



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
09	2025/04/30	<p>第九次正式发布。</p> <ul style="list-style-type: none">更新“安全态势 > 安全概览”，增加“攻击链”统计图。新增“安全体检”，支持从云安全中心控制台快速使用安全体检服务。
08	2025/03/21	<p>第八次正式发布。</p> <ul style="list-style-type: none">更新“威胁运营 > 通知管理 > 通知联系人”，增加“是否同时设置为日志分析用量不足和每日日报接受的联系人”开关。
07	2025/03/04	<p>第七次正式发布。</p> <ul style="list-style-type: none">新增“查看审计事件”章节。更新“安全态势 > 安全概览”。更新“安全态势 > 威胁攻击态势”。更新“资产中心 > 资产管理”，支持导入、导出、删除资产。
06	2025/01/15	<p>第六次正式发布。</p> <ul style="list-style-type: none">新增“告警通知相关”常见问题，补充钉钉机器人和微信机器人相关配置参数获取方式。
05	2024/12/06	<p>第五次正式发布。</p> <ul style="list-style-type: none">更新“威胁运营 > 通知管理”，新增钉钉、企微通知方式。
04	2024/11/08	<p>第四次正式发布。</p> <ul style="list-style-type: none">更新“安全态势 > 安全成果展示”和“安全态势 > 威胁攻击态势”，新增“设置定时刷新时间”。更新“分析中心 > 专题分析”，新增“删除图表库”。新增“设置 > 规则标签设置”。
03	2024/10/17	<p>第三次正式发布。</p>



		<ul style="list-style-type: none">● 新增“威胁运营 > 通知管理”。● 新增“分析中心 > 告警查询”。● 优化文档部分描述。
02	2024/08/16	<p>第二次正式发布。</p> <ul style="list-style-type: none">● 新增“威胁运营 > 告警管理”。● 更新“产品规格”。● 删除“工单管理”。● 删除“威胁运营 > 威胁检测 > 白名单管理”。● 删除“集成管理”。● 优化文档部分描述。
01	2024/07/10	第一次正式发布。

目 录

1. 产品简介	1
1.1. 产品定义	1
1.2. 产品优势	2
1.3. 功能特性	2
1.4. 应用场景	3
1.5. 产品规格	6
2. 计费说明	8
2.1. 计费模式	8
2.2. 升级扩容	8
2.3. 续订	10
2.4. 退订	14
2.5. 查看账单	15
3. 快速入门	19
3.1. 使用流程	19
3.2. 注册天翼云账号	20
3.3. 购买云安全中心实例	20
3.4. 接入日志、告警	23
3.5. 查看安全概览	25
4. 用户指南	27
4.1. 安全态势	27
4.1.1. 安全概览	27
4.1.2. 安全成果展示	36
4.1.3. 威胁攻击态势	38
4.2. 资产中心	39



4.2.1. 资产概览	40
4.2.2. 资产管理	40
4.3. 风险管理	46
4.3.1. 漏洞管理	46
4.3.2. 弱口令管理	49
4.4. 威胁运营	52
4.4.1. 告警概览	52
4.4.2. 告警列表	53
4.4.3. 告警管理	61
4.4.4. 通知管理	63
4.4.5. 威胁检测	70
4.5. 安全体检	73
4.6. 分析中心	74
4.6.1. 日志查询	75
4.6.2. 原始告警查询	77
4.6.3. 告警查询	79
4.6.4. 专题分析	80
4.7. 编排响应	83
4.7.1. 剧本管理	83
4.7.2. 插件管理	91
4.7.3. 规则配置	92
4.8. 报表中心	93
4.8.1. 报表任务	93
4.8.2. 报表模板	95
4.9. 设置	97
4.9.1. 集成配置	97
4.9.2. 数据源监控	98

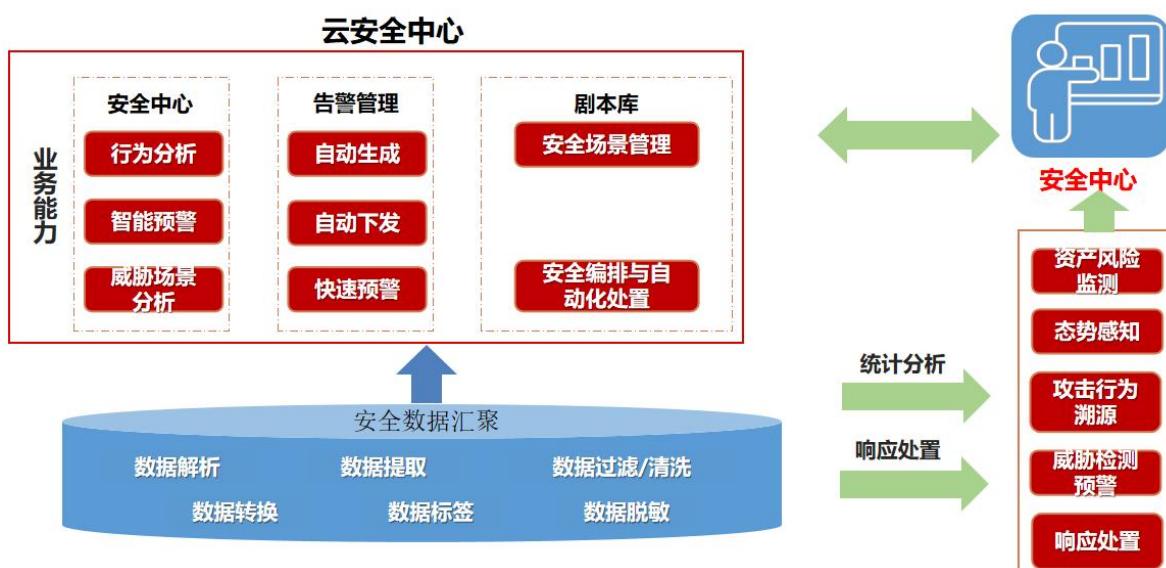


4.9.3. 规则标签配置.....	99
4.10. 查看审计事件.....	103
5. 最佳实践	105
5.1. 如何进行剧本管理.....	105
5.2. 如何进行漏洞管理	110
5.3. 如何对资产进行查看管理.....	113
5.4. 如何进行威胁建模	117
5.5. 等级保护测评解读.....	120
5.6. 如何接入产品日志、告警.....	123
6. 常见问题	125
6.1. 产品咨询类	125
6.2. 计费购买类	125
6.3. 配置类.....	128
6.3.1. 数据接入相关.....	128
6.3.2. 告警通知相关.....	129

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、告警响应的业务能力，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及处置效率。

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**

从多告警、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。

- **安全告警快速处置**

对接联动安全防护设备，在安全告警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、威胁运营、分析中心、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。
- **威胁运营**: 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。
- **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告警处理的“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

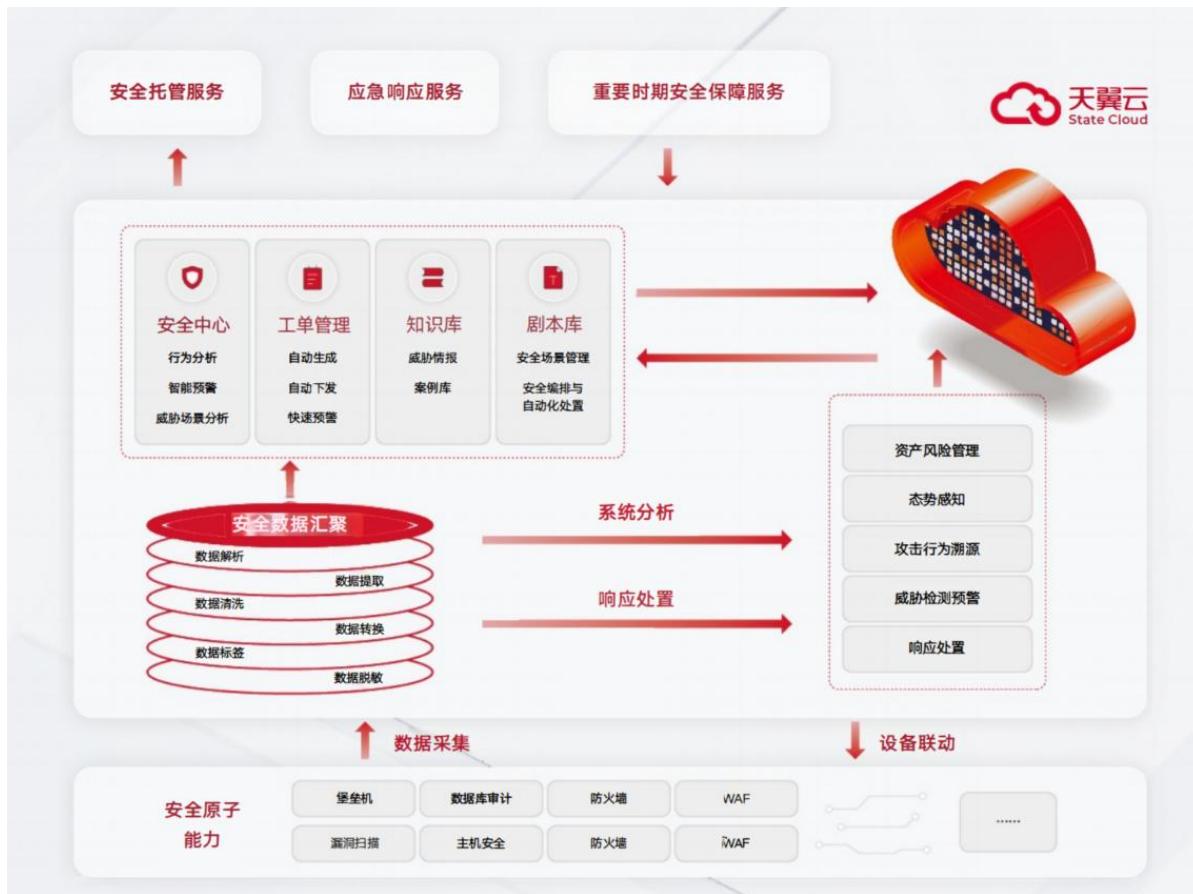
场景一：安全运营场景

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告警，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



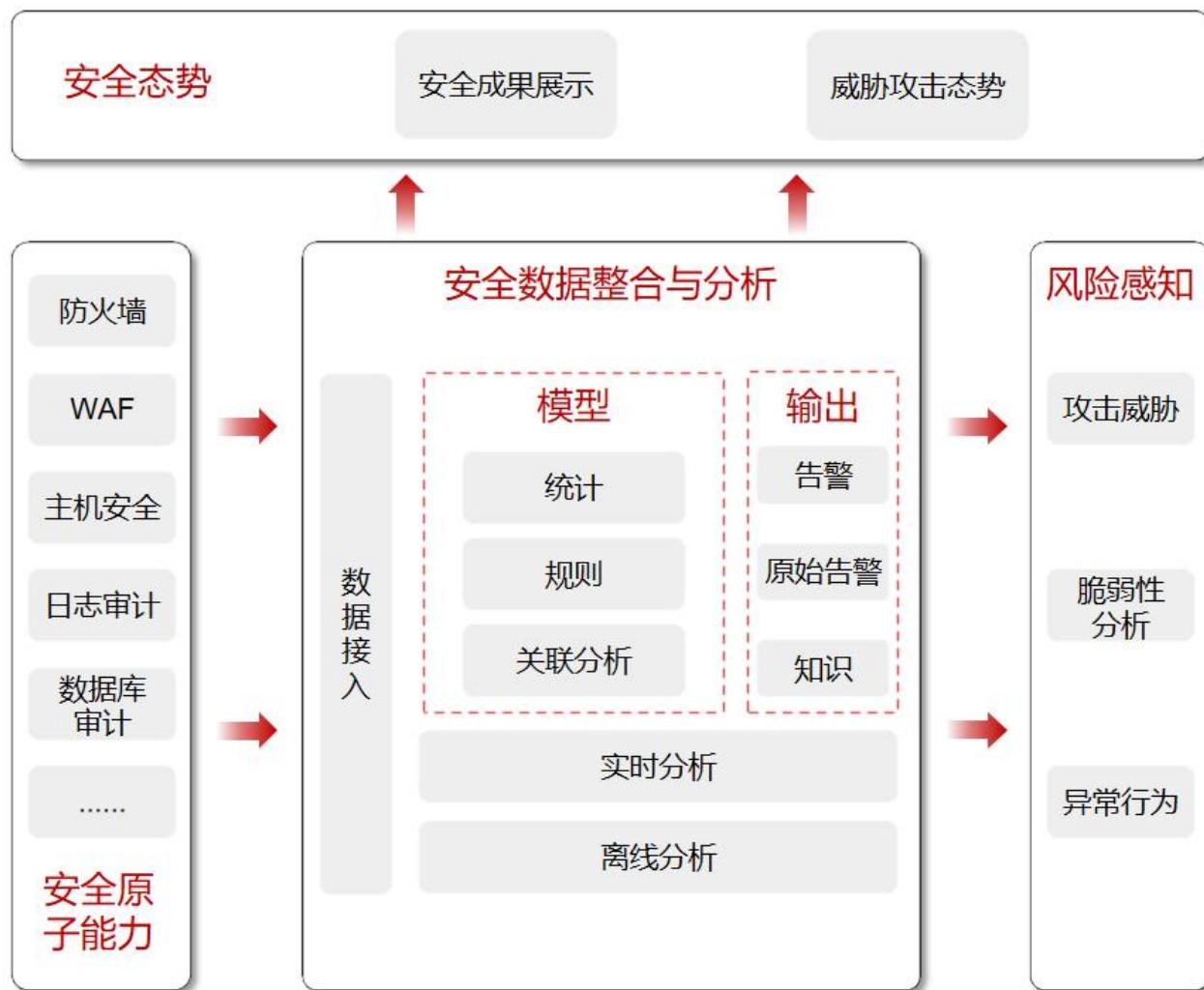
场景二：安全合规场景

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

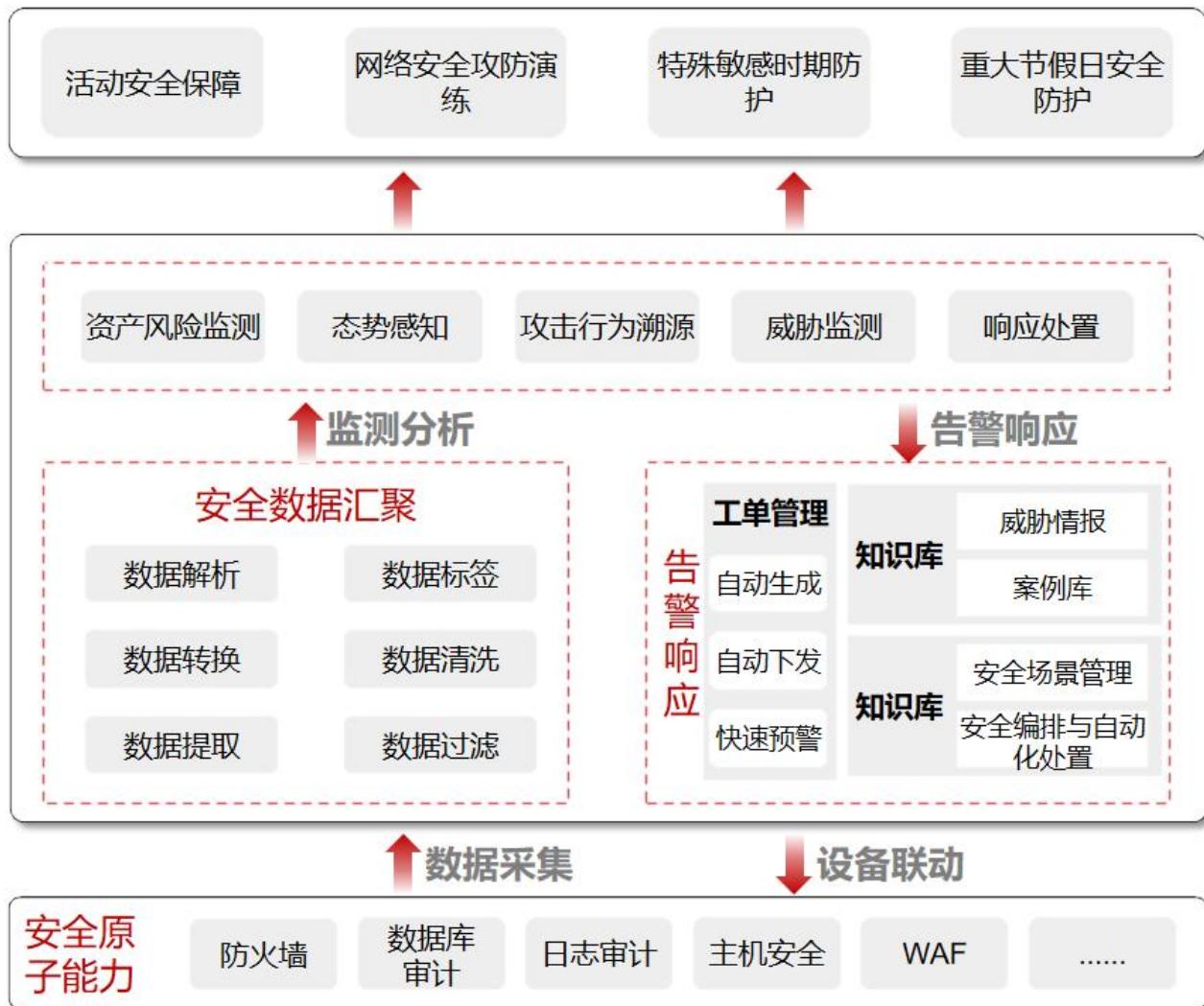
随着逐步接受和了解公有云的安全性，企业用户的重点转向了公有云‘内部’的安全。根据常见的责任分担模型，云运营商主要负责云基础设施的安全，而客户则负责云中数据和应用的安全，针对云中数据和应用的攻防实战就显得尤为重要了。

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	10000 条/月	50G/月

说明：

- 标准版包含的即时通知服务为每月 10000 条，月初余量进行重置，上月末用完的不进行转结。
- 标准版包含的日志分析量为每月 50G，月初余量进行重置，上月末用完的不进行转结。

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。

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

云安全中心

产品信息

云安全中心 (标准版) 包周期 付费方式

到期时间: 2024-09-06 00:35:48 (距离到期还有22天)

续订

态势大屏

实时、可视化地监控和分析网络安全态势，提供全面的安全威胁信息和预警，助力用户快速响应和处置告警。

未购买

购买态势大屏

日志分析量

云安全中心免费为您提供每月 50G 的日志分析额度，如果您需要额外的额度，请[另外购买](#)。

已使用(GB) 0 剩余量(GB) 100 购买日志分析量

100%

- 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。

购买态势大屏

* 态势大屏

- 1 + 个



购买日志分析量

* 日志分析量 GB

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. 在左侧导航栏，选择“已购资源”。

The screenshot shows the 'Cloud Security Center' page. On the left sidebar, under 'Bought Resources', the 'Cloud Security Center' is selected. The main area displays product information for 'Cloud Security Center (Standard Edition)'. It shows a renewal period of 30 days and a due date of 2024-09-06 00:35:48. A button labeled 'Renew' is visible. To the right, there's a 'Log Analysis' section with a progress bar indicating 100% usage of the monthly 50G log analysis quota.

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”。

The screenshot shows the 'Renewal Management' interface. On the left sidebar, under 'Renewal Management', the 'Cloud Security Center' is selected. The main area shows a list of renewal tasks. One task for 'Cloud Security Center' is listed, showing it was created on 2024-06-27 10:00 and will expire on 2024-07-27 10:00. Buttons for 'Manual Renewal' and 'Automatic Renewal' are present at the top of the list table.

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。



续订管理 / 手动续订

1. 从资源续订到续订完成存在一定时间间隔,“续订后到期时间”以续订完成时开始计算。

产品名称	资源ID	资源池	资源状态	倒计时	续订周期	时间	操作后续订周期、到期时间
云安全中心	18c13	-	在用	27 天	3个月	2024-10-13 17:26:09	3个月

续订周期： 1个月 2个月 3个月 4个月 5个月 6个月 7个月 8个月 9个月 10个月 11个月 1年 2年 3年

续订金额： ¥ [redacted]

提示：最终费用以计费出账为准

续订提交 取消

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”。

订购

* 购买时长
1 个月 2 个月 3 个月 4 个月 5 个月 6 个月 7 个月 8 个月 9 个月 10 个月 11 个月 1 年 2 年 3 年 1 个月

* 自动续订 开启 关闭
按月购买：自动续订周期为3个月；按年购买：自动续订周期为1年

我已阅读，理解并接受《云安全中心服务协议》

预置费用 ¥ [redacted]
参考价格，具体扣费请以账单为准。 [了解计费详情](#)

取消 立即购买

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。

- 进入天翼云“费用中心 > 订单管理 > 续订管理”页面。
- 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。



费用中心

续订管理

1. 支持自动续订的产品范围见[帮助文档](#)
2. 如果在自动续订前已完成人工续订，则同一周期内不会再自动续订。
3. 对于天翼云到期的资源，或已到期的资源，不支持设置修改自动续订。
4. 对于设置了自动续订，且10天内到期的资源，如果用户尝试修改自动续订周期，可能会因当期自动续订已完成导致当前变更未生效的情况。
5. 非独享订购且具有绑定或挂载关系的资源，需要分别开通自动续订，例如对云硬盘设置自动续订，该硬盘所挂载的云主机到期后将不可用。
6. 若资源到期后续费，续费周期由资源续订开始，计算新的服务有效期。

续订时间：全部时间、7天内到期、15天内到期、30天内到期、未到期、已到期、自定义
搜索框：云安全中心、请输入资源ID或控制台资源ID、请输入订单号、搜索
操作列：手动续订、自动续订、到期转按需
批量续订、开通自动续订
产品名称、资源ID/订单号、资源池、资源状态、资源名称、企业项目、倒计时、续订周期、订购方式、时间、操作
云安全中心、在用、default、26天、包周期、创建:2024-06-13 17:26 手动续订、到期:2024-07-13 17:26 开通自动续订
已选择: 0 / 1
共 1 条、10条/页、1页

- 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”。

自动续订
关闭 开通

续订周期：1个月、2个月、3个月、4个月、5个月、6个月、7个月、8个月、9个月、10个月、11个月、1年、2年、3年
续订金额：
 我已阅读并同意遵守[《天翼云自动续订服务协议》](#)
确定提交 取消
提示：最终费用以计费出账为准

3. 修改自定义续订周期。

- 进入天翼云“费用中心 > 订单管理 > 续订管理”页面。
- 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。
- 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。

自动续订
关闭 开通

续订周期：1个月、2个月、3个月、4个月、5个月、6个月、7个月、8个月、9个月、10个月、11个月、1年、2年、3年
续订金额：
 我已阅读并同意遵守[《天翼云自动续订服务协议》](#)
确定提交 取消
提示：最终费用以计费出账为准

4. 修改自定义续订开关。

- 进入天翼云“费用中心 > 订单管理 > 续订管理”页面。
- 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。

产品名称	资源ID / 订单号	资源池	资源状态	资源名称	企业项目	倒计时	时间	操作
云安全中心	[REDACTED]	-	在用	-	default	30 天	① 创建: 2024-06-27 10:05:57 ② 到期: 2024-07-27 10:05:54	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”。



退订管理/退订申请

满意度评价 资源被锁定

退订须知：

- 1、退订成功后资源不可恢复；
- 2、绑定退订前建议完成数据备份或者数据迁移；
- 3、除特殊约定（云电脑、云间高速专享版两款产品，退订后资源立即释放）以外，退订后的资源将被以冻结形式保留15天后释放；
- 4、退订可能会导致其他存在的关联业务产生影响。

退订规则请查看：[退订规则说明](#)

产品名称	资源ID	资源池	资源状态	时间	产品金额	可退订金额
云安全中心	[REDACTED]		在用	① 创建:2024-06-27 10:05:57 ② 到期:2024-07-27 10:05:54	元	元

* 请选择退订原因：

- 购买云服务时选择参数 (配置、时长、台数等)
- 云服务功能不完善，不满足业务需求
- 其他云服务商的性价比更高
- 区域选择错误
- 云服务故障无法修复
- 其他

产品金额: ￥ 元
退订金额: ￥ 元

我已确认本次退订金额和相关费用

退订 **取消**

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。

我的订单/订单详情

订单号： [REDACTED] 订单类型：退订 创建时间：2024-06-26 11:02:56 更新时间：2024-06-26 11:03:45

退订完成	发起退订	退订中	退订完成
------	------	-----	------

产品1 退订完成

产品	配置	订购数量	所属资源池	周期	金额(元)
云安全中心	—	1	—	30天	元

订单金额: 元
合计退订金额: 元

4. 当状态变为退订完成时，订单完成退订。

我的订单

满意度评价 查看帮助 常见问题

云订单 网订单

历史订单 ▶

订单号	产品	项目	类型	计费方式	创建时间	状态	金额(¥)	操作
[REDACTED]	云安全中心	default	订购	包周期	2024-06-27 10:05:17	已完成	元	详情

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。



费用中心

账单概览

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

合同管理

① 您可能想了解：对账指引、按需产品周期结算说明。

- 1、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。
- 2、CDN、VPC等按月结算的产品，当月消费可在次月3日查看账单。
- 3、月账单概览汇总数据由多个拆分数据组成，查询结果仅作参考，不作为对账依据，实际费用以导出明细账单为准。

账期 **近6个月消费汇总(¥)**

金额 (¥)

5,000
4,000
3,000
2,000
1,000
0

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。

① 您可能想了解：对账指引、按需产品周期结算说明。

- 1、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。
- 2、CDN、VPC等按月结算的产品，当月消费可在次月3日查看账单。
- 3、月账单概览汇总数据由多个拆分数据组成，查询结果仅作参考，不作为对账依据，实际费用以导出明细账单为准。

统计维度 统计周期 计费模式 账期

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

合同管理

账期	产品名称	账单类型	官网价(¥)	优惠金额(¥)	应付金额(¥)	实付金额(¥)
202311	弹性云主机	退款-退订	0.00	0.00	56.00	0
202311	云硬盘	退款-退订	0.00	0.00	5.20	0
202311	云硬盘	退款-退订	0.00	0.00	3.20	0
202311	SSL VPN	退款-退订	0.00	0.00	20.00	0
202311	弹性云主机	退款-退订	0.00	0.00	182.00	0



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



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

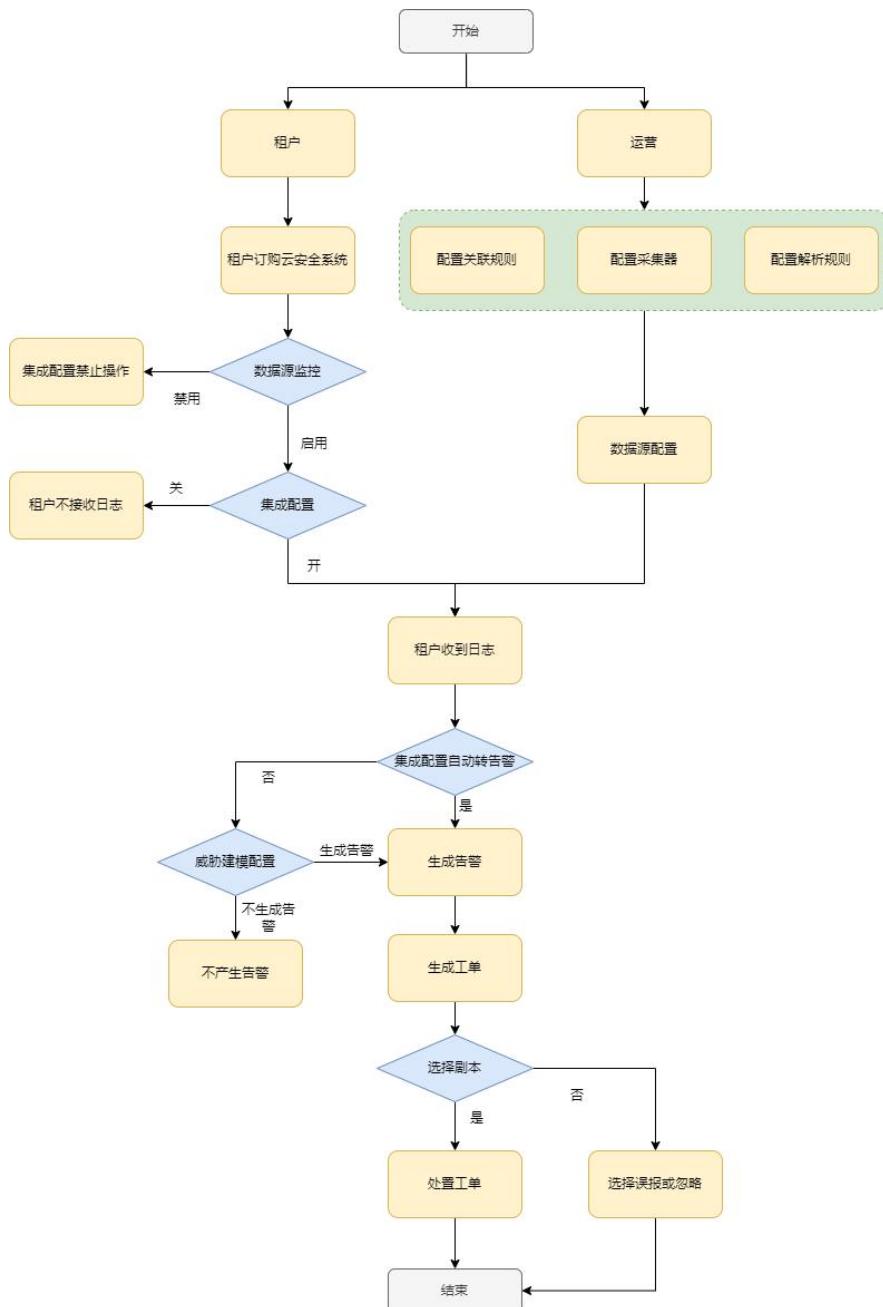
导出

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。

The screenshot shows the official website for Cloud Wings (天翼云). At the top, there is a navigation bar with links for '最新活动' (Latest Activities), '产品' (Products), '解决方案' (Solution), '应用商城' (Application Marketplace), '合作伙伴' (Partners), '开发者' (Developer), '支持与服务' (Support & Services), and '了解天翼云' (Learn about Cloud Wings). On the right side of the header is a search bar and a red '免费注册' (Free Registration) button. Below the header, there is a large banner with the text '加入天翼云合作伙伴计划' (Join the Cloud Wings Partner Program) and a subtext '回报高、响应快、培训全，持续为客户与伙伴创造价值' (High returns, fast response, full training, continuously creating value for customers and partners). In the background of the banner, there are stylized icons of servers and clouds.

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。

The screenshot shows the registration form for Cloud Wings. It includes fields for '邮箱地址' (Email Address), '密码' (Password), '确认密码' (Confirm Password), '+86 手机号码' (Phone Number), '验证码' (Captcha), and a '验证码(选填)' (Optional) field. There is also a '获取验证码' (Get Captcha) button. Below the form is a checkbox labeled '我已阅读《中国电信天翼云用户协议》和《中国电信天翼云隐私政策》' (I have read the 'China Telecom Tianyi Cloud User Agreement' and 'China Telecom Tianyi Cloud Privacy Policy'). At the bottom is a large grey button labeled '同意协议并提交' (Agree to the agreement and submit).

