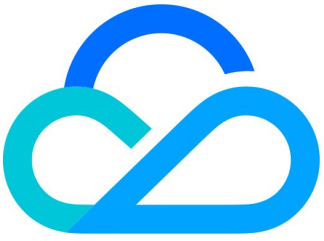
安全运营中心

操作指南



腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

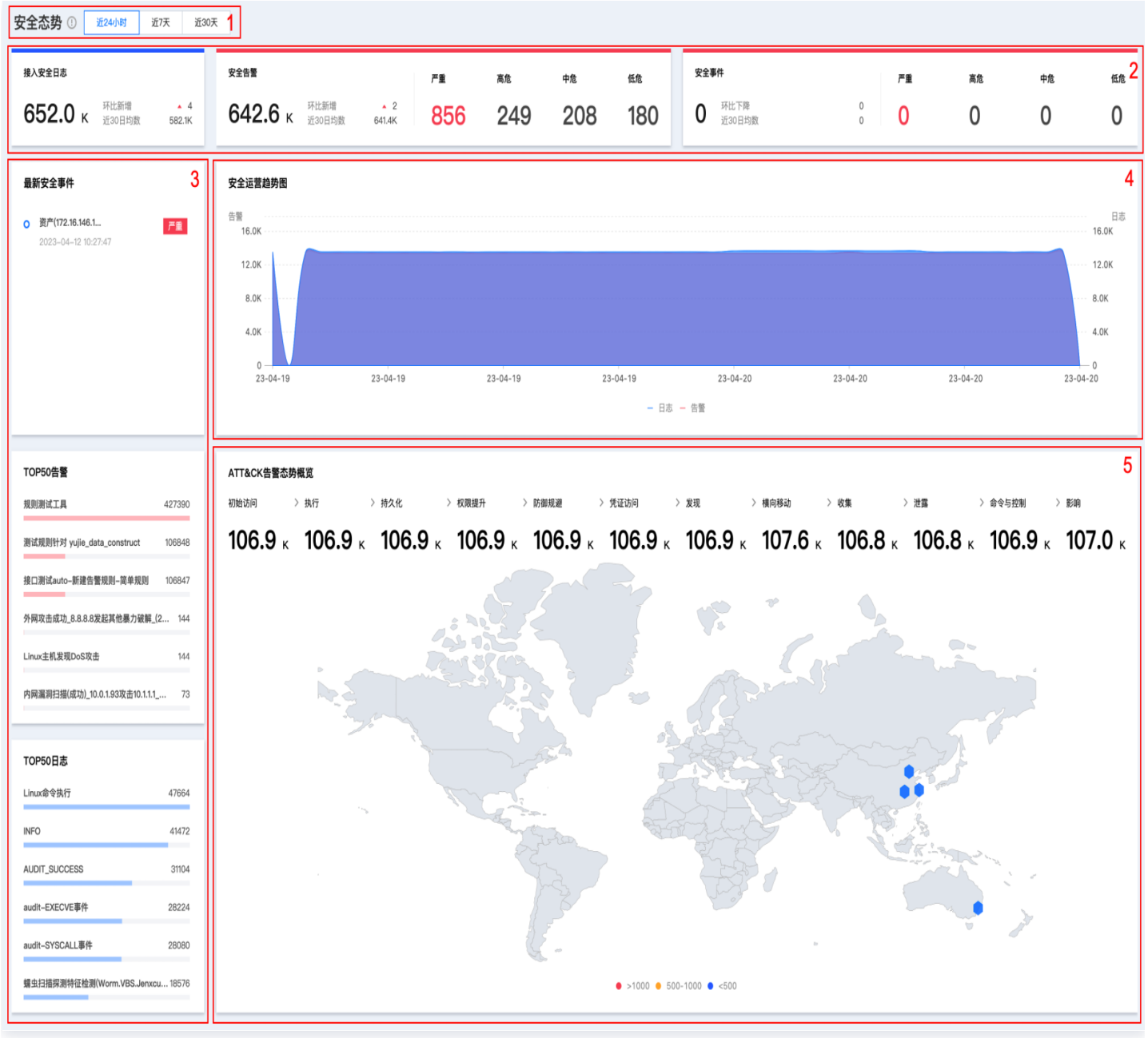
文档目录

操作指南
安全可视

最近更新时间：2024-12-17 18:09:02

安全态势

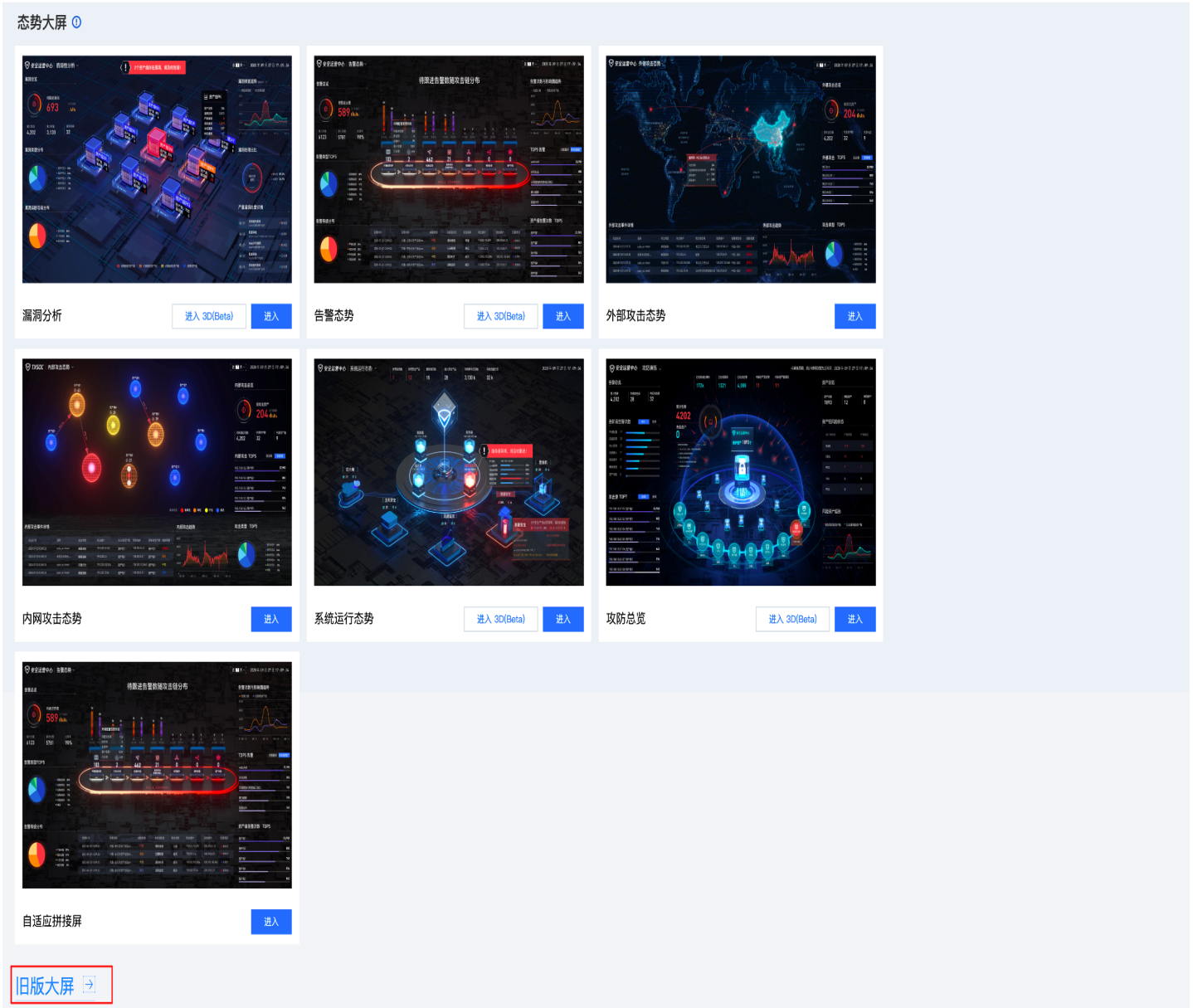
在**安全可视 > 安全态势**页面，数据监测能够帮助安全运维人员及时发现和处理威胁，以便于有效洞察企业面临的外部威胁和内部脆弱性风险，提高安全运维团队监测、管理、处置安全事件的效率。
在**安全可视 > 安全态势**页面，可以查看企业在全网范围内的安全日志、安全告警、安全事件数量，TOP 排行，安全运营趋势图，ATT&CK 告警态势概览。展示方式包括安全评分、趋势图、条形图和分布图等，如图所示。



