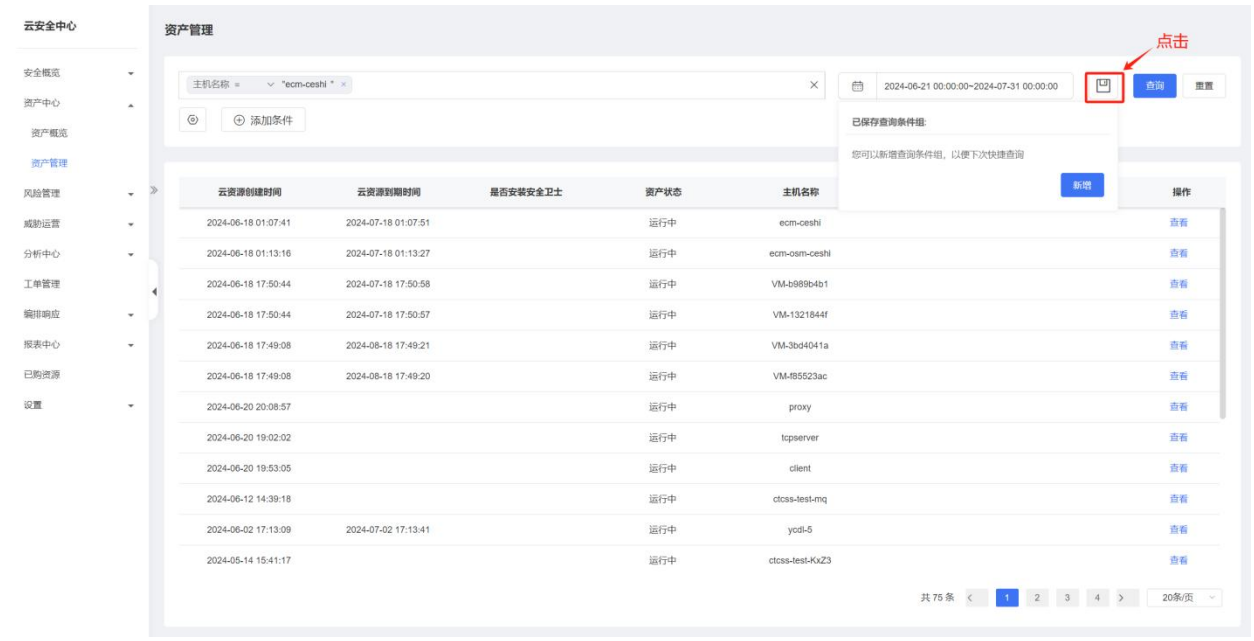
选择常用时间查询。

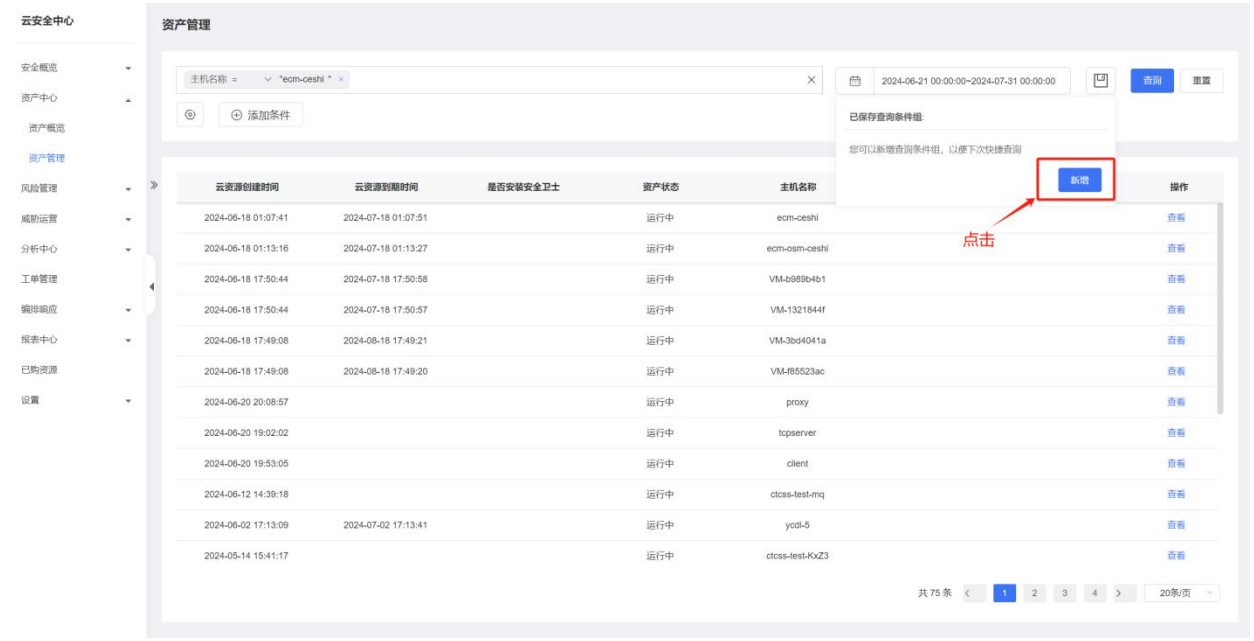


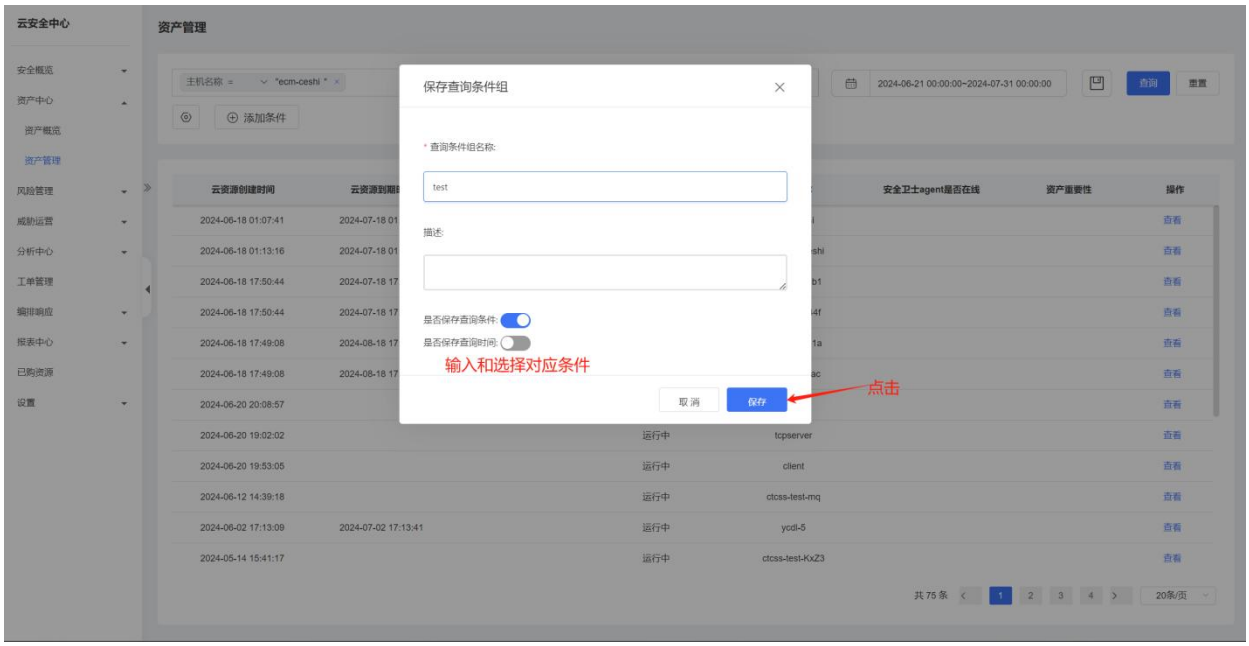
选择时间段查询。



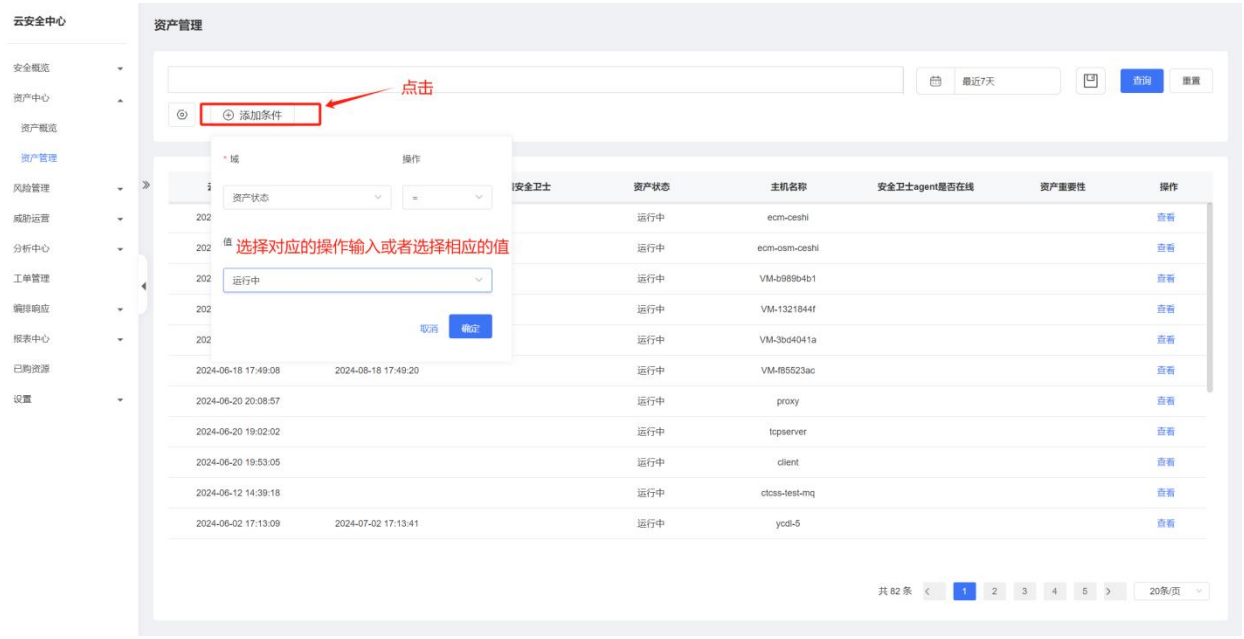
查询条件组：保存查询条件，方便用户快速查询。


云安全中心
资产管理
点击
查询
重置
添加条件
已保存查询条件组:
您可以新增查询条件组，以便下次快捷查询
新增
操作
查看


云安全中心
资产管理
查询
重置
添加条件
已保存查询条件组:
您可以新增查询条件组，以便下次快捷查询
新增
点击
操作
查看



添加条件查询。



4.3. 风险管理

云安全中心风险管理提供给用户漏洞管理和弱口令管理的能力。

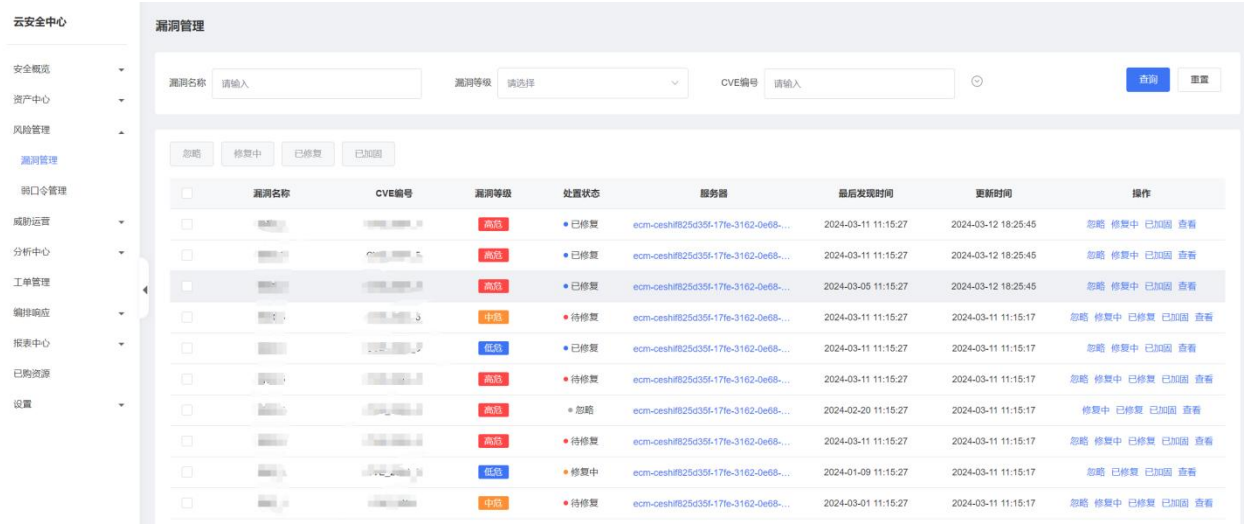
前提条件

- 已开通云安全中心实例。

- 具有云上资产数据。

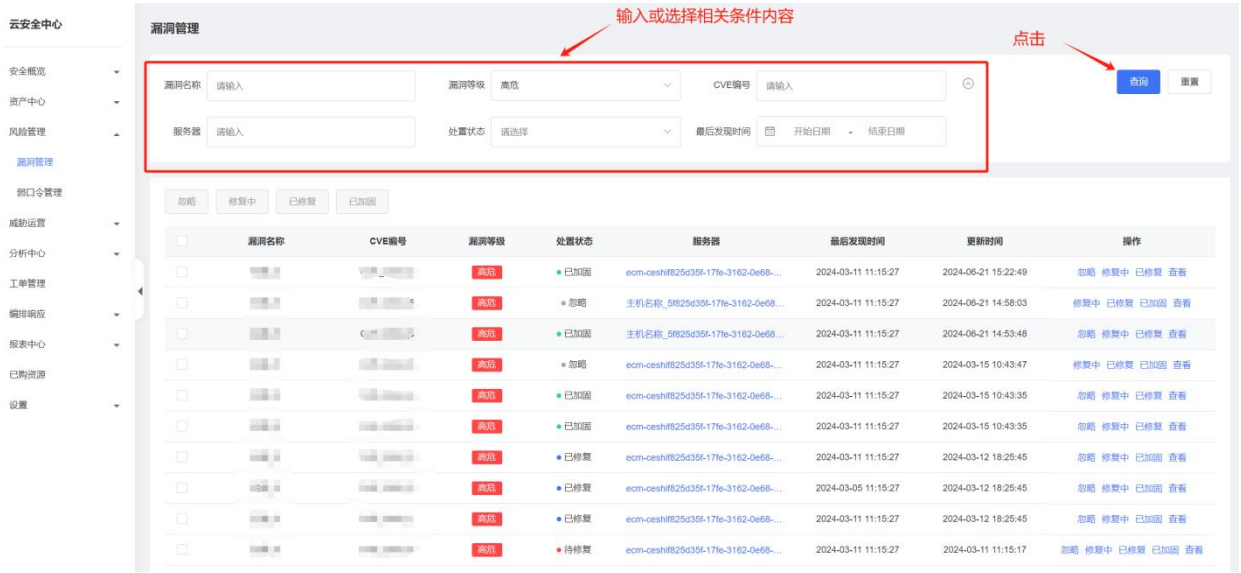
4.3.1. 漏洞管理

为租户提供漏洞查询及处置功能。



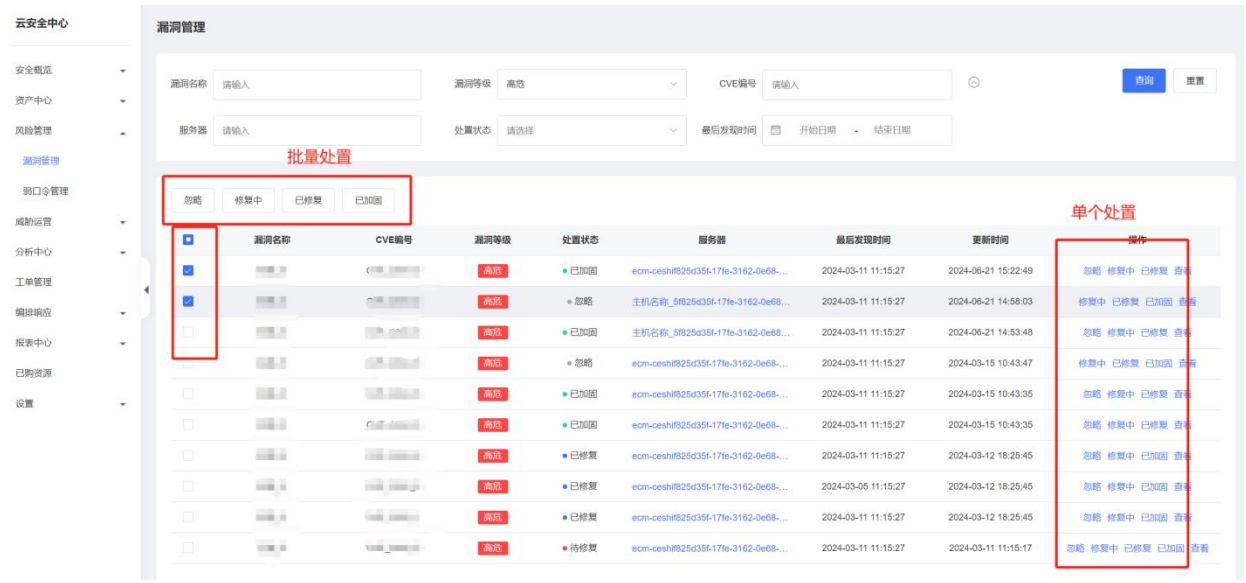
条件查询

支持条件查询，用户输入或选择相关条件内容。

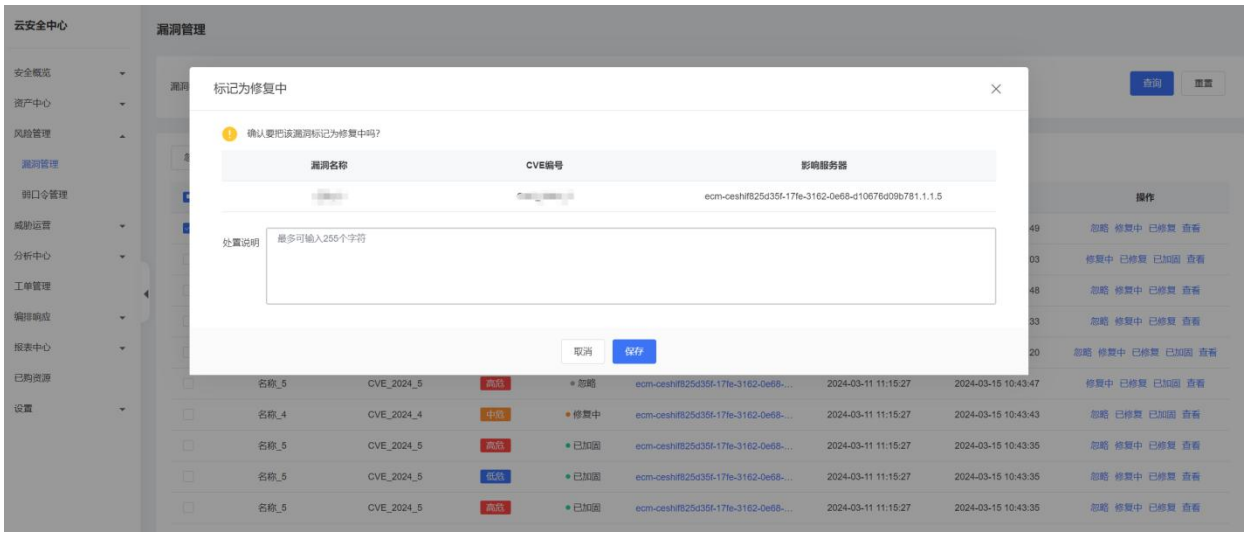


处置漏洞

提供处置能力，可直接或批量修改漏洞处置状态。状态枚举值：修复中、已修复、忽略、已加固等。

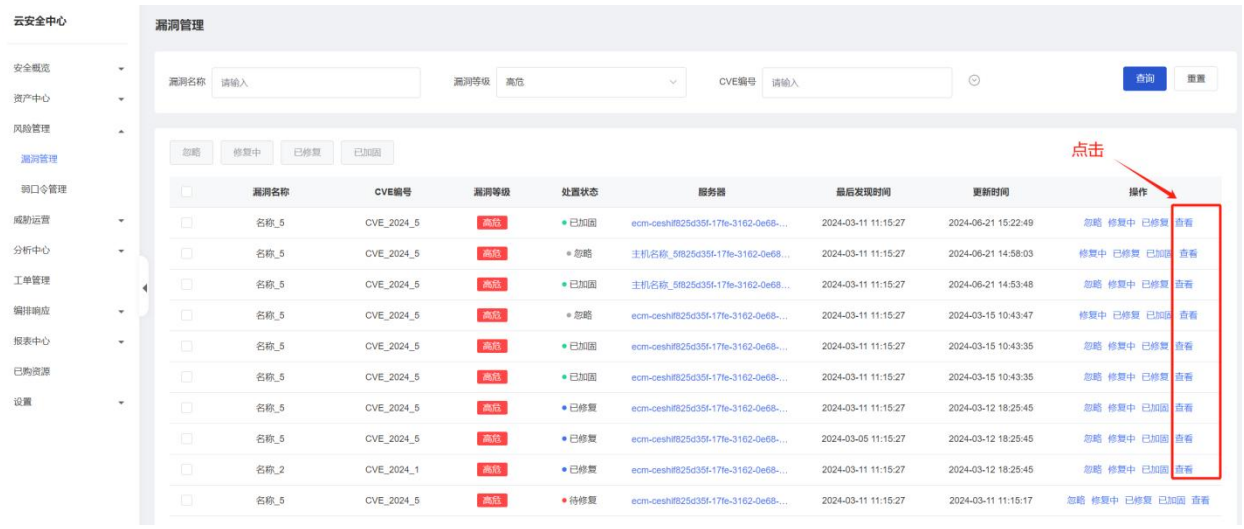


修改处置状态可填写处置说明，便于后续查看状态变更原因。



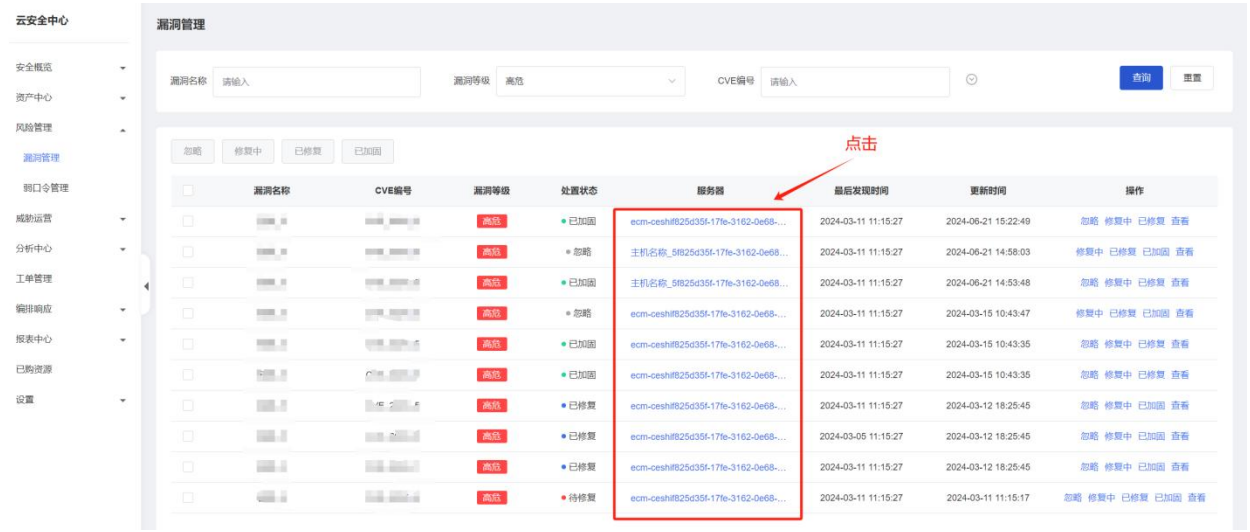
查看漏洞详情

在漏洞详情中，可以查看所有历史状态变更记录的信息，包括：处置人、处置状态、处置说明、处置时间等。



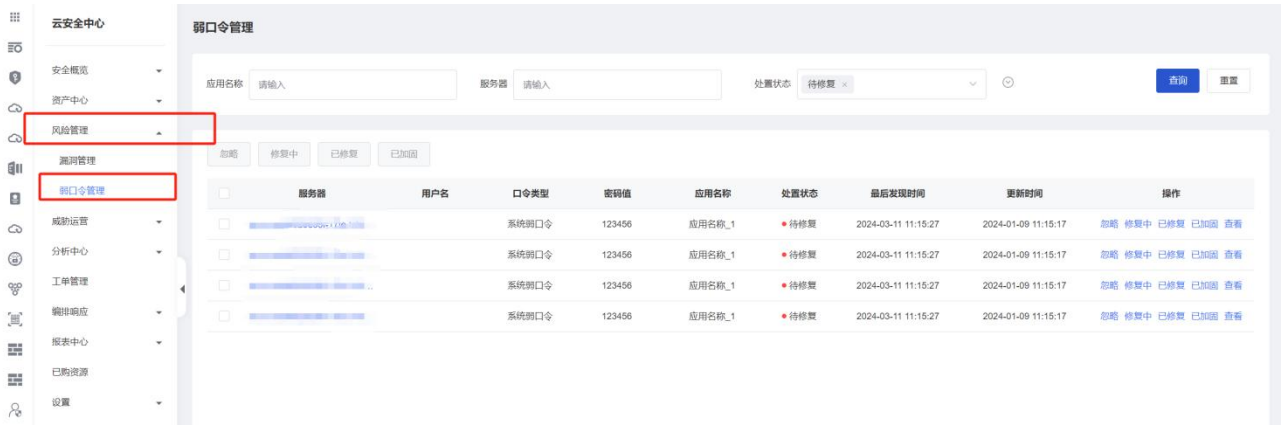
查看漏洞关联资产

每条漏洞能够关联资产信息，可快速查看关联的资产详情。

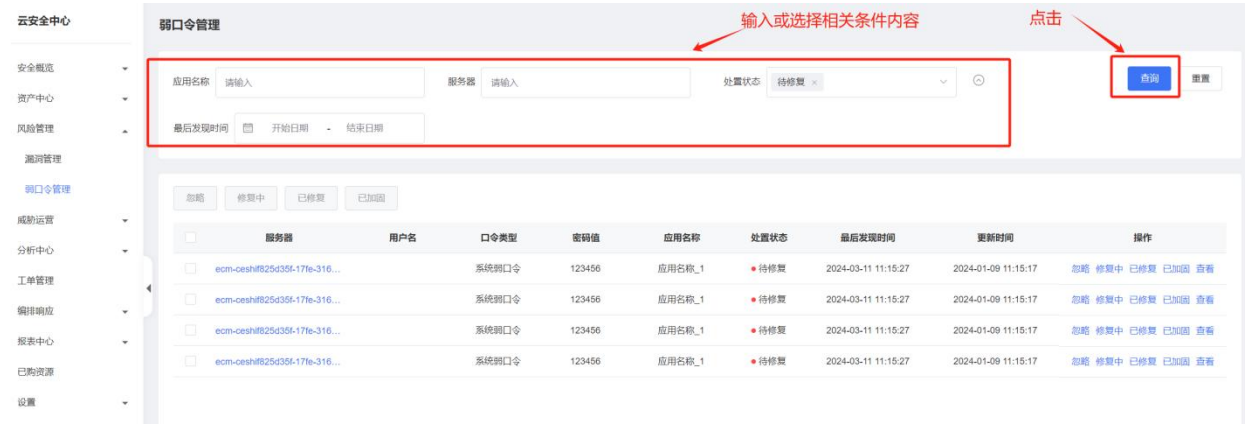


4.3.2. 弱口令管理

为租户提供弱口令查询及处置功能。

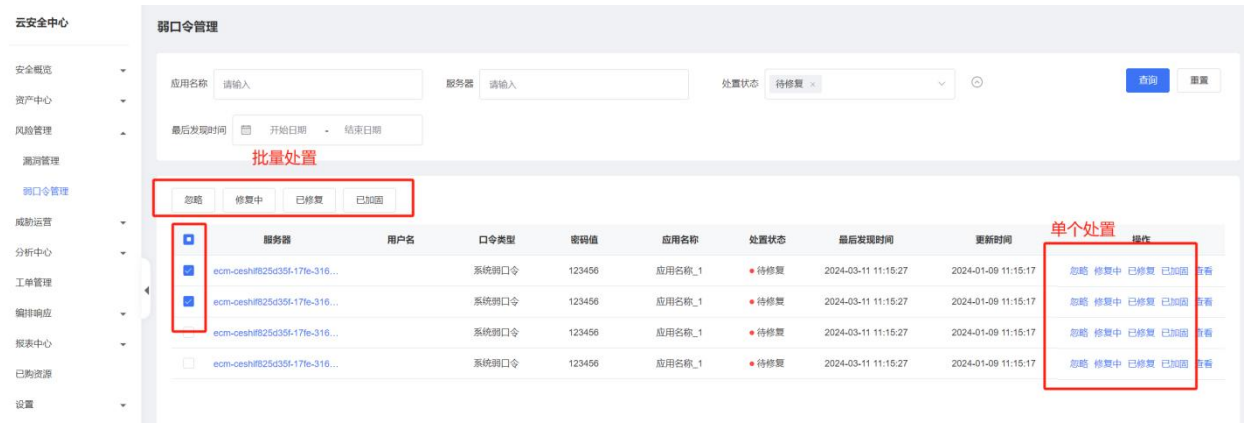


条件查询

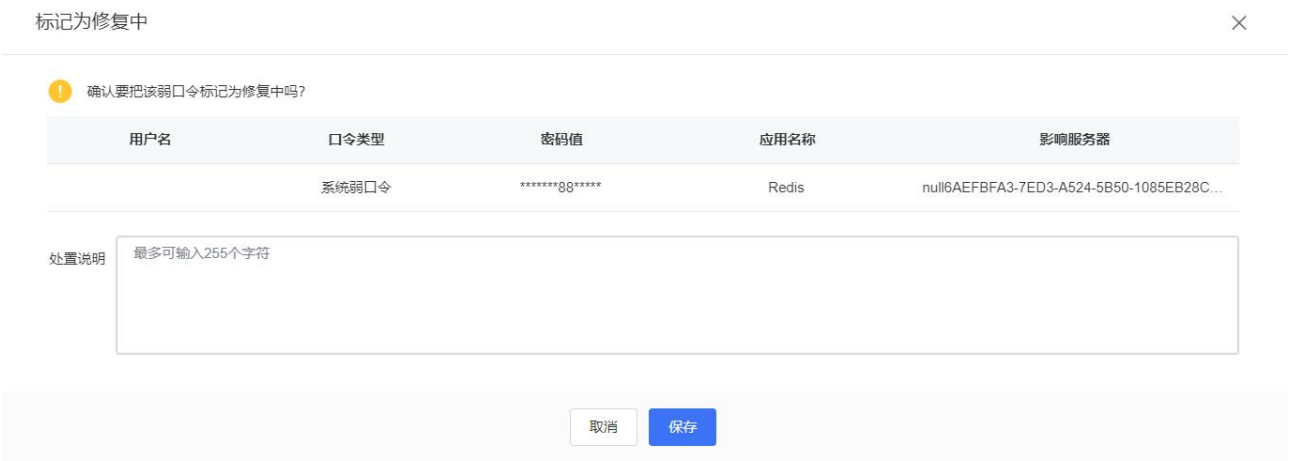


处置弱口令

提供处置能力，可直接或批量修改漏洞处置状态。状态枚举值：修复中、已修复、忽略、已加固等。

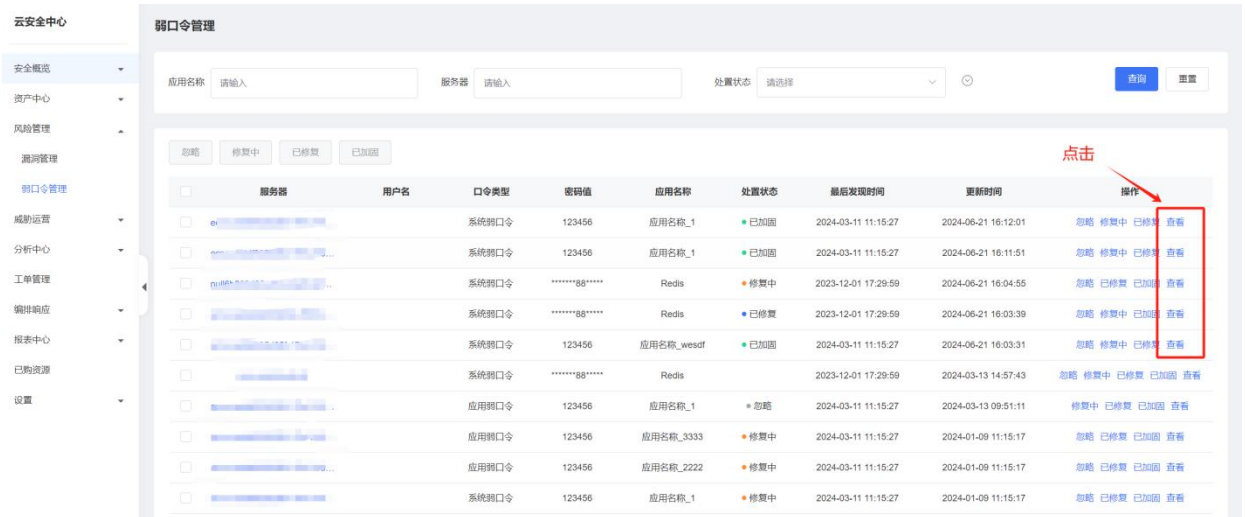


修改处置状态可填写状态变更原因。



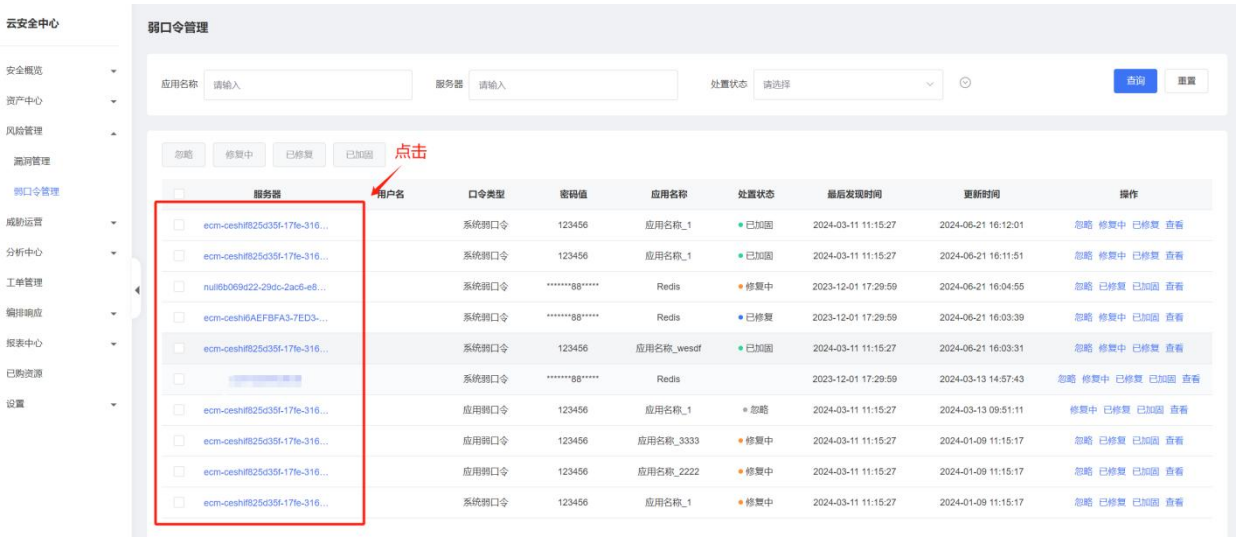
查看弱口令详情

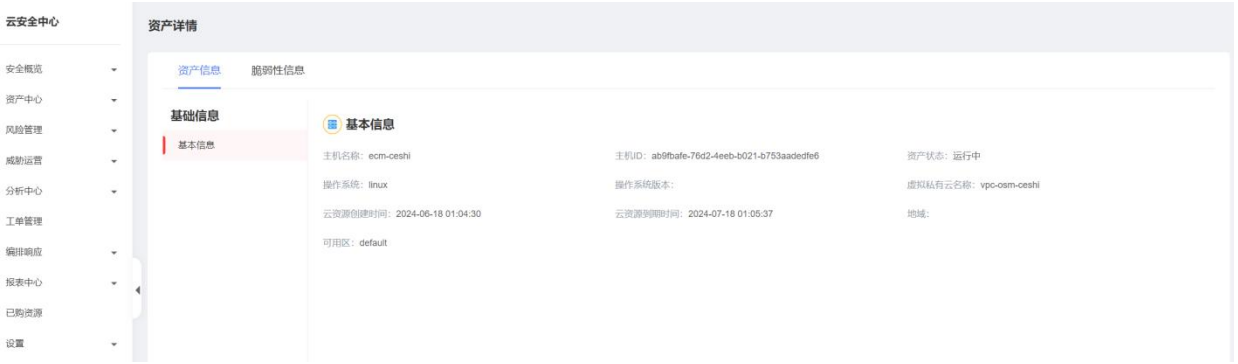
在弱口令详情中，可以查看所有历史状态变更记录的信息，包括：处置人、处置状态、处置说明、处置时间等。



