安全运营中心（SOC）

产品文档

腾讯云TCE

版权所有：亿算云平台

文档目录

- 产品简介
  - 产品概述
  - 产品优势
  - 应用场景
- 操作指南
  - 安全可视
    - 安全态势
    - 态势大屏
  - 资产管理
    - 资产列表
    - 资产发现
  - 漏洞管理
  - 安全检测
    - 告警列表
    - 策略管理
  - 调查中心
    - 日志列表
    - 智能检索
  - 响应中心
  - 报表中心
    - 说明
    - 报表列表
    - 报表任务
- 常见问题
  - 常见问题
- 词汇表
  - 词汇表

产品简介
产品概述

最近更新时间: 2024-12-19 17:12:00

什么是安全运营中心

云服务商安全面向政府、金融、制造业、医疗、教育等大中型企事业单位推出的智能化安全运营平台。以云原生技术为基础，仓湖一体化大数据平台为底座，MITRE ATT&CK技战术框架为指导，结合云服务商领先的威胁情报能力、AI和可视化技术，聚焦TDIR（Threat Detection, Investigation and Response）威胁运营，打造智能化安全运营平台，提升企业安全运营效率，实现企业全网安全态势可知、可见、可控的闭环。

主要功能

安全可视、安全检测、调查中心、响应中心、资产管理、漏洞管理。

安全可视

安全态势数据监测能够帮助安全运营管理人员及时发现和处理威胁，以便于有效洞察企业面临的外部威胁和内部脆弱性风险，极大提高安全运维团队监测、管理、处置安全事件的效率。

从安全态势页面可以查看企业在全网范围内的日志、告警、安全事件的数量、趋势和TOP详情。安全运营趋势图，ATT&CK告警态势概览等。

资产管理

为用户提供资产可视功能，从资产角度了解安全态势，盘点现有资产，对资产进行编辑管理，同时方便运维人员对企业内网资产进行管理。可对用户环境中的各个资产实现列表管理，包含列表呈现各个资产基本信息，例如资产名称、资产IP、资产来源、资产分组等。用户可选取资产列表中的相关资产以Excel表格的形式进行导出。针对单个资产的详细信息，御见提供详细直观的可视化展示，包含该资产的详细信息、安全告警、安全事件及脆弱性的展示。

漏洞管理

实时收集互联网最新安全漏洞情报，扫描内网资产安全状况，发现并生成漏洞事件，方便运维跟踪处理。

安全检测

将接收的来自第三方安全设备、系统、应用日志归一化后的日志，通过多源日志关联、日志与漏洞信息关联匹配，生成高确信安全告警。

调查中心

供用户对日志进行查询、检索。通过接收并保存企业内部各种设备日志及流量日志，提供给安全运维人员进行关键字段筛选搜索。

响应中心

通过响应中心，可以在发现安全事件或漏洞事件后进一步处置操作。目前支持工单通报与流转。

报表中心

可根据用户实际需求制定并输出安全报表，方便安全运维人员总结一段时间内的安全工作成果，提供向上汇报，内部总结分析的材料支撑。

订购管理

提供用户对安全运营中心(SOC)的订阅、取消订阅、查看订阅信息的功能。

产品优势

最近更新时间: 2024-12-19 17:12:00

领先的技术架构

云平台多年的大数据架构技术，以及云原生安全技术、检测和分析能力赋能到SOC平台，为企业客户提供云平台累积多年的安全能力和经验，帮助其安全能力建设的快速搭建和落地。

支持采集多源数据，构建安全数据湖，SOC 具备支持不同来源、不同类型、不同格式的数据聚合能力。具体数据源包括以下几方面：

- 网络流量：通过将核心交换或其他网络节点上的流量旁路到智能态势感知平台的流量探针。
- 设备、主机和系统日志：支持主流网络设备日志、Windows 系统日志、Linux 系统日志等。
- 业务及应用的日志：Web 服务器日志（IIS 日志、nginx 等常见Web日志）、代理服务器日志、FTP 日志、VPN 日志、RDP 日志、主流数据库日志等。
- 安全设备事件日志（告警日志）：支持安全设备、安全软件的安全事件日志（例如：哈勃沙箱的分析日志）、防火墙、WAF 的拦截日志以及终端安全软件日志。

完善的检测手段

SOC平台为客户提供完善检测手段，包括网络流量入侵检测、威胁情报、多源关联分析。依赖传统检测手段和行业领先技术实践在SOC平台的落地，为客户构建完善、立体的威胁检测工具，及时发现威胁和风险让企业没有安全盲点。

在强大的检测能力基础上，SOC建立了基于ATT&CK知识矩阵构建安全检测评价体系。威胁可视能力业界领先，内置告警策略ATT&CK覆盖率高达74%超越国内安全厂商。

威胁情报能力

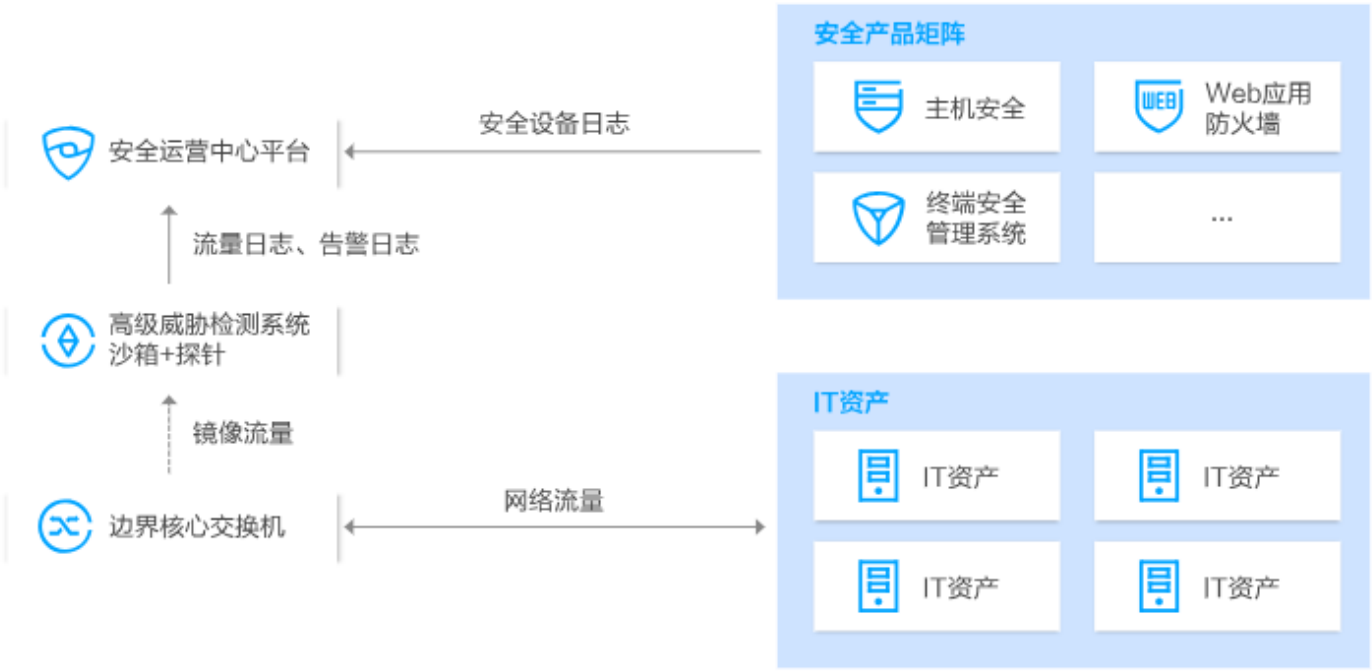
百亿级恶意文件样本库、数亿级 IP 信誉库、域名信誉库、木马病毒样本、日均新增100W+、数千万级恶意网址、高质量情报云查、数十万级漏洞情报。SOC 内置的威胁情报关联能力，在关联分析中能够将系统采集到的流量、各种安全日志与威胁情报进行碰撞比对。

应用场景

最近更新时间: 2024-12-19 17:12:00

安全管理合规运营

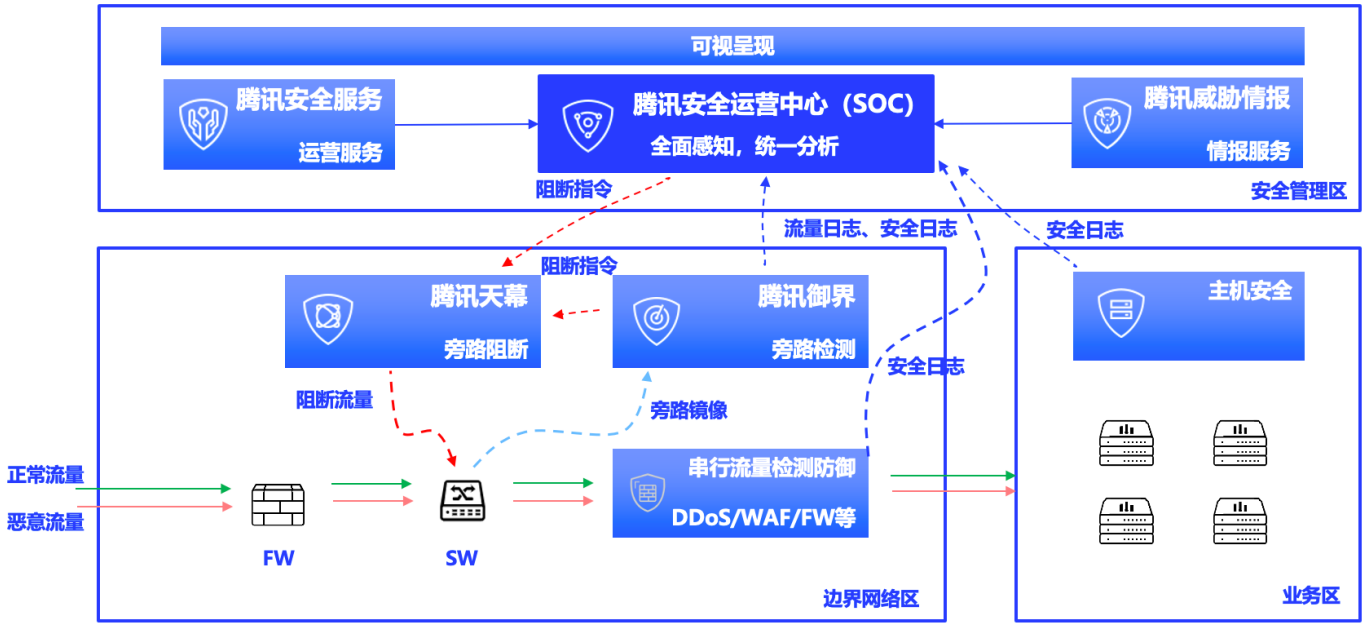
需要对安全事件、漏洞、资产等安全要素进行全方面运营，感知整体安全态势，满足等保2.0关于日志审计、安全管理等合规需求。



实战化安全运营与自动化闭环

目标客户为政府、金融、能源、医疗、教育、交通、零售等，适用于央企、大中型集团组织。用户需要对安全事件、漏洞、资产等安全要素全方面运营，满足等保2.0关于安全管理、日志审计等合规需求。

通过接入现网的串行流量检测设备、旁路检测设备、主机端安全、外网情报等数据，实现统一检测，统一运营，并可搭配安全设备联动阻断实现自动化安全闭环。

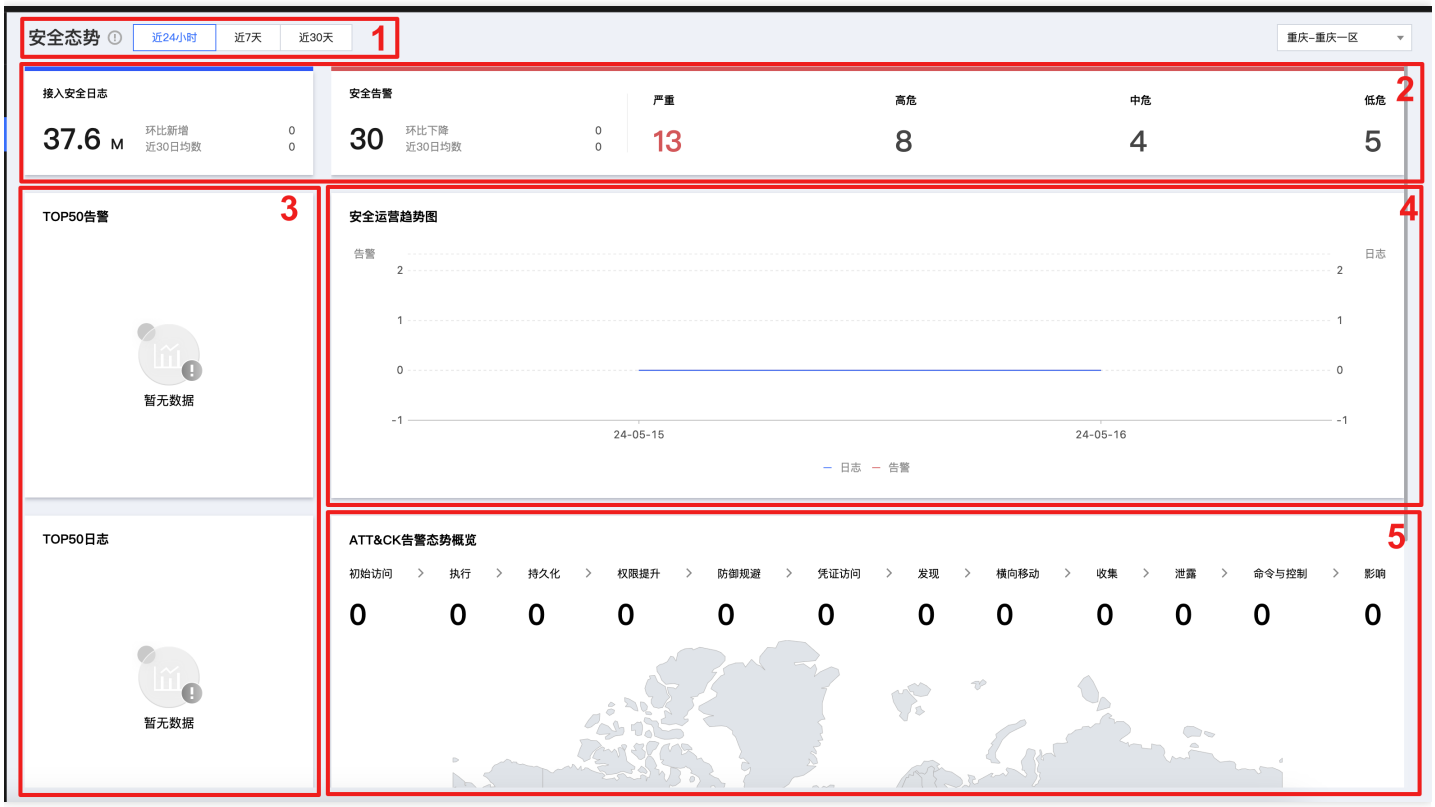

可视呈现
腾讯安全服务
运营服务
腾讯安全运营中心（SOC）
全面感知，统一分析
腾讯威胁情报
情报服务
安全管理区
阻断指令
流量日志、安全日志
安全日志
阻断指令
腾讯天幕
旁路阻断
腾讯御界
旁路检测
主机安全
安全日志
阻断流量
旁路镜像
正常流量
恶意流量
串行流量检测防御
DDoS/WAF/FW等
FW
SW
边界网络区
业务区