态势大屏

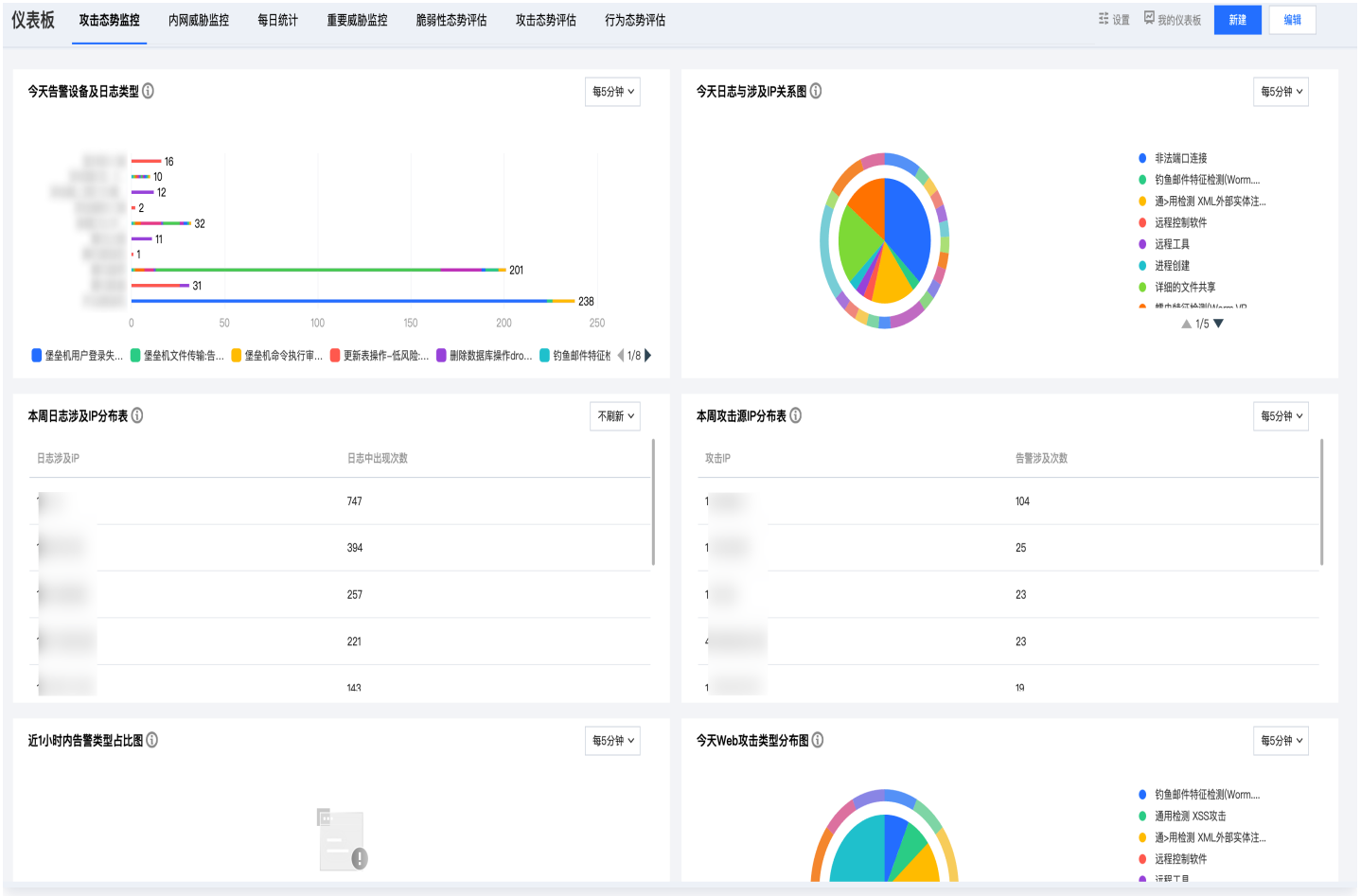
在**安全可视** > **态势大屏**页面，包括七块3D大屏（漏洞分析大屏、告警态势大屏、外部攻击态势大屏、内网攻击态势大屏、系统运行态势大屏、攻防总览大屏、自适应拼接屏）。以及通过单击左下方的**旧版大屏**，可切换为七块2D大屏（综合态势大屏、攻击态势大屏、资产态势大屏、威胁大屏、脆弱性态势大屏、流量态势大屏、租户安全运营大屏）。

