安恒信息
DAS-security 安全中国

数据安全管控平台

用户手册

前言

概述

感谢您选择安恒信息的网络安全产品。本手册详细描述了数据安全管控平台（以下简称“系统”）的配置方法，包括快速入门、Web 配置页面，首页、态势感知、资产档案、安全告警、合规中心、安全运营、用户中心以及系统管理。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于期望了解数据安全管控平台的读者，包括系统管理员、网络管理员、技术爱 好者等。本文假设读者对以下领域的知识有一定了解：

- 数据安全相关基础知识，包括数据采集、数据存储、数据变换、数据传输等。
- 网络安全相关知识，包括 DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段。

格式约定

本手册内容格式约定如下。

内容	说明
粗体字	Web 界面上的各类控件名称以及内容。例如：“在菜单栏选择‘**系统状态**’进入**系统状态**页面，选择**接口状态**页签”。
< >	Web 界面上的按钮。例如：“微信认证失败，点击<**我要上网**>不弹出微信认证界面”。
➢	介绍 Web 界面的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等）。例如：“在菜单栏选择‘**策略配置➢认证管理➢认证策略**’查看是否开启了认证策略”。
斜体字	可变参数，必须使用实际值进行替代。例如：“在浏览器地址栏输入‘http://*管理 IP*’，回车后进入系统 Web 管理平台登录页面”。

本手册图标格式约定如下。

图标	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或者数据丢失。
	警告，该图标后的内容需引起格外重视，否则可能导致人身伤害。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn 获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310052

电话：0571-88380999

传真：0571-28863666

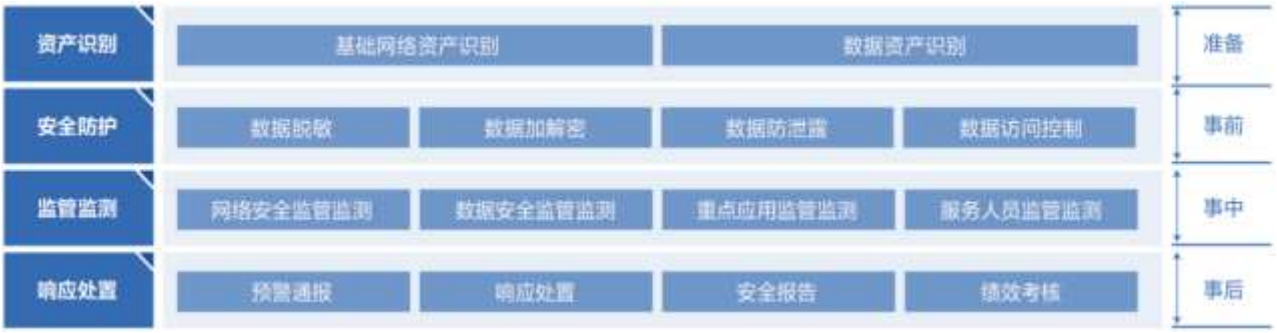
官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

1. 快速入门

1.1 产品概述

数据安全管控平台作为新形势下数据安全的一站式解决方案平台，提供了数据流动视角下的安全管控能力。利用复杂系统建模方法和大数据智能分析能力，建立适应数据动态流动的安全管控机制。从网络、数据、业务以及人员四个视角对数据流动场景下的关键节点进行合规监控和防护，对发现的网络攻击和数据安全风 险进行及时预警和通报。以管控平台为基础工具，可以建立“**资产识别>安全防护>监管监测>响应处置**”的数据安全运营体系。



模块介绍如下表所示。

功能	描述
资产识别	通过半自动化的方式识别梳理网络中的基础设施资产及数据资产，并按组织和系统进行分类归集，进行统一管理。
安全防护	采用相应的安全防护技术措施，包括数据脱敏、数据加密、数据防泄漏、数据访问控制等，确保数据流转过程的安全（依托于安恒信息 AiGuard 数据安全产品系列）。
监管监测	采集相关的安全数据，并进行数据处理和智能分析，从网络、业务、数据和人员四个维度识别安全风险。
响应处置	对发现的安全风险进行及时告警和预警，并对高危风险进行工单下发，便于及时响应和处理。

1.2 产品功能

平台主要功能请参见下表。

功能		描述
资产管理	基础资产管理	采用自动发现、手工录入、批量导入等方式，对全网基础网络资产信息（包括主机、安全设备资产等）进行统一梳理和统计。通过对资产

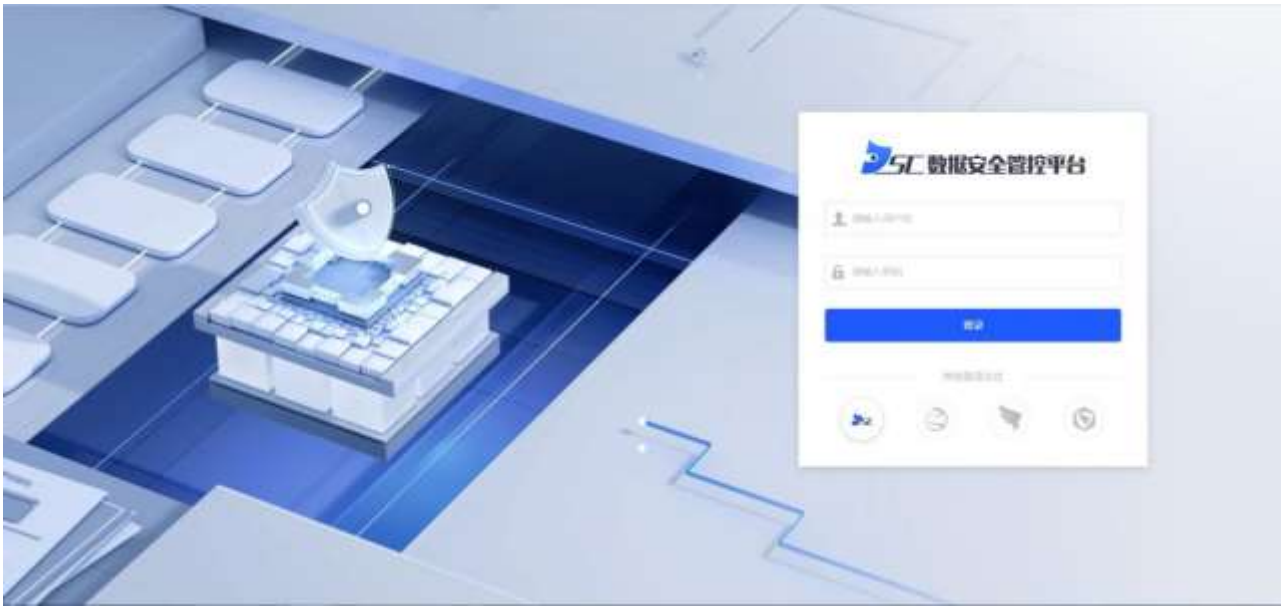
功能		描述
		从单位、系统等多方位的类型划分，以图表形式帮助客户整体掌握当前组织结构下，资产总量、各单位的系统数量、系统所使用的资产数量等信息。从不同维度对基础资产进行分析，帮助使用者直观、快速的掌握资产整体情况。
	数据资源管理	数据安全治理，始于数据资产梳理。数据资源管理模块可通过自动化方式扫描用户的数据库表，建立全局的数据资源目录，并内置了敏感数据识别规则，可以有效识别敏感数据在系统内的分布情况。同时数据资产管理模块支持对数据库、表、字段的备注定义和分类打标，可根据数据价值和特征，梳理出核心数据资产，对其进行分级分类，从而落实对数据更为精细的安全管理措施。
	系统资产管理	资产管理的系统资产，主要提供了网络资产、数据服务、应用服务所属资产的管理，并可上报其等保情况、防护情况、并统计与该系统相关的工单运维情况，包括了三高一弱的统计和工单处置率。
	应用接口管理	采用自动发现、手工录入、批量导入等方式，对用户的应用服务、接口进行统一梳理。对应用服务（如 API 接口服务、应用服务等）的流量和日志进行监测，对接口访问进行统计，结合业务规则对高频的访问行为进行及时的告警。对接口的健康状况进行实时监测，包括高延时、返回报错、404 异常访问进行监测和记录，及时告警。
	账号人员管理	对数据库、应用、主机账号进行集中管理，并对账号权限进行梳理，并且建立了人员账号（关联到自然人）—业务系统（业务系统账号）—数据服务—数据资产的访问关系。明确人员尤其是开发测试人员的数据操作权限范围，通过数据库审计、堡垒机日志、VPN 日志等进行关联分析，对其数据访问操作行为进行监督审核，确保相关人员的操作及行为在权限范围内，操作合理合规，同时可对越权行为及高危操作进行告警和记录。针对一些特权账户的使用，监管团队会定期进行审计，判断特权账户使用的必要性和合理性。
态势感知		态势感知可视化大屏通过地图、热力图、柱形图、折线图、饼图、仪表盘等方式有效的展示出复杂数据中蕴含的最有价值的信息，实时展示全局不同维度的安全态势信息。 ◆ 数据安全监管平台：对数据安全全方面进行监管，包含了对数据流动的监管、安全告警分析，接口访问统计分析以及工单状态分析。 ◆ 敏感数据监管大屏：通过对敏感数据库、敏感数据表、敏感字段、敏感数据分布、敏感数据访问、敏感数据告警等对敏感数据进行监管。