操作指南
安全可视
安全态势

最近更新时间: 2024-12-19 17:12:00

安全态势数据监测能够帮助安全运维人员及时发现和处理威胁，以便于有效洞察企业面临的外部威胁和内部脆弱性风险，极大提高安全运维团队监测、管理、处置安全事件的效率。

进入安全态势页面，可以查看企业在全网范围内的安全日志、安全告警、安全事件数量，TOP排行，安全运营趋势图，ATT&CK告警态势概览。展示方式包括安全评分、趋势图、条形图和分布图等，如图所示。



以查看近24小时的安全态势为例，页面各区域说明如下：

1. 时间筛选范围

可选择时间范围，查看此范围内的数据统计，系统默认近24小时、近7天和近30天三个选项，可在系统默认数值设置修改。

2. 值得关注和跟进的信息总览

- 接入安全日志数量、环比上个周期数量变化，近30天日均接入日志数。
- 产生安全告警数量、环比上个周期数量变化、近30天日均告警数、各个威胁等级的告警数量分布。
- 产生安全事件数量、环比上个周期数量变化、近30天日均事件数、不同严重性的事件数量分布。

3. 重点信息TOP50——日志、告警、事件

最近24小时内排名TOP50的日志、告警和事件。单击名称可进入对应的管理页面，并过滤出对应的信息。

4. 安全运营趋势图

最近24小时接入的日志和产生告警数量趋势图，鼠标悬浮图表上可显示当前时间具体数值，点击下发图例可控制是否显示。

5. ATT&CK告警态势概览

- 最近24小时内产生告警按照ATT&CK战术阶段分类，展示处在每个战术阶段告警数。单击战术及下方的数字可进入告警管理页面并过滤出对应的告警信息。
- 最近24小时内产生告警的攻击者IP地理位置分布图。将鼠标悬浮在高亮点即可查看攻击者的国家/地区和IP地址，单击高亮点可进入告警管理页面并过滤出对应的告警信息。

态势大屏

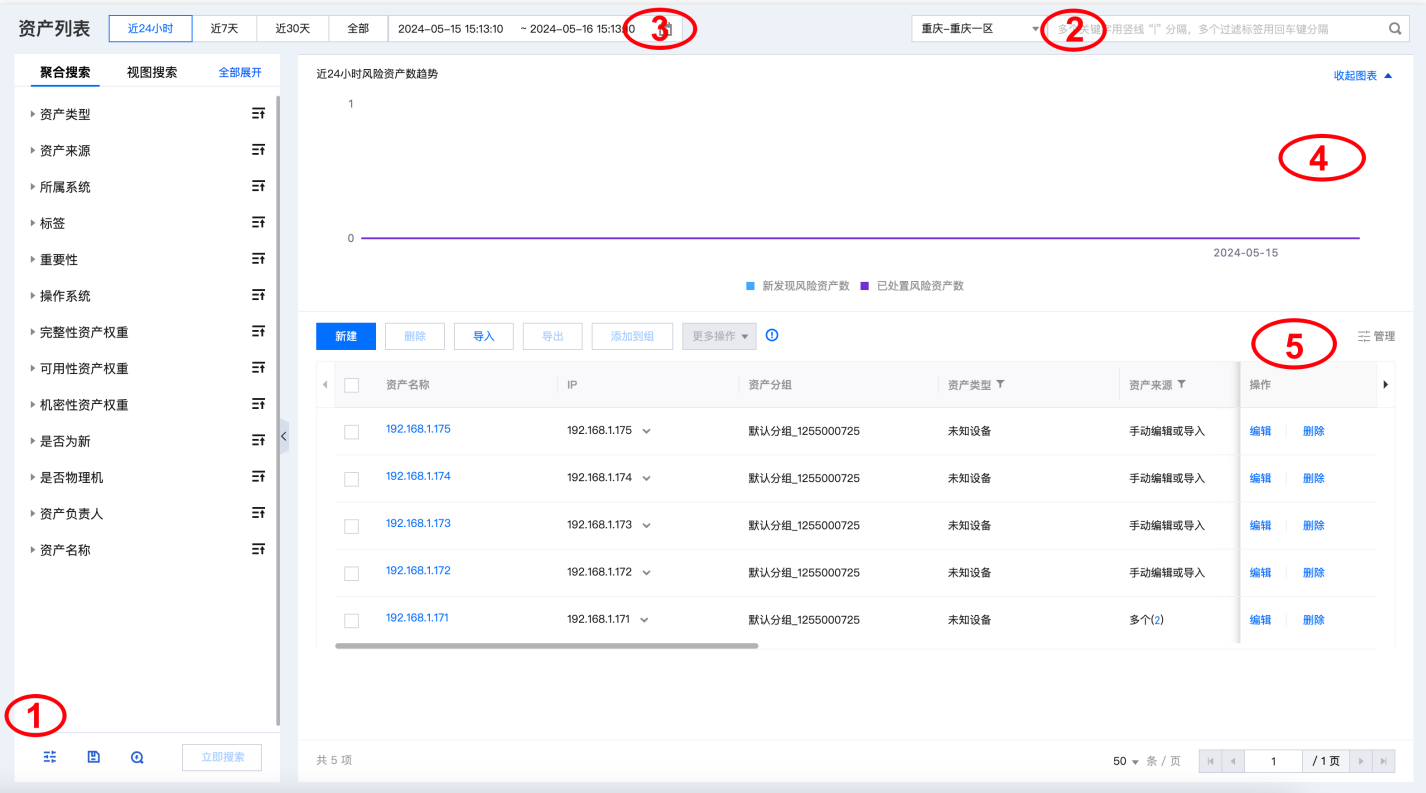
最近更新时间: 2024-12-19 17:12:00

提供针对租户安全场景的可视化大屏。展示了24小时以内、7天以内或30天以内的告警分布情况、告警趋势、告警TOP10、受害者IP TOP10、攻击者IP TOP10、安全防护漏斗图以及已处理告警数，如图所示。

资产管理
资产列表

最近更新时间: 2024-12-19 17:12:00

进入资产管理 > 资产列表，资产管理的页面布局如图所示。管理员可以查看网络环境中的资产详情和当前资产的安全事件、待处置告警和待修复漏洞，还可进行资产的新建、编辑、导入、导出、删除、搜索、编辑资产标签和添加资产组等操作。



1、资产搜索栏

- 支持以下两种搜索模式：

（1）聚合搜索——按照资产类型、资产来源、重要性、资产IP和标签等类目，选择一个或多个条件进行搜索。

（2）视图搜索——以树状结构展示资产的业务分组、组织分组、地理分组、网域分组和应用分组，选择一个或多个资产分组进行搜索。

- 单击底部的 即可添加或删除复合搜索模式的搜索类目。

- 单击底部的 即可将当前所选的搜索条件保存为快速搜索任务。
- 单击底部的 即可调取一个快速搜索任务，无需重新设置搜索条件。
- 每个搜索条件都可排序显示，部分搜索条件还支持快速检索和“是非”快捷操作。
- 不用资产搜索栏时，可将其隐藏起来。

2、简单搜索

在搜索框中输入资产IP、CIDR或资产名称进行搜索。

3、时间筛选框

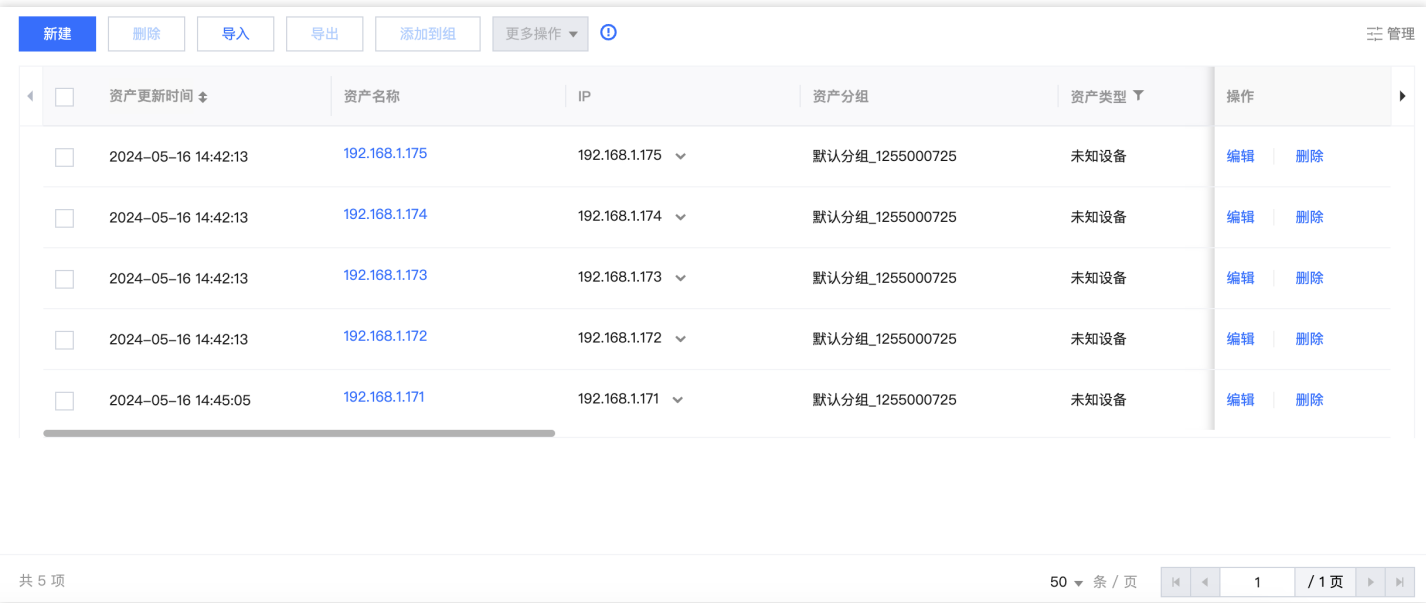
可设定资产更新时间范围，查看此时间段内的资产，也可以点击全部查看全部资产。

4、险资产数量趋势图

展示时间段内新发现风险资产数、已处置风险资产数与时间的关系，将鼠标悬浮在图中可显示具体日期及其对应的数量。单击【收起图表】可将风险资产数量趋势图隐藏起来。

5、资产列表

在资产列表的右上方，单击【管理】可以自定义资产列表的显示项，如图所示。更多介绍，详见查看资产详情至编辑资产标签。



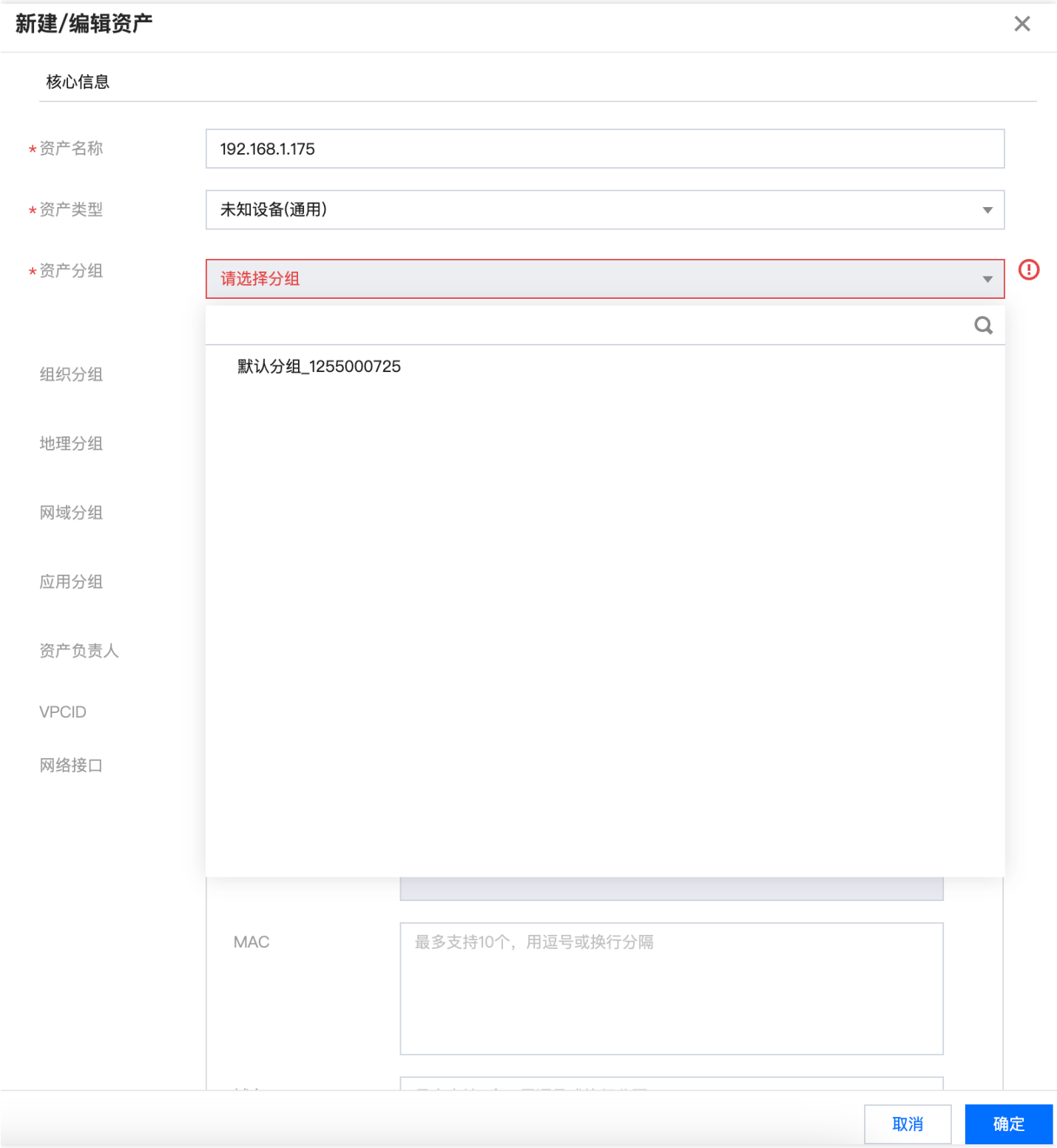
查看资产详情

如图所示，管理员在资产列表底部拖拽滚动条可以查看资产信息，还可以单击资产名称查看资产的完整信息：

- 资产注册信息（资产类型、资产来源、资产IP、端口、服务和域名）；
- 资产核心信息（资产名称、资产类型、资产分组、资产负责人、VPCID、网络接口、操作系统和资产发现时间等）；
- 资产安全指数（安全评分、重要性、待处置告警数、7天内事件数、待修复漏洞数），单击【一键更新】可即时更新该资产的安全评分；
- 资产拓展信息（资产所属部门、安全域、所属网段、探针名、设备ID和首次发现时间等）；
- 指定时间范围的待处置告警信息；
- 指定时间范围的安全事件；
- 待修复漏洞信息。