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。



云安全中心

欢迎使用云安全中心

云安全中心是天翼云一站式安全管理与运营平台，它具备实时监测、多维关联分析与快速响应安全威胁的能力，通过一体化的安全运营解决方案，助力用户实现云安全的全面管理和控制，降低用户的安全风险，提升用户安全运营效率。

立即购买



3. 单击“立即购买”，进入购买页面。

基础信息

* 版本选择 标准版

* 计费模式 包年/包月

扩展配置

* 购买态势大屏 现在购买 暂不购买

* 购买日志分析量 现在购买 暂不购买

50 GB

云安全中心免费为您提供50G的日志分析额度，如果您需要额外的额度，请另外购买。

订购

* 购买时长 1个月 2个月 3个月 4个月 5个月 6个月 7个月 8个月 9个月 10个月 11个月 1年 2年 3年

* 自动续订 开启 关闭

按月购买：自动续订周期为3个月；按年购买：自动续订周期为1年

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”。
扩展配	购买态势大 默认为“现在购买”，也可以选择“暂不购买”。



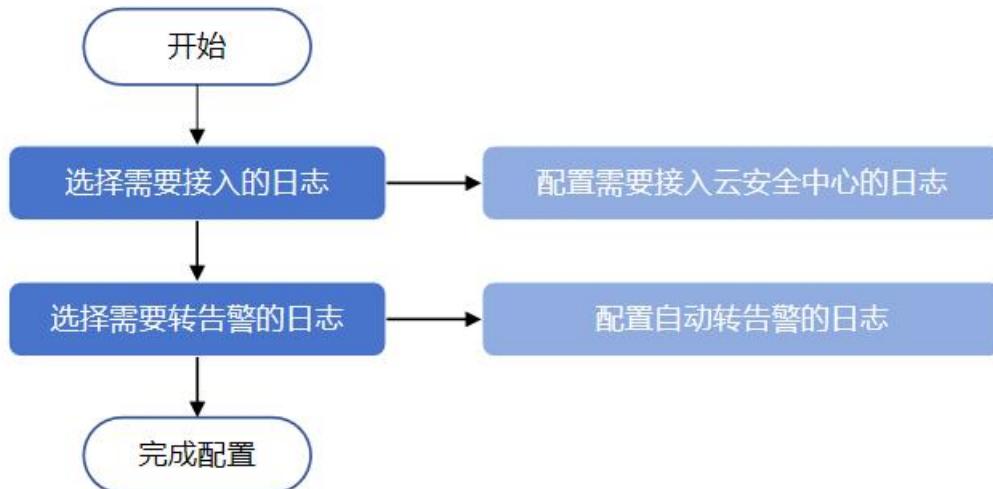
参数	说明
置屏	<p>说明：</p> <p>态势大屏只可购买一次。</p>
购买日志分析量	<p>默认为“现在购买”，也可以选择“暂不购买”。</p> <p>说明：</p> <p>云安全中心标准版免费提供 50G 的日志分析额度，如果您需要额外的额度，请另外购买。</p> <p>日志分析量扩展资源的购买资源最小单位为 50G，即购买时只能选择 50G 的整数倍。</p>
购买时长	拖动时间轴设置购买时长，可以选择 1 个月~3 年的时长。
订购自动续订	<p>开启“自动续订”后，当服务到期前，系统会自动按照默认的续费周期生成续费订单并进行续费，无须用户手动续费。</p> <ul style="list-style-type: none">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。 <p>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。</p>

- 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”。
- 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。

在云安全中心的集成配置页面，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。



操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“设置 > 数据源监控”，打开数据源监控页面。
3. 在操作列点击“启用”，确保数据源监控处于启用状态。



4. 在左侧导航栏，选择“设置 > 集成配置”，打开数据集成配置页面。
5. 选择需要接入的日志，并打开日志接入开关。



安全服务	日志类型	状态	日志接入	自动转告警
1		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7		未接入	<input type="checkbox"/>	<input type="checkbox"/>

6. 选择需要转告警的日志，并打开自动转告警的开关。

集成配置				
安全服务	日志类型	状态	日志摄入	自动转告警
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		未接入	<input type="checkbox"/>	<input type="checkbox"/>

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。
- 需要先在数据源监控页面启用开关后，才可以在集成配置页面中开启日志和告警配置。
- 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。

3.5. 查看安全概览

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、威胁动态、日志分布TOP5、风险资产TOP5、告警处置概览、近七天趋势图、攻击链统计图。

前提条件

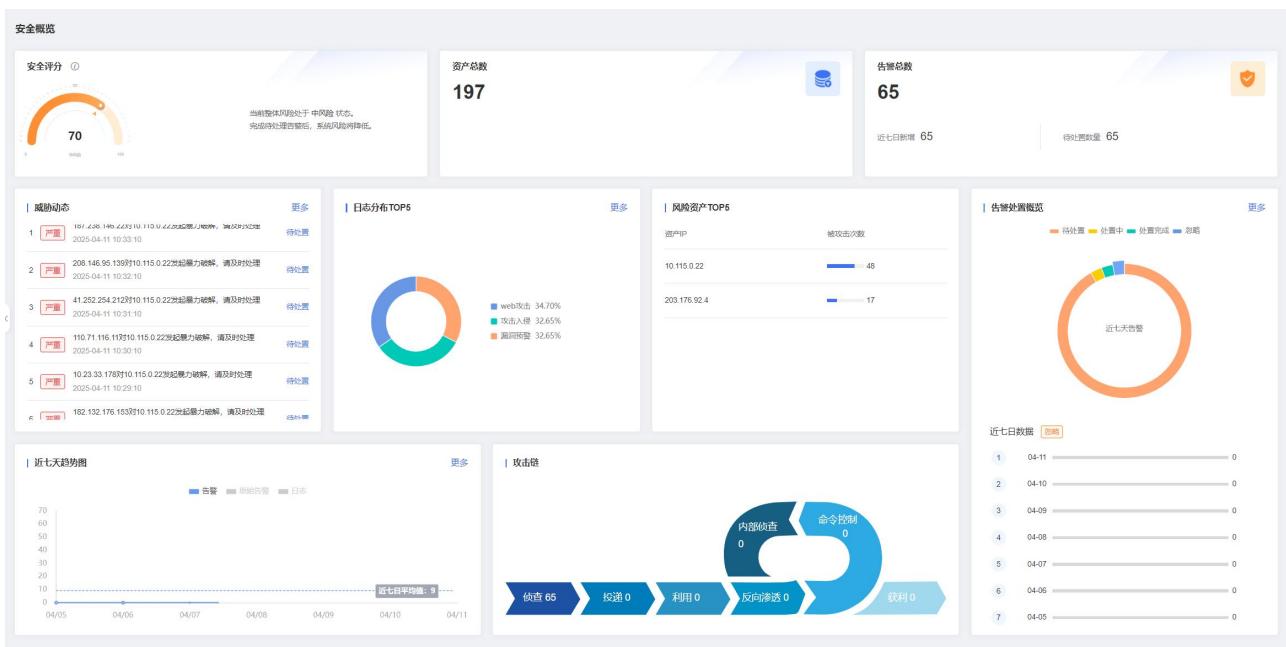
安全概览的数据来源于接入系统的数据量，需要确保已完成数据接入。具体操作请参见[接入日志、告警](#)。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择“安全态势 > 安全概览”，进入安全概览页面，查看安全评分和风险数据统计。

说明：

- 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。



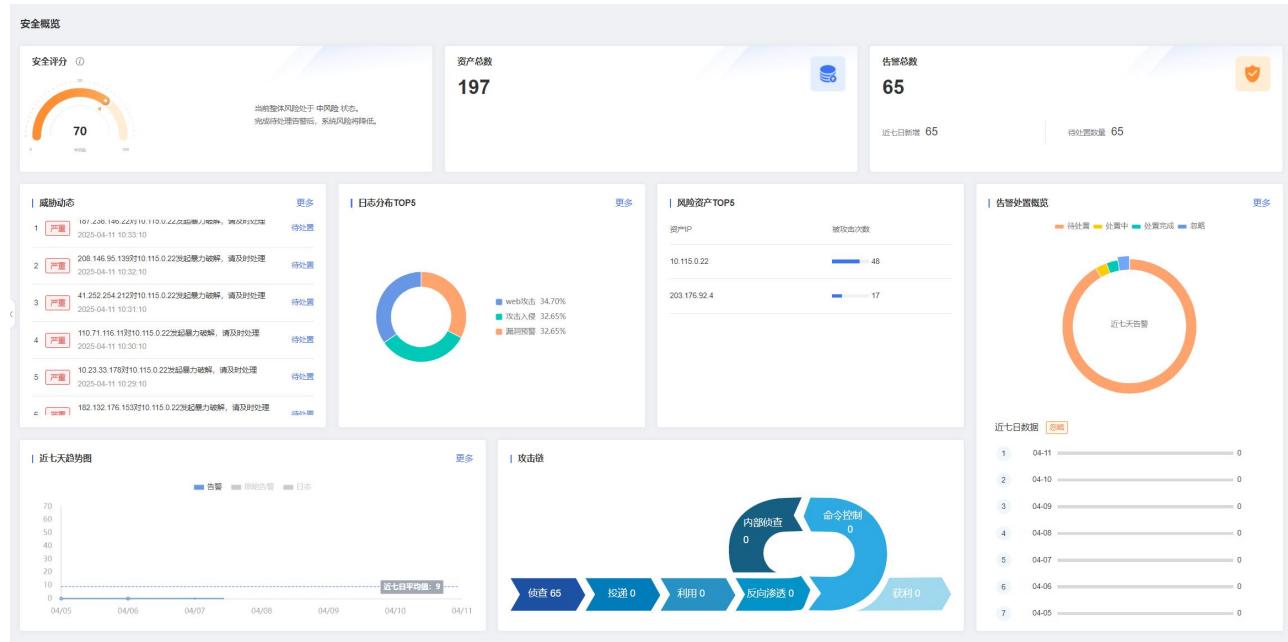
4. 用户指南

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：展示安全评分、资产总数、告警总数、威胁动态、日志分布 TOP5、风险资产 TOP5、告警处置概览、近七天趋势图、攻击链统计图。其中告警总数、威胁动态、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%。

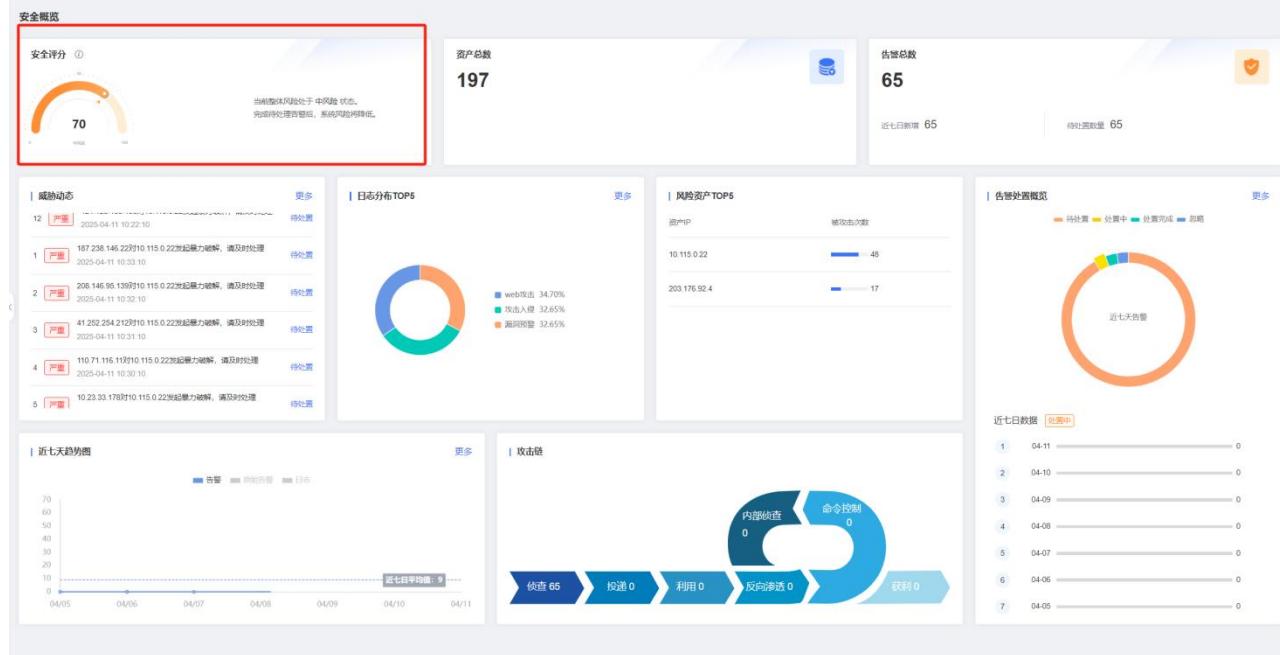
扣分规则：【弱口令】10 分/项；【漏洞】高危 5 分/项，中危 2 分/项；【告警】致命 5 分/项，严重 3 分/项，警告 1 分/项。