单击**进入**后，即可显示相应的大屏。在3D大屏中，选择**大屏名称**，便可切换至相应的大屏界面。



仪表板

在**安全可视 > 仪表板**页面，可以根据攻击态势、威胁、脆弱性态势和攻击态势等以仪表板的形式进行监控，还可以使用本系统的组件库新建仪表板，页面布局如图所示。



安全专题

在**安全可视 > 安全专题**页面，针对安全运营中常见的几种关键安全场景，SOC 将以安全专题的形式向安全运营管理人员展示，以便重点关注和分析。

报表中心

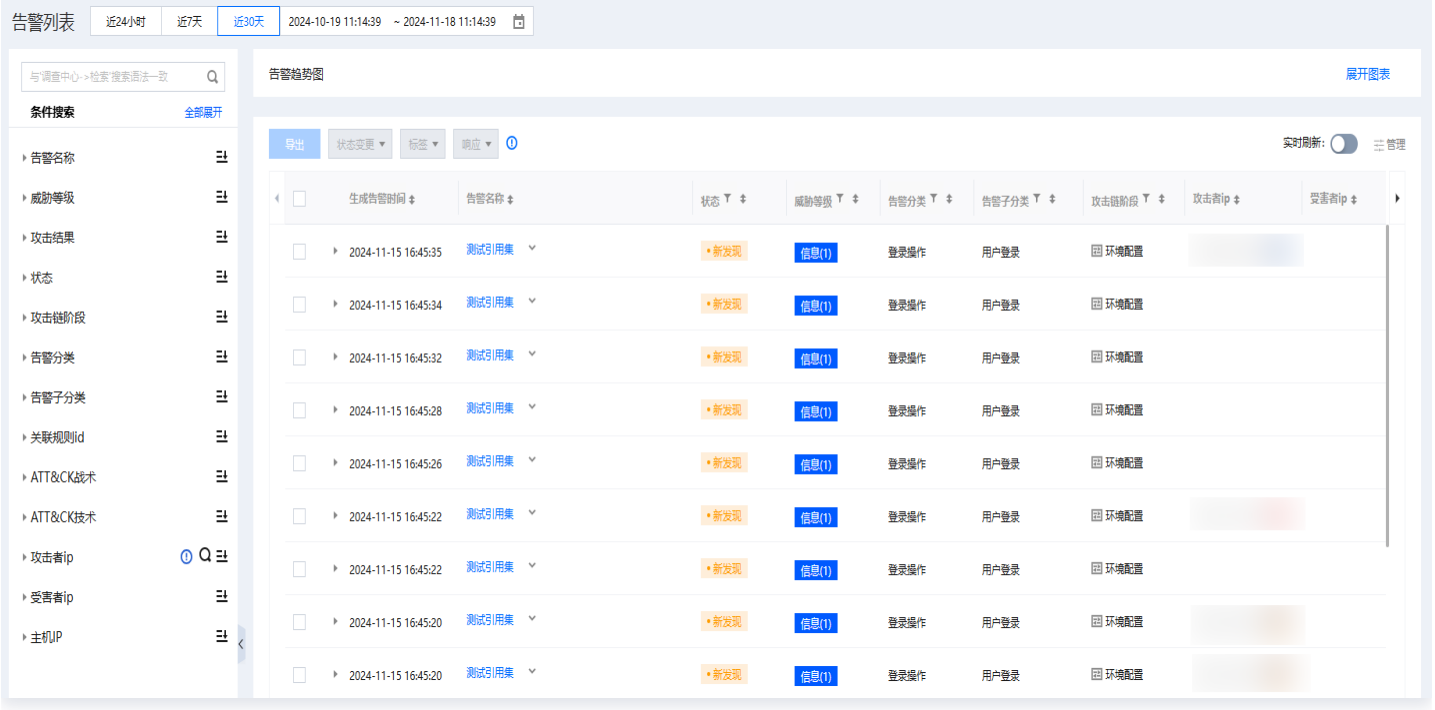
在**安全可视 > 报表中心**页面，内置了两种报表模板，可根据需求选择时间范围和资产范围对安全告警情况、资产风险情况及脆弱性情况等进行统计和呈现，并可将报表导出为 PDF 文件。

安全检测

最近更新时间：2024-12-17 18:09:02

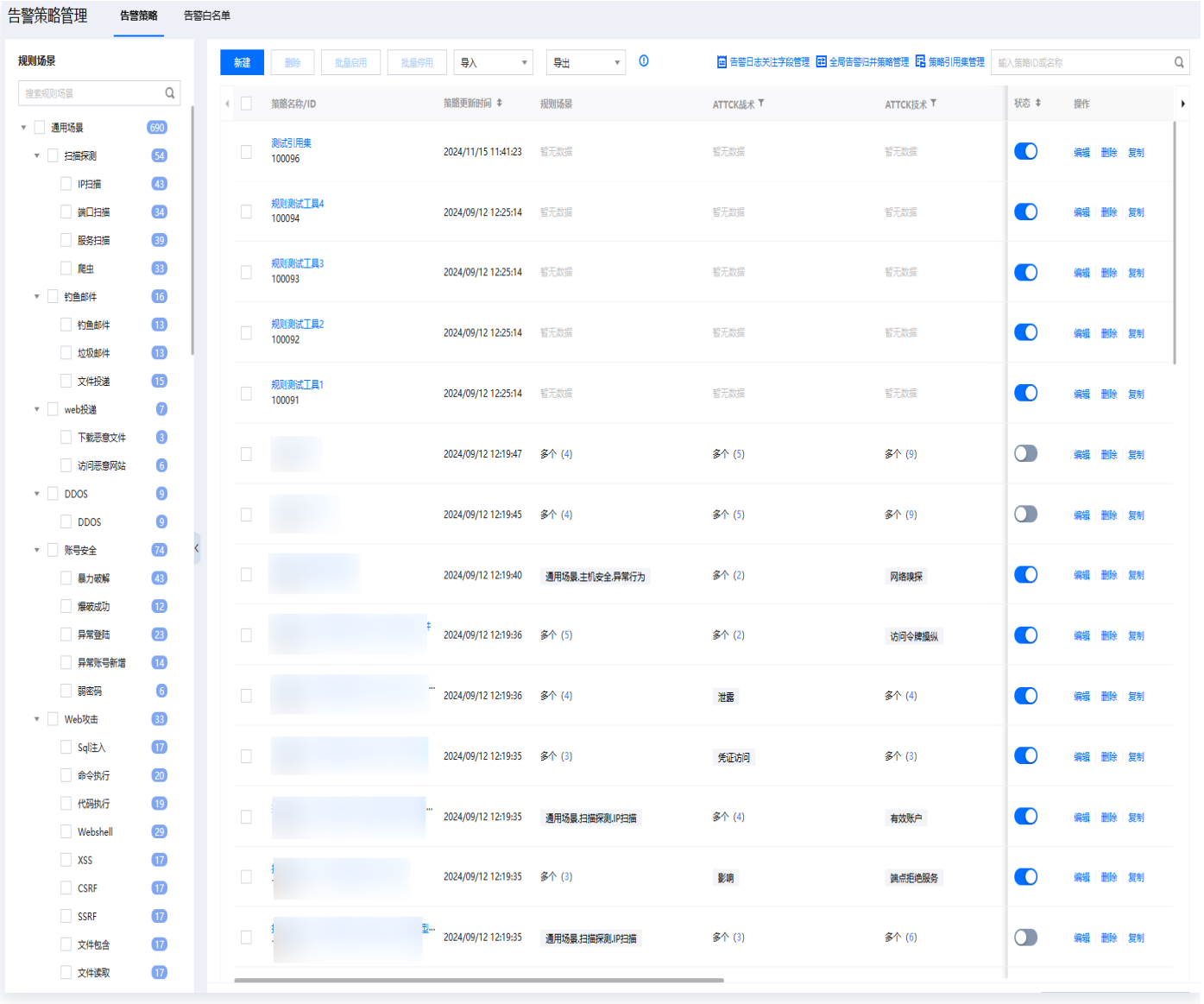
告警列表

在安全检测 > 告警列表页面，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。



关联分析

1. **在安全检测 > 关联分析页面，选择告警策略管理。**
2. **在告警策略管理页面，管理员可以创建触发告警的策略并对其编辑和删除，也可以对全局告警归并策略和策略引用集进行管理。**



威胁情报

SOC 集成威胁情报本地查询功能，安全人员可以针对指定 ioc 查询情报信息，支持自定义，利用情报能力获得更快速更精准的检测与响应。

1. 在**安全检测 > 威胁情报**页面，选择**威胁情报查询**。
2. SOC 平台集成本地威胁情报查询页面，可主动对 ioc 查询，支持单次和批量查询，方便研判分析。