手动添加资产/添加到组

单击【新建】，填写资产的核心信息和拓展信息，如图所示。每个资产最多可配置10个IP/MAC。 若资产的业务分组尚未创建或暂不确定所属分组，可先处于“默认分组”状态；若添加资产后才确认资产组，批量选择资产并单击【添加到组】即可将其分组。


新建/编辑资产
核心信息
*资产名称
192.168.1.175
*资产类型
未知设备(通用)
*资产分组
请选择分组
默认分组_1255000725
组织分组
地理分组
网域分组
应用分组
资产负责人
VPCID
网络接口
MAC
最多支持10个，用逗号或换行分隔
取消
确定

导入/导出资产

单击【导入】即可批量导入资产信息（需要从页面下载模板制作资产信息文件）。若导入时发生资产冲突，可以选择三种操作：撤销导入、仅导入新资产或者覆盖导入。 选中多个资产并单击【导出】，即可将所选资产信息导出为Excel文件。

> **说明：**
>
> 导入资产信息时，需要注意以下几点：
>
> 1）请提前在运营端中设置资产组，否则会导致导入的资产分组错乱。
>
> 2）导入的资产数量应控制在1万条以内；若填写的资产信息非常丰富，建议控制在2千条以内，避免因系统性能问题导致超时（若超过6分钟系统无响应，表示超时）。

编辑/删除资产信息

单击【编辑】，除了资产IP和APPID，其他信息均可修改；对于DHCP资产，MAC地址也不可修改。 单击【删除】或者选中多个资产并单击【删除】，即可删除所选资产。资产被删除后，历史数据（例如：事件和告警的关联资产信息）不会被清除。

编辑资产标签

选中单个或多个资产并单击更多操作> 编辑标签，即可为所选资产添加标签。资产标签可与事件联动，关联资产的事件会附带对应的资产标签。 选中单个或多个资产并单击更多操作> 编辑其他，即可批量选择字段并编辑各个字段的内容。

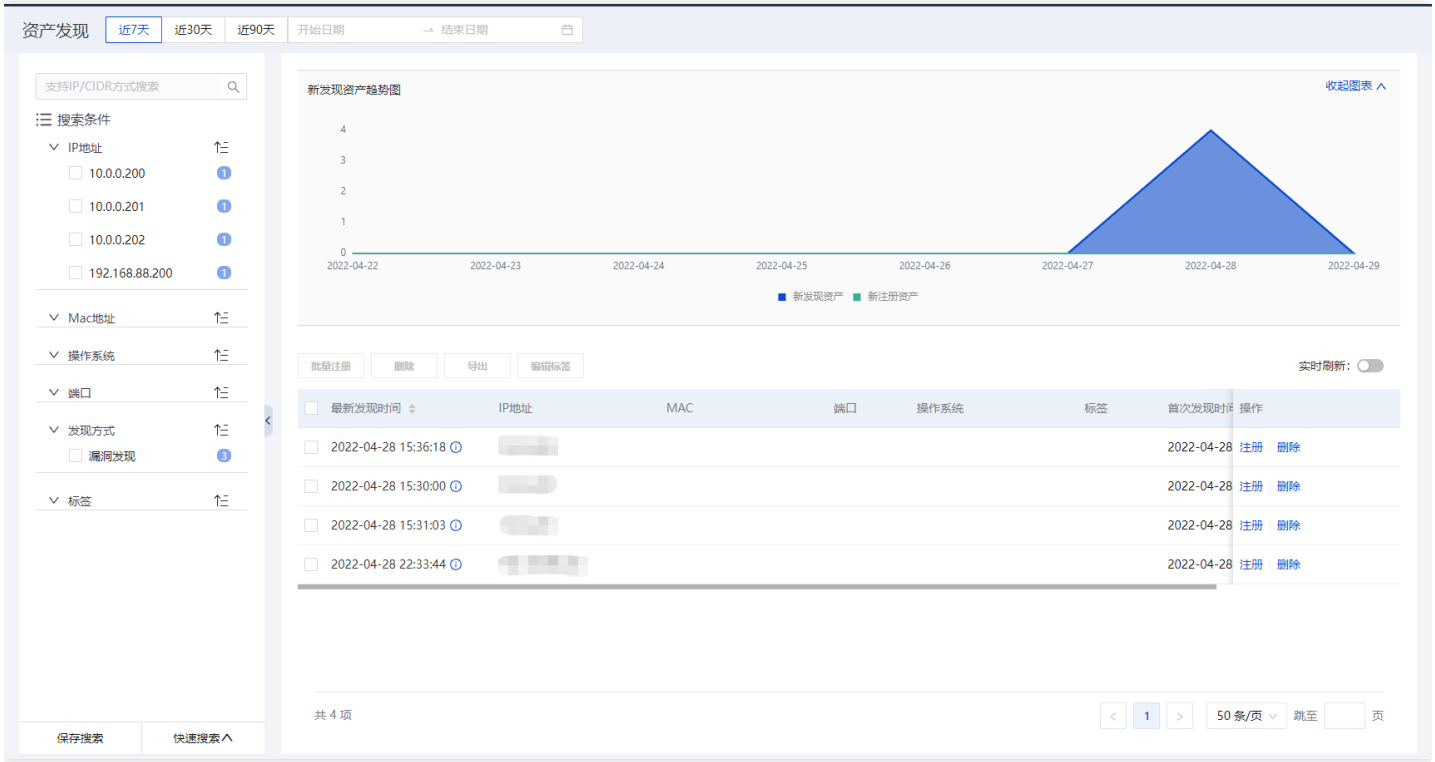
资产列表快捷菜单

与告警列表的快捷菜单基本相同，详见告警列表快捷菜单。

资产发现

最近更新时间: 2024-12-19 17:12:00

资产发现页面如图所示，可以对自动发现的资产进行注册、导出、删除或编辑标签。



注册资产

对于自动发现的资产，需要进行注册才能进入资产列表接受安全监控。

单个注册资产

步骤1 在资产发现列表中单击操作栏下的【注册】。

步骤2 在弹出的注册资产页面中，填写该资产的核心信息和拓展信息。

步骤3 填写完毕，单击【完成注册】。

步骤4 进入资产列表页面，出现页面提示表示该资产注册成功。

步骤5 注册后的资产，单击【编辑】定义它的资产类型和资产分组，单击【更多操作】定义它的标签或其他字段，单击资产名称查看它的告警、事件、漏洞详情和安全指数。

批量注册资产

步骤1 在资产发现列表中选中多个想要注册的资产。

步骤2 单击【批量注册】即可注册所选资产。

步骤3 批量注册资产之后，资产信息为空，建议进入资产列表通过编辑、更多操作-编辑其他或添加到组的功能继续补充。

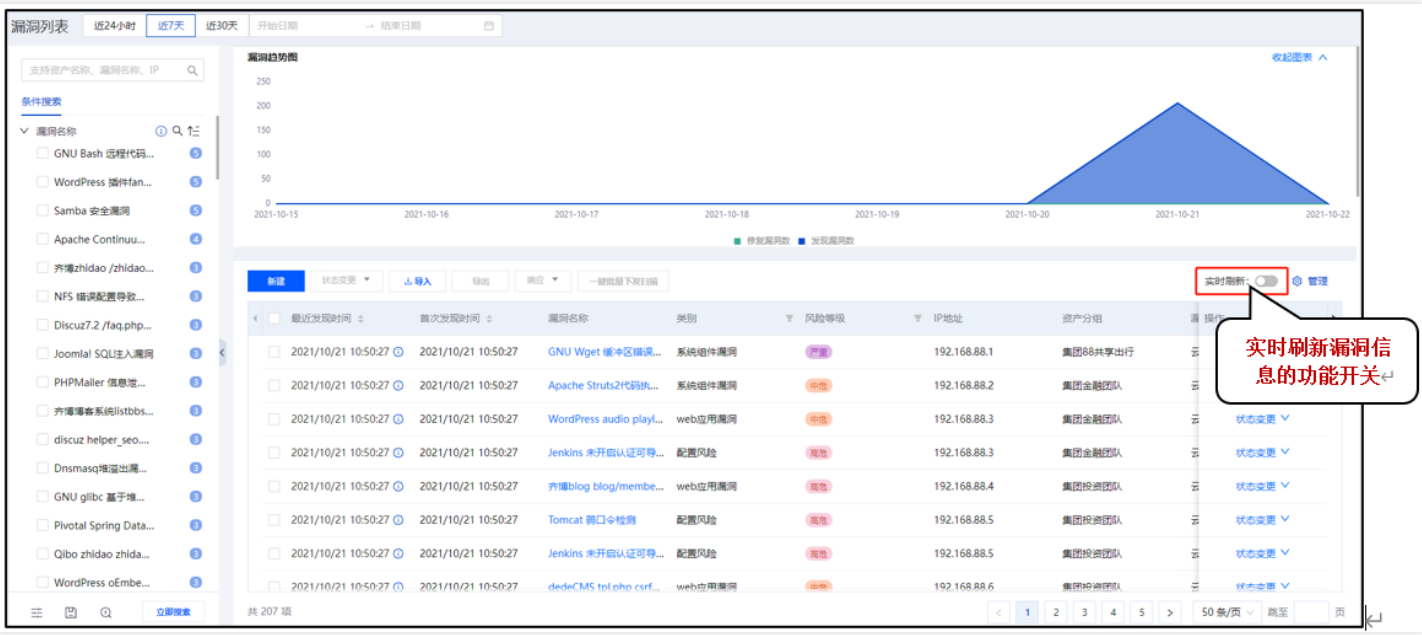
漏洞管理

最近更新时间: 2024-12-19 17:12:00

聚合多种来源产生的漏洞事件，展示漏洞相关信息，为漏洞修复和资产风险管理提供支持。

漏洞列表

进入漏洞列表，漏洞管理的页面布局如图所示，与资产管理相似。管理员可以查看漏洞趋势和漏洞详情，还可进行漏洞的新建、导入、导出、响应、搜索、状态变更和批量下发扫描等操作。



漏洞趋势图

选择时间范围查看漏洞的趋势，将鼠标悬浮在图中可以显示时间、修复漏洞数和发现漏洞数（与漏洞列表的数据实时同步）。单击【收起图表】可以将漏洞趋势图隐藏起来。

查看漏洞详情

在漏洞列表中，单击漏洞名称可以查看漏洞的基本信息、风险等级、状态、待修复资产数量、发现时间、漏洞编号、漏洞描述和修复建议等，如图所示。

Bash 安全漏洞 高危 • 待处置

待修复资产: 1 首次发现时间: 2021/03/11 10:52:52

最近发现时间: 2021/03/11 10:52:52

基本信息

类别:	系统组件漏洞	子类别:	输入验证
CVSS评分:	7.2	漏洞编号:	CVE-2016-7543 CNNVD-201609-621
租户名称:		资产负责人:	
漏洞标签:		影响版本:	
发布时间:	2016/09/28 00:00:00	更新时间:	2017/01/20 00:00:00

参考链接: http://www.openwall.com/lists/oss-security/2016/09/26/9,https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/F7XOQSHU63Y357NHU5FPTFBM6I3YOCQB/,http://www.securityfocus.com/bid/93183,https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OU3C756YPHDAAPFX76UGZBAQQQ5UMHS5/,https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/Z2VRBSIPZDZ75ZQ2DLITHUIDW4W26KVR/,https://lists.gnu.org/archive/html/bug-bash/2016-09/msg00018.html,https://security.gentoo.org/glsa/201701-02,http://www.securityfocus.com/bid/93183

漏洞描述: Bash是美国软件开发者布莱恩-福克斯（Brian J. Fox）为GNU计划而编写的一个Shell（命令语言解释器），它运行于类Unix操作系统中（Linux系统的默认Shell），并能够从标准输入设备或文件中读取、执行命令，同时也结合了一部分ksh和csh的特点。 Bash 4.4之前的版本中存在安全漏洞。本地攻击者可借助特制的SHELLOPTS和PS4环境变量利用该漏洞以root权限执行任意命令。

修复建议: 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://lists.gnu.org/archive/html/bug-bash/2016-09/msg00018.html

查看漏洞状态

如图所示，将鼠标悬浮在漏洞状态的图标 ⓘ 即可显示该漏洞最近10次状态修改记录。

查看漏洞发现时间

如图所示，将鼠标悬浮在最近发现时间的图标 即可显示该漏洞最近10次发现的时间。

新建漏洞

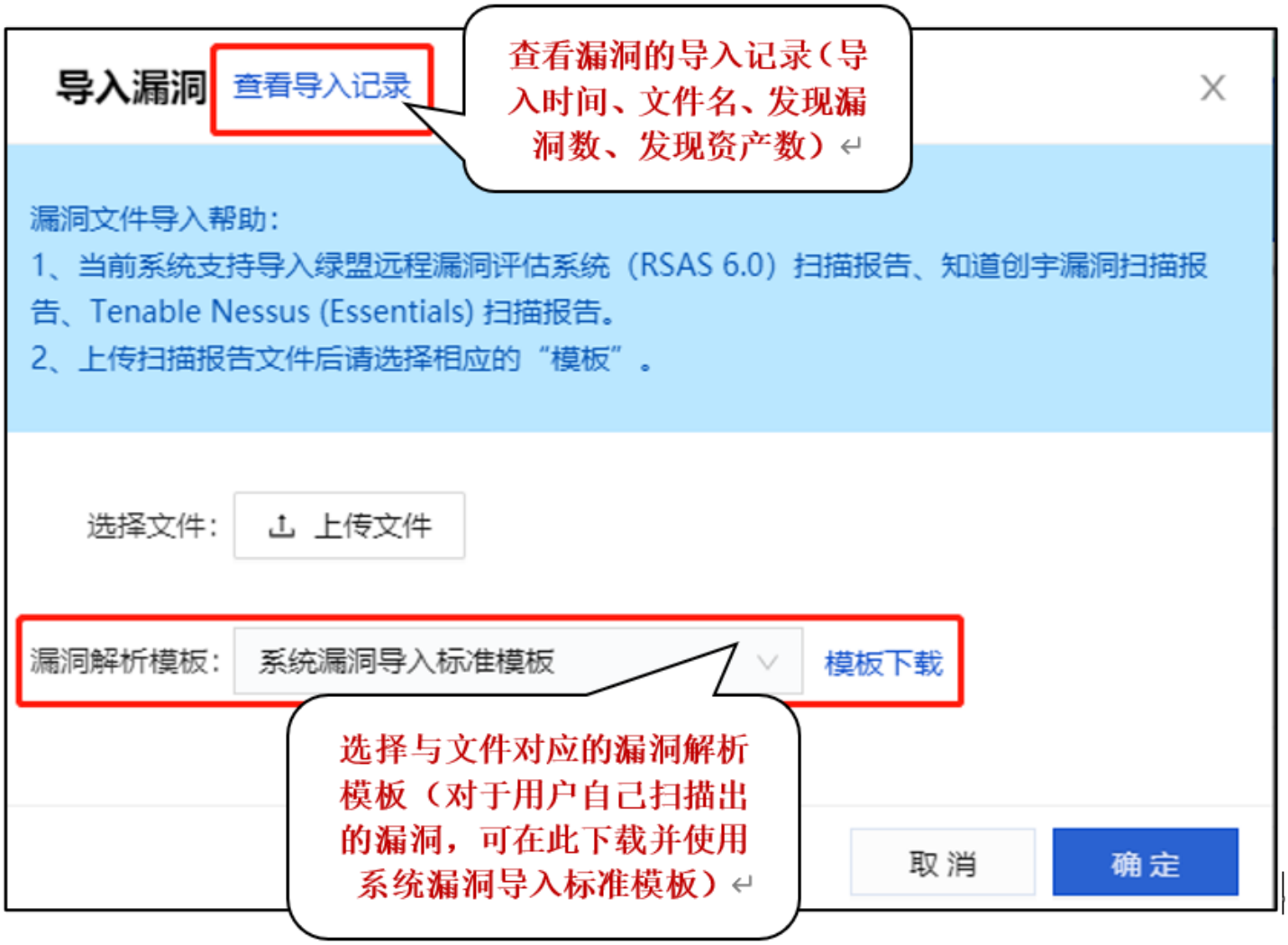
在漏洞列表的上方单击【新建】，弹出新建漏洞页面填写各项信息，如图所示。其中，IP地址必须在“资产网段配置”定义的IP范围内。