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）。

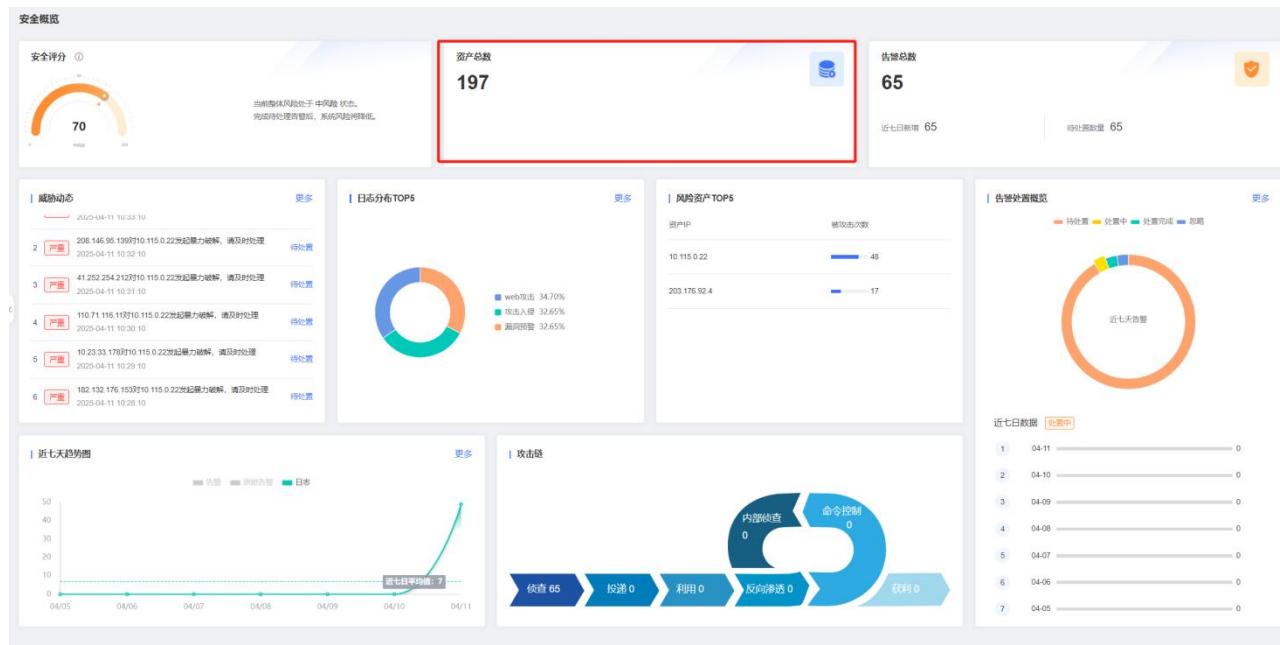
说明：

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

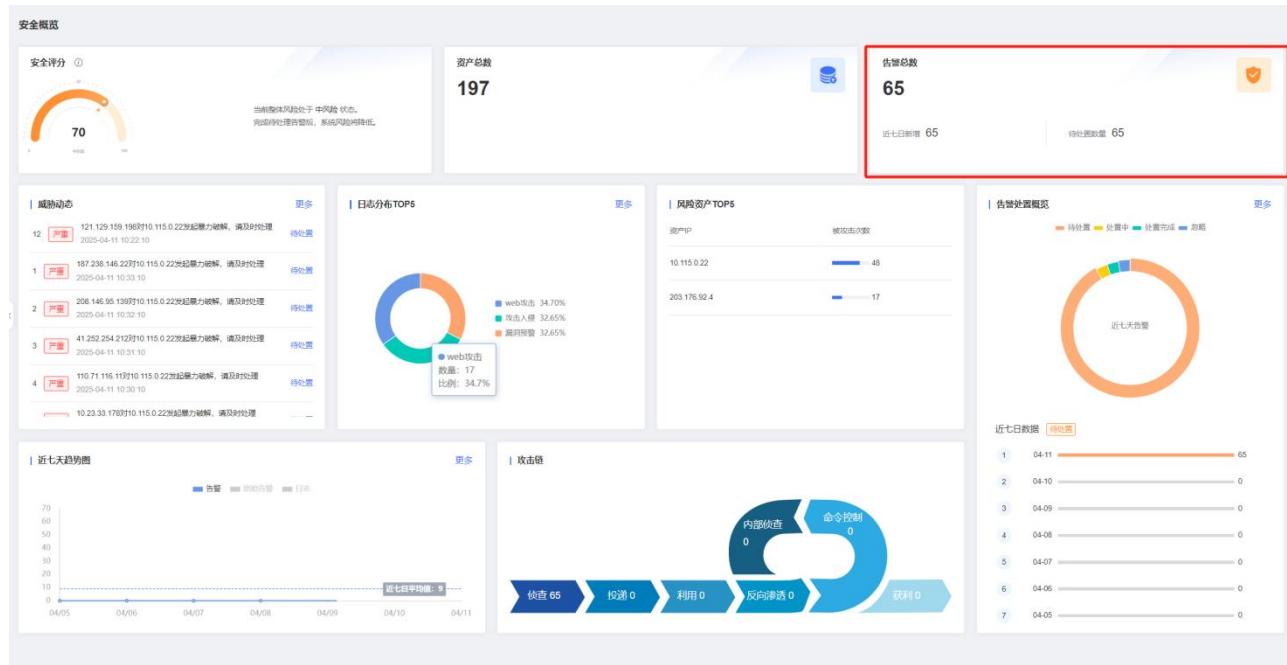
统计已经接入云安全中心的资产总数。



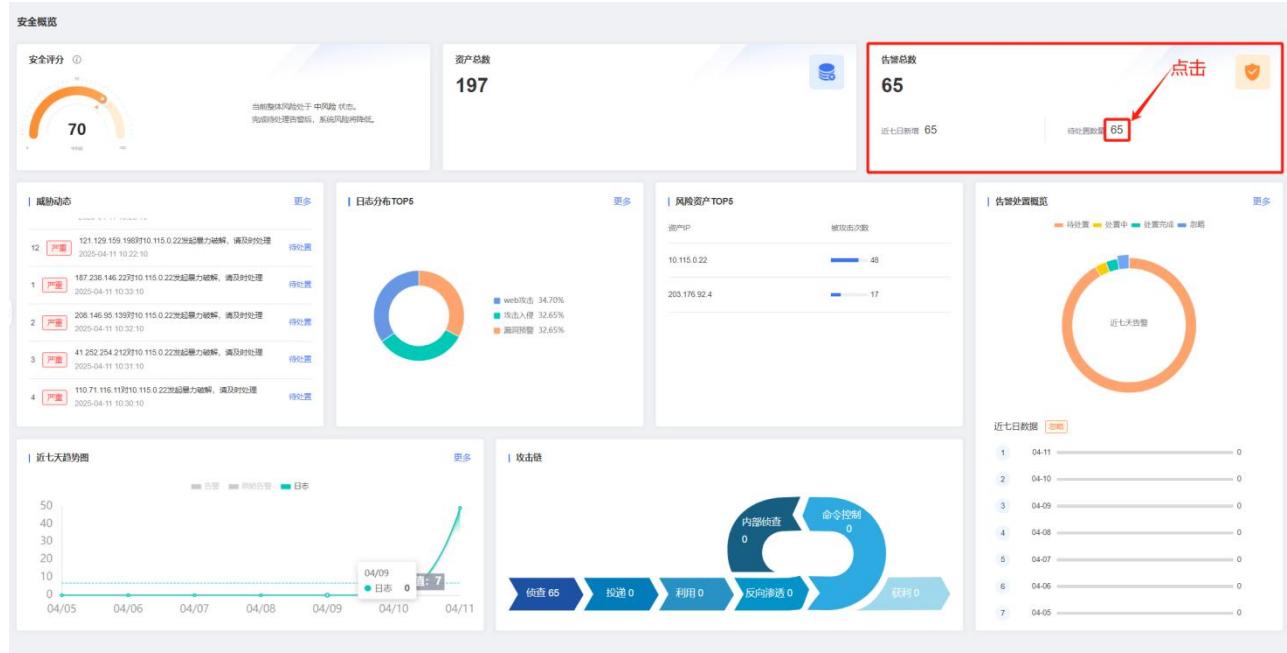


告警总数

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。

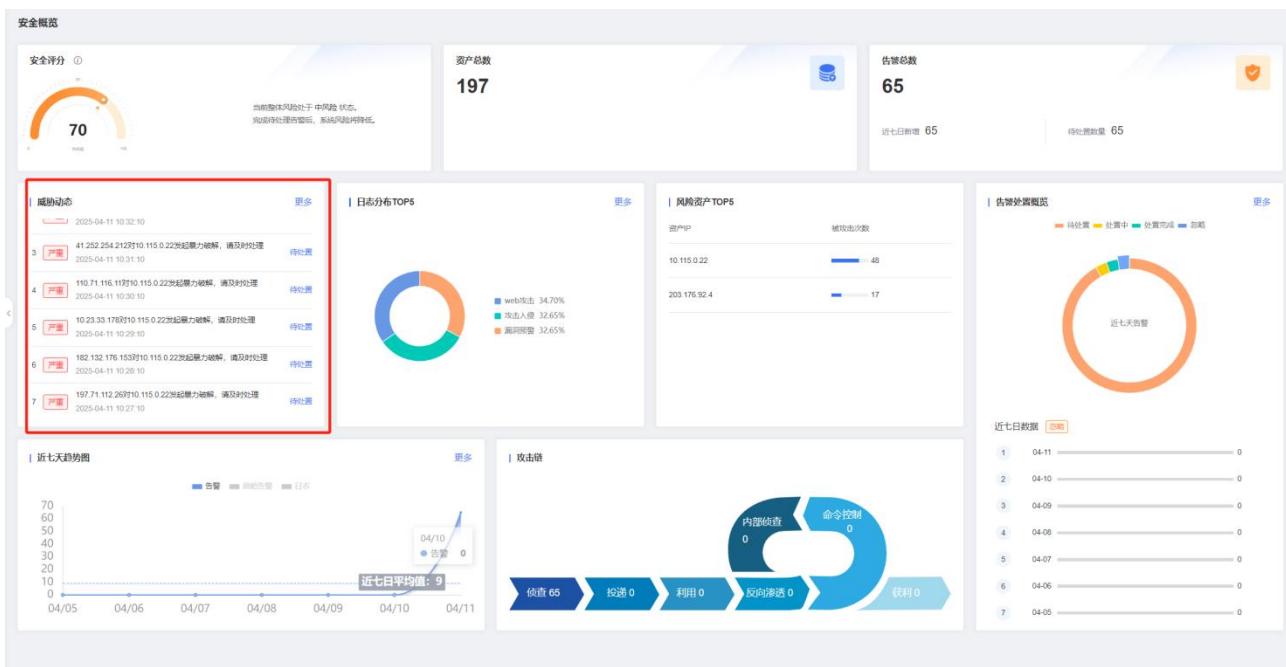


近 7 日新增，支持下钻至告警管理页面。

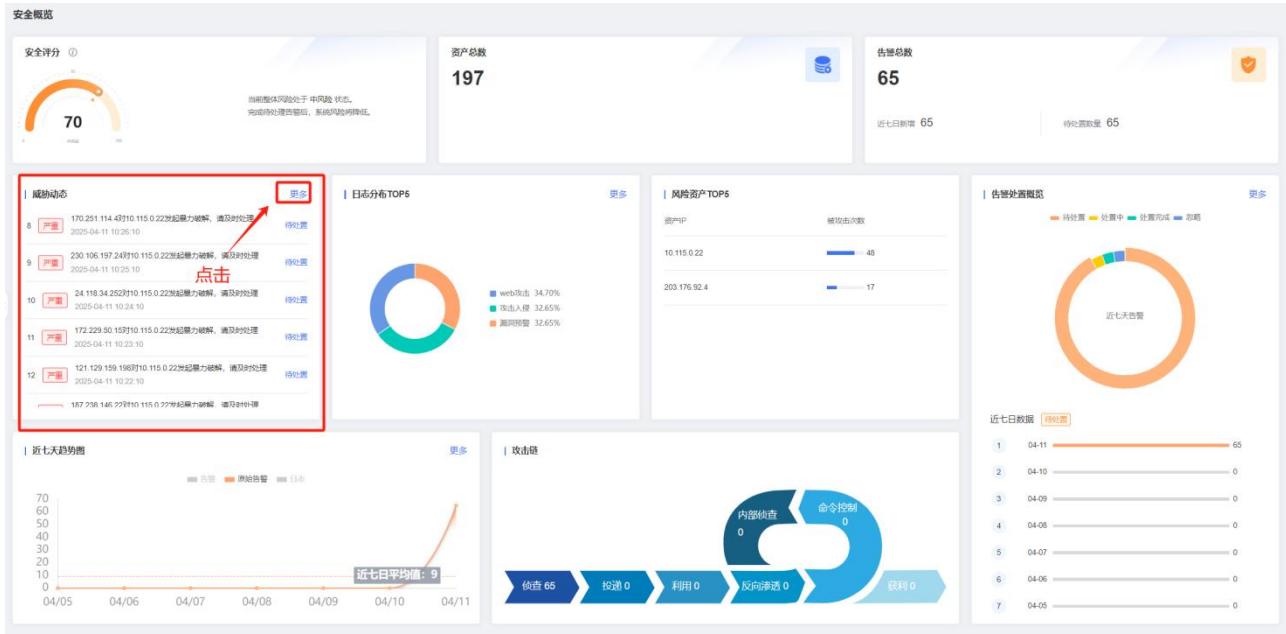


威胁动态

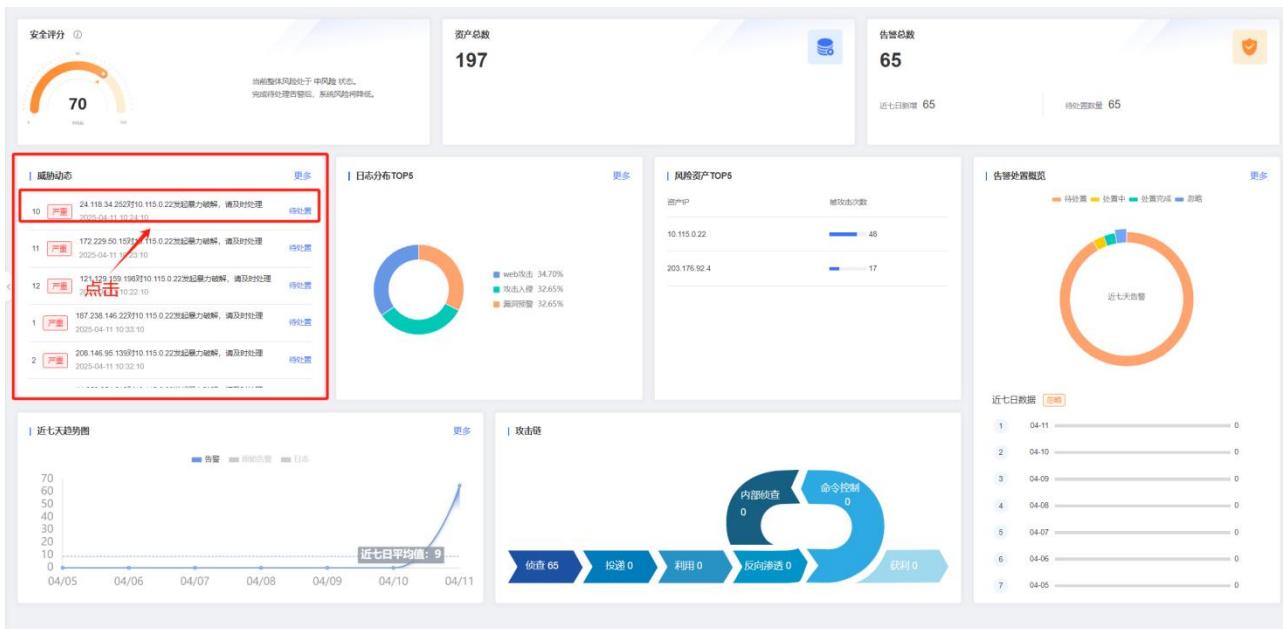
提供有效告警 TOP12 的滚动展示，快速定位高风险事件，提升响应效率。



点击更多，支持下钻至告警管理页面。

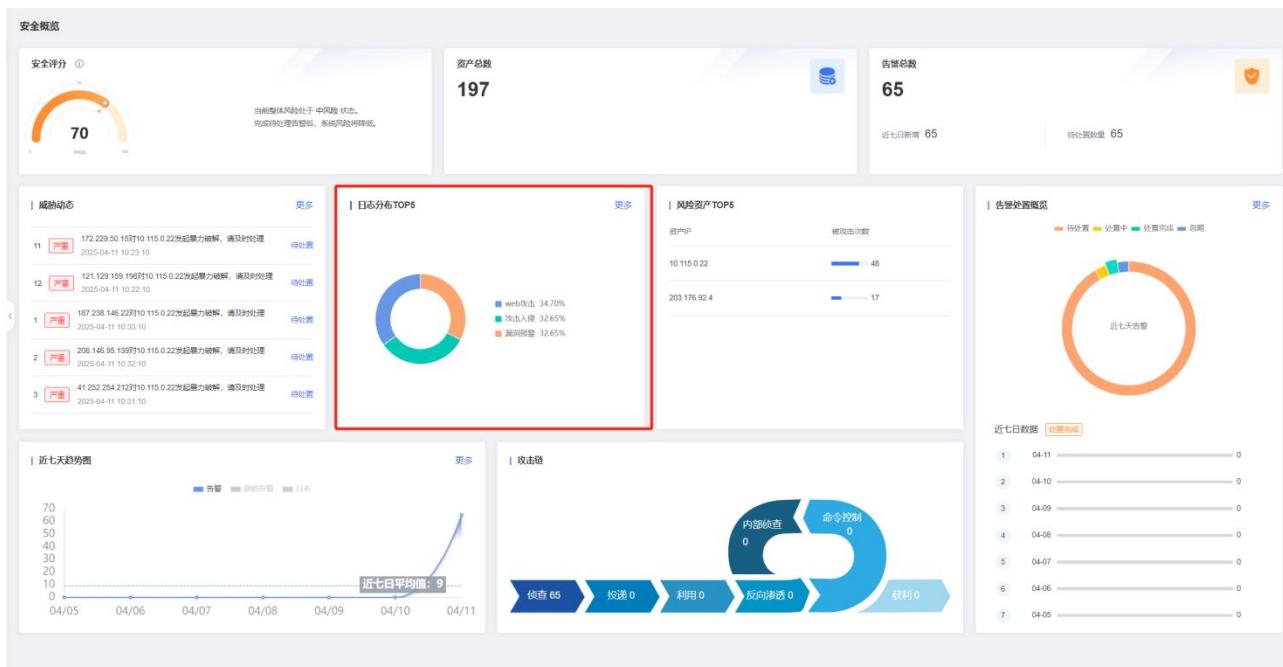


点击告警消息，支持下钻至告警消息详情页面。

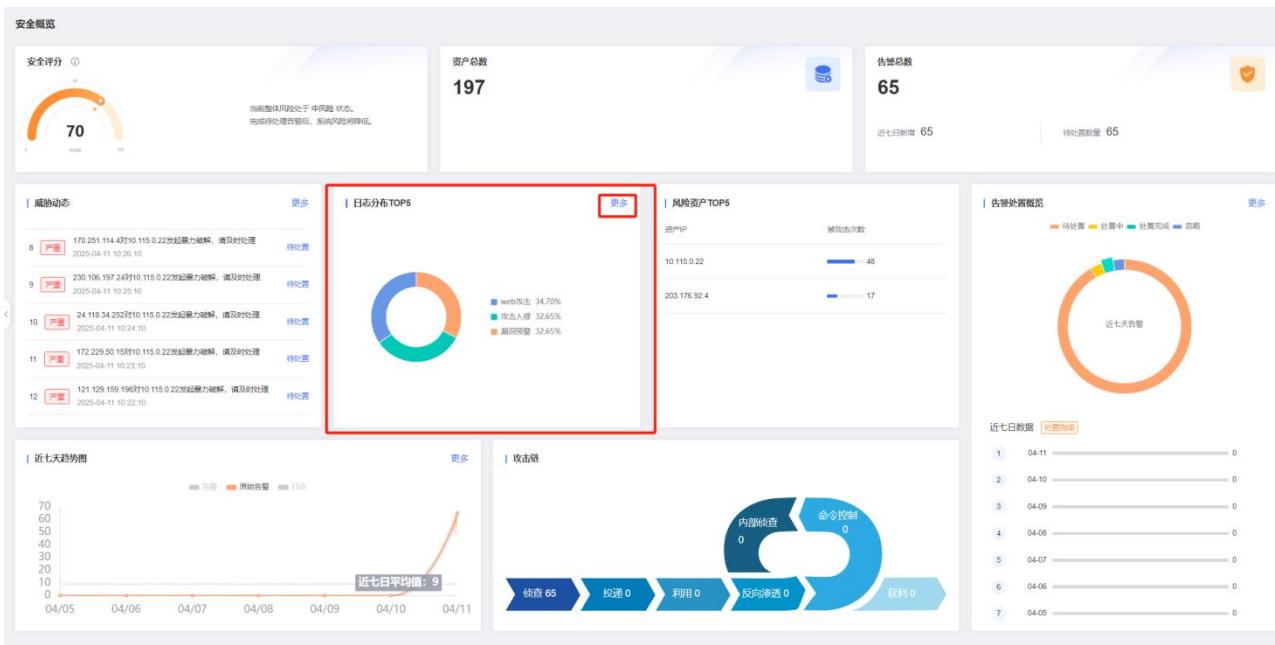


日志分布 TOP5

提供日志分布 TOP5 的展示。

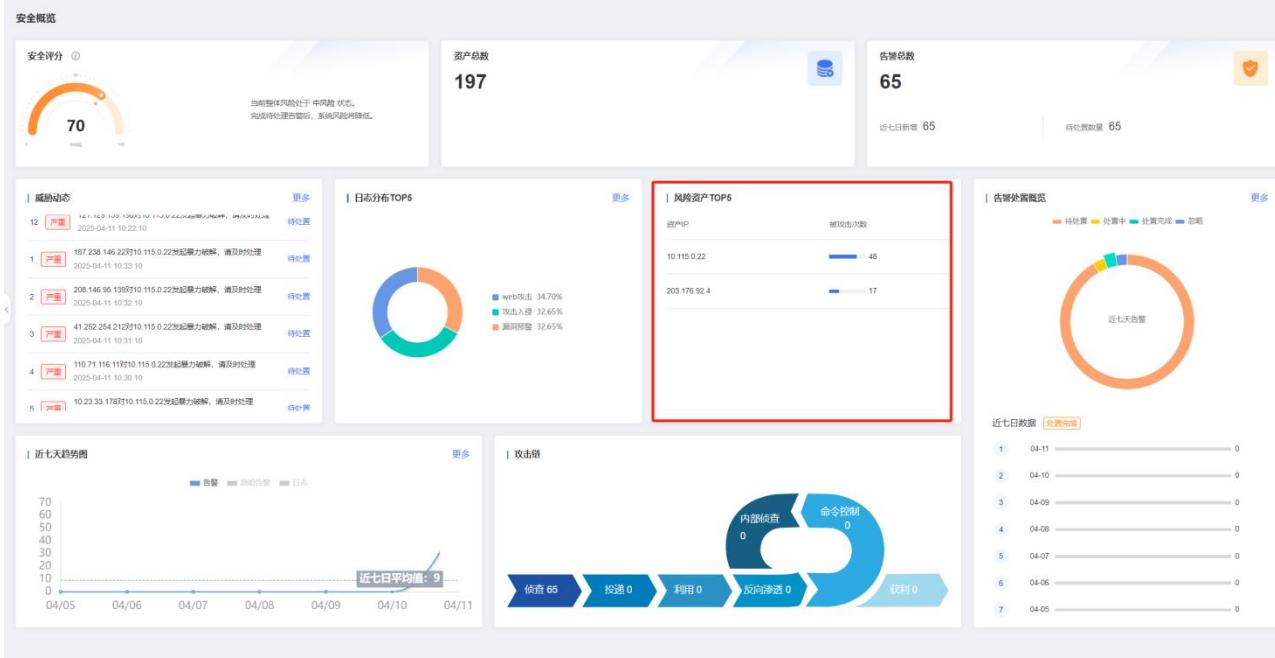


点击更多，支持下钻至日志查询页面



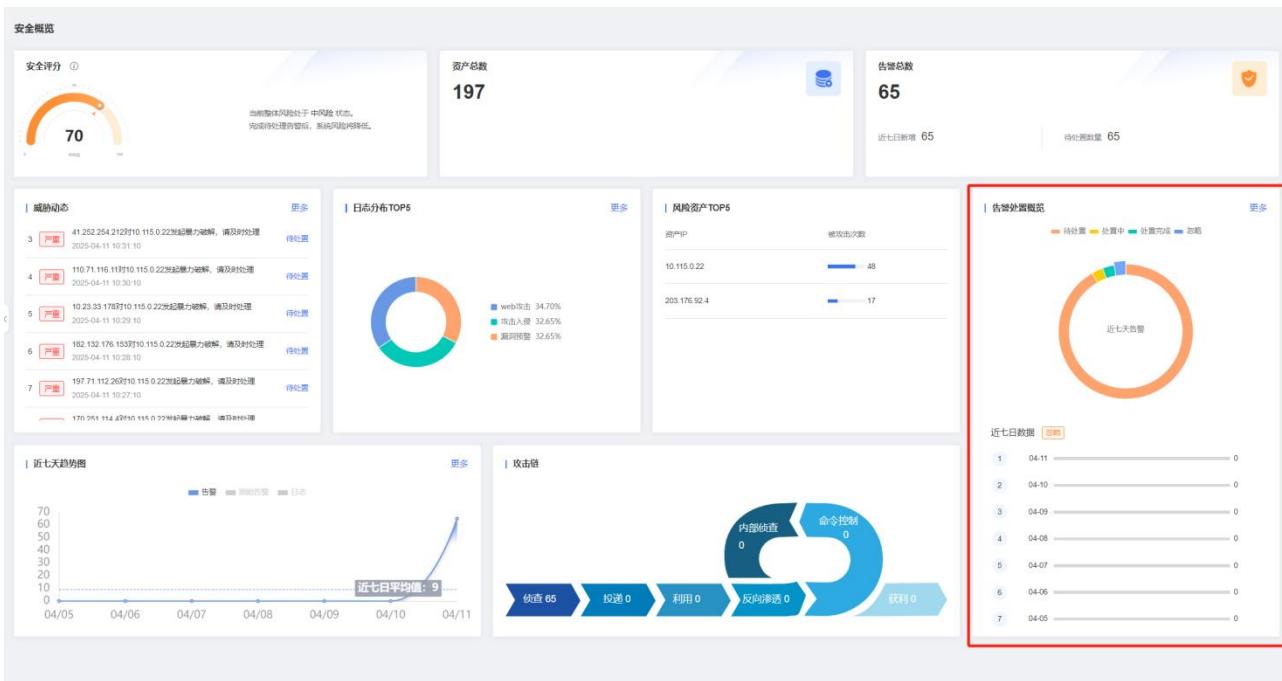
风险资产 TOP5

展示您当前系统中风险最多的 5 个资产信息

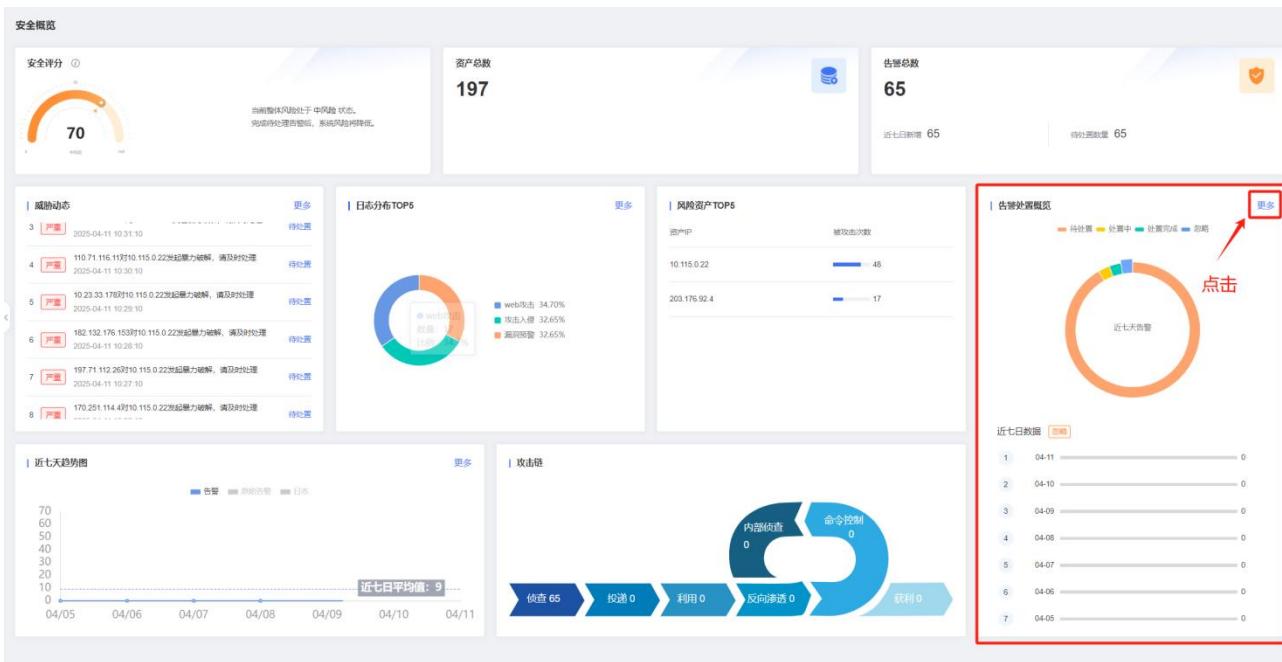


告警处置概览

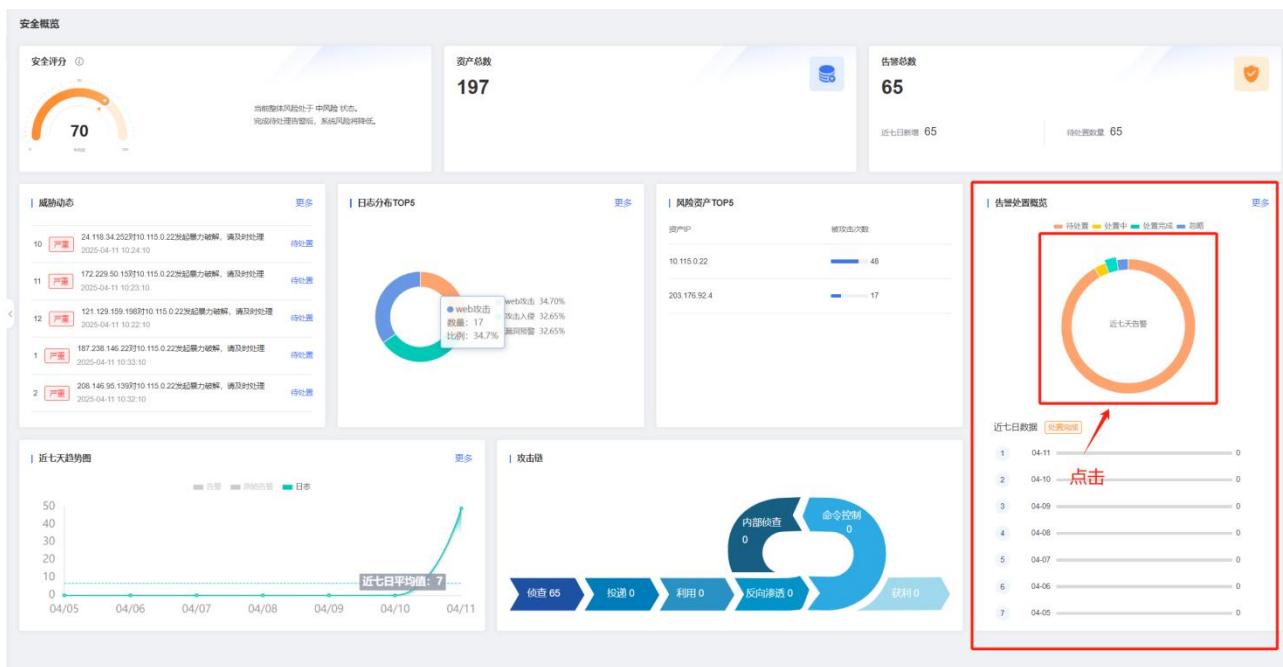
展示近七天的告警处置情况。



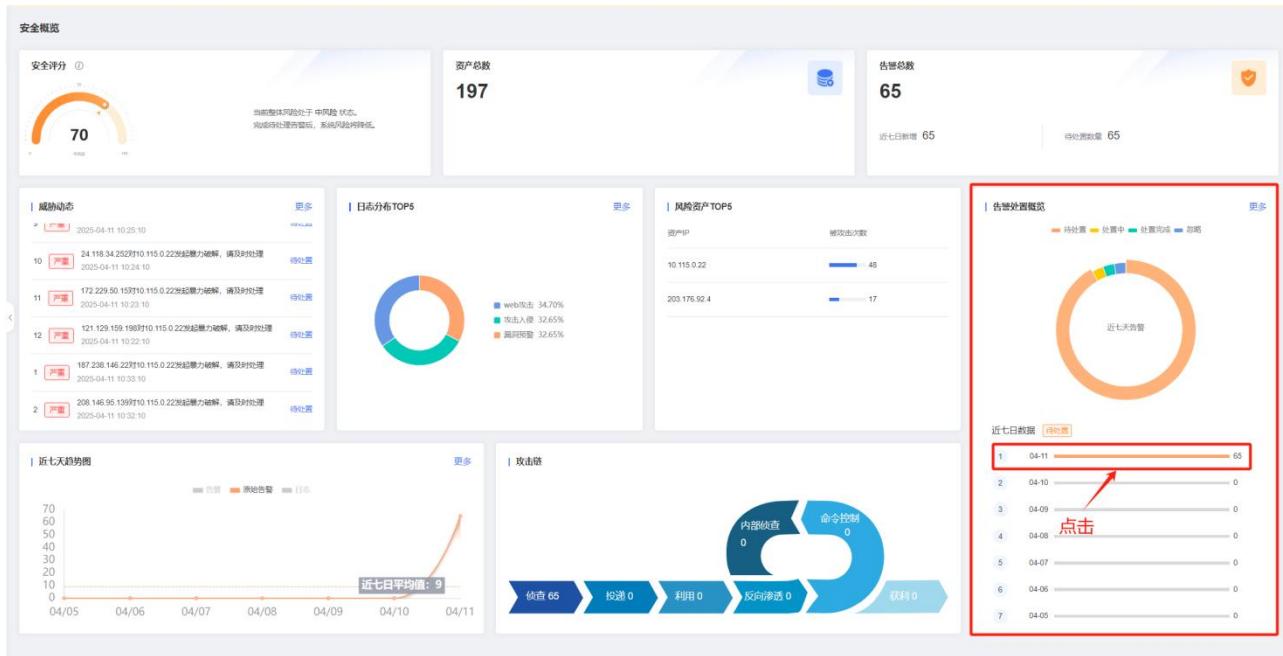
点击更多，支持下钻至告警管理页面



点击饼图，下钻至告警管理并查询对应条件的数据

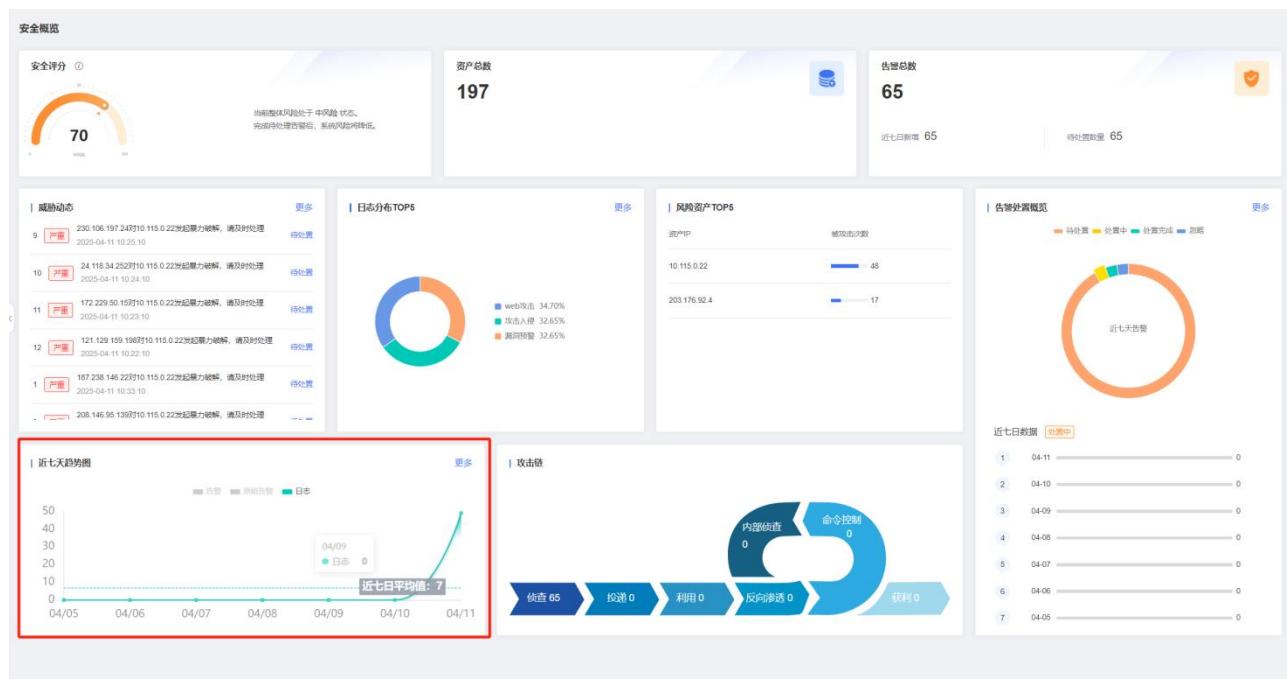


点击 7 日数据中的其中一天，下钻至告警管理，并查询当天的数据

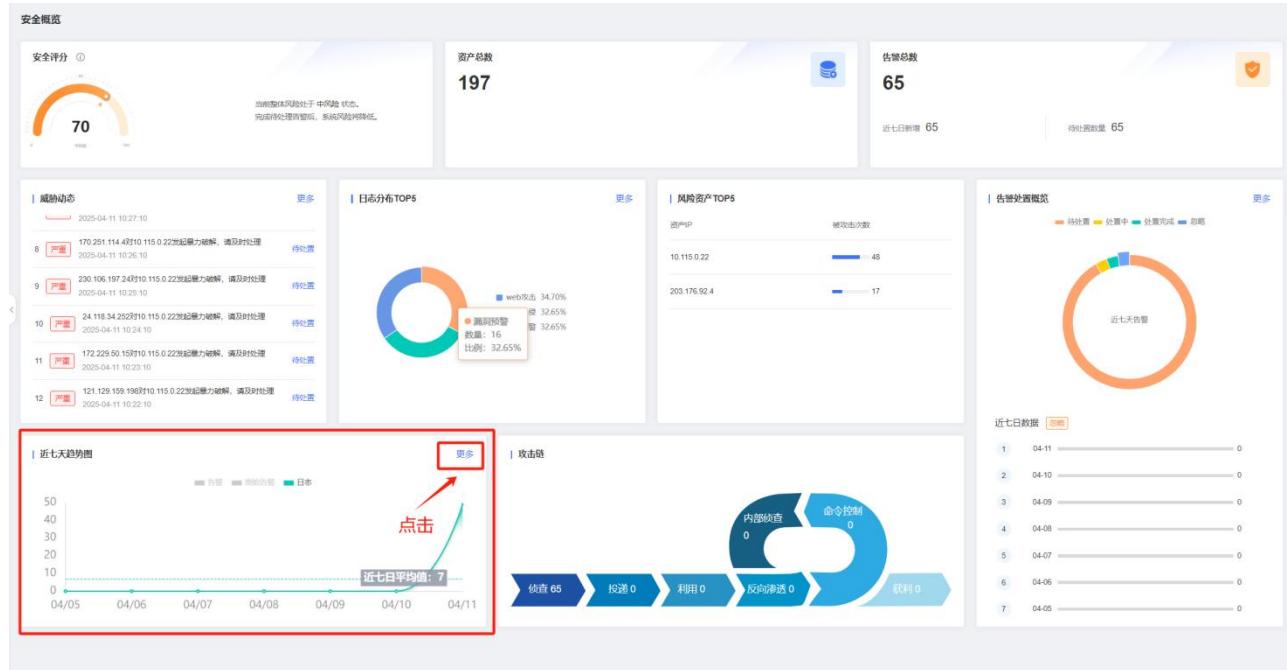


近七天趋势图

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。

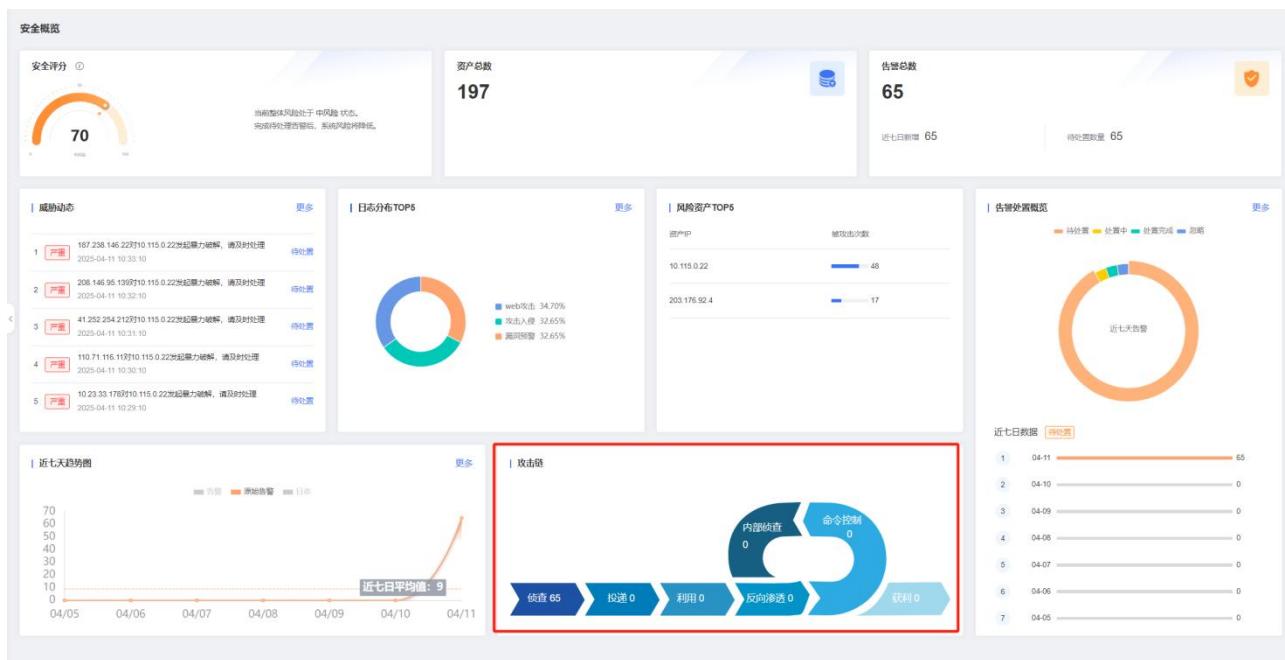


点击更多，下钻至对应的告警管理、告警查询、日志查询页面



攻击链

统计近七天告警阶段的分布情况。



4.1.2. 安全成果展示

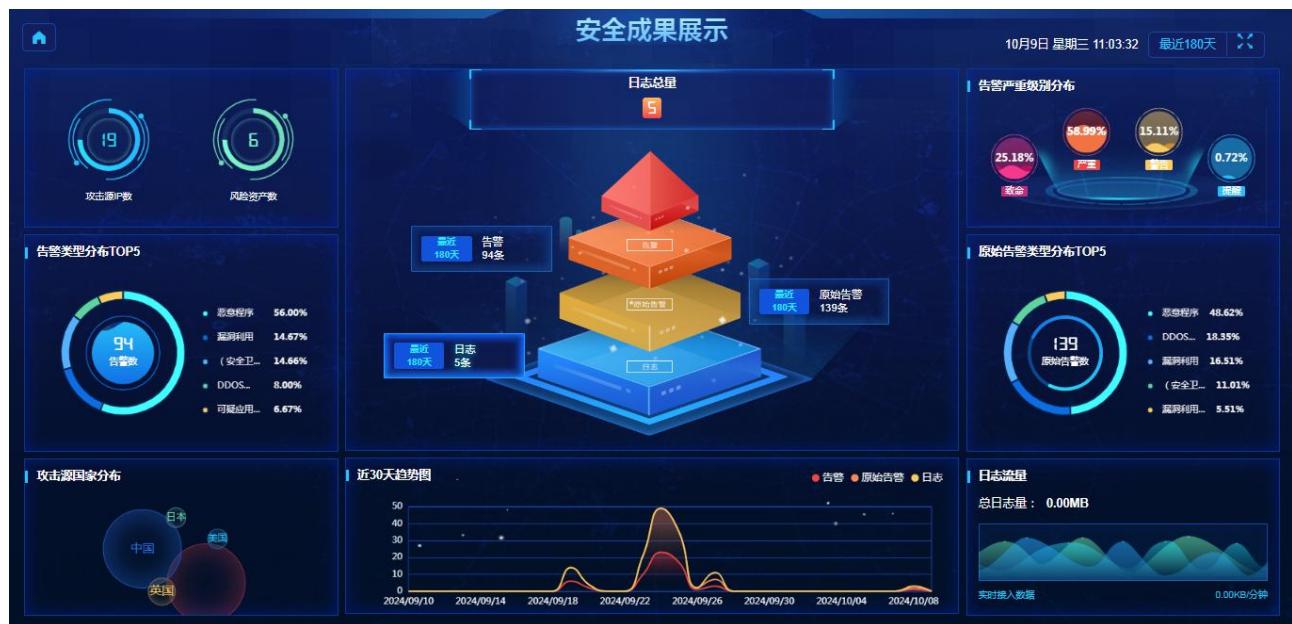
用户从日志接收解析到最终形成告警过程全流程的数据统计。

前提条件

安全成果展示需要购买态势大屏扩展资源，具体操作请参见升级扩容。

查看安全成果展示大屏

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“安全态势 > 安全成果展示”，进入安全成果展示大屏页面。
 - 在右上角支持选择时间范围，也可以设置定时刷新时间。
 - 单击右上角的图标，进入全屏模式。
 - 单击左上角的图标，返回“安全概览”页面。

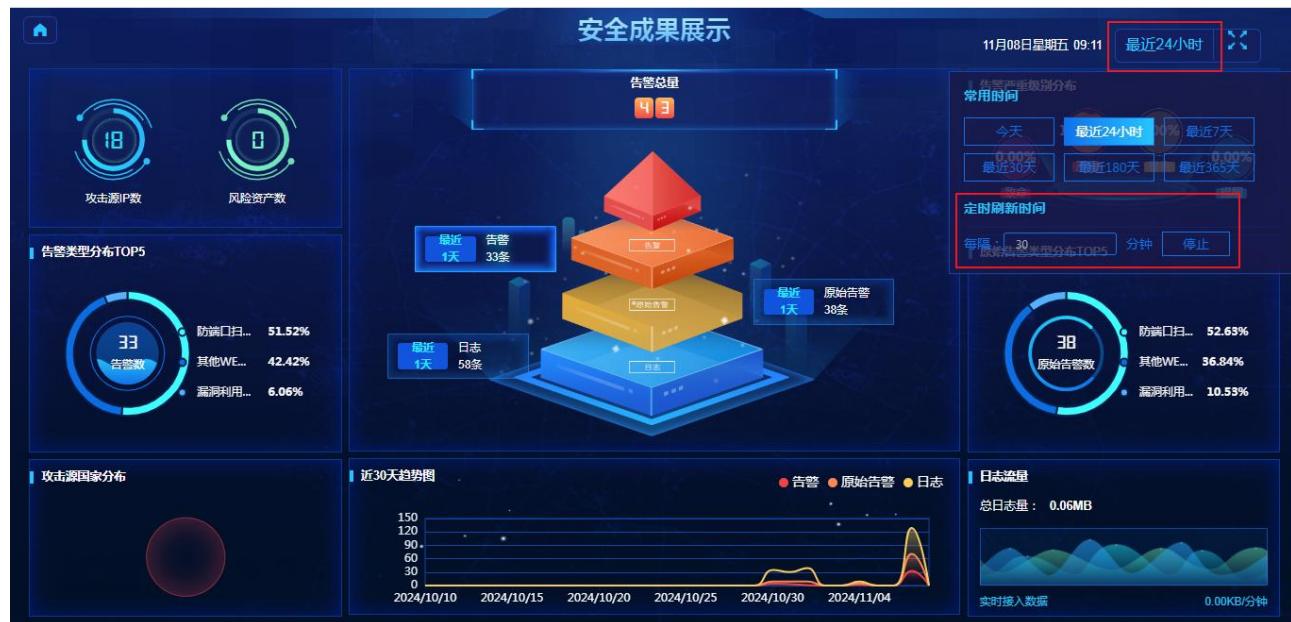


设置定时刷新时间

安全成果展示大屏支持定时刷新大屏数据，定时刷新时间最小为 5 分钟刷新一次，最大为 720 分钟刷新一次，进入大屏默认为 30 分钟刷新一次。

您可以执行以下步骤修改定时刷新时间：

1. 在威胁攻击态势大屏页面，单击右上角时间范围。
2. 单击“停止”，间隔时间变为可配置。配置完时间后，再单击“开始”，即可完成修改。



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。

前提条件

威胁攻击态势需要购买态势大屏扩展资源，具体操作请参见升级扩容。

查看威胁攻击态势大屏

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“安全态势 > 威胁攻击态势”，进入威胁攻击态势大屏页面。
 - 在右上角支持选择时间范围，也可以设置定时刷新时间。

- 单击右上角的图标，进入全屏模式。
- 单击左上角的图标，返回“安全概览”页面。



4. 单击右上角的图标，进入全屏模式。
5. 单击左上角的图标，返回“安全概览”页面。

设置定时刷新时间

威胁攻击态势大屏支持定时刷新大屏数据，定时刷新时间最小为 5 分钟刷新一次，最大为 720 分钟刷新一次，进入大屏默认为 30 分钟刷新一次。

您可以执行以下步骤修改定时刷新时间：

1. 在威胁攻击态势大屏页面，单击右上角时间范围。
2. 单击“停止”，间隔时间变为可配置。配置完时间后，再单击“开始”，即可完成修改。



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。

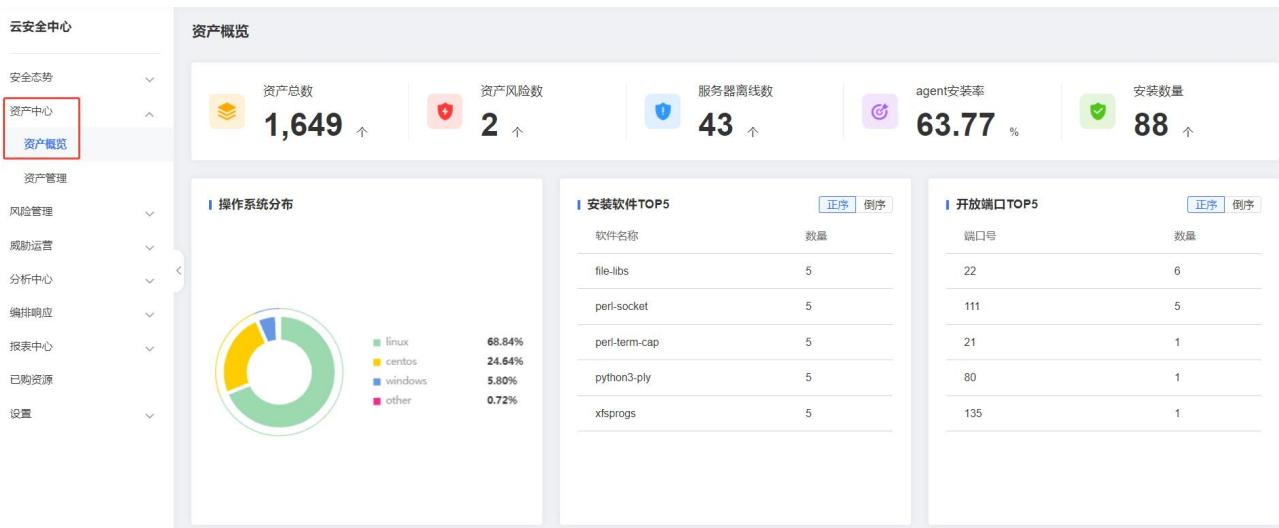
前提条件

- 已开通云安全中心实例。
- 具有云上资产数据。



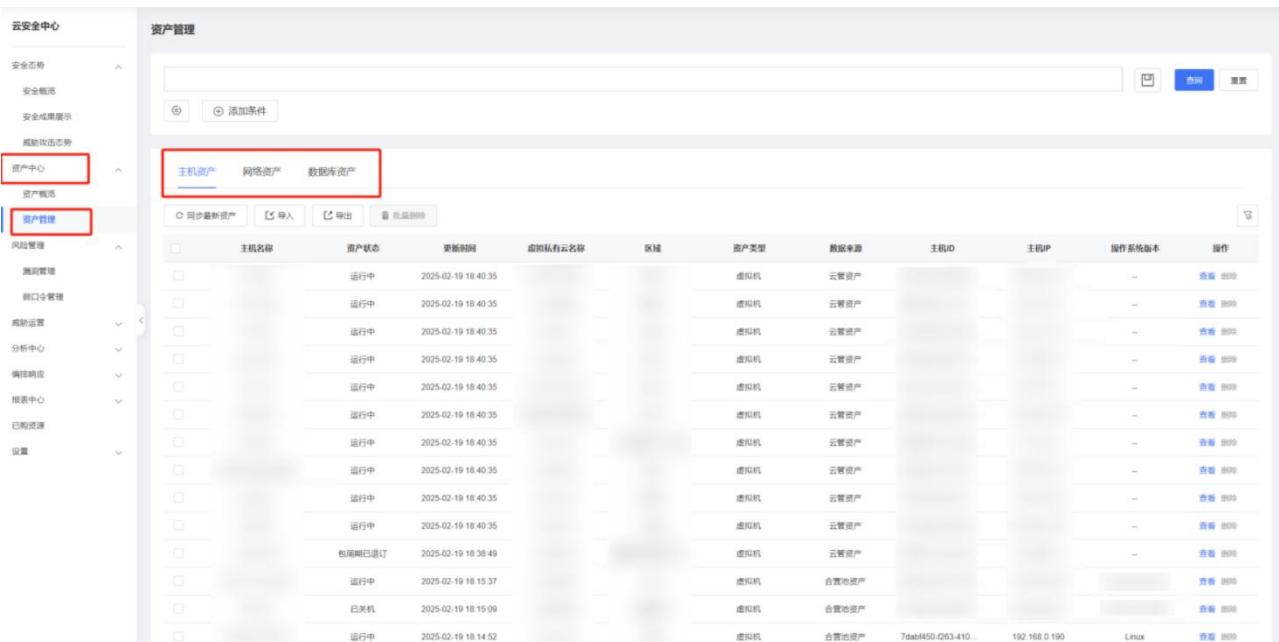
4.2.1. 资产概览

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，操作系统分布，安装软件 TOP 排行（支持倒序和正序），开放端口号 TOP 排行（支持倒序和正序）。



4.2.2. 资产管理

为租户提供主机资产、网络资产、数据库资产及资产属性的查询、资产导入导出以及导入资产的删除功能。



选择常用搜索项查询。



资产管理

主机名称: ecm-loglog2

资产状态: 是否安装安全卫士 主机名称 资产重要性 安全卫士agent是否在线 应用私有云名称 区域 可用区 资产ID 操作系统 操作系统的版本 安全组id 安全组名称

1.点击搜索框
2.点击搜索选项
3.输入搜索条件
4.查询搜索过滤展示

资产状态	是否安装安全卫士	主机名称	云资源创建时间	云资源创建时间	资产ID	可用区	操作系统	操作系统的版本	操作
运行中	已安装	ecm-loglog2	2025-02-19 18:23:29	2024-08-19 18:23:16	1	cn-vincent-1A	centos	centos	查看

共1条 < 1 > 20条/页

查询条件组：保存查询条件，方便用户快速查询。

资产管理

① ② 新加条件

③ ④ 重新查询

1.查询已保存条件
2.新增已保存查询条件

资产状态	是否安装安全卫士	主机名称	云资源创建时间	云资源创建时间	资产ID	可用区	操作系统	操作	
运行中	已安装	ecm-loglog2	2025-02-19 18:23:29	2024-08-19 18:23:16	1	cn-vincent-1A	centos	centos	查看

共1条 < 1 > 20条/页



资产管理

主机名称: * "ecm-loglog" *

添加条件

更新历史

资产状态	是否安装安全卫士
运行中	已安装

保存查询条件组

查询条件组名称: 资产名称:ecm-loglog

描述:

是否保存查询条件: 是否保存查询时间:

取消 保存

账户ID: cn-xinan1-1A 操作系统: centos 操作: 查看

添加条件查询。

资产管理

主机名称: * "ecm-loglog" *

添加条件 1.点击添加条件
2.编写过滤条件

或

更新

资产状态	是否安装安全卫士
运行中	已安装

筛选

主机名称	云资源创建时间	云资源修改时间	账户ID	可用区	操作系统	操作
ecm-loglog2	2023-02-19 18:23:29	2024-08-19 18:23:16	A33F5CDB-5CE9-16F7-94D5-ED397BA0F757	cn-xinan1-1A	centos	查看

共 1 条 < 1 > 20条/页



资产管理

字段筛选：对查询结果栏进行字段的选择和移除

资产安全管理							
资产中心		资产管理					
资产概况		资产列表					
资产管理		资产列表					
风险评估		资产列表					
漏洞管理		资产列表					
弱口令管理		资产列表					
威胁运营		资产列表					
告警概览		资产列表					
告警管理		资产列表					
告警列表		资产列表					
通知管理		资产列表					
威胁检测		资产列表					
分析中心		资产列表					
模型响应		资产列表					
剧本管理		资产列表					
插件管理		资产列表					
规则配置		资产列表					
报表中心		资产列表					
其他功能		资产列表					

更新资产信息

单击“同步最新资产”，获取最新资产状态。



资产管理

⑥ ⑦ 添加条件 查询 重置

主机资产 网络资产 数据库资产

⑧ 同步最新资产 导入 导出 批量删除

资产名称	资产状态	更新时间	虚拟私有云名称	区域	资产类型	数据来源	资产ID	主机IP	操作系统版本	操作
ecm-fnIHuv	运行中	2025-03-02 18:00:00	vpc-hSgk	湖北黄冈一城...	虚拟机	云管资产	4AB08AF6-144...	192.168.1.5	--	查看 删除
ecm-b27f	运行中	2025-03-02 18:00:00	NyuPGotWwJd...	华东1	虚拟机	云管资产	99DDBA72-BC...	192.168.0.9	--	查看 删除

查看资产详情

资产详情包括资产信息和脆弱性信息组成。

资产管理

⑨ 主机名称 - ecm-d409 ⑩ 添加条件 查询 重置

⑪ 更新资产

资产状态	是否安装安全卫士	主机名称	云资源创建时间	云资源更新时间	资产ID	可用区	操作系统	操作
运行中	已安装	ecm-d409	2024-10-20 19:53:33	2024-09-20 19:53:18	...	az2	linux	查看

点击查看，展示资产详情 ⑫ 查看

资产信息展示如下图：

资产详情

资产信息 脆弱性信息

基础信息

基本信息

主机ID: ecm-d409	主机ID: 14...	资产状态: 运行中
操作系统: linux	操作系统: vpc-b	虚拟私有云名称: vpc-b
开放端口: 云资源创建时间: 2024-09-20 19:53:33	云资源更新时间: 2024-09-20 19:53:18	地域: --
可用区: az2	安全组: Default-Security-Group [sg-tm7nrlve1]	

管理属性

是否安装安全卫士: 已安装

安全卫士agent是否在线: 在线

资产重要性: 高级资产

开放端口(3)

端口	协议	监听IP	进程ID
22	tcp	--	1515
111	tcp	0.0.0.0	603
25	tcp	127.0.0.1	1139

网卡信息(1)

网卡名称	mac地址	IPv4	IPv6
...