行为分析

在**安全检测 > 行为分析**页面，可以检测组织可能面临的高级网络威胁、内部人员风险等常规安全方案难以覆盖的风险点，进而提升整个安全运营态势。

智能检测

在**安全检测 > 智能检测**页面，通过对流量日志进行基于深度学习的 AI 智能检测，能够进行安全检测与分析。

ATT&CK 能力矩阵

SOC 基于 ATT&CK 知识矩阵构建安全检测评价体系，提供2个维度的覆盖率展示，包括关联策略和关联告警。
SOC 平台内置 MITRE ATT&CK V10 矩阵，及相关知识库，共12个战术阶段，188个技术点。
在**安全检测 > ATT&CK 能力矩阵**页面，直观展示当前关联规则覆盖的 ATT&CK 矩阵，包括覆盖每个战术、技术的关联规则数及列表，并能根据 ATTCK 技术名词、关联规则名称进行搜索。

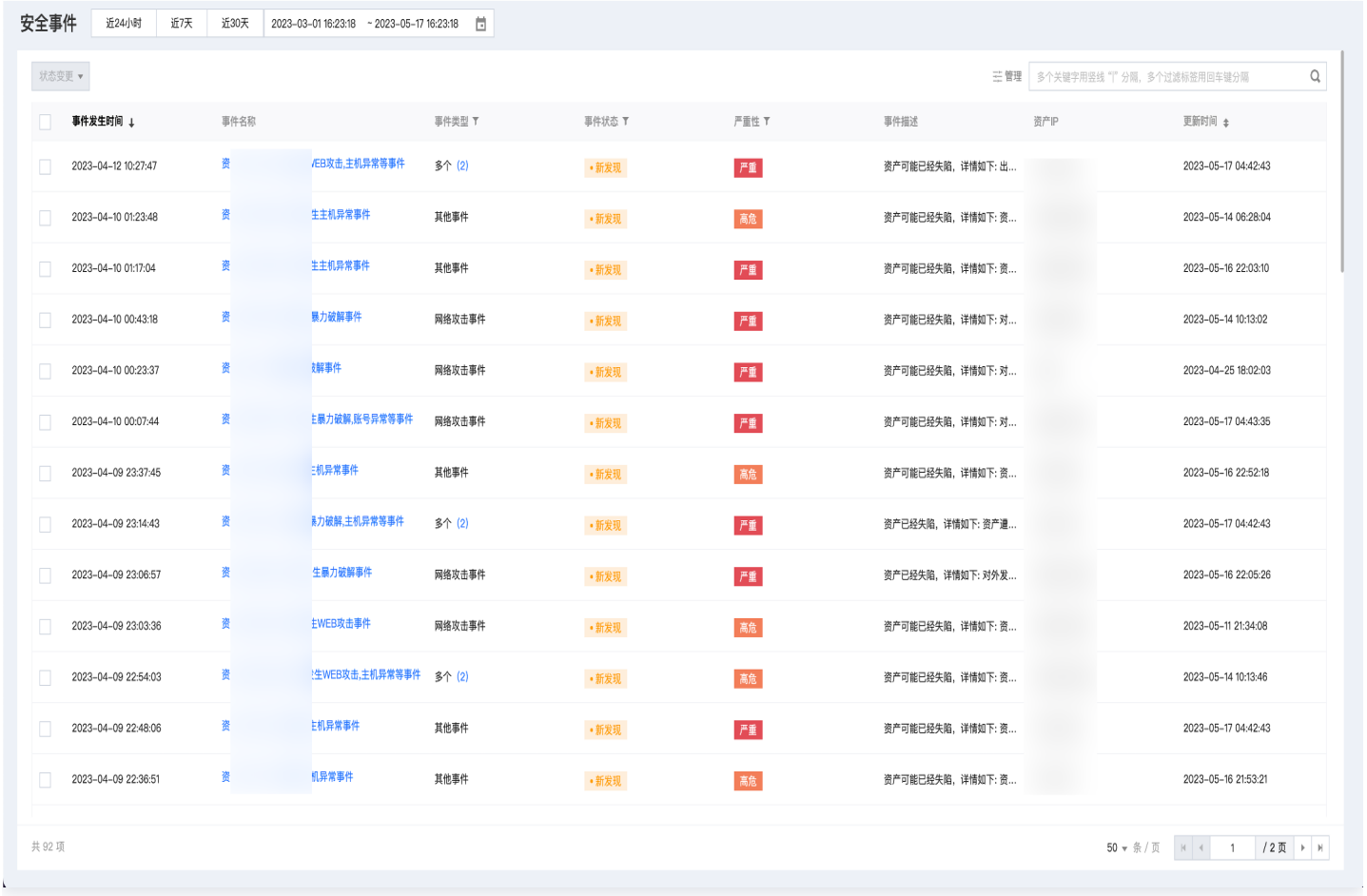

ATT&CK能力矩阵
关联策略
关联告警
全部状态策略
输入ATT&CK技术名称、告警策略名称以搜索告
初始访问 103 策略 9 /9技术
执行 95 策略 10 /12技术
持久化 154 策略 15 /19技术
权限提升 148 策略 13 /13技术
防御规避 210 策略 31 /39技术
凭证访问 118 策略 12 /15技术
发现 69 策略 25 /27技术
横向移动 76 策略 9 /9技术
收集 36 策略 13 /17技术
命令与控制 82 策略 14 /16技术
泄露 28 策略 8 /9技术
影响 94 策略 13 /13技术
网络钓鱼(38)
命令与脚本解释器(35)
创建账户(7)
计划任务/作业(6)
在主机上构建映像
中间人(4)
网络服务扫描(13)
远程服务(23)
自动收集(1)
远程访问软件(15)
通过 Web 服务泄露(7)
固件损坏(1)
硬件添加(6)
WMI Windows 管理规范(18)
浏览器扩展
创建或修改系统进程(7)
修改系统镜像
操作系统凭证转储(38)
云服务发现(1)
通过可移动媒体复制(6)
来自信息库的数据(1)
Web 服务(9)
数据传输大小限制(4)
网络拒绝服务(4)
通过可移动媒体复制(6)
原生 API(5)
植入内部镜像
事件触发执行(15)
混淆的文件或信息(6)
双因素身份验证拦截
网络嗅探(17)
软件部署工具(14)
电子邮件收集(5)
数据编码
通过 C2 通道进行泄露(1)
为影响而加密的数据(20)
路过式攻击(8)
计划任务/作业(6)
账户操作(8)
劫持执行流程(12)
执行护栏
窃取或伪造 Kerberos 票证(5)
系统信息发现(1)
横向工具转移(15)
中间人(4)
非标准端口(2)
通过其他网络介质进行泄露(4)
资源劫持(11)
利用面向公众的应用程序(28)
容器管理命令(1)
BITS任务(1)
特权提升的利用(4)
直接卷访问(1)
伪造 Web 凭据(3)
系统所有者/用户发现(2)
使用替代身份验证材料(9)
视频截取
入口工具传输(3)
将数据传输到云账户(4)
磁盘擦除(2)
有效账户(56)
共享模块
攻陷客户端软件二进制文件
启动或登录初始化脚本(3)
访问令牌操纵(5)
修改认证流程(2)
云基础设施发现(1)
远程服务会话劫持(2)
来自云存储对象的数据(4)
交通信号(6)
通过物理介质进行泄露(1)
数据销毁(22)
外部远程服务(9)
进程间通信(1)
在操作系统前启动
进程注入(18)
BITS任务(1)
强制认证(6)
账户发现(5)
利用远程服务(19)
浏览器中的人攻击
多级通道(1)
计划传输(14)
损毁(2)
供应链攻击(13)
部署容器
事件触发执行(15)
有效账户(56)
修改云计算基础设施(2)
网络嗅探(17)
远程系统发现(2)
污染共享内容(1)
屏幕截图(2)
协议隧道(4)
替代协议上的泄露(4)
系统关闭/重启(3)
信任关系(5)
利用客户端执行(13)
劫持执行流程(12)
访问令牌操纵(5)
签名二进制代理执行(15)
来自密码存储的凭据(4)
文件和目录发现(3)
内部鱼叉式网络钓鱼(1)
剪贴板数据(1)
应用层协议(12)
自动泄露
端点拒绝服务(12)
污染共享内容（Taint Shared Content） 子技术 0
攻击者可以通过向共享存储位置（例如网络驱动器或内部代码存储库）添加内容来向远程系统提供有效载荷。存储在网络驱动器或其他共享位置的内容可能会因向其他有效文件添加恶意程序、脚本或漏洞利用代码而受到污染。一旦用户打开共享的受污染内容，就可以执行恶意部分以在远程系统上运行对手的代码。攻击者可能会使用受污染的共享内容横向移动。 目录共享数据透视是此技术的一种变体，它使用其他几种技术在用户访问共享网络目录时传播恶意软件。它使用目录 .LNK 文件的快捷方式修改，使用伪装着起来像真实的目录，这些目录通过Hidden Files 和 Directories 隐藏。基于 .LNK 的恶意目录具有嵌入式命令，该命令执行目录中隐藏的恶意软件文件，然后打开真正的预期目录，以便用户的预期操作仍然发生。当与经常使用的网络目录一起使用时，该技术可能会导致频繁的再感染和对系统的广泛访问，并可能导致对新的和更高特权的账户的访问。 攻击者还可以通过将其代码附加或预先添加到共享网络目录上的健康二进制文件中来通过二进制感染破坏共享网络目录。恶意软件可能会修改健康二进制文件的原始入口点 (OEP)，以确保它在合法代码之前执行。当远程系统执行新感染收起
1 条策略已关联 前往策略列表查看
策略名称/ID
策略更新时间
规则场景
威胁等级
告警分类
告警子类
攻击结果
状态
多个 (12)
自动计算
自动计算
自动计算
自动计算