漏洞状态变更

如图所示，可以将漏洞的状态变更为待处置、处置中、已处置或忽略。既可单个操作也可以批量操作。

导入/导出漏洞

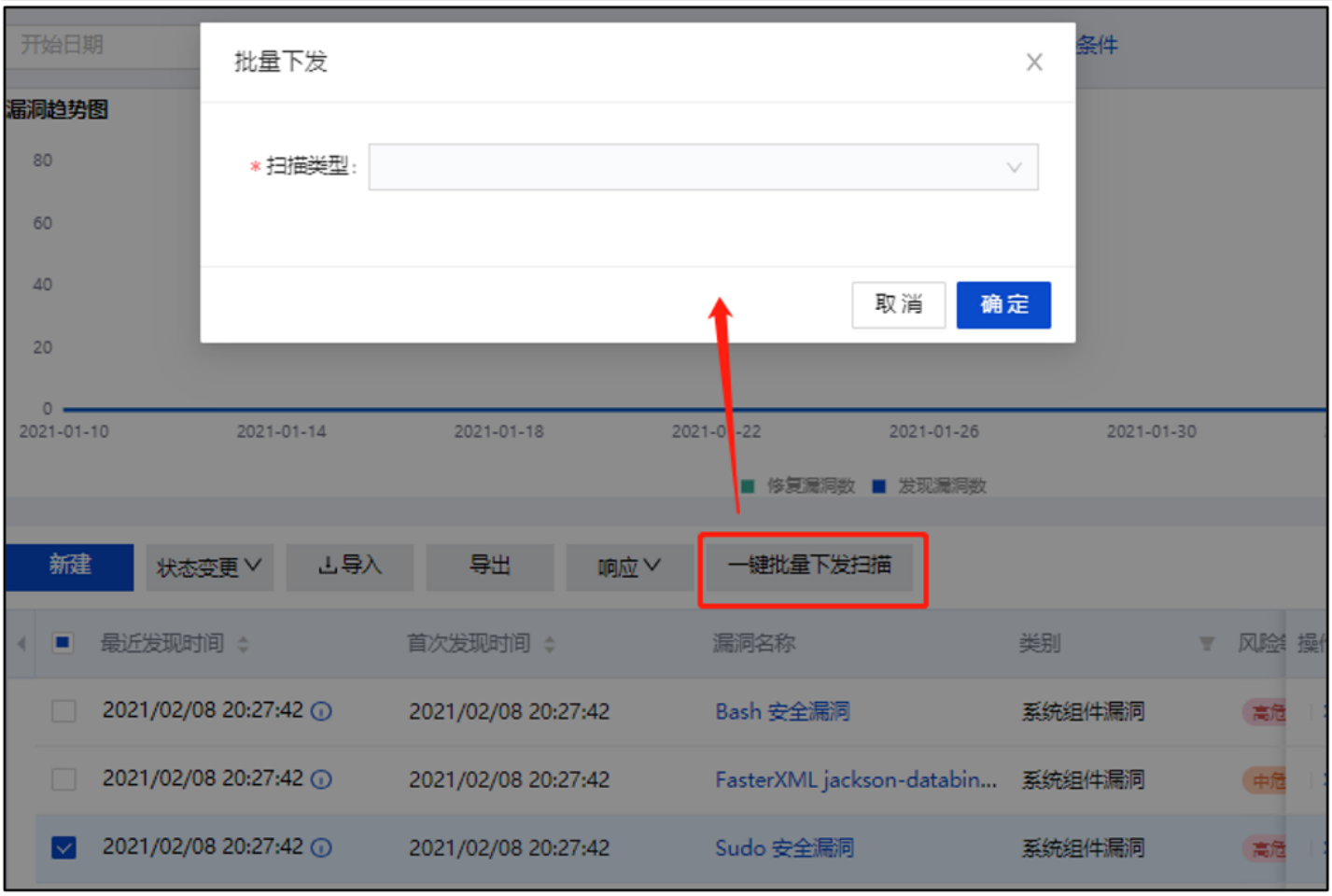
在漏洞列表中选中漏洞并单击【导出】，即可将所选漏洞导出为Excel文件。 在漏洞列表的上方单击【导入】，选择要上传的漏洞扫描报告及其对应的漏洞解析模板，即可将相关漏洞扫描系统扫描出的漏洞导入本系统，如图所示。



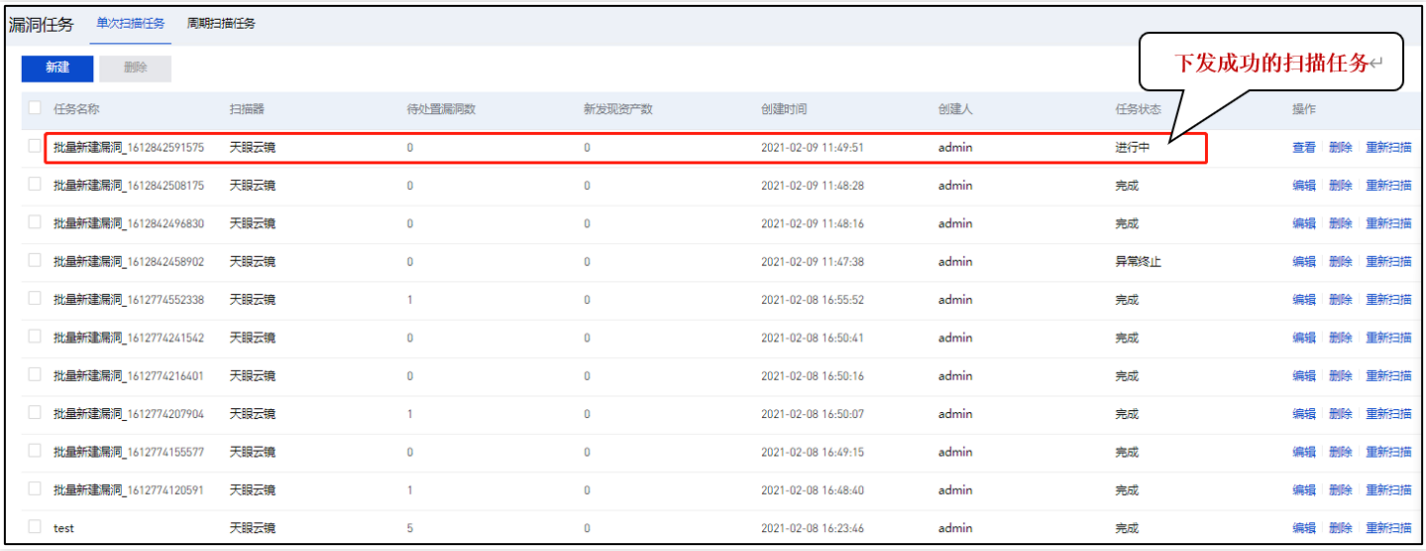
> **注意：**
>
> 导入漏洞文件时，请避免第三方平台的漏洞编号重复。

批量下发扫描任务

本功能仅适用于漏洞来源是天眼云镜的漏洞。 在漏洞列表中，选择单个或多个漏洞来源是“天眼云镜”的漏洞，单击【一键批量下发扫描】并选择与漏洞类型一致的扫描类型，如图所示。



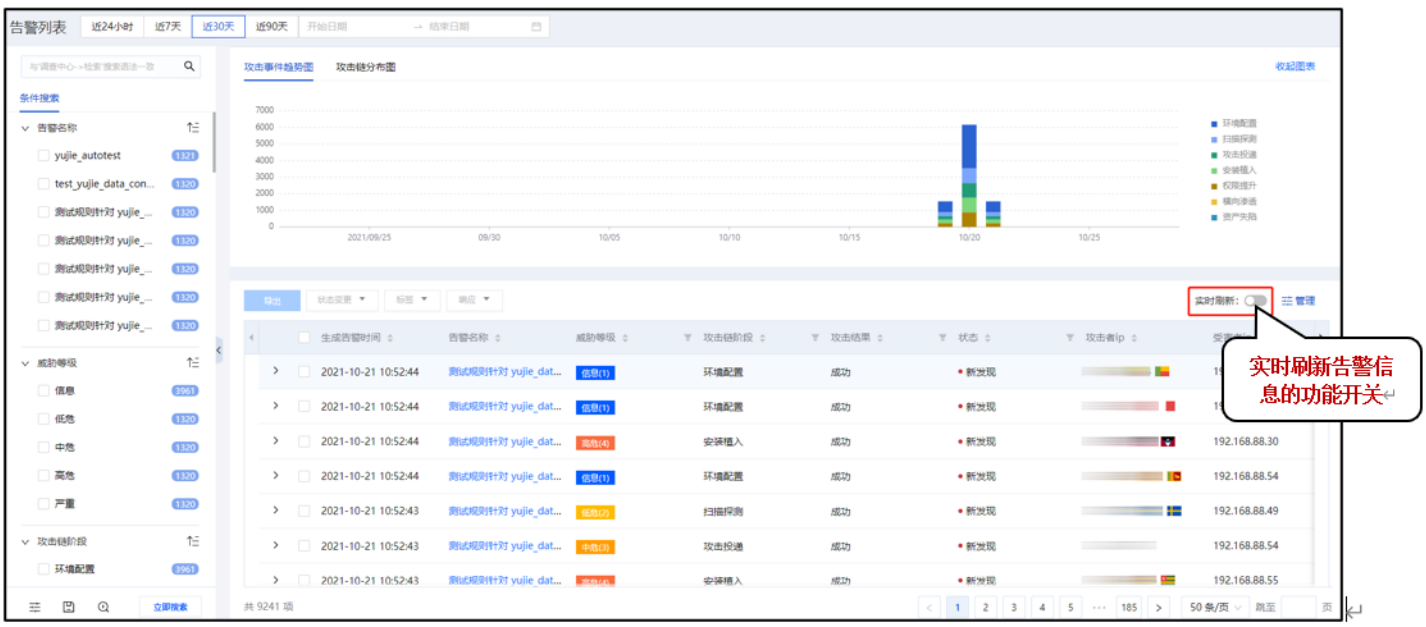
下发成功后，进入漏洞任务 > 单次扫描任务，该任务状态是“进行中”，如图所示。



安全检测
告警列表

最近更新时间: 2024-12-19 17:12:00

进入告警列表页面，页面布局如图所示，与资产管理相似。管理员可以查看攻击事件趋势图、攻击链分布图、告警详情和告警策略，还可进行告警的导出、响应、搜索、状态变更和编辑标签等操作。



告警搜索

与事件搜索的操作相同，详见事件搜索。

攻击事件趋势图

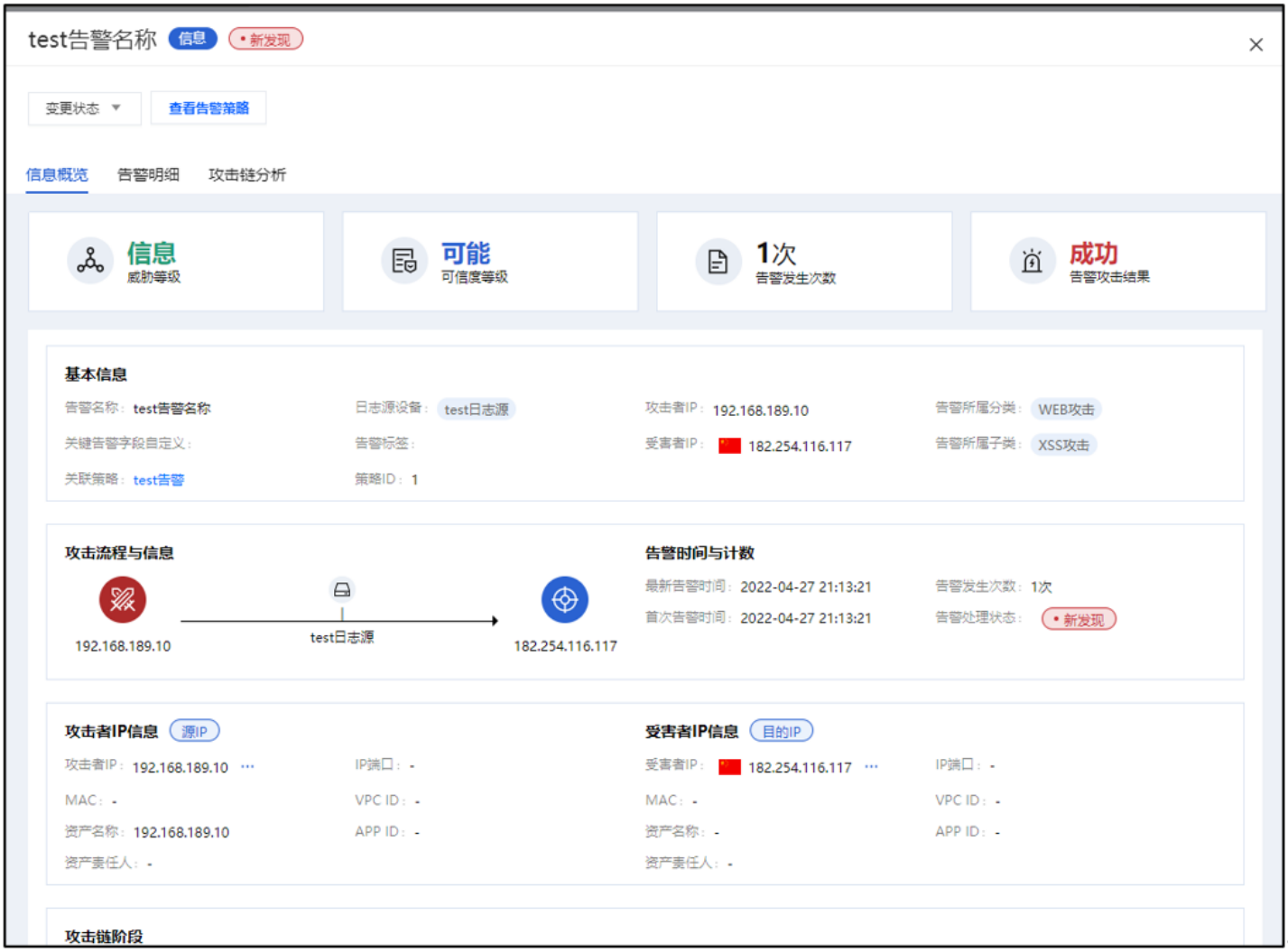
选择时间范围查看攻击事件的趋势，将鼠标悬浮在图中可以显示时间和各类攻击事件数（与告警列表的数据实时同步）。单击【收起图表】可以将攻击事件趋势图隐藏起来。