查看弱口令关联资产

每条弱密码能够关联资产信息，可快速查看关联的资产详情。





4.4. 威胁运营

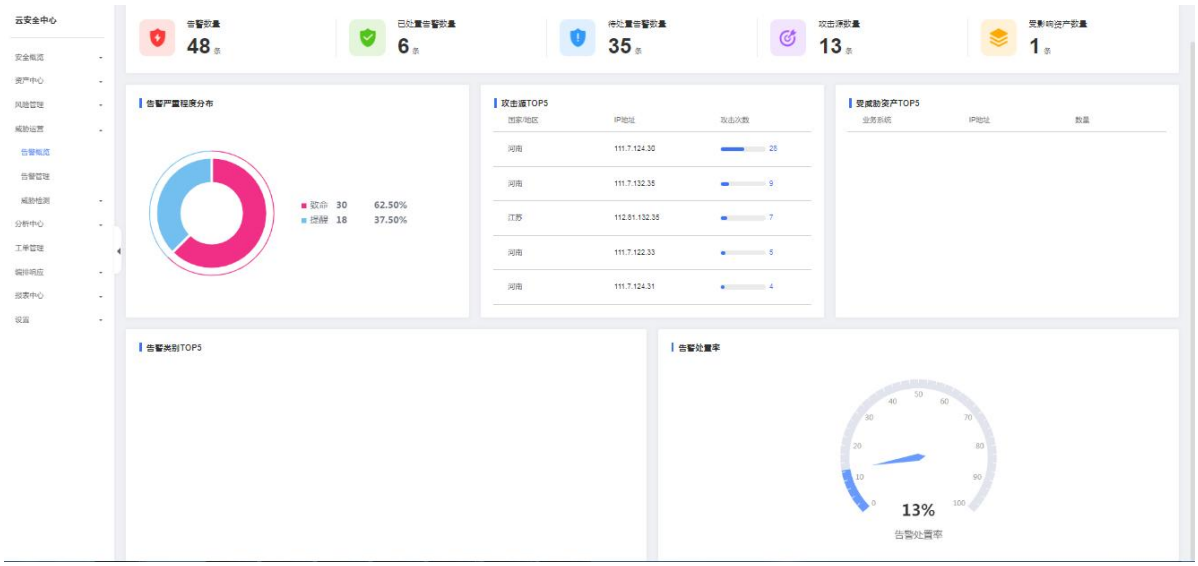
为了便于用户对平台告警数据进行整理分析与管理，威胁运营提供告警概览、告警管理、威胁检测三个便于管理告警的功能。

前提条件

已开通云安全中心实例。

4.4.1. 告警概览

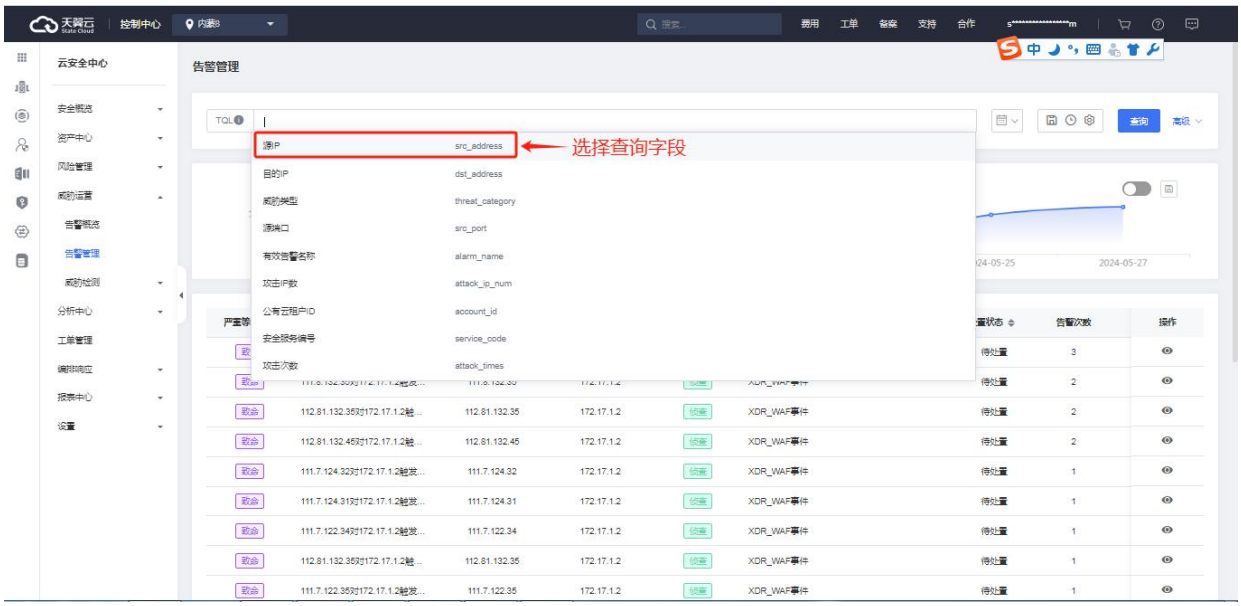
告警概览由告警数量、已处置告警数量、待处置告警数量、攻击源数量、受影响资产数量、告警严重程度分布、攻击源 TOP5、受威胁资产 TOP5、告警类别 TPO5、告警处置率的告警体现。