功能	描述
	◆ 数据安全驾驶舱：根据数据资产、风险资产、敏感数据访问、周安全事件趋势、重点应用调用、API 访问趋势、安全事件统计等指标形成完整的数据安全驾驶舱。
场景监管	**业务数据建模：**面向多部门协同的业务场景或复杂的数据流转场景，根据数据的流向，利用数据流节点，采用简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑配置和统一管理。同时，基于业务需求对其节点及节点之间的数据流转设置监控策略。基于业务的数据流转拓扑作为数据、业务和人员安全监控的参考基线，包括节点对象的访问量、访问流量、访问速率、请求延时、异常访问和敏感数据访问的监控，同时支持对特定数据的全网数据流转拓扑自动梳理。
告警事件统一查询	对探针发现的告警事件进行统一管理并提供各维度的查询功能。 ◆ **海量数据高速检索** ● 经过预处理后的安全数据以结构化的形式分布式存储在系统大数据库中，对外提供数据查询与统计服务，从而实现海量数据检索与挖掘。 ● 平台支持对安全告警的分类检索。支持数据搜索输入框，可输入关键字包括不限于设备 IP、日志发生时间、原始信息等进行检索；支持输入时间段、表达式等条件进行检索；支持快速选项卡检索；可指定多个查询条件进行组合查询；搜索结果以列表方式实现清晰展示，可在前端页面直接导出检索结果。 ◆ **丰富的规则库支持**：支持各种告警规则：SQL 注入、漏洞攻击、暴力破解、数据泄露、违规操作、违规访问、违规访问、违规应用、数据外发、弱口令风险、明文传输风险、HTTP 配置风险、数据库配置风险、登录异常、暴力破解、行为异常、Web 攻击等。
漏洞事件统一管理	以资产和漏洞为视角，结合内部管理制度和流程，通过内置工单系统，实现资产弱点的全生命周期管理。通过弱点标准化引擎，资产对扫描器扫描发现漏洞、安全服务人工渗透漏洞、内部运维人员运维发现漏洞、互联网公布漏洞等不同的漏洞进行统一管理。扫描能力如下： ◆ **全方位安全评估**：提供对 Windows 系列操作系统、Linux 主流操作系统、Unix 主流操作系统、Apache 等 web 中间件服务器以及 Office 等常用软件进行漏洞、弱口令、安全配置扫描检查。 ◆ **Web 弱点检测**：提供对 Web 应用弱点检测，支持 OWASP TOP 10 等主流安全漏洞，如：SQL 注入、Cookie 注入、CSRF 跨站伪造请求、命令注入、命令执行、代码注入、遍历目录、弱口令、其他各类 CGI 漏洞等各种类型。 ◆ **数据库弱点检测**：提供支持如 Oracle、MySQL、SQLServer、DB2、

功能	描述
	informix、达梦、人大金仓数据库漏洞扫描。
安全合规检查	支持一体化、标准化和自动化的合规检查流程。建立安全知识库，管理维护安全相关的标准、指导性文件等。
安全运营机制	平台结合用户的工作机制定制安全运营流程，符合用户的实际工作需要，满足其通报预警及相应处置的流程。平台支持邮件、钉钉等多种方式及时将情况上报、通报、下达，进行预警及快速处置。
专家服务	平台提供智能在线服务和问题库服务，方便用户查找常见问题的答案和建议，提高用户体验。

1.3 系统登录

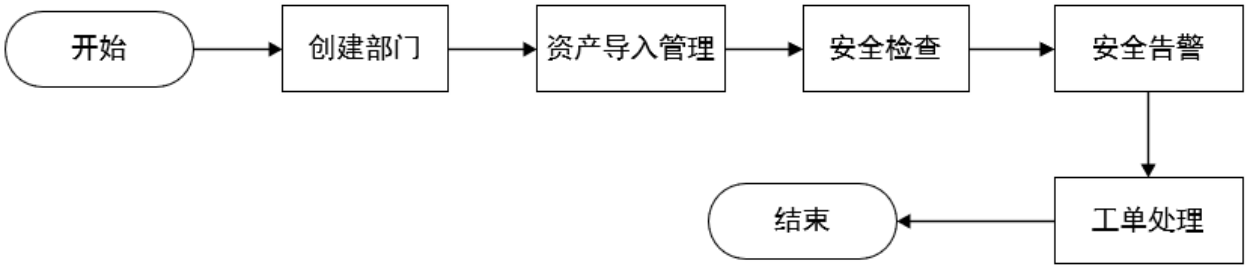
步骤1. 在 PC 的 Web 浏览器（建议使用 Chrome 浏览器）地址栏中输入“https://*数据安全管控平台 IP*”（出厂默认 IP 地址），并回车，进入系统 Web 管理平台登录页面。



步骤2. 输入用户名以及密码（默认用户名为 admin，密码为 1qaz@WSX），点击<**登录**>进入系统 Web 管理平台页面。

1.4 主要业务流程

系统的主要业务流程如下图所示。



步骤1. **创建部门：**在资产导入之前需要创建部门。详情请参见人员管理。

步骤2. **资产导入管理：**部门创建成功后，可以在系统内添加和导入资产。详情请参见资产档案。

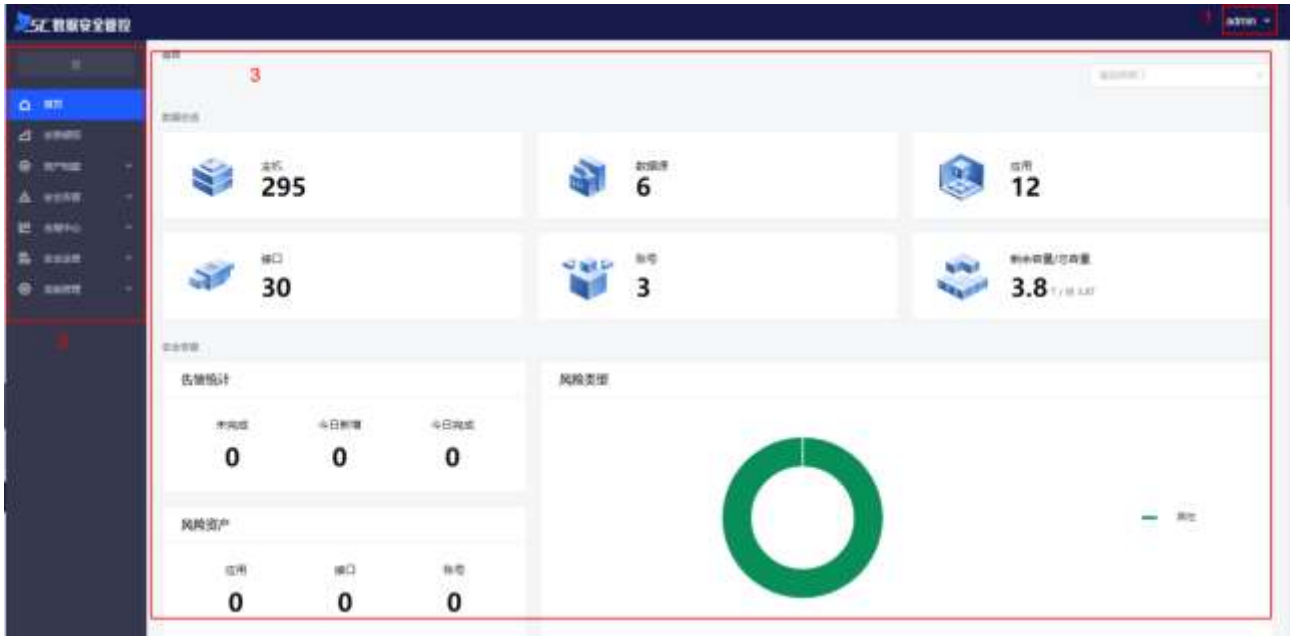
步骤3. **安全检查：**可以对资产进行安全合规检查和自查，并制定相应的检查标准。详情请参见合规中心。

步骤4. **安全告警：**检查完成后会形成相应的告警日志信息以及漏洞信息，系统进行统一管理和维护。详情请参见数据告警。

步骤5. **工单处理：**针对告警日志信息和漏洞信息可以发布工单进行处理，同时系统支持指派。详情请参见工单管理。

2. Web 配置页面

系统提供简便的 Web 配置页面，主要包含三个部分：1.个人中心；2.菜单栏；3.操作区。



2.1 修改个人基本信息

个人中心支持用户查看当前账号基本信息，并支持对个人基本信息进行修改。

将光标悬停于右上角用户名，在下拉框中选择“**个人中心**”，重新填写姓名、手机号码以及邮箱，点击<**保存**>完成个人信息的修改。

2.2 修改密码

可对当前账户登录密码进行修改。

步骤1. 将光标悬停于右上角用户名，在下拉框中选择“**个人中心**”，点击<**修改密码**>进行账号登录密码的修改。

步骤2.　输入当前密码、新密码并确认新密码，点击<**确定**>完成登录密码的修改。

2.3　关联 IP 地址

系统支持账号与 IP 地址进行关联。

将光标悬停于右上角用户名，在下拉框中选择“**个人中心**”，点击<**添加**>，填写 IP 地址后，点击<**保存**>即可完成 IP 地址和账户的关联操作。

2.4　退出 Web 配置页面

将光标悬停于右上角用户名，在下拉框中选择“**退出**”，退出当前用户登录状态。

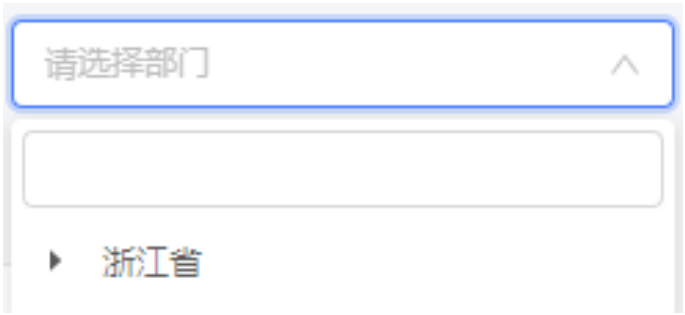
3.　首页

登录系统后默认进入首页界面，在菜单栏选择“**首页**”进入**首页**页面，可按部门进行数据总览、安全告警

统计分析、弱点漏洞统计分析、预警分析、工单分析、合规中心进度管理等信息，各模块详细说明如下。

3.1 部门选择

可按部门进行数据展示，部门管理详细信息请参考部门管理。



3.2 数据总览

- 主机：展示该部门下在系统监控中的主机数量，点击数字链接将跳转至网络资产。
- 数据源：展示该部门下在系统监控中的数据服务数量，点击数字链接将跳转至数据资源。
- 应用：展示该部门下在系统监控中的应用服务数量，点击数字链接将跳转至应用管理。
- 接口：展示该部门下在系统监控中的接口数量，点击数字链接将跳转至接口管理。
- 账号：展示该部门下在系统监控中的账号数量，点击数字链接将跳转至人员管理。
- 剩余容量/总容量：展示系统的剩余容量以及总容量。

3.3 数据告警

- 数据告警统计：显示所选部门未完成（状态为未处理、处理中）今日数据告警数量、本周告警数量、本月告警数量，点击数字链接将跳转至**错误!未找到引用源。**。
- 风险类型：显示所选部门告警类型分布情况。
- 风险趋势：显示所选部门告警等级的最近 7 天的发生趋势。

3.4 隐患告警

- 隐患告警统计：显示所选部门未处理（状态为新增）弱点数量、本月新增漏洞数、本月处理漏洞数，点击数字链接将跳转至**错误!未找到引用源。**。
- 风险类型：显示所选部门漏洞类型分布情况。
- 风险资产 TOP10：显示未处理（状态为新增）弱点数最多的 10 个主机资产。

3.5 预警分析

显示所选部门紧急、告警、一般级别的预警数量，按照级别搜索完成，同时可按日、月显示每日、每月新增的各级别预警单，点击数字链接将跳转至预警管理。

3.6 工单分析

- 显示所选部门未完成（未处理+处理中）、新增、完成（已解决+已关闭）状态的工单数量，点击跳转到安全运营-工单管理，并按状态搜索完成，点击数字链接将跳转至工单管理。
- 显示最近 10 天的未完成（未处理+处理中）、今日新增、今日解决（已解决）的工单数。