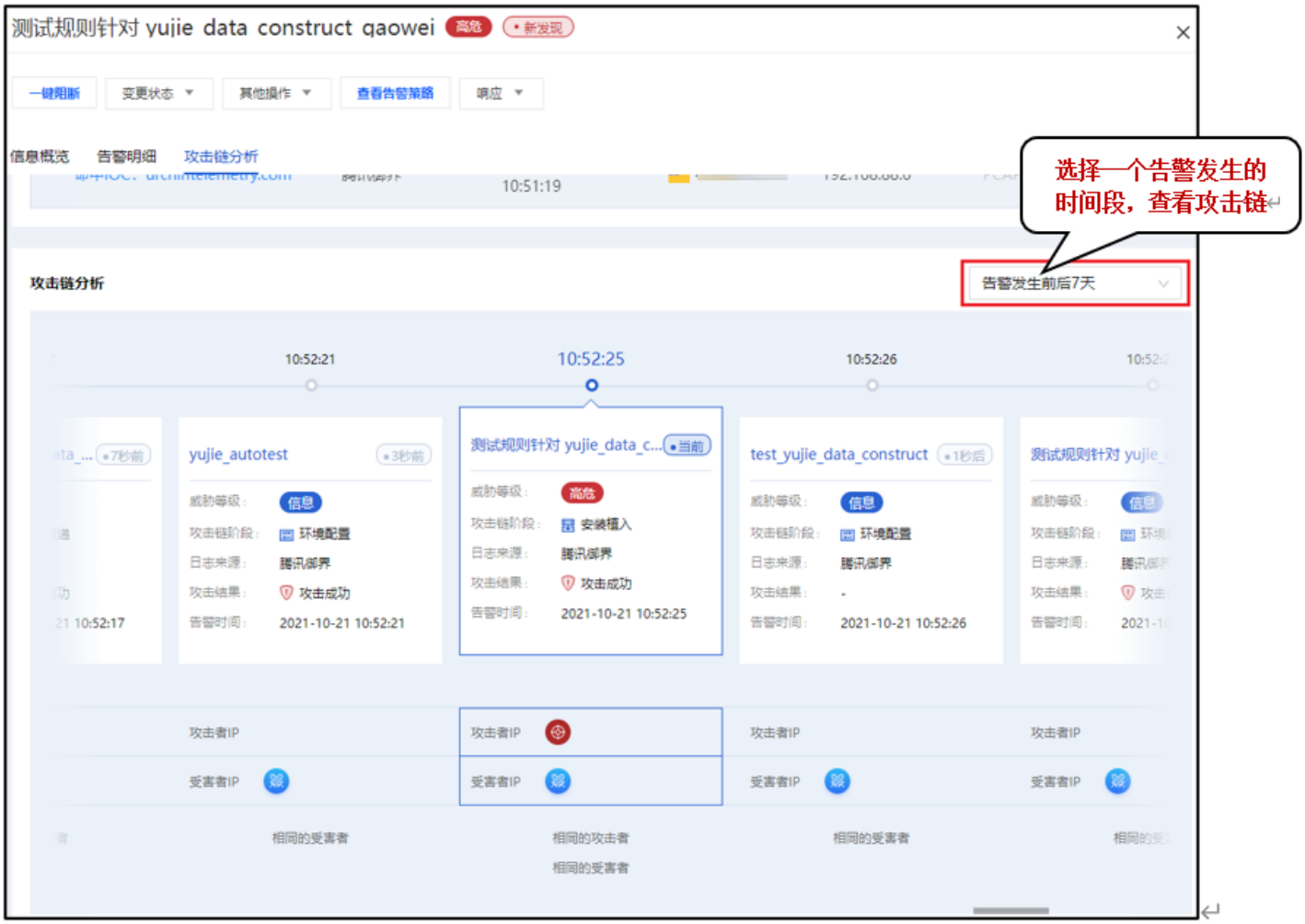
攻击链分布图

选择时间范围查看攻击链的分布，将鼠标悬浮在色块上可以显示时间和对应攻击类别的事件数（与告警列表的数据实时同步）。单击【收起图表】可以将攻击链分布图隐藏起来。

查看告警详情

在告警列表中，单击告警名称可以查看告警的状态、威胁等级、可信度等级、发生次数、攻击结果、基本信息、攻击流程与信息、攻击者IP信息、攻击链阶段、告警描述、处置建议、告警明细和攻击链分析等，如图所示。





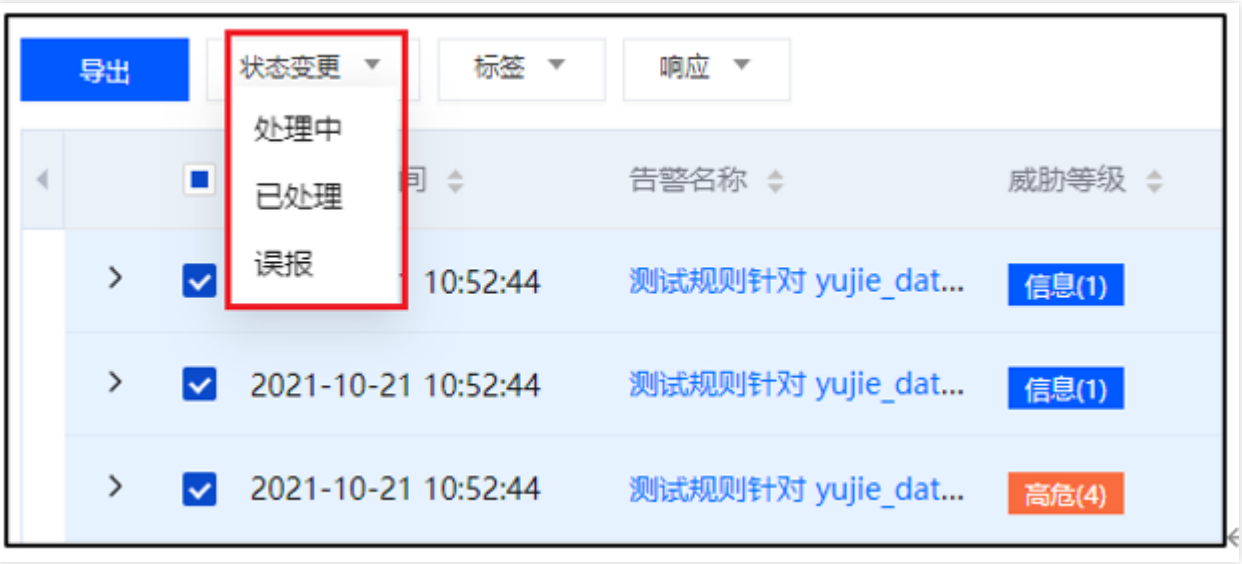
查看攻击者IP和受害者IP信息时，单击IP右侧的图标...弹出快捷菜单，可以针对该IP进一步操作，如图所示。

告警标签

选择单个或多个告警后，在告警列表上方，单击标签，可为所选告警添加标签或删除已有标签，如图所示。

告警状态变更

如图所示，可以批量选择将告警的状态变更为处理中、已处理或误报。



导出告警

在告警列表中，单击【导出】即可将所选告警导出为Excel文件，导出的告警内容即当前告警列表的展示列。

> **说明：**
>
> 导出告警之前，建议在告警列表的右上方，单击【管理】自定义告警列表的展示列。

告警列表快捷菜单

在告警列表中，鼠标右键单击告警名称、攻击者IP、受害者IP、源IP、目的IP、关联规则ID、关联规则名、资产名称、资产组或者资产负责人，即可弹出快捷菜单，以便于一系列操作的连贯性。例如：鼠标右键单击受害者IP，弹出快捷菜单，如图所示。

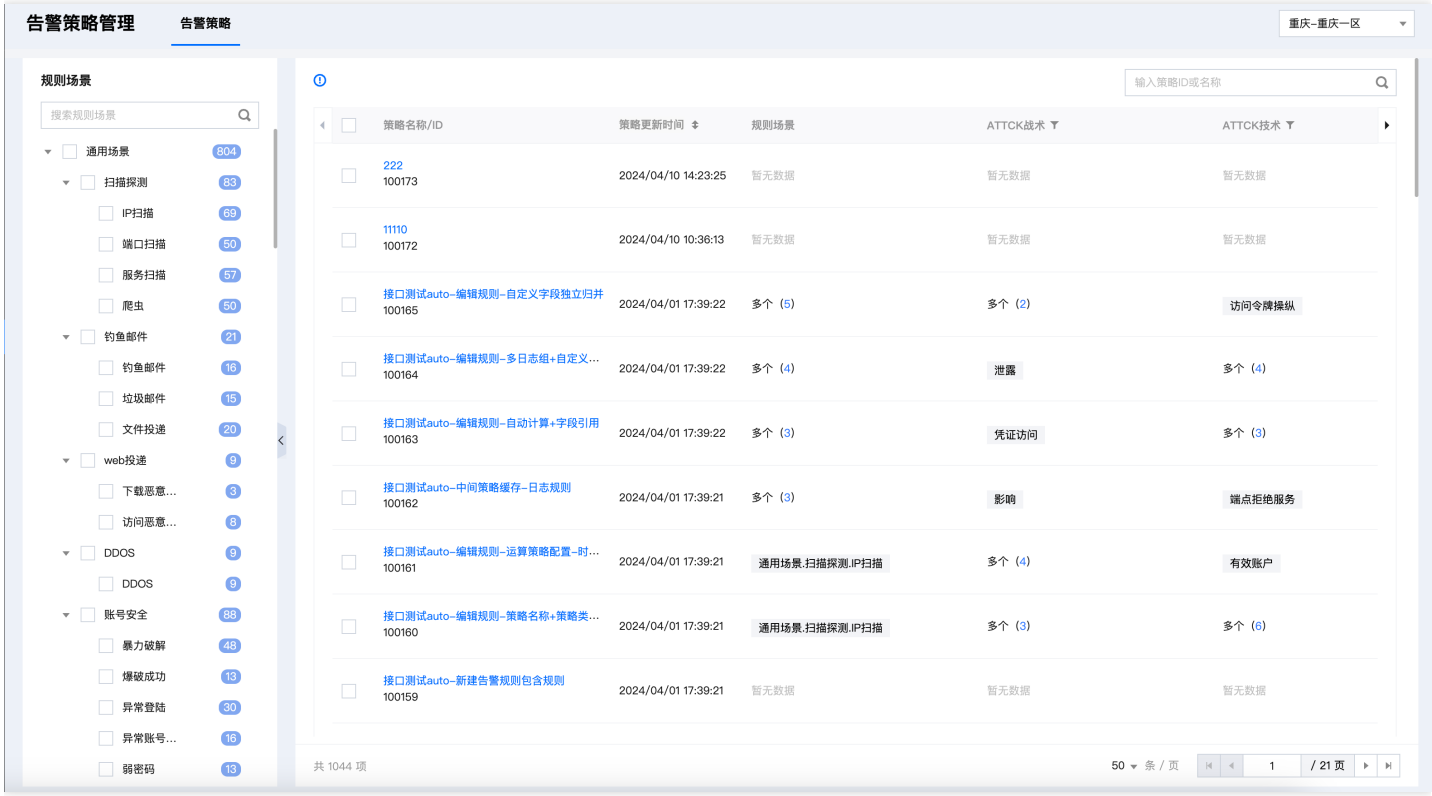
说明：

1. 不同的告警字段和资产状态，对应的快捷菜单项也会稍有不同。
2. 只有外网IP，才能进行威胁情报查询和Virus Total查询。

策略管理

最近更新时间: 2024-12-19 17:12:00

展示目前平台上所有的告警检测规则，支持搜索、过滤等功能，可查看规则详情。

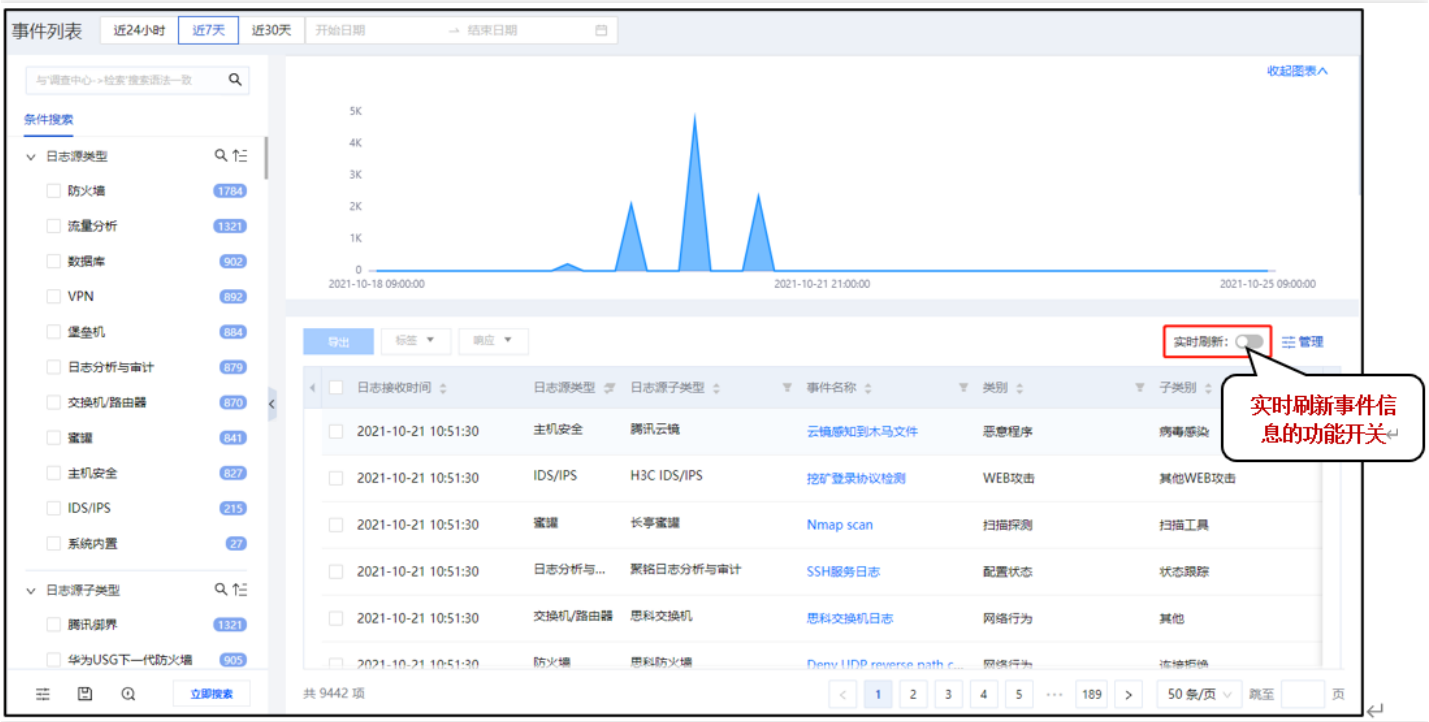


调查中心

日志列表

最近更新时间: 2024-12-19 17:12:00

进入日志列表页面，页面布局如图所示。管理员可以查看日志趋势和日志详情，还可进行日志的导入、导出、响应和搜索等操作。



日志搜索

在页面左侧的日志搜索栏中，除了选择详细类别，还可以直接输入lucene查询语句进行搜索。

> **说明：**
>
> 关于lucene查询语句的更多介绍，详见官方网址：https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html