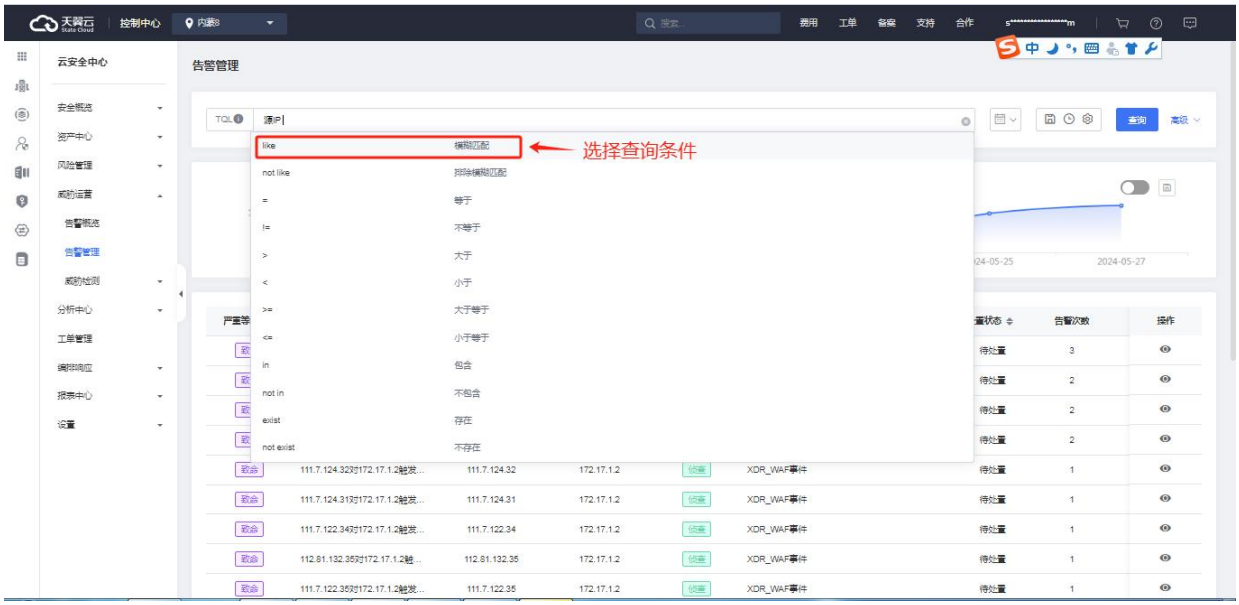


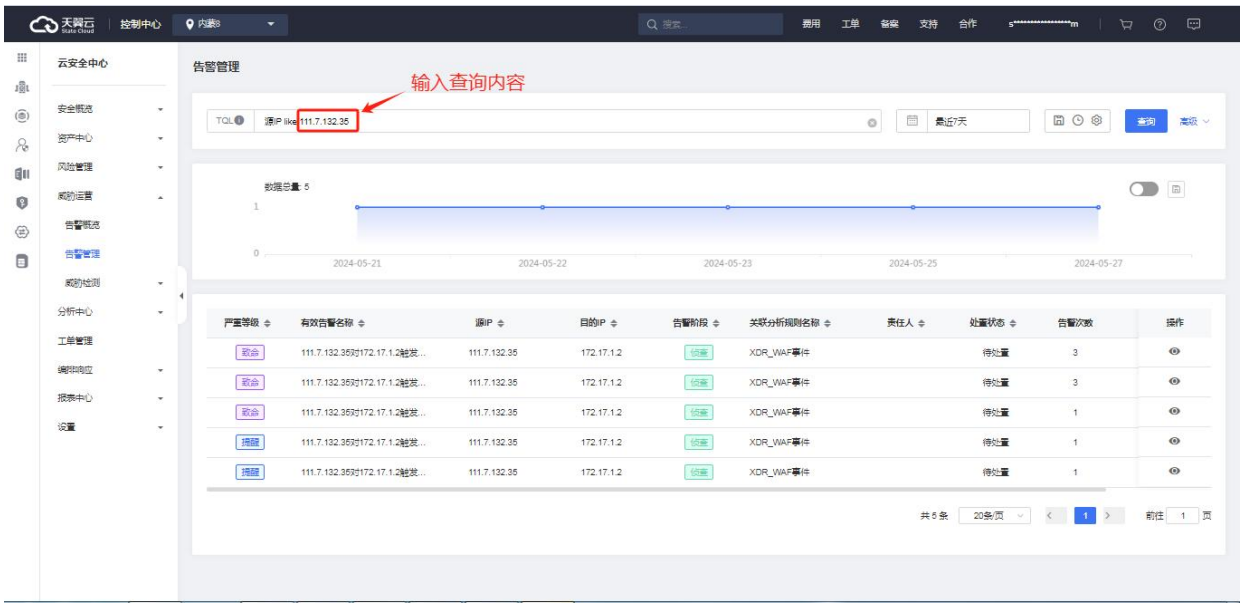
4.4.2. 告警管理

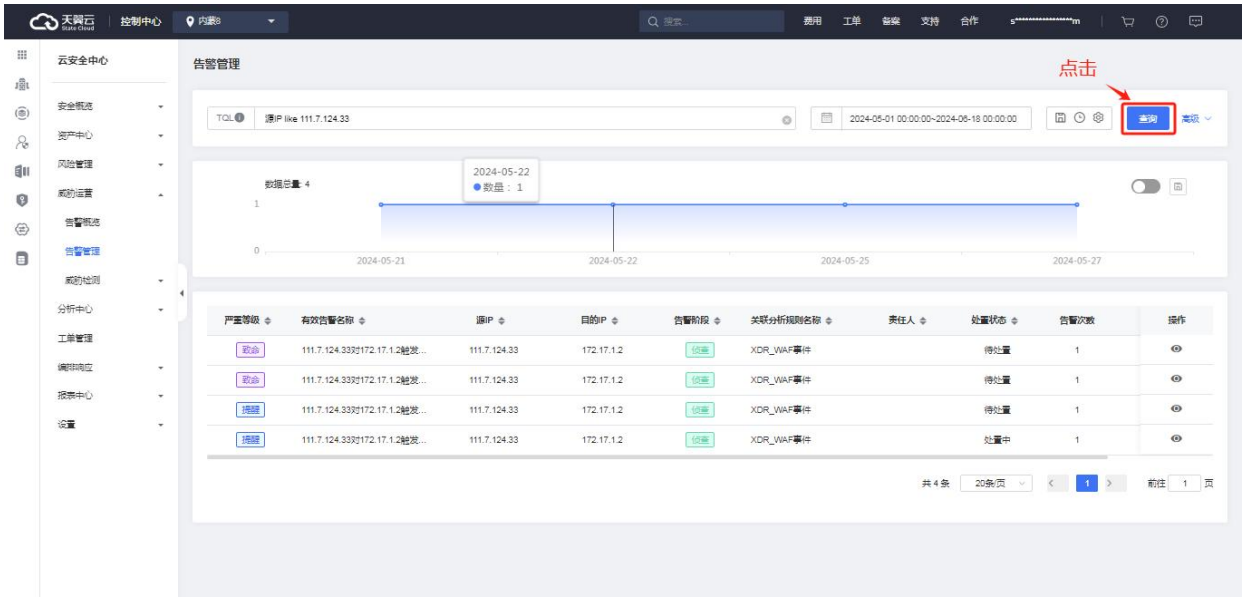
为用户提供查询、解决建议、处置威胁等功能

TQL 条件查询

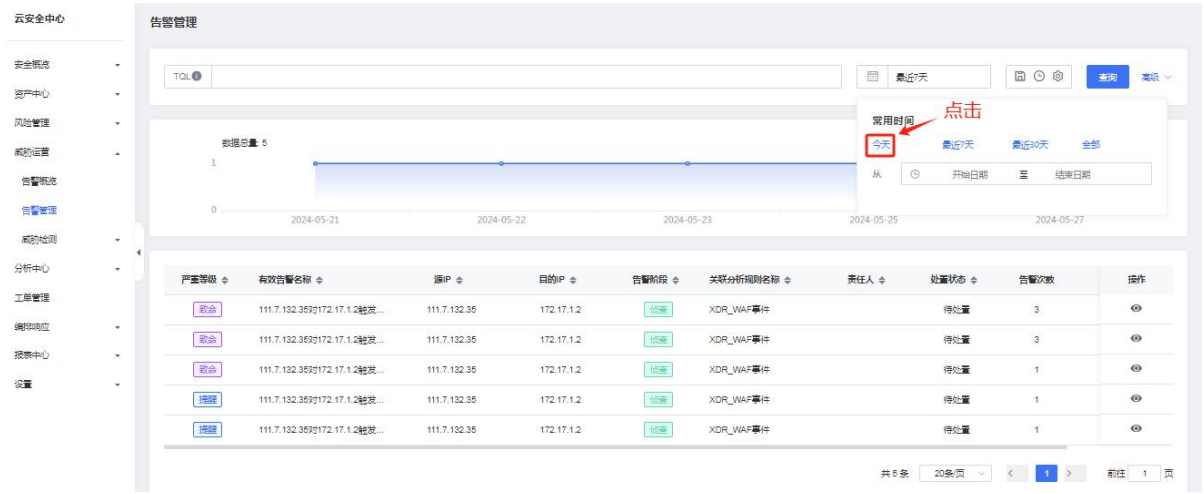

选择查询字段


选择查询条件

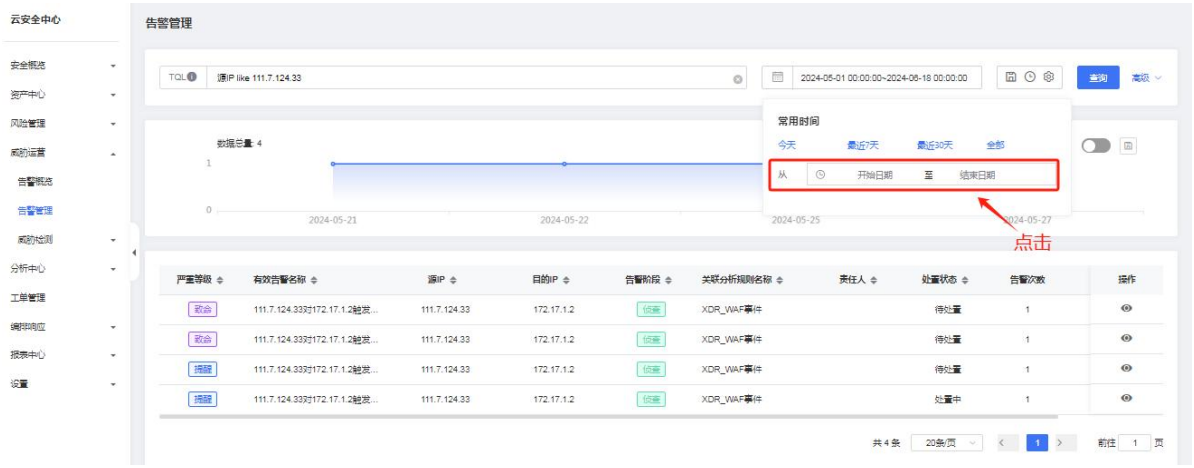


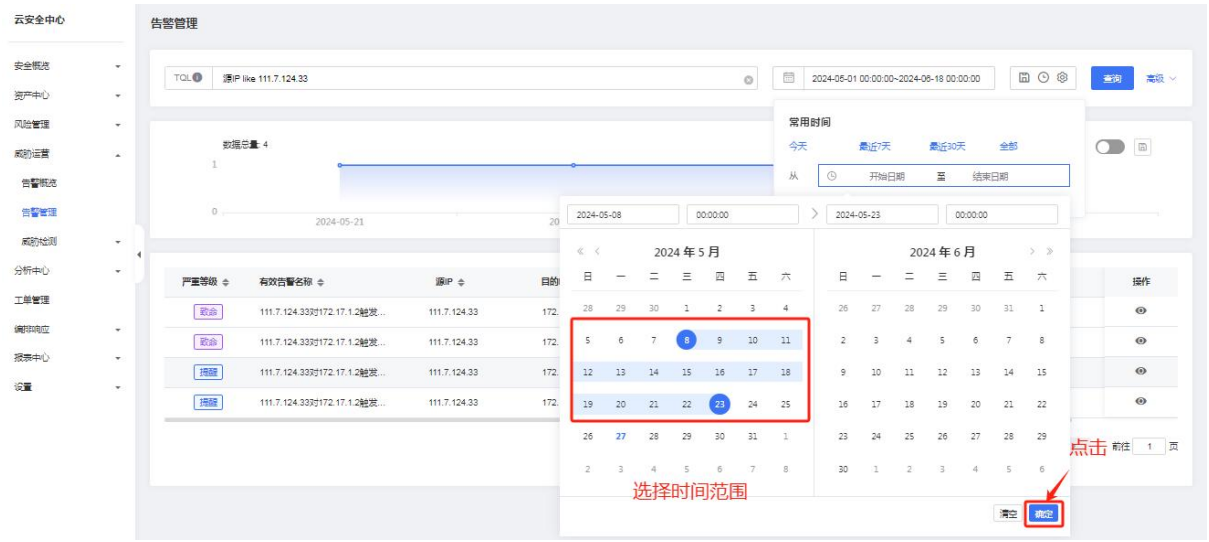


选择常用时间查询



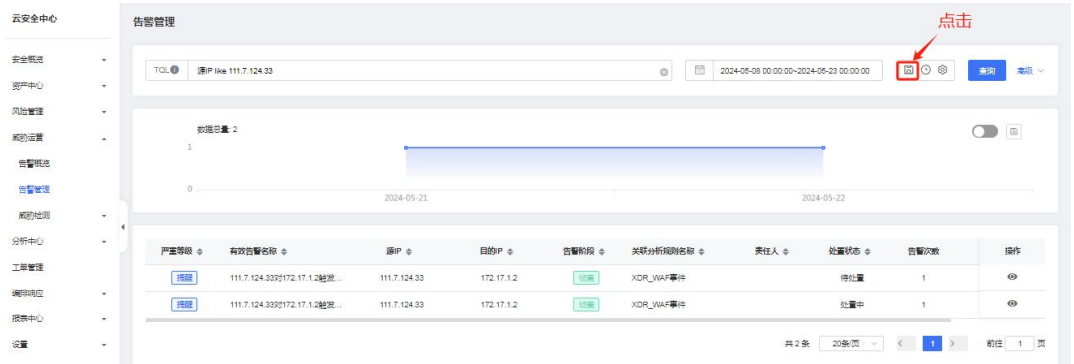
选择时间范围

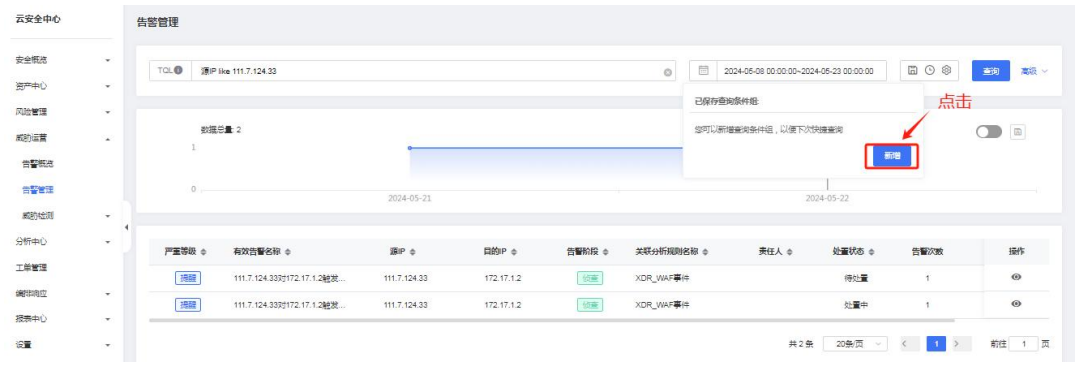


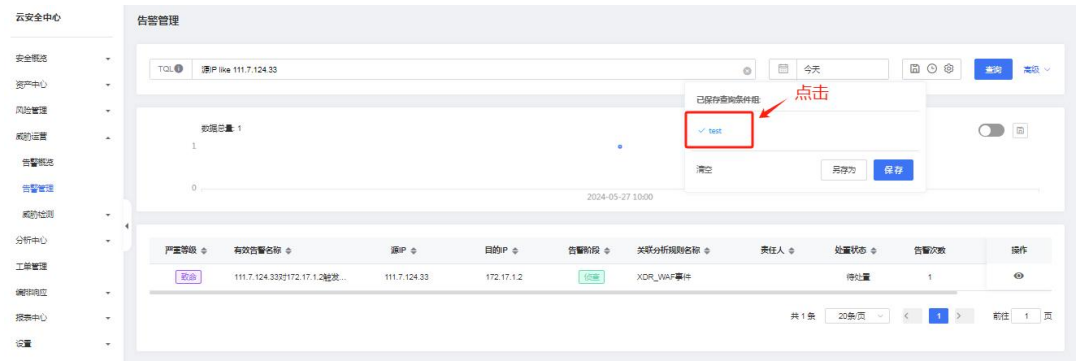


查询条件组

保存查询条件，方便用户查询

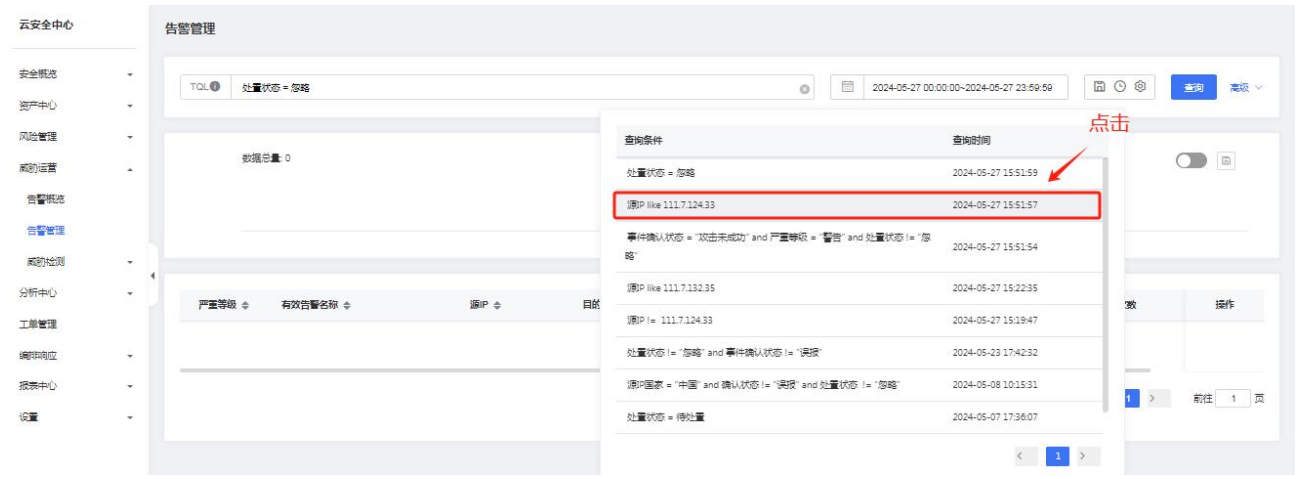






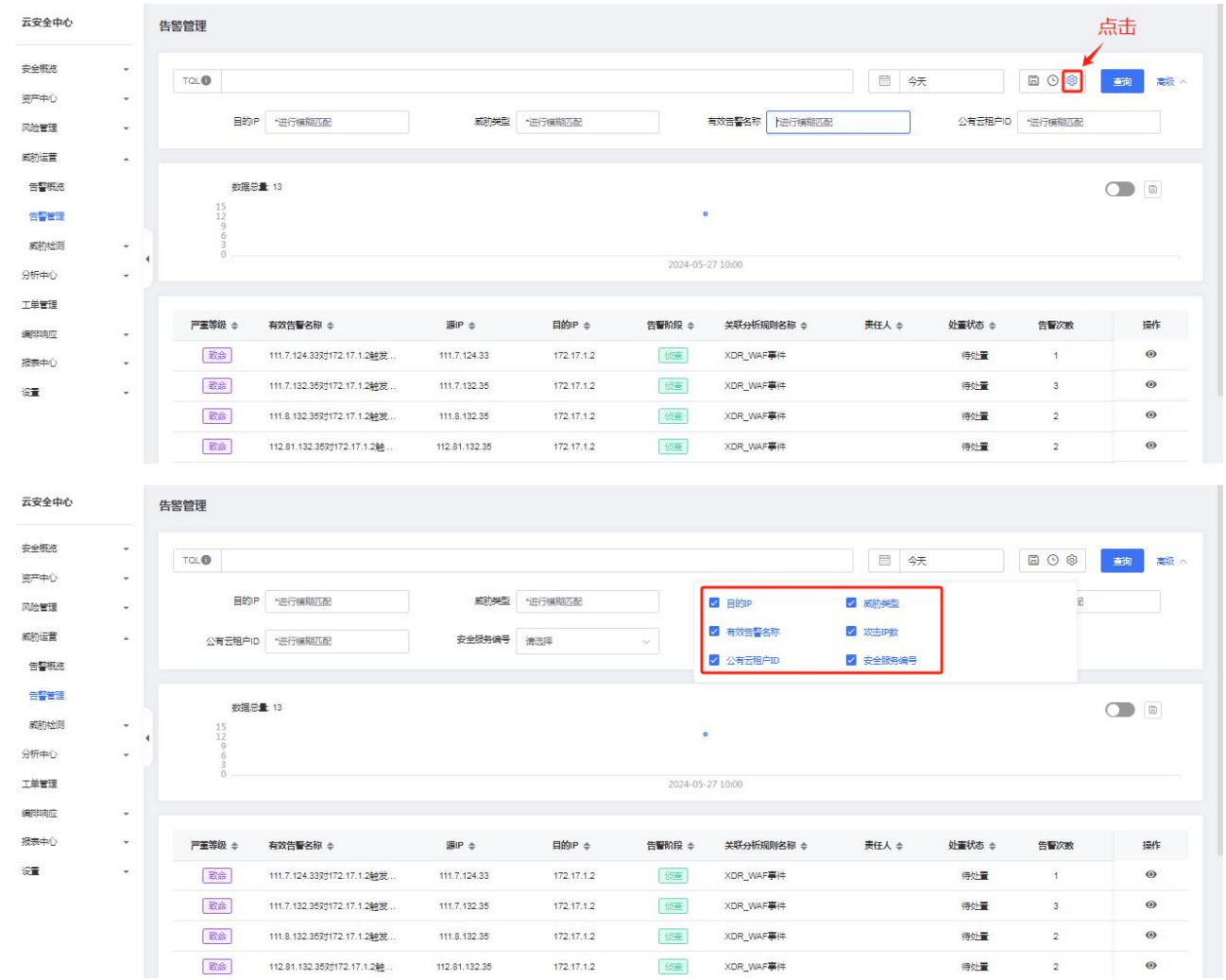
查看与选择历史查询记录

历史记录最多保存 100 条

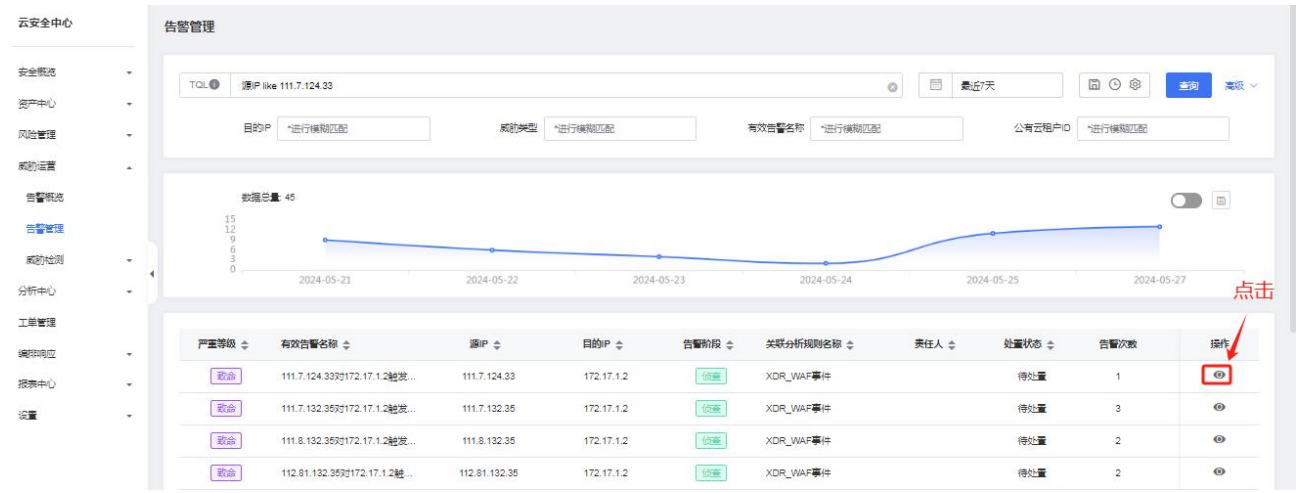


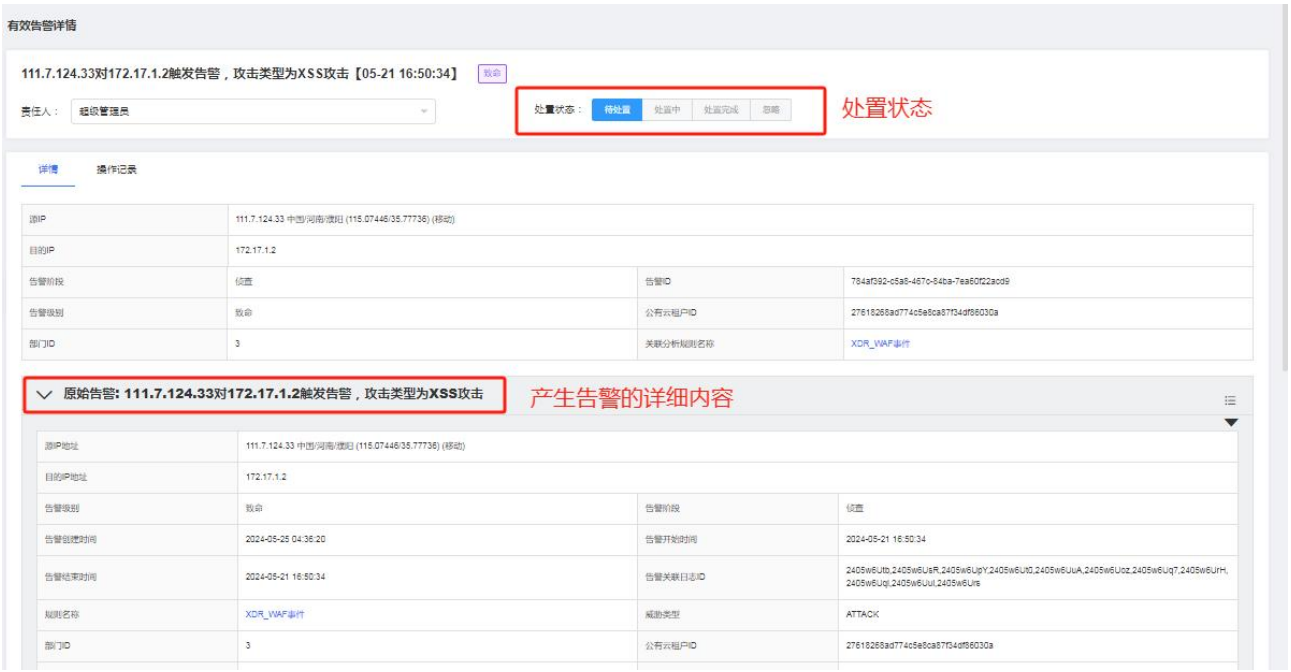
快速查询条件

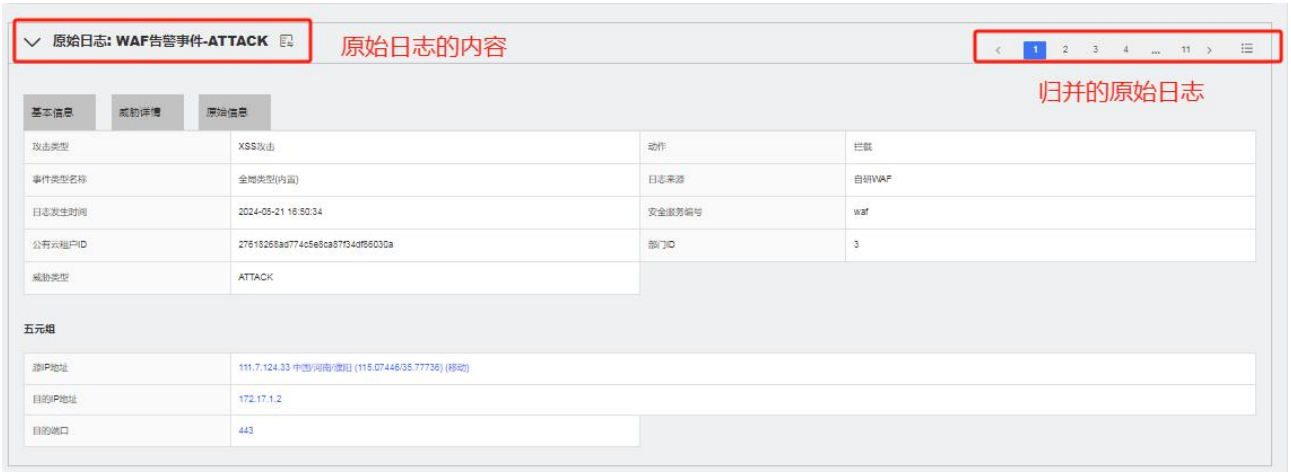
使用模糊查询时需要带*



查看告警详情


云安全中心
告警管理
安全概览
资产中心
风险管理
威胁运营
告警概览
告警管理
威胁检测
分析中心
工单管理
编排响应
报表中心
设置
TQL
源IP like 111.7.124.33
最近7天
查询
高级
目的IP
威胁类型
有效告警名称
公有云租户ID
数据总量: 45
2024-05-21
2024-05-22
2024-05-23
2024-05-24
2024-05-25
2024-05-27
点击
严重等级
有效告警名称
源IP
目的IP
告警阶段
关联分析规则名称
责任人
处置状态
告警次数
操作
111.7.124.33对172.17.1.2触发...
111.7.132.35对172.17.1.2触发...
111.8.132.35对172.17.1.2触发...
112.81.132.35对172.17.1.2触...
XDR_WAF事件
待处置
1
3
2


有效告警详情
111.7.124.33对172.17.1.2触发告警，攻击类型为XSS攻击【05-21 16:50:34】
责任人：
超级管理员
处置状态：
待处置
处置中
处置完成
忽略
处置状态
详情
操作记录
源IP
111.7.124.33 中国/河南/濮阳 (115.07446/35.77736) (移动)
目的IP
172.17.1.2
告警阶段
侦查
告警ID
784af392-c5a8-467c-84ba-7ea60f22acd9
告警级别
致命
公有云租户ID
27618268ad774c5e8ca87f34df86030a
部门ID
3
关联分析规则名称
XDR_WAF事件
原始告警: 111.7.124.33对172.17.1.2触发告警，攻击类型为XSS攻击
产生告警的详细内容
源IP地址
目的IP地址
告警级别
致命
告警阶段
侦查
告警创建时间
2024-05-25 04:36:20
告警开始时间
2024-05-21 16:50:34
告警结束时间
2024-05-21 16:50:34
规则名称
威胁类型
ATTACK
部门ID


原始日志: WAF告警事件-ATTACK
原始日志的内容
归并的原始日志
基本信息
威胁详情
原始信息
攻击类型
XSS攻击
动作
拦截
事件类型名称
全局类型(内置)
日志来源
自研WAF
日志发生时间
2024-05-21 16:50:34
安全服务编号
waf
公有云租户ID
27618268ad774c5e8ca87f34df86030a
部门ID
3
威胁类型
ATTACK
五元组
源IP地址
111.7.124.33 中国/河南/濮阳 (115.07446/35.77736) (移动)
目的IP地址
172.17.1.2
目的端口
443

4.4.3. 威胁检测

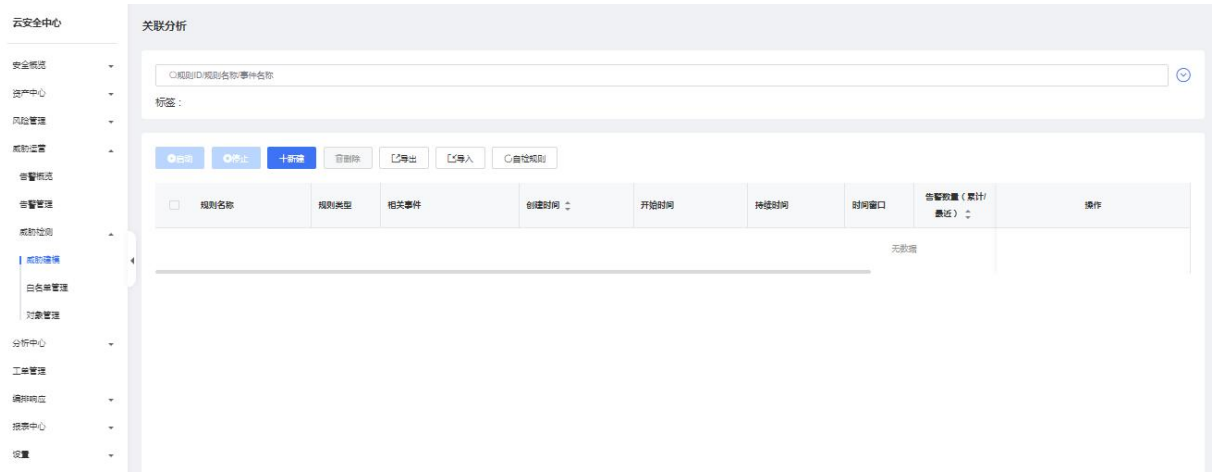
4.4.3.1. 威胁建模

通过关联分析规则，匹配威胁源是否满足告警条件。

可以通过关键字、快捷方式、规则类型和标签查询关联分析规则。

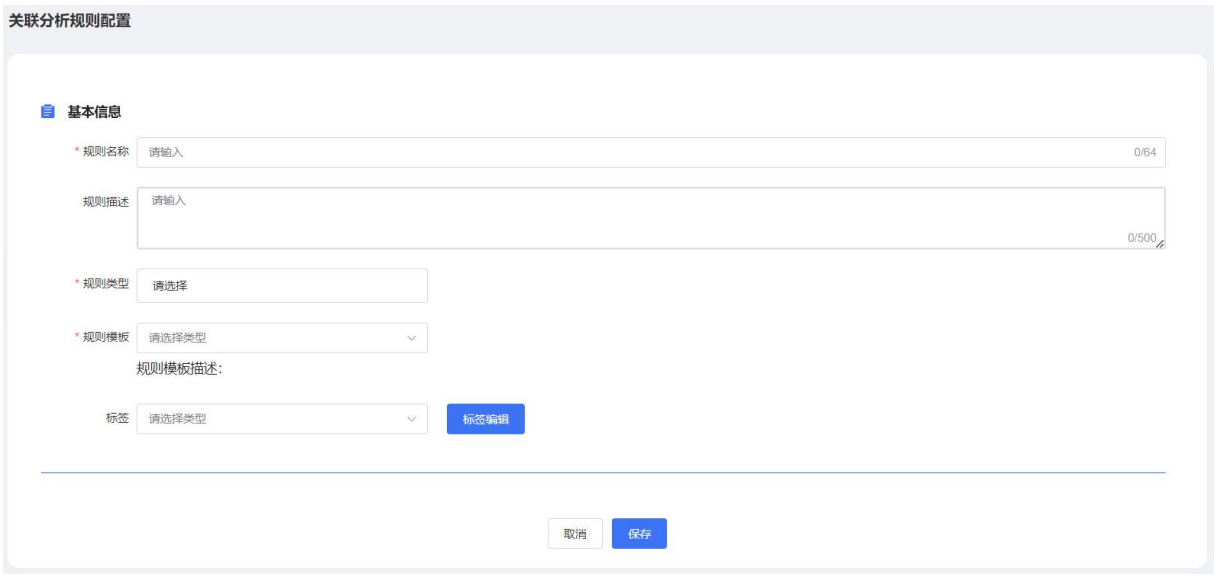
新建规则

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“威胁运营 > 威胁检测 > 威胁建模”。

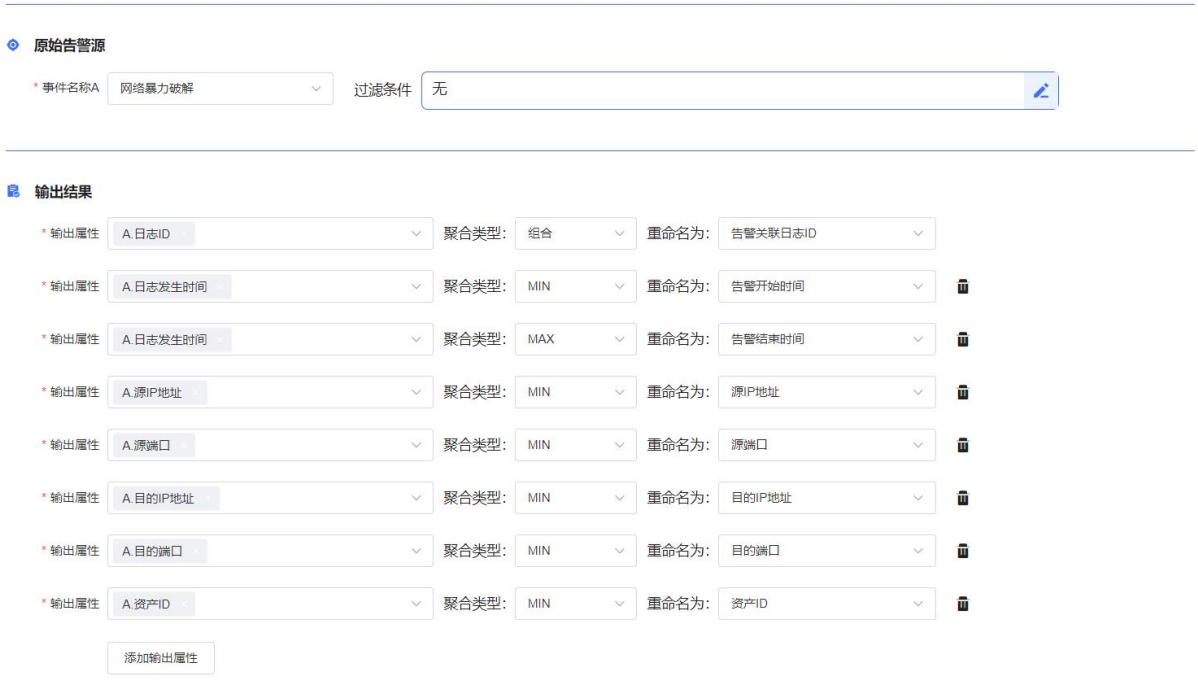


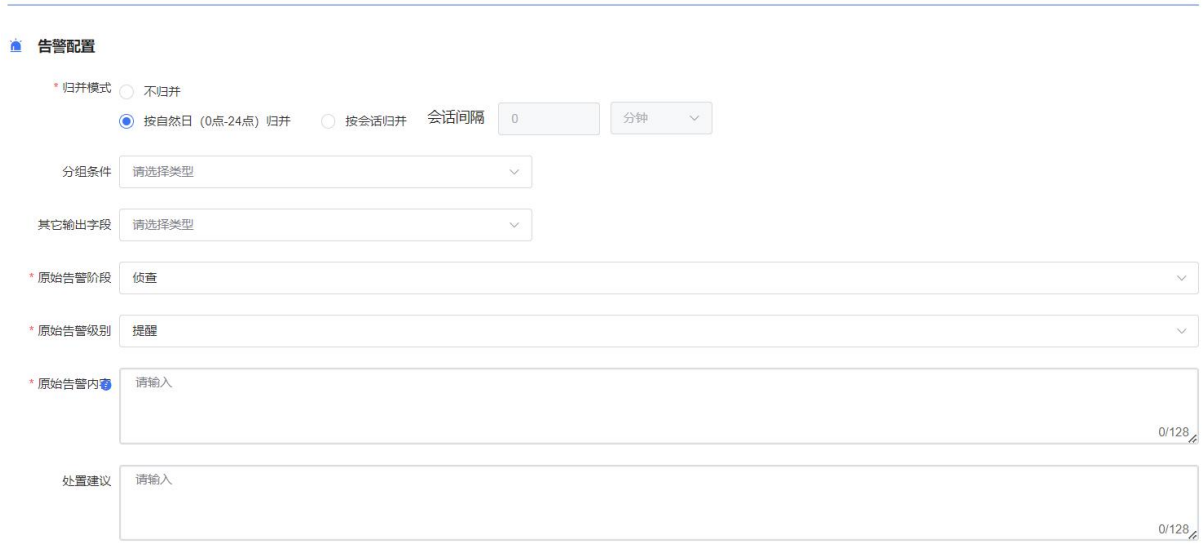
3. 单击“新建”。

4. 基本信息填写，带有*的为必填项。



5. 选择规则类型和规则模板后，还需要配置原始告警源、输出结果、告警配置等。





6. 配置完成后，单击“保存”。列表中可以看到新建的规则。

启动规则

新建规则默认为停止状态，在规则操作列单击启动图标，或勾选规则后，单击列表上方的“启动”，即可启动规则。

停止规则

在规则操作列单击停止图标，或勾选规则后，单击列表上方的“停止”，即可停止规则。

删除规则

> 注意：
>
> 启动状态的规则，不允许删除，删除规则前，请先停止规则。

在规则操作列单击删除图标，或勾选规则后，单击列表上方的“删除”，即可删除规则。

自检规则

进入规则页面时，系统会自动检测规则的可用性，也可以单击列表上方的“自检规则”，手动检测规则的可用性。

4.4.3.2. 白名单管理

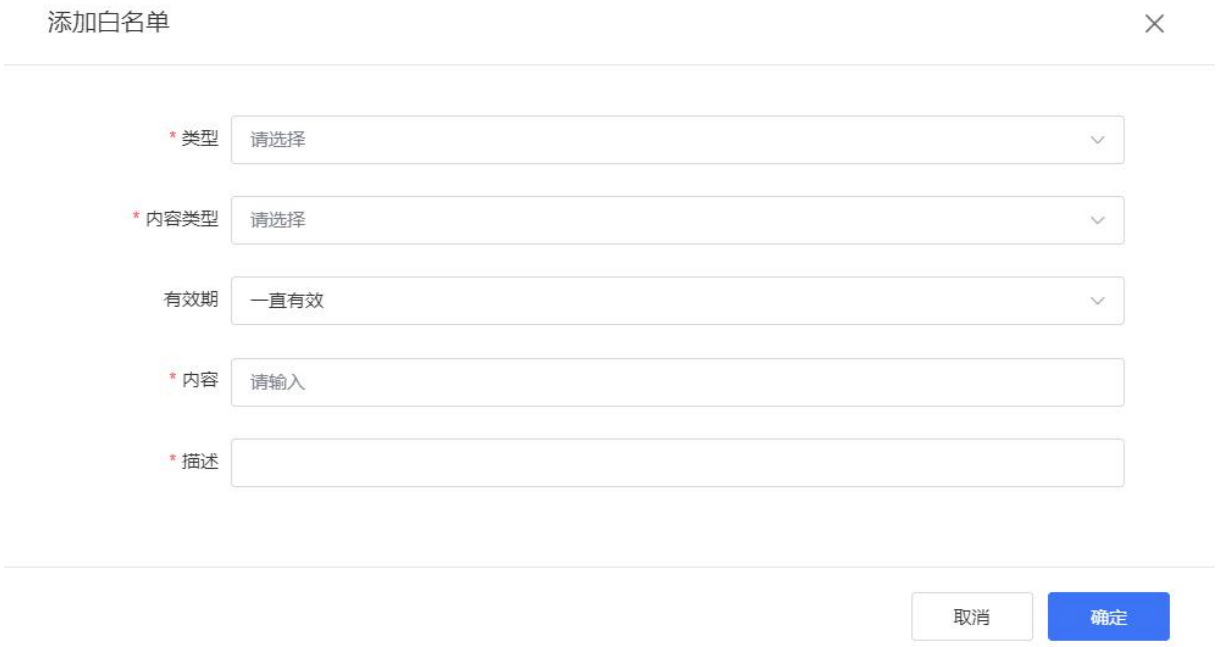
用于展示和管理全局的白名单信息。当发送的日志中包含全局白名单时，就不会触发 SAE 规则产生告警。