调查中心

最近更新时间：2024-12-17 18:09:02

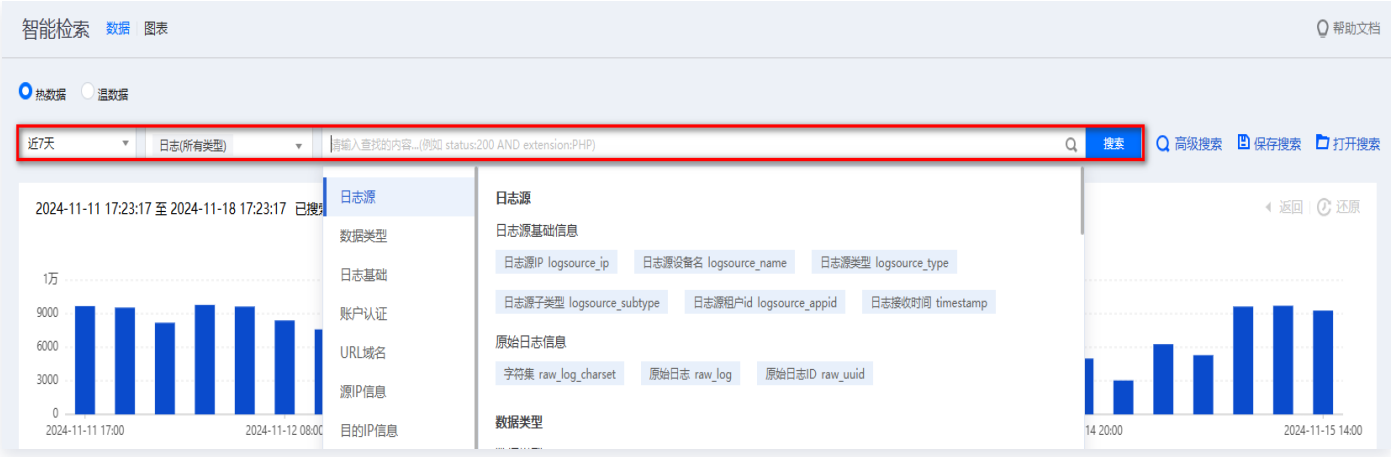
安全事件

在**调查中心 > 安全事件**页面，支持针对告警线索展开自动化调查，生成待处置分析的安全事件。支持自动将威胁告警基于影响资产、时间线、ATT&CK 技战术进行关联，自动还原攻击过程，采集战术、技术、过程和相关上下文，以及受影响资产信息，并给出安全事件的严重级别、类型、描述和处置建议等。