日志趋势图

选择时间范围查看日志的趋势，将鼠标悬浮在图中可以显示时间和日志数（与日志列表的数据实时同步）。单击【收起图表】可以将事件趋势图隐藏起来。

查看日志详情

在日志列表中，单击日志名称可以查看日志的严重性、信息概览和日志明细（对于日志源是御界的日志，还可以查看会话还原和PCAP信息），如图所示。

单击【编辑标签】即可为该日志添加标签。详见日志标签。

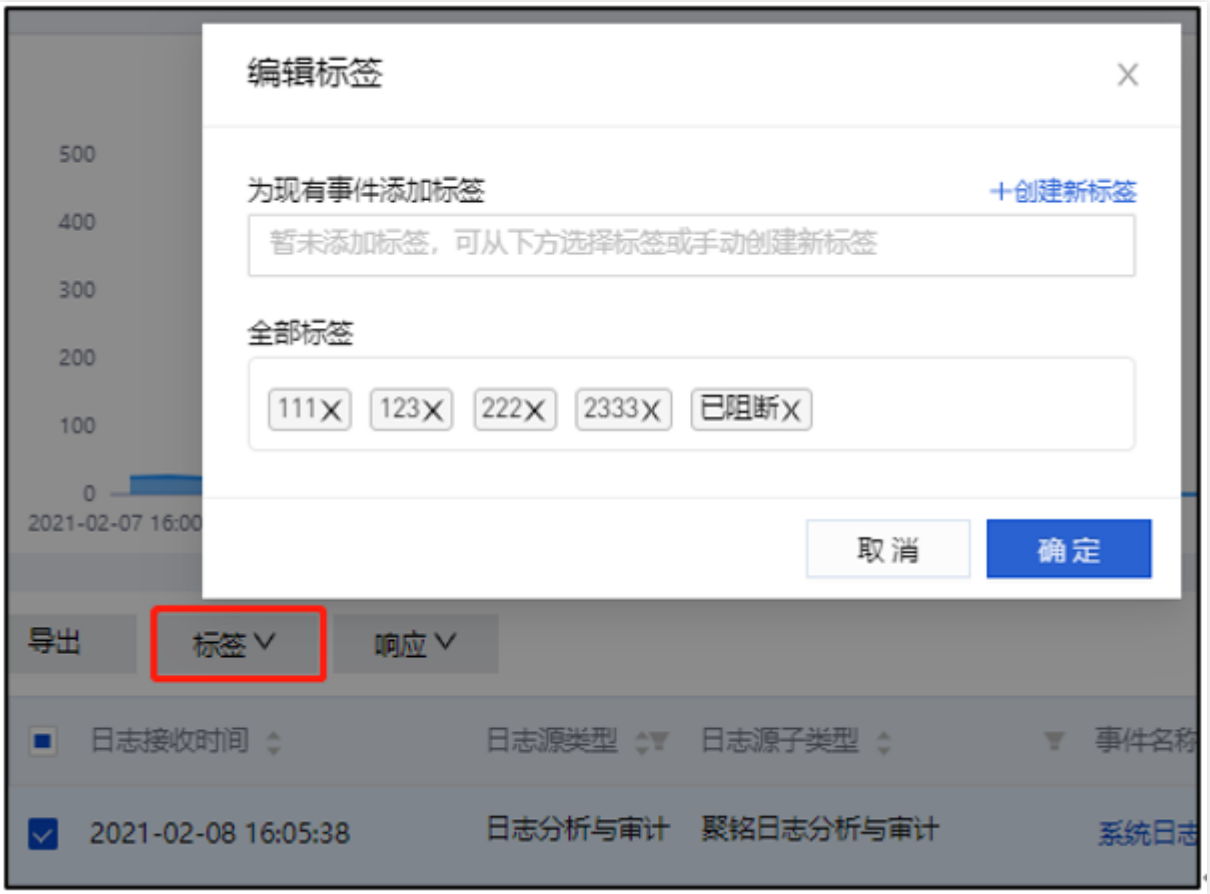
导出日志

在日志列表中，单击【导出】即可将所选日志导出为Excel文件，导出的日志内容即当前日志列表的展示列。

> **说明：**
>
> 导出日志之前，建议在日志列表的右上方，单击【管理】自定义日志列表的展示列。

日志标签

在日志列表上方，单击【标签】可以为所选的日志添加标签或删除已有标签，如图所示。



日志列表快捷菜单

与告警列表的快捷菜单基本相同，详见告警列表快捷菜单。

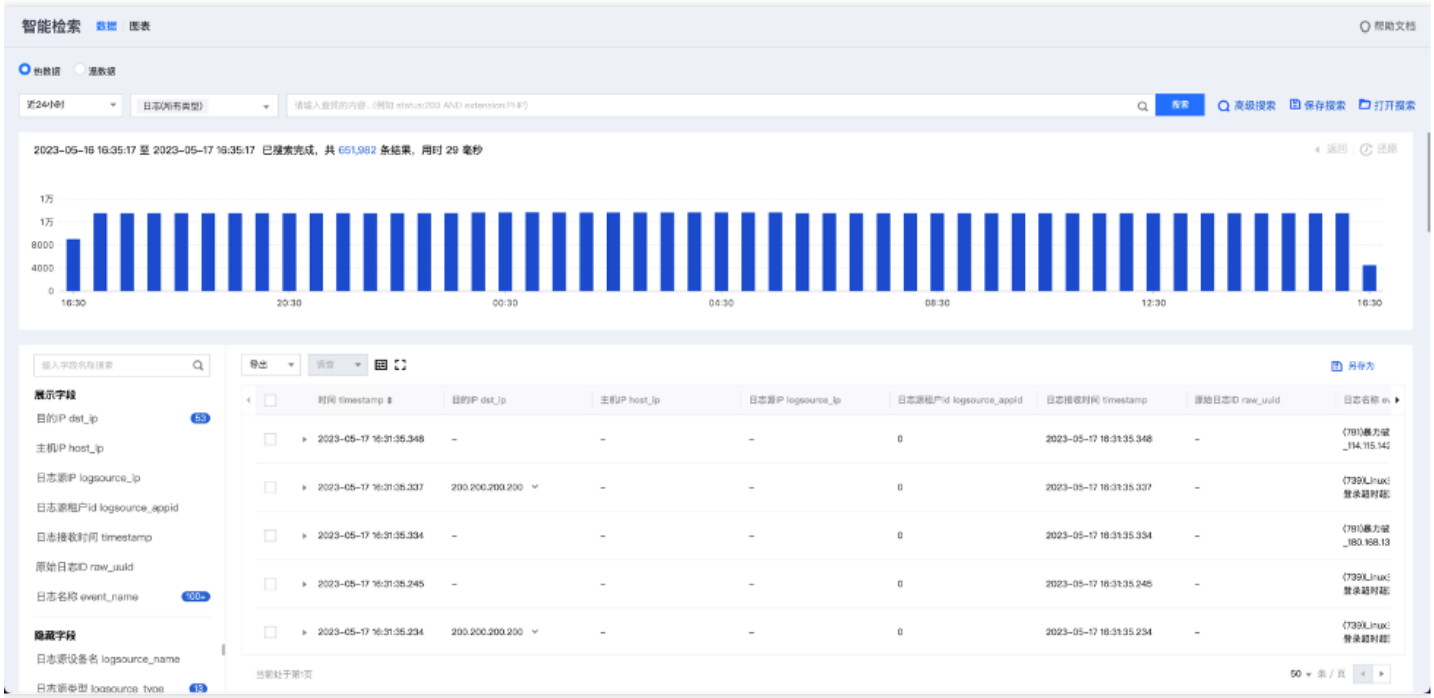
智能检索

最近更新时间: 2024-12-19 17:12:00

管理员可以根据需要对本系统存储的数据进行检索，实现安全威胁的调查与分析。

日志

进入日志检索页面，页面布局如图所示。管理员可以进行高级搜索，将日志导出或生成图表，还可以添加到调查任务。



1、帮助文档/数据源单位

- 日志检索的在线帮助文档，提供三种搜索方式的语法说明。在线查看文档时，单击【下载文档】可将PDF文档下载到本地。
- 在基础版或旗舰版的级联部署模式下，可以切换数据源单位进行日志搜索（本操作仅限超级管理员）。

2、日志搜索框

- 支持时间范围、日志类型和lucene查询语句进行日志搜索；单击【高级搜索】可以通过字段进行更精确的搜索。操作方法详见日志普通/高级检索。

- 单击【保存搜索】可以将当前搜索条件保存为搜索模板，以便于之后的搜索操作；单击【打开搜索】可以直接调用搜索模板并对其进行管理。操作方法详见日志检索模板。

3、日志统计柱状图

展示了符合搜索条件的日志在时间维度上的分布情况，包括时间范围、搜索用时和日志数量。将鼠标悬浮在柱状图上可显示具体时间及其对应的日志数量。

4、日志展示字段配置区

配置日志列表的展示字段，分为展示字段区和隐藏字段区。操作方法详见日志展示字段。

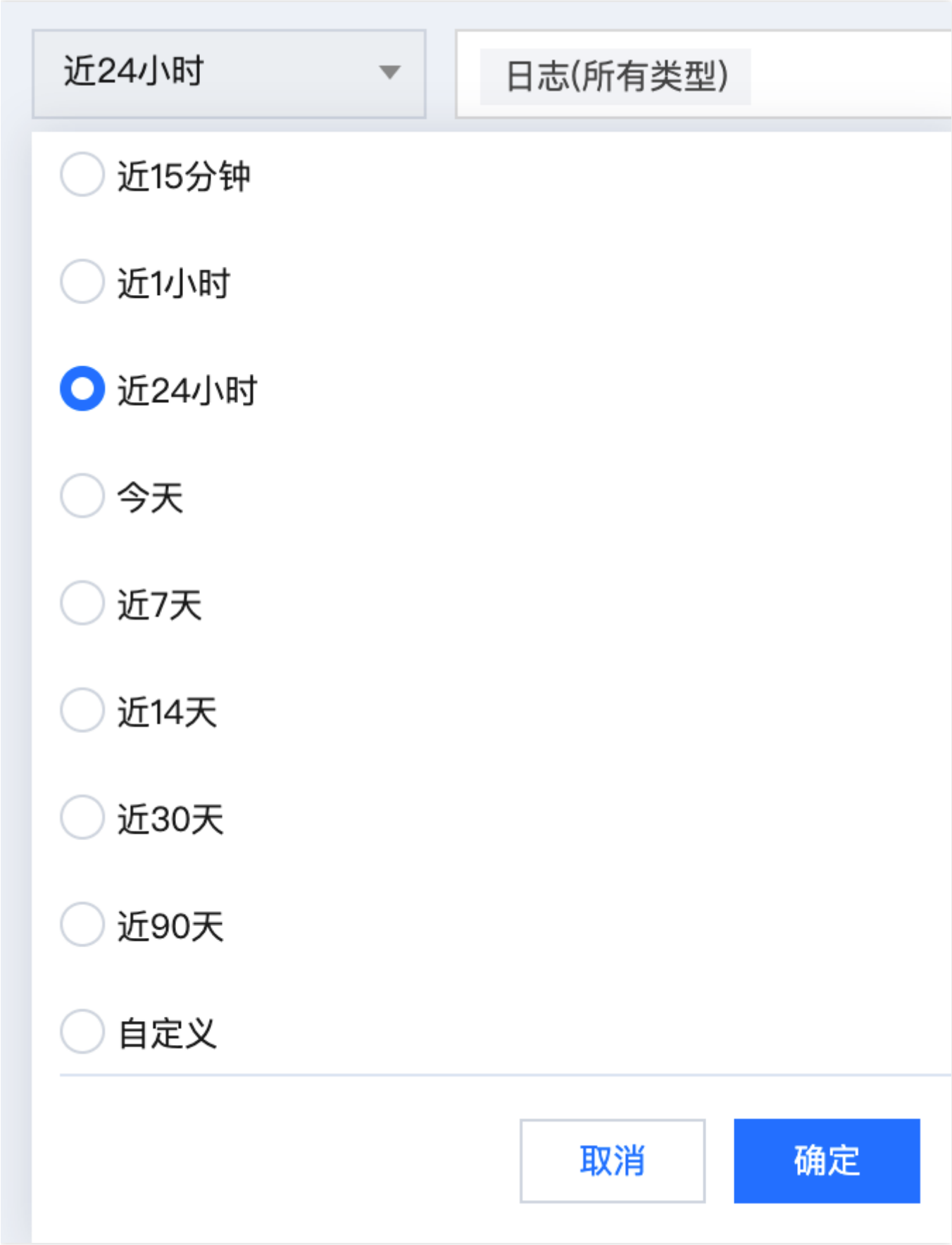
5、日志列表

以列表形式展示了符合搜索条件的日志详情，操作方法详见日志列表。

日志普通/高级检索

- **日志普通检索**
- **检索条件1：时间范围和日志类型**

日志搜索时，时间范围和日志类型不能为空，如图所示。默认情况下，时间范围是“近24小时”，类型是“日志（全部类型）”。


近24小时
日志(所有类型)
近15分钟
近1小时
近24小时
今天
近7天
近14天
近30天
近90天
自定义
取消
确定

日志(所有类型)

请输入查找的内容...(例如 status:2

- 全部数据
  - [ ] 告警
  - [x] 日志
    - [x] 流量分析
    - [x] 主机安全
    - [x] VPN
    - [x] 防火墙
    - [x] IDS/IPS
    - [x] 蜜罐
    - [x] 堡垒机
    - [x] 主机syslog
    - [x] 系统内置
    - [x] 日志分析与审计
    - [x] 终端安全管理系统
    - [x] 邮件安全
  - [ ] 漏洞