您可以在配置页面新增、修改、删除和查询全局白名单内容。

新增白名单

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“威胁运营 > 威胁检测 > 白名单管理”。

3. 单击“新建”，弹出添加白名单窗口，配置相关参数。
   白名单类型支持：IP、 DOMAIN、URL 、 ACCOUNT、PORT、LOOPHOLES。



4. 配置完成后，单击“确定”，新建白名单完成。

修改白名单

在白名单列表操作列单击编辑图标，在弹出的编辑白名单窗口中进行修改，修改完成后单击“确定”。

> 注意：
>
> 白名单“类型”和“内容类型”不支持修改。

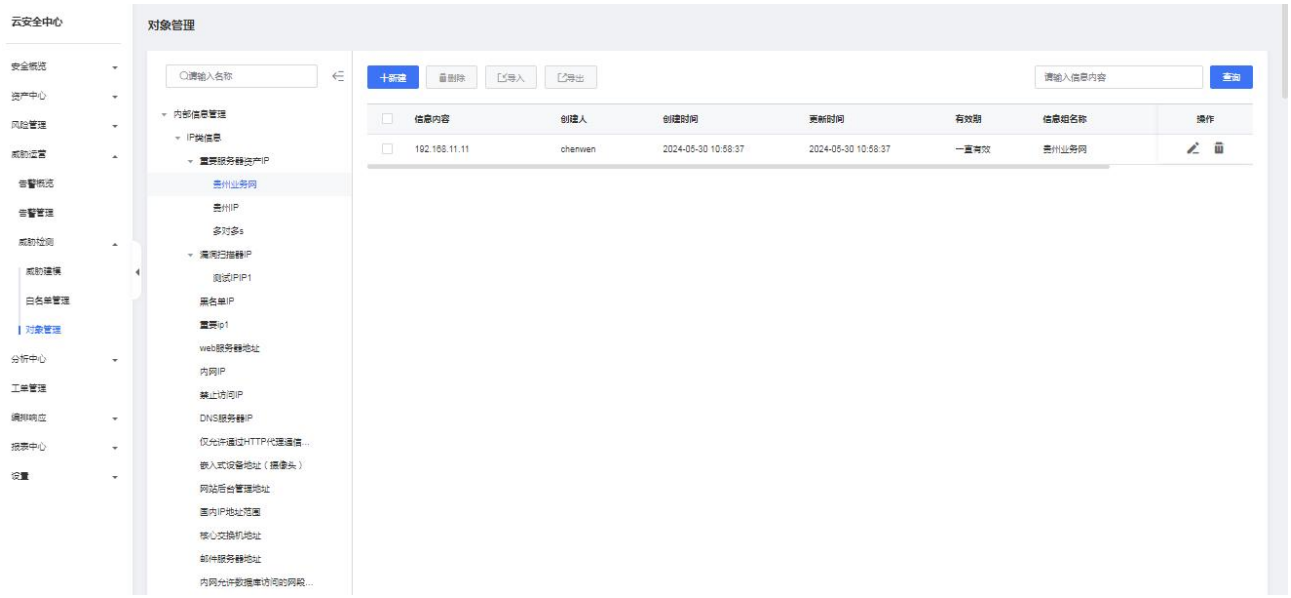
删除白名单

在白名单列表操作列单击删除图标，或勾选白名单后，单击列表上方的“删除”，即可删除白名单。

> 注意：
>
> 删除操作无法恢复，请谨慎操作。

4.4.3.3. 对象管理

展示有价值的内部信息，在关联分析时，对于 IP 类型、数字类型或字符类型的字段，可以添加过滤条件属于信息，便于进行分析。通过导入内容包，系统已内置一些信息。



4.5. 分析中心

分析中心可分别针对日志详情、告警信息和资产信息进行列表或图形化展示。以时间为横轴、发生事件的数量为纵轴，展示符合查询关键字和查询时间窗的事件趋势图。

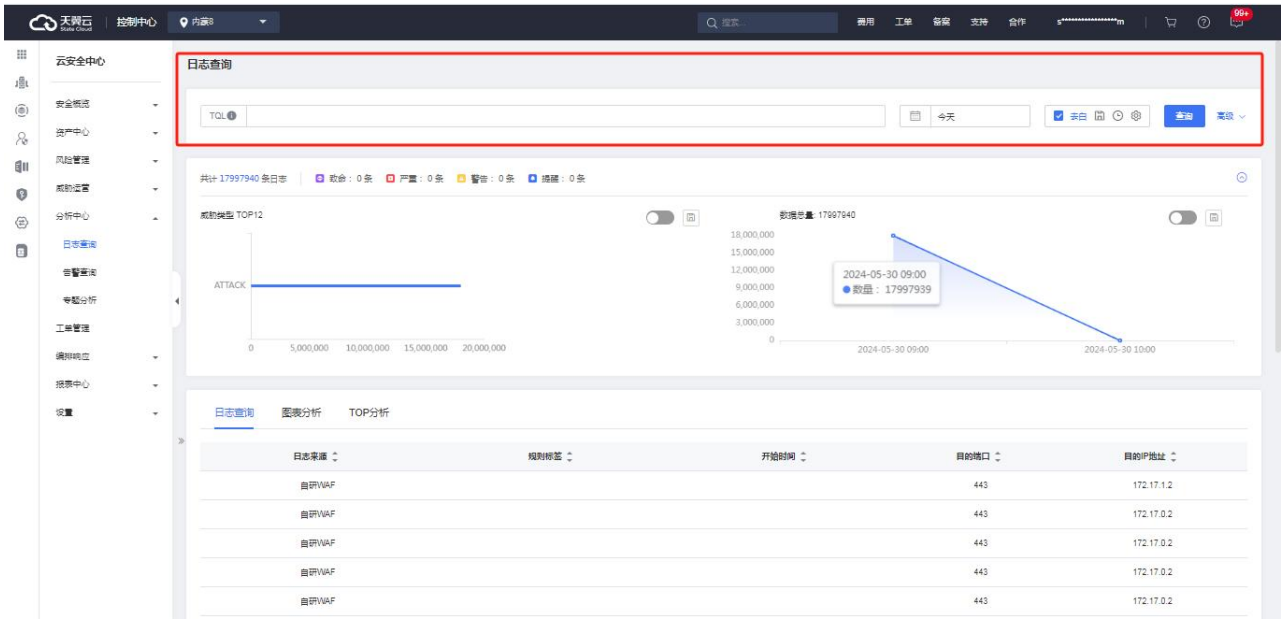
前提条件

已开通云安全中心实例。

4.5.1. 日志查询

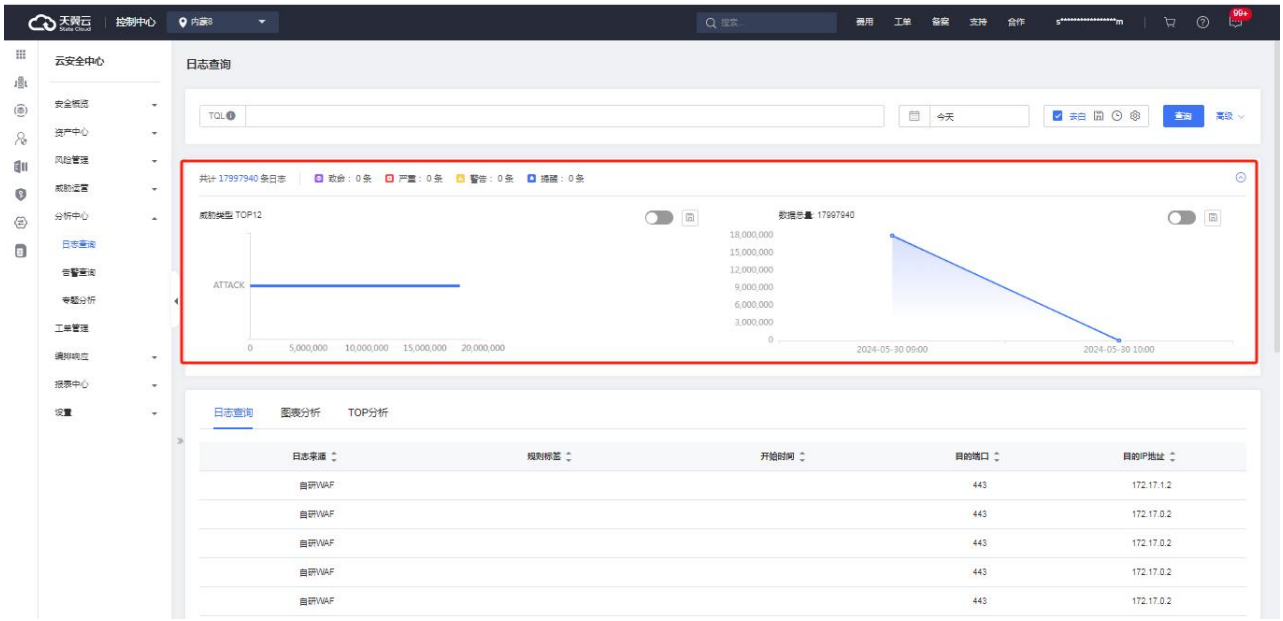
查询条件

头部为自定义查询条件，方便管理人员通过关键字段信息或者时间段获取更精确的数据。具体操作参考“告警管理”。



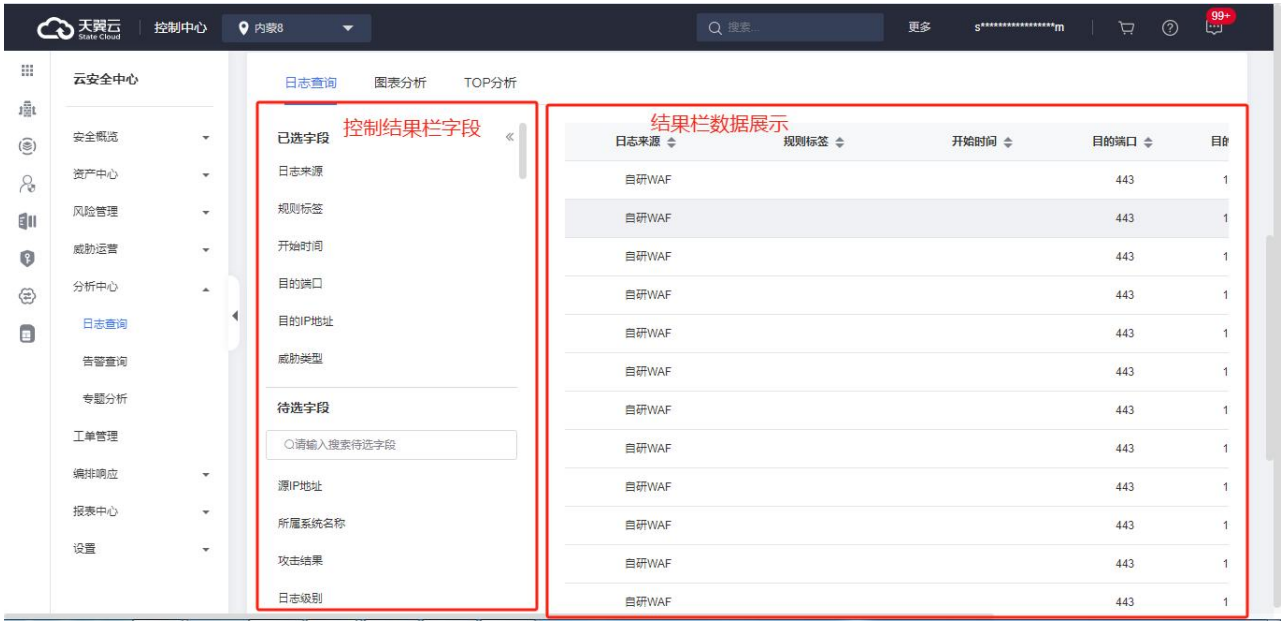
线性图

中间的线性图，展现在某个时间的日志数据量。



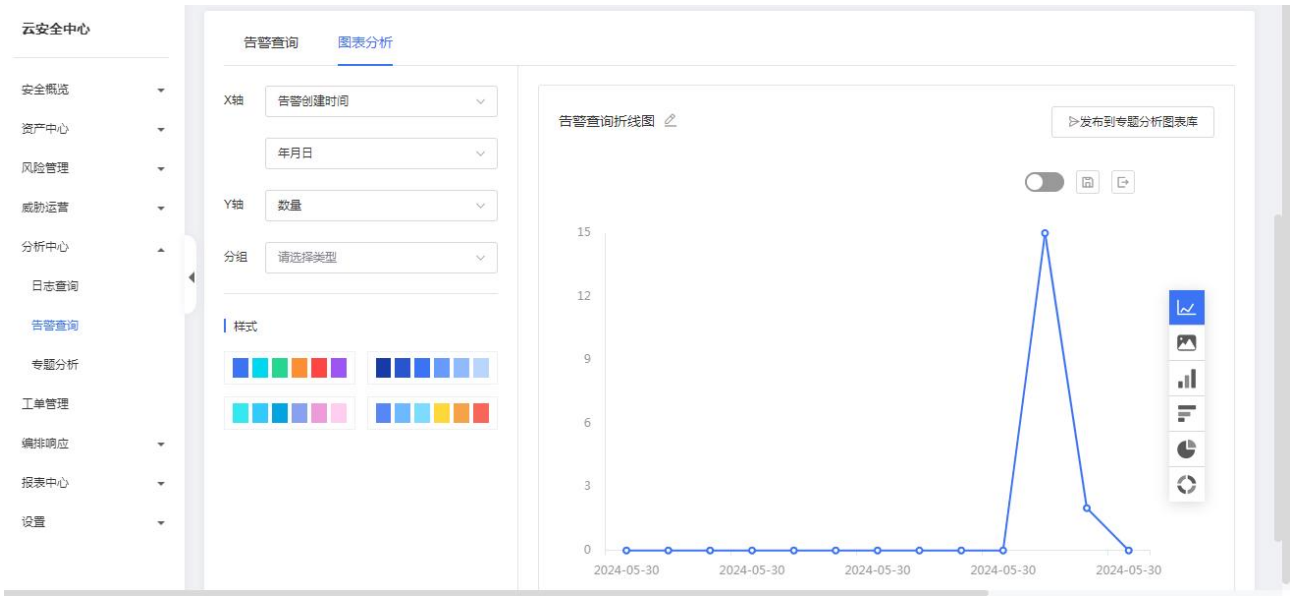
日志查询

最下面表格是展示查询的数据，表格中展示的字段可以自己定义，每条数据下拉能够看到详细数据。



图表分析

图表分析可以选择不同的图表类型与样式，并可以自定义发布到专题分析图表库。

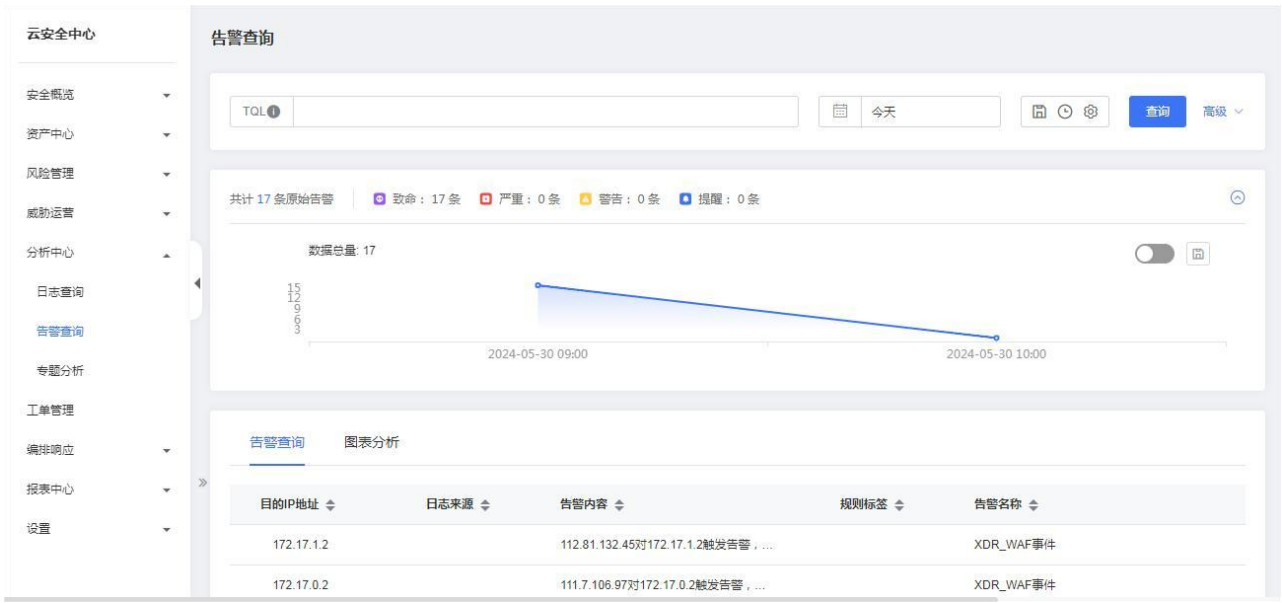


单击“发布到专题分析图表库”，弹出如下对话框，选择分类后，单击“确定”，将图表发布到专题分析图表库。

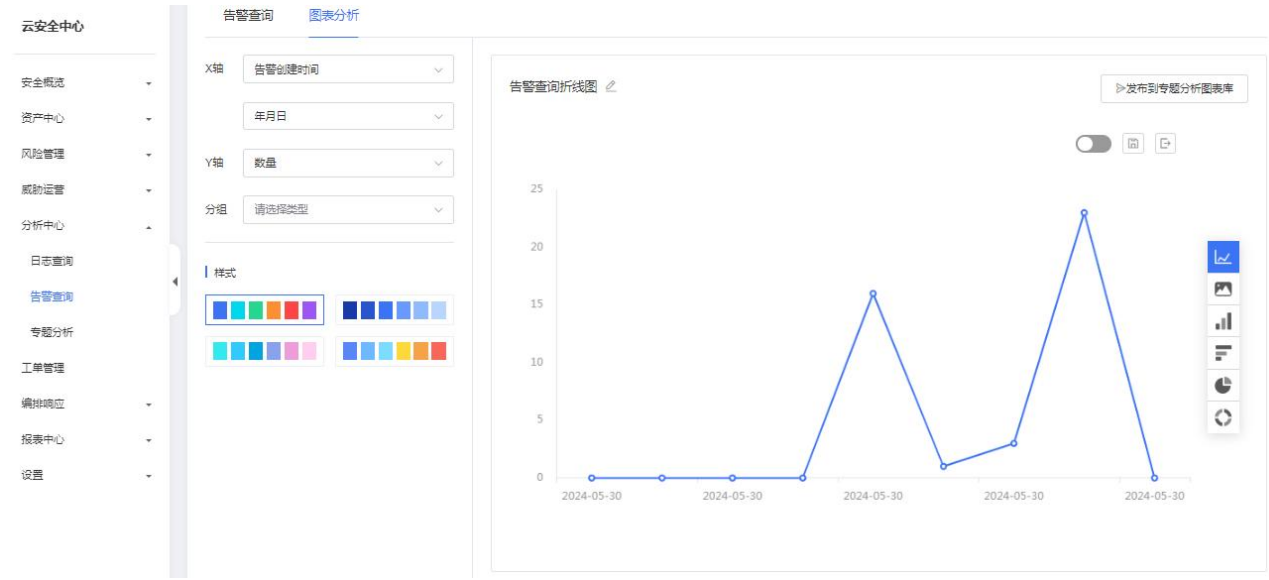
4.5.2. 告警查询

告警查询具体操作请参考“日志查询”。

告警查询



图表分析



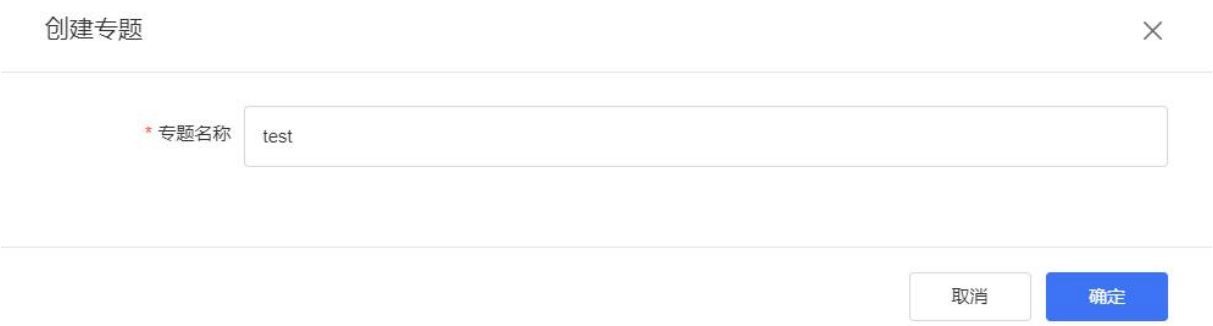
4.5.3. 专题分析

专题分析可以提供多个内部页签的大盘展示页，用户可以新增、编辑、删除专题。

创建专题

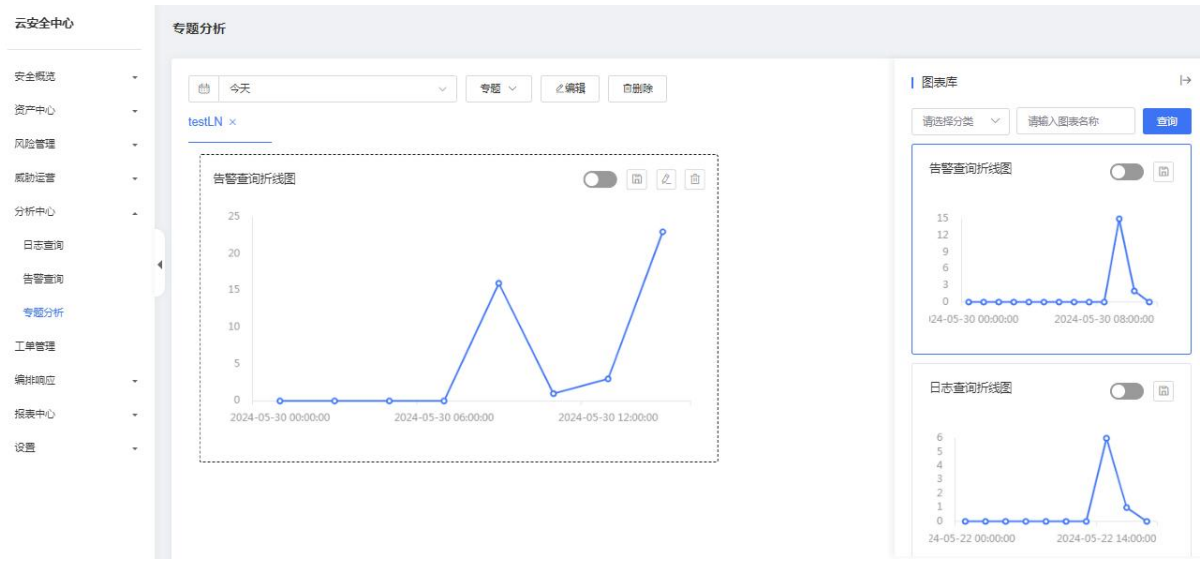
1. 登录云安全中心控制台。
2. 在左侧导航栏选择“分析中心 > 专题分析”。
3. 单击“专题 > 创建专题”。

4. 在弹出的创建专题对话框中，填写专题名称，单击“确定”，完成创建。

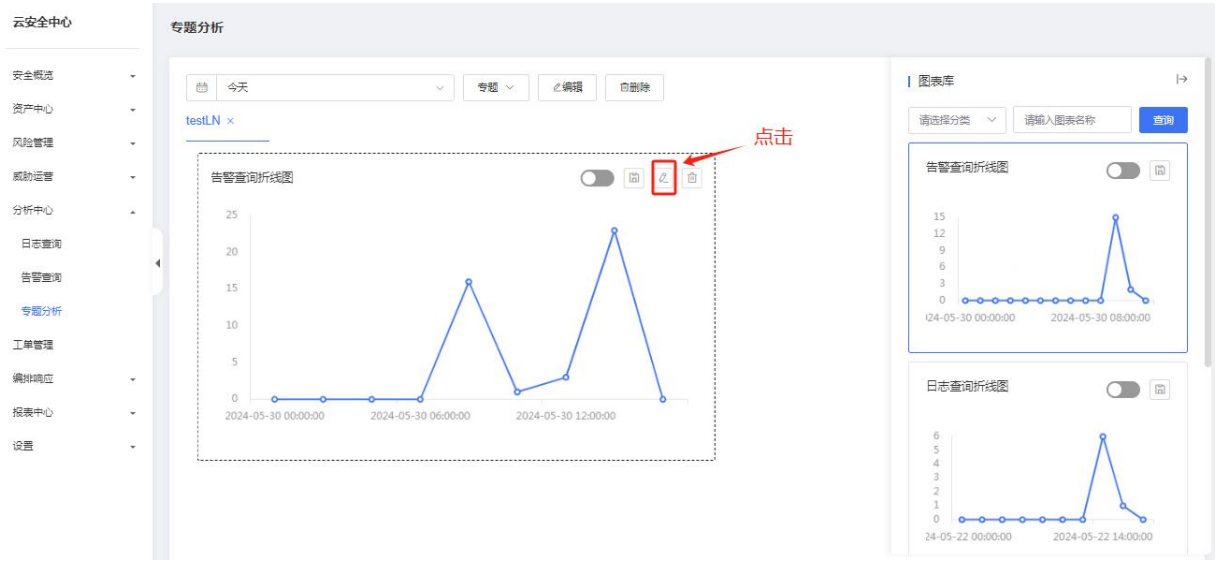


配置专题

1. 从图表库中拖拽所需图表至左侧空白处。



2. 如果需要编辑图表，单击图表框右上角的编辑按钮，会跳转至对应图表分析页面。如下图点击后会跳转至“告警查询”的图表分析页面。编辑完图表后，需要重新将图表发布到专题分析图表库。



4.6. 工单管理

工单管理是为了便于对告警的统一管理、处置与后续分析。工单管理用于告警的统一管理，进行事件的处置。工单管理界面可以很详细地看到告警的基本属性，以及告警工单的处置情况，事件管理界面可以以工单编号、事件名称、事件分类、事件级别、工单状态、事件来源及时间段查询指定的事件工单。

前提条件

已开通云安全中心实例。

新增事件

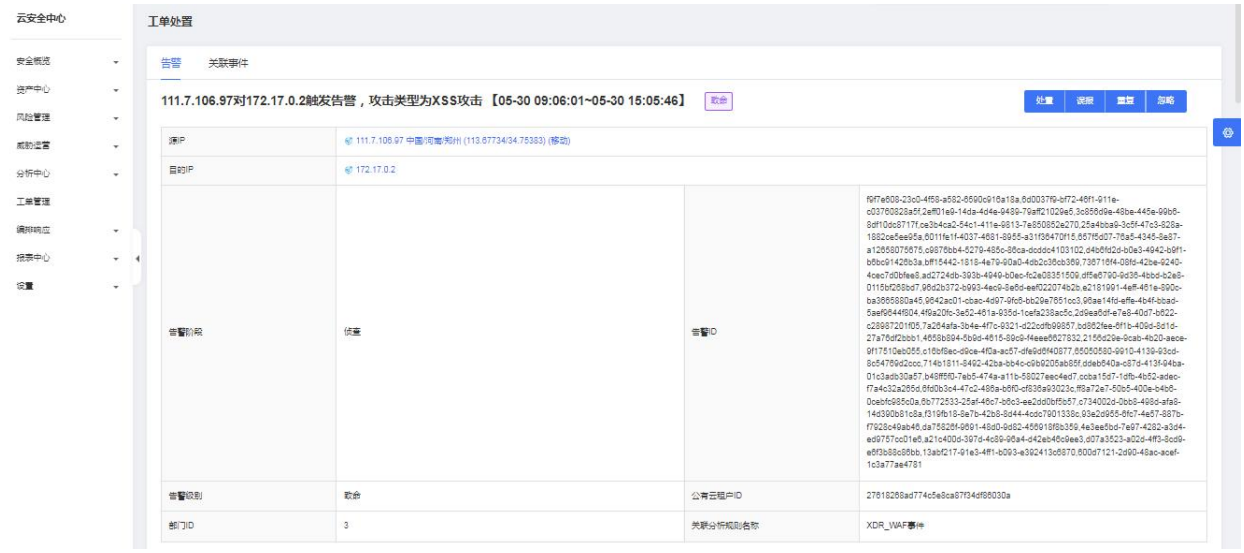
1. 登录云安全中心控制台。
2. 在左侧导航栏选择“工单管理”。
3. 点击“新建”，选择“默认模板表”，手动新增事件。

4. 在新增事件窗口中，配置相关参数后，单击“保存”。

查看事件详情

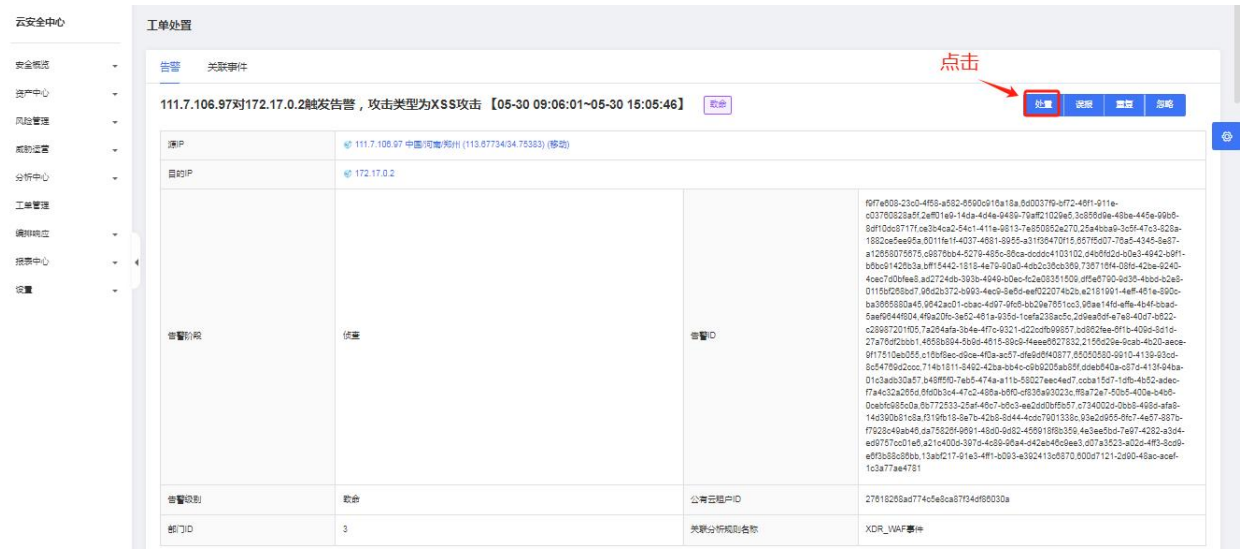
在事件列表中，点击事件名。

进入工单处置页面，可以看到事件相关详细信息。

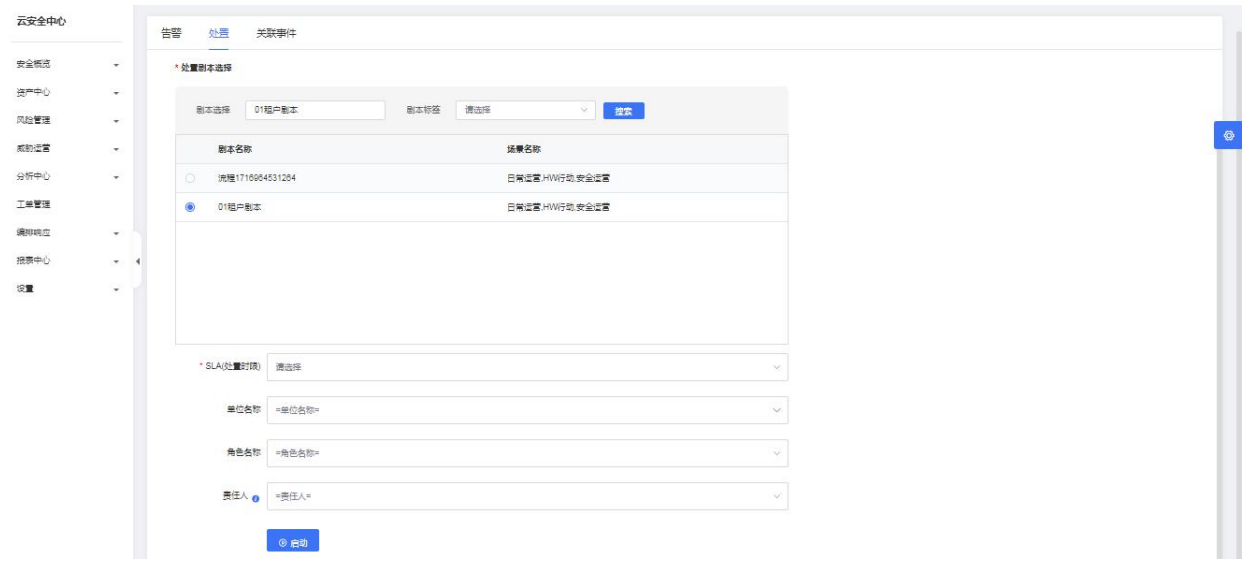


处置事件

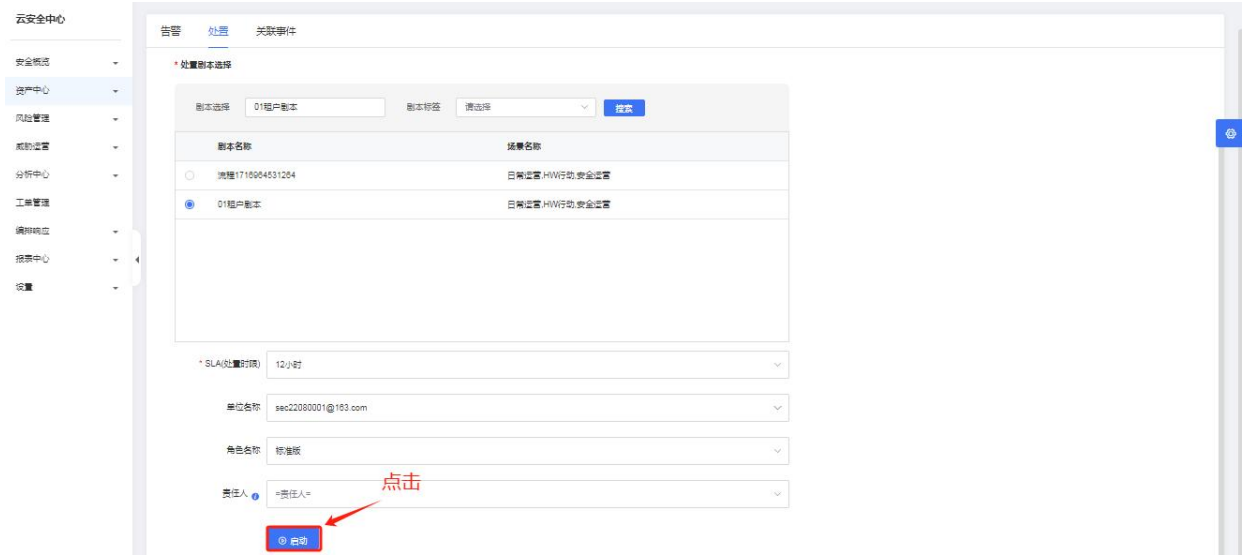
在事件详情界面，点击“处置”。



进入处置界面，可以选择处置剧本、处置时限及责任人。

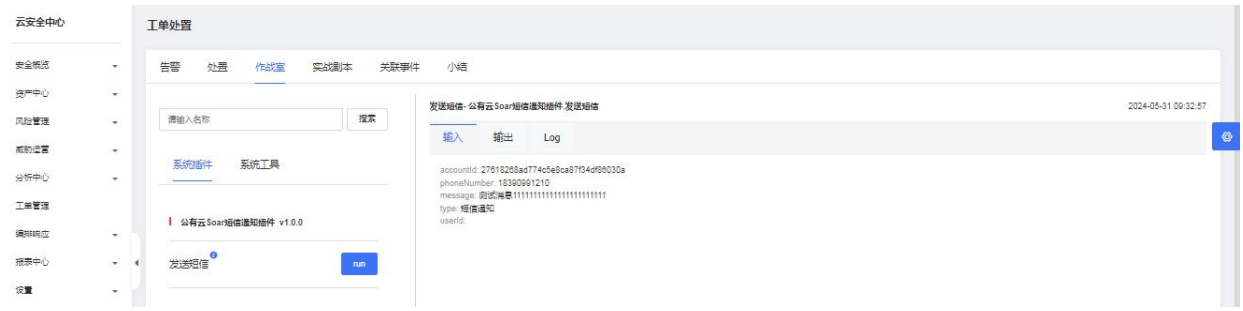


配置完成后，点击“启动”。

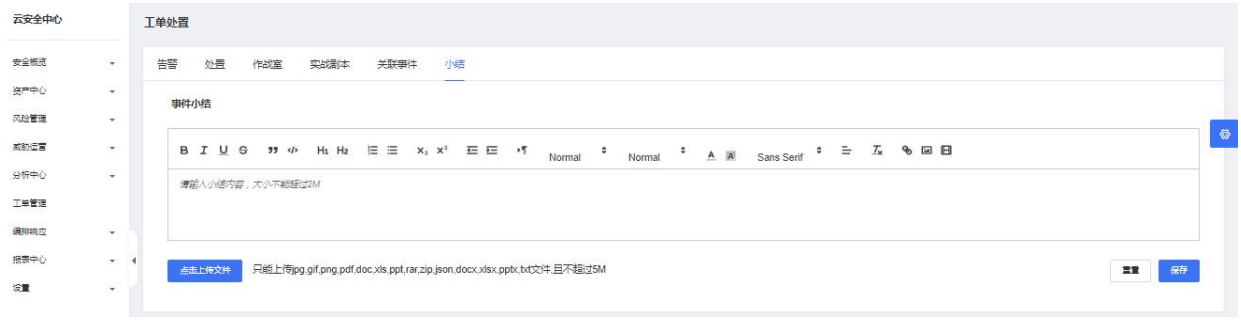


在处置界面，查看处置记录，并可进行相关的处置。

进入作战室，可以快速调用插件进行自动化处置，左侧是插件名称与介绍，右侧是按执行时间排序的已执行插件的输入、输出和 Log 日志信息。



事件处置完成之后，用户可以编辑小结，同时可以上传相关文件，方便后续的回顾分析。



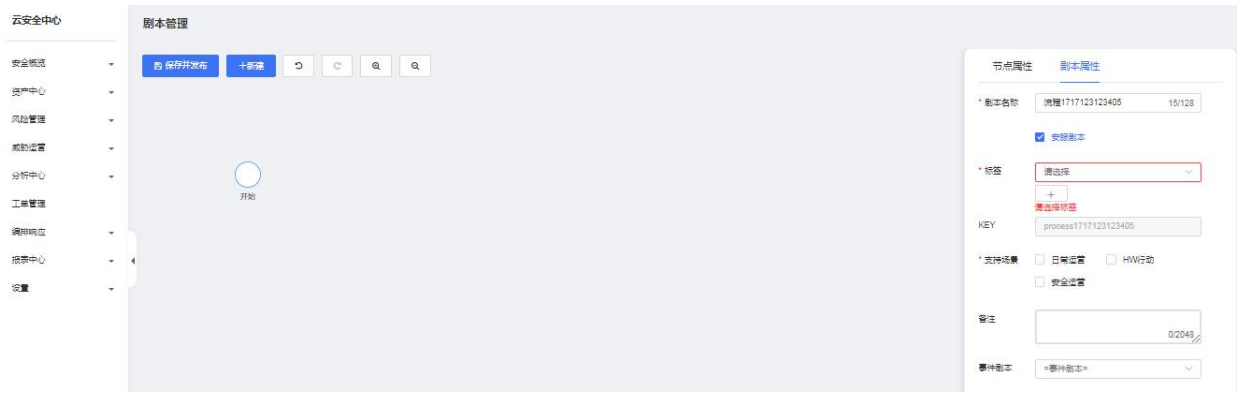
4.7. 编排响应

4.7.1. 剧本管理

为了提高告警处置的自动化程度及效率，提高告警解决方案的复用性。可以使用剧本将某些处置操作模板化，程序化。在类似告警发生时，可以自动规则匹配或人工选择相关剧本进行自动化的处置。其中的剧本匹配规则，则用于告警发生后，自动匹配并调用剧本进行操作。剧本管理模块则用于对这些剧本和剧本匹配规则进行统一管理。剧本管理的的剧本列表，可以查看、新建、编辑、导入导出相关的剧本。

新建剧本

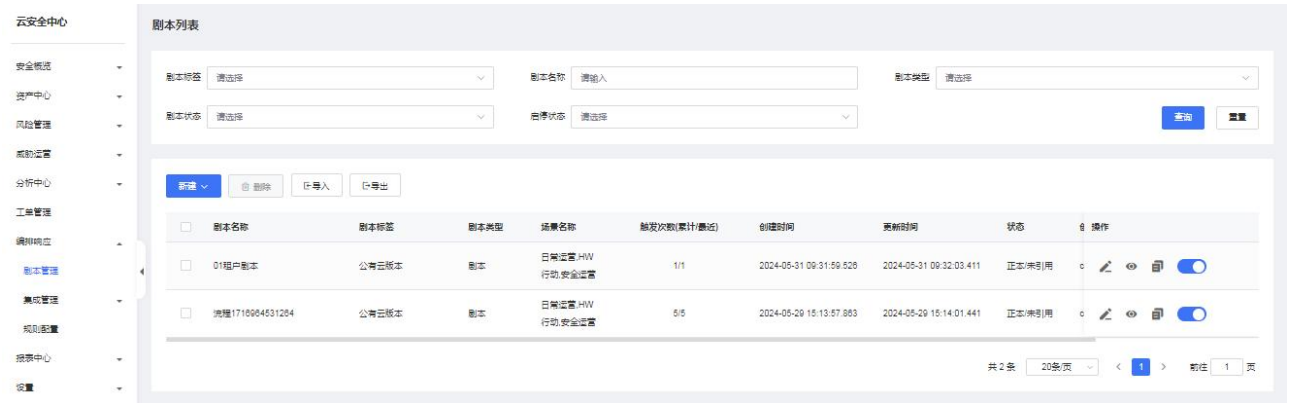
打开剧本管理的剧本列表界面，点击“新建”，创建一个只有一个开始节点的新剧本。剧本新增页面右侧可对剧本属性进行编辑。



说明：

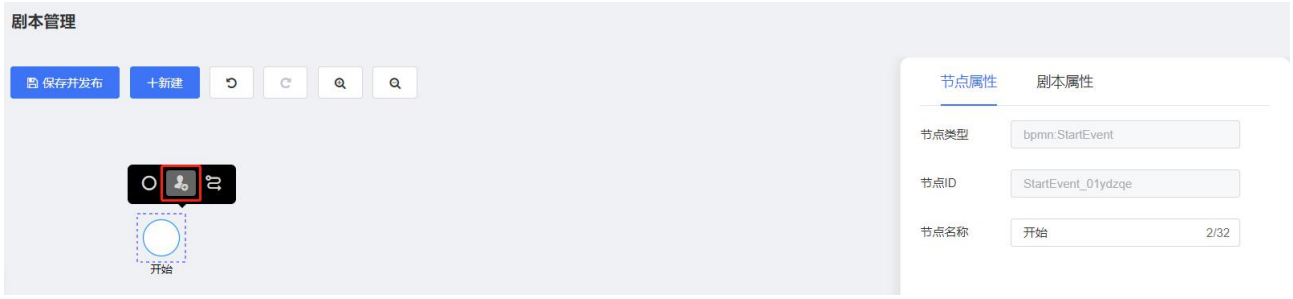
- 一个剧本有且只有一个开始节点和结束节点。
- 每个用户在新增的剧本编辑界面停留过长时，会最多保留一份新增草稿，在用户下次新增时会提示是否进入草稿。
- 在对已存在剧本进行修改时，若在修改页面停留时间过长，会自动为改剧本保留一份草稿，在下次重新对剧本进行编辑时提示是否进入草稿。
- 剧本保存时会对剧本进行校验，若该剧本存在不能到达或不能结束的孤立节点，需用户完善后才能保存。后续版本将会升级启停功能，非正常剧本允许保存，不允许启用。