资产信息展示基础信息的丰富程度和购买的安全产品相关（购买了服务器安全卫士（原生版）或者云等保专区的主机安全产品后其基础信息会更加丰富）。

脆弱性信息如下图：



< 资产详情

资产信息 漏洞性信息

告警

告警(致命数)/已处置数
告警(严重数)/已处置数
告警(告警数)/已处置数
初始告警(置信度数)/已处置数

0 / 0 0 / 0 2 / 0 0 / 0

漏洞扫描结果

漏洞总数
高危漏洞/已处置数
中危漏洞/已处置数
低危漏洞/已处置数
最新发现时间

1477 521 / 0 810 / 0 146 / 0
2024-09-05 11:19:55

基线检测结果

检测不合规数/已处置数
检测合规数
最新发现时间

0 / 0 0 00-00-00 00:00:00
2024-09-05 11:19:55

账号检测结果

账号密码数/已处置数
最新发现时间

0 / 0 00-00-00 00:00:00
00-00-00 00:00:00

资产导入

云安全中心 资产管理

1.选择需要导入的资产类型 主机资产 网络资产 数据库资产

2.点击导入按钮

3.下载导入模板 资产导入模板下载

注意：请参考导入模板字段说明，确保数据正常导入。

4.上传模板文件 选择文件

5.点击导入按钮完成导入 导入

主机ID	主机IP	操作系统版本	操作
2-8364	192.168.1.1	v5.1.0	查看 编辑
E-7100	192.168.1.2	v5.1.0	查看 编辑
虚机1	云管资产	4.0	查看 编辑
虚机2	云管资产	4.0	查看 编辑

资产导出

云安全中心 资产管理

1.选择资产类型 主机资产 网络资产 数据库资产

2.点击导出按钮

提示 确定导出当前查询条件下的资产数据吗？

3.点击确定按钮 确定

主机名称	资产状态	更新时间	虚拟私有云名称	区域	资产类型	数据来源	主机ID	主机IP	操作系统版本	操作
虚机1	运行中	2025-02-19 18:40:35	华东1	虚机	云管资产	...	2-8364	192.168.1.1	v5.1.0	查看 编辑
虚机2	运行中	2025-02-19 18:40:35	华东1	虚机	云管资产	...	E-7100	192.168.1.2	v5.1.0	查看 编辑

导入资产删除

云安全中心 资产管理

1.选择资产类型 主机资产 网络资产 数据库资产

2.点击删除按钮

提示 确定删除【测试主机】吗？

3.点击确定按钮 确定

主机名称	资产状态	更新时间	虚拟私有云名称	区域	资产类型	数据来源	主机ID	主机IP	操作系统版本	操作
虚机1	运行中	2025-02-20 15:33:29	华东1	虚机	导入资产	...	2-8364	192.168.1.1	v5.1.0	查看 编辑
虚机2	运行中	2025-02-19 18:40:35	华东1	虚机	云管资产	...	E-7100	192.168.1.2	v5.1.0	查看 编辑

4.3. 风险管理

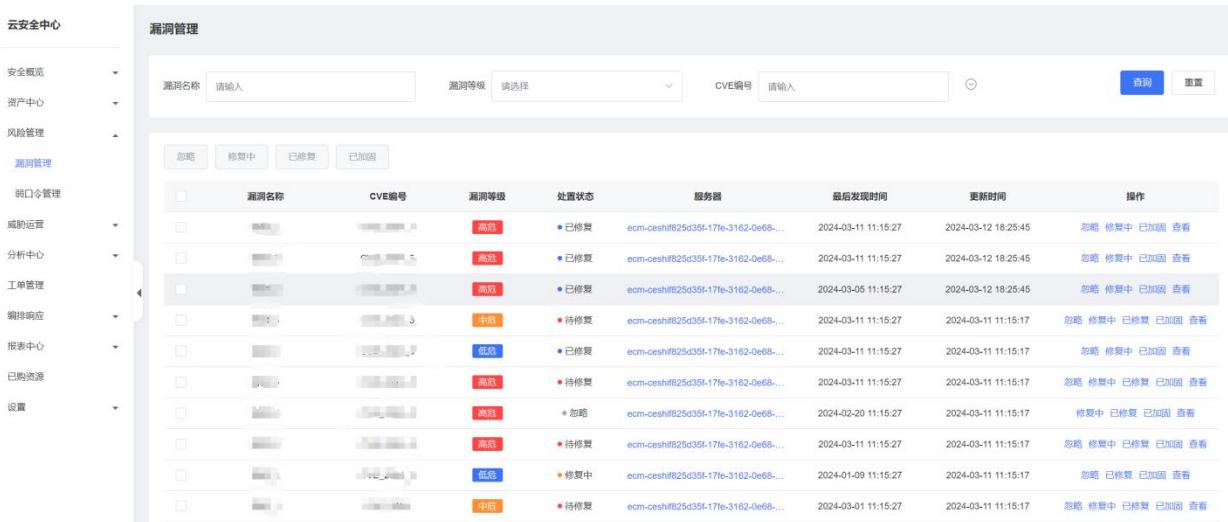
云安全中心风险管理提供给用户漏洞管理和弱口令管理的能力。

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

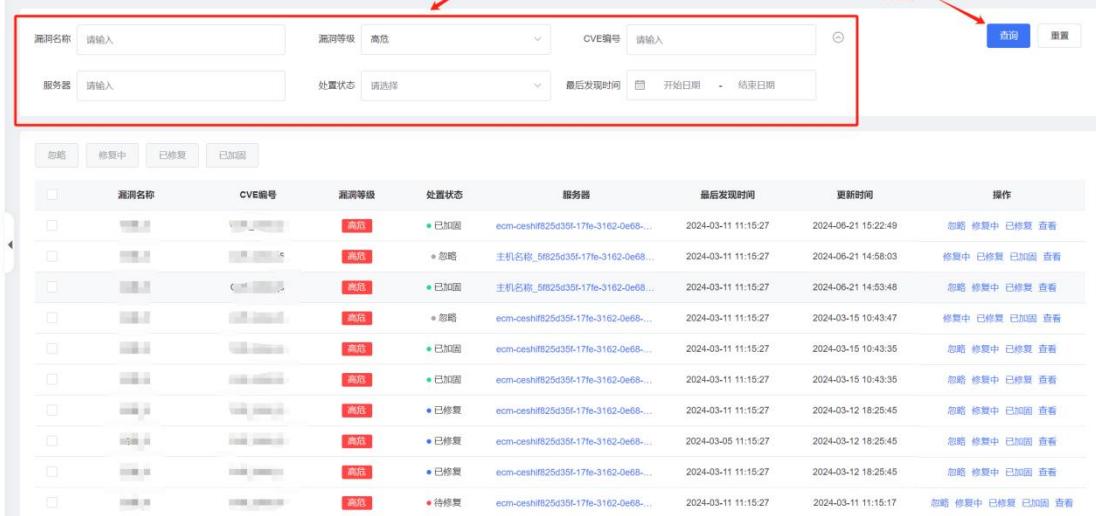
为租户提供漏洞查询及处置功能。



条件查询

支持条件查询，用户输入或选择相关条件内容。

输入或选择相关条件内容
点击

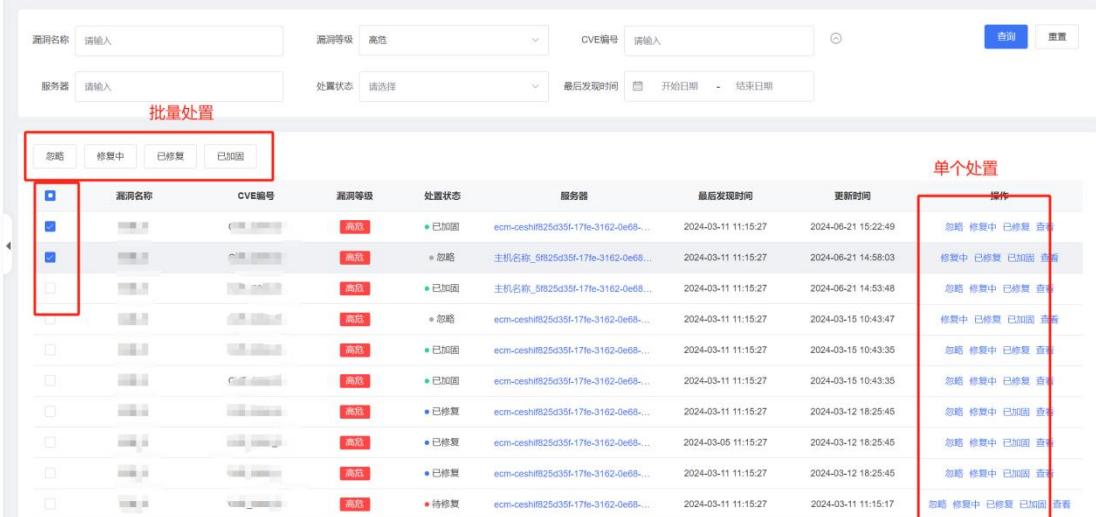


The screenshot shows the 'Vulnerability Management' section of the cloud security center. At the top, there are search fields for '漏洞名称' (Input), '漏洞等级' (High危), 'CVE编号' (Input), and '服务器' (Input). Below these are dropdowns for '处置状态' (Select) and '最后发现时间' (Input). A red box highlights the search area, and two red arrows point to the 'Search' button and the 'List' button. The main area displays a table of vulnerabilities with columns: 漏洞名称 (Name), CVE编号 (ID), 漏洞等级 (Level), 处置状态 (Status), 服务器 (Server), 最后发现时间 (Last Found Time), 更新时间 (Update Time), and 操作 (Operation). The table contains 12 rows of vulnerability data.

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（此处修改漏洞状态仅用于云安全中心展示使用）。

批量处置
单个处置



This screenshot shows the 'Vulnerability Management' interface with a focus on disposition. It includes the same search and filter fields as the previous screen. A red box highlights the 'Batch Disposition' section at the top, which contains buttons for '忽略' (Ignore), '修复中' (In Progress), '已修复' (Fixed), and '已加固' (加固). Below this is a table of vulnerabilities with a red box around the first column containing checkboxes. To the right, a red box highlights the 'Single Disposition' section, which lists individual vulnerability details with a '操作' (Operation) column containing disposition status and notes.

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。



云安全中心 漏洞管理

漏洞 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

操作

	操作	修复中	已修复	已加固	查看
49	忽略	修复中	已修复	查看	
03	修复中	已修复	已加固	查看	
48	忽略	修复中	已修复	查看	
33	忽略	修复中	已修复	查看	
20	忽略	修复中	已修复	已加固	查看

名称_5 CVE_2024_5 高危 忽略 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-15 10:43:47 修复中 已修复 已加固 查看
名称_4 CVE_2024_4 中危 修复中 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-15 10:43:43 忽略 已修复 已加固 查看
名称_5 CVE_2024_5 高危 已加固 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-15 10:43:35 忽略 修复中 已修复 查看
名称_5 CVE_2024_5 低危 已加固 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-15 10:43:35 忽略 修复中 已修复 查看
名称_5 CVE_2024_5 高危 已加固 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-15 10:43:35 忽略 修复中 已修复 查看

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。

云安全中心 漏洞管理

漏洞名称 漏洞等级 CVE编号

操作

点击

操作	忽略	修复中	已修复	已加固
忽略	修复中	已修复	已加固	查看
修复中	已修复	已加固	查看	
已修复	已加固	查看		
已加固	查看			

名称_5 CVE_2024_5 高危 已加固 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-06-21 15:22:49 忽略 修复中 已修复 查看
名称_5 CVE_2024_5 高危 忽略 主机名称_5f825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-06-21 14:58:03 修复中 已修复 已加固 查看
名称_5 CVE_2024_5 高危 已加固 主机名称_5f825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-06-21 14:53:48 忽略 修复中 已修复 查看
名称_5 CVE_2024_5 高危 忽略 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-15 10:43:47 修复中 已修复 已加固 查看
名称_5 CVE_2024_5 高危 已加固 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-15 10:43:35 忽略 修复中 已修复 查看
名称_5 CVE_2024_5 高危 已加固 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-15 10:43:35 忽略 修复中 已修复 查看
名称_5 CVE_2024_5 高危 已修复 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-12 18:25:45 忽略 修复中 已加固 查看
名称_5 CVE_2024_5 高危 已修复 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-05 11:15:27 2024-03-12 18:25:45 忽略 修复中 已加固 查看
名称_2 CVE_2024_1 高危 已修复 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.2 2024-03-11 11:15:27 2024-03-12 18:25:45 忽略 修复中 已加固 查看
名称_5 CVE_2024_5 高危 待修复 ecm-ceshif825d35f-17fe-3162-0e68-d10676d09b781.1.1.5 2024-03-11 11:15:27 2024-03-11 11:15:17 忽略 修复中 已修复 已加固 查看

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
超级管理员	已修复	22222	2024-03-12 18:25:45
超级管理员	修复中	11111	2024-03-12 18:25:36
超级管理员	已修复	批量测试修复中	2024-03-12 17:29:17
超级管理员	已修复	批量测试修复中	2024-03-12 17:28:07
超级管理员	修复中	批量处置修复中	2024-03-12 17:27:42
超级管理员	忽略		2024-03-12 17:26:25

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。



云安全中心

漏洞管理

漏洞名称: 请输入 漏洞等级: 高危 CVE编号: 请输入

操作: 查询 重置

弱口令管理

忽略 修复中 已修复 已加固

服务器	最后发现时间	更新时间	操作
ecm-ceshi825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 查看
主机名称_5fb25d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-06-21 14:58:03	修复中 已修复 已加固 查看
主机名称_5fb25d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 查看
ecm-ceshi825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 查看
ecm-ceshi825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
ecm-ceshi825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
ecm-ceshi825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
ecm-ceshi825d35f-17fe-3162-0e68-...	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
ecm-ceshi825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
ecm-ceshi825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看

点击

云安全中心

资产详情

资产信息 脆弱性信息

基础信息 基本信息

主机名称: ecm-ceshi 主机ID: ab9fbaf6-76d2-4eeb-b021-a753aaadedfe6
操作系统: linux 操作系统版本: 虚拟机有云名称: vpc-ceshi-ceshi
云资源创建时间: 2024-06-18 01:04:30 云资源别名时间: 2024-07-18 01:05:37
可用区: default 地域:

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 已购资源 设置

4.3.2. 弱口令管理

为租户提供弱口令查询及处置功能。

云安全中心

弱口令管理

应用名称: 请输入 服务器: 请输入 处置状态: 待修复

操作: 查询 重置

弱口令管理

忽略 修复中 已修复 已加固

服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作
系统弱口令	应用名称_1	123456	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看		
系统弱口令	应用名称_1	123456	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看		
系统弱口令	应用名称_1	123456	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看		
系统弱口令	应用名称_1	123456	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看		

条件查询



云安全中心

弱口令管理

输入或选择相关条件内容 点击

查询 重置

服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作
ecm-ceshi#825d35f-17fe-316...		系统弱口令	123456	应用名称_1	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
ecm-ceshi#825d35f-17fe-316...		系统弱口令	123456	应用名称_1	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
ecm-ceshi#825d35f-17fe-316...		系统弱口令	123456	应用名称_1	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
ecm-ceshi#825d35f-17fe-316...		系统弱口令	123456	应用名称_1	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看

处置弱口令

提供处置能力，可直接或批量修改弱口令处置状态。状态枚举值：修复中、已修复、忽略、已加固等（此处修改弱口令状态仅用于云安全中心展示使用）。

云安全中心

弱口令管理

批量处置

单个处置

服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作
ecm-ceshi#825d35f-17fe-316...		系统弱口令	123456	应用名称_1	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
ecm-ceshi#825d35f-17fe-316...		系统弱口令	123456	应用名称_1	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
ecm-ceshi#825d35f-17fe-316...		系统弱口令	123456	应用名称_1	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看
ecm-ceshi#825d35f-17fe-316...		系统弱口令	123456	应用名称_1	待修复	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 修复中 已修复 已加固 查看

修改处置状态可填写状态变更原因。

标记为修复中

确认要把该弱口令标记为修复中吗？

用户名	口令类型	密码值	应用名称	影响服务器
系统弱口令	*****88*****		Redis	null6AEFBFA3-7ED3-A524-5B50-1085EB28C...

处置说明

最多可输入255个字符

取消 保存

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。

服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作
ecm-ceshi825d35f-17fe-316...	系统弱口令	123456	应用名称_1	已加固	2024-03-11 11:15:27	2024-06-21 16:12:01	忽略 修复中 已修复 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	123456	应用名称_1	已加固	2024-03-11 11:15:27	2024-06-21 16:11:51	忽略 修复中 已修复 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	*****88*****	Redis	修复中	2023-12-01 17:29:59	2024-06-21 16:04:55	忽略 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	*****88*****	Redis	已修复	2023-12-01 17:29:59	2024-06-21 16:03:39	忽略 修复中 已修复 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	123456	应用名称_wesdf	已加固	2024-03-11 11:15:27	2024-06-21 16:03:31	忽略 修复中 已修复 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	*****88*****	Redis	已加固	2023-12-01 17:29:59	2024-03-13 14:57:43	忽略 修复中 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	应用弱口令	123456	应用名称_1	忽略	2024-03-11 11:15:27	2024-03-13 09:51:11	修复中 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	应用弱口令	123456	应用名称_3333	修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	应用弱口令	123456	应用名称_2222	修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	123456	应用名称_1	修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查看	

处置人	处置状态	处置说明	处置时间
ctyunsectest3@chinatelecom.cn	已加固	test	2024-06-21 16:12:01

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。

服务器	用户名	口令类型	密码值	应用名称	处置状态	最后发现时间	更新时间	操作
ecm-ceshi825d35f-17fe-316...	系统弱口令	123456	应用名称_1	已加固	2024-03-11 11:15:27	2024-06-21 16:12:01	忽略 修复中 已修复 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	123456	应用名称_1	已加固	2024-03-11 11:15:27	2024-06-21 16:11:51	忽略 修复中 已修复 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	*****88*****	Redis	修复中	2023-12-01 17:29:59	2024-06-21 16:04:55	忽略 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	*****88*****	Redis	已修复	2023-12-01 17:29:59	2024-06-21 16:03:39	忽略 修复中 已加固 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	123456	应用名称_wesdf	已加固	2024-03-11 11:15:27	2024-06-21 16:03:31	忽略 修复中 已修复 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	*****88*****	Redis	已加固	2023-12-01 17:29:59	2024-03-13 14:57:43	忽略 修复中 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	应用弱口令	123456	应用名称_1	忽略	2024-03-11 11:15:27	2024-03-13 09:51:11	修复中 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	应用弱口令	123456	应用名称_3333	修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	应用弱口令	123456	应用名称_2222	修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查看	
ecm-ceshi825d35f-17fe-316...	系统弱口令	123456	应用名称_1	修复中	2024-03-11 11:15:27	2024-01-09 11:15:17	忽略 已修复 已加固 查看	



云安全中心

资产详情

资产信息 脆弱性信息

基础信息

基本信息

主机名称: ecm-ceshi	主机ID: ab9fbafe-76d2-4eef-b021-b753aaadedfe6	资产状态: 运行中
操作系统: linux	操作系统版本:	虚拟私有云名称: vpc-osm-ceshi
云资源创建时间: 2024-06-18 01:04:30	云资源到期时间: 2024-07-18 01:05:37	地域:
可用区: default		

4.4. 威胁运营

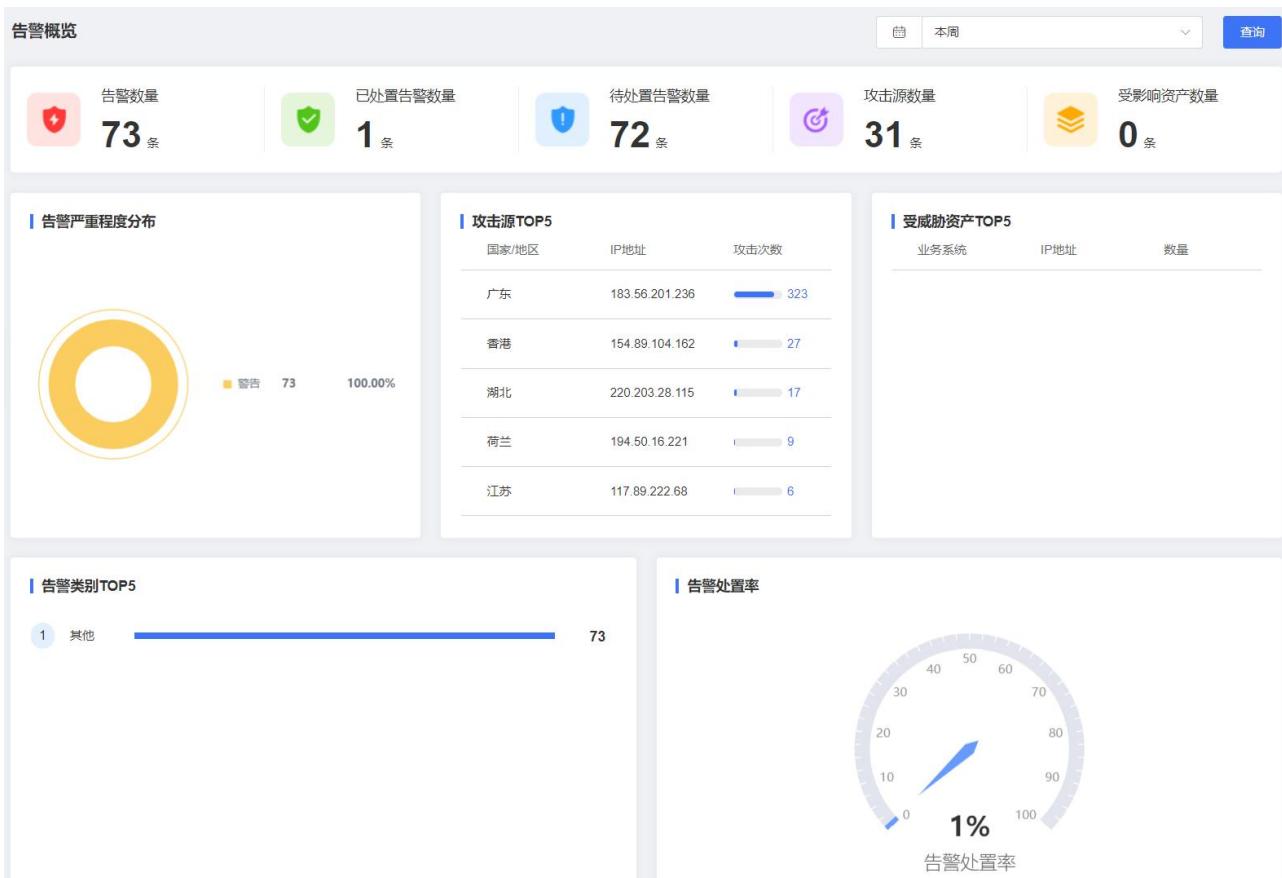
为了便于用户对平台告警数据进行整理分析与管理，威胁运营提供告警概览、告警管理、告警列表、通知管理和威胁检测等功能。

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 以及告警处置率等指标展现。



4.4.2. 告警列表

为用户提供查询、解决建议、处置威胁等功能

云安全中心 告警管理

TQL: 最近7天 搜索 高级

数据总量: 48

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

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
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	待处置	XDR_WAF事件	待处置	1	①	
致命	111.7.124.32对172.17.1.2触发...	111.7.124.32	172.17.1.2	待处置	XDR_WAF事件	待处置	1	①	
致命	111.7.124.31对172.17.1.2触发...	111.7.124.31	172.17.1.2	待处置	XDR_WAF事件	待处置	1	①	
致命	111.7.122.34对172.17.1.2触发...	111.7.122.34	172.17.1.2	待处置	XDR_WAF事件	待处置	1	①	

Detailed description: This screenshot shows the 'Alarm Management' section of the cloud security center. On the left is a sidebar with various management options. The main area features a timeline chart showing the volume of alarms over time. Below the chart is a table listing specific alarms, each with details such as source and destination IP addresses, current status (e.g., '待处置' - pending handling), and a handle icon.

TQL 条件查询

TQL | 源IP sro_address ← 选择查询字段

目的IP	dst_address
威胁类型	threat_category
源端口	sro_port
有效告警名称	alarm_name
攻击IP数	attack_ip_num
公有云租户ID	account_id
安全服务编号	service_code
攻击次数	attack_times
111.0.124.30对172.17.1.2触发...	111.0.124.30
112.81.132.35对172.17.1.2触...	112.81.132.35
112.81.132.45对172.17.1.2触...	112.81.132.45
111.7.124.32对172.17.1.2触发...	111.7.124.32
111.7.124.31对172.17.1.2触发...	111.7.124.31
111.7.122.34对172.17.1.2触发...	111.7.122.34
112.81.132.35对172.17.1.2触...	112.81.132.35
111.7.122.35对172.17.1.2触发...	111.7.122.35

时间轴：2024-05-25 到 2024-05-27

告警状态	告警次数	操作
待处置	3	①
待处置	2	②
待处置	2	③
待处置	1	④
待处置	1	⑤
待处置	1	⑥
待处置	1	⑦

TQL | 源IP like 模糊匹配 ← 选择查询条件

not like	排除模糊匹配
=	等于
!=	不等于
>	大于
<	小于
>=	大于等于
<=	小于等于
in	包含
not in	不包含
exist	存在
not exist	不存在
111.7.124.32对172.17.1.2触发...	111.7.124.32
111.7.124.31对172.17.1.2触发...	111.7.124.31
111.7.122.34对172.17.1.2触发...	111.7.122.34
112.81.132.35对172.17.1.2触...	112.81.132.35
111.7.122.35对172.17.1.2触发...	111.7.122.35

时间轴：2024-05-25 到 2024-05-27

告警状态	告警次数	操作
待处置	3	①
待处置	2	②
待处置	2	③
待处置	1	④
待处置	1	⑤
待处置	1	⑥
待处置	1	⑦

输入查询内容

TQL | 源IP like 111.7.132.35

最近7天

高级

数据总量: 5

1

0

2024-05-21 2024-05-22 2024-05-23 2024-05-25 2024-05-27

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
致命	111.7.132.35对172.17.1.2触发...	111.7.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	3	
致命	111.7.132.35对172.17.1.2触发...	111.7.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	3	
致命	111.7.132.35对172.17.1.2触发...	111.7.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	1	
提醒	111.7.132.35对172.17.1.2触发...	111.7.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	1	
提醒	111.7.132.35对172.17.1.2触发...	111.7.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	1	

共 5 条 20条/页 < 1 > 前往 1 页

点击

TQL | 源IP like 111.7.124.33

2024-05-01 00:00:00~2024-05-18 00:00:00

高级

数据总量: 4

1

0

2024-05-21 2024-05-22 2024-05-25 2024-05-27

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
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	待查	XDR_WAF事件		待处置	1	
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	待查	XDR_WAF事件		待处置	1	
提醒	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	待查	XDR_WAF事件		待处置	1	
提醒	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	待查	XDR_WAF事件		处置中	1	

共 4 条 20条/页 < 1 > 前往 1 页

选择常用时间查询



选择时间范围（最大查询时间窗口为 30 天）

TQL ① 源IP like 111.7.124.33

2024-05-01 00:00:00~2024-05-18 00:00:00

查询 高级

数据总量: 4

1

0

2024-05-21 2024-05-22 2024-05-25 2024-05-27

常用时间

今天 最近7天 最近30天 全部

从 ② 开始日期 至 结束日期

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
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	③	XDR_WAP事件	待处置	1	④	
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	③	XDR_WAP事件	待处置	1	④	
提醒	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	③	XDR_WAP事件	待处置	1	④	
提醒	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	③	XDR_WAP事件	处置中	1	④	

TQL 滤IP like 111.7.124.33

2024-05-01 00:00:00~2024-06-18 00:00:00

常用时间
今天 最近7天 最近30天 全部

从 开始日期 到 结束日期

数据总量: 4

严重等级	有效告警名称	源IP	目的
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.
堵塞	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.
堵塞	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.

2024-05-21 2024-05-23

2024年5月 2024年6月

日	一	二	三	四	五	六	日	一	二	三	四	五	六
28	29	30	1	2	3	4	26	27	28	29	30	31	1
5	6	7	8	9	10	11	2	3	4	5	6	7	8
12	13	14	15	16	17	18	9	10	11	12	13	14	15
19	20	21	22	23	24	25	16	17	18	19	20	21	22
26	27	28	29	30	31	1	23	24	25	26	27	28	29
2	3	4	5	6	7	8	30	1	2	3	4	5	6

选择时间范围

清空 确定

点击前往 1 / 页



查询条件组

保存查询条件，方便用户查询（保存的查询条件最多为 10 个）

The screenshot shows a search interface with the following details:

- TQL: 源IP like 111.7.124.33
- Date Range: 2024-05-08 00:00:00~2024-05-23 00:00:00
- Data Count: 2
- Log Entries:

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
低级	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	低级	XDR_WAF事件		待处置	1	①
低级	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	低级	XDR_WAF事件		处置中	1	②

- Pagination: 共 2 条 20条/页 < 1 > 前往 1 页

The screenshot shows the same search interface with the following changes:

- A message at the top right says "已保存查询条件组" (Query condition group saved).
- A message below it says "您可以新增查询条件组，以便下次快速查询" (You can add a new query condition group for quick querying next time).
- A red arrow points to the "新增" (Add) button.
- The log entries remain the same as the previous screenshot.
- Pagination: 共 2 条 20条/页 < 1 > 前往 1 页

The dialog box contains the following fields:

- 查询条件组名称: test
- 描述: (empty text area)
- 是否保存查询条件:
- 是否保存查询时间:
- 输入和选择对应条件 (Input and select corresponding conditions): (text area)
- Buttons: 取消 (Cancel) and 保存 (Save) with a red arrow pointing to it.



TQL 源IP like 111.7.124.33

已保存查询条件组 点击

数据总量: 1

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
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	生成	XDR_WAF事件		待处置	1	①

共 1 条 20条/页 < 1 > 前往 1 页

查看与选择历史查询记录

历史记录最多保存 50 条

TQL 处置状态 = 忽略

点击

数据总量 0

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
无数据									

共 0 条 20条/页 < 1 > 前往 1 页

TQL 处置状态 = 忽略

点击

数据总量 0

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
无数据									

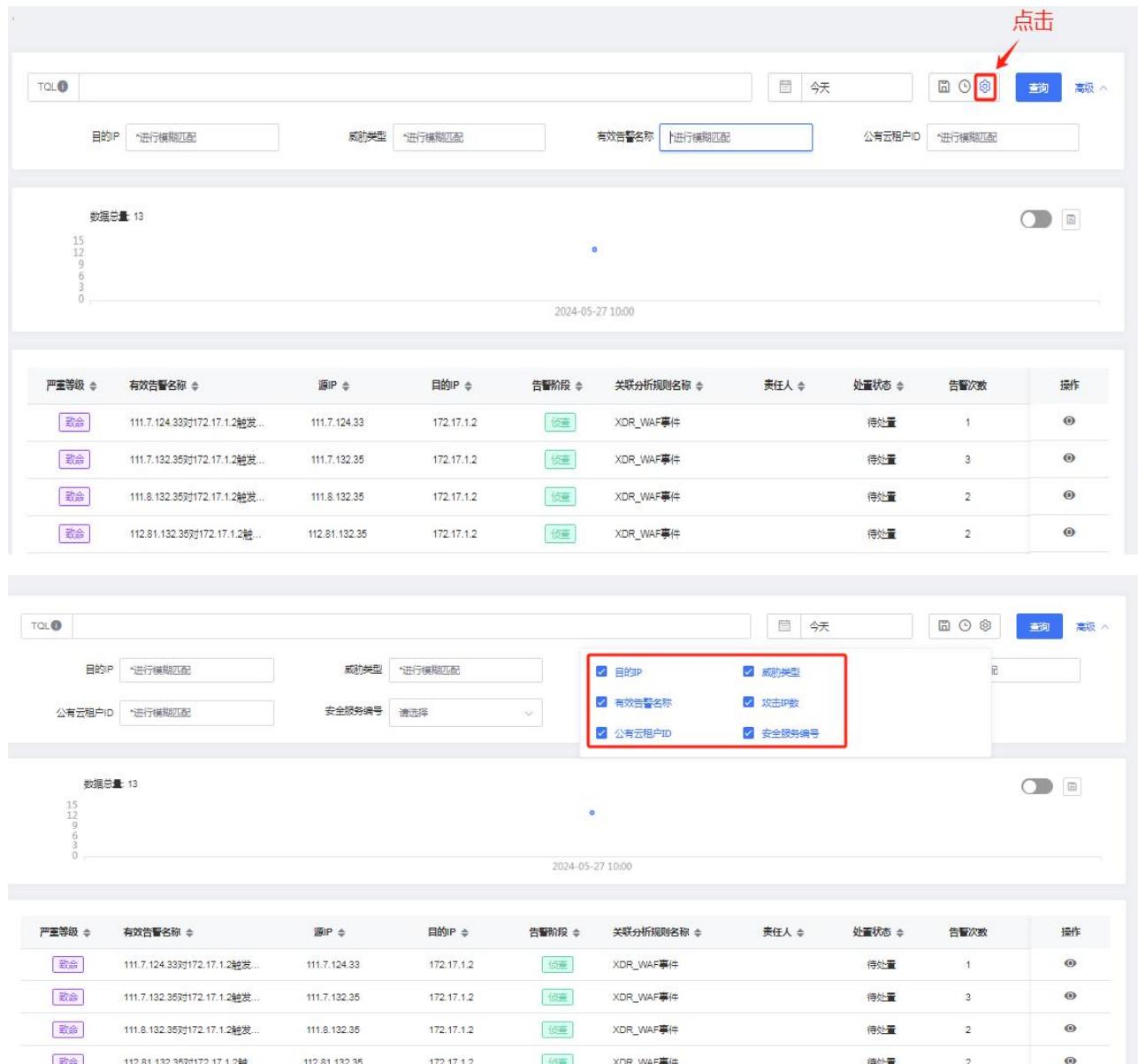
查询条件

查询条件	查询时间
处置状态 = 忽略	2024-05-27 15:51:59
源IP like 111.7.124.33	2024-05-27 15:51:57
事件确认状态 = “攻击未成功” and 严重等级 = “警告” and 处置状态 != “忽略”	2024-05-27 15:51:54
源IP like 111.7.132.35	2024-05-27 15:22:35
源IP != 111.7.124.33	2024-05-27 15:19:47
处置状态 != “忽略” and 事件确认状态 != “误报”	2024-05-23 17:42:32
源IP国家 = “中国” and 确认状态 != “误报” and 处置状态 != “忽略”	2024-05-08 10:15:31
处置状态 = 待处置	2024-05-07 17:36:07

< 1 > 前往 1 页

快速查询条件

使用模糊查询时需要带*



The screenshot shows two identical search interfaces for security alerts. The top interface has a red arrow pointing to the 'Search' button, with the text '点击' (Click) above it. The bottom interface has a red box highlighting several search filters: '目的IP' (Destination IP), '威胁类型' (Threat Type), '有效告警名称' (Effective Alert Name), and '公有云租户ID' (Public Cloud Tenant ID). All these fields contain the placeholder text '*进行模糊匹配' (Perform fuzzy matching).