- **检索条件2：标签**

通过标签可以进行更精确的日志搜索，同时支持标签的全部清空功能，如图所示。

- **检索条件3：lucene查询语句**

除了以上几个搜索条件，还可以直接输入lucene查询语句进行搜索，如图所示。

- **日志高级检索**

进行日志高级检索之前，系统会清空搜索框中的日志标签。

单击【高级检索】，可以设置多个搜索条件并匹配字段进行日志搜索，如图所示。

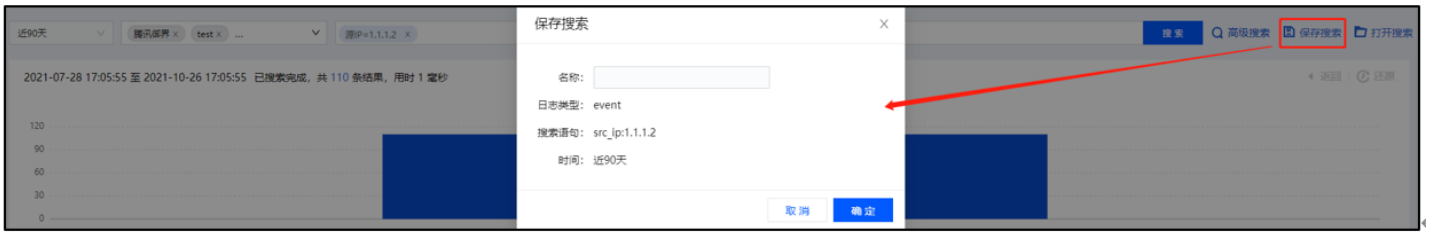
> **说明：**
>
> 关于lucene查询语句的更多介绍，详见官方网址：https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html

日志检索模板

本系统支持检索模板的复用，可以将常用的检索场景进行保存，减少管理员重复操作。

- **保存检索模板**

单击【保存搜索】填写搜索模板名称，即可将当前的检索条件存储为日志搜索模板，如图所示。



- **打开检索模板**

单击【打开搜索】单击某个日志搜索模板，即可快速检索，如图所示。

日志展示字段

可通过字段的展示/隐藏来控制日志列表的展示内容。

- **展示字段**

展示字段，即日志列表的表头。若不想该字段出现在日志列表，单击字段旁边的图标即可下移到隐藏字段区域，如图所示。

- **隐藏字段**

单击隐藏字段旁边的图标即可上移到展示字段区域，该字段出现在日志列表的表头，操作方法与展示字段的基本相同。

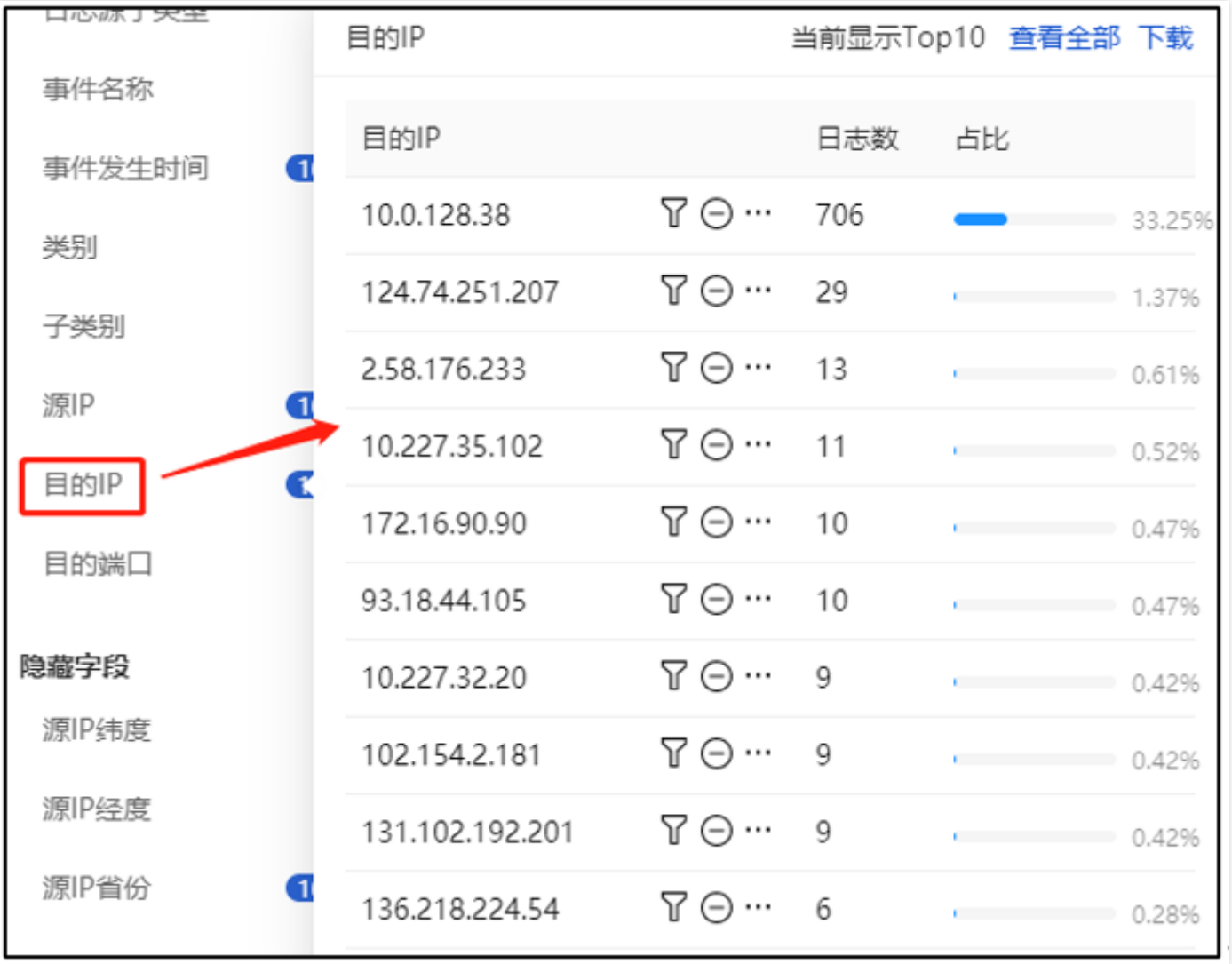
- **搜索字段**

在日志展示字段配置区，可以进行字段的模糊搜索，如图所示。

- **查看字段值列表**

单击某个展示字段名，显示该字段的日志数与占比TOP10，单击【下载】可以将当前日志字段值的全部内容导出为Excel文件，如图所示。

若字段值超过10个，单击【查看全部】即可查看所有字段值。对于源IP和目的IP，还可以单击图标 进行字段值的过滤、排除、新建搜索和新建资产。



日志列表

如图所示，符合搜索条件的日志出现在日志列表中，可以查看每个日志的Table和Json，也可以将所选日志导出、创建调查任务或添加到调查任务中。 单击)可以全屏展示日志列表；若日志字段太多导致日志列表查看不便，可

单击 将所有字段内容切换到列表中显示，如图所示。

响应中心

最近更新时间: 2024-12-19 17:12:00

通过响应中心，可以在发现安全事件或漏洞事件后进一步处置操作。目前支持工单通报，包括人工处置工单和联动SOAR（自动化安全运营平台）的自动处置工单。

处置任务

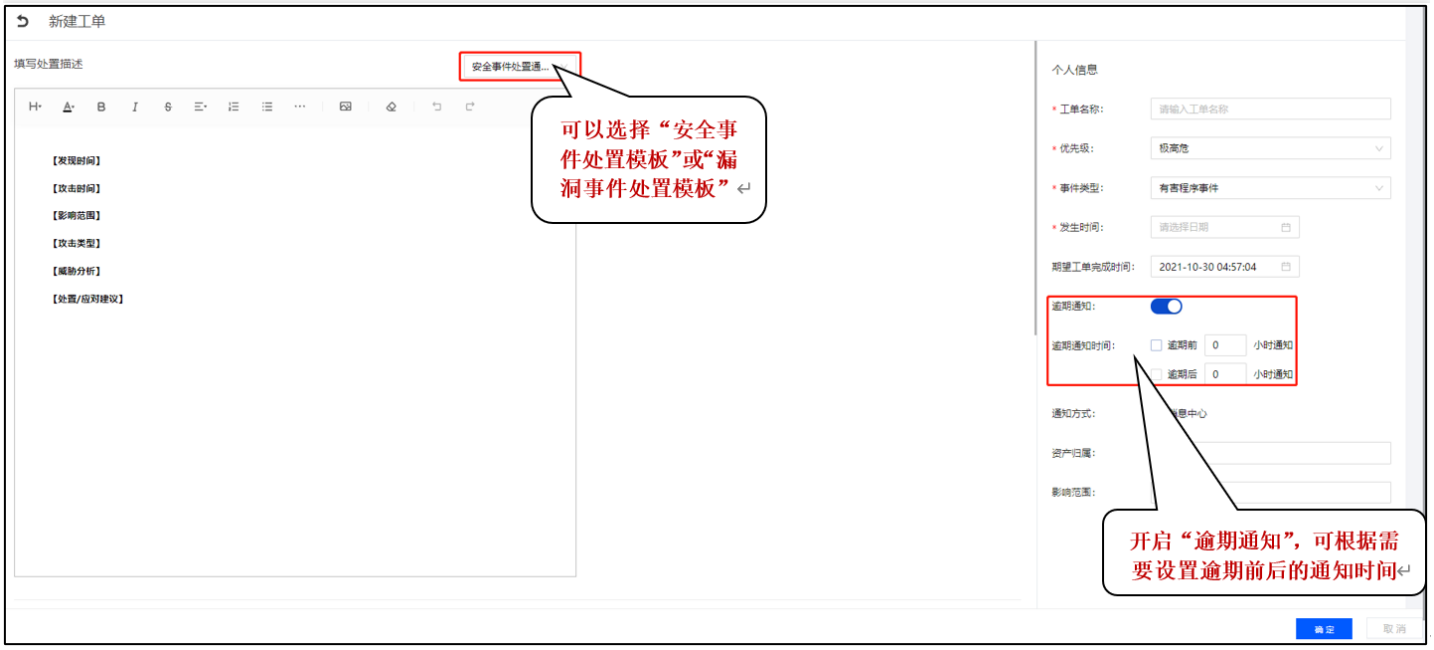
针对本系统分析出的安全告警及资产脆弱性，管理员可通过通报处置工单平台将不同的安全告警、事件及脆弱性按需下发给相关流转组或责任人进行处置，实现安全运营的分级响应与处置。

人工处置工单

进入响应中心 > 处置任务 > 人工处置工单，对于租户用户，只能看到自己创建和负责的工单信息；对于非租户用户，可以看到所有人工处置工单信息，如图所示。 对于超过2个责任人/流转组的工单，将鼠标悬浮在“多个（n）”即可显示具体的责任人或流转组名称。

新建工单

在人工处置工单列表的上方，单击【新建】进入创建工单页面。创建一个完整的工单步骤如下： 步骤1：在新建工单页面右侧填写个人信息，在页面左侧填写处置描述（支持三种模板），如图所示。



步骤2：在新建工单页面左侧填写处置信息。若有告警需要处置，可以选择一个或多个告警，如图43-所示；若有漏洞需要处置，可以选择一个或多个漏洞，如图所示。

步骤3：填写流转信息。选择下一阶段的处置动作、责任人/流转组、期望完成时间和逾期通知时间，如图所示。

步骤4：工单设置完毕，单击【确定】，该工单进入下一阶段，该工单下一阶段的责任人登录系统后会收到新工单的通知。

筛选/搜索工单

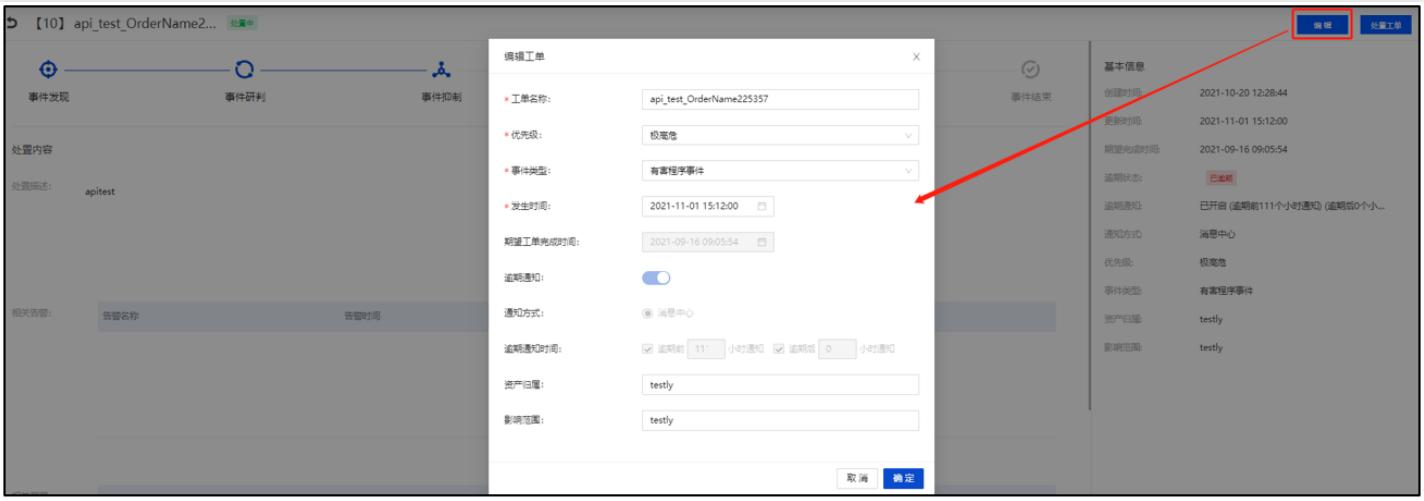
在人工处置工单列表的上方，可以通过以下条件进行人工处置工单的筛选/搜索：

- 时间范围（近24小时、近7天、近30天或自定义起止时间）
- 事件等级（极高危、高危、中危、低危或全部事件等级）
- 事件类型（有害程序事件、网络攻击事件、信息失窃密事件、信息内容安全事件、设备设施故障、灾害性事件、其他或全部事件类型）
- 工单创建人
- 工单责任人
- 工单逾期状态（是、否或全部逾期状态）
- 工单当前的处置动作（事件发现、事件研判、事件抑制、事件根除、事件溯源、事件关闭和全部处置动作）

在人工处置工单列表中，单击表头“ID”、“创建时间”或“工单处置时长”，可以按照工单ID、工单的创建时间或工单处置时长进行排序。

编辑工单

在人工处置工单列表中，单击工单名称即可进入人工处置工单的详情页，只有超级管理员角色的用户才有权限编辑工单。对于当前处置动作为“事件关闭”的工单，无法编辑。 如图所示，除了期望工单完成时间、逾期通知及通知方式，其余各项均可编辑。