新建完成后，可以在列表中看到新建的剧本。

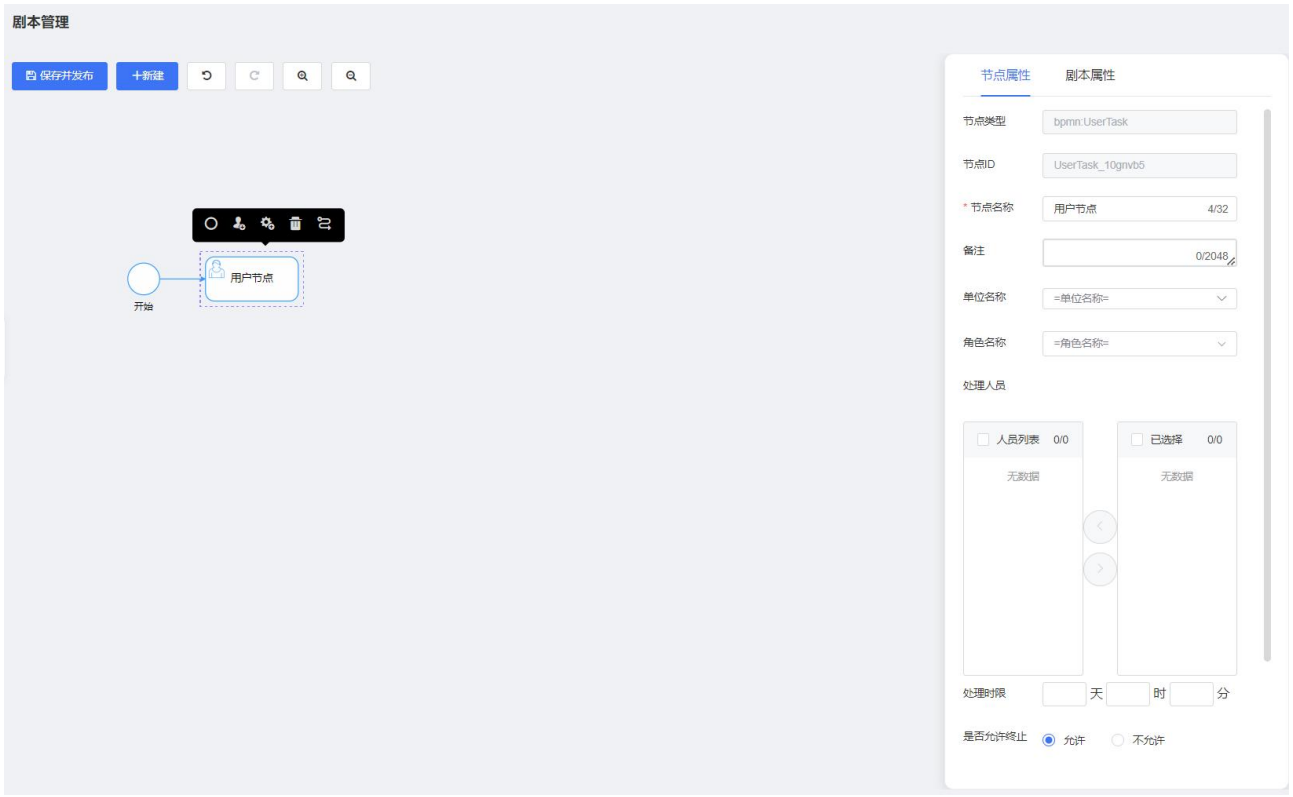


新增剧本节点

选择节点后，点下如下按钮，新增剧本节点。

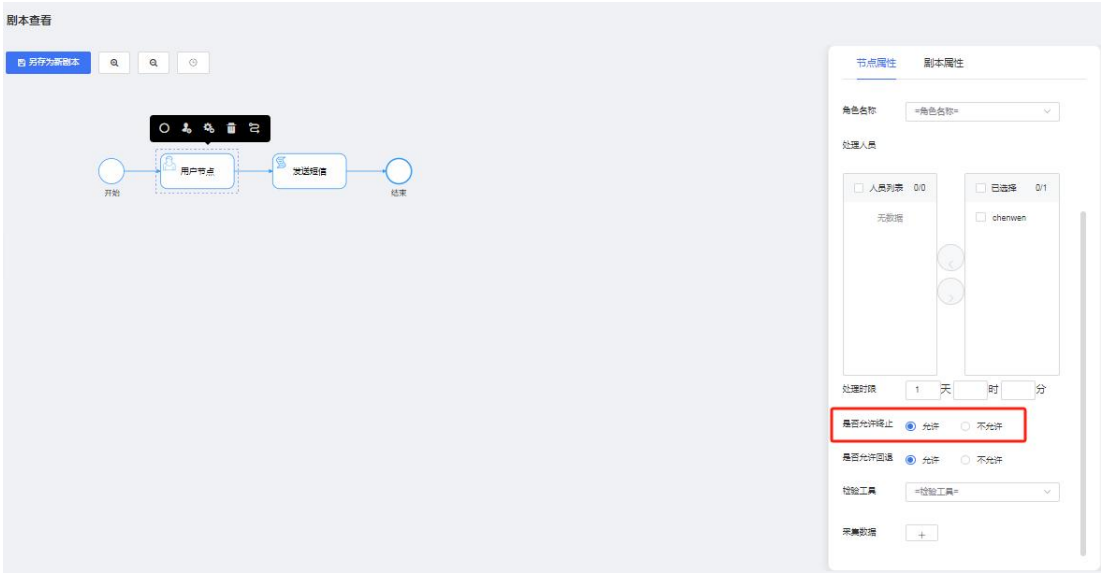


新增的节点默认为用户节点。选取节点后，右侧可对节点属性进行编辑。



- 是否允许终止

  终止功能，剧本编辑界面如图所示。

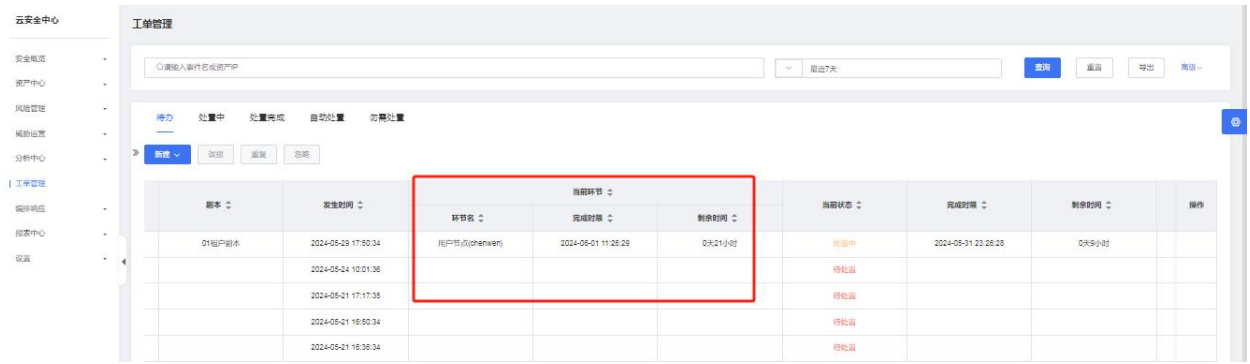


有“终止”权限的人工节点（在剧本编辑中设置），可以“终止”当前工单的剧本执行。

- 处理时限

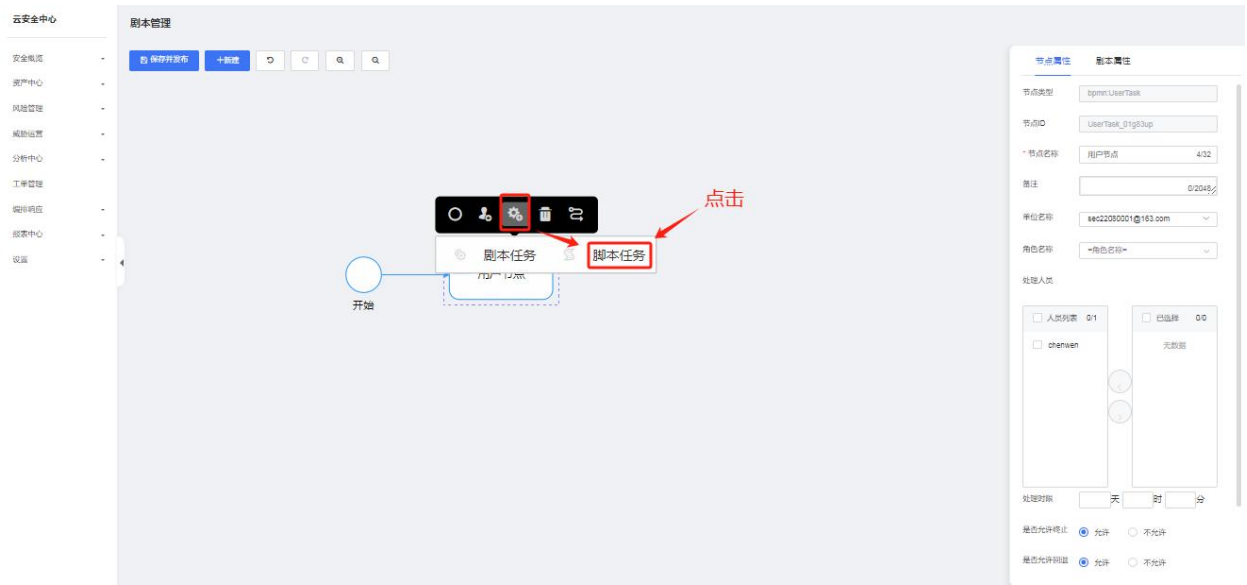
人工节点处理时限，剧本编辑中，人工节点编辑界面，可以设置该节点处理时限设置。剧本编辑，设置人工节点处理超时时限，如下图所示。

设置后，在工单管理列表和事件处置中会显示是否超时。



新增脚本任务节点

点击默认新增的用户节点，在节点上方显示节点工具，选择脚本任务。

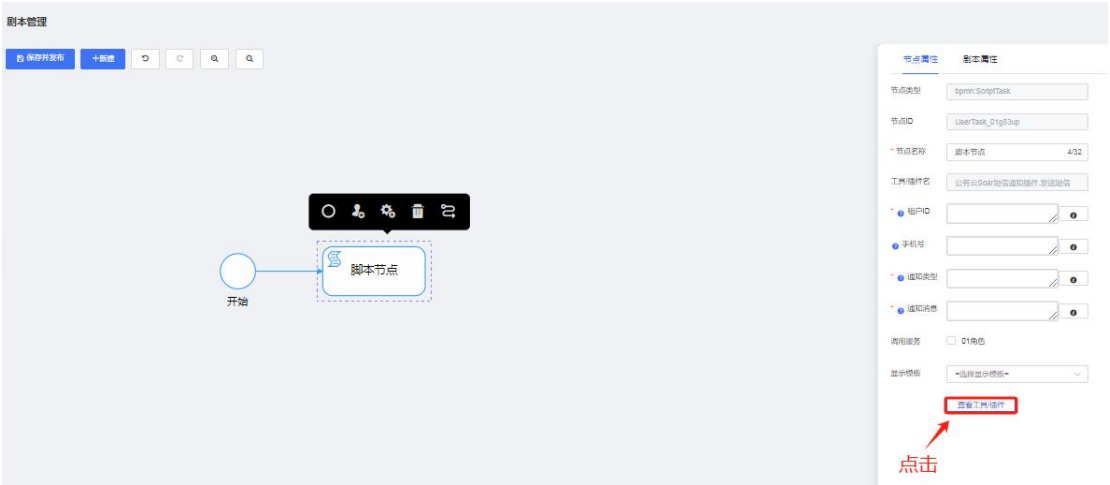


切换为脚本任务后，系统默认从左侧弹出插件选取栏，可通过插件选取栏搜索相关插件或直接选取。

说明：

- 当剧本配置了发送短信的插件时，工单处置时会发送短信至用户手机号。
- 依据定时任务配置，当系统在配置的间隔时间内触发了告警时，每间隔一段时间发送产生的告警数量，紧急告警数量的短信通知用户。

也可通过右侧的节点属性中的查看工具/插件按钮弹出插件选取栏。



选取完插件后，设置插件的入参。

剧本线条设置

点击线条，可以在线条上增加线条说明，以及在线条上添加判断条件，以控制流程走向。

点击“选择判断条件”，增加或修改线条判断条件。

4.7.2. 集成管理

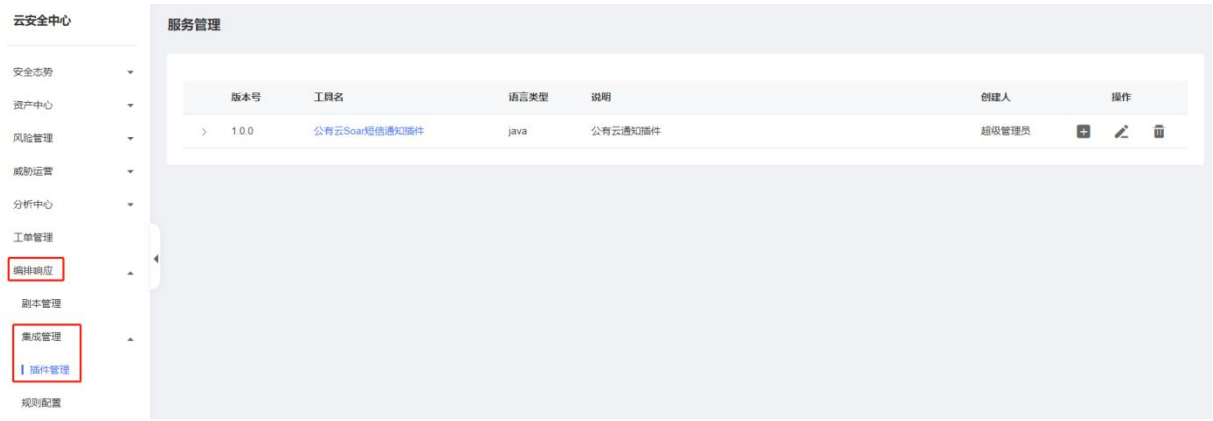
4.7.2.1. 插件管理

插件管理支持管理所有的一类插件工具，这类插件工具拥有相同的接口调用。

通过插件管理，一类插件可以新建多个不同的连接服务，方便在剧本调用时灵活切换调用。

新增服务

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“编排响应 > 集成管理 > 插件管理”，进入插件管理页面。



3. 单击操作列的新增图标，弹出新增服务对话框。

4. 填写服务名称和备注信息后，单击“确定”。服务新增完成后如下所示。

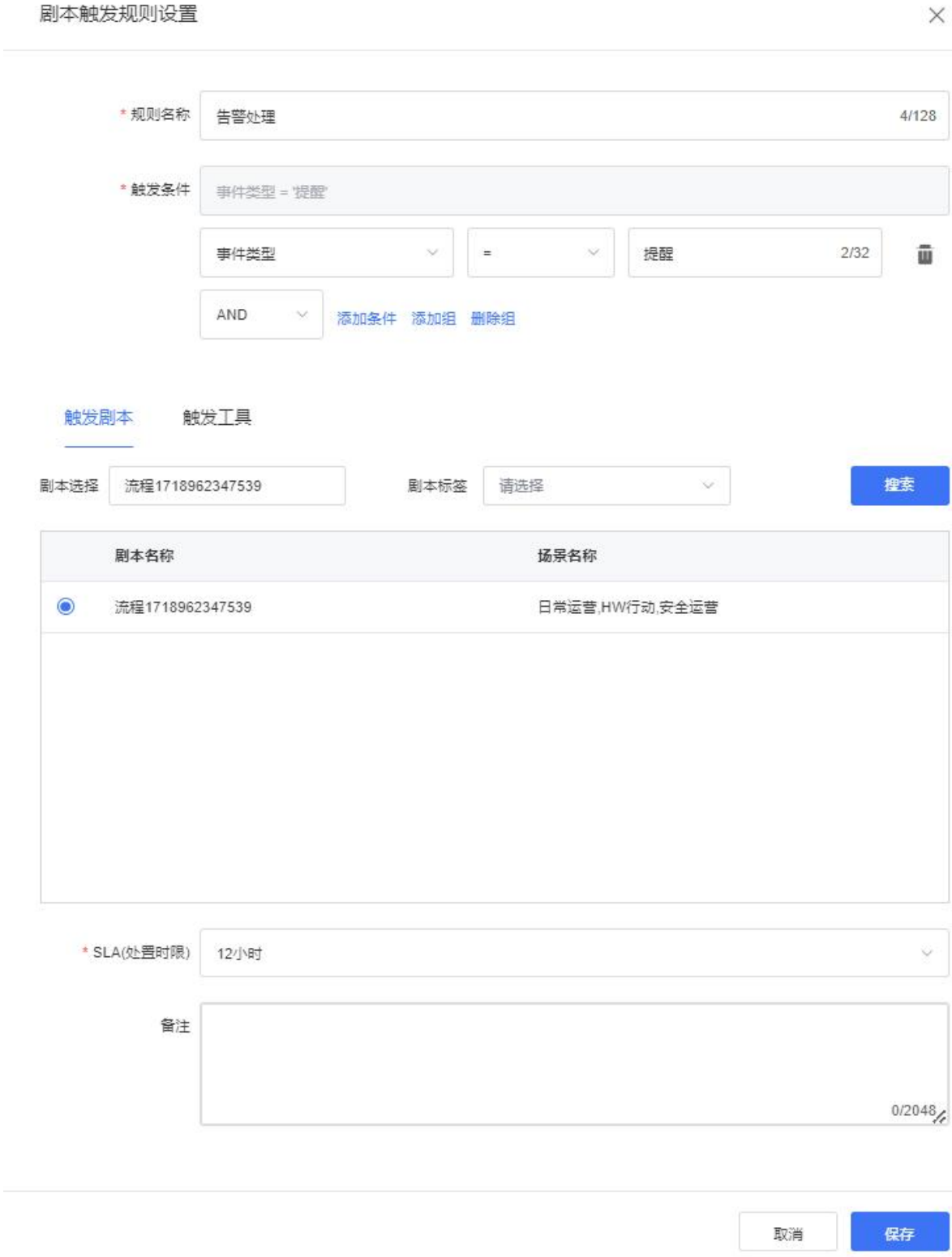
5. 服务状态默认为关闭，单击操作列的“启用”图标，启用服务。

4.7.3. 规则配置

规则配置模块可以进行规则的新建、查找、启动、暂停、查看与删除。

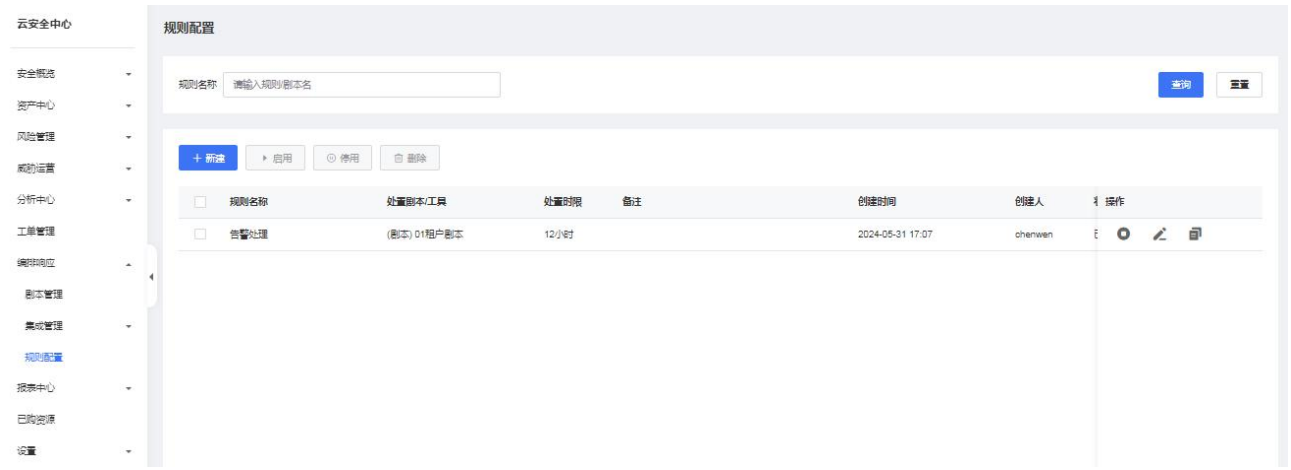
新建规则

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“编排响应 > 规则配置”，进入规则配置页面。
3. 点击“新建”，新建剧本触发规则。填写规则名称，以及剧本触发条件，再勾选相关剧本即可。



启动规则

规则新建完成后，默认为“未启动”，单击操作列的启动图标，启动规则。



4.8. 报表中心

报表中心是用户生成报表的功能模块。该功能模块主要由两部分组成，分别是报表任务和报表模版。通过报表任务，用户能够定时的生成报表内容。通过报表模版，用户能指定报表的格式以及排版。

4.8.1. 报表任务

报表任务功能，实现管理和维护报表任务，用户可以自定义报表的生成周期，每个用户需要自行管理自己的报表任务。

可以实现：新建即时报表任务、新建周期报表任务、查看报表任务、删除报表任务以及生成报表等功能。

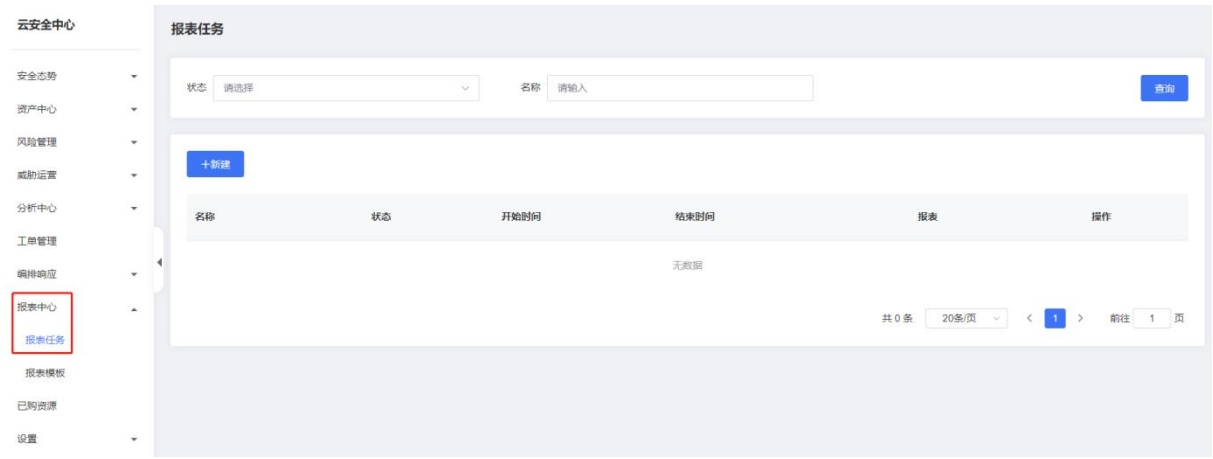
> 说明：
>
> 周期报表任务执行时发送报表短信到用户在系统配置的手机号。

前提条件

已创建报表模板。

新建报表任务

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“报表中心 > 报表任务”。



3. 单击“新建”，弹出新建报表任务对话框。填写报表名称、选择报表模板、选择报表类型（支持即时报表任务、周期报表任务）。

4. 配置完成后，单击“保存”。

管理报表任务

- 启动周期性任务

  在周期性报表任务的操作列，单击“立即启动”图标。

- 编辑报表任务

  在周期性报表任务的操作列，单击“编辑”图标。报表名称不支持修改，其余参数均可修改。

查看报表

单击如下图标，查看已生成的报表列表。并支持下载报表到本地。

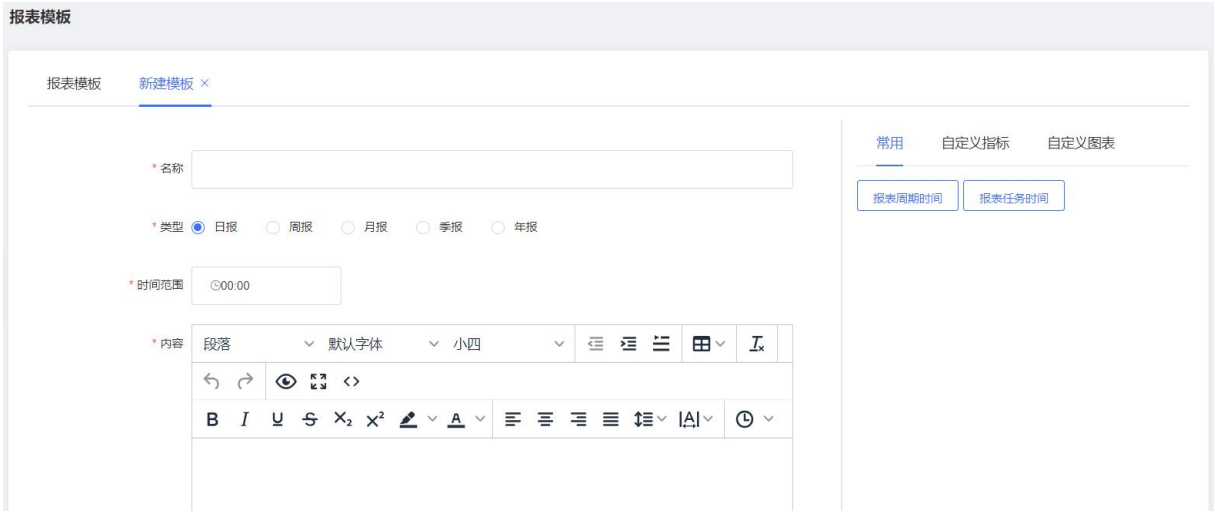
4.8.2. 报表模板

报表模板，维护和定义报表模板，用户可以自定义报表的模版，每个用户需要自行管理自己的报表模版。

支持自定义指标、自定义图表以及报表预览等功能。

新建模板

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“报表中心 > 报表模板”。
3. 单击“新建”，进入新建模板页面。



4. 配置模板名称、类型、时间范围和报表内容。
5. 单击“保存”，保存模板。

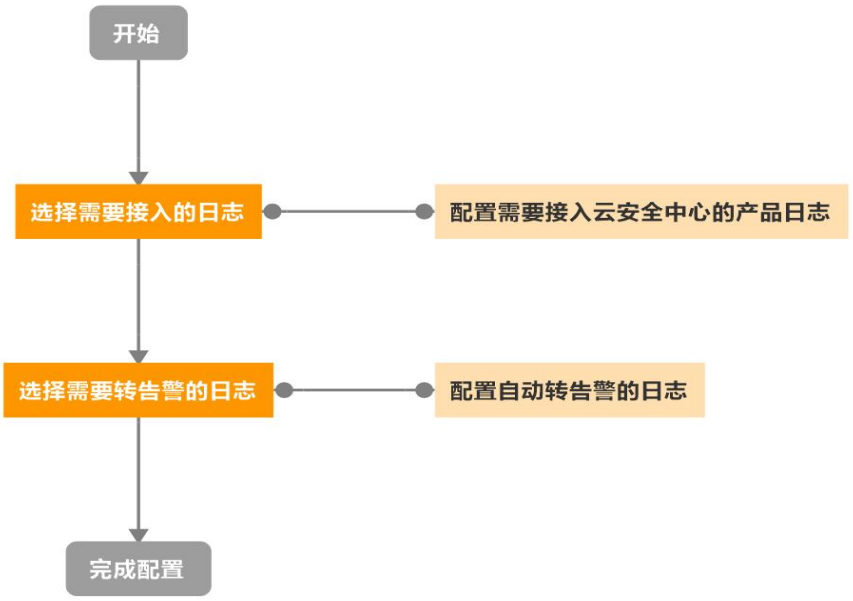

云安全中心
安全概览
资产中心
风险管理
威胁运营
分析中心
工单管理
编排响应
报表中心
报表任务
报表模板
已购资源
设置
报表模板
报表模板
+ 新建
删除
请输入名称
ID
名称
类型
状态
创建时间
更新时间
操作
21
周报
周报
可用
2024-04-22 10:57:56
2024-04-22 10:57:56
20
日报
日报
使用中
2024-04-22 10:50:01
2024-04-22 10:52:42
共 2 条
20条/页
1
前往
1
页

4.9. 设置

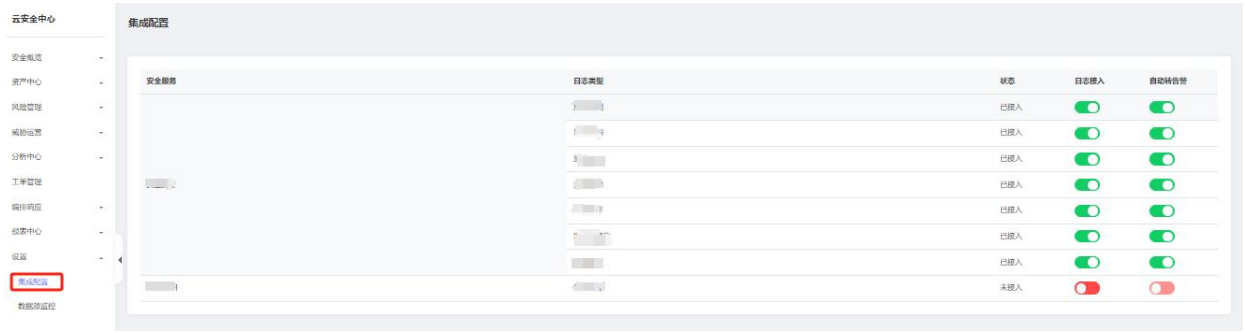
4.9.1. 集成配置

开通云安全中心实例后，系统默认会接入部分日志数据并对用户进行初始化配置。您可以根据自己的业务特性修改初始化配置。

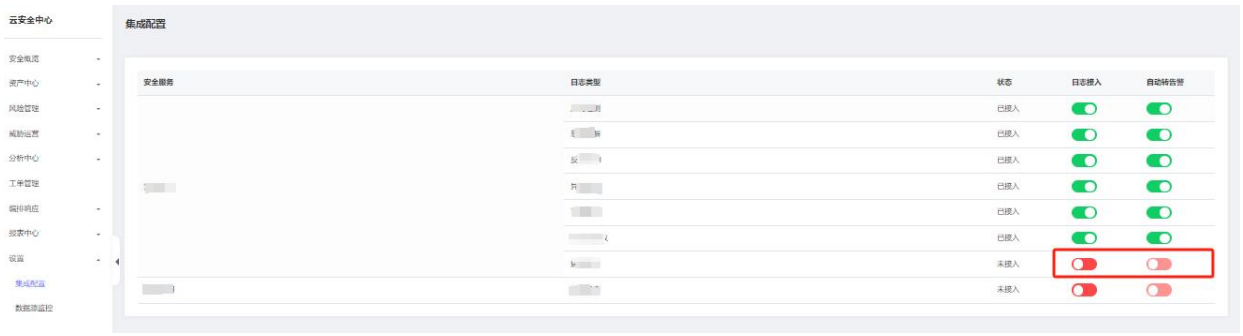
打开云安全中心的“设置 > 集成配置”，在集成配置中选择需要接入的日志类型。部分日志支持直接转告警，可以直接打开转告警开关，云安全中心会根据内置转告警规则进行转告警配置。

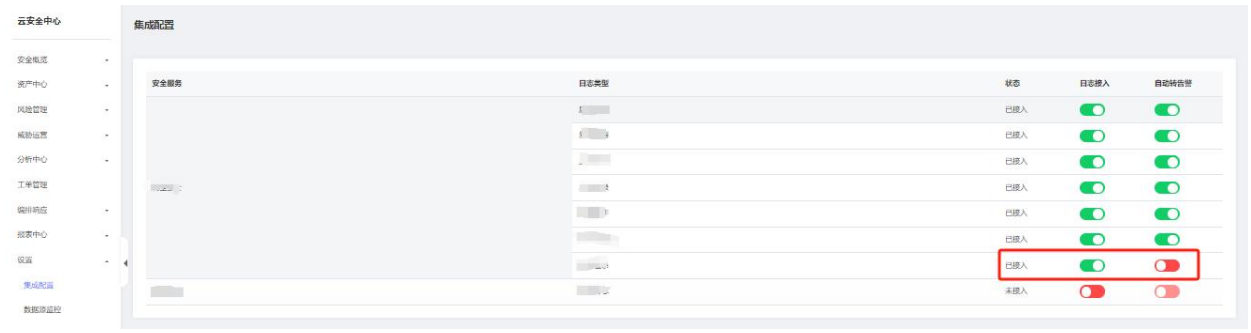


1. 选择“设置 > 集成配置”，打开数据集成配置页面。

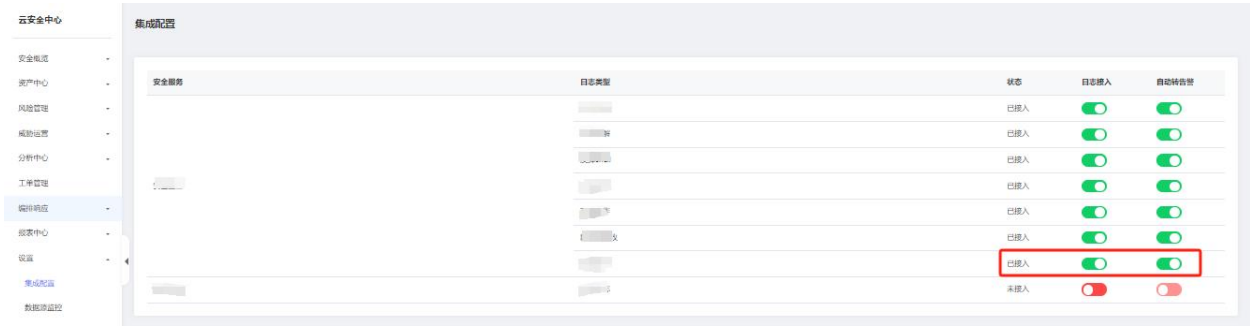


2. 选择需要接入的日志，并打开日志接入开关。





3. 选择需要转告警的日志，并打开自动转告警的开关。



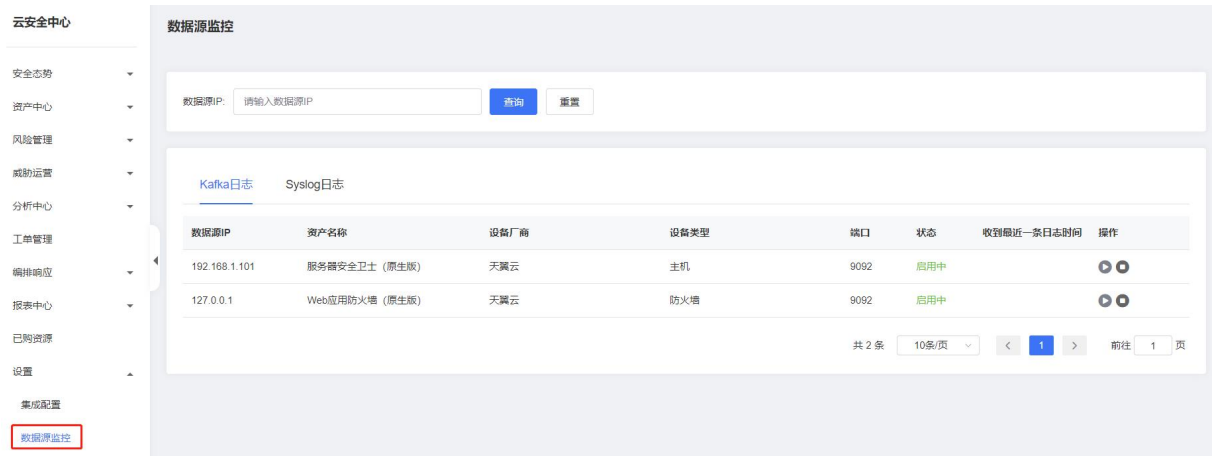
说明：

- 系统默认会接入部分日志，用户如有需要，可以自行关闭。
- 选择需要接入的日志时，只能针对您已经购买的云产品。
- 选择需要转告警的日志，只能针对已经选择接入的日志进行。