智能检索

1. 在**调查中心 > 智能检索**页面，您可以根据时间、数据类型以及所需查找的内容进行搜索，单击**搜索**生成图表，管理员支持进行高级搜索。



2. 选择所筛选出的目标日志，单击**导出**，可将日志下载至本地；单击**调查**，可将日志添加到调查任务。

调查任务

- 在**调查中心 > 调查任务**页面，支持按照时间范围、ID、调查名称、创建人进行搜索。

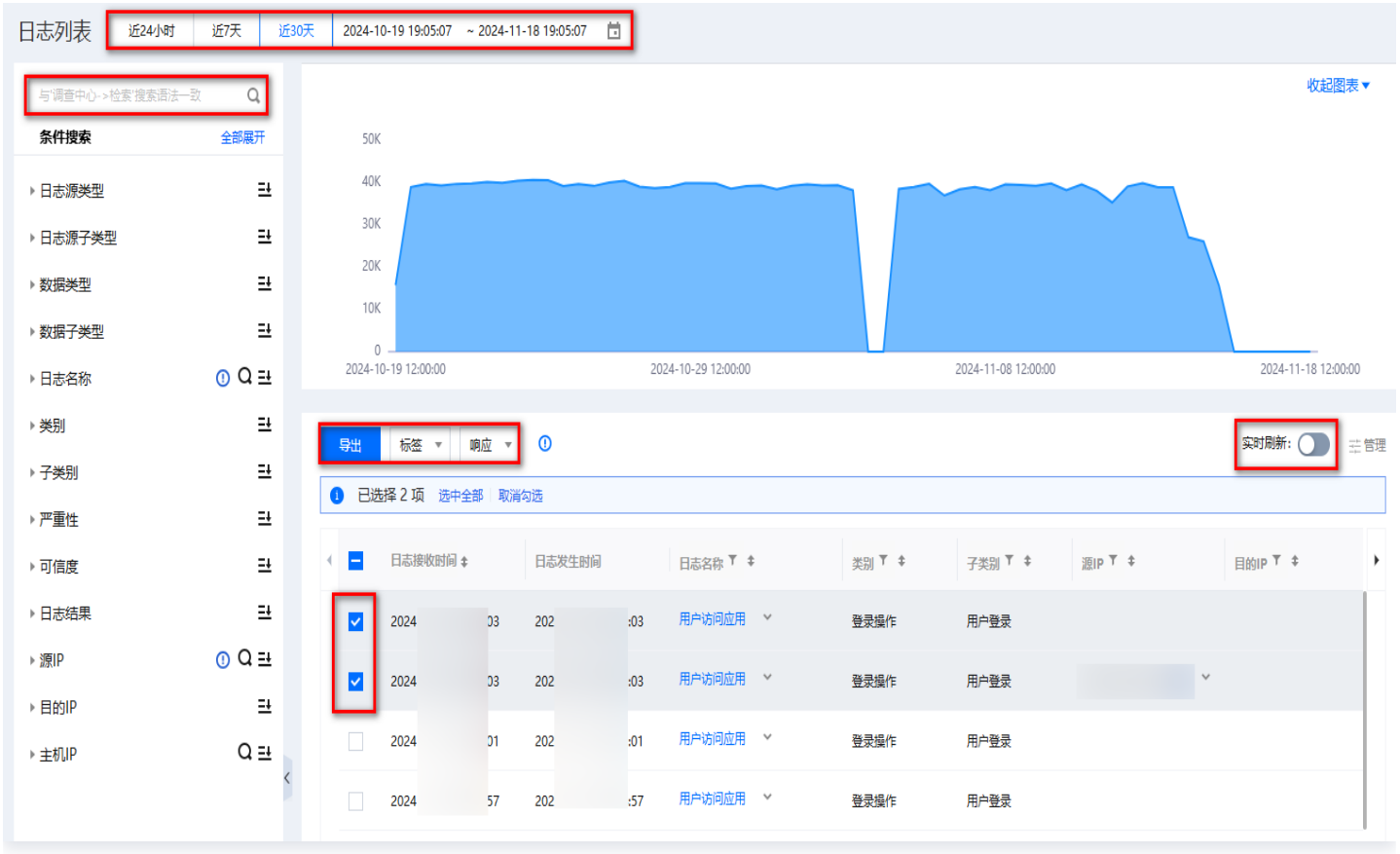
- 在**调查中心 > 调查任务**页面，管理员单击**新建**，输入任务名称和任务说明，单击**确定**即可新建调查任务。

- 在**调查中心 > 调查任务**页面，选择目标 ID 并单击**详情**，支持对调查任务进行编辑、导出、删除和结束任务。

日志列表

在**调查中心 > 日志列表**页面，管理员可以查看日志趋势和日志详情，还可进行日志的导出、响应和搜索等操作。

- 单击**实时刷新开关**，支持开启实时刷新事件信息功能。
- 支持根据时间范围、日志名称、类别、子类别、源 IP、目的 IP 等参考筛选所需日志，查看日志趋势和日志详情。
- 选择所需日志，支持进行日志导出、标签-添加标签/删除标签、响应操作。


日志列表
近24小时
近7天
近30天
2024-10-19 19:05:07 ~ 2024-11-18 19:05:07
与'调查中心->检索'搜索语法一致
条件搜索
全部展开
日志源类型
日志源子类型
数据类型
数据子类型
日志名称
类别
子类别
严重性
可信度
日志结果
源IP
目的IP
主机IP
收起图表
50K
40K
30K
20K
10K
0
2024-10-19 12:00:00
2024-10-29 12:00:00
2024-11-08 12:00:00
2024-11-18 12:00:00
导出
标签
响应
实时刷新:
管理
已选择 2 项
选中全部
取消勾选
日志接收时间
日志发生时间
日志名称
类别
子类别
源IP
目的IP
用户访问应用
登录操作
用户登录

响应中心

最近更新时间：2024-12-17 18:09:02

通过响应中心，管理员可以在发现安全日志或漏洞日志后进一步处置操作。目前支持工单通报，包括人工处置工单和联动 SOAR 的自动处置工单。

处置工单

在**响应中心** > **处置工单**页面，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、漏洞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。

通知策略

在**响应中心** > **通知策略**页面，可以对本系统产生的安全告警设置通知策略，通过系统消息、邮件或短信进行通知，实现威胁信息的及时获取与感知。

联动响应

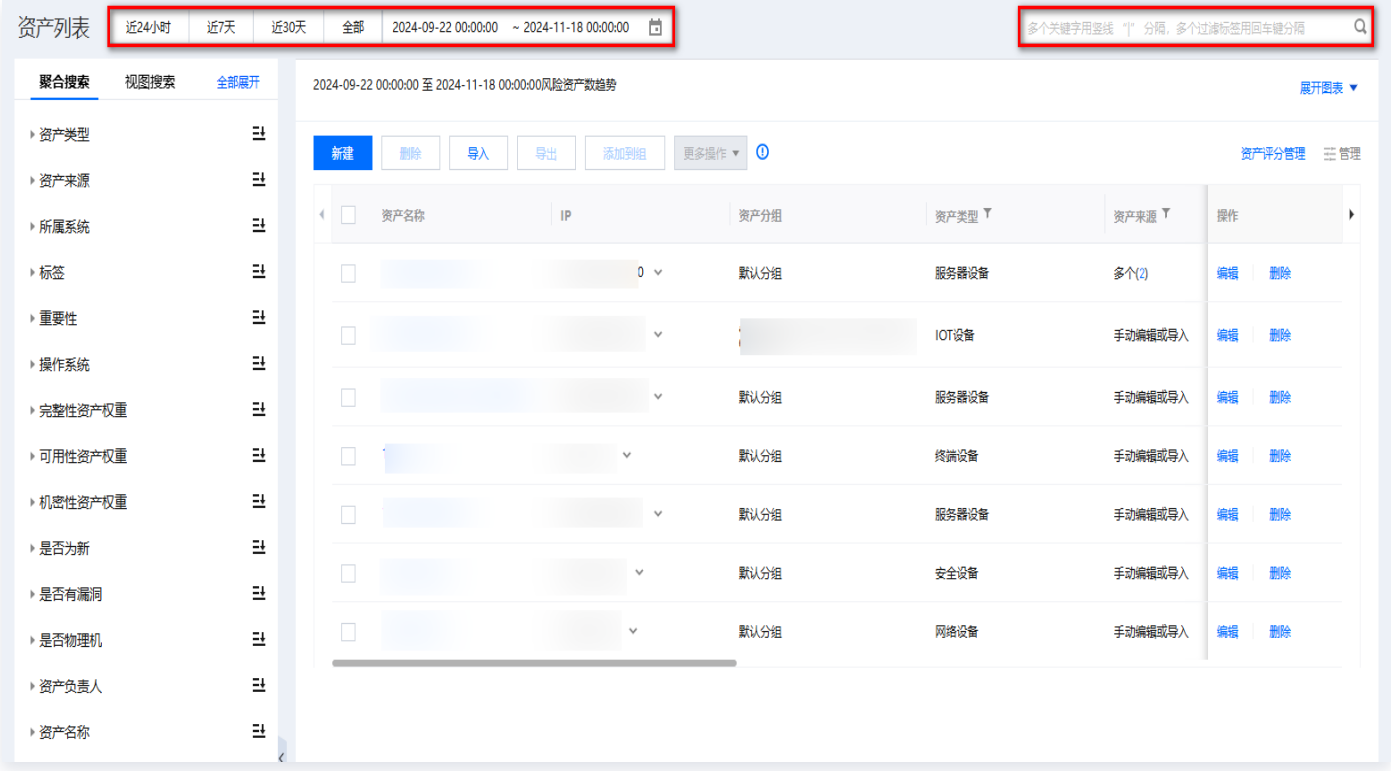
在**响应中心** > **联动响应**页面，联动阻断策略用于对已确定的威胁访问进行阻断。目前，本系统支持联动腾讯 NIPS 网络入侵防御系统进行阻断响应操作。