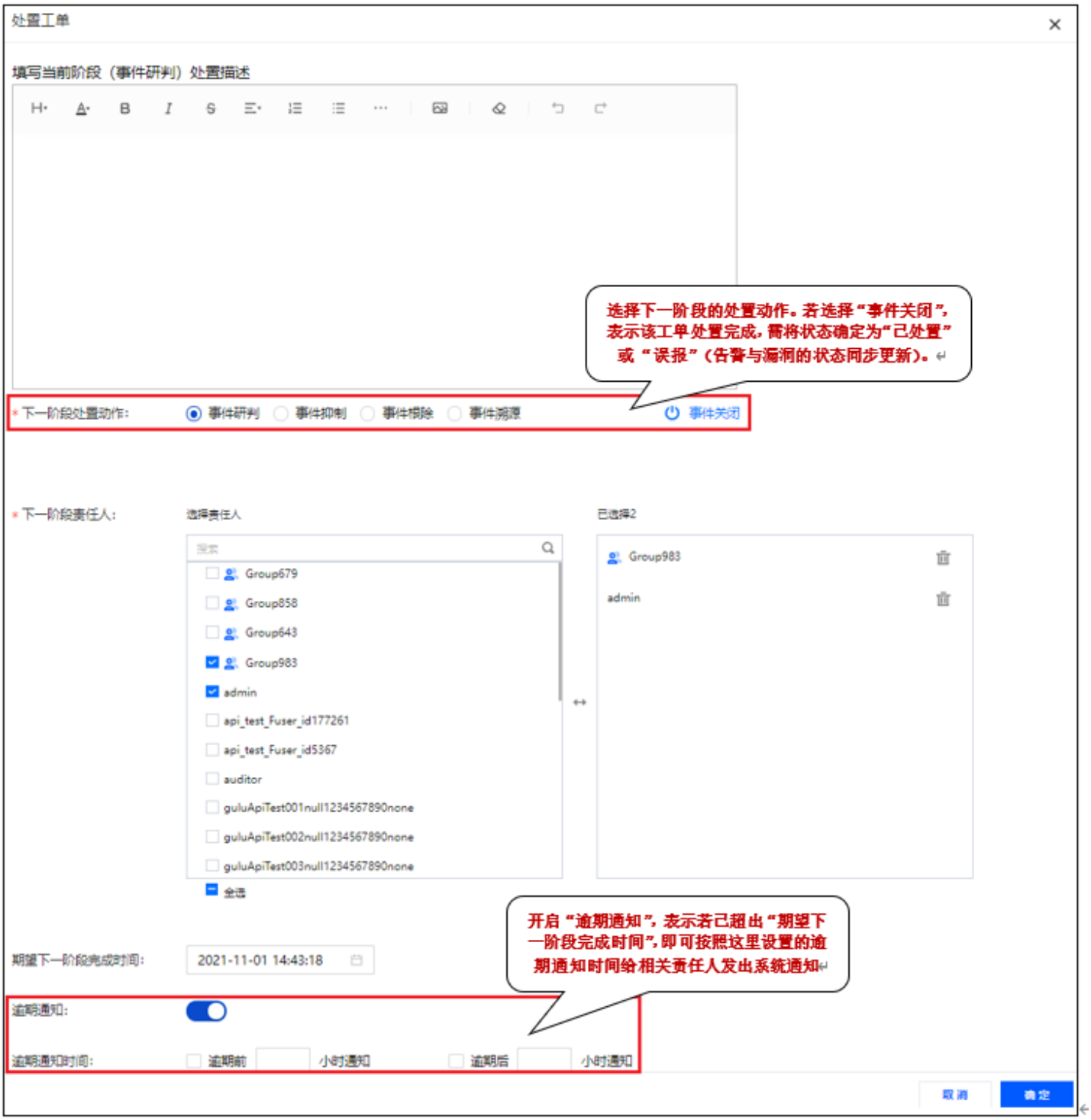
认领工单

在人工处置工单列表中，单击工单名称进入人工处置工单的详情页，认领工单的说明如下：

- 对于当前处置动作为“事件关闭”的工单，无法进行认领工单。
- 若当前用户是当前阶段的处置人或归属在处置组中，可以进行处置工单的操作。
- 若当前用户不是当前阶段的处置人或归属在处置组中，单击【认领工单】即可认领该工单。认领成功后，按钮变为【处置工单】，当前用户被加到当前阶段的处置人中。

处置工单

只有工单的当前责任人，才可进行处置工单的操作。 在人工处置工单列表中，单击工单名称进入人工处置工单的详情页，单击【处置工单】即可进行各项处置操作，如图所示。



删除工单

在人工处置工单列表中，单击【删除】，确认后将删除对应的工单。

> **说明：**
>
> 1. 工单一旦删除，将不可恢复，请谨慎操作。
> 2. 只有工单的创建用户和超级管理员角色，才有删除工单的权限。

报表中心
说明

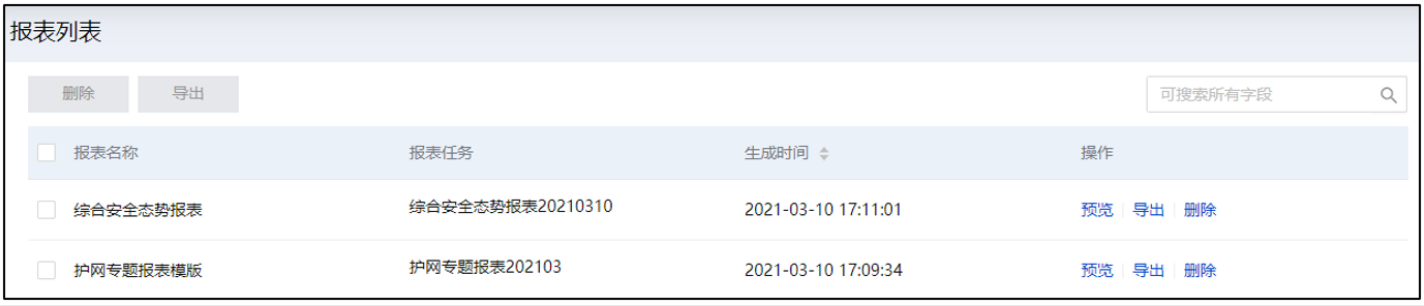
最近更新时间: 2024-12-19 17:12:00

本系统内置两种报表模板，可根据需求选择时间范围和资产范围对安全告警情况、资产风险情况及脆弱性情况等进行统计和呈现，并可将报表导出为PDF文件。

报表列表

最近更新时间: 2024-12-19 17:12:00

初始状态下，报表列表为空。只有在创建并生成报表任务之后，才会出现在报表列表中，并可对已生成的报表进行搜索、删除、导出和预览操作，如图所示。



报表任务

最近更新时间: 2024-12-19 17:12:00

报表任务分为单次报表任务和周期报表任务。

单次报表任务

进入报表中心 > 报表任务 > 单次报表任务，可以立即创建报表任务，如图所示。 单次报表任务创建后自动生成，并出现在单次报表任务列表中，如图所示。

报表任务
* 任务名称：
请输入任务名称
报告描述：
报告中展示的描述内容
报表模板：
综合安全态势报表
时间范围：
近24小时
包含资产：
所有分组
数据展示：
Top10
邮件发送：
* 收件人：
* 邮件标题：
邮件正文：
开启此功能，系统自动发送报表到指定邮箱
取 消
确 定

周期报表任务

进入报表中心 > 报表任务 > 周期报表任务，可以按“每日一次”、“每周一次”或“每月一次”创建周期报表任务，如图所示。 创建成功的任务出现在周期报表任务列表中，开启任务后，即可按指定时间生成报表，如图所示。

报表任务
任务启停：
* 任务名称：
请输入任务名称
报告描述：
报告中展示的描述内容
报表模板：
综合安全态势报表
时间范围：
近24小时
包含资产：
所有分组
数据展示：
Top10
重复：
每天一次
生成时间：
每天一次
17:00:00
邮件发送：
* 收件人：
* 邮件标题：
邮件正文：
开启此功能，系统自动
发送报表到指定邮箱

新建
删除
任务名称/创建人
任务名称
报表模板
包含资产组
时间范围
创建人
下一次启动时间
任务启停
操作
护网专题报表2020
护网专题报表模版
所有分组
近一年
admin
2021-03-31 23:00:00
编辑
删除
周报
综合安全态势报表
所有分组
近24小时
admin
2021-03-15 17:00:00
编辑
删除

常见问题

常见问题

最近更新时间: 2024-12-19 17:12:00

安全运营中心支持接入哪些设备日志？

安全运营中心支持接入TCE上的主机安全、Web应用防火墙（WAF）、高级威胁检测系统（INTA）、堡垒机（BH），运营端还支持接入underlay层面的安全设备日志，对整个云平台安全做分析检测。

安全运营中心可以管控安全设备吗？

安全运营中心定位为感知分析，将流量、日志等数据汇聚后，进一步关联分析与展现。安全运营中心 不对其他设备进行管理与控制。

安全运营中心是如何发现资产的？

资产主动发现是从日志和其他接入数据源，提取其中的源目IP放到资产发现列表，可注册到资产列表。

安全运营中心是否支持ipv6环境使用？

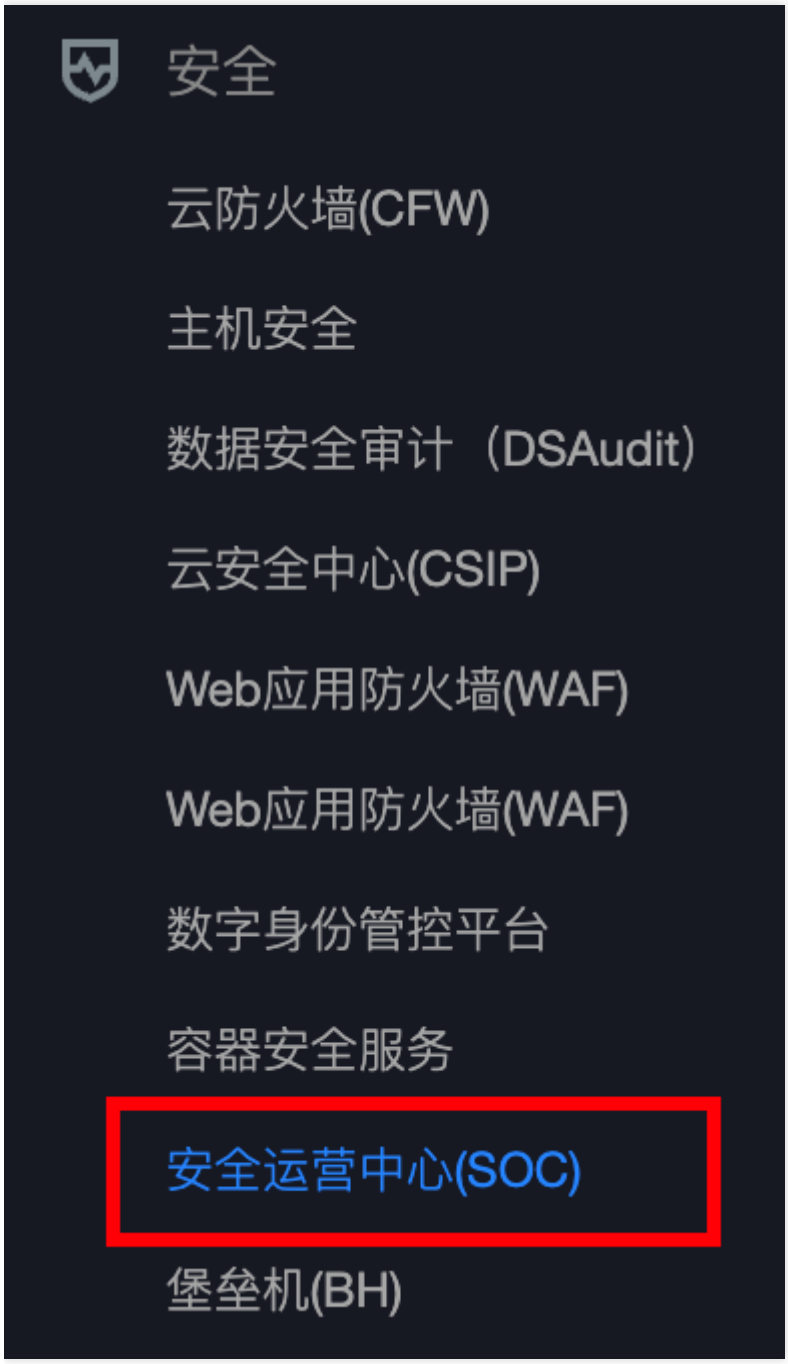
安全运营中心支持ipv4和ipv6的数据接入、告警检出、资产和漏洞列表的使用。

安全运营中心对国产化/信创的支持程度？

TCE版本	CPU/架构	架构	操作系统
3100	海光-7280	x86	tlinux 2.4 (5.4.119-19-0008) x86_64
3100	FT-2500	arm	Tlinux2.4 (4.14.105-19-0004) aarch64
3100	鲲鹏-920	arm	Tencent tlinux release 2.4 for ARM64 5.4.119-19-0008 aarch64

如何购买安全运营中心？

安全运营中心提供租户端使用，租户如果未开通产品，控制台点击产品会弹出开通页面，点击开通即可。


安全
云防火墙(CFW)
主机安全
数据安全审计（DSAudit）
云安全中心(CSIP)
Web应用防火墙(WAF)
Web应用防火墙(WAF)
数字身份管控平台
容器安全服务
安全运营中心(SOC)
堡垒机(BH)

词汇表

词汇表

最近更新时间: 2024-12-19 17:12:00

原始数据

data/raw_msg从其他环境（IDC环境、云环境、混合环境等）、第三方设备数据源采集的原始数据，包括日志和流量。流量通常仅支持御界的流量通信日志，日志通常包括：第三方安全设备告警日志、御界告警日志、系统日志（linux/Win）、应用日志等。

日志

event/log经过SOC归一化引擎，将多源异构数据进行采集、解析、归一化和补充上下文信息后的泛化数据，方便用户进行统一的检测与分析。

告警

alarm经过SOC威胁检测模块（关联分析、UEBA）对日志进行检测分析，日志命中规则或策略后产生的结果，该结果待用户进行闭环处置。

事件/安全事件

incident经过SOC的自动化调查引擎，将相关联的告警数据根据时间线、资产和ATT&CK技战术串联起来，生成一个待响应处置的安全事件，并给出严重级别、事件描述和处置建议。目的是将需要人工介入和关注的严重事件收敛至合理的数量级。

TI

TI（Threat intelligence）是威胁情报的简称，是基于背景、机制、指标、影响和可采取行动等证据、知识或建议，涉及对资产的现有或新出现的威胁或危害，可用于为有关主体应对措施的决定，提供这种威胁或危险的信息。

沙箱

沙箱（Sandbox）是一个在沙盘环境中运行浏览器或其他程序的虚拟系统程序，因此运行所产生的变化可以随后删除。它创造了一个类似沙盒的独立作业环境，在其内部运行的程序并不能对硬盘产生永久性的影响。

IDS

IDS（Intrusion Detection System）是入侵检测系统的简称，是一种对网络传输进行即时监视，在发现可疑传输时，发出警报或者采取主动反应措施的网络安全设备。

态势感知

态势感知（Situation Awareness）是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。

威胁狩猎

威胁狩猎（Threat Hunting）通过主动和交互式搜索网络数据的过程，来挖掘和处置一些能逃避现有安全解决方案的高级威胁。

ETL

ETL 是 Extract-Transform-Load 的缩写，即提取、转化、存储。用来描述将数据从来源端经过抽取（extract）、交互转换（transform）、加载（load）至目的端的过程。