3.7 合规中心

- 展示结束时间最新的 3 次合规检查情况。
- 展示合规检查名称、时间、状态、未完成部门数、已完成部门数，及得分最高的 10 个部门的得分排名，点击数字链接将跳转至检查。

4. 态势感知

态势感知可视化大屏通过地图、热力图、柱形图、折线图、饼图以及仪表盘等方式有效的展示出复杂数据中蕴含的最有价值的信息，实时展示全局不同维度的安全态势信息。

在菜单栏选择“**态势感知**”进入**态势感知**页面，可以查看态势感知可视化大屏，可视化大屏的制作、发布和下架请参考业务。

4.1 数据安全驾驶舱

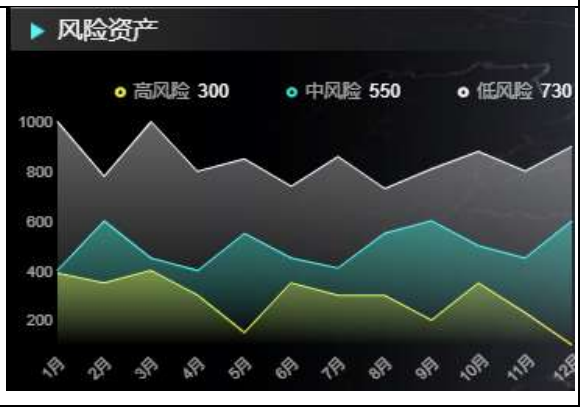
安全驾驶舱大屏主要对整个平台的资产、风险进行监控。主要由数据资源、风险资产、敏感数据访问、周安全事件趋势、今日新增、重点应用调用、API 访问趋势、安全事件统计、共享交换业务流几部分组成。

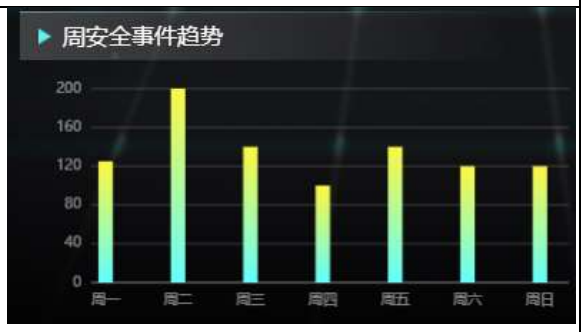
点击数据安全驾驶舱，可在另一个页面全屏查看大屏，数字安全驾驶舱大屏分为共享交换版以及地图版两种。

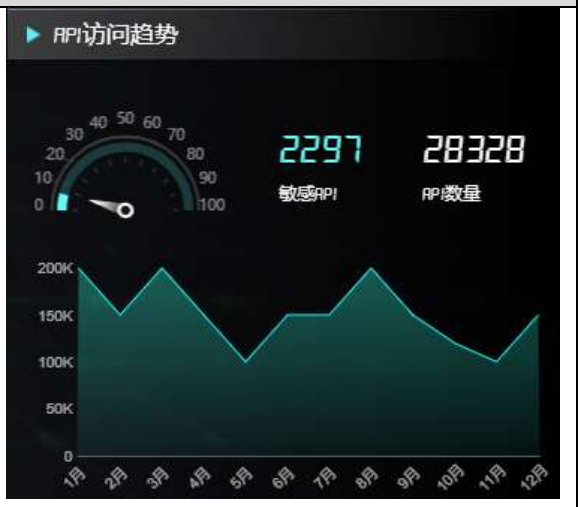
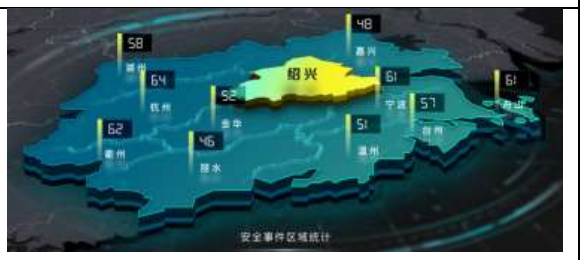
◆ 数字安全驾驶舱（共享交换版）

◆ 数字安全驾驶舱（地图版）

各模块详细说明如下。

展示项	说明	其他
数据资产	◆ 部门数：显示本系统内部门总数。 ◆ 应用数：显示本系统内应用总数。 ◆ 数据库：显示数据库的数量、敏感库的数量以及敏感库占比。 ◆ 数据表：显示数据表的数量、敏感表的数量以及敏感表占比。 ◆ 数据字段：显示数据字段的数量、敏感字段的数量以及敏感字段占比。	
风险资产	◆ 显示高、中、低风险数据资产的变化趋势。	

展示项	说明	其他
敏感数据访问	◆ 显示访问敏感数据次数最多的 4 个接口名称。 ◆ 显示接口名称和敏感数据访问次数。	
批量交换数量	◆ 交换机上数据库审计日志数量。 ◆ 显示系统批量交换总次数。	
数据共享次数	◆ 数据共享应用总访问次数。 ◆ 显示系统数据共享总次数。	
周安全事件趋势	◆ 显示未完成工单数量最近 7 天的变化趋势。 ◆ 横坐标显示最近 7 天的日期，纵坐标显示未完成（状态为未处理+处理中）的工单数量。	
今日新增	◆ 显示今日新增的工单数。	
重点应用调用	◆ 显示调用敏感数据次数最多的 4 个应用名称。 ◆ 显示应用名称和敏感数据访问次数。	

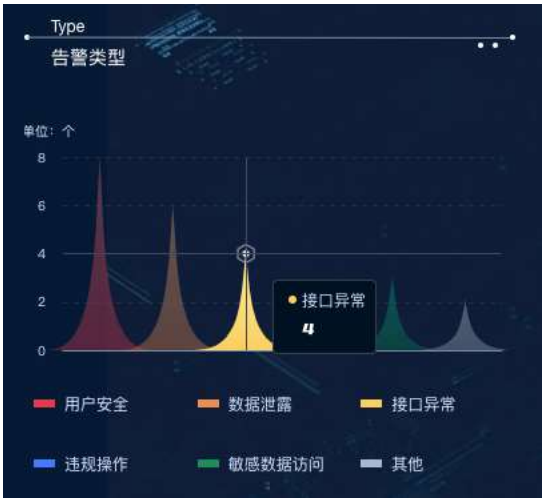
展示项	说明	其他
API 访问趋势	◆ 显示 API 和敏感 API 数量（存在访问敏感数据行为）、同时显示敏感 API 占比情况。 ◆ 横坐标表示时间，纵坐标表示敏感 API 月访问总次数。	
安全事件统计	◆ 显示工单总数、未完成（状态为未处理+处理中）工单数。 ◆ 按工单标签进行统计，显示次数最多的 4 个标签名称，同时展示标签名称和工单次数。	
地图版	◆ 显示所在地地图。 ◆ 地图上显示各地未完成工单数量。	
共享交换版	◆ 显示用户的共享交换业务流程。	

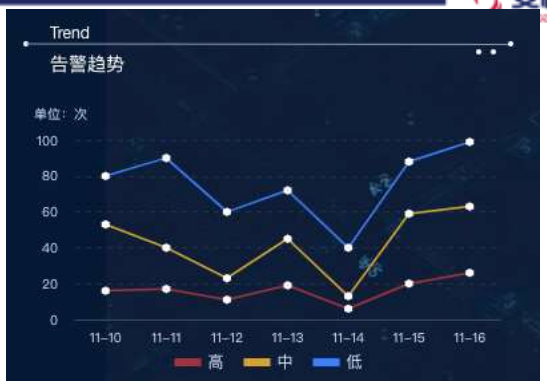
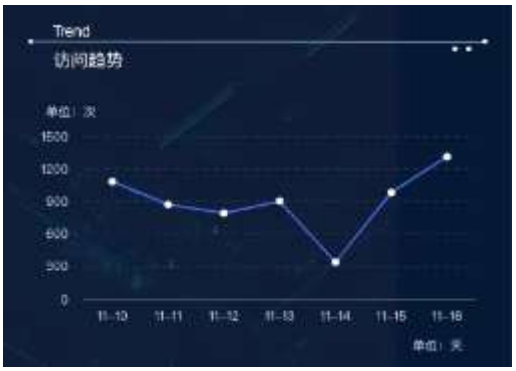
4.2 数据安全监控

数据安全监控大屏主要是对数据安全全方面进行监管，包含了对数据资产的统计、数据流动的监管、安全

告警分析，接口访问统计分析以及工单状态分析。

展示项	说明	其他
资产统计	◆ 部门数：显示本系统内部门总数。点击数字下钻到资产管理/部门管理页面 ◆ 主机数：显示本系统内主机总数资产管理/网络资产/网络资产页面。 ◆ 应用数：显示本系统内应用总数资产管理/应用管理/应用管理页面。 ◆ 接口数：显示本系统内接口总数资产管理/应用管理/接口管理页面。 ◆ 数据库：显示本系统内的数据库总数资产管理/数据资源/数据库页面。 ◆ 账号数：显示该系统内的账号总数资产管理/人员管理/账号管理页面。	

数据流动监管	◆ 数据来源：显示库表交换条数和接口访问次数 TOP6 的数据来源的部门。 ◆ 数据赋能：显示库表交换条数和接口访问次数 TOP6 的数据赋能的部门。	
告警数量	◆ 显示数据告警的今日告警数量、本周告警数量、本月告警数量 ◆ 点击今日告警跳转到数据告警/数据原始告警页面筛选条件为本日的告警列表。 ◆ 点击本周告警跳转到数据告警/数据原始告警页面筛选条件为本周的告警列表。 ◆ 点击本月告警跳转到数据告警/数据原始告警页面筛选条件为本月的告警列表。	、 
告警类型	◆ 显示本日数据告警的告警类型统计	

告警趋势	◆ 显示最近 7 天，数据告警，高、中、低的次数趋势图	
接口访问 数据访问	◆ 显示今日访问次数最多的 5 个接口和今日访问次数最多的 5 个数据库 ◆ 点击接口访问的接口名称和数字跳转到应用管理/接口管理/对应接口详情。 ◆ 点击数据访问的数据库名称和数字跳转到资产管理/数据资源/数据库/对应的数据库详情。	
接口访问趋势 数据库访问趋势	◆ 显示近 7 日接口访问趋势和近 7 日数据库访问趋势	
工单状态分析	◆ 显示工单总数、未处理、处理中、已完成和已关闭的工单数 ◆ 点击环形图跳转到安全运营的工作台。 ◆ 点击工单总数跳转到安全运营/工	