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
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	待查	XDR_WAF事件		待处置	1	
致命	111.7.132.35对172.17.1.2触发...	111.7.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	3	
致命	111.8.132.35对172.17.1.2触发...	111.8.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	2	
致命	112.81.132.35对172.17.1.2触...	112.81.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	2	

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
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	待查	XDR_WAF事件		待处置	1	
致命	111.7.132.35对172.17.1.2触发...	111.7.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	3	
致命	111.8.132.35对172.17.1.2触发...	111.8.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	2	
致命	112.81.132.35对172.17.1.2触...	112.81.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	2	

查看告警详情

TQL 源IP like 111.7.124.33

目的IP ~进行模糊匹配 威胁类型 ~进行模糊匹配 有效告警名称 ~进行模糊匹配 公有云租户ID ~进行模糊匹配

最近7天

数据总量: 45

2024-05-21 2024-05-22 2024-05-23 2024-05-24 2024-05-25 2024-05-26 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
致命	111.7.124.33对172.17.1.2触发...	111.7.124.33	172.17.1.2	待查	XDR_WAF事件		待处置	1	
致命	111.7.132.35对172.17.1.2触发...	111.7.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	3	
致命	111.8.132.35对172.17.1.2触发...	111.8.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	2	
致命	112.81.132.35对172.17.1.2触...	112.81.132.35	172.17.1.2	待查	XDR_WAF事件		待处置	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: 级别管理员

处置状态: 待处置 处置中 处置完成 忽略

处置状态

详细 操作记录

源IP	111.7.124.33 中国河南洛阳 (115.07446/35.77736) (移动)
目的IP	172.17.1.2
告警阶段	侦查
告警级别	致命
部门ID	3
关联分析规则名称	XDR_WAF事件

产生告警的详细内容

源IP地址	111.7.124.33 中国河南洛阳 (115.07446/35.77736) (移动)
目的IP地址	172.17.1.2
告警级别	致命
告警创建时间	2024-05-25 04:38:20
告警结束时间	2024-05-21 16:50:34
规则名称	XDR_WAF事件
部门ID	3

原始日志: WAF告警事件-ATTACK

原始日志的内容

1 2 3 4 ... 11 > 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(内网)	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	27618268ad774c5e8ca87f04df86030a	部门ID	3
威胁类型	ATTACK		

五元组

源IP地址	111.7.124.33 中国河南洛阳 (115.07446/35.77736) (移动)
目的IP地址	172.17.1.2
目的端口	443

4.4.3. 告警管理

告警管理是为了便于对告警的统一管理、处置与后续分析。告警管理用于告警的统一管理，进行告警的处置。

告警管理界面可以很详细地看到告警的基本属性，以及告警的处置情况，告警管理界面可以以告警编号、告警名称、告警分类、告警级别、告警工单状态、告警来源及时间段查询指定的告警工单。

前提条件

已开通云安全中心实例。

查看告警详情

在告警管理中，点击告警名。

进入告警处置页面，可以看到告警相关详细信息。



源IP	192.168.0.4		
目的IP	106.40.51.168 中国/内蒙古/ (118.719421/45.383339) (电信)		
告警阶段	侦查	告警ID	00a92fd1-4506-4c96-b3b9-fcd2e63371c4
告警规则类型名称	其他	告警级别	警告
关联分析规则名称	服务器安全卫士 (原生版) _漏洞扫描		

^ 原始告警: 192.168.0.4对106.40.51.168触发告警

处置告警



在告警详情界面，点击“处置”。

告警 关联告警

192.168.0.4对106.40.51.168触发告警 【08-15 15:37:40~08-15 15:37:45】 警告

源IP	192.168.0.4		
目的IP	106.40.51.168 中国/内蒙古/ (118.719421/45.383339) (电信)		
告警阶段	侦查	告警ID	00a92fd1-4506-4c96-b3b9-fcd2e63371c4
告警规则类型名称	其他	告警级别	警告
关联分析规则名称	服务器安全卫士 (原生版) _漏洞扫描		

^ 原始告警: 192.168.0.4对106.40.51.168触发告警

进入处置界面，可以选择处置剧本、处置时限。

< 工单处置

告警 处置 关联告警

机器【5...】发现暴力破解问题，对1...进行暴力破解行为，请及时处理！

攻击阶段：【侦查】 发生时间：2024-09-05 12:04:08 外部威胁IP： 处置建议：

* 处置剧本选择

剧本名称	场景名称
云服务器 - 安全加固_提权	日常运营
...	日常运营
...	日常运营
...	日常运营

* SLA(处置时间) 1天12小时

④ 启动

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。

告警 处置 作战室 实战剧本 关联事件 小结

111.7.106.97对172.17.0.2触发告警，攻击类型为XSS攻击 责任人修改

攻击阶段：【侦查】 发生时间：2024-06-30 09:06:01 外部威胁IP： 影响资产：

完成时限：2024-06-30 21:12:43 处置建议：

工单处置

用户节点
处置意见
test
当期剩余：1天0小时10分钟
4/255

终止执行 确定

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。



工单处置

告警 处置 作战室 实战剧本 关联事件 小结

请输入名称 搜索

发送短信 - 公有云 Soar 短信通知插件.发送短信

2024-05-31 09:32:57

输入 输出 Log

系统插件 系统工具

公有云 Soar 短信通知插件 v1.0.0

发送短信 run

accountId: 2781828ad774c5e0ca87734df86030a
phoneNumber: 18390991210
message: 测试消息11111111111111111111111111
type: 短信通知
userId:

告警处置完成之后，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。

工单处置

告警 处置 作战室 实战剧本 关联事件 小结

事件小结

B I U S " " Hs Hz 三 三 x² 三 三 Normal Normal A 圆 Sans Serif

请输入小结内容，大小不能超过2M

点击上传文件 只能上传jpg,gif,png,doc,xls,ppt,zip,json,docx,xlsx,pptx,txt文件,且不超过5M

重置 保存

4.4.4. 通知管理

4.4.4.1. 通知规则

- #### 创建通知规则
1. 登录云安全中心控制台。
 2. 在左侧导航栏选择“威胁运营 > 通知管理 > 通知规则”，进入通知规则页面。
 3. 点击“新建”按钮，弹出创建通知规则窗口。



创建通知规则

X

规则定义

* 通知类型 * 通知对象 * 通知方式 短信 邮箱 钉钉机器人 微信机器人* 生效周期 星期一 星期二 星期三 星期四 星期五 星期六 星期日* 通知时段 * 重复通知

规则信息

* 名称 描述

取消

确定

4. 配置通知规则信息。

说明：

只有在生效周期和通知时段产生的告警会进行通知。

参数	说明
通知类型	选择需要通知的告警类型，数据来源于威胁建模中的类型（可多选）。
通知对象	选择通知联系人，数据来源于在通知联系人页面创建的通知联系组（可多选）。
通知方式	<p>说明：</p> <p>如果需要向钉钉或微信发送告警的消息，需要先在通知联系组中配置钉钉机器人或微信机器人。</p>
生效周期	选择需要通知的星期（可多选）。

通知时段	选择需要通知的时间段。
重复通知	配置对于已通知但未及时处置的告警是否采用重复策略进行通知。
规则信息	用于标识特定规则的信息。



5. 配置完成后，单击“确定”，回到通知规则页面，可以看到已创建的通知规则，状态默认为“启用”。

管理通知规则

创建通知规则后，支持对通知规则进行管理，包括启用、停用、编辑、删除操作。

通知规则						
<input type="checkbox"/>	名称	通知类别	通知对象	状态	最近通知时间	操作
<input type="checkbox"/>	test4	Web应用防火墙（原生版）告警	test-cw1	停用	2024-09-27 13:48:03	启用 编辑 删除
<input type="checkbox"/>	test-cw1	常见攻击	test-cw1	停用	2024-09-10 01:46:09	启用 编辑 删除
<input type="checkbox"/>	通知组	(安全卫士) 网络暴力破解	[REDACTED]	停用	2024-10-12 11:22:13	启用 编辑 删除
<input type="checkbox"/>	lij	关联分析类型	test3	启用		停用 编辑 删除

4.4.4.2. 通知联系人

通知联系人由联系人和联系组组成，其中通知联系人需要填写名称、手机号以及邮箱。



通知联系人

新建联系人

1. 点击“新建”，创建联系人。
2. 填写姓名、手机号以及邮箱等信息。

“是否同时设置为每日告警提醒和每日日报接收的联系人”开关默认打开。关闭则不会收到相关通知。

创建联系人

X

此联系人设置用于接受各类告警提醒

* 姓名

* 手机号码

* 邮箱

是否同时设置为每日告警提醒和每日日报接收的联系人

取消

确定

3. 单击“确定”，完成创建。

配置日志分析量通知接收人和日报接收人

若您未配置日志分析量通知接收人和日报接收人时，页面上方会展示如下横幅通知：

The screenshot shows the Cloud Security Center (云安全中心) dashboard. On the left, there is a sidebar with various navigation items like '安全态势' (Security Status), '资产中心' (Asset Center), '威胁运营' (Threat Operations), etc. A prominent red banner at the top right states: '为保障用户个人信息与隐私数据，云安全中心于2025年3月18日起不再自动获取您的用户名、手机号与邮箱，您可前往【威胁运营】 - 【通知管理】 - 【通知联系人】配置通知接收人，否则将无法接受日志分析量不足提醒和日报等通知，给您带来不便请谅解。' (To ensure user information and privacy data security, the Cloud Security Center will no longer automatically obtain your username, mobile number, and email starting March 18, 2025. You can go to [Threat Operations] - [Notification Management] - [Notification Contact Person] to configure notification recipients, otherwise you will not receive timely notifications for insufficient log analysis and reports, which may cause inconvenience. Please understand.) Below the banner, the main dashboard displays several key metrics: '安全评分' (70), '资产总数' (1517), '告警总数' (154), and '威胁动态' (with four recent threat logs listed). There are also sections for '日志分布TOP5', '风险资产TOP5', and '告警处置概览'.



若您需要接收日志分析量不足的通知、接收日报，您可以执行以下步骤创建通知接收人：

1. 登录云安全中心控制台。
2. 单击页面上方横幅通知中的“前往配置”，跳转进入通知联系人页面。
4. 点击“新建”，创建联系人。
5. 填写姓名、手机号以及邮箱等信息。

“是否同时设置为每日告警提醒和每日日报接收的联系人”开关默认打开。

3. 单击“确定”，完成创建。

编辑联系人

点击编辑按钮实现联系人信息的变更。

删除联系人

单个删除：选择需要删除的联系人，点击删除按钮。

The screenshot shows a table with columns: Name, Phone Number, Email, and Operation. A single row is selected for 'Cloud Audit 1'. The 'Operation' column contains two buttons: 'Edit' and 'Delete', with 'Delete' being highlighted with a red box.

名称	手机号码	邮箱	所属通知联系组	操作
云等保1	13333333333			编辑 删除

共1条 10条/页 < 1 > 前往 1 页

多个删除：多选联系人，点击删除按钮。

The screenshot shows a table with three contacts selected. The 'Operation' column for each contact has two buttons: 'Edit' and 'Delete'. The 'Delete' button for the first contact is highlighted with a red box. A modal dialog box titled 'Warning' is displayed, containing a message: '此操作同步删除用户组和通知规则内的通知人信息,确定删除吗?' (This operation will synchronize delete user groups and notification rules. Do you want to proceed?). The 'Delete' button in the dialog box is also highlighted with a red box.

名称	手机号码	邮箱	所属通知联系组	操作
云 [REDACTED]	13333333333			编辑 删除
云 [REDACTED]	13333333333			编辑 删除
云 [REDACTED]	13333333333			编辑 删除

共3条 10条/页 < 1 > 前往 1 页

注意：

删除联系人会同步删除用户组和通知规则内的通知人信息。

通知联系组

新建联系组

1. 点击新建按钮，创建联系组。
2. 输入联系组组名和备注信息。
3. 根据需要开启钉钉机器人或微信机器人。

说明：

钉钉机器人的 token 与 secret 获取方式与微信机器人获取 key 的方式见 “常见问题 > 配置类 > 告警通知相关”。

创建联系组

X



* 组名

钉钉机器人

* token

* secret

微信机器人

* key

备注

选择联系人

待选联系人	0/1
<input type="checkbox"/> test1	<input type="radio"/> 请输入联系人姓名

已选联系人	0/0
<input type="checkbox"/>	<input type="radio"/> 请输入联系人姓名

无数据

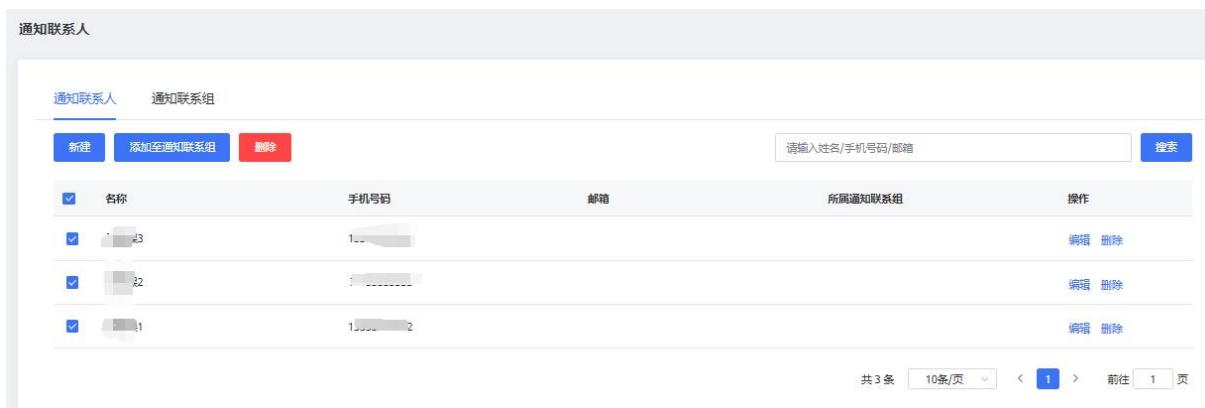
4. 勾选需要添加到组的联系人，点击向右按钮将待选联系人移动到已选联系人中。



5. 点击确定，完成联系人组的新建。

快捷添加入联系人组

1. 在联系人页面多选联系人。
2. 点击添加至通知联系组。



名称	手机号码	邮箱	所属通知联系组	操作
43	13.....			编辑 删除
42	13.....			编辑 删除
41	13.....2			编辑 删除

3. 选择需要添加的通知联系组。
4. 点击确定，实现快捷添加。

删除联系组

注意：

删除联系组不会删除联系人。

单个删除：选择需要删除的联系组，点击删除按钮。



通知联系人 通知联系组

新建 **删除**

组名称	操作
组1	编辑 删除
组2	编辑 删除

共 2 条 10条/页 < 1 > 前往 1 页

多个删除：多选需要删除的联系组，点击删除按钮。在弹出的提示框中，单击“确定”。

通知联系人 通知联系组

新建 **删除**

组名称	操作
组1	编辑 删除
组2	编辑 删除

共 2 条 10条/页 < 1 > 前往 1 页

4.4.5. 威胁检测

4.4.5.1. 威胁建模

通过威胁建模规则，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威胁建模规则。

用户初次订购时会复制所有的威胁建模模板，并开启对应的威胁建模规则（如：租户订购了 Web 应用防火墙原生版，集成配置开启开关，则会开启对应的威胁建模规则）。

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”。

启动 停止 **+新建** 自删除 自检规则

规则名称	规则类型	相关事件	创建时间	开始时间	持续时间	操作
						无数据



4. 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: 请输入 0/64

规则描述: 请输入 0/500

* 规则类型: 请选择

* 规则模板: 请选择类型
规则模板描述:

标签: 请选择类型 标签编辑

取消 保存

5. 选择规则类型和规则模板后，还需要配置原始告警源、时间窗口、告警配置等。其中时间窗口需要在 2 小时以内。

① 原始告警源

A: 原始告警 请选择告警名称 过滤条件: 无 编辑 删除

B: 原始告警 请选择告警名称 过滤条件: 无 编辑 删除

添加告警

② 时间窗口

* 窗口大小: 请输入 分钟: 0 分钟

分组条件: 请选择类型

③ 告警配置

* 归并模式: 不归并 按自然日 (0点-24点) 归并 按会话归并 会话间隔: 0 分钟

分组条件: 请选择类型

其它输出字段: 请选择类型

* 原始告警阶段: 侦查

* 原始告警级别: 提醒

* 原始告警内容: 请输入 0/128

处置建议: 请输入 0/128



6. 配置完成后，单击“保存”。列表中可以看到新建的规则。

The screenshot shows the Wing Cloud management console with the 'Rules' section selected. At the top, there are buttons for '启动' (Start), '停止' (Stop), '+新建' (+New), '自删除' (Auto Delete), and '自检规则' (Self-inspection Rule). Below these are two tabs: '规则组' (Rule Group) and '规则类型' (Rule Type). Under '规则组', a single item '系统异常规则组' (System Abnormality Rule Group) is listed. In the main table, there is one row for a newly created rule: '云等保专区_下一代防火墙_威胁日志_1.0模板' (Cloud Security Protection Zone下一代 Firewall Threat Log 1.0 Template), which is a 'System Abnormality' rule created on 2024-12-02 at 12:31:12, with a duration of 5 minutes.

复制规则

1. 选择模板规则或者已经创建好的规则。
2. 点击复制按钮复制规则。

This screenshot shows the same rule configuration interface as the previous one, but with a red arrow pointing to the '操作' (Operation) column of the selected rule ('云等保专区_下一代防火墙_威胁日志_1.0模板'). The '操作' column contains icons for Start, Stop, Delete, and Copy. A red box highlights the 'Copy' icon, which is also annotated with a red arrow and the word '点击' (Click).

3. 编辑规则信息。
4. 保存规则（规则名称不能相同）。

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。

注意：

如果日志在集成配置中关闭了自动转告警，则会使对应的规则不生效，不产生告警。

4.4.5.2. 对象管理

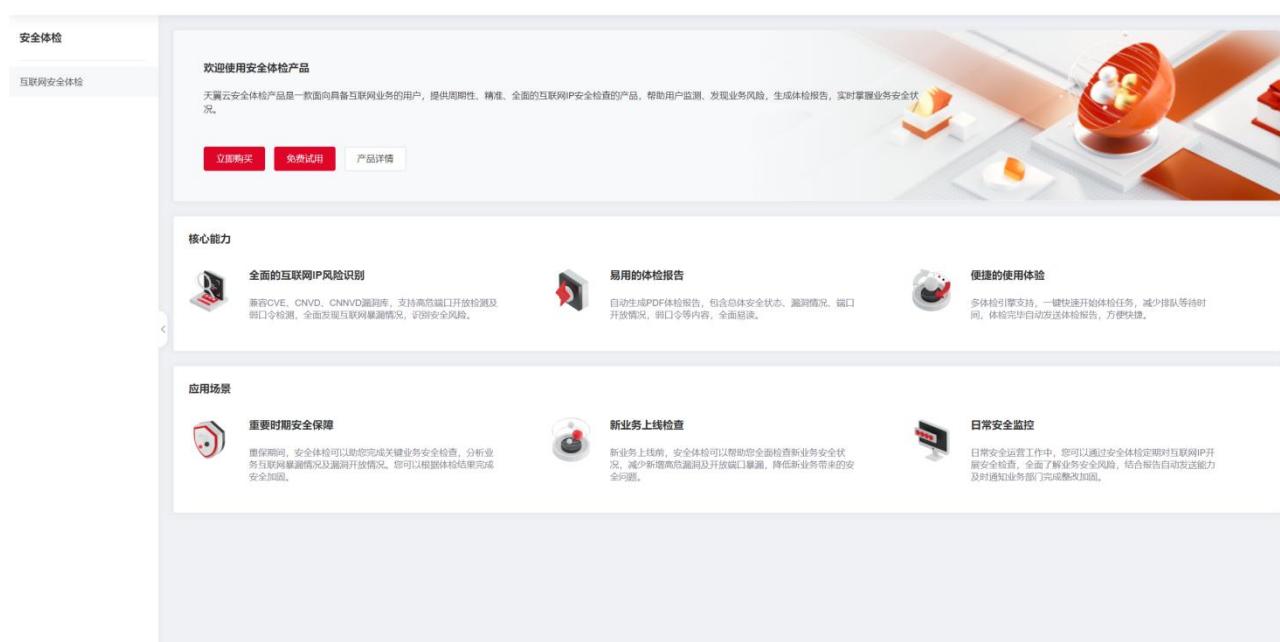
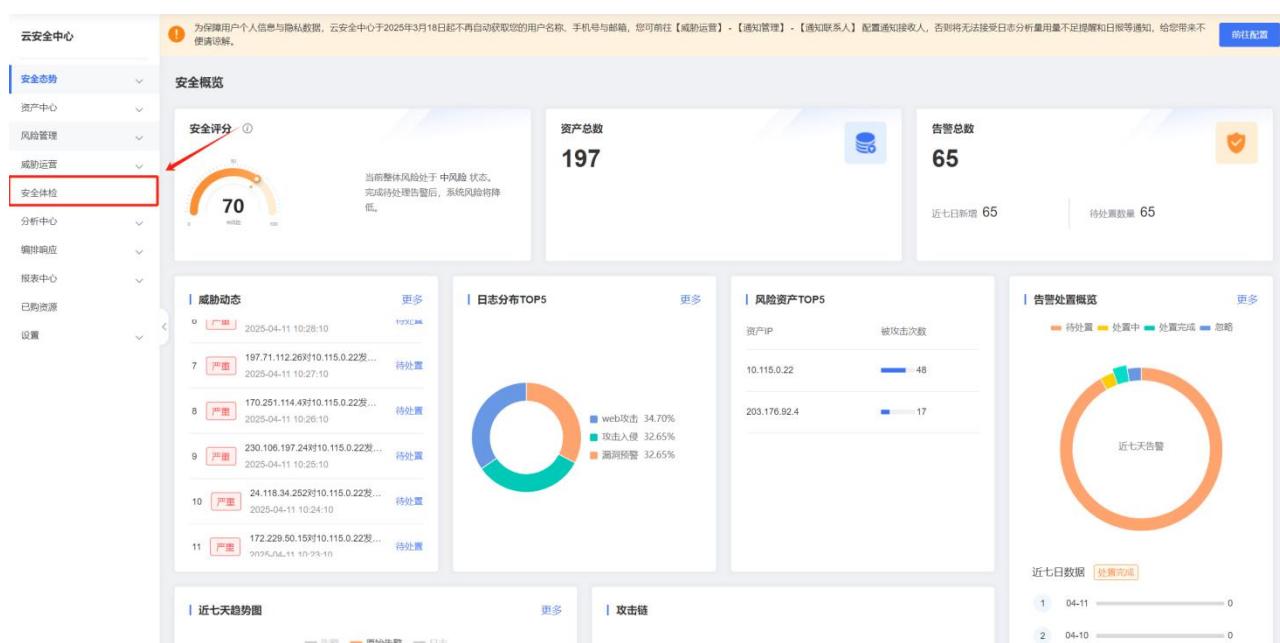
展示有价值的内部信息，在关联分析时，对于IP类型、数字类型或字符类型的字段，可以添加过滤条件属于信息，便于进行分析。通过导入内容包，系统已内置一些信息。

The screenshot shows the 'Object Management' interface. On the left, there is a sidebar with a search bar and a tree view of internal information categories: Internal Information Management, IP Category Information (selected), Network IP, DNS Server IP, Mail Server Address, Log Server Address, Important Network Equipment Asset IP, Database Server IP, Reserved IP Address List, Number Category Information, Character Category Information, and Time Category Information. The main area displays a table with columns: Information Content, Creation Time, Update Time, Validity Period, Status, and Operation. A single row is shown with the following data: [redacted] (Information Content), 2024-08-15 14:15:42 (Creation Time), 2024-08-15 14:15:42 (Update Time), Always Valid (Validity Period), Internal Network (Status), and edit/pencil and delete icons (Operation). At the bottom right, there are pagination controls: 1/1 pages, 30 items per page, and a search bar.

4.5. 安全体检

云安全中心提供安全体检产品的功能，可支持的场景包括高危端口开放情况、弱口令、漏洞开放情况，并输出体检报告。用户根据需求单独购买。

产品详细介绍地址：<https://www.ctyun.cn/products/nsc>。



4.6. 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、发生告警的数量为纵轴，展示符合查询关键字和查询时间窗的告警趋势图。

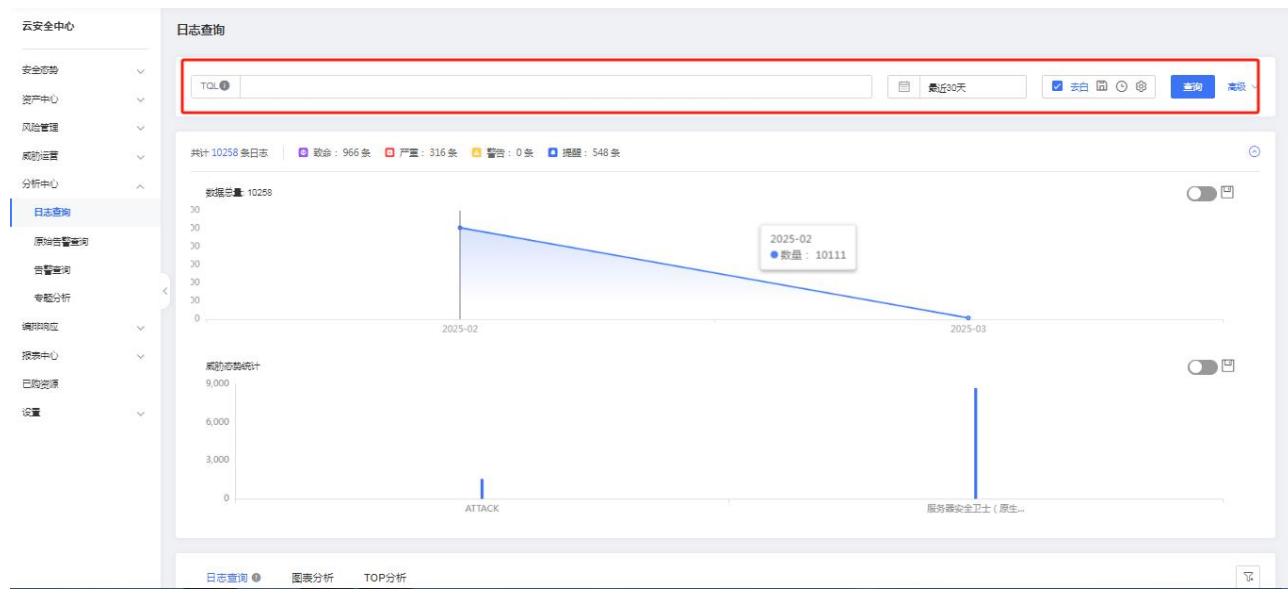
前提条件

已开通云安全中心实例。

4.6.1. 日志查询

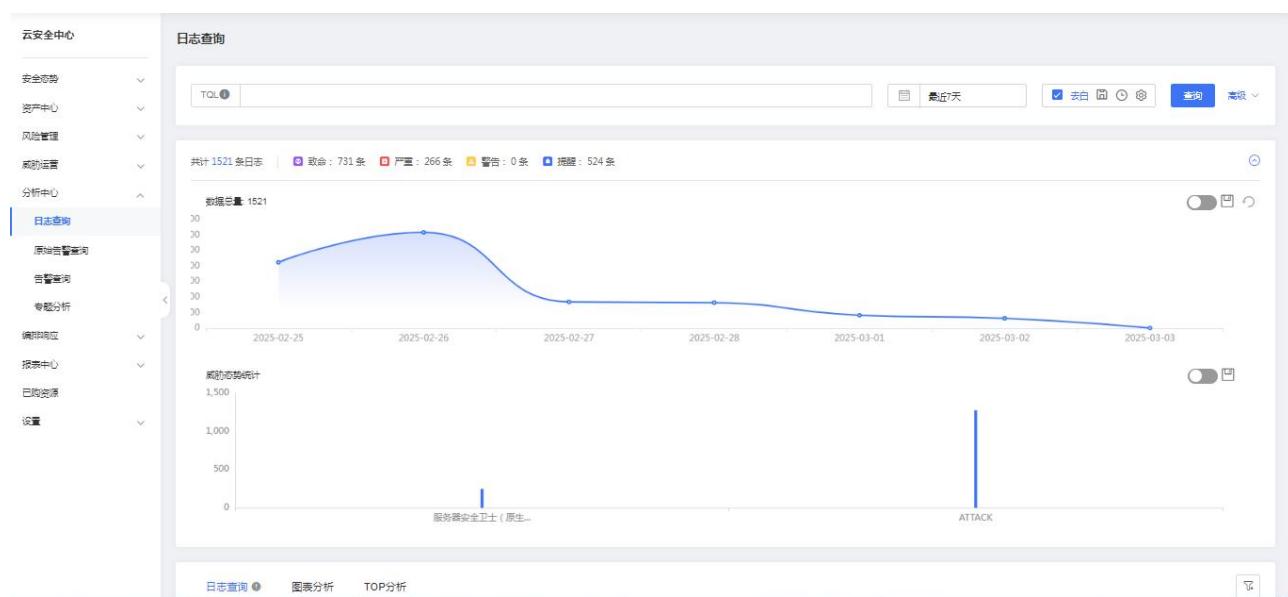
查询条件

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，单击每条数据能够看到详细数据。

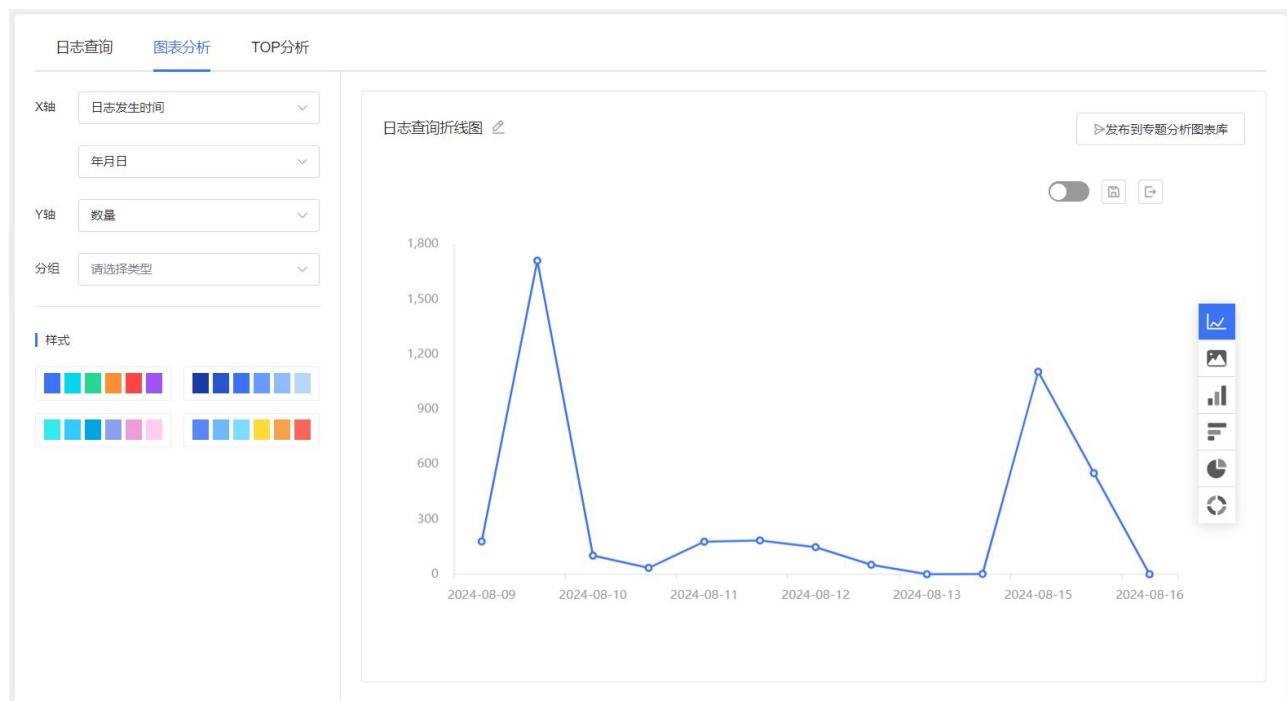
日志查询结果栏字段筛选：

目的IP地址	开始时间	目的端口	源IP地址	日志级别	攻击类型	日志发生时间
192.168.24.80		80		致命	本地文件包含	2024-12-05 14:22:51
192.168.24.80		443		致命	文件上传	2024-12-05 14:22:51
192.168.24.80		443		致命	PHP 反序列化	2024-12-05 14:22:41
192.168.24.80		80		致命	Java 反序列化	2024-12-05 14:22:41
192.168.24.80		443		致命	ASP 代码执行	2024-12-05 14:22:41
192.168.24.80		80		致命	Java 代码执行	2024-12-05 14:22:31
192.168.24.80		443		致命	通用代码执行	2024-12-05 14:22:31
192.168.24.80		443		致命	Java 代码执行	2024-12-05 14:22:30
192.168.24.80		80		致命	Java 代码执行	2024-12-05 14:22:20
192.168.24.80		443		致命	Java 代码执行	2024-12-05 14:22:20
192.168.24.80		80		致命	本地文件包含	2024-12-05 14:22:10
192.168.24.80		80		致命	SQl注入	2024-12-05 14:21:28
192.168.24.80		80		致命	XSS攻击	2024-12-05 14:21:28

已选字段
目的IP地址
开始时间
目的端口
源IP地址
日志级别
攻击类型
日志发生时间
待选字段
□请输入搜索待选字段
日志来源
规则标签
所属系统名称
攻击结果

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。



发布到专题分析图表库

X

请选择分类

图例类型 / 账户安全



取消

确定

4.6.2. 原始告警查询

原始告警查询具体操作请参考“日志查询”。

原始告警查询

原始告警查询

TQL

共计 1021 条原始告警 致命: 0 条 严重: 0 条 警告: 1021 条 提醒: 0 条

数据总量: 1021

告警查询 图表分析

告警内容	告警产品	源IP地址	目的端口	源端口	日志来源	告警威胁类型
192.168.1.5对106.63.100.42触发告警		192.168.1.5				
10.115.0.24对触发告警		10.115.0.24				
10.115.0.23对触发告警		10.115.0.23				

原始告警查询结果栏字段筛选:



图表分析

告警查询 图表分析

X轴 告警创建时间
年月日
Y轴 数量
分组 请选择类型

样式

告警查询折线图 ↗

发布到专题分析图表库

开关图标

操作图标

日期	数量
2024-08-09	165
2024-08-10	95
2024-08-11	110
2024-08-12	120
2024-08-13	10
2024-08-14	5
2024-08-15	15
2024-08-16	5



4.6.3. 告警查询

告警查询具体操作请参考“日志查询”。

告警查询

告警查询结果栏字段筛选

图表分析



The screenshot shows the Cloud Security Center's main dashboard. On the left, there's a sidebar with various navigation items like '安全态势', '资产中心', '风险管理', etc. The '专题分析' item is highlighted. The main area is titled '告警查询' (Alert Query). It features a search bar with 'TQL' and a date range selector ('最近7天'). Below that, it says '共计 1 条告警' (1 alert found) with categories: 0 Critical, 0 Severe, 1 Warning, 0 Minor. A chart titled '数据总量: 1' (Data Total: 1) is shown, with a single point at 2024-10-08 labeled '数量: 1'. At the bottom right of the main area, there's a button to '发布到专题分析图表库' (Publish to Special Topic Analysis Chart Library).