4.9.2. 数据源监控

打开云安全中心的设置>数据源监控，在数据源监控中可以查看到已经接入到系统的数据源。可以直接通过开关对数据源进行开启或关闭，云安全中心会根据您的操作对数据源数据进行收取或拒绝收取。

1. 点击“设置 > 数据源监控”，打开数据源监控页面。



2. 选择需要接入的数据源，并启用数据源。

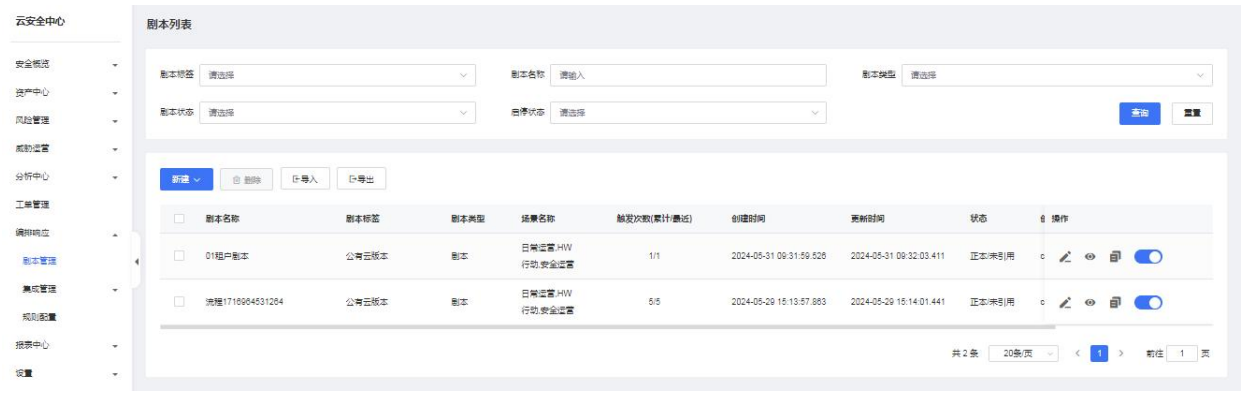
说明：

- 选择需要接入的数据源时，只能针对您已经购买的云产品。
- 停止数据源，对应的“集成配置”将不允许操作。

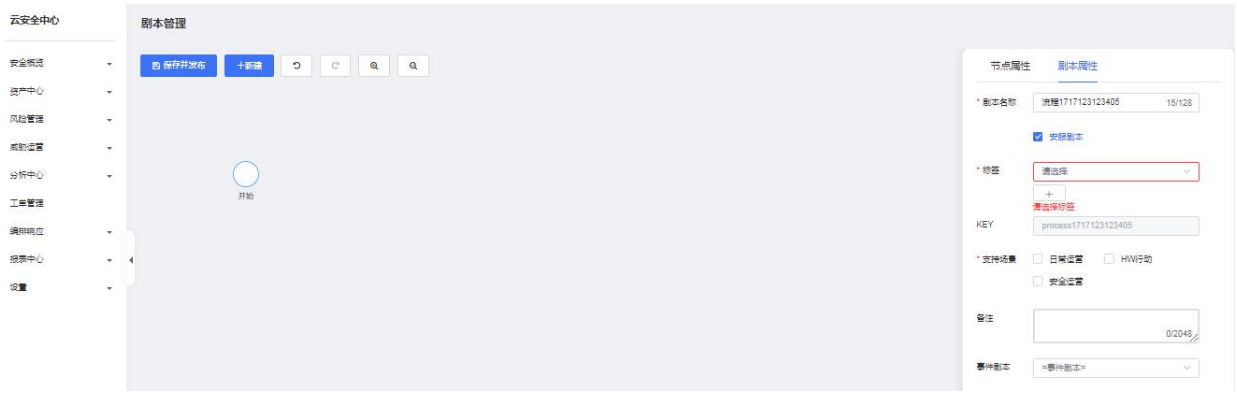
5. 最佳实践

5.1. 如何进行剧本管理

为了提高告警处置的自动化程度及效率，提高告警解决方案的复用性。可以使用剧本将某些处置操作模板化，程序化。在类似告警发生时，可以自动规则匹配或人工选择相关剧本进行自动化的处置。其中的剧本匹配规则，则用于告警发生后，自动匹配并调用剧本进行操作。剧本管理模块则用于对这些剧本和剧本匹配规则进行统一管理。剧本管理的的剧本列表，可以查看、新建、编辑、导入导出相关的剧本。



1、打开剧本管理的剧本列表界面，点击新建，创建一个只有一个开始节点的新剧本。剧本新增页面右侧可对剧本属性进行编辑。



说明：

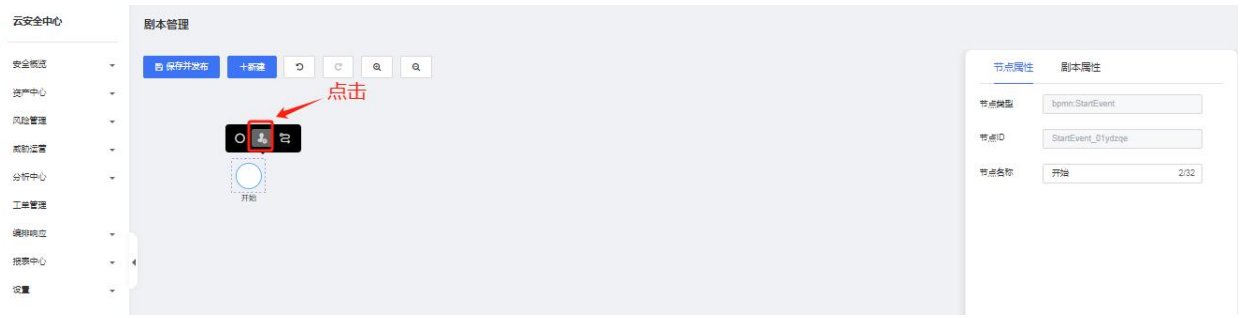
一个剧本有且只有一个开始节点和结束节点。

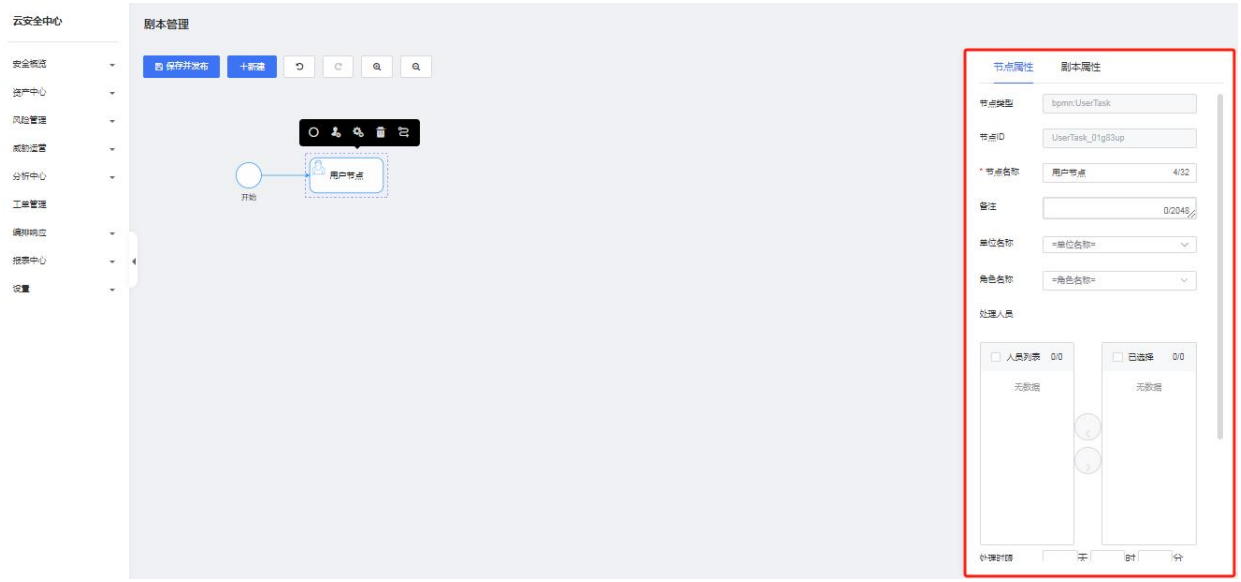
每个用户在新增的剧本编辑界面停留过长时，会最多保留一份新增草稿，在用户下次新增时会提示是否进入草稿。

在对已存在剧本进行修改时，若在修改页面停留时间过长，会自动为改剧本保留一份草稿，在下次重新对剧本进行编辑时提示是否进入草稿。

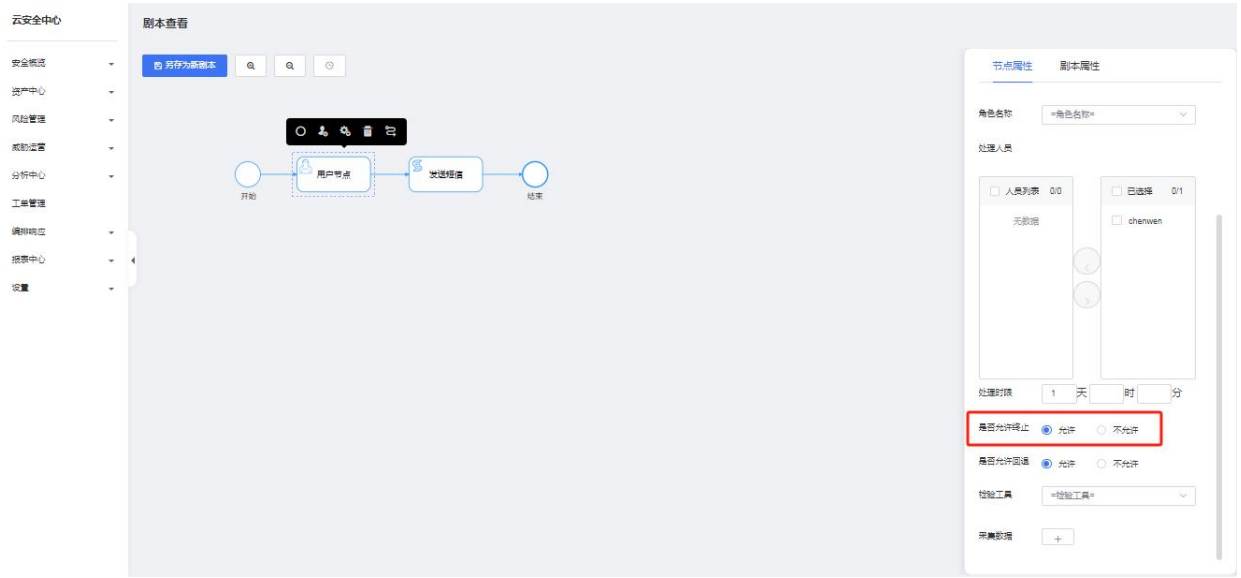
剧本保存时会对剧本进行校验，若改剧本存在不能到达或不能结束的孤立节点，需用户完善后才能保存。后续版本将会升级启停功能，非正常剧本允许保存，不允许启用。

2、剧本新增节点，默认为用户节点。选取节点后，右侧可对节点属性进行编辑。

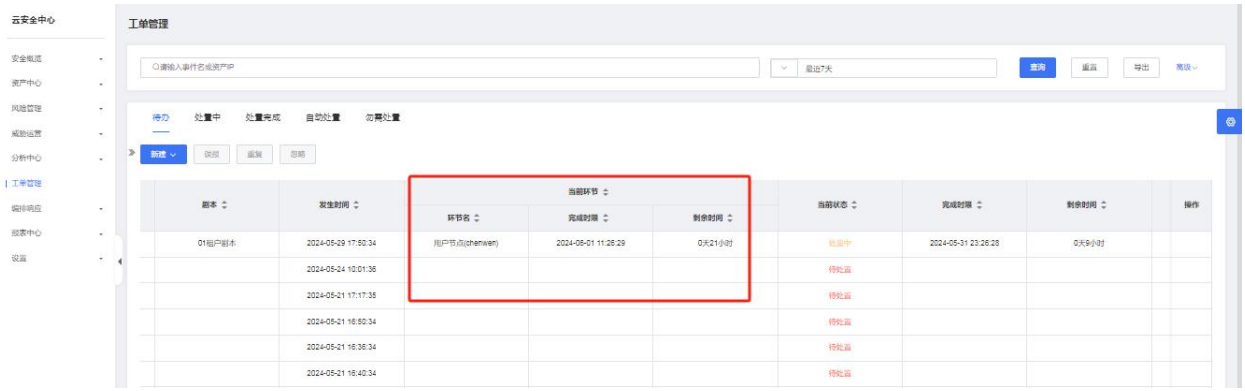




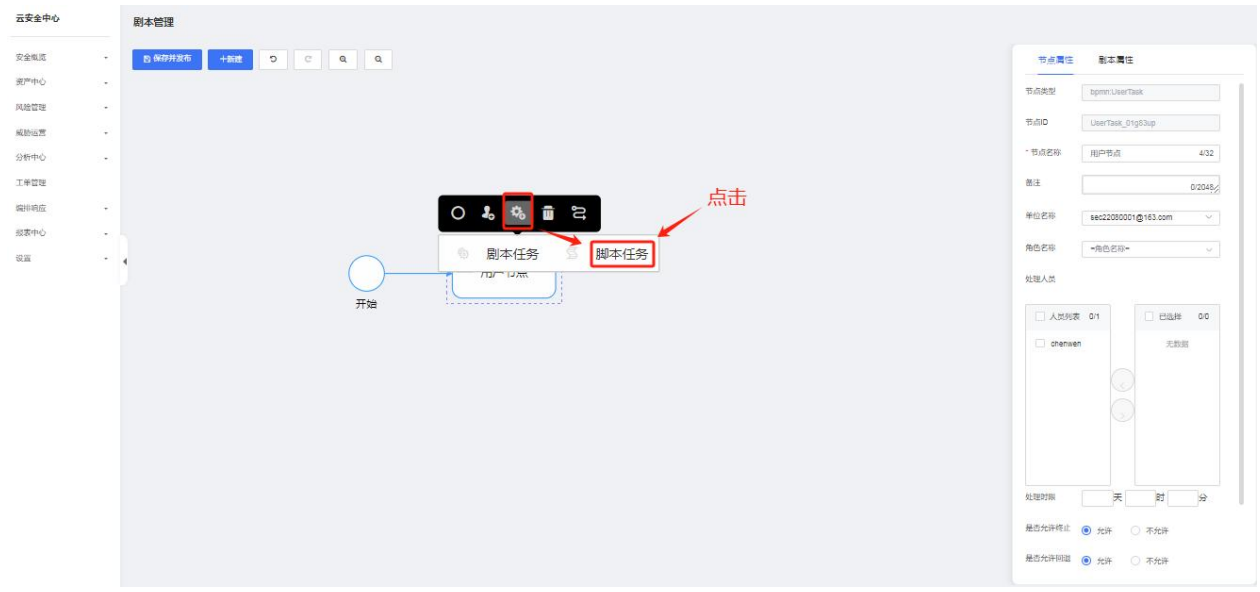
3、终止功能，有“终止”权限的人工节点（在剧本编辑中设置），可以“终止”当前工单的剧本执行。剧本编辑界面如图所示。



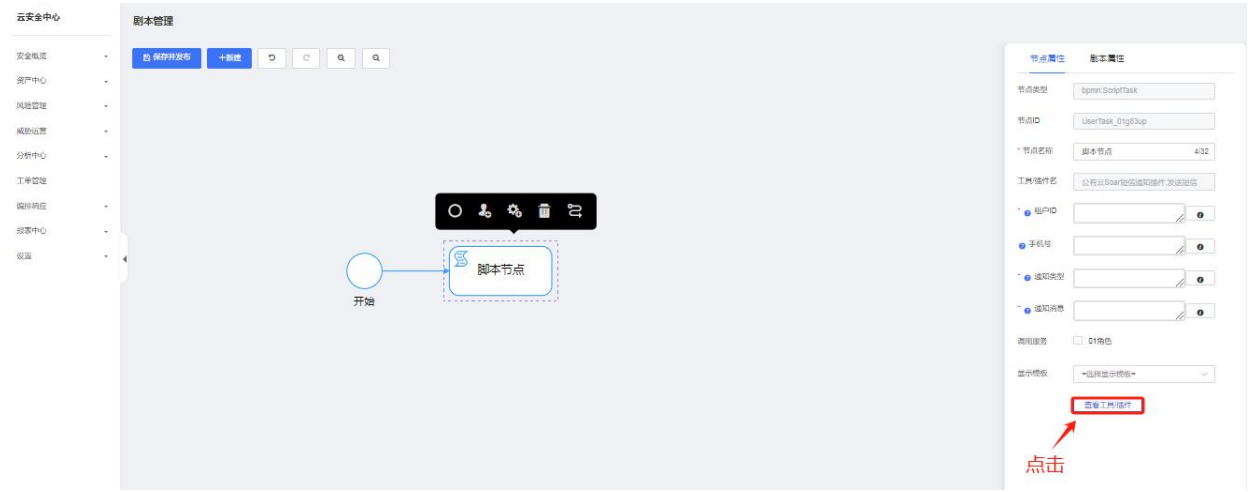
4、人工节点处理时限，剧本编辑中，人工节点编辑界面，可以设置该节点处理时限设置。设置后，在工单管理列表和事件处置中会显示是否超时。剧本编辑，设置人工节点处理超时时限，如下图所示。



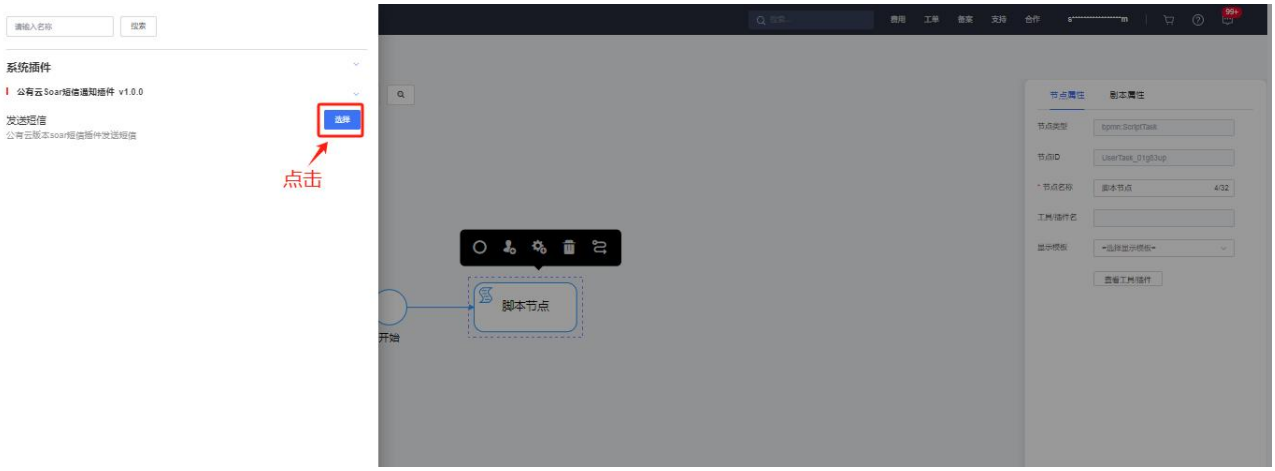
5、脚本任务节点新增，点击默认新增的用户节点，在节点上方显示节点工具，选择脚本任务



6、切换为脚本任务后，系统默认从左侧弹出插件选取栏，也可通过右侧的节点属性中的查看工具/插件按钮弹出插件选取栏



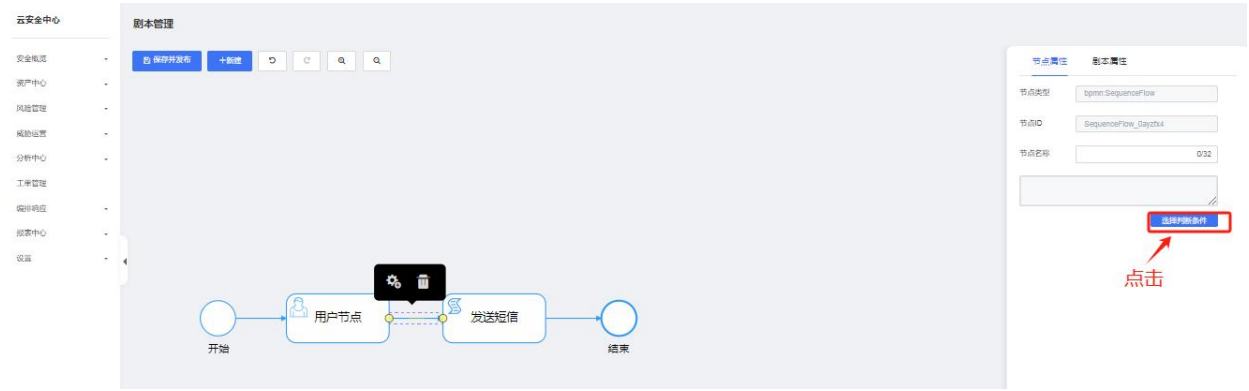
7、可通过插件选取栏搜索相关插件或直接选取



8、选取完插件后，设置插件的入参

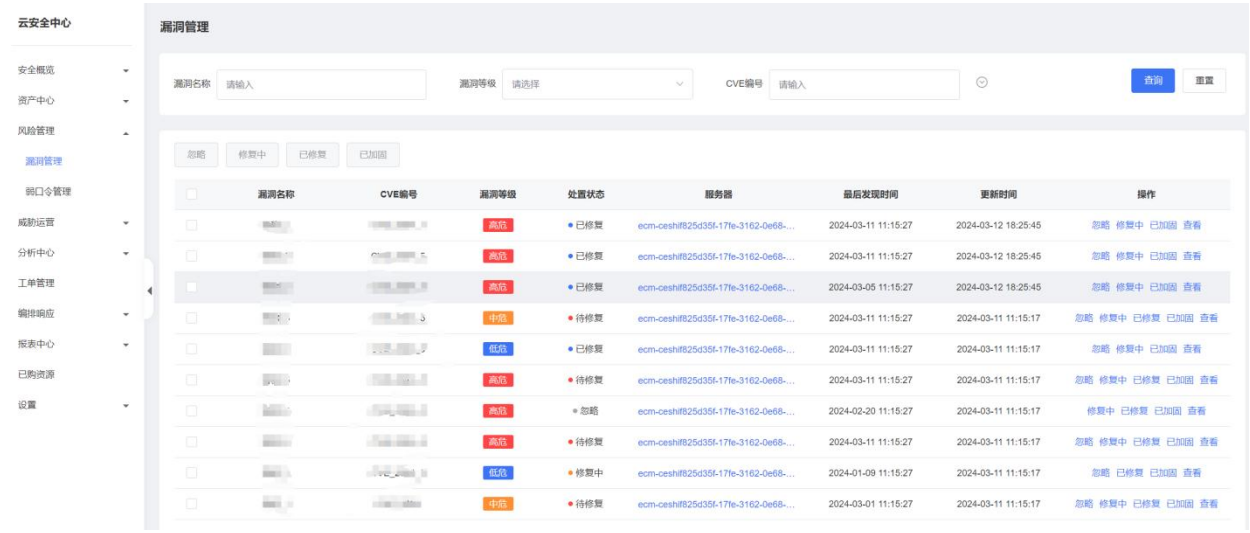
9、剧本线条设置，点击线条，可以在线条上增加线条说明，以及在线条上添加判断条件，以控制流程走向。

10、点击选择判断条件，增加或修改线条判断条件

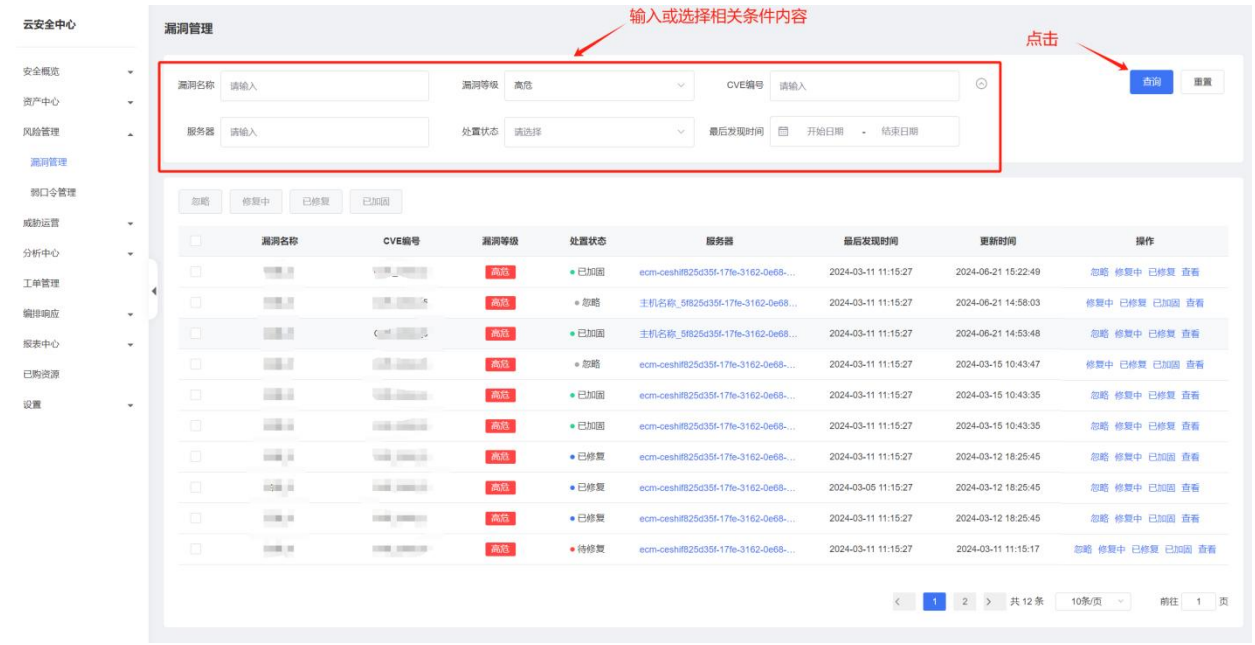


5.2. 如何进行漏洞管理

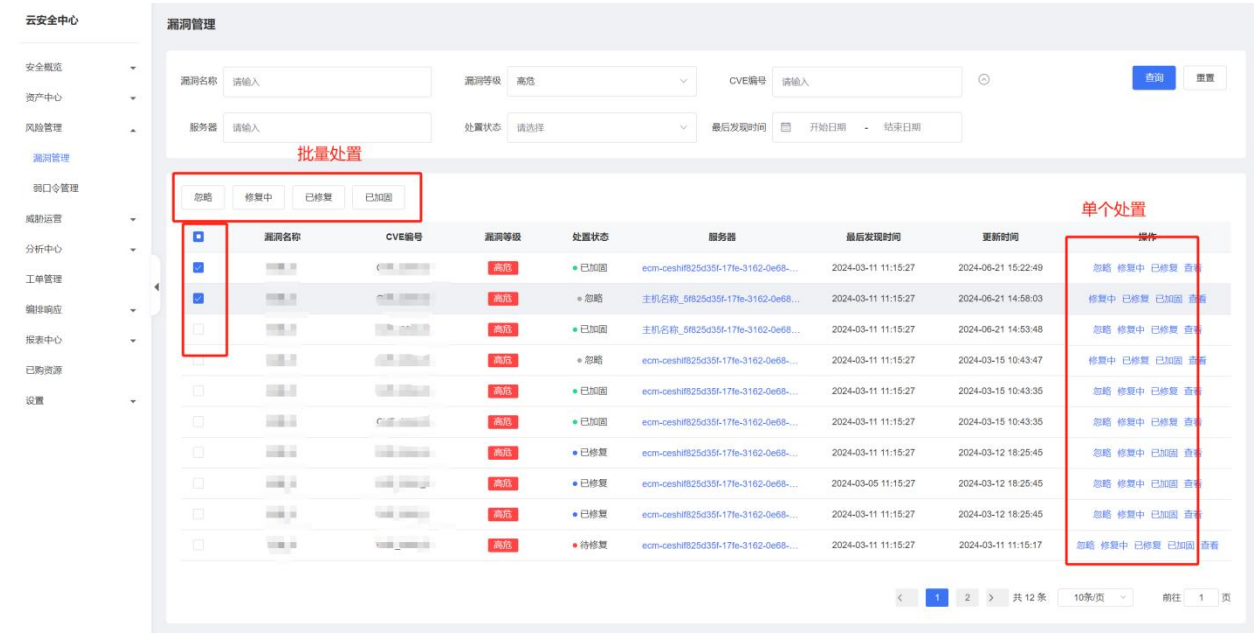
1、进入风险管理-漏洞管理页面，为租户提供漏洞查询及处置功能。



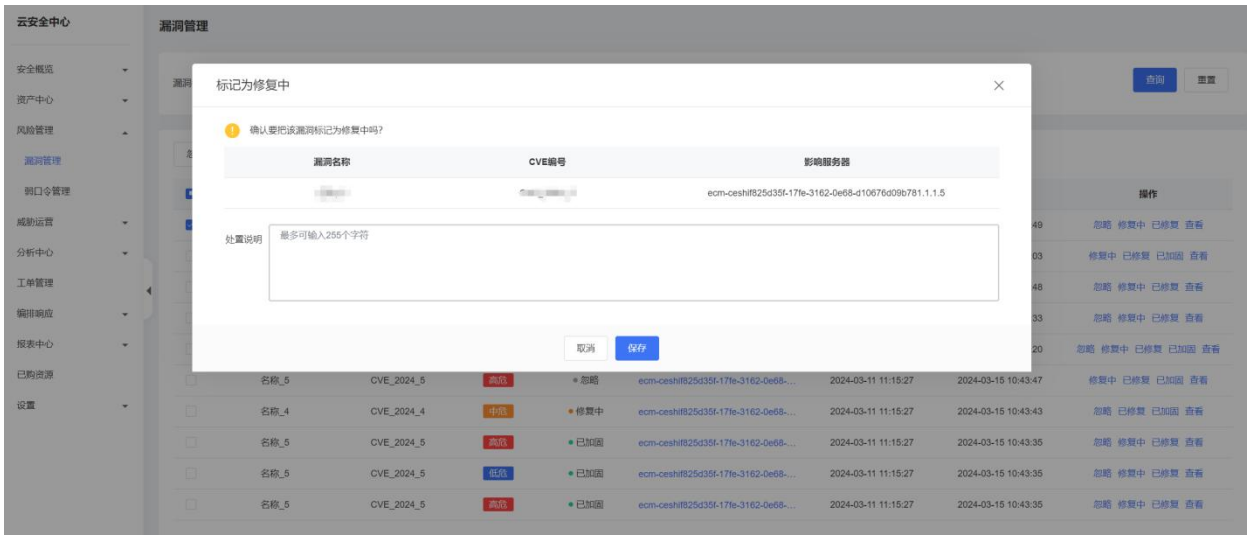
2、支持条件查询，用户输入或选择相关条件内容

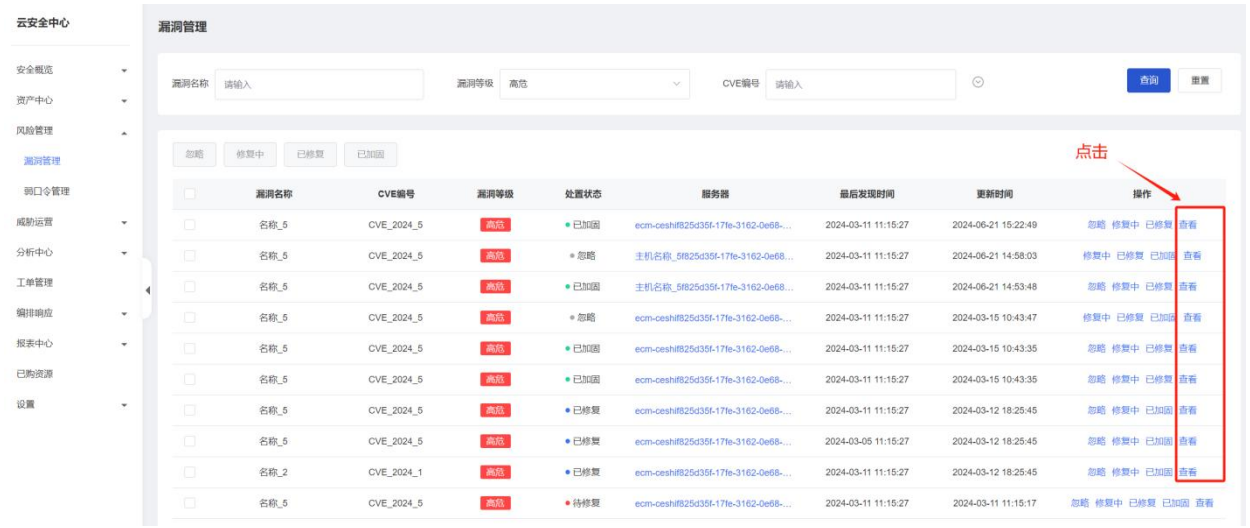


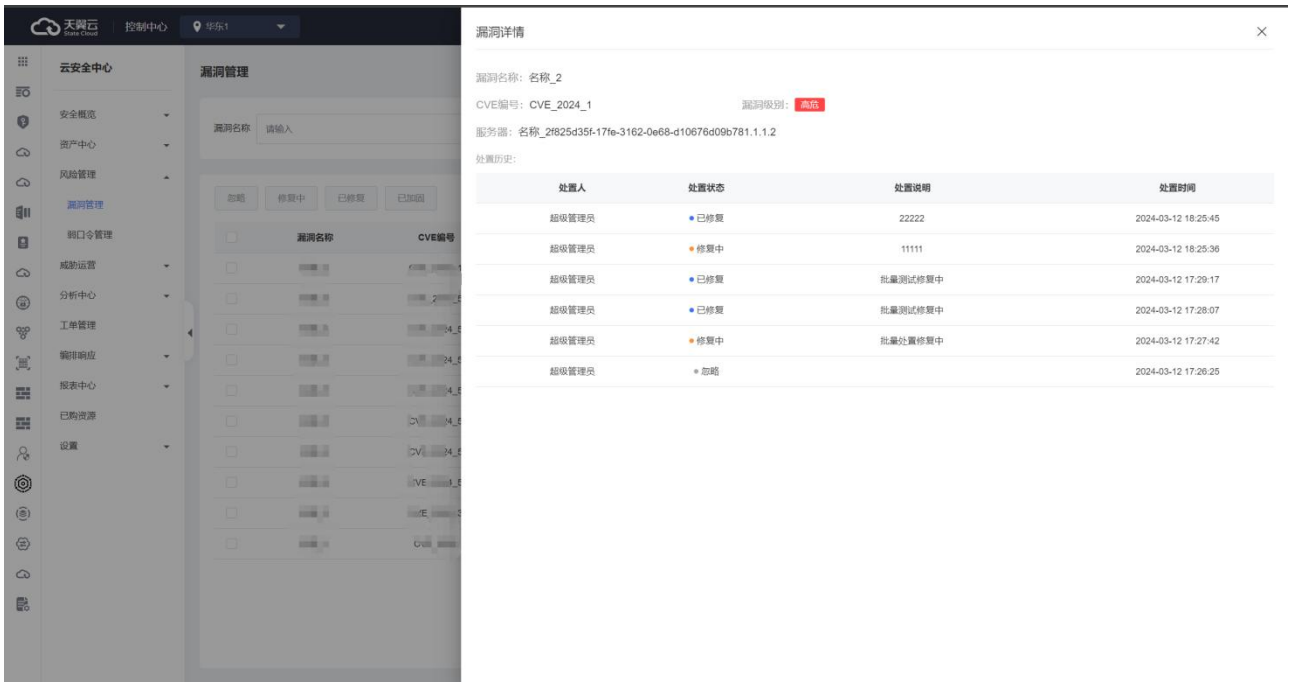
3、提供处置能力，可直接或批量修改漏洞处置状态。状态枚举值：修复中、已修复、忽略、已加固等。修改处置状态可填写状态变更原因。