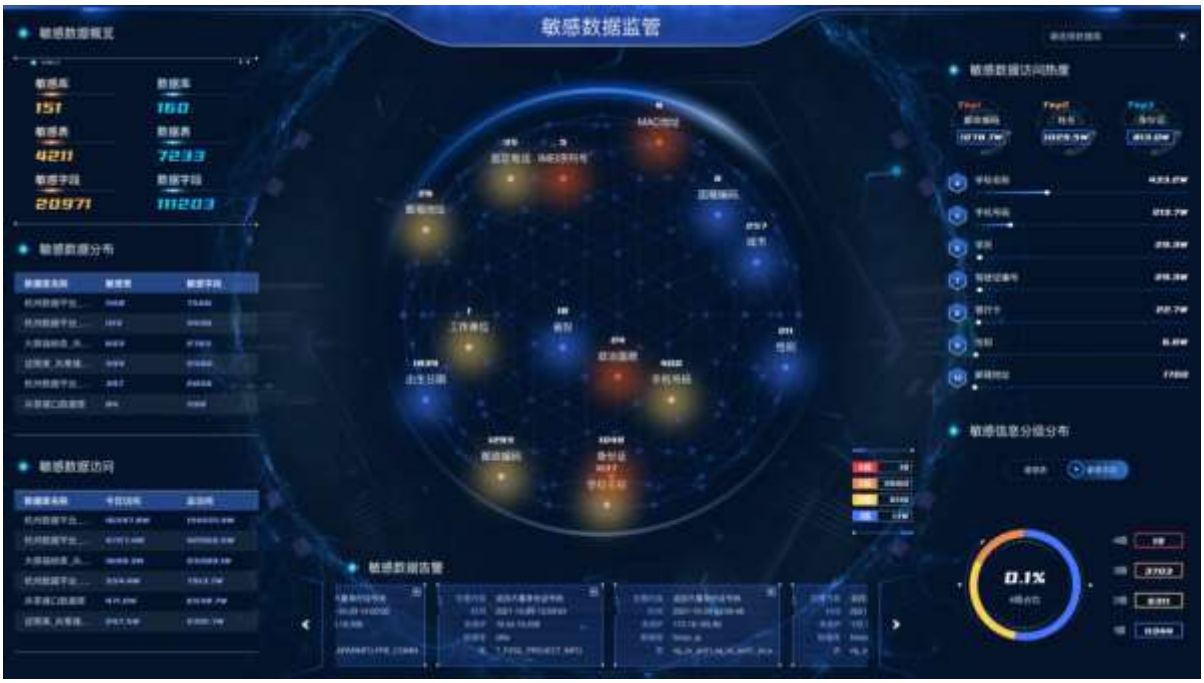
	单管理页面。	

4.3 敏感数据监管大屏

敏感数据监管大屏主要是通过对敏感数据库、敏感数据表、敏感字段、敏感数据分布、敏感数据访问、敏感数据告警等对敏感数据进行监管。

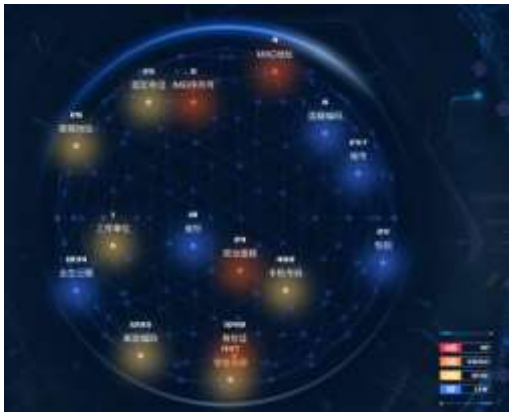
敏感数据监管大屏分成主屏和副屏，主屏对所有数据库下的敏感数据进行监管，通过选择框选择单个数据库，跳转到副屏，针对当前数据库的敏感数据情况。

4.3.1 主屏

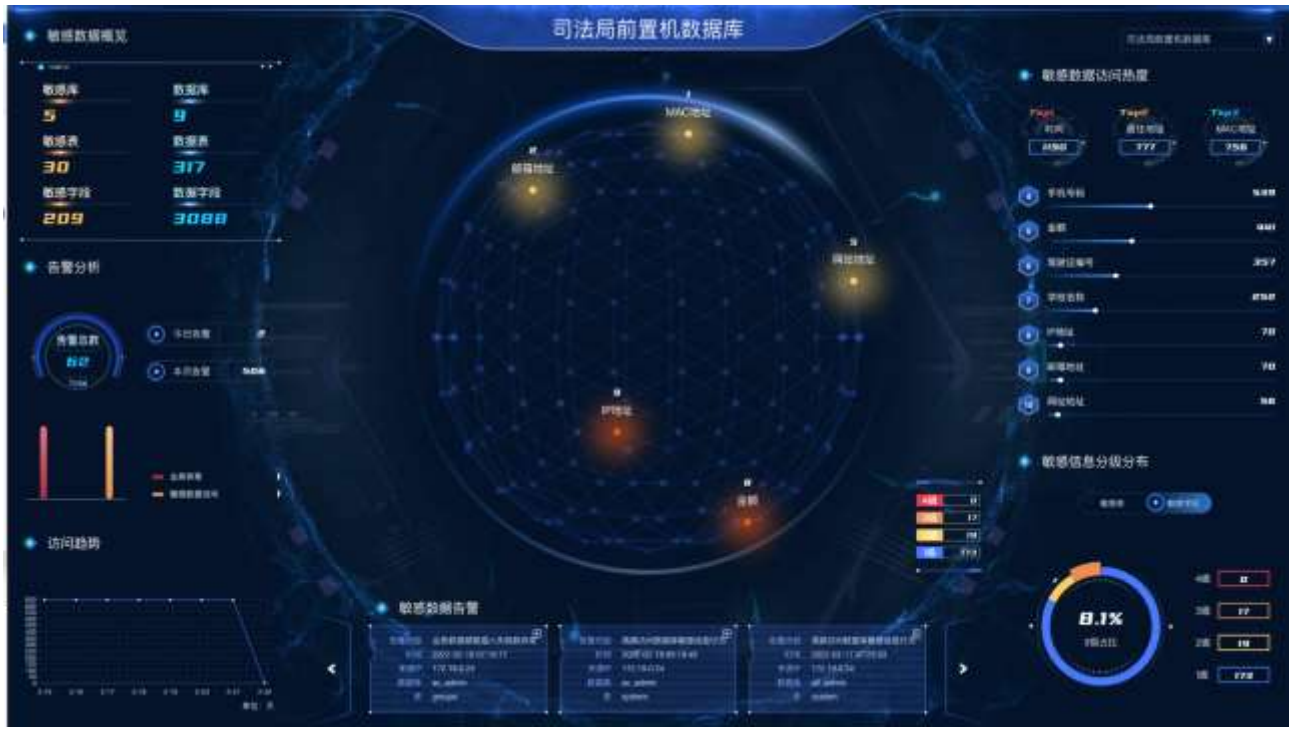


展示项	说明	其他
数据库选择	◆ 主屏默认所有数据库的数据。 ◆ 点击选择单个数据库跳转到副屏。	

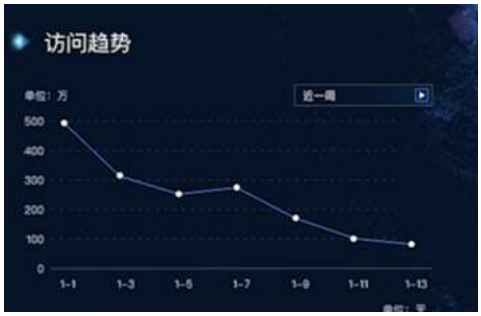
敏感数据概览	◆ 展示敏感库、敏感表、敏感字段的数量 ◆ 展示数据库、数据表、数据字段的数量	
敏感数据分布	◆ 展示数据库的敏感表、敏感字段数量	
敏感数据访问	◆ 展示数据库的访问信息，包括今日访问该数据库的次数和总访问次数。	
敏感数据告警	◆ 展示敏感数据的相关告警信息，包含告警名称、告警时间、来源IP、数据库、数据表 ◆ 点击单个告警下钻到对应的告警详情页面	

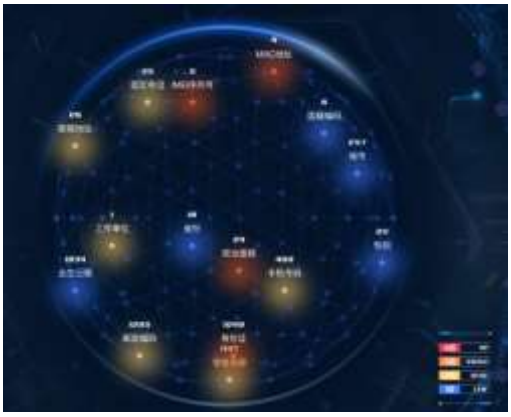
敏感数据访问热度	◆ 展示近 7 日数据资源的元数据管理的敏感字段的 TOP10 的访问情况。	
敏感信息分级分布	◆ 展示敏感表和敏感字段的分级分布以及占比情况 ◆ 以 tab 的形式点击切换敏感表和敏感字段	
中间动图	◆ 展示敏感标签和敏感标签的数据 ◆ 展示敏感标签根据分级情况的总数量 ◆ 点击敏感标签下钻到球体下钻页	

4.3.2 副屏

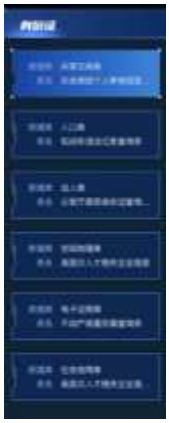


展示项	说明	其他
敏感数据概览	◆ 展示所选数据库下的敏感库、敏感表、敏感字段的数量 ◆ 展示所选数据库的数据库、数据表、数据字段的数量	

告警分析	◆ 展示所选数据库下今日告警数量、本月告警数据和告警总数 ◆ 柱状图的形式展示所选数据库下的根据告警类型的告警数量分布	
访问趋势	◆ 折线图的形式展示所选数据库下的近一周的访问趋势	
敏感数据告警	◆ 展示所选数据库下的敏感数据的相关告警信息，包含告警名称、告警时间、来源 IP、数据库、数据表 ◆ 点击单个告警下钻到对应的告警详情页面	

敏感数据访问热度	◆ 展示所选数据库下近 7 日数据资源的元数据管理的敏感字段的 TOP10 的访问情况。	
敏感信息分级分布	◆ 展示所选数据库下的敏感表和敏感字段的分级分布以及占比情况 ◆ 以 tab 的形式点击切换敏感表和敏感字段	
中间动图	◆ 展示所选数据库下的敏感标签和敏感标签的数据 ◆ 展示所选数据库下的敏感标签根据分级情况的总数量 ◆ 点击敏感标签下钻到球体下钻页	