4.6.4. 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”。



专题分析

专题

+ 创建专题

请创建一个新专题或打开已创建的专题

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。

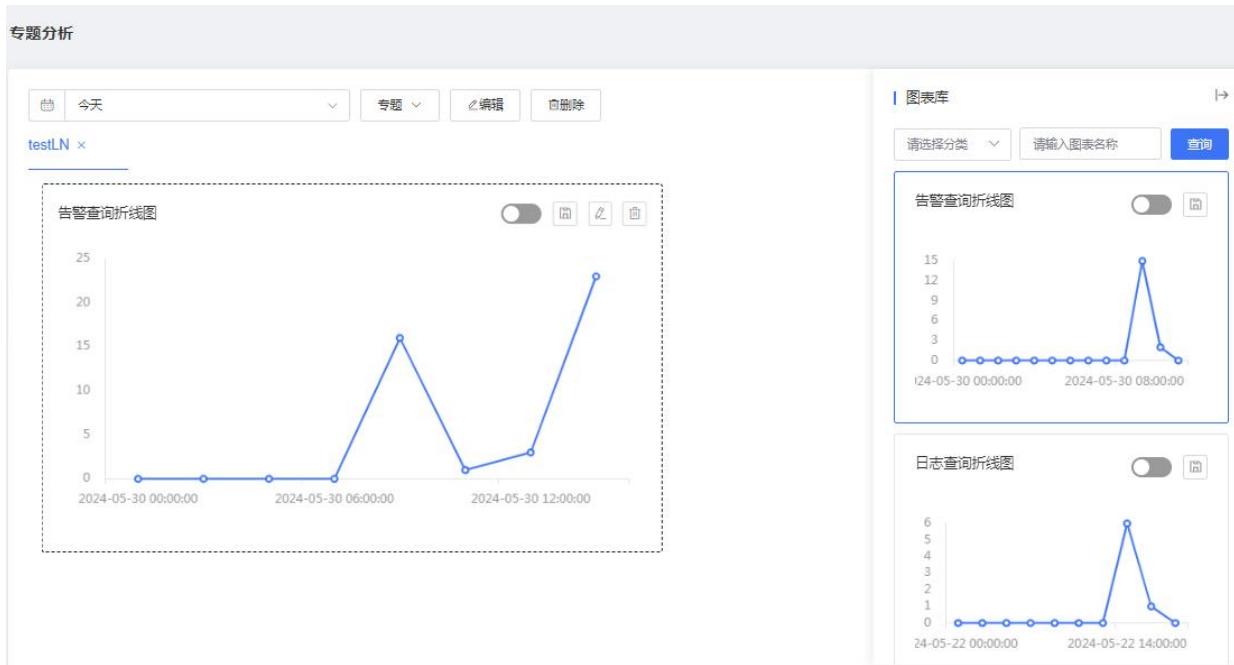
创建专题

* 专题名称 test

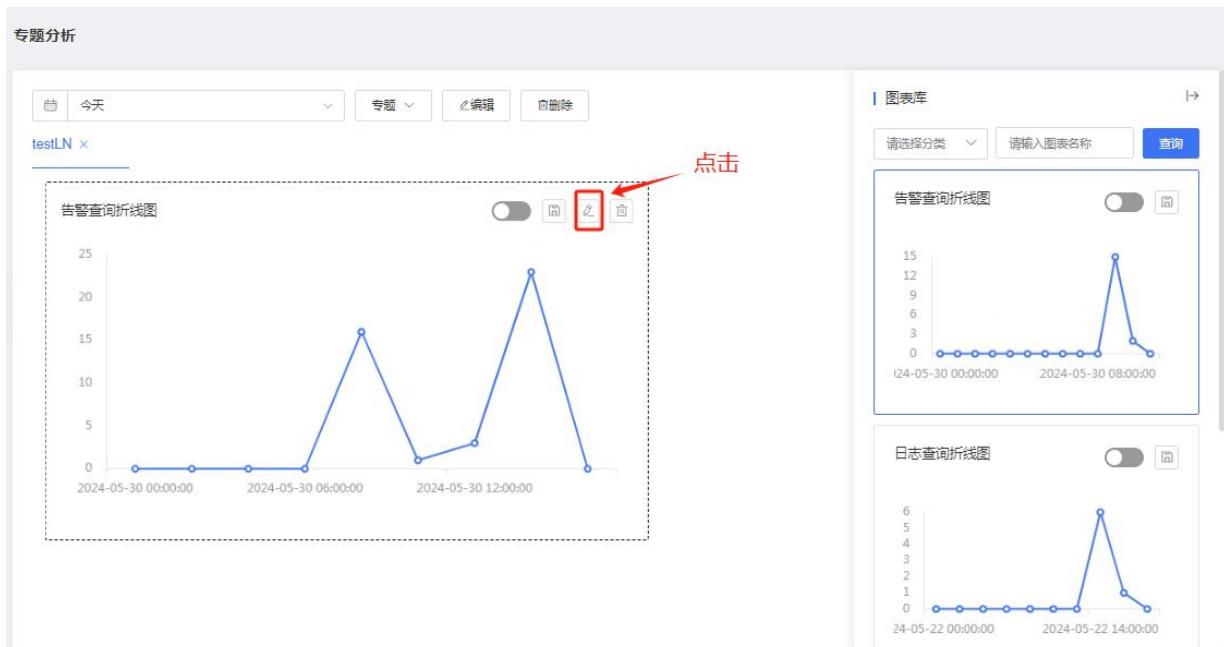
取消 确定

配置专题

1. 从图表库中拖拽所需图表至左侧空白处。



- 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。



- 图表库增加删除按钮，删除后报表模板中的图表分析也会进行对应删除。



The screenshot shows the WingCloud Control Panel interface. On the left, there's a sidebar with '云安全中心' (Cloud Security Center) and '专题分析' (Topic Analysis) selected. The main area is titled '专题分析' (Topic Analysis). It features a search bar, date range selector ('今天'), and a dropdown for '专题'. A central modal dialog box displays a warning message: '当前操作会影响该图表在报表中的展示, 请确认是否删除?' (This operation will affect the display of this chart in the report, please confirm whether to delete?). Below the modal, a message says '请创建一个新专题或打开已创建的专题' (Please create a new topic or open an already created topic). To the right, there are two sections: '图表库' (Chart Library) and '系统异常行为' (System Abnormal Behavior). The '图表库' section has a search bar and a dropdown for '请选择分类'. The '系统异常行为' section has a toggle switch and three bar charts for '病毒防护' (Antivirus Protection), '流量日志' (Traffic Log), and '访问异常' (Access Abnormal).

The screenshot shows the WingCloud Control Panel interface. On the left, there's a sidebar with '云安全中心' and '报表模板' selected. The main area is titled '报表模板' (Report Template). It features a search bar, a '编辑模板' (Edit Template) button, and a form for creating a new template. The form includes fields for '名称' (Name) set to 'test', '类型' (Type) set to '月报' (Monthly Report), '报表生成时间' (Report Generation Time) set to '1号 00:00', and a rich text editor for '内容' (Content). To the right, there are three chart cards: '常用' (Common), '自定义指标' (Custom Metrics), and '自定义图表' (Custom Chart). The '自定义图表' card is highlighted with a red border. It contains a search bar, a '请选择' (Select) button, and a line chart titled '端口扫描情况' (Port Scan Situation) showing a sharp drop from 100 to 0 at the timestamp '100.89.2.190'.

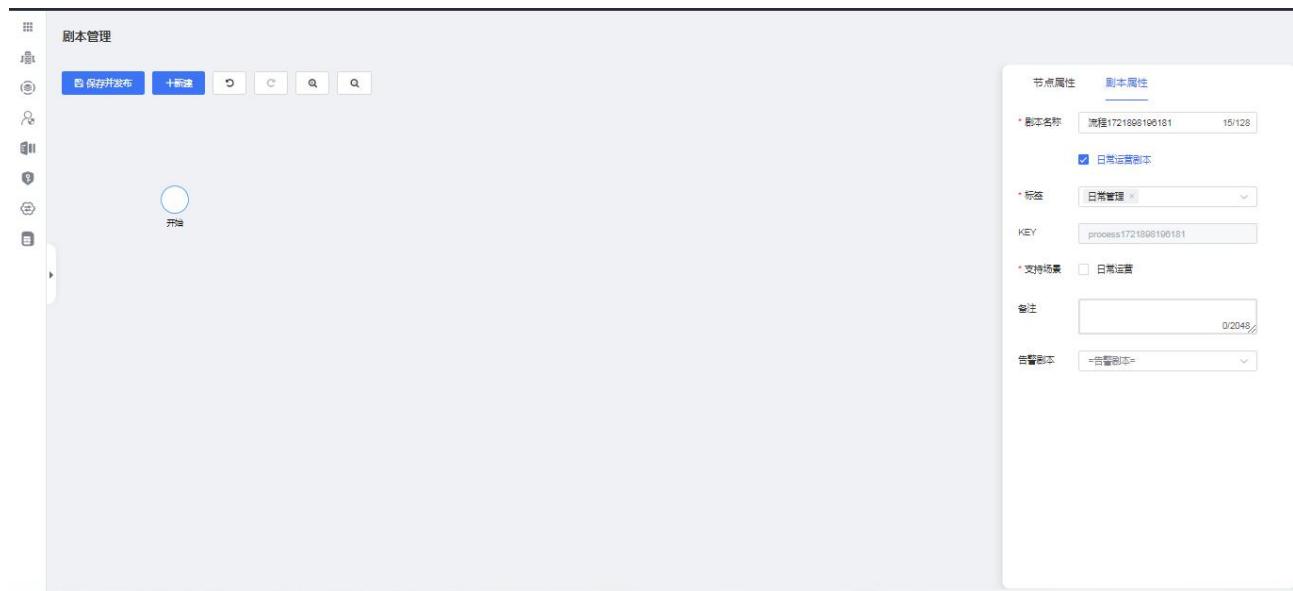
4.7. 编排响应

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。



剧本列表

剧本列表

剧本标签:请选择 剧本名称:请输入 剧本类型:请选择
剧本状态:请选择 启停状态:请选择

[查询] [重置]

[新建] [删除] [导入] [导出]

□	剧本名称	剧本标签	剧本类型	场景名称	触发次数(累计/最近)	创建时间	更新时间	状态	操作
<input type="checkbox"/>	01租户剧本	公有云版本	剧本	日常运营:HW 行动,安全运营	1/1	2024-05-31 09:31:59.626	2024-05-31 09:32:03.411	正常/未引用	
<input type="checkbox"/>	流程1710004531284	公有云版本	剧本	日常运营:HW 行动,安全运营	5/5	2024-05-29 15:13:57.983	2024-05-29 15:14:01.441	正常/未引用	

共2条 20条页 < 1 > 前往 1 页

新增剧本节点

选择节点后，点下如下按钮，新增剧本节点。

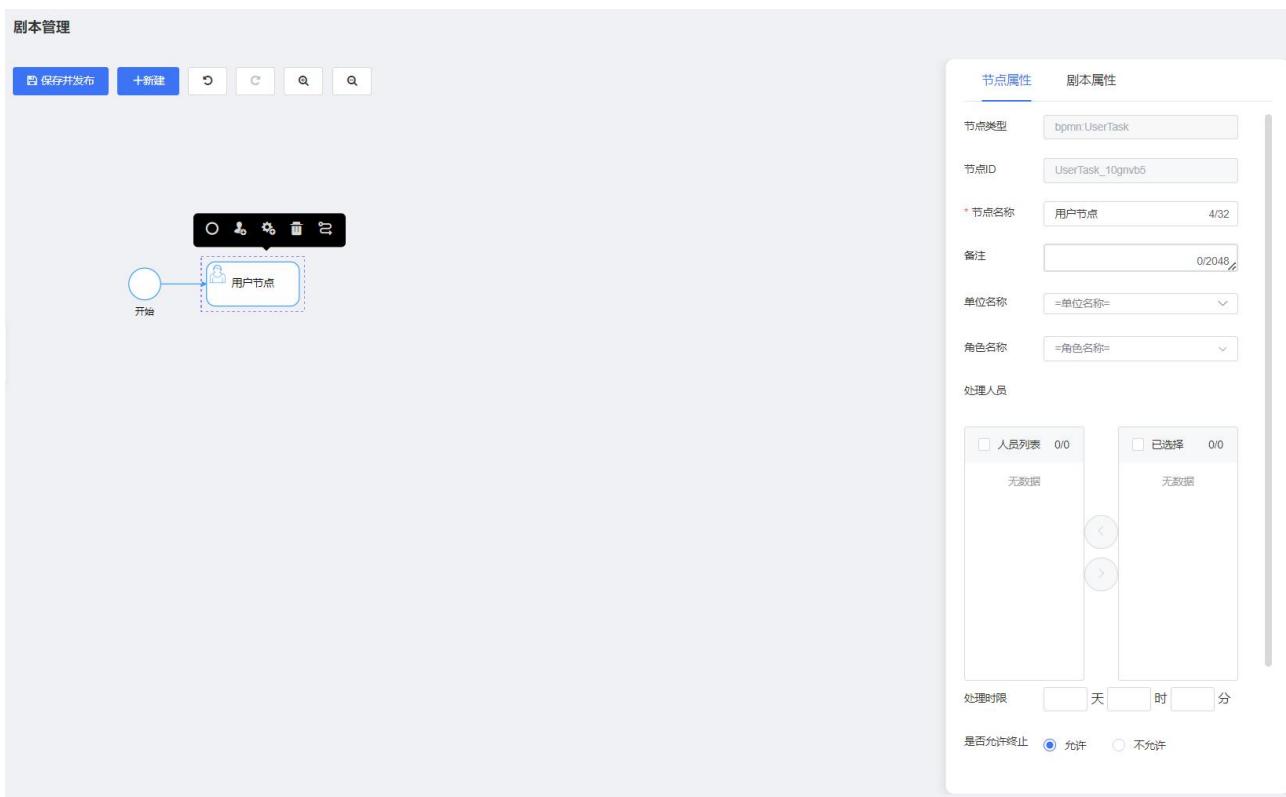
剧本管理

[保存并发布] [十新建] [撤销] [重做] [搜索] [刷新]

节点属性 剧本属性

节点类型: bpmn:StartEvent
节点ID: StartEvent_01ydzqe
节点名称: 开始 2/32

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”当前告警工单的剧本执行。

告警 处置 作战室 实战剧本 关联事件 小结

111.117.106.197对172.17.0.2触发告警，攻击类型为XSS攻击

攻击阶段：【侦查】责任人修改
发生时间：2024-05-29 17:50:34
外部威胁IP：
完成时候：2024-05-31 23:26:28
处置建议：

工单处置

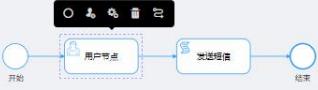
用户节点 处置意见	当期剩余：1天0小时0分钟 0/255
<input type="button" value="终止执行"/> <input type="button" value="确定"/>	

● 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。

剧本查看

另存为新剧本 另存为新剧本 搜索 重置 刷新



备注	0/2048
单位名称	sec2208001@163.com
角色名称	=角色名称=
处理人员	
<input type="checkbox"/> 人员列表 0/0 无数据	<input type="checkbox"/> 已选择 0/1 chenwen
处理时限 <input type="text" value="1"/> 天 <input type="text" value="0"/> 时 <input type="text" value="0"/> 分	
是否允许终止 <input checked="" type="radio"/> 允许 <input type="radio"/> 不允许	
是否允许回退 <input checked="" type="radio"/> 允许 <input type="radio"/> 不允许	

设置后，在告警管理列表和告警处置中会显示是否超时。

工单管理

请输入事件名或资产ID 最近7天 查询 重置 导出 高级

待办 处置中 处置完成 自动处置 勿需处置 新建 试播 重置 忽略

剧本	发生时间	当前环节			当前状态	完成时间	剩余时间	操作
		环节名	完成时间	剩余时间				
01账户剧本	2024-05-29 17:50:34	用户节点(chenwen)	2024-05-31 23:26:28	0天21小时	处手中	2024-05-31 23:26:28	0天0小时	
	2024-05-24 10:01:36				待处置			
	2024-05-21 17:17:38				待处置			
	2024-05-21 18:50:34				待处置			
	2024-05-21 18:50:34				待处置			

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。



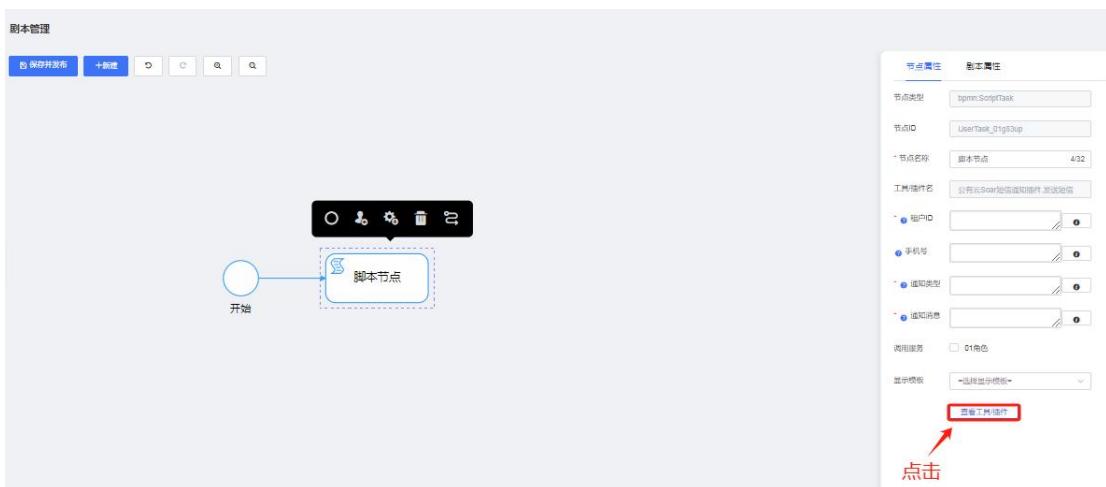
切换为脚本任务后，系统默认从左侧弹出插件选取栏，可通过插件选取栏搜索相关插件或直接选取。

说明：

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。

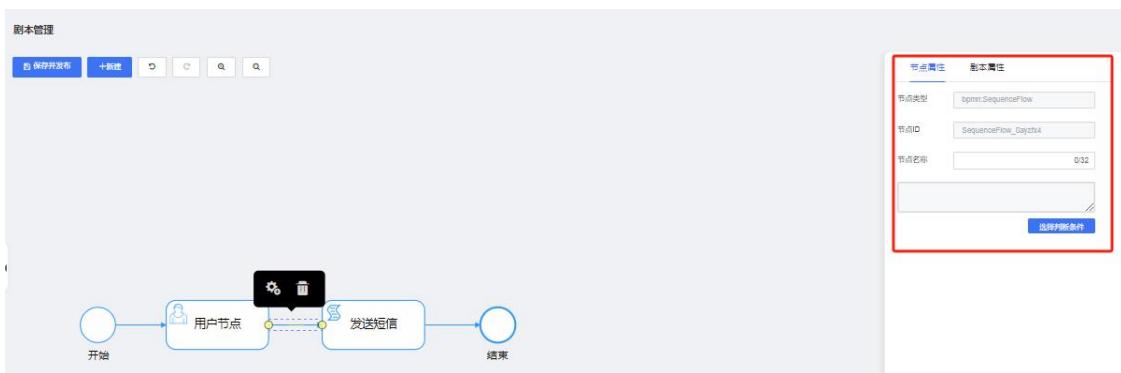


选取完插件后，设置插件的入参。



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。



判断条件设置

请选择字段 请选择 请输入 0/32

AND 添加条件 添加组 删除组

取消 确定

复制剧本

1. 选择已经创建好的剧本。
2. 点击复制按钮。

剧本管理

剧本标签: 请选择 剧本名称: 请输入 剧本类型: 请选择
剧本状态: 请选择 启停状态: 请选择

新建 <|> |> |重置 |查询

操作	创建时间	模板类型	触发次数(累计/最近)	场景名称	剧本类型	剧本标签	剧本名称
	2024-09-03	预置模板	-	日常运营	剧本	云等保专区_下一代防火墙_境外IP攻击封堵_接板	
	2024-08-28	预置模板	-	日常运营	剧本	外部扫描攻击处置	
	2024-09-03	预置模板	-	日常运营	剧本	测试获取租户ID服务副本4	
	2024-08-16	预置模板	-	日常运营	剧本	atest	

共 4 条 20条/页 < 1 > 前往 1 页

3. 编辑剧本信息，确保剧本名称不重复。



< 剧本管理

The screenshot shows the 'Script Management' interface. On the left, there's a script flow diagram with nodes: '查询' (Query), '新增' (Add), '成功' (Success), '查询参数' (Query Parameters), '查询黑名单' (Query Blacklist), '是否封堵境外ip' (Is it blocked by foreign IP), and '填写ip' (Fill IP). Arrows indicate the flow from '查询' to '新增', then through '成功' to the sequence of nodes. The '是否封堵境外ip' node has two paths: '是' (Yes) leading to '填写ip', and '否' (No) leading back to '失败' (Failure). On the right, the 'Script Properties' panel is open, showing fields like 'Script Name' (云等保专区_下一代防火墙_境外IP 38/128), '日常运营剧本' (Daily Operation Script) checked, 'Label' (日常管理), 'KEY' (processcc1725539596959), 'Support Scenario' (日常运营 Daily Operation) checked, 'Remarks' (0/2048), and 'Report Script' (=告警剧本=).

4. 点击保存并发布，完成剧本复制。

4.7.2. 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 > 插件管理”，进入插件管理页面。

The screenshot shows the 'Plugin Management' interface. It displays a table of services:

版本号	工具名	语言类型	说明	操作
> 1.0.0	公有云Web应用防火墙（原生版）插件	java	公有云Web应用防火墙（原生版）插件	
> 1.0.0	公有云Soar短信通知插件	java	公有云通知插件	

3. 单击操作列的新增图标，弹出新增服务对话框。



新增

X

* 服务名称

test

4/128

备注

0/2048

测试连接

确定

- 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。

版本号	工具名	语言类型	说明	创建人	操作
v 1.0.0	公有云soar短信通知插件	java	公有云通知插件	超级管理员	
<hr/>					
服务名称	状态	说明	创建人	操作	
test	off		chenwen		

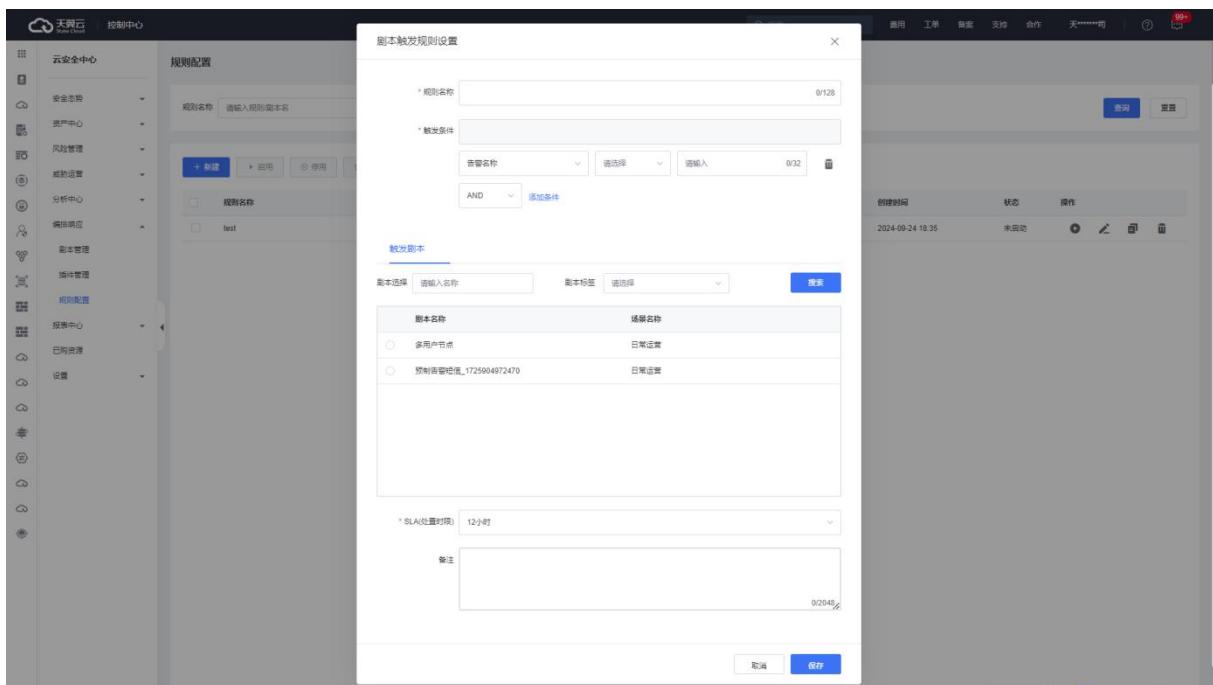
- 服务状态默认为关闭，单击操作列的“启用”图标，启用服务。

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

- 登录云安全中心控制台。
- 在左侧导航栏选择“编排响应 > 规则配置”，进入规则配置页面。
- 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。



规则名称	处置剧本/工具	处置时限	备注	创建时间	状态	操作			
test	(剧本) 预制告警短信_1725904972470	12小时		2024-09-24 18:35	未启动				

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：

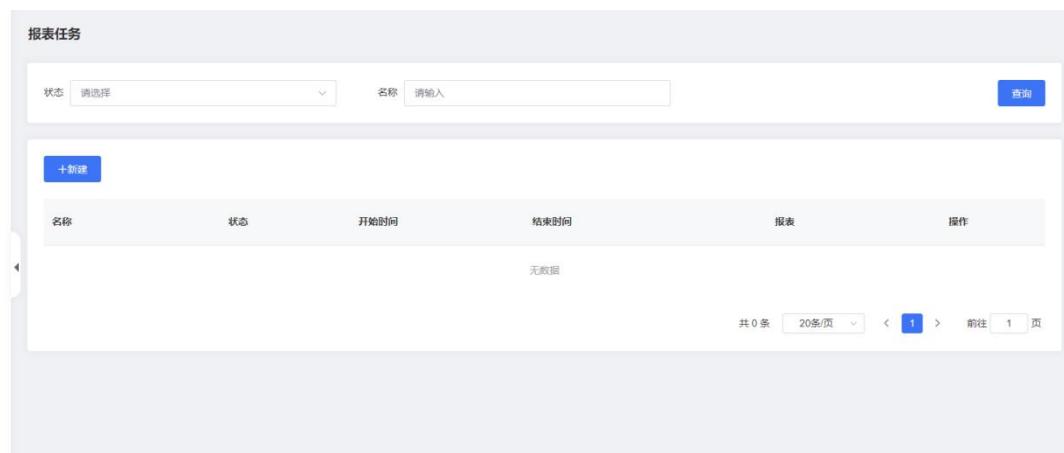
周期报表任务执行时发送报表短信到用户在系统配置的手机号。

前提条件

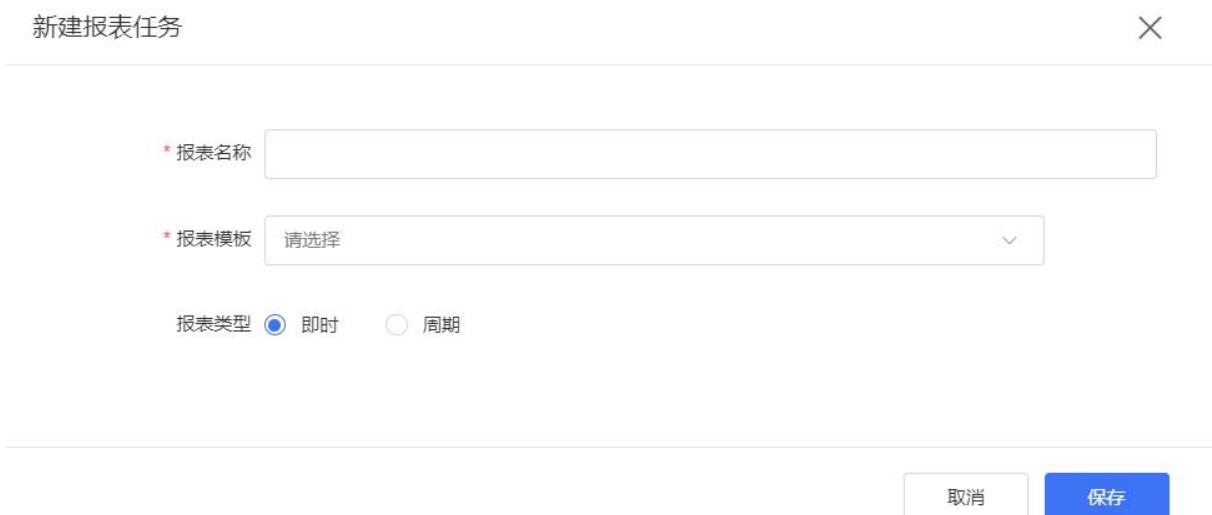
已创建报表模板。

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）。



新建报表任务

* 报表名称

* 报表模板 请选择

报表类型 即时 周期

取消 保存



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。（周期性报表任务最多启动 10 个任务）

周期性报表任务列表					
名称	状态	开始时间	结束时间	报表	操作
日报3	创建	2024-06-27 17:53:08	2024-06-27 18:23:08		

● 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。

周期性报表任务列表					
名称	状态	开始时间	结束时间	报表	操作
日报3	创建	2024-06-27 17:53:08	2024-06-27 18:23:08		

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。

已生成报表列表					
名称	状态	开始时间	结束时间	报表	操作
日报3	创建	2024-06-27 17:53:08	2024-06-27 18:23:08		

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。



报表模板

报表模板 新建模板 ×

* 名称:

* 类型: 日报 周报 月报 季报 年报

* 时间范围: 00:00

* 内容:

段落	默认字体	小四	粗	斜	下划线	右对齐	左对齐	居中	文本框	插入
左	右	眼睛	剪切	粘贴						
B	I	U	S	X ²	插入	A	等宽	等高	A	①