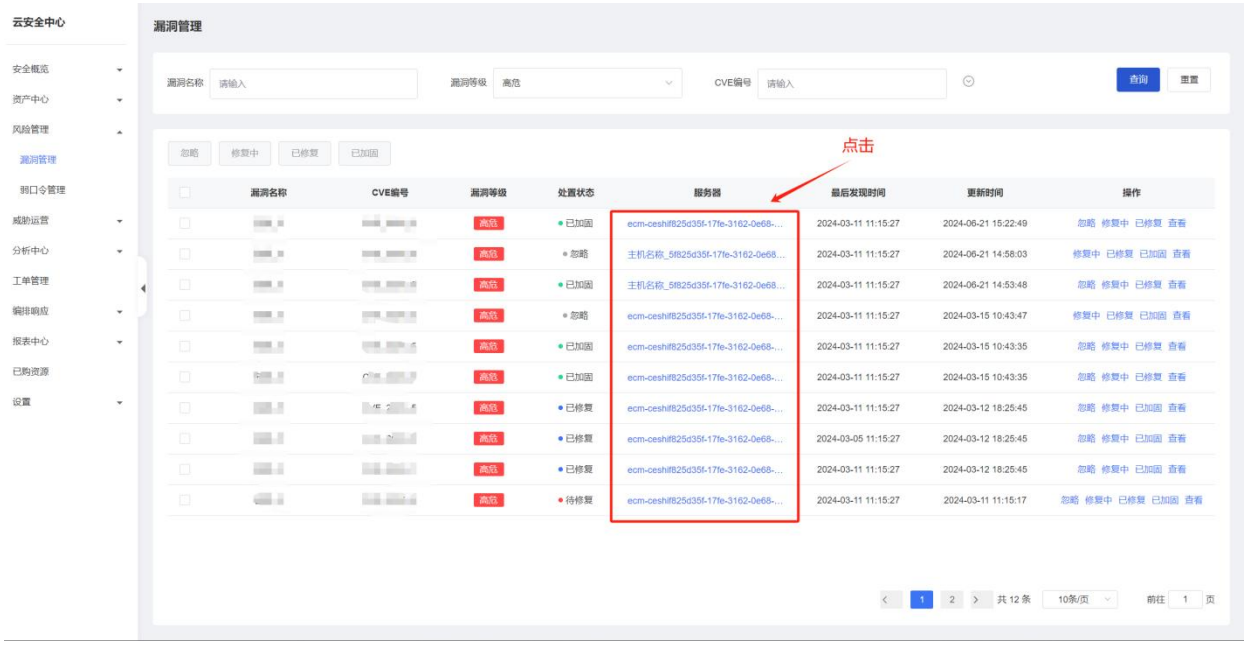
4、进行处置，在漏洞详情中可以历史所有的状态变更记录的信息：处置人、处置状态、处置说明等。

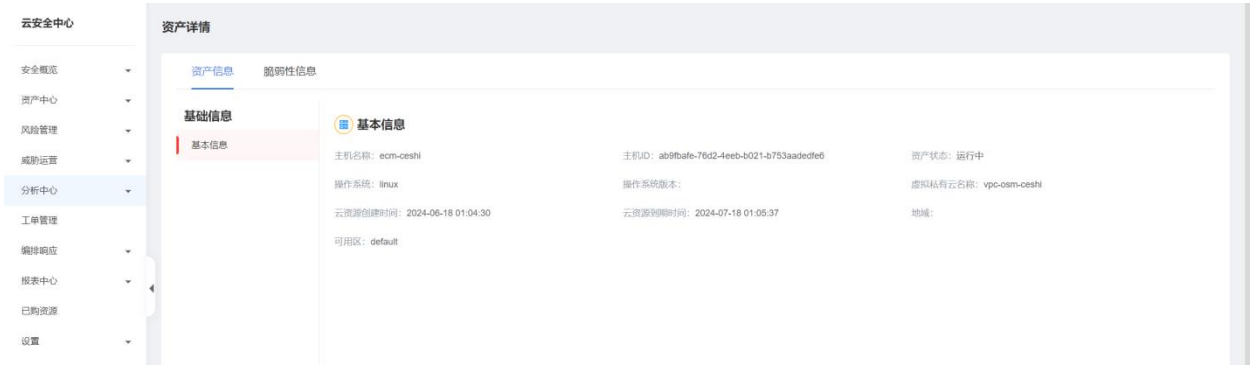

云安全中心
漏洞管理
标记为修复中
确认要把该漏洞标记为修复中吗?
漏洞名称
CVE编号
影响服务器
处置说明
最多可输入255个字符
取消
保存


云安全中心
漏洞管理
漏洞名称
漏洞等级
CVE编号
查询
重置
点击
操作


云安全中心
漏洞管理
漏洞详情
漏洞名称：名称_2
CVE编号：CVE_2024_1
漏洞级别：高危
服务器：名称_2f825d35f-17fe-3162-0e68-d10676d09b781.1.1.2
处置历史：
处置人
处置状态
处置说明
处置时间

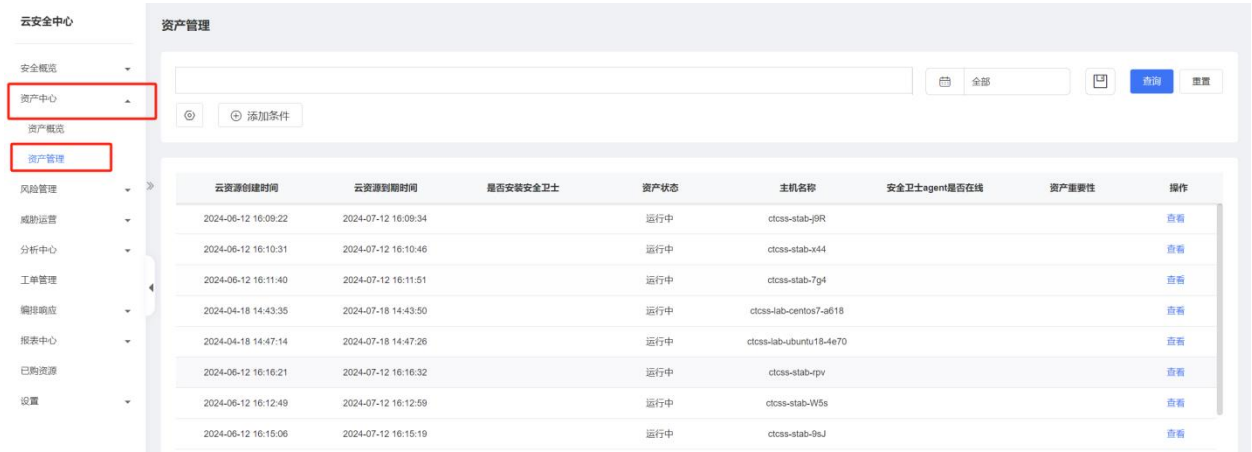
5、每条漏洞能够关联资产信息，可快速查看关联的资产详情。



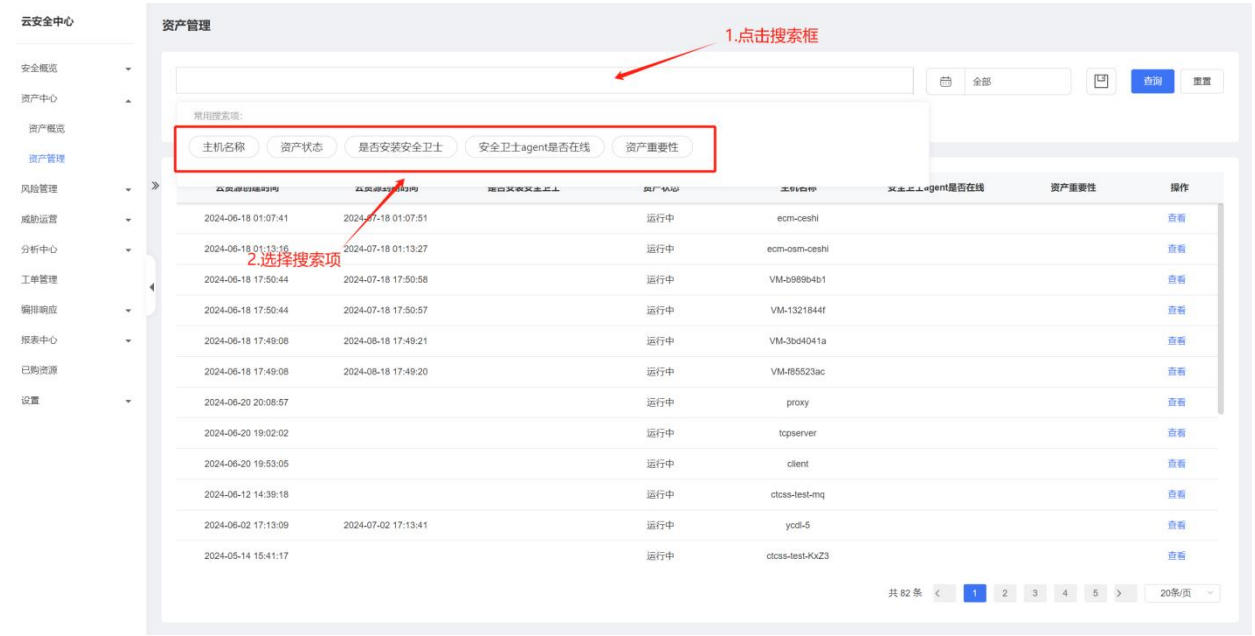


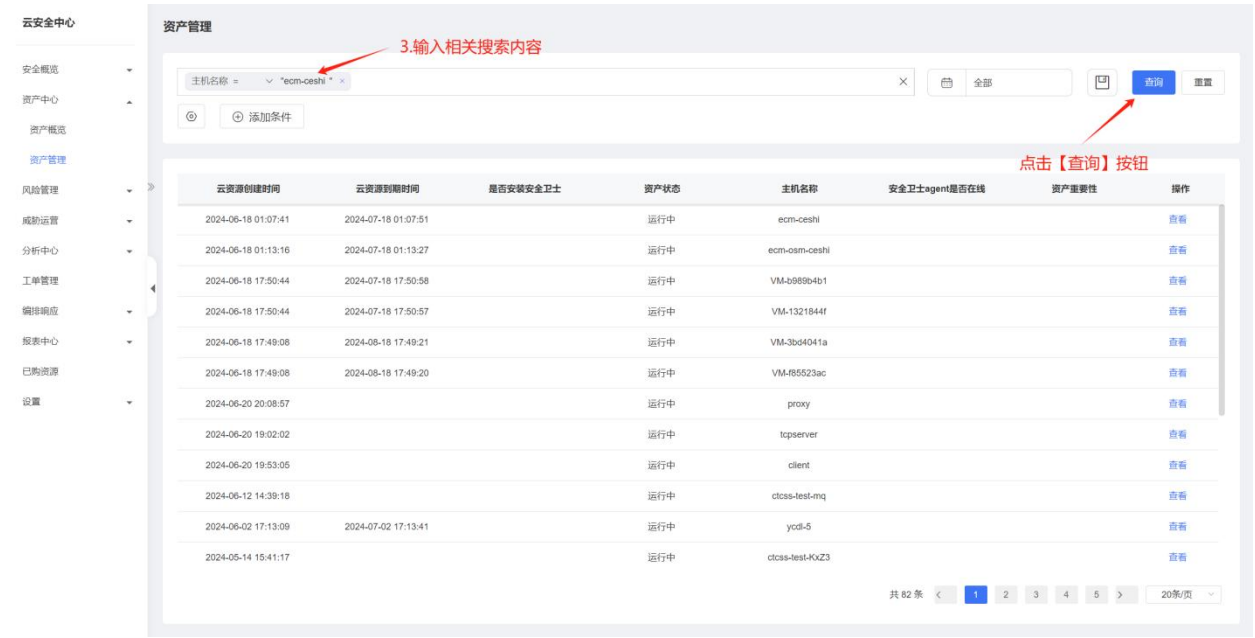
5.3. 如何对资产进行查看管理

1、进入资产中心-资产管理页面，为租户提供资产及资产属性的查询功能。

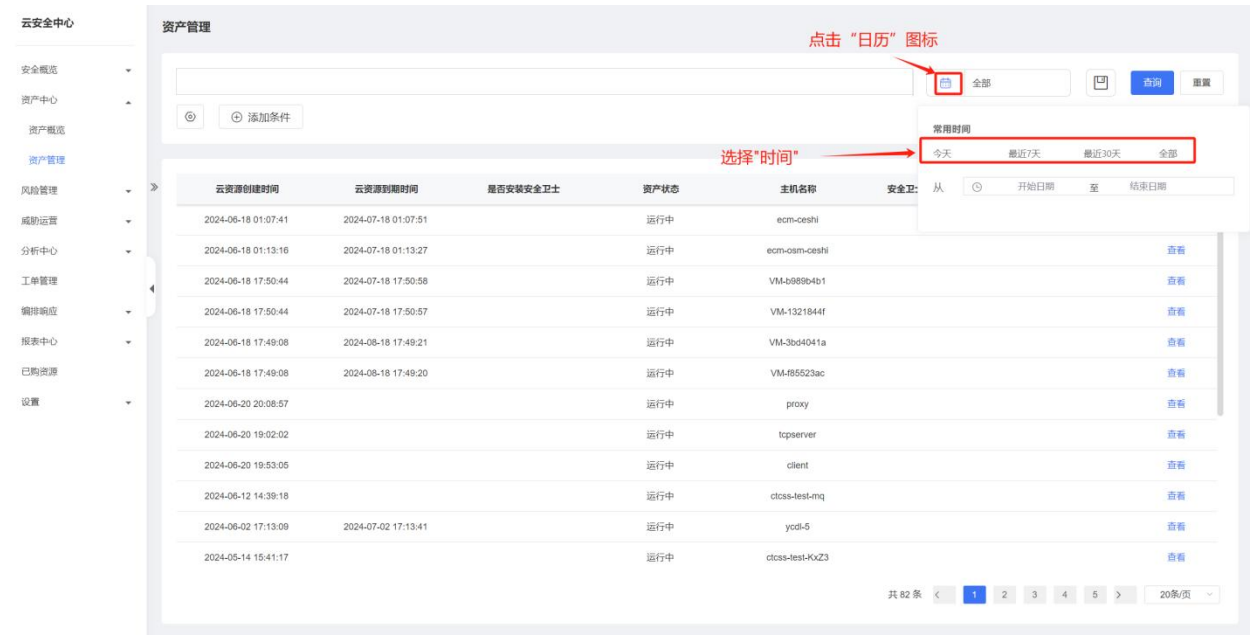


2、选择常用搜索项查询。

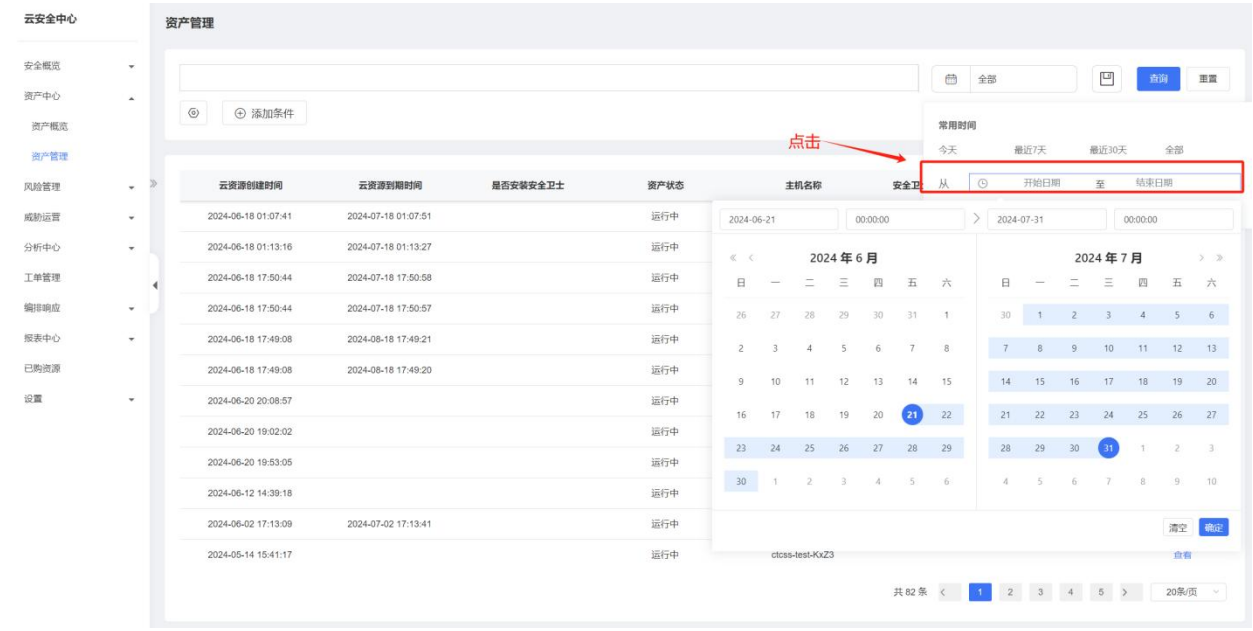




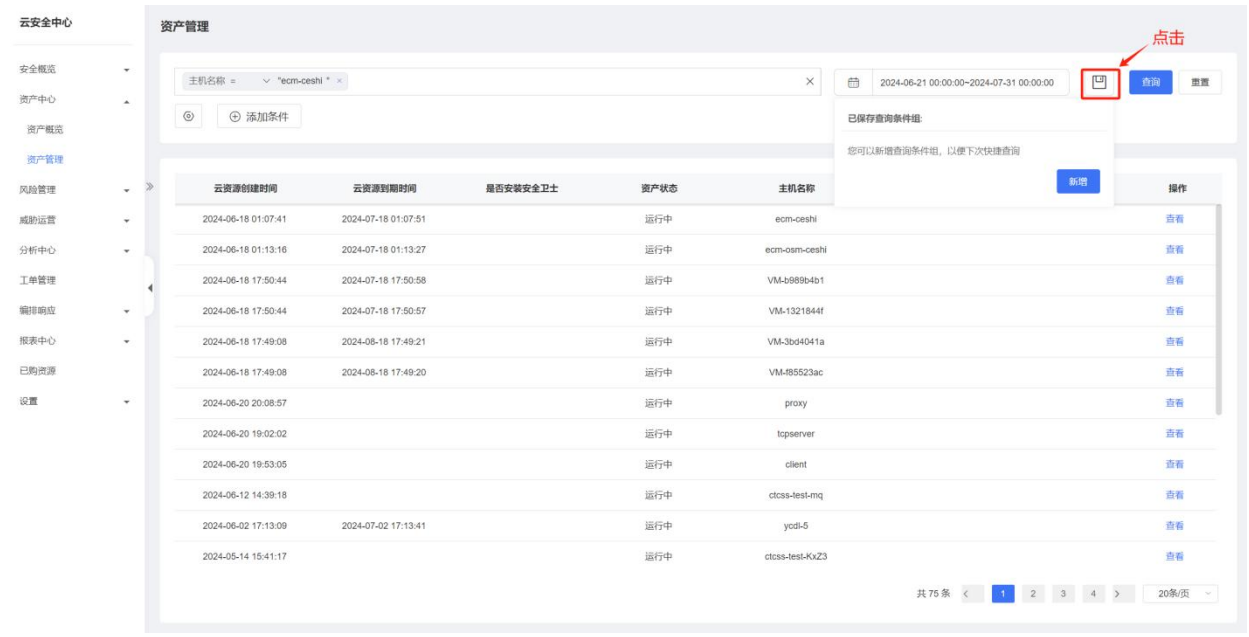
3、选择常用时间查询。

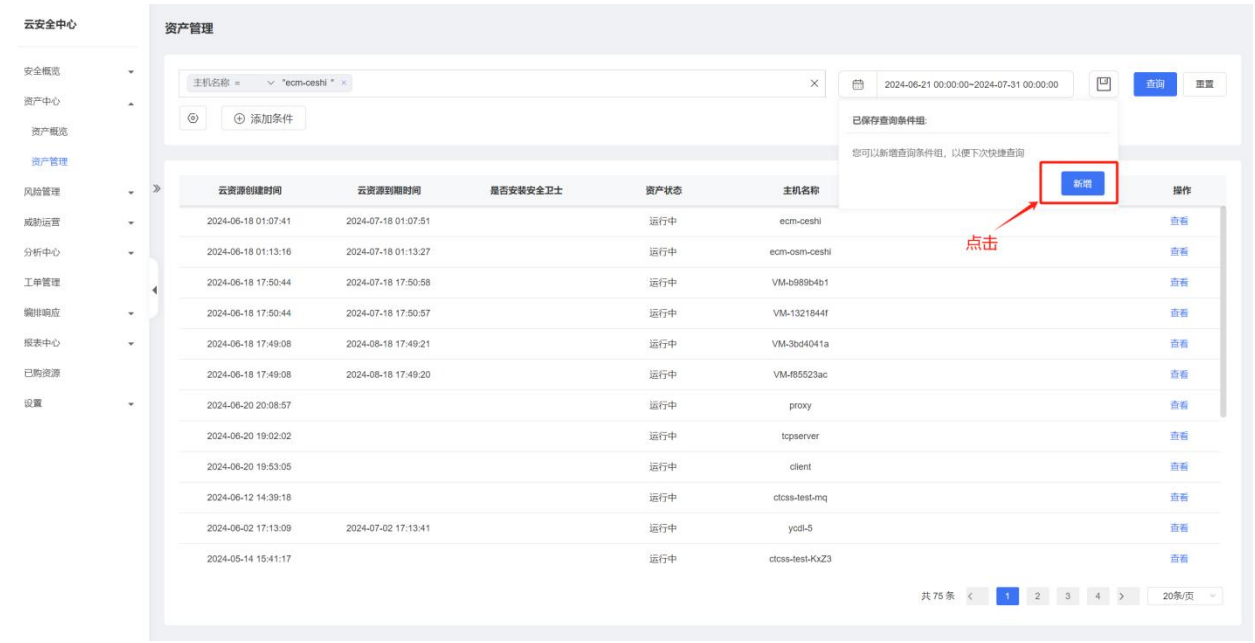


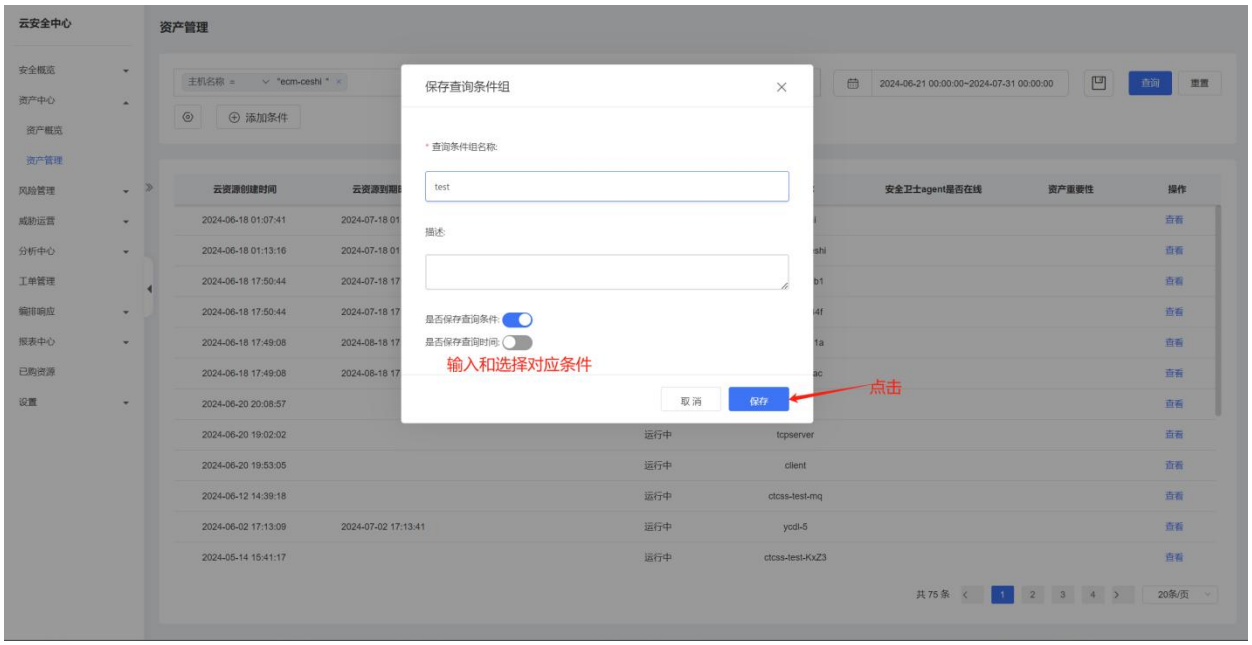
4、选择时间段查询。



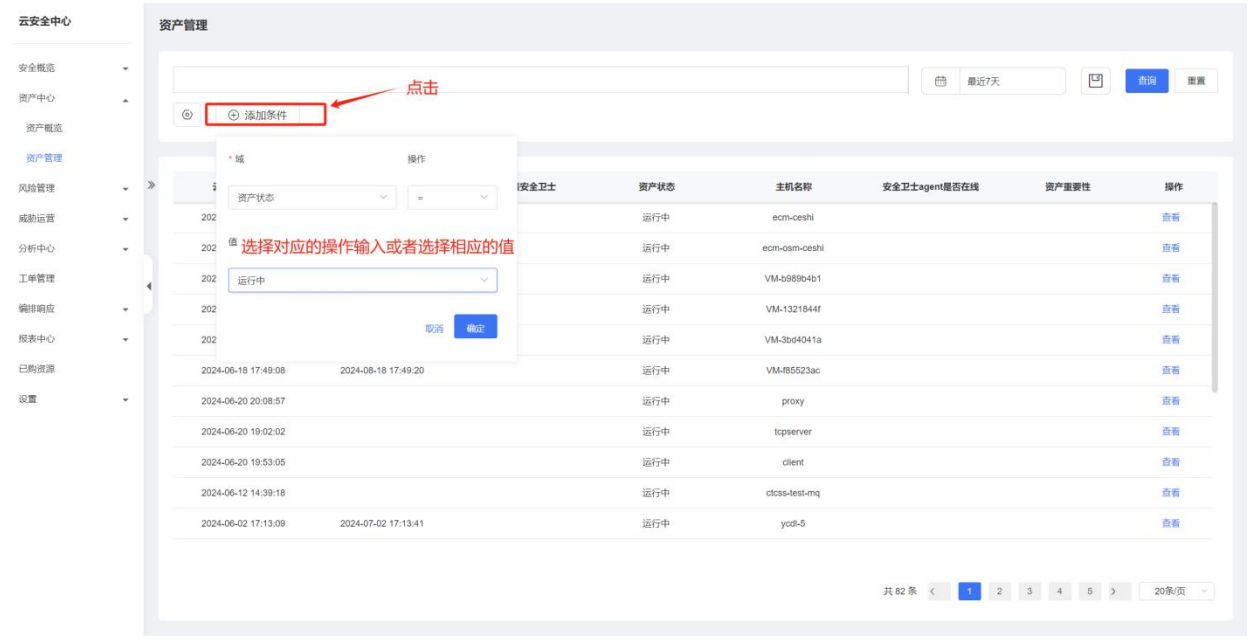
5、查询条件组：保存查询条件，方便用户快速查询。


云安全中心
资产管理
点击
主机名称 = "ecm-ceshi *
2024-06-21 00:00:00~2024-07-31 00:00:00
查询
重置
添加条件
已保存查询条件组:
您可以新增查询条件组，以便下次快捷查询
新增
云资源创建时间 云资源到期时间 是否安装安全卫士 资产状态 主机名称 操作
2024-06-18 01:07:41 2024-07-18 01:07:51 运行中 ecm-ceshi 查看
2024-06-18 01:13:16 2024-07-18 01:13:27 运行中 ecm-osm-ceshi 查看
2024-06-18 17:50:44 2024-07-18 17:50:58 运行中 VM-b989b4b1 查看
2024-06-18 17:50:44 2024-07-18 17:50:57 运行中 VM-1321844f 查看
2024-06-18 17:49:08 2024-08-18 17:49:21 运行中 VM-3bd4041a 查看
2024-06-18 17:49:08 2024-08-18 17:49:20 运行中 VM-f85523ac 查看
2024-06-20 20:08:57 运行中 proxy 查看
2024-06-20 19:02:02 运行中 tcpserver 查看
2024-06-20 19:53:05 运行中 client 查看
2024-06-12 14:39:18 运行中 ctcss-test-mq 查看
2024-06-02 17:13:09 2024-07-02 17:13:41 运行中 ycdl-5 查看
2024-05-14 15:41:17 运行中 ctcss-test-KxZ3 查看
共 75 条 1 2 3 4 20条/页