资产管理

最近更新时间：2024-12-17 18:09:02

在资产中心 > 资产列表页面，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。

- **支持通过时间范围、IP、资产名称、组件名称、组件版本筛选所需资产。**



- **单击新建，输入资产名称、资产类型、资产分组、网络参数、重要性等参数，单击确定即可创建资产。**

- 选择目标资资产，单击操作列的**编辑**，即可修改相关参数；单击更多操作，支持**编辑标签**、编辑其他字段。

- 选择目标资资产，支持对资产进行删除、导入、导出、添加到组操作。

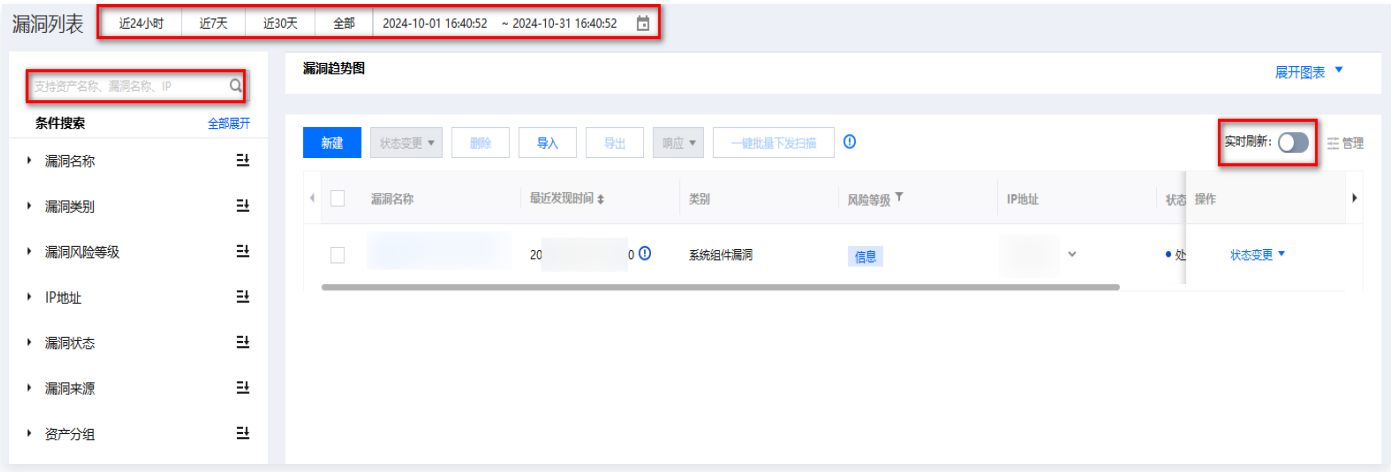
漏洞管理

最近更新时间：2024-12-17 18:09:02

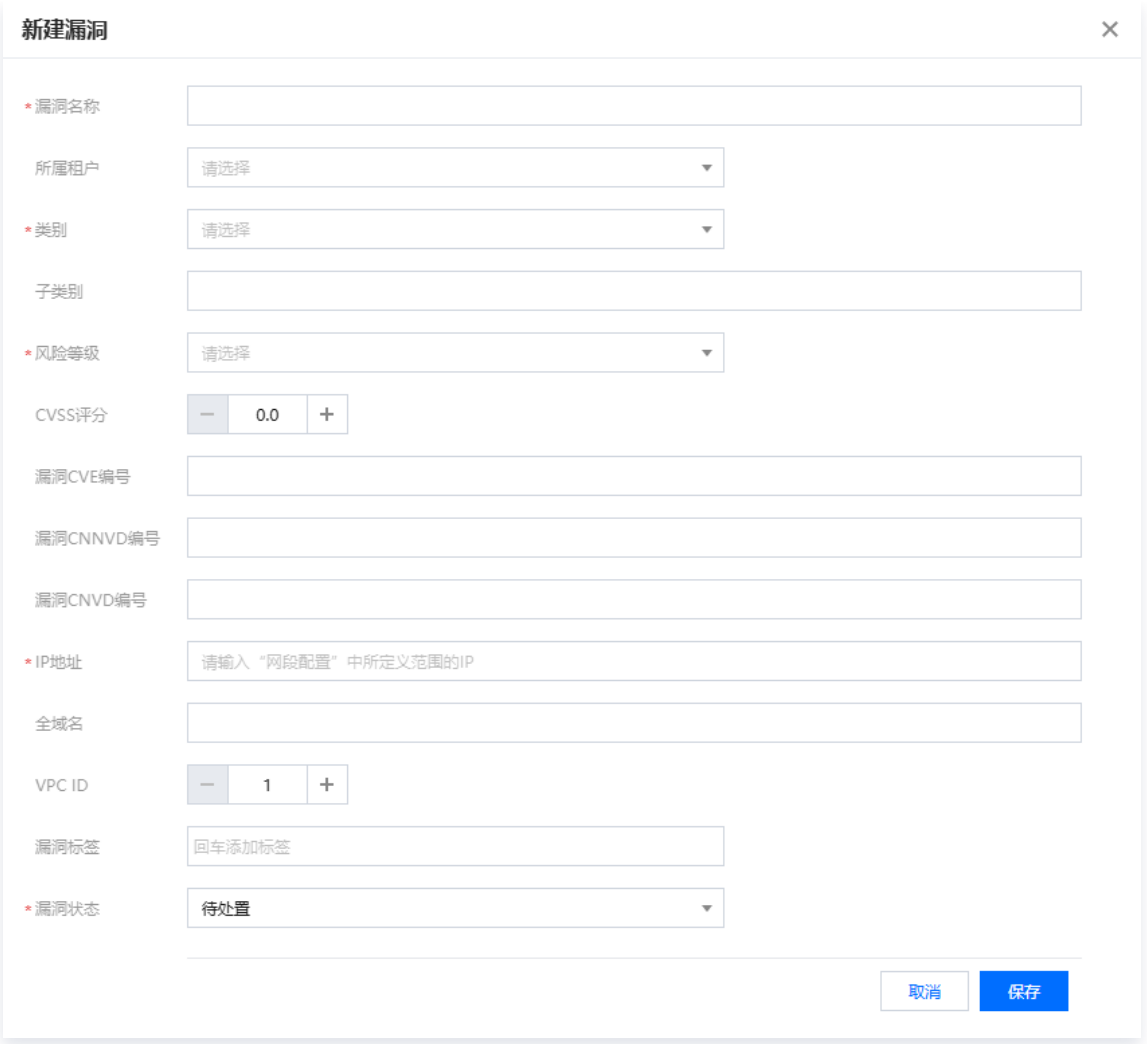
漏洞列表

在**漏洞管理** > **漏洞列表**页面，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。

- 支持通过时间范围、资产名称、漏洞名称、IP 筛选所需漏洞，单击**实时刷新开关**，支持开启实时刷新漏洞信息功能。



- 单击**新建**，输入漏洞名称、类别、风险等级、网络参数、重要性等参数，单击**保存**即可创建漏洞。



- **选择所需漏洞，单击状态变更，可以选择将状态调整为待处置、处置中、已处置、忽略。**

> **说明：**
>
> - **待处置：新发现的漏洞，还未进行处置。**
> - **处置中：漏洞正在处置中。**
> - **已处置：已完成对漏洞的处置。**
> - **忽略：漏洞可以不用处置。**