4.3.3 球体下钻页

展示项	说明	其他
数据库名和表名	◆ 展示所选敏感标签的相关的所有数据库和数据表 ◆ 点击列表中的每一行展示访问趋势和最新告警数据	
访问趋势	◆ 展示所选敏感标签下所选数据库的数据表的近一周的访问趋势	

最新告警	◆ 展示所选敏感标签下所选数据库的数据表的告警信息 ◆ 点击具体的每一条下钻到具体的告警详情页 ◆ 点击更多，下钻到告警页面	

5. 资产档案

资产档案主要对全网资产进行统一梳理和统计，主要包括用户基础资产、数据资源资产、应用接口资产以及账号人员资产等。

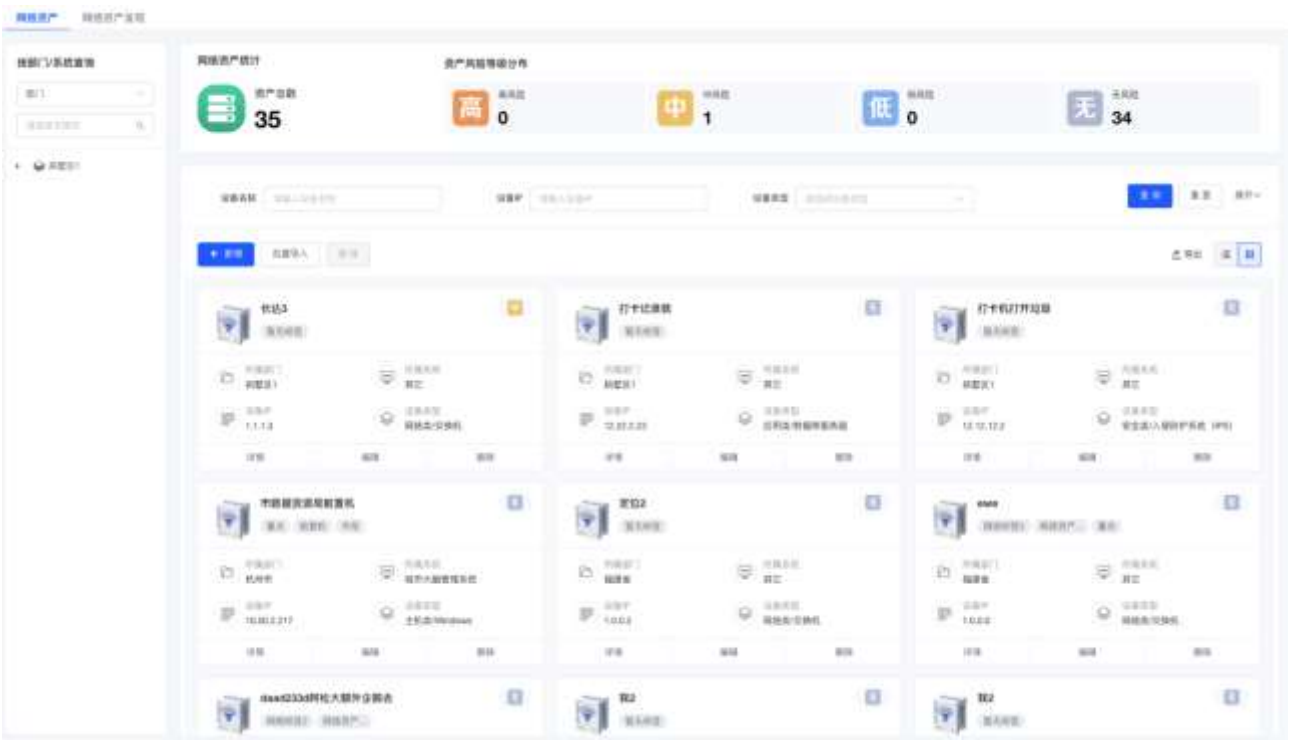
5.1 网络资产

采用自动发现、手工录入以及批量导入等方式，对全网基础网络资产信息（包括主机、安全设备资产等）进行统一梳理和统计。通过对资产从单位和系统等多方位的类型划分，以图表形式帮助用户整体掌握当前组织结构下，资产总量、各单位的系统数量以及系统所使用的资产数量等信息。从不同维度对基础资产进行分析，帮助使用者更加直观和快速的掌握资产整体情况。

5.1.1 查询资产

支持通过设备名称、设备 IP、设备类型、网络区域、云环境、标签以及部门/系统进行条件查询。

5.1.2 网络资产卡片

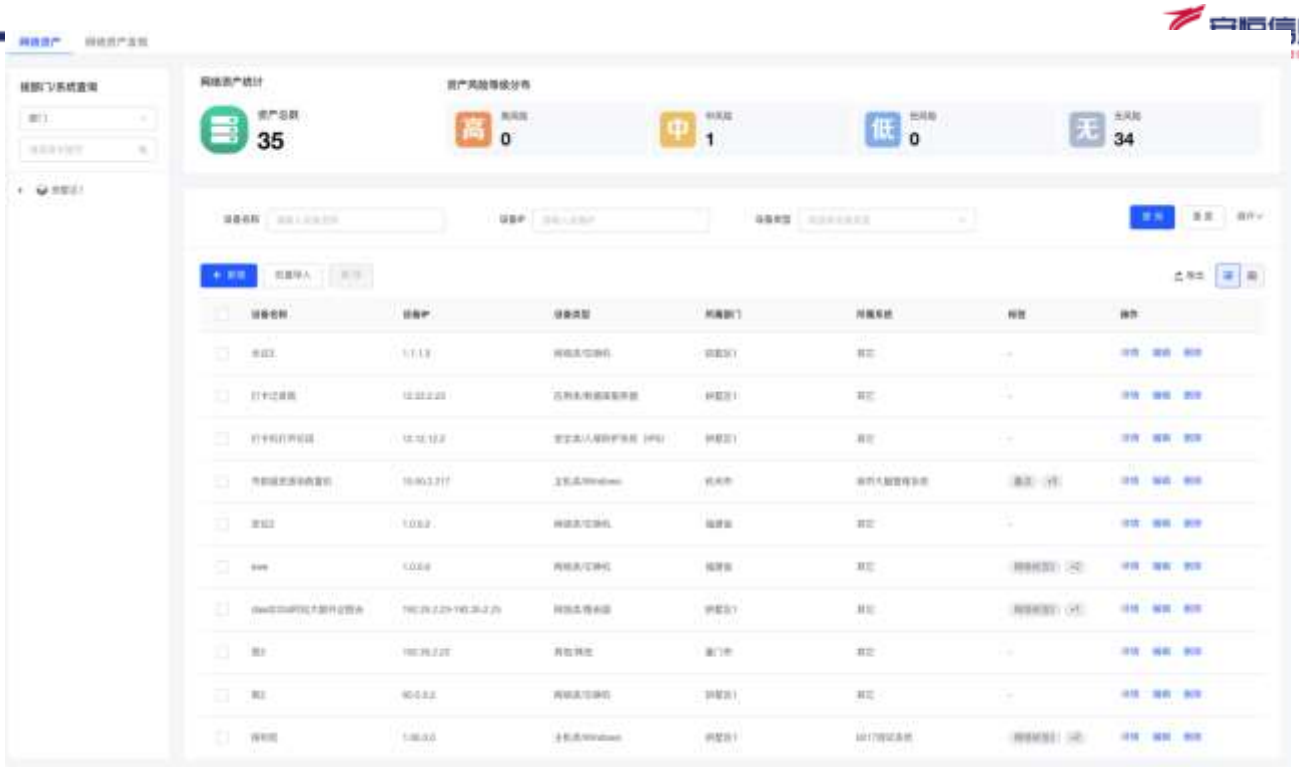


统计区域展示该账号权限下资产总数，以及存在高风险、中风险、低风险以及无风险的资产数量。

默认以卡片的形式展示网络资产的基本信息，包括：资产名称、资产标签、资产风险等级、所属部门、所属系统、设备 IP、设备类型。且可在卡片页面进行查看详情、编辑和删除操作。

5.1.3 网络资产列表

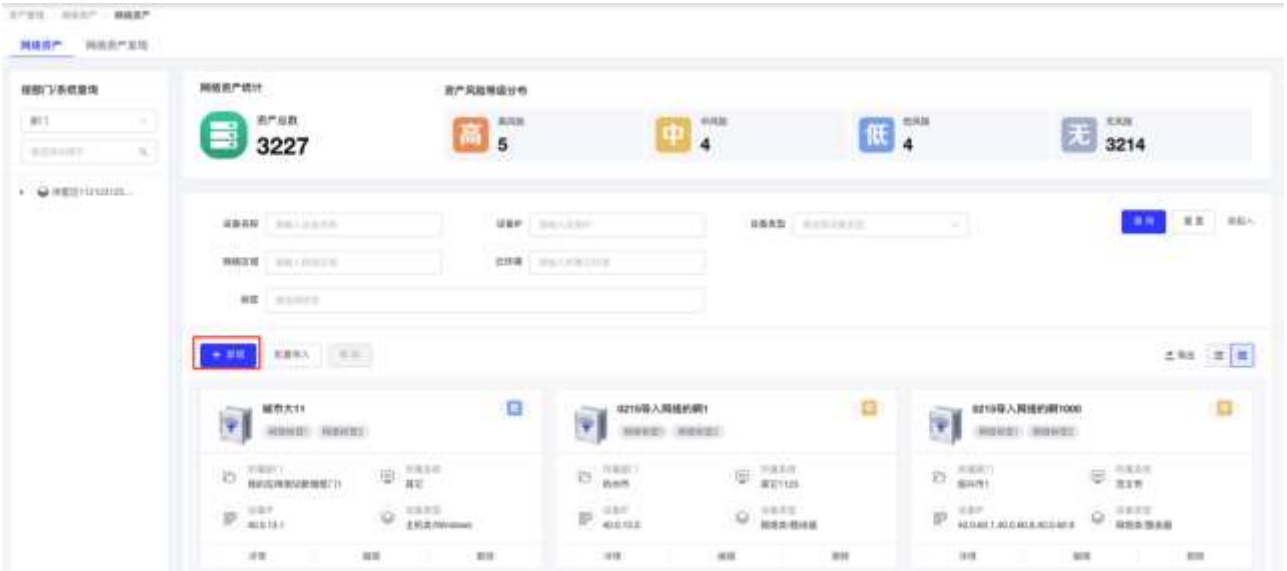
点击  切换到列表页面，在列表页面展示字段包含设备名称、设备 IP、设备类型、所属部门、所属系统、标签。且可在列表页面进行查看详情、编辑和删除操作。