云安全中心
资产管理
主机名称 = "ecm-ceshi *
2024-06-21 00:00:00~2024-07-31 00:00:00
查询
重置
添加条件
已保存查询条件组:
您可以新增查询条件组，以便下次快捷查询
新增
点击
云资源创建时间 云资源到期时间 是否安装安全卫士 资产状态 主机名称 操作
2024-06-18 01:07:41 2024-07-18 01:07:51 运行中 ecm-ceshi 查看
2024-06-18 01:13:16 2024-07-18 01:13:27 运行中 ecm-osm-ceshi 查看
2024-06-18 17:50:44 2024-07-18 17:50:58 运行中 VM-b989b4b1 查看
2024-06-18 17:50:44 2024-07-18 17:50:57 运行中 VM-1321844f 查看
2024-06-18 17:49:08 2024-08-18 17:49:21 运行中 VM-3bd4041a 查看
2024-06-18 17:49:08 2024-08-18 17:49:20 运行中 VM-f85523ac 查看
2024-06-20 20:08:57 运行中 proxy 查看
2024-06-20 19:02:02 运行中 tcpserver 查看
2024-06-20 19:53:05 运行中 client 查看
2024-06-12 14:39:18 运行中 ctcss-test-mq 查看
2024-06-02 17:13:09 2024-07-02 17:13:41 运行中 ycdl-5 查看
2024-05-14 15:41:17 运行中 ctcss-test-KxZ3 查看
共 75 条 1 2 3 4 20条/页



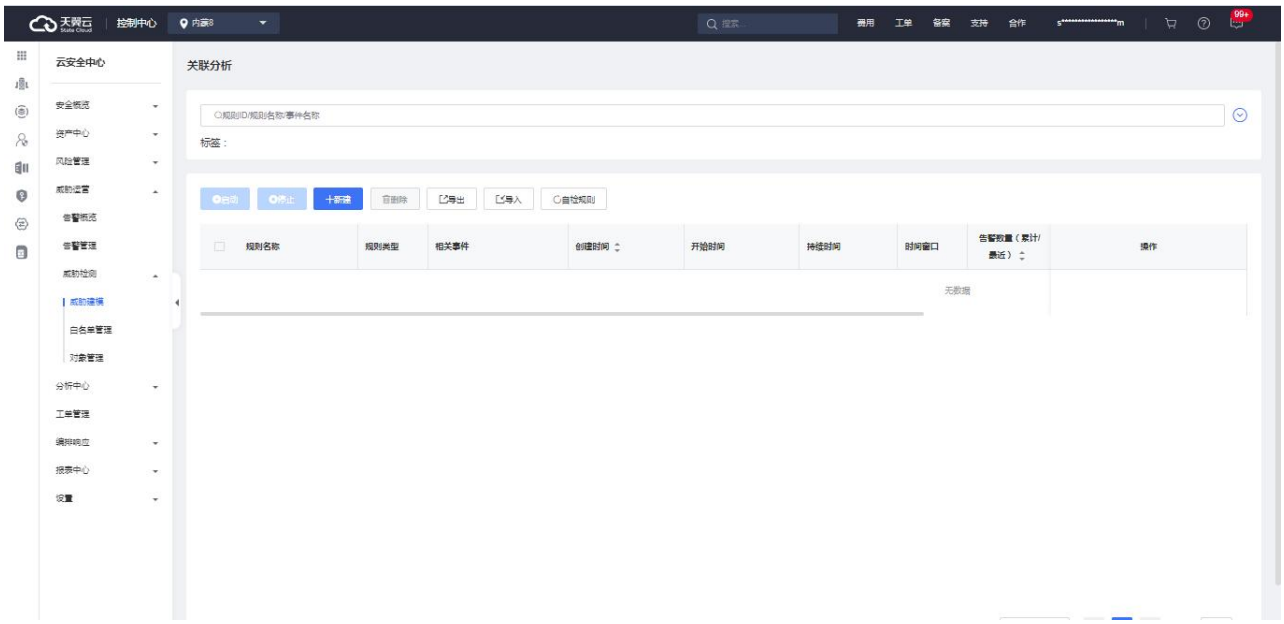
6、添加条件查询。



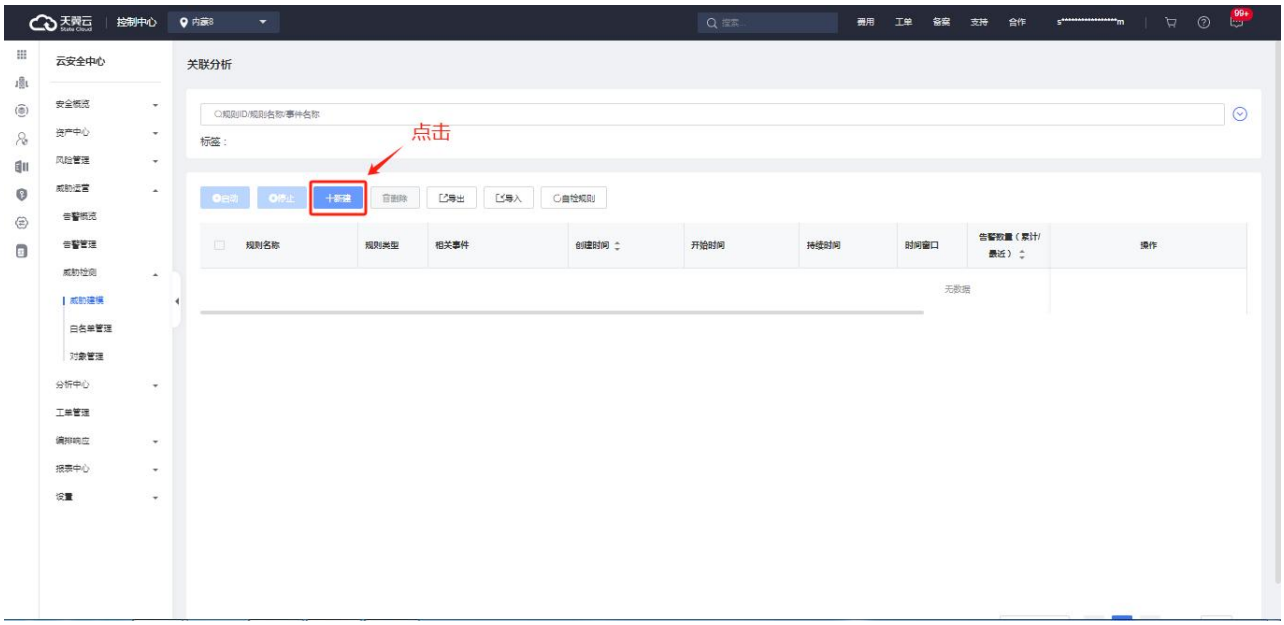
5.4. 如何进行威胁建模

1、进入云安全中心-威胁监测-威胁建模页面

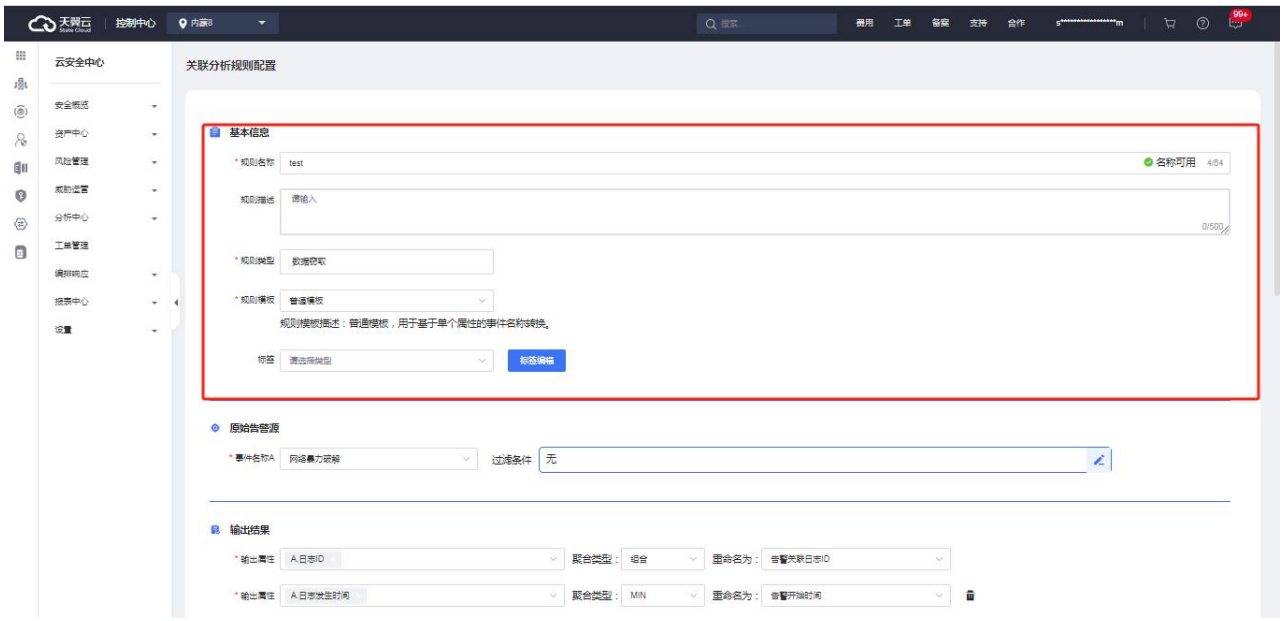
可以通过关键字、快捷方式、规则类型和标签查询关联分析规则。

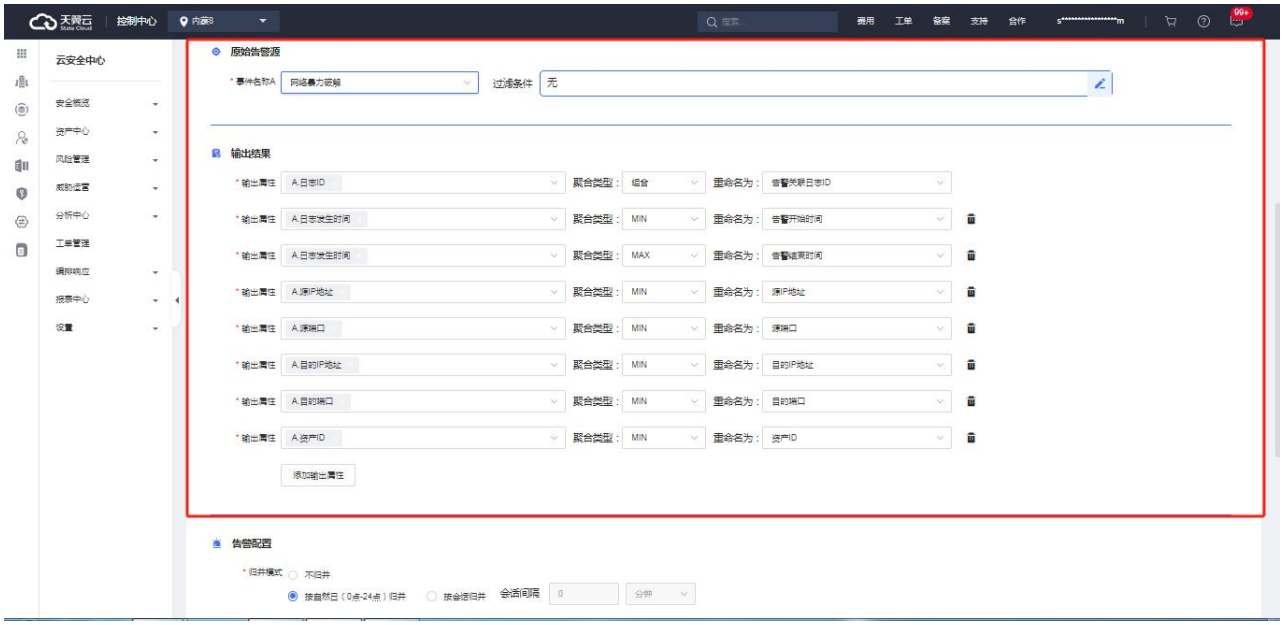


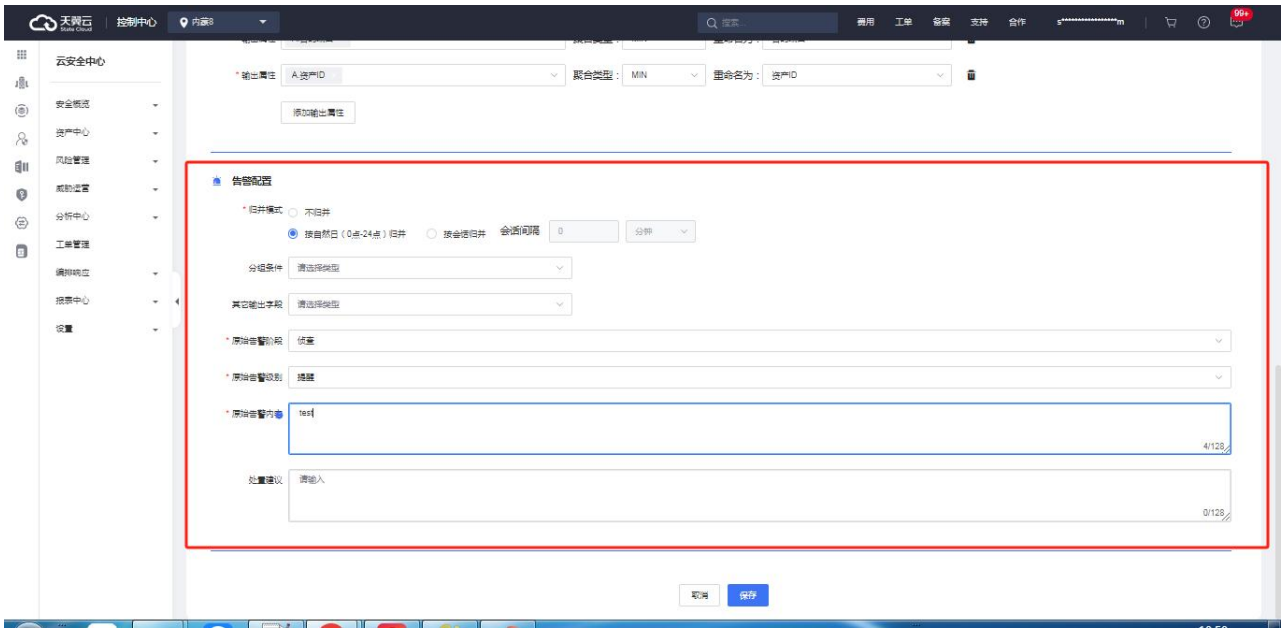
2、点击“新建规则”按钮

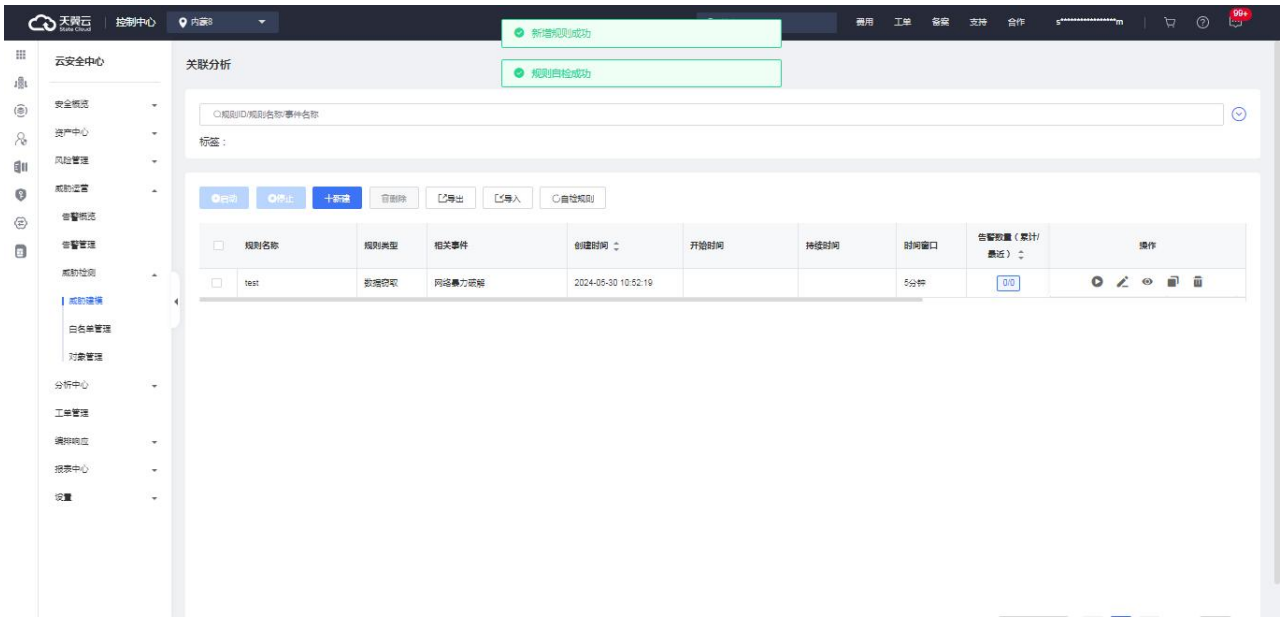


3、填写基本信息填写，带有*的为必填项


关联分析规则配置
基本信息
规则名称
test
名称可用
规则描述
请输入
规则类型
数据获取
规则模板
普通模板
规则模板描述：普通模板，用于基于单个属性的事件名称转换。
标签
标签编辑
原始告警源
事件名称A
网络暴力破解
过滤条件
无
输出结果
输出属性
聚合类型：
重命名为：


原始告警源
事件名称A
网络暴力破解
过滤条件
无
输出结果
添加输出属性
告警配置





5.5. 等级保护测评解读

云安全中心产品符合等级保护 2.0 标准体系主要标准。根据《网络安全等级保护基本要求》（GB/T 22239-2019），云安全中心满足第三级及以下安全要求：

等保标准章节	等保标准序号	云安全中心对应功能	功能解读
安全区域边界-边界防护	8.1.3.1	集成管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。同时能够对

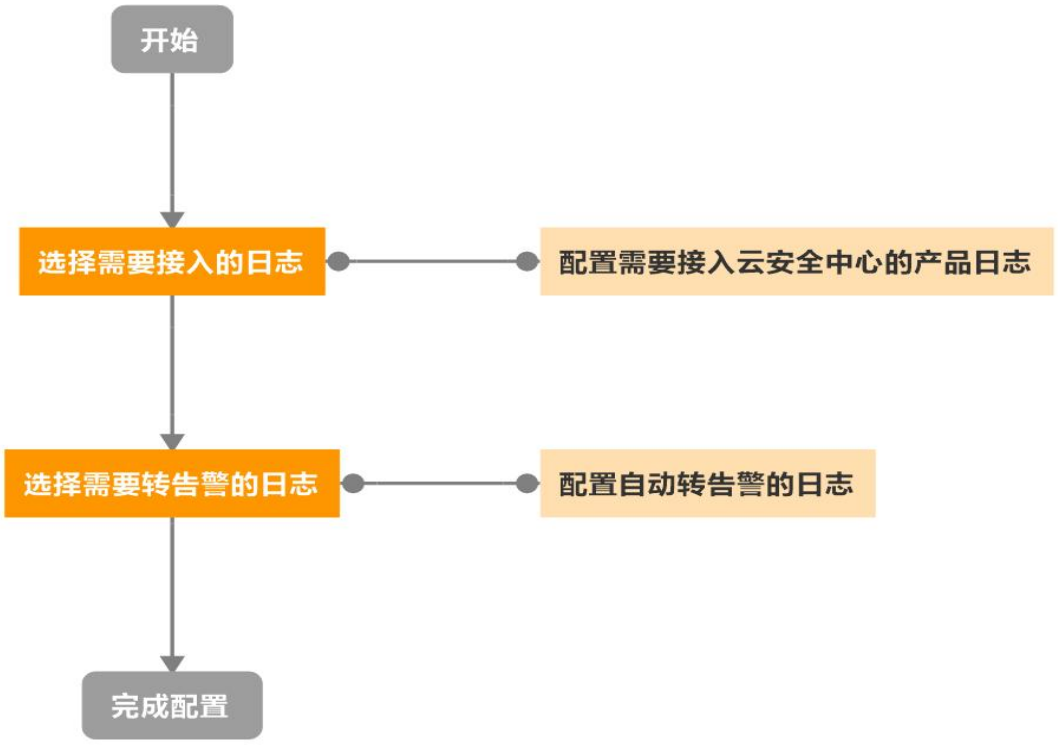
等保标准章节	等保标准序号	云安全中心对应功能	功能解读
			非授权设备私自联到内部网络的行为进行检查，通过处置功能实现对相关访问进行限制
安全区域边界-访问控制	8.1.3.2	集成管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。同时能够对非授权设备私自联到内部网络的行为进行检查，通过处置功能实现对相关访问进行限制
安全区域边界-入侵防范	8.1.3.3	集成管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，可在关键网络节点处检测、防止或限制从外部/内部发起的网络攻击行为，并对这些攻击行为进行分析、记录以及提供报警
安全区域边界-恶意代码和垃圾邮件防范	8.1.3.4	集成管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，可在关键网络节点处对恶意代码进行检测、分析，并通过处置功能实现对相关机器访问进行限制
安全区域边界-安全审计	8.1.3.5	集成管理、威胁运营	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，可以在网络边界以及重要网络节点进行安全审计，记录包括相关告警事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，通过威胁运营，能将单独用户行为审计和数据分析。
安全计算环境-安全审计	8.1.4.3	集成管理、威胁运营	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，可以在网络边界以及重要网络节点进行安全审计，记录包括相关告警事件的日期和

等保标准章节	等保标准序号	云安全中心对应功能	功能解读
			时间、用户、事件类型、事件是否成功及其他与审计相关的信息。云安全中心日志通过多副本实时存储多分，保障用户日志在其存储周期内不丢失、可恢复
安全计算环境-入侵防范	8.1.4.4	集成管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，能发现可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞，同时应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警
安全计算环境-恶意代码防范	8.1.4.5	集成管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，能够及时采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为。通过处置功能将其有效阻断。
安全区域边界-集中管控	8.1.5.4	集成管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，以及不同安全设备的处置集成，实现对分布在网络中的安全设备或安全组件进行管控; 通过内网建立一条安全的信息传输路径,对网络中的安全设备或安全组件进行管理; 形成对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测; 通过实时的日志采集，对分散在各个设备上的审计数据进行收集汇总和集中分析,并保证审计记录的留存时间符合法律法规要求;

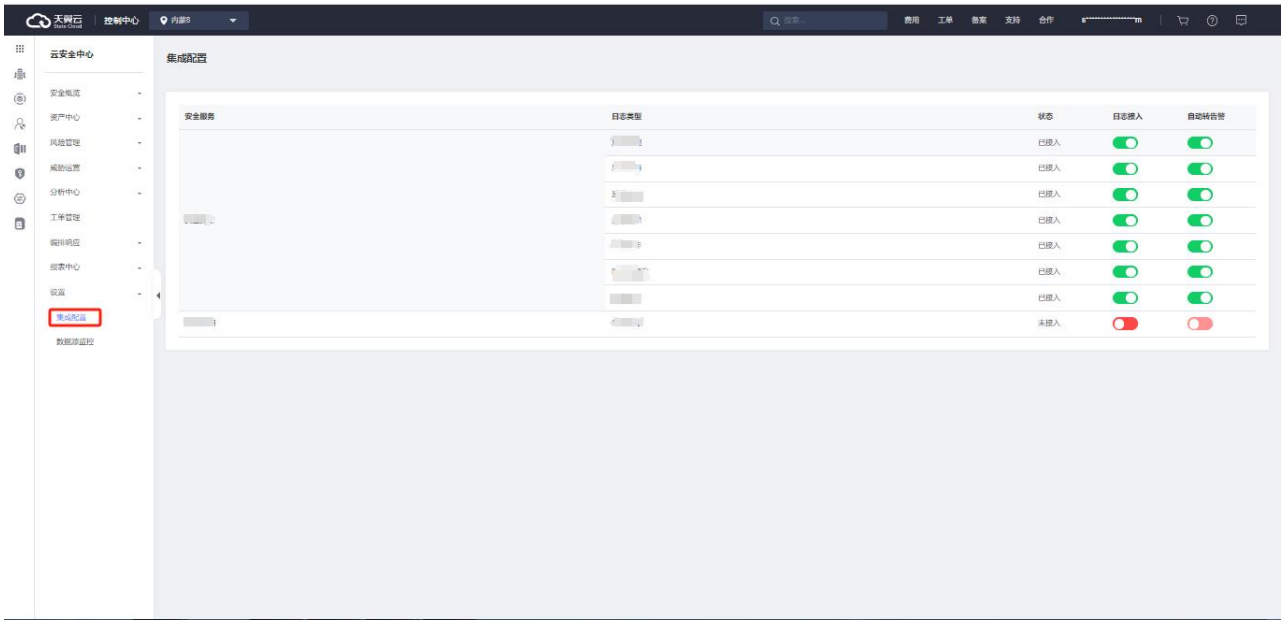
等保标准章节	等保标准序号	云安全中心对应功能	功能解读
			同时在应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； 通过编排响应能对网络中发生的各类安全事件进行识别、报警和分析；

5.6. 如何接入产品日志

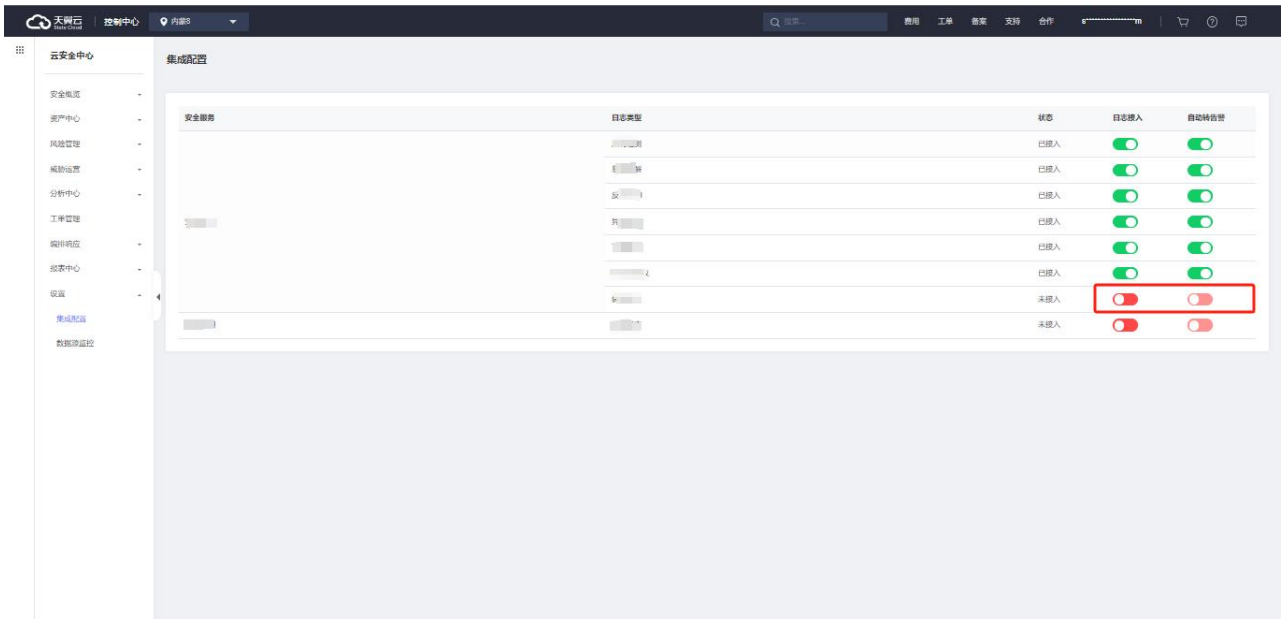
打开云安全中心的设置>集成配置，在集成配置中选择需要接入的日志类型。部分日志支持直接转告警，可以直接打开转告警开关，云安全中心会根据内置转告警规则进行转告警配置。接入流程如下：



1. 打开数据集成配置页面，点击设置>集成配置



2. 选择需要接入的日志，并打开日志接入开关。



6. 常见问题

6.1. 产品咨询类

Q：云安全中心是否只是对其他云安全产品日志进行采集分析?

A：云安全中心产品除了采集其他安全产品的日志进行统一管理外，还提供编排响应以及处置的能力，能够对告警形成自己的处置流程，并进行自动化处置。云安全中心打通了云上的各类安全产品形成联动响应处置，帮助用户提升威胁响应处置效率。

Q：云安全中心如何帮助客户满足等保合规要求?

A：云安全中心提供的集成管理、威胁运营、编排响应等功能，可以满足等保的“边界防护”、“访问控制”、“入侵防范”、“恶意代码和垃圾邮件防范”、“安全审计”、“恶意代码防范”、“集中管控”等要求。具体可参见等级保护测评解读。

Q：云安全中心支持采集云上哪些安全日志?

A：云安全中心目前支持采集云上安全产品的安全事件日志，包括主机安全、WAF 以及防火墙等产品。

Q : 短信使用余量是否进行提醒?

A ： 云安全中心会在剩余 500 条和全部使用完短信时提醒用户的短信剩余量。

6.2. 计费购买类

6.2.1. 计费常见问题

Q：同一个账号可以购买多个云安全中心实例吗?

A：同一个账号在同一个区域只能购买一个云安全中心实例，对应一个主资源版本。购买云安全中心实例后，您可以购买扩展资源。

Q：云安全中心实例到期后，数据还会保留吗?

A：购买的云安全中心实例到期后如未按时续费，公有云平台会提供一定的保留期。

- 保留期内，平台会冻结云安全中心的服务，用户配置的各类数据会继续生效，但用户无法访问云安全中心。
- 保留期满，用户若仍未续费，平台会清除实例资源，用户原有的配置信息将会被删除，同时云安全中心将不再获取第三方日志、用户云上资产等信息。

Q：云安全中心实例可以降低规格吗?

A：云安全中心实例不支持降级，同时已绑定的扩展资源也不支持单独退订。如您需要降低当前规格，你可以先退订当前的云安全中心实例，再重新购买云安全中心实例。

Q：云安全中心是否支持自动续订?

A：支持。您可以在购买套餐的同时勾选自动续订，同时也支持在使用过程中，在订单中心中设置自动续订。

Q：云安全中心存在规格差异吗?

A：当前云安全中心只有一个标准版，标准版版本附带的服务如下所示。

版本	即时通知服务	日志分析量
标准版	2000 条/月	40G/月

Q：云安全中心有哪些扩展服务可以购买?

A：云安全中心支持 2 种类型的扩展资源，用户可支持根据实际使用需求购买日志分析量扩展资源和态势大屏扩展资源。其中，态势大屏扩展资源只可购买一次，日志分析量扩展资源的购买资源最小单位为 50G，即扩展资源需要购买 50G 的整数倍。

Q：续费时是否可同时变更云安全中心版本或规格?

A：续费时您只能为当前的云安全中心实例版本规格进行续费，增加使用时长。续费时不能同时变更云安全中心的规格。您可以在续费完成后，对云安全中心实例版本进行升级。

Q：扩展资源购买上限是什么?

A：当前云安全中心提供态势大屏扩展资源及日志分析量拓展包。态势大屏扩展资源订购上限为 1 个，日志分析量拓展包订购暂无订购上限。请您根据业务需要按需订购。

Q：云安全中心是否支持按需计费？

A：当前云安全中心不支持按需计费。

Q：云安全中心有促销折扣吗？

A：当前云安全中心暂无优惠折扣。

Q：在使用期间购买了扩展资源，资源到期时间是何时？

A：扩展资源购买后与主资源绑定，资源到期时间与主资源一致。

Q：购买的扩展资源，支持单独退订吗？

A：不支持。扩展资源购买后与主资源绑定，不支持单独退订。

Q：退订重购后，原实例的配置数据可以保留吗？

A：用户退订后在 15 天内重新购买实例时，可恢复原有配置。当重新购买时距离退订已超过 15 天，原资源已释放且配置数据已删除，则无法恢复。

Q：如何选择日志分析量扩展资源？

A：购买日志分析量扩展资源时，您需要测算接入云安全中心的所有日志数据总量，确保您选购的日志分析量能覆盖每月的日志数据总量。

Q：日志分析量扩展资源会过期吗？

A：每月优先使用主资源赠送的日志分析量，当赠送部分使用完毕后再消耗日志分析量扩展资源。未用完的日志分析量扩展资源会一直累积（赠送部分每月清零不进行累积）。

6.2.2. 如何查看当前购买产品的产品规格

购买、续订、升级扩容后可以通过产品信息页面查看所购买产品的规格，同时个人消息中心以及用户绑定的手机也能够收到相关的购买成功提示短信。查看购买后的云安全中心规格方式如下：

1. 登录天翼云控制中心。
2. 在控制台列表页，选择“安全>云安全中心”。
3. 进入产品服务页面，选择“已购资源”。

注意：

购买成功后需要等待一段时间相关规格才能刷新，预计等到 1-2 分钟左右。

6.3. 配置类

6.3.1. 数据接入相关

Q：为什么要进行数据接入？

A：云安全中心（CT-CSC，Cloud Security Center，简称 CSC）作为用户侧的安全中心，其核心数据来源是用户的各种安全设备。

Q：云安全中心数据接入要如何配置？

A：打开云安全中心的设置>集成配置，在集成配置中选择需要接入的日志类型即可。

Q：云安全中心告警需要如何配置？

A：打开云安全中心的设置>集成配置，在集成配置中选择需要接入的日志类型。部分日志支持直接转告警，可以直接打开转告警开关，云安全中心会根据内置转告警规则进行转告警配置。同时云安全中心还支持自定义转告警配置，即通过云安全中心的“威胁运营>威胁建模”功能实现自定义告警配置。