漏洞任务

在**漏洞管理** > **漏洞任务**页面，支持创建单次扫描任务和周期扫描任务。

1. 在**漏洞任务**页面，选择所需任务类型，单击**新建**。

2. 在新建任务窗口中，配置相关参数，单击**确定**。

参数名称	说明

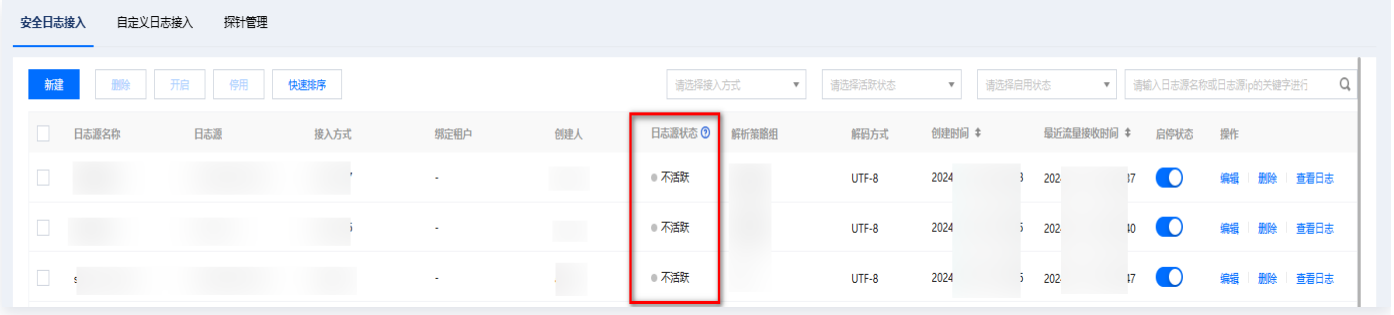
任务名称	不能超过64字符。
扫描器	暂无数据时，请在**系统管理 > 安全性及其他设置 >功能模块对接 > 漏洞扫描器对接配置**中配置。
扫描 IP 范围	支持输入多个 IP 及网段，使用换行分隔，网段格式使用192.168.240.0/20。
扫描资产组范围	仅可对不属于租户的资产组下发扫描任务。
扫描周期	仅支持周期扫描任务配置。
任务启停	仅支持周期扫描任务配置。

系统管理

最近更新时间：2024-12-17 18:09:02

数据接入

1. 在**系统管理 > 数据接入 > 日志接入**页面，选择**安全日志接入**。
2. 在安全日志接入页签，初始状态下，安全事件接入页面为空，可以进行安全事件日志源的新建、编辑、删除、控制开启/关闭和查看日志的操作。对于最近15分钟无数据上报的日志源，状态变为“不活跃”。



系统运维

在**系统管理 > 系统运维**页面，提供系统监控、版本管理、审计日志和消息中心的管理功能。

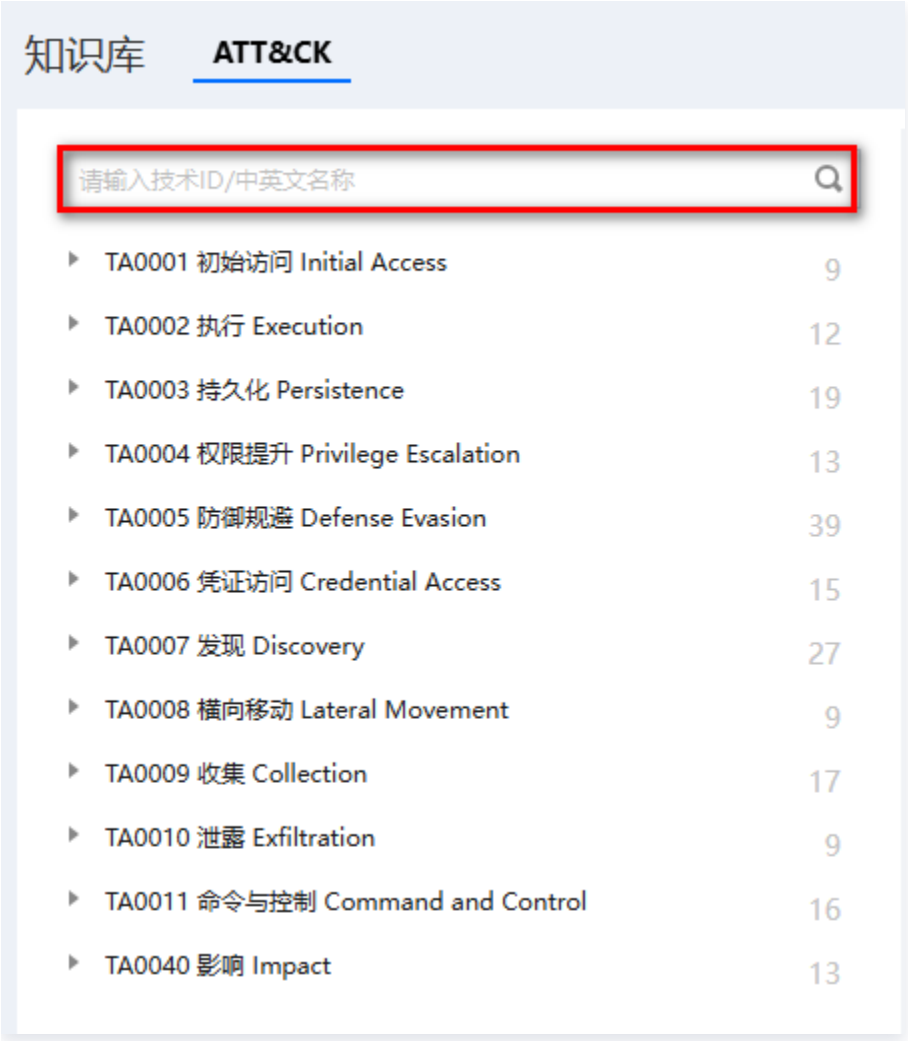
账号管理

本系统内置三个用户角色：超级管理员、普通管理员和审计员。只有超级管理员才能进行用户及权限管理。

知识库

ATT&CK 全称 Adversarial Tactics, Techniques, and Common Knowledge，框架由 MITRE 公司在2013年首次提出，是用于描述攻击行为的知识库和模型，一个基于现实世界所观察到的真实攻击向量的集合，其包含了已公开报告的众多威胁组织及其使用的工具和攻击技术，可以作为红蓝对抗、安全运营人员提供良好的参考和学习指导。

在**系统管理 > 知识库 > ATT&CK** 页面，增加 ATT&CK 知识手册，提供战技术信息、适用平台、详细描述等信息。同时，支持通过战技术名称、技术 ID 进行搜索。



安全性及其他设置

在系统管理 > 安全性及其他设置页面，包括登录安全、密码安全、自定义标题、自定义 Logo、与其他功能模块对接配置和第三方平台数据对接配置。