5.1.4 新增网络资产

可以根据部门以及系统进行展示资产详细信息。新增资产操作步骤如下。

步骤1. 在菜单栏选择“**资产管理➤网络资产**”进入**网络资产**页面，选择**网络资产**页签，点击<**新增**>。



步骤2. 进入**添加设备**页面，填写设备基本信息以及设备基础属性，点击<**保存**>。


添加设备
* 设备名称
请输入设备名称
* 设备IP
请输入设备IP，示例：192.168.1.2或192.168.2.2-192.168.3.100
实例ID
请输入云资源的实例ID
* 设备类型
请选择设备类型
* 所属部门
请选择部门
所属系统
请选择所属系统
安全责任人
请输入安全责任人
请输入安全责任人手机号
系统开发商
请输入系统开发商
系统联系人
请输入系统联系人
请输入系统联系人手机号
网络区域
请输入网络区域
所属云环境
请输入所属云环境
操作系统及版本
请输入操作系统及版本号
设备厂商及型号
请输入设备厂商及型号
标签
请选择标签
设备基础属性
内存
请输入内存大小和单位
GB
硬盘
请输入硬盘大小和单位
TB
处理器
请输入设备处理器信息
核
取消
保存

详细配置请参见下表。

配置项	说明
设备基本信息	
设备名称	填写需要添加的设备名称。
设备 IP	填写需要添加的设备 IP 地址。
实例 ID	如果该资产为云资产，需要填写云资源的唯一编号 ID。
设备类型	选择需要添加的设备类型。
所属部门	选择需要添加的资产所属部门，部门管理相关信息请参考部门管理。
所属系统	请先选择所属部门，再选择需要添加的资产所属系统。
安全责任人	填写该项资产的责任归属人。
安全责任人手机号	填写该项资产的责任归属人的手机号。
系统开发商	该项资产设备所属系统的开发商。
系统联系人	该项资产设备所属系统的联系人。
系统联系人手机号	该项资产设备所属系统的联系人手机号。
网络区域	该项资产设备的网络区域。
所属云环境	该项资产设备的所属云环境。
操作系统及版本	该项资产设备的操作系统及版本。
设备厂商及型号	该项资产设备的厂商及型号。
标签	选择该项资产所识别的标签，点击<**新增标签**>，填写标签名称即可完成自定义标签。
设备基础属性	
内存	填写该项资产的内存大小和单位。
磁盘	填写该项资产的磁盘大小和单位。
处理器	填写该项资产的处理器信息。

5.1.5 导入资产

系统支持批量导入基础资产。

步骤1. 在**网络资产**页面，点击<**批量导入**>，继续点击<**模版下载**>模板将以 xlsx 格式导出至本地，根据模板格式进行填写。

步骤2.　继续点击<**点击上传**>将填写完成的模板拖拽或上传。

只支持 Excel 格式，上传内容会覆盖原有数据。

5.1.6　导出

支持根据查询筛选条件导出。导出字段如下：

5.1.7　查看资产详情

点击资产列表**操作**列的<**详情**>，可以查看设备基本信息、设备属性、设备状态、告警统计、弱点统计以及

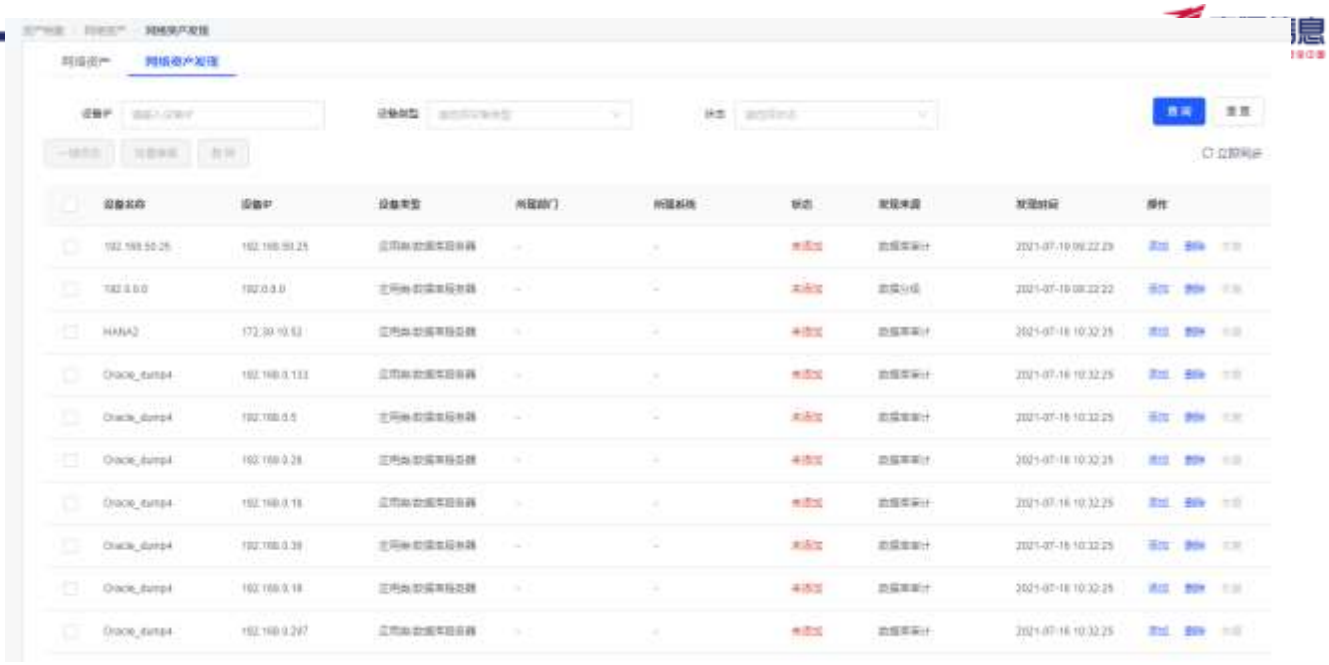
服务统计。

其中在告警统计和弱点统计区域，点击风险总数可跳转到数据告警/数据原始告警页面；点击弱点总数可跳转到数据告警/安全隐患事件页面。

5.1.8 网络资产发现

在菜单栏选择“**资产档案➤网络资产**”进入**网络资产**页面，选择**网络资产发现**页签，可以对系统自动发现的网络资产进行统一管理。

- 系统支持通过设备 IP、设备类型以及状态进行条件查询。
- 在右上角点击<**立即同步**>，可以立即同步平台探针上的资产数据。
- 在资产列表**操作**列点击<**添加**>，可以将该项资产添加至网络资产内进行管理。
- 在资产列表**操作**列点击<**删除**>，可以删除该项自动发现的资产。
- 在资产列表**操作**列点击<**恢复**>，可以将该项资产恢复至网络资产列表内。