常用 自定义指标 自定义图表

报表周期时间 报表任务时间

4. 配置模板名称、类型、时间范围和报表内容。

其中类型指定的时间为报表自定义指标的默认数据周期时间（当自定义指标中指定了绝对时间后，会覆盖默认数据周期时间）。

5. 单击“保存”，保存模板。

云安全中心 报表模板

报表模板

+ 新建 重命名

请输入名称 C

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	

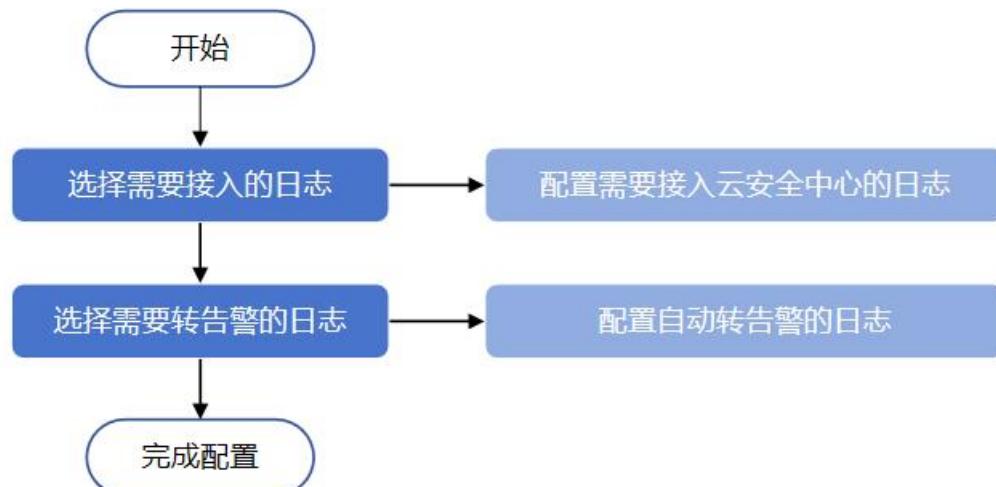
共2条 20条/页 < 1 > 前往 1 页

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。

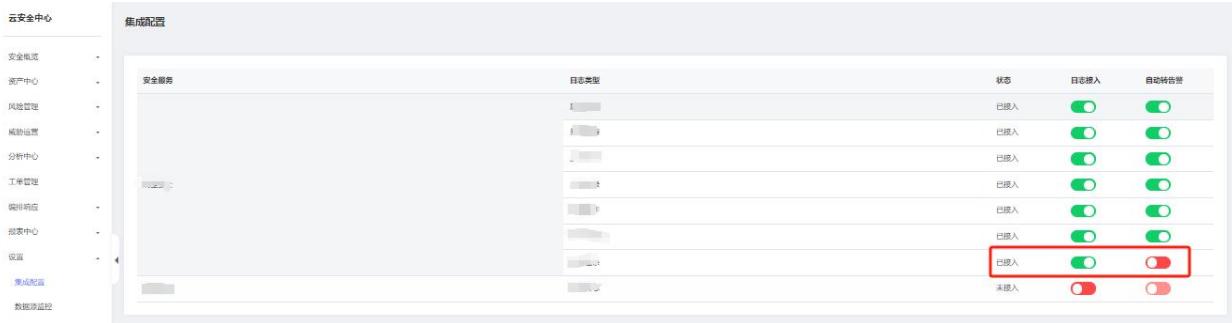


前提条件

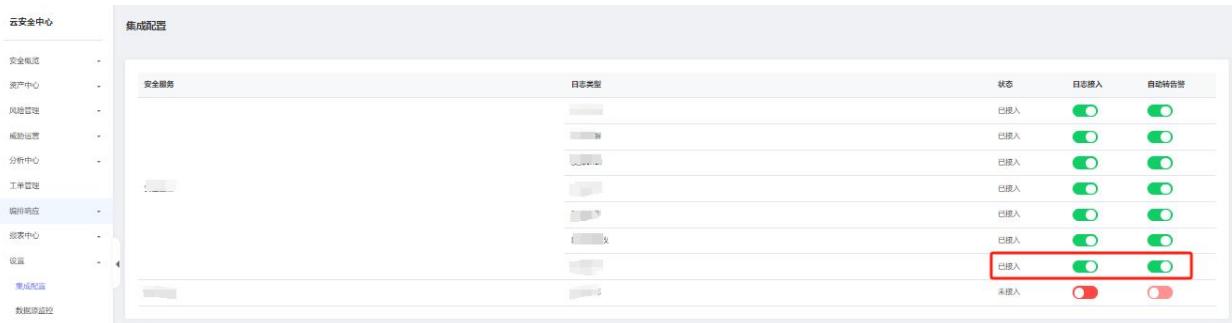
需确保要接入日志的数据源监控处于启用状态。具体操作请参见数据源监控。

操作步骤

1. 登录云安全中心控制台。
2. 选择“设置 > 集成配置”，打开数据集成配置页面。
3. 选择需要接入的日志，并打开日志接入开关。



4. 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。
- 需要先在数据源监控页面启用开关后，才可以在集成配置页面中开启日志和告警配置。
- 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。
- 自动转告警打开，对应的日志类型才能产生告警。

4.9.2. 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。



云安全中心

数据源监控

安全态势
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
已购资源
设置
集成配置
数据源监控

数据源IP: **查询** **重置**

Kafka日志 Syslog日志

数据源IP	资产名称	设备厂商	设备类型	端口	状态	收到最近一条日志时间	操作
192.168.1.101	服务器安全卫士 (原生版)	天翼云	主机	9092	启用中	2023-07-10 10:00:00	
127.0.0.1	Web应用防火墙 (原生版)	天翼云	防火墙	9092	启用中	2023-07-10 10:00:00	

共 2 条 10条/页 < 1 > 前往 1 页

2. 选择需要接入的数据源，并启用数据源。

Kafka日志 Syslog日志

数据源IP	资产名称	设备厂商	设备类型	端口	状态	收到最近一条日志时间	操作
192.168.1.101	服务器安全卫士 (原生版)	天翼云	主机	9092	启用中	2023-07-10 10:00:00	
127.0.0.1	Web应用防火墙 (原生版)	天翼云	防火墙	9092	启用中	2023-07-10 10:00:00	

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。

4.9.3. 规则标签配置

云安全中心的规则标签功能，提供白名单及自定义的规则标签，用户可设置需要打标签的日志筛选范围，并赋予其白名单或自定义的标签。

- 白名单标签：当日志解析出的内容匹配到了白名单标签规则，日志则会被标记为白名单，对应日志将不会产生告警。
- 自定义标签：当日志解析出的内容匹配到了自定义标签规则，日志则会被标记为自定义标签，仍然会产生告警。

新增标签规则

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“设置 > 规则标签配置”，单击“新建”。

规则标签配置

查询

状态: 启用
标签: 多选项

+新建 已删除

□	有效期	标签	内容	命中次数	创建时间	
<input type="checkbox"/>	永久有效	白名单	源IP地址 = 192.168.0.9 and 目的IP地址 = 100.89.2.190 and 威胁类型 = EDR and 日志来源 = 云等保专区	0	2024-11-08 09:51:40	编辑 删除 禁用

3. 在弹出的新增窗口中，配置标签、匹配条件、有效期、备注信息。

- 标签：支持选择一个或多个标签。
 - 标签设置为白名单时，当日志解析出的内容匹配到了标签规则，日志则会被标记为白名单，对应日志将不会生成告警。
 - 标签设置为自定义标签时，当日志解析出的内容匹配到了标签规则，日志则会被标记为自定义标签，不影响告警产生。
 - 标签同时设置了白名单标签和自定义标签时，当日志解析出的内容匹配到了标签规则，日志则会被标记为白名单+自定义标签，对应日志将不会生成告警。
- 匹配条件：配置日志内容需要匹配的条件。
- 有效期：标签规则仅在有效期内生效。若不配置，则永久有效。

新增

* 标签 白名单 测试标签 +

* 匹配条件 源IP地址 = 1.2.3.4 ×

有效期 2024-11-08 至 2024-11-16 ?

* 备注 test

取消 保存

4. 参数配置完成后，单击“保存”，回到规则标签配置页面。

启用/停止标签规则

- 启用标签规则，规则生效，日志匹配标签规则。



	有效期	标签	内容	命中次数	创建时间	启用状态
<input type="checkbox"/>	永久有效	白名单	源IP地址 = 192.168.0.9 and 目的IP地址 = 100.89.2.190 and 威胁类型 = EDR and 日志来源 = 云等保专区	0	2024-11-08 09:51:40	

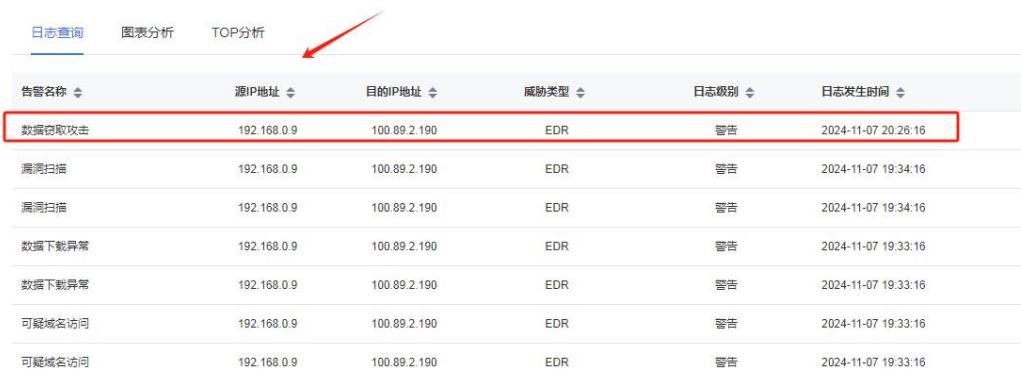
- 停用标签规则，规则失效，日志不匹配标签规则。



	有效期	标签	内容	命中次数	创建时间	停用状态
<input type="checkbox"/>	永久有效	白名单	源IP地址 = 192.168.0.9 and 目的IP地址 = 100.89.2.190 and 威胁类型 = EDR and 日志来源 = 云等保专区	0	2024-11-08 09:51:40	

从日志添加标签规则

- 登录云安全中心控制台。
- 在左侧导航栏选择“设置 > 规则标签配置”。
- 在日志查询列表找到需要添加标签的日志，点击日志。



日志查询	图表分析	TOP分析
告警名称	源IP地址	目的IP地址
数据窃取攻击	192.168.0.9	100.89.2.190
漏洞扫描	192.168.0.9	100.89.2.190
漏洞扫描	192.168.0.9	100.89.2.190
数据下载异常	192.168.0.9	100.89.2.190
数据下载异常	192.168.0.9	100.89.2.190
可疑域名访问	192.168.0.9	100.89.2.190
可疑域名访问	192.168.0.9	100.89.2.190

- 在日志详情页，单击白名单按钮。



查看详情

点击白名单按钮

基本信息

威胁详情

原始信息

X

日志来源	云等保专区	进程路径	123
厂商	云等保	安全服务编号	platform-c
产品	主机安全	登录账号	cm9vdA==
公有云租户ID	1ff24e947fb4af9a66a48f66591b5a6		
协议	TCP	动作	已拦截
日志级别	警告	事件类型名称	全局事件
告警名称	数据窃取攻击	日志发生时间	2024-11-07 20:26:16
服务ID	2183	威胁类型	EDR

| 五元组

源IP地址	192.168.0.9
源端口	58164
目的IP地址	100.89.2.190 共享地址/共享地址/()

5. 在弹出的新增窗口中，配置标签、匹配条件、有效期、备注信息。参数配置完成后，单击“保存”。

新增 选择对应标签 X

* 标签 白名单 测试标签 +

* 匹配条件 源IP地址 = 192.168.0.9 and 目的IP地址 = 100.89.2.190 and 威胁类型 = EDR and 日志来源 = 云等保专区

有效期 开始日期 至 结束日期

* 备注 test 点击保存

取消 保存

查看日志的标签

1. 登录云安全中心控制台。
2. 在左侧导航栏选择“设置 > 规则标签配置”。
3. 在日志查询列表的“规则标签”列，可以查看日志的标签。

日志查询	图表分析	TOP分析				
源IP地址	目的IP地址	威胁类型				
警告	139.200.108.9	47.109.21.183	ALARM	致命	2024-11-04 15:15:30	规则标签
警告	139.200.108.9	47.109.21.183	ALARM	致命	2024-11-04 15:14:30	[“测试标签”]
警告	139.200.108.9	47.109.21.183	ALARM	致命	2024-11-04 15:13:30	[“测试标签”]
警告	139.200.108.9	47.109.21.183	ALARM	致命	2024-11-04 09:31:30	[“测试标签”]

4. 在日志查询列表找目标日志，点击日志。



5. 在日志详情页的基本信息中，可以看到“规则标签”。

查看详情 X

基本信息 威胁详情 原始信息 导出

规则标签	<input type="checkbox"/> <input checked="" type="checkbox"/> [测试标签]	日志来源	<input type="checkbox"/> <input checked="" type="checkbox"/> Web应用防火墙 (原生版)
安全服务编号	<input type="checkbox"/> <input checked="" type="checkbox"/> waf		
公有云租户ID	<input type="checkbox"/> <input checked="" type="checkbox"/> 1ff24e947bfb4af9a66a48f66591b5a6		
攻击类型	22	动作	拦截
日志级别	<input type="checkbox"/> <input checked="" type="checkbox"/> 警告	事件类型名称	全局类型(内置)
告警名称	<input type="checkbox"/> <input checked="" type="checkbox"/> Web应用防火墙 (原生版) 告警		
注入规则ID	<input type="checkbox"/> <input checked="" type="checkbox"/> -6b139e43c9ca456a9b9be04bc4c9694c		
日志发生时间	2024-11-04 15:15:30	威胁类型	<input type="checkbox"/> <input checked="" type="checkbox"/> ALARM

五元组

源IP地址	139.200.108.9 中国/四川/宜宾 (104.16293/28.64369) (电信)
目的IP地址	47.109.21.183 中国/四川/成都 (104.06151/30.67387) (阿里云/电信/联通/移动/教育网)
目的端口	<input type="checkbox"/> <input checked="" type="checkbox"/> 8090

4.10. 查看审计事件

支持审计的操作列表

事件名称	读写类型
资产管理-资产导入模板下载	写类型
资产管理-资产导入	写类型
告警管理-工单处置-小结-上传文件	写类型
资产管理-资产导出	读类型
分析中心-图表分析-导出	读类型
告警管理-工单处置-小结-下载文件	读类型

查看云审计事件

1. 登录云审计产品控制台，默认进入云审计事件列表页面。
2. 事件来源选择“安全”，资源类型选择“云安全中心”，单击“查询”，筛选云安全中心事件。



防护事件 帮助文档

The screenshot shows the 'Event Protection' section of the WingCloud management console. At the top, there are time range selection buttons: '近30分钟' (Last 30 Minutes), '近一小时' (Last Hour), '近一天' (Last Day), '近七天' (Last 7 Days) (which is highlighted in blue), and '自定义时间段' (Custom Time Range). Below this is a '筛选条件' (Filter Conditions) section with dropdown menus for '读写类型' (Read/Write Type), '事件级别' (Event Level), '操作用户' (Operator User), '事件来源' (Event Source) (set to '安全' (Security)), '资源类型' (Resource Type) (set to '云安全中心' (Cloud Security Center)), and '资源筛选' (Resource Filter) (set to '所有筛选类型' (All Filter Types)). There are also '查询' (Search) and '重置' (Reset) buttons. The main area displays a table of event logs.

3. 在需要查看的事件左侧，单击 展开该事件的详细信息。

事件级别	事件名称	事件来源	资源类型	资源名称	资源ID	事件时间	操作
▼	资产管理-资产导入模...	安全	云安全中心	云安全中心	-	2025-03-03T17:17:57.570	查看详情
	事件ID d7ef06dfd34a4a6a8e26f701e660e5ca		请求ID		来源IP		
	操作用户		主账号ID				

4. 在需要查看的事件右侧，单击操作列的“查看详情”，弹出一个窗口显示该操作事件结构的详细信息。

事件详情

```
{  
    "id": "d7ef06dfd34a4a6a8e26f701e660e5ca",  
    "eventName": "资产管理-资产导入模板下载",  
    "eventTime": "2025-03-03T17:17:57.570",  
    "eventLevel": {  
        "code": "null",  
        "value": ""  
    },  
    "eventType": {  
        "code": "0",  
        "value": "API调用事件 (ApiCall)"  
    },  
    "eventActType": {  
        "code": "1",  
        "value": "写类型"  
    },  
    "srcRegion": "all",  
    "srcServiceType": "安全",  
    "srcProdTypeName": "云安全中心",  
    "srcProdName": "云安全中心",  
    "userId": "",  
    "accountId": "",  
    "reqData": "/business/assetManage/templateDownload",  
    "createTime": "2025-03-03T17:17:57.739",  
    "updateTime": "2025-03-03T17:17:57.739",  
    "subUserEmail": ""  
}
```

5. 最佳实践

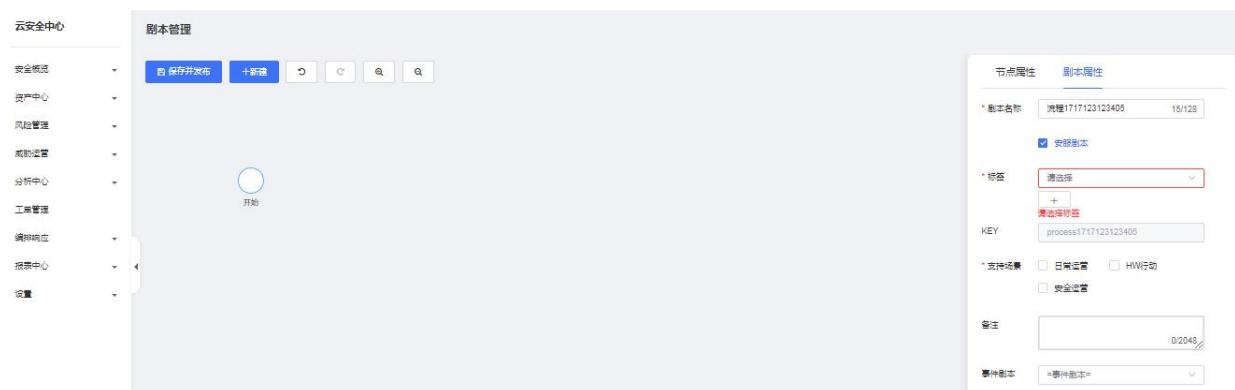
5.1. 如何进行剧本管理

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。



The screenshot shows the 'Script List' page within the Cloud Security Center. On the left is a sidebar with various security modules like 'Security Overview', 'Asset Center', 'Risk Management', etc. The main area has a search bar at the top with dropdowns for 'Script Tag' (请选择), 'Script Name' (请输入), and 'Script Type' (请选择). Below the search bar are buttons for 'New' (新建), 'Delete' (删除), 'Import' (导入), and 'Export' (导出). The main table lists two scripts: '01租户剧本' (Public Cloud Version) and '流程1716904531204' (Public Cloud Version). Each row includes columns for 'Script Name', 'Script Tag', 'Script Type', 'Scenario Name', 'Trigger Count', 'Create Time', 'Update Time', 'Status', and 'Operations'. At the bottom right, there are pagination controls showing '20条/页' (20 items per page), '1' (page 1), and '1' (total pages).

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。



The screenshot shows the 'New Script' creation page. The left sidebar is identical to the previous screenshot. The main area has a 'Save and Publish' (保存并发布) button and a 'Create' (新建) button. A circular 'Start' (开始) node icon is shown. On the right, the 'Script Properties' (剧本属性) section is visible. It includes fields for 'Script Name' (请输入, e.g., '流程1717123123405'), 'Tag' (请选择标签, e.g., 'process1717123123405'), 'KEY' (KEY), 'Support Scenario' (支持场景: 日常运营, HW行动, 安全运营), 'Remarks' (备注: 0/2048), and 'Script Description' (剧本描述: "事件剧本").

说明：

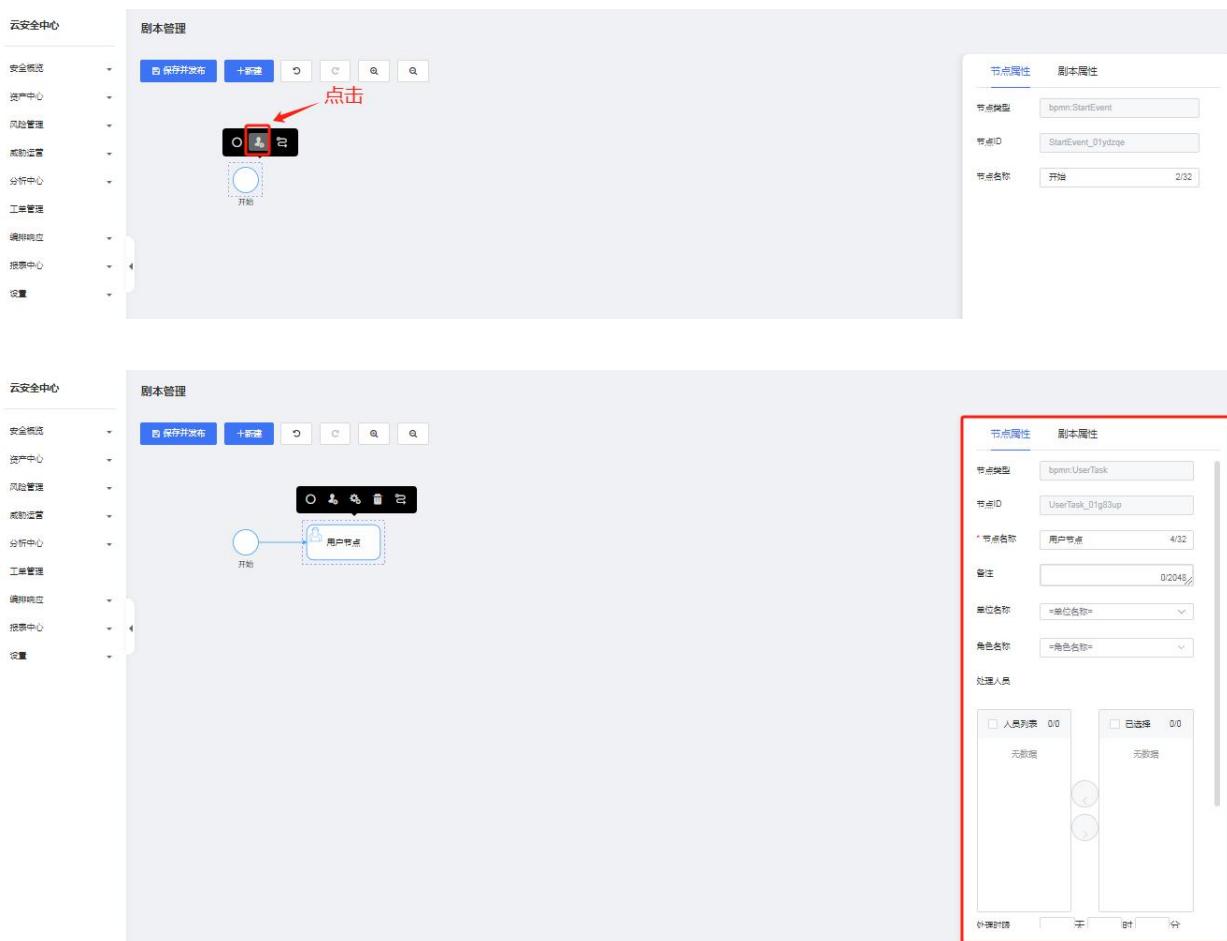
一个剧本有且只有一个开始节点和结束节点。

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”当前告警工单的剧本执行。

剧本编辑界面如图所示。



云安全中心

剧本查看

另存为新剧本

开始 -> 用户节点 -> 发送短信 -> 结束

节点属性

角色名称: #角色名称#

处理人员

人员列表: 0/0 无数据 已选择: 0/1 chenwen

处理时限: 1 天 时 分

是否允许终止: 允许 不允许

是否允许回退: 允许 不允许

检验工具: 检验工具

采集数据: +

云安全中心

告警 处置 作战室 实战剧本 关联事件 小结

111.117.106.197对172.17.0.2触发告警，攻击类型为XSS攻击

攻击阶段: 【恢复】

发生时间: 2024-05-29 17:50:34

外部威胁IP:

完成时间: 2024-05-31 23:28:28

处置建议:

工单处置

用户节点 处置意见

当前剩余: 1天0小时0分钟 0:255

终止执行 确定

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，在告警管理列表和告警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。

云安全中心

剧本查看

另存为新剧本

开始 -> 用户节点 -> 发送短信 -> 结束

节点属性

备注: 0:2048

单位名称: sec2208001@163.com

角色名称: #角色名称#

处理人员

人员列表: 0/0 无数据 已选择: 0/1 chenwen

处理时限: 1 天 时 分

是否允许终止: 允许 不允许

是否允许回退: 允许 不允许

云安全中心

工单管理

搜索框：请输入事件名或客户IP
筛选：待办、处置中、处置完成、自动处置、紧急处置
操作：新建、读取、重置、忽略

当期环节		当前状态	完成时间	剩余时间	操作
环节名	完成时间	剩余时间			
用户节点(chenwen)	2024-05-01 11:28:29	0天21小时	待执行	2024-05-31 23:28:28	0天0小时
			待处置		

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

云安全中心

剧本管理

操作按钮：暂存并发布、+新建、

右侧节点属性：

- 节点类型：bpmn:UserTask
- 节点ID：UserTask_01g33up
- 节点名称：用户节点 432
- 备注：0/208/
- 单位名称：sec22080001@163.com
- 角色名称：角色名称
- 处理人员：
 - 人员列表：01 chenwen
 - 已选择：00 无数据
- 处理时间：天 时 分
- 是否允许终止：允许 不允许
- 是否允许调用：允许 不允许



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

云安全中心

剧本管理

操作按钮：暂存并发布、+新建、

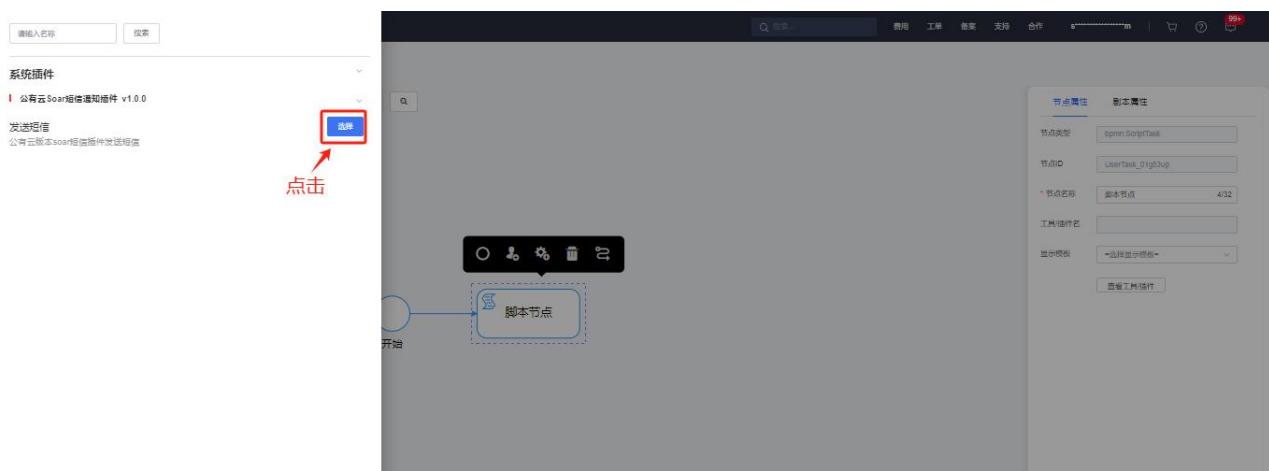
右侧节点属性：

- 节点类型：bpmn:ScriptTask
- 节点ID：UserTask_01g33up
- 节点名称：脚本节点 432
- 工单插件名：公有云Scan跑完流程后操作脚本
- 租户ID：
- 手机号：
- 通知类型：
- 通知消息：
- 调用服务：01角色
- 显示模板：选择显示模板

下方工具栏：查看工具/插件、



7、可通过插件选取栏搜索相关插件或直接选取



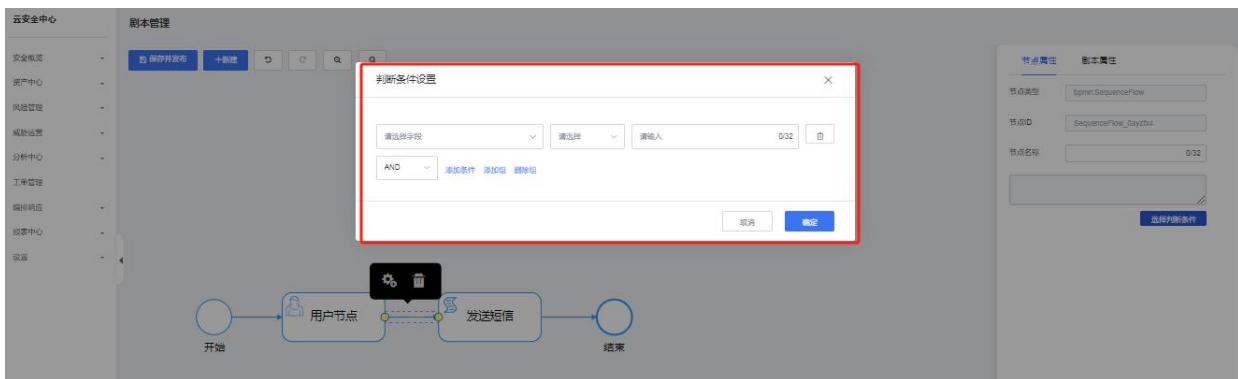
8、选取完插件后，设置插件的入参



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。

云安全中心

漏洞管理

漏洞名称: 漏洞等级: CVE编号:

忽略 修复中 已修复 已加固

	漏洞名称	CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	操作
忽略	高危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看		
忽略	高危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看		
忽略	高危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看		
忽略	中危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 待修复 已加固 查看		
忽略	低危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 待修复 已加固 查看		
忽略	高危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-02-20 11:15:27	2024-03-11 11:15:17	修复中 待修复 已加固 查看		
忽略	高危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 待修复 已加固 查看		
忽略	低危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-01-09 11:15:27	2024-03-11 11:15:17	忽略 待修复 已加固 查看		
忽略	中危	待修复	ecm-cehoff825d35f-17fe-3162-0e68...	2024-03-01 11:15:27	2024-03-11 11:15:17	忽略 修复中 待修复 已加固 查看		

2、支持条件查询，用户输入或选择相关条件内容



云安全中心

漏洞管理

输入或选择相关条件内容

点击

The screenshot shows the 'Vulnerability Management' section of the Tianyi Cloud Security Center. It includes search fields for 'Vulnerability Name', 'CVE Number', 'Server', 'Severity' (High), and 'Disposal Status'. A red box highlights the search area, and arrows point to the search button and the results table. The results table lists vulnerabilities with columns for Name, CVE Number, Severity, Disposal Status, Server, Last Discovery Time, Update Time, and Operation. The status column uses color-coded icons: green for '已加固' (加固), yellow for '已修复' (修复), and red for '忽略' (Ignore). The operation column contains links for 'View' and 'Edit'.

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。

云安全中心

漏洞管理

批量处置

单个处置

This screenshot shows the 'Vulnerability Management' interface with a 'Batch Disposal' section highlighted by a red box. It includes checkboxes for selecting multiple vulnerabilities and a 'Disposal Status' dropdown. The main table lists vulnerabilities with columns for Name, CVE Number, Severity, Disposal Status, Server, Last Discovery Time, Update Time, and Operation. A red box highlights the 'Operation' column, which shows various disposal actions like '忽略' (Ignore), '修复中' (Repairing), '已修复' (Repaired), and '已加固' (Strengthened). The right side of the table has a 'Single Disposal' section with a list of disposal actions for each row.

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

漏洞 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
名称_5	CVE_2024_5	ecm-ceshf825d35f-17fe-3162-0e68-d10676d09b781.1.1.5

处置说明: 最多可输入255个字符

操作
49 忽略 修复中 已修复 查看
03 修复中 已修复 已加固 查看
48 忽略 修复中 已修复 查看
33 忽略 修复中 已修复 查看
20 忽略 修复中 已修复 已加固 查看
修重中 已修复 已加固 查看
忽略 修复中 已修复 查看
忽略 修复中 已修复 查看
忽略 修复中 已修复 查看
忽略 修复中 已修复 查看

云安全中心 漏洞管理

漏洞名称: 漏洞等级: CVE编号:

点击

操作	修复中	已修复	已加固
名称_5 CVE_2024_5 高危 *忽略 ecm-ceshf825d35f-17fe-3162-0e68... 2024-03-11 11:15:27 2024-03-15 10:43:47 忽略 修复中 已修复 查看			
名称_4 CVE_2024_4 中危 *修复中 ecm-ceshf825d35f-17fe-3162-0e68... 2024-03-11 11:15:27 2024-03-15 10:43:43 忽略 修复中 已修复 查看			
名称_5 CVE_2024_5 高危 *已加固 ecm-ceshf825d35f-17fe-3162-0e68... 2024-03-11 11:15:27 2024-03-15 10:43:35 忽略 修复中 已修复 查看			
名称_5 CVE_2024_5 低危 *已加固 ecm-ceshf825d35f-17fe-3162-0e68... 2024-03-11 11:15:27 2024-03-15 10:43:35 忽略 修复中 已修复 查看			
名称_5 CVE_2024_5 高危 *已加固 ecm-ceshf825d35f-17fe-3162-0e68... 2024-03-11 11:15:27 2024-03-15 10:43:35 忽略 修复中 已修复 查看			

云安全中心 漏洞管理

漏洞名称: 漏洞级别:

处置说明:

处置人	处置状态	处置说明	处置时间
超级管理员	*已修复	22222	2024-03-12 18:25:45
超级管理员	*修复中	11111	2024-03-12 18:25:36
超级管理员	*已修复	批量测试修复中	2024-03-12 17:29:17
超级管理员	*已修复	批量测试修复中	2024-03-12 17:28:07
超级管理员	*修复中	批量处置修复中	2024-03-12 17:27:42
超级管理员	*忽略		2024-03-12 17:26:25



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。

The screenshot illustrates the integration between the Vulnerability Management and Asset Details pages in the WingCloud Cloud Security Center.

Vulnerability Management Page: This page lists vulnerabilities across various assets. A specific row for a host named "ecm-ceshi" is highlighted with a red box and a red arrow pointing to it from the text above. The table includes columns for Vulnerability Name, CVE Number, Severity, Status, Server, Last Discovery Time, Update Time, and Operations.