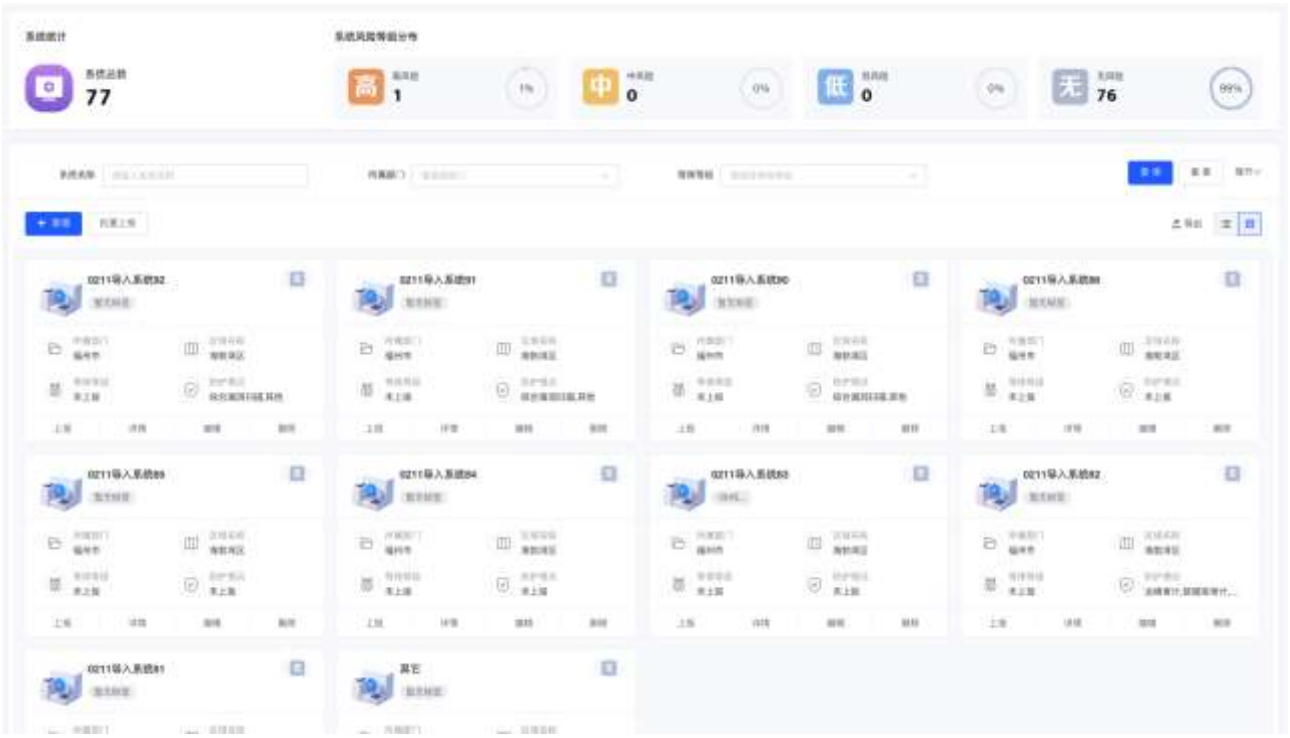
5.2 系统资产

资产管理的系统资产，主要提供了网络资产、数据服务、应用服务所属资产的管理，并可上报其等保情况、防护情况、统计其工单运维情况。

5.2.1 查询条件

可根据系统名称、所属部门、等保等级、防护情况、标签进行查询搜索。

5.2.2 系统资产卡片



统计区域展示当前账号权限内系统总数以及系统存在高风险、中风险、低风险、无风险的分布情况。

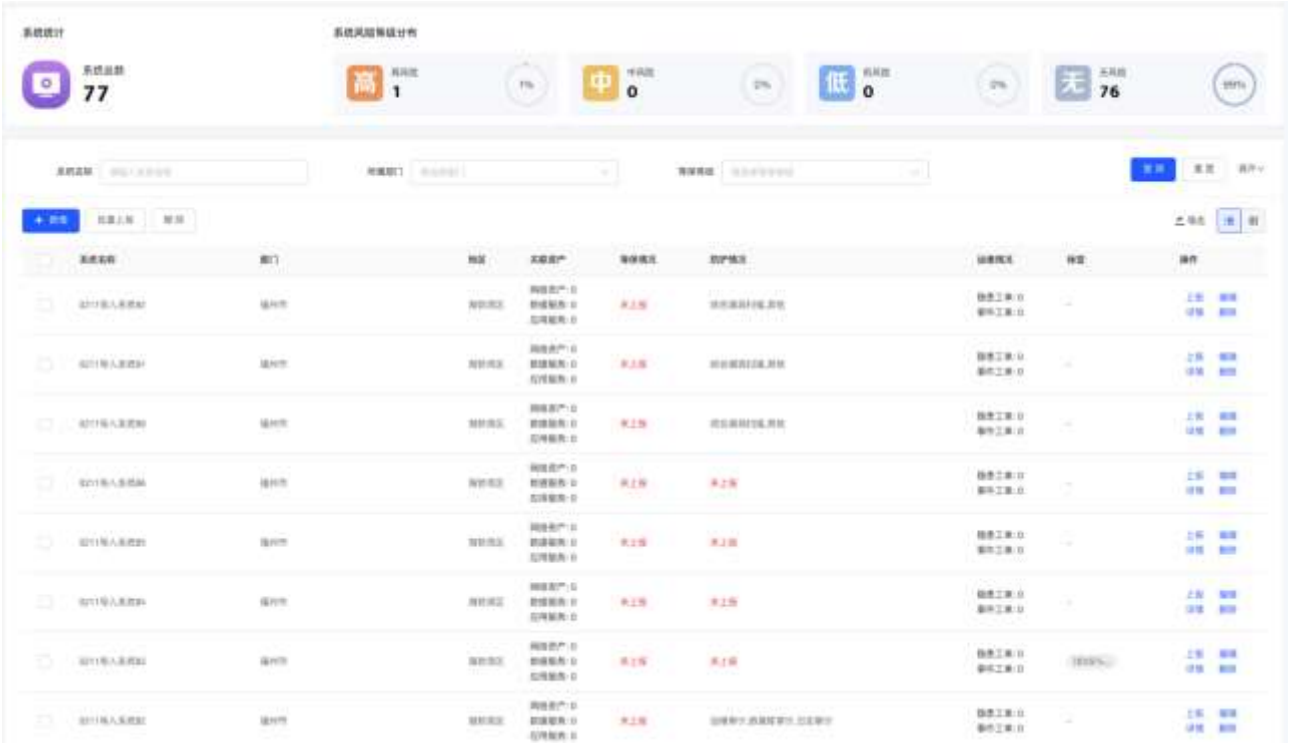
默认以卡片的形式展示系统资产的基本信息，包括：系统名称、系统标签、系统风险等级、所属部门、区域名称、等保等级、防护情况。且可在卡片页面进行上报、查看详情、编辑和删除操作。

鼠标悬浮在卡片中间区域展示与该系统的关联资产情况，包括网络资产、数据服务、应用服务的数量；以及安全运营的情况，包含了工单总数和处置率。

5.2.3 系统资产列表

点击  切换到列表页面，在列表页面展示字段包含系统名称、部门、地区、关联资产、等保情况、

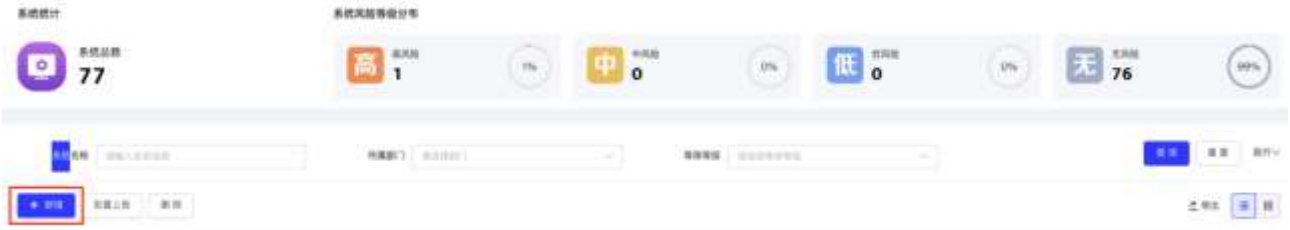
防护情况标签。且可在列表页面进行上报、查看详情、编辑和删除操作。



5.2.4 新增系统

新增系统操作步骤如下：

步骤 1. 在菜单栏选择“资产管理➤系统资产”进入系统资产页面，点击<**新增**>。



步骤 2. 进入新增系统页面，填写系统的名称和所属部门，点击<**保存**>。

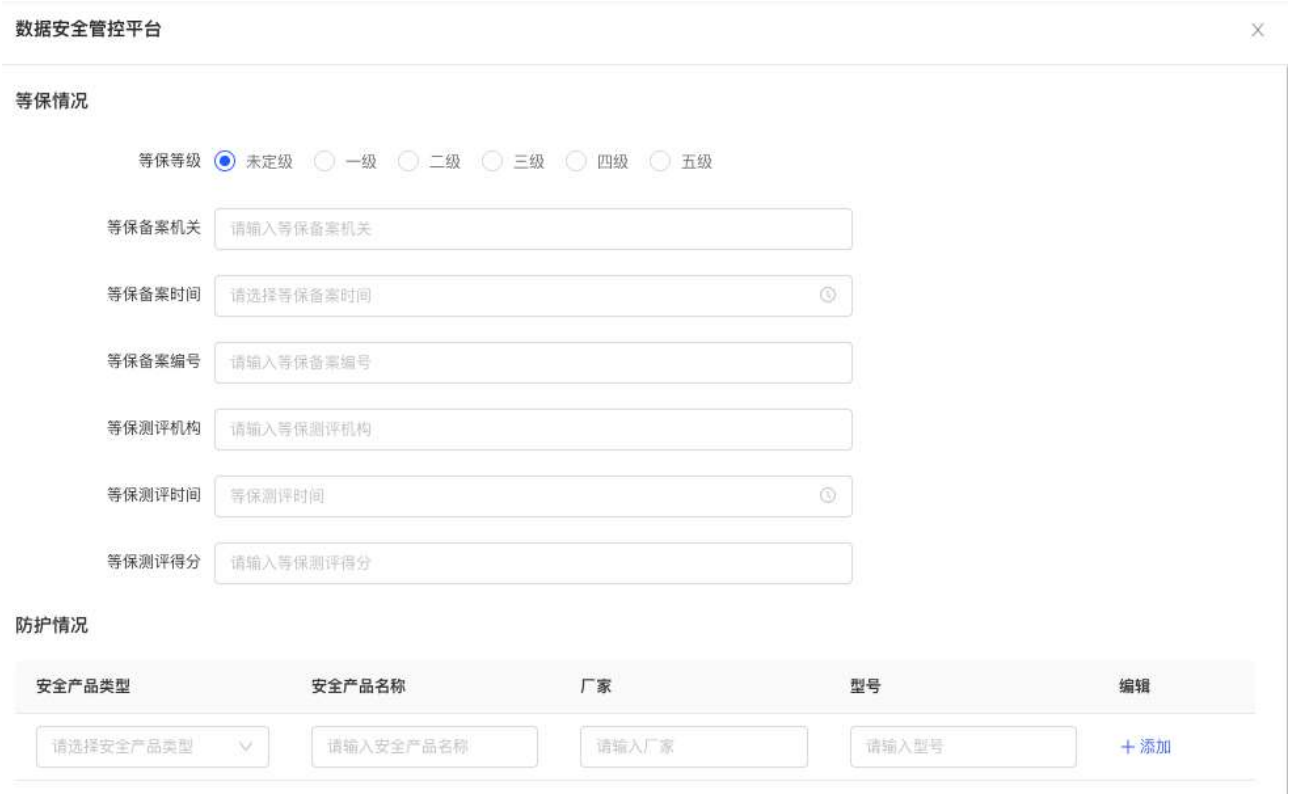
配置项	说明
设备基本信息	
系统名称	填写需要添加的系统名称。
所属部门	选择需要添加的资产所属部门，部门管理相关信息请参考部门管理。
标签	选择该项资产所识别的标签，点击<**新增标签**>，填写标签名称即可完成自定义标签。

5.2.5 等保上报

等保上报操作步骤如下：

步骤 1. 在菜单栏选择“资产档案”➤“系统资产”进入系统资产页面，点击<**上报**>。

步骤 2. 进入系统上报页面，填写系统的等保情况和防护情况，点击<**保存**>。



详细配置请参见下表。

配置项	说明
等保情况	
等保等级	勾选等保的等级
等保备案机关	填写等保备案的机关。
等保备案时间	填写等保备案的最新的时间。
等保备案编号	填写等保备案的编号。
等保测评机构	填写等保测评的机构。
等保测评时间	填写等保测评的最新时间。
等保测评得分	填写该项资产的责任归属人。
防护情况	
安全产品类型	选择防护的安全产品的类型。
安全产品名称	填写防护的安全产品的名称。
厂家	填写安全产品厂商的名称。
型号	填写安全产品的型号。
编辑	点击添加新增一条数据。