漏洞名称	CVE编号	漏洞等级	处置状态	服务器	最后发现时间	更新时间	操作
... (highlighted)	... (highlighted)	高危	已加固	ecm-ceshi b25d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-06-21 15:22:49	忽略 修复中 已修复 查看
... (highlighted)	... (highlighted)	高危	忽略	主机名 b5825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-06-21 14:58:03	修复中 已修复 已加固 查看
... (highlighted)	... (highlighted)	高危	已加固	主机名 b5825d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-06-21 14:53:48	忽略 修复中 已修复 查看
... (highlighted)	... (highlighted)	高危	忽略	ecm-ceshi b25d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-15 10:43:47	修复中 已修复 已加固 查看
... (highlighted)	... (highlighted)	高危	已加固	ecm-ceshi b25d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-15 10:43:35	忽略 修复中 已修复 查看
... (highlighted)	... (highlighted)	高危	已修复	ecm-ceshi b25d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
... (highlighted)	... (highlighted)	高危	已修复	ecm-ceshi b25d35f-17fe-3162-0e68-...	2024-03-05 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
... (highlighted)	... (highlighted)	高危	已修复	ecm-ceshi b25d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-12 18:25:45	忽略 修复中 已加固 查看
... (highlighted)	... (highlighted)	高危	待修复	ecm-ceshi b25d35f-17fe-3162-0e68-...	2024-03-11 11:15:27	2024-03-11 11:15:17	忽略 修复中 已修复 已加固 查看

Asset Details Page: This page provides detailed information about the selected asset, "ecm-ceshi". The "Basic Information" tab is active, displaying details such as Host ID, OS, Creation Time, and Location.

基本信息	资产ID	资产状态	资产位置
主机ID: ab9fbafe-76d2-4eeb-b021-b753aaeddef6	主机名: ecm-ceshi	资产状态: 运行中	虚拟私有云名称: vpc-osm-ceshi
操作系统: linux	操作系统版本:	...	地域:
云资源创建时间: 2024-06-18 01:04:30	云资源到期时间: 2024-07-18 01:05:37	可用区: default	

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。

The screenshot shows the Asset Management page under the Asset Center section. The left sidebar highlights the "Asset Management" section. The main area displays a table of assets with columns for Cloud Resource Creation Time, Cloud Resource Expiry Time, Whether it is equipped with a security卫士 (Security Agent), Asset Status, Host Name, Security Agent Status, Asset Importance, and Operations.

风险管理	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	安全卫士agent是否在线	资产重要性	操作
威胁运营	2024-06-12 10:09:22	2024-07-12 10:09:34	运行中	ctcss-stab-j9R			查看	
分析中心	2024-06-12 16:10:31	2024-07-12 16:10:46	运行中	ctcss-stab-x44			查看	
工单管理	2024-06-12 16:11:40	2024-07-12 16:11:51	运行中	ctcss-stab-7g4			查看	
编排响应	2024-04-18 14:43:35	2024-07-18 14:43:50	运行中	ctcss-lab-centos7-a618			查看	
报表中心	2024-04-18 14:47:14	2024-07-18 14:47:26	运行中	ctcss-lab-ubuntu18-4e70			查看	
已购资源	2024-06-12 16:16:21	2024-07-12 16:16:32	运行中	ctcss-stab-pv			查看	
设置	2024-06-12 16:12:49	2024-07-12 16:12:59	运行中	ctcss-stab-W5s			查看	
	2024-06-12 16:15:06	2024-07-12 16:15:19	运行中	ctcss-stab-9sJ			查看	



2、选择常用搜索项查询。

The screenshot shows the 'Asset Management' section of the 'Cloud Security Center'. On the left, there's a sidebar with categories like 'Cloud Security Center', 'Overview', 'Assets', 'Risk Management', 'Incident Response', 'Report Center', 'Purchased Resources', and 'Settings'. The main area has a title 'Asset Management' and a search bar with placeholder text '常用搜索项:'. Below the search bar is a row of filters: '主机名称' (Host Name), '资产状态' (Asset Status), '是否安装安全卫士' (Is Security Guardian Installed), '安全卫士agent是否在线' (Is Security Guardian Agent Online), and '资产重要性' (Asset Importance). A red arrow labeled '1.点击搜索框' points to the search bar. Another red arrow labeled '2.选择搜索项' points to the filter row.

This screenshot shows the same 'Asset Management' interface after applying the search criteria from the previous step. The search bar now contains the value '主机名称 = *ecm-ceshi*'. A red arrow labeled '3.输入相关搜索内容' points to the search bar. Another red arrow labeled '点击【查询】按钮' points to the blue 'Query' button on the right side of the search bar. The table below shows the results of the search, listing various hosts with their details and status.

3、选择常用时间查询。



云安全中心 资产管理

点击“日历”图标
选择“时间”

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	安全卫士
2024-06-18 01:07:41	2024-07-18 01:07:51	运行中	ecm-ceshi	ecm-aem-ceshi	从
2024-06-18 01:13:16	2024-07-18 01:13:27	运行中	VM-b889b4b1	VM-1321844f	至
2024-06-18 17:50:44	2024-07-18 17:50:58	运行中	VM-3bd4041a	ctcss-test-KxZ3	结束日期
2024-06-18 17:50:44	2024-07-18 17:50:57	运行中	proxy	tcpserver	全部
2024-06-18 17:49:08	2024-08-18 17:49:21	运行中	client	ctcss-test-mq	今天
2024-06-18 17:49:08	2024-08-18 17:49:20	运行中	ycdl-5	ycdl-5	最近7天
2024-06-20 20:08:57		运行中			最近30天
2024-06-20 19:02:02		运行中			全部
2024-06-20 19:53:05		运行中			
2024-06-12 14:39:18		运行中			
2024-06-02 17:13:09	2024-07-02 17:13:41	运行中			
2024-05-14 15:41:17		运行中			

常用时间：今天、最近7天、最近30天、全部
开始日期：2024-06-21
结束日期：2024-07-31
共 82 条 1 2 3 4 5 > 20条/页

4、选择时间段查询。

云安全中心 资产管理

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	安全卫士
2024-06-18 01:07:41	2024-07-18 01:07:51	运行中	ecm-ceshi	ecm-aem-ceshi	从
2024-06-18 01:13:16	2024-07-18 01:13:27	运行中	VM-b889b4b1	VM-1321844f	至
2024-06-18 17:50:44	2024-07-18 17:50:58	运行中	VM-3bd4041a	ctcss-test-KxZ3	结束日期
2024-06-18 17:50:44	2024-07-18 17:50:57	运行中	proxy	tcpserver	全部
2024-06-18 17:49:08	2024-08-18 17:49:21	运行中	client	ctcss-test-mq	今天
2024-06-18 17:49:08	2024-08-18 17:49:20	运行中	ycdl-5	ycdl-5	最近7天
2024-06-20 20:08:57		运行中			最近30天
2024-06-20 19:02:02		运行中			全部
2024-06-20 19:53:05		运行中			
2024-06-12 14:39:18		运行中			
2024-06-02 17:13:09	2024-07-02 17:13:41	运行中			
2024-05-14 15:41:17		运行中			

常用时间：今天、最近7天、最近30天、全部
开始日期：2024-06-21
结束日期：2024-07-31
日历选择：2024年6月 21日
日历选择：2024年7月 31日
共 82 条 1 2 3 4 5 > 20条/页

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

资产概览

资产管理

风险管理

威胁运营

分析中心

工单管理

编排响应

报表中心

已购资源

设置

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

查看

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-b889b4b1

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

ctoss-test-mq

查看

2024-06-02 17:13:09

2024-07-02 17:13:41

运行中

yndl-5

查看

2024-05-14 15:41:17

运行中

ctoss-test-KxZ3

查看

共 75 条 < 1 2 3 4 > 20条/页

点击

查询

重置

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

新建

云安全中心

资产管理

资产概览

资产管理

风险管理

威胁运营

分析中心

工单管理

编排响应

报表中心

已购资源

设置

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

查看

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-b889b4b1

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

ctoss-test-mq

查看

2024-06-02 17:13:09

2024-07-02 17:13:41

运行中

yndl-5

查看

2024-05-14 15:41:17

运行中

ctoss-test-KxZ3

查看

共 75 条 < 1 2 3 4 > 20条/页

点击

新建

查询

重置

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



云安全中心 资产管理

资产概览

资产中心

资产概览

资产管理

风险管理

威胁运营

分析中心

工单管理

编排响应

报表中心

已购资源

设置

云资源创建时间 云资源到期日

主机名称 = *ecm-ceshi*

添加条件

保存查询条件组

查询条件组名称: test

描述:

是否保存查询条件:

是否保存查询时间:

输入和选择对应条件

取消 保存

安全卫士agent是否在线 资产重要性 操作

安全卫士	资产状态	主机名称	安全卫士agent是否在线	资产重要性	操作
ceshi	运行中	ecm-ceshi	运行中	高	查看
b1	运行中	VM-b985b4b1	运行中	高	查看
4f	运行中	VM-1321844f	运行中	高	查看
1a	运行中	VM-3bd4041a	运行中	高	查看
ac	运行中	proxy	运行中	高	查看
	运行中	tcpserver	运行中	高	查看
	运行中	client	运行中	高	查看
	运行中	ctcss-test-mq	运行中	高	查看
	运行中	yodl-5	运行中	高	查看
	运行中	ctcss-test-kxZ3	运行中	高	查看

共 75 条 < 1 2 3 4 > 20条/页

6、添加条件查询。



云安全中心 资产管理

资产概览

资产中心

资产概览

资产管理

风险管理

威胁运营

分析中心

工单管理

编排响应

报表中心

已购资源

设置

* 域 操作

资产状态 =

添加条件

最近7天

搜索 重置

安全卫士 资产状态 主机名称 安全卫士agent是否在线 资产重要性 操作

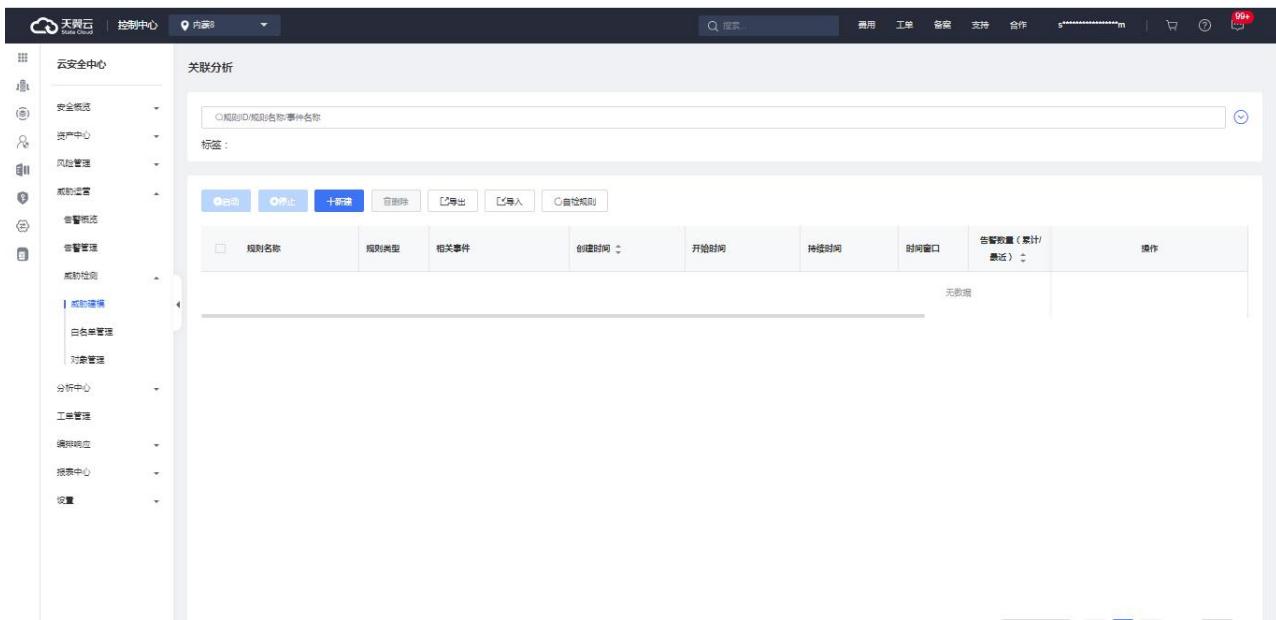
安全卫士	资产状态	主机名称	安全卫士agent是否在线	资产重要性	操作
ceshi	运行中	ecm-ceshi	运行中	高	查看
b1	运行中	ecm-osm-ceshi	运行中	高	查看
4f	运行中	VM-b985b4b1	运行中	高	查看
1a	运行中	VM-1321844f	运行中	高	查看
ac	运行中	VM-3bd4041a	运行中	高	查看
	运行中	proxy	运行中	高	查看
	运行中	tcpserver	运行中	高	查看
	运行中	client	运行中	高	查看
	运行中	ctcss-test-mq	运行中	高	查看
	运行中	yodl-5	运行中	高	查看

共 82 条 < 1 2 3 4 5 > 20条/页

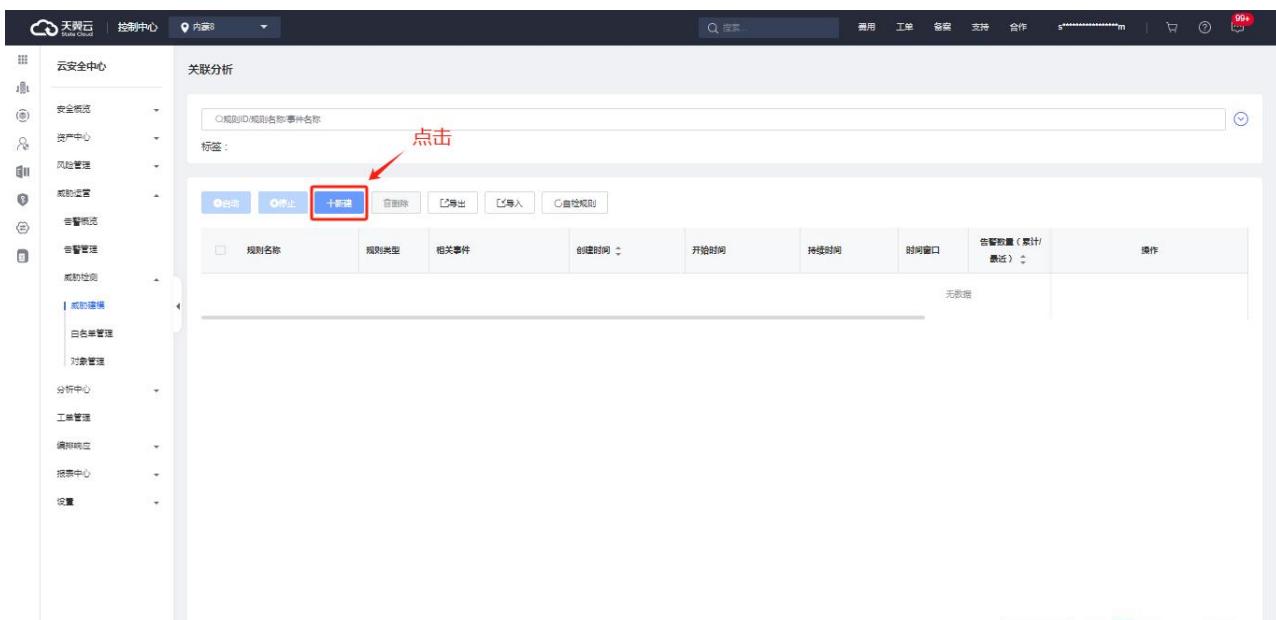
5.4. 如何进行威胁建模

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



控制中心 | 内容8 | 搜索 | 费用 工单 备案 支持 合作 | 99+

云安全中心 | 关联分析规则配置

基本信息

- * 规则名称: test
- 规则描述: 流输入
- * 规则类型: 异常检测
- * 规则模板: 普通模板
规则模板简述: 普通模板, 用于基于单个属性的事件名称转换。
- 标签: 流告警类型

原始告警源

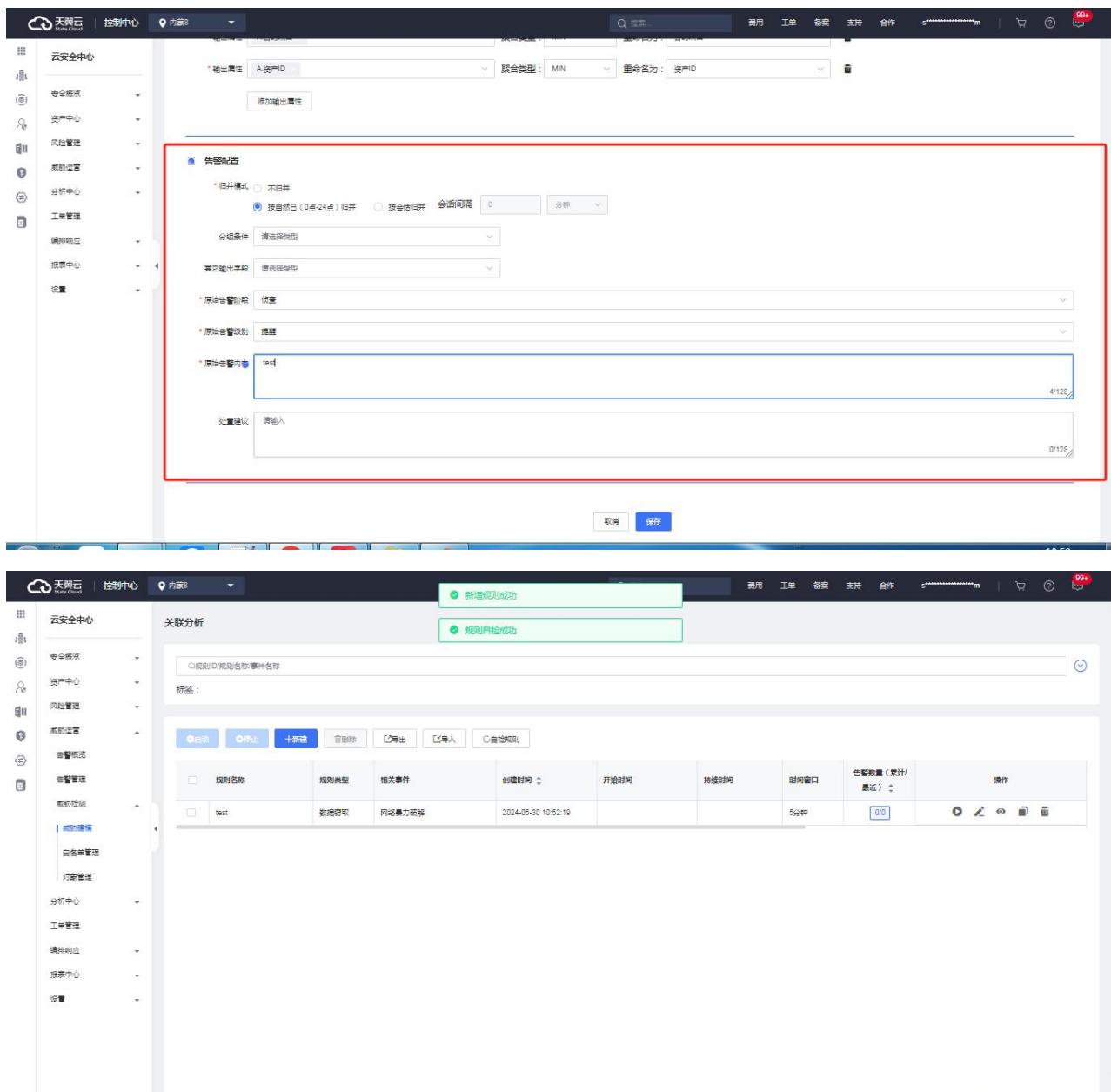
- * 事件名称A: 网络暴力报警 过滤条件: 无

输出结果

- * 输出属性 A 日志ID 聚合类型: 组合 重命名为: 告警关联日志ID
- * 输出属性 A 日志发生时间 聚合类型: MIN 重命名为: 告警开始时间
- * 输出属性 A 日志发生时间 聚合类型: MAX 重命名为: 告警结束时间
- * 输出属性 A 源IP地址 聚合类型: MIN 重命名为: 源IP地址
- * 输出属性 A 源端口 聚合类型: MIN 重命名为: 源端口
- * 输出属性 A 目的IP地址 聚合类型: MIN 重命名为: 目的IP地址
- * 输出属性 A 目的端口 聚合类型: MIN 重命名为: 目的端口
- * 输出属性 A 资产ID 聚合类型: MIN 重命名为: 资产ID

告警配置

- * 归并模式: 按自然日 (0点-24点) 归并 按会话归并 会话间隔: 0 分钟



The screenshot displays two main sections of the Tianyi Cloud Security Center:

- Top Section (Rule Configuration):** A red box highlights the "告警配置" (Alert Configuration) section. It includes fields for "输出属性" (Output Properties), "聚合类型" (Aggregation Type: MIN), and "聚合名称" (Aggregation Name: 资产ID). Below this are settings for "归并模式" (Merge Mode: 自然日 (0点-24点) 归并), "分组条件" (Grouping Conditions), and "其它输出字段" (Other Output Fields). The "原始告警级别" (Original Alert Level) is set to "低级" (Low), and the "原始告警内容" (Original Alert Content) field contains "test". The "处置建议" (Disposal Suggestion) field is empty.
- Bottom Section (Analysis Results):** This section shows the results of a rule analysis. It includes a "规则ID/规则名称/事件名称" (Rule ID/Rule Name/Event Name) search bar, a "标签" (Label) input field, and a toolbar with buttons for "启动" (Start), "停止" (Stop), "加载" (Load), "删除" (Delete), "导出" (Export), "导入" (Import), and "自动规则" (Automatic Rule). Below these are two green success messages: "新增规则成功" (Rule added successfully) and "规则自检成功" (Rule self-inspection successful). A table lists rules, showing one entry: "test" (Rule Name), "数据窃取" (Rule Type), "网络暴力数据" (Related Event), "2024-05-30 10:52:19" (Create Time), and "0分钟" (Duration).

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	插件管理、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	插件管理、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	插件管理、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	插件管理、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	插件管理、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，记录包括相关告警的日期和时间、用户、告警类型、告警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	插件管理、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，记录包括相关告警的日期和时间



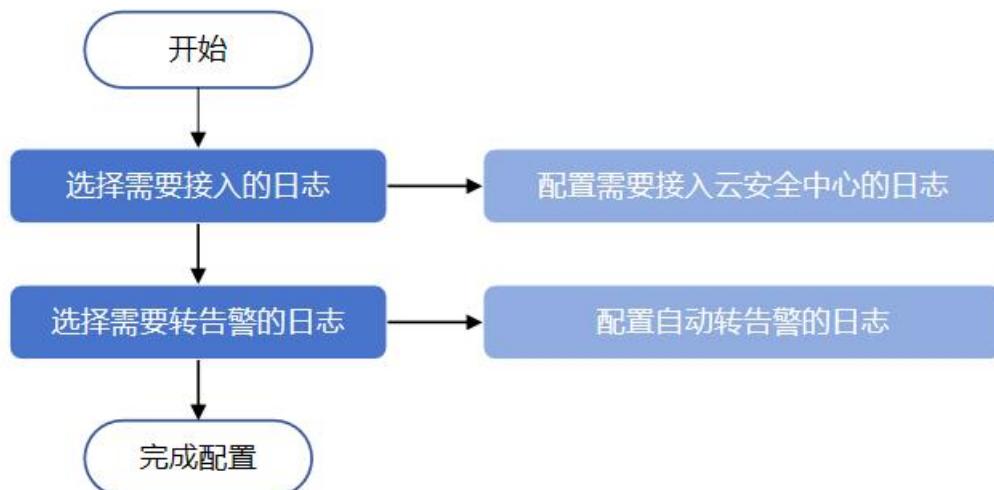
等保标准章节	等保标准序号	云安全中心对应功能	功能解读
			、用户、告警类型、告警是否成功及其他与审计相关的信息。云安全中心日志通过多副本实时存储多分，保障用户日志在其存储周期内不丢失、可恢复
安全计算环境-入侵防范	8.1.4.4	插件管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞，同时应能够检测到对重要节点进行入侵的行为，并在发生严重入侵时提供报警
安全计算环境-恶意代码防范	8.1.4.5	插件管理、威胁运营、编排响应	云安全中心通过获取 WAF、防火墙以及安全卫士等日志数据，能够及时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	插件管理、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
			<p>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；</p> <p>通过编排响应能对网络中发生的各类安全告警进行识别、报警和分析；</p>

5.6. 如何接入产品日志、告警

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，可以直接受到转告警开关，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. 选择“设置 > 数据源监控”，打开数据源监控页面。
2. 在操作列点击“启用”，确保数据源监控处于启用状态。





3. 选择“设置 > 集成配置”，打开数据集成配置页面。
4. 选择需要接入的日志，并打开日志接入开关。

集成配置					
安全服务	日志类型	状态	日志接入	自动转告警	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		未接入	<input type="checkbox"/>	<input type="checkbox"/>	

5. 选择需要转告警的日志，并打开自动转告警的开关。

集成配置					
安全服务	日志类型	状态	日志接入	自动转告警	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		已接入	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		未接入	<input type="checkbox"/>	<input type="checkbox"/>	

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。
- 需要先在数据源监控页面启用开关后，才可以在集成配置页面中开启日志和告警配置。
- 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。

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：云安全中心提供的插件管理、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告警日志，包括服务器安全卫士、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

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	10000 条/月	50G/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）。

Q: 如何查看当前购买产品的规格

A: 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”。

云安全中心

产品信息

云安全中心 (标准版) • 包周期: 付费方式

到期时间: 2024-09-06 00:35:48 (距离到期还有22天)

续订

态勢大屏

实时、可视化地监控和分析网络安全态势，提供全面的安全威胁信息和预警，助力用户快速响应和处置告警。

日志分析量

云安全中心免费为您提供每月 50G 的日志分析额度，如果您需要额外的额度，请[另外购买](#)。

已使用(GB) | 剩余量(GB)

0 | 100

购买日志分析量

100%

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 > 威胁检测 > 威胁建模”功能实现自定义告警配置。

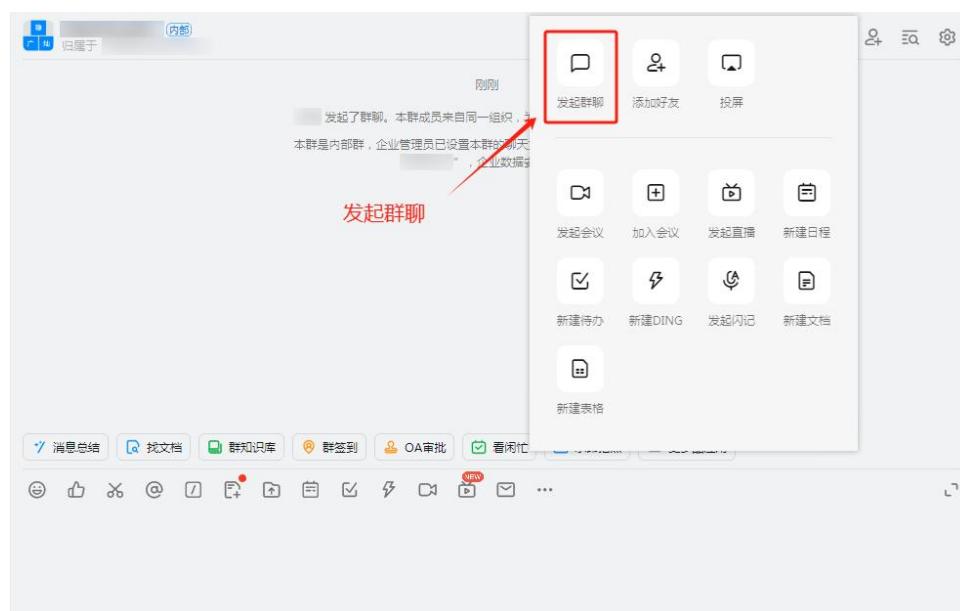
6.3.2. 告警通知相关

Q: 如何获取钉钉机器人的 token 和 secret?

1. 进入钉钉选择组织团队



2. 发起群聊

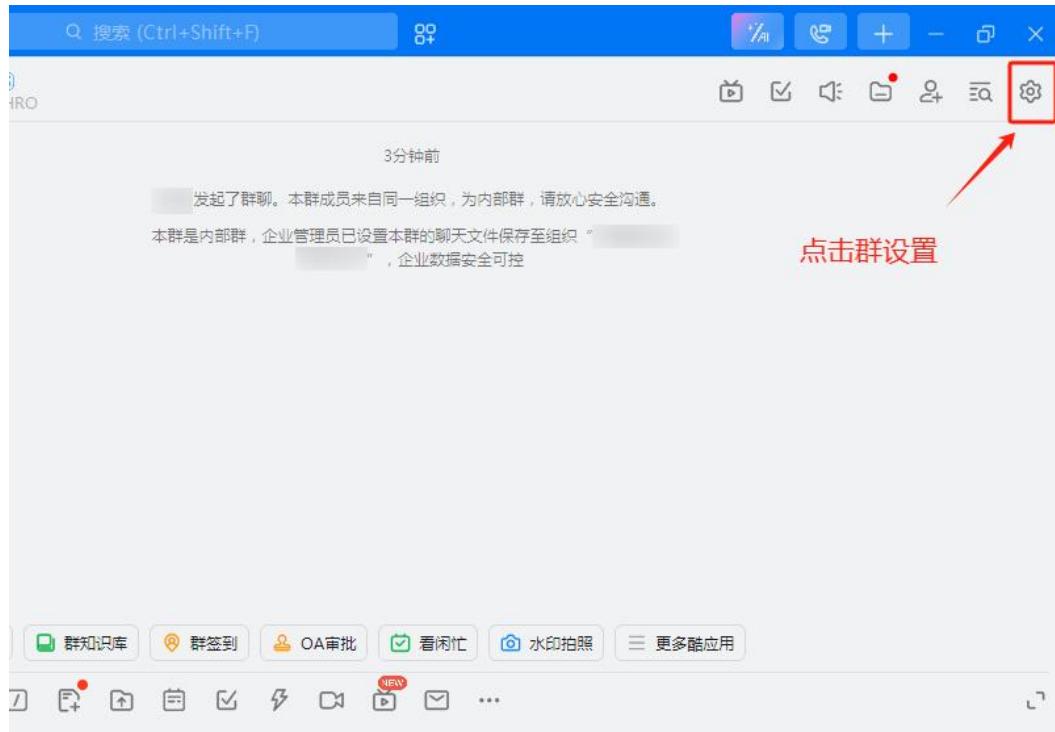




3. 创建群聊



4. 点击群设置



5. 下拉点击机器人



群设置

AI实时翻译 >

群管理

群类型 内部群 >

机器人 1 >

机器人具备丰富的技能，让沟通协同更智能高效

第三方密盾加密 未开通 >

其他功能

标签 未设置 >

清空聊天记录

退出群聊

解散该群

6. 点击添加机器人

小钉 钉钉官方机器人，提供丰富的技能 >

已开启的技能

日程提醒 投票提醒 群汇报

添加机器人 多款丰富的精选机器人 >

热门推荐

自动化小助手 智能联通不同应用，让工作自动完成 添加至本群 查看使用场景

【AI藏头诗】 新人入群时，自动写AI藏头诗欢迎
④ 自动化小助手 欢迎新人！快来查看AI为你创作的专属藏头诗：
谦谦君子温润如玉，夏花烂漫笑语如珠

【定时提醒】 每日9:00时，自动发送条例提醒
④ 自动化小助手 每日安全条例提醒
1. 进入现场，戴好安全帽。
2. 二米以上高空作业，扣好保险带。
3. 高处作业时，不准乱抛材料工具。

7. 选择自定义机器人



机器人

×

选择要添加的机器人



自动化小助手
智能联通不同的应用
让工作自动完成



心知天气
自动推送天气预报和
预警信息



阿里云Codeup
阿里云提供的代码托
管服务



GitHub
基于Git的代码托管服
务



极狐GitLab
基于ROR的开源代码
托管软件



JIRA
出色的项目与事务跟
踪工具



Travis
出色的项目与事务跟
踪工具



Trello
实时的卡片墙，管理
任何事情



自定义
通过Webhook接入自

8. 点击添加

机器人详情

×

简介：使用钉钉机器人API，可以将任何你需要的服务消息推送到钉钉

消息预览：



信息来源网站: <https://www.dingtalk.com/>

取消

添加



9. 勾选加签（产生的密码对应云安全中心中钉钉通知联系组的 secret）

添加机器人

* 添加到群组：

* 安全设置
* 说明文档 自定义关键词

加签 **勾选加签**

SECa387469edd930eaaef10d948f13b8

密钥如上，签名方法请参考 [说明文档](#)

IP地址(段)

是否开启Outgoing机制 (该功能正在维护中，给你带来不便敬请见谅)
 我已阅读并同意 [《自定义机器人服务及免责条款》](#)

10. 完成后点击机器人



内部

13分钟前

发起了群聊。本群成员来自同一组织，为内部群，请放心安全沟通。

本群是内部群，企业管理员已设置本群的聊天文件保存至组织“
”，企业数据安全可控

添加了机器人: test

test 白机器人

大家好！我是 test 机器人，很高兴为你们服务。

消息总结 找文档 群知识库 群签到 OA审批 看闲忙 水印拍照 更多酷应用

发送

11. 点击机器人设置

简介
使用钉钉机器人API，可以将任何你需要的服务消息推送到钉钉

消息预览

VIP监控报警 机器人
消息发送失败率高于5%，模块202，
网络类型4G。@易楠 紧急处理

预案提醒 机器人
[P3][线上][提前预案]
- 移动端首页tab个数显示降级
- 操作人：须莫

信息来源网站
<https://www.dingtalk.com/>

添加

更多机器人 >



12. 复制 Webhook



13. 获取 Webhook 后

https://oapi.dingtalk.com/robot/send?access_token=39c0d034b99e9818aaa56e07c907f91b54ec8cd
d5dfddd78ff73e8bc99e955d4

token=后的部分为云安全中心联系组钉钉需要的 token

Q: 如何获取企业微信机器人的 key?

注: 微信群必须是内部群 外部群添加不了群机器人

1. 添加群机器人





2. 获取到机器人的 key 值



添加机器人

完成



已添加 test

配置Webhook后可推送消息到群

配置说明 >

Webhook地址

<https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=0317a550-1837-46ea-bf69-4a04dcd876c0> 复制

<https://qyapi.weixin.qq.com/cgi-bin/webhook/send?key=0317a550-1837-46ea-bf69-4a04dcd876c0>

Key=后面的值为云安全中心联系组中的 KEY