5.2.6 批量上报

系统支持批量导入系统。

步骤 1. 在**系统资产**页面，点击<**批量上报**>，继续点击<**模版下载**>模板将以 xlsx 格式导出至本地，根据模板格式进行填写。

步骤 2. 继续点击<**点击上传**>将填写完成的模板拖拽或上传。

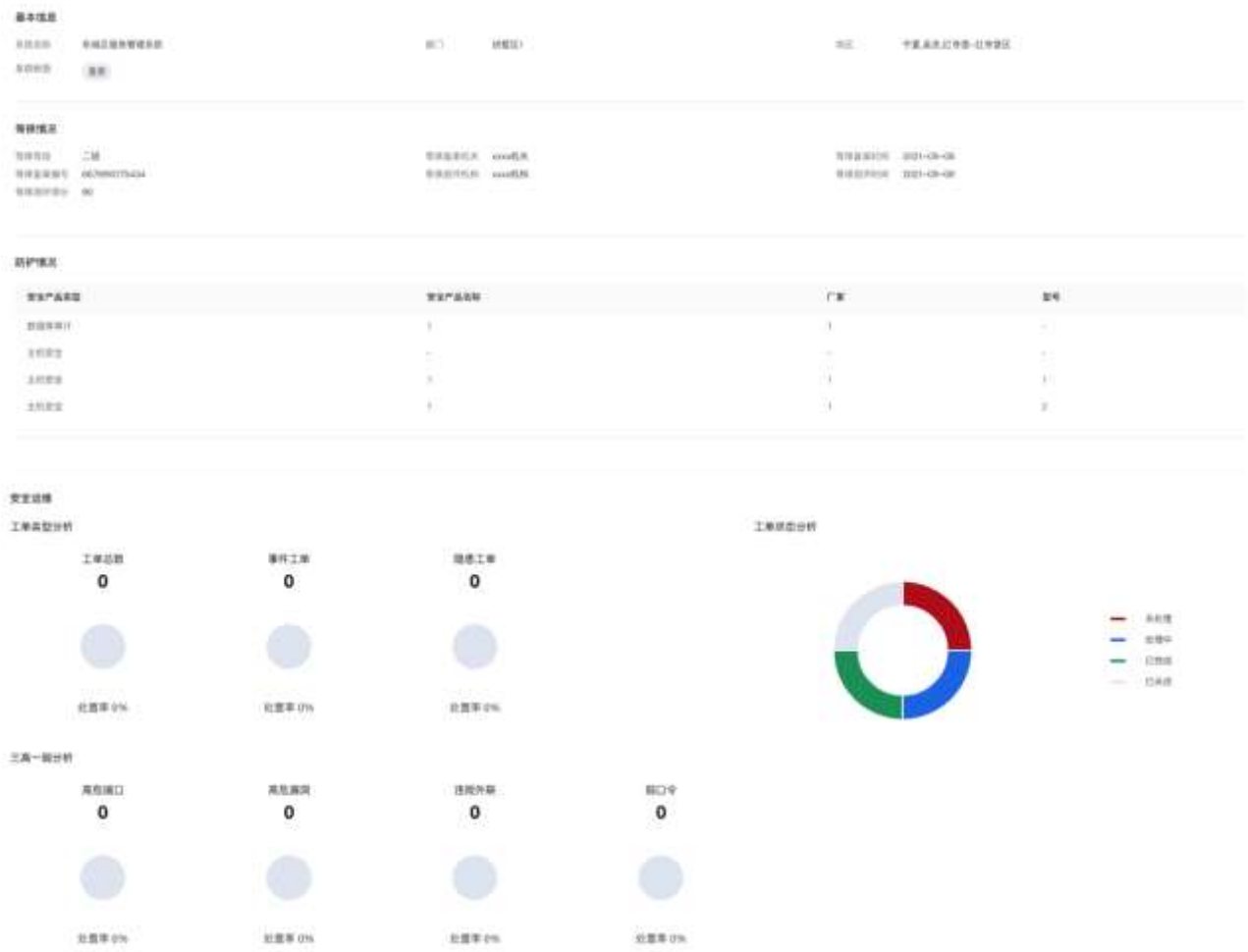
只支持 Excel 格式，上传内容会覆盖原有数据。

5.2.7 导出

支持根据查询筛选条件导出。导出字段如下：

5.2.8 系统详情

在资产列表**操作**列点击<**详情**>，可以查看该项服务的基本信息、等报情况、防护情况、安全运维信息。



5.3 数据资源

数据安全治理，始于数据资产梳理。数据资产管理模块可以通过自动化方式扫描用户的数据库表，建立全局的数据资源目录，并内置了敏感数据识别规则，可以有效识别敏感数据在系统内的分布情况。

同时数据资产管理模块支持对数据库、表以及字段的备注定义和分类标签，可以根据数据价值和特征，梳理出核心数据资产，对其进行分级分类，从而落实对数据更为精细的安全管理措施。

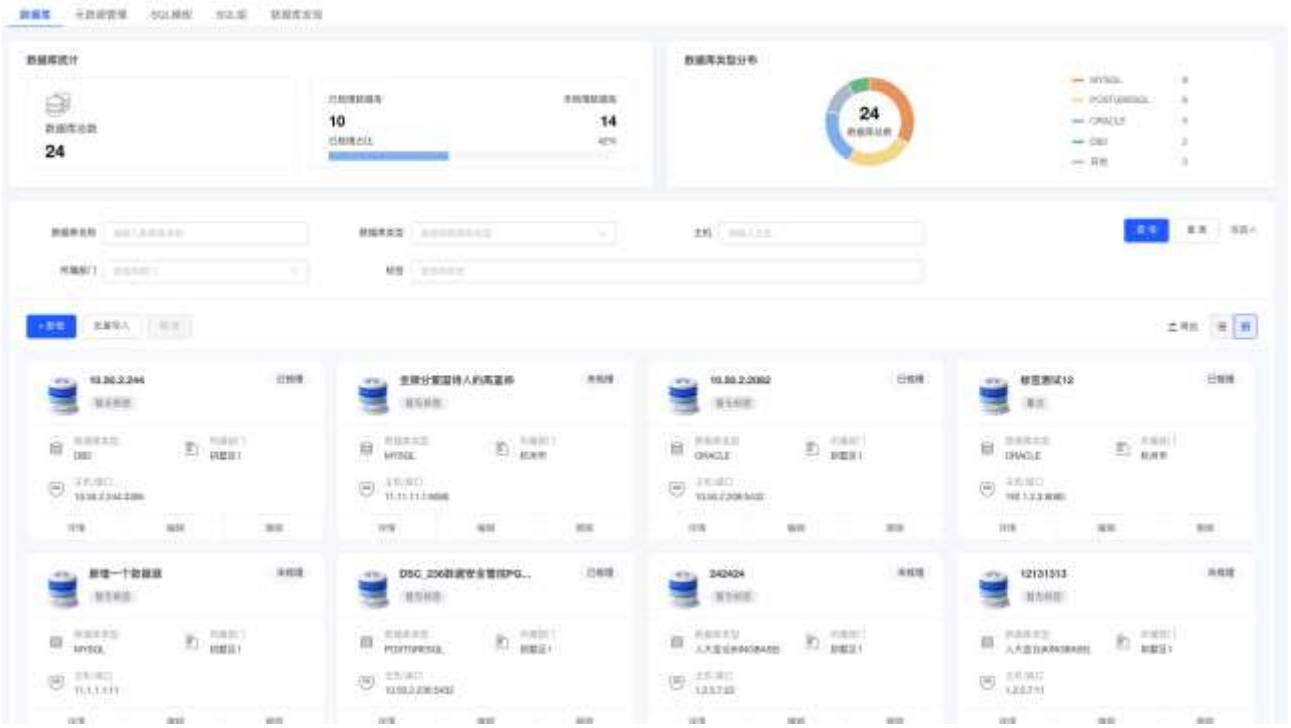
5.3.1 数据库

在数据源中存储了所有建立数据库连接的信息，包括数据库名称、数据库类型以及所包含的对象等等，系统支持对数据库信息进行统一管理和维护。

5.3.1.1 查询数据库

系统支持按照数据库名称、数据库类型以及主机进行条件查询。

5.3.1.2 数据库卡片

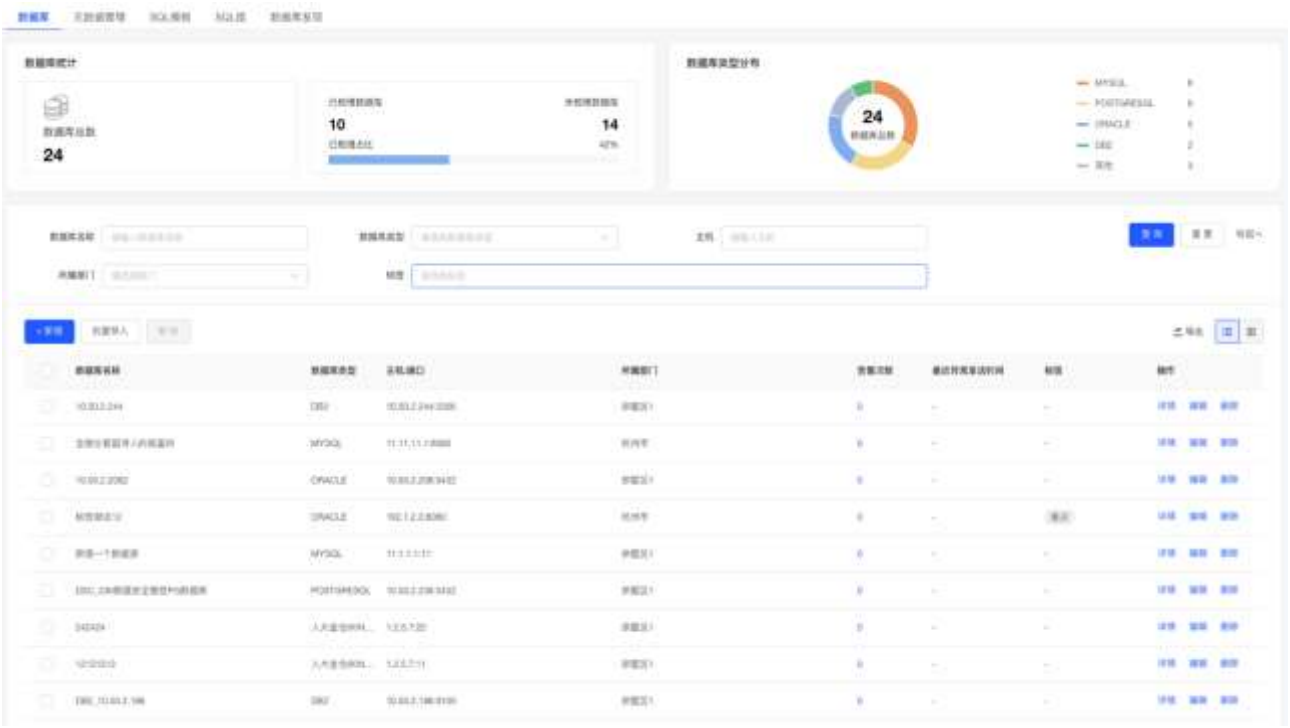


统计区域展示当前账号权限内数据库总数，已梳理数据库和未梳理数据库的数量以及梳理的占比情况；另展示根据数据库类型的分布情况。

默认以卡片的形式展示数据库的基本信息，包括：数据库名称、数据库标签、数据库梳理情况、数据库类型、所属部门、主机：端口。且可在卡片页面进行查看详情、编辑和删除操作。

5.3.1.3 数据库列表

点击  切换到列表页面，在列表页面展示字段包含数据库名称、数据库类型、主机：端口、所属部门、告警次数、最近异常发生时间、标签。且可在列表页面进行查看详情、编辑和删除操作。



5.3.1.4 新增数据库

步骤1. 在菜单栏选择“**资产管理➤数据资源**”进入**数据资源**页面，选择**数据库**页签，点击〈**新增**〉。

步骤2. 进入**新增数据库**页面，填写数据源相关信息，点击〈**保存**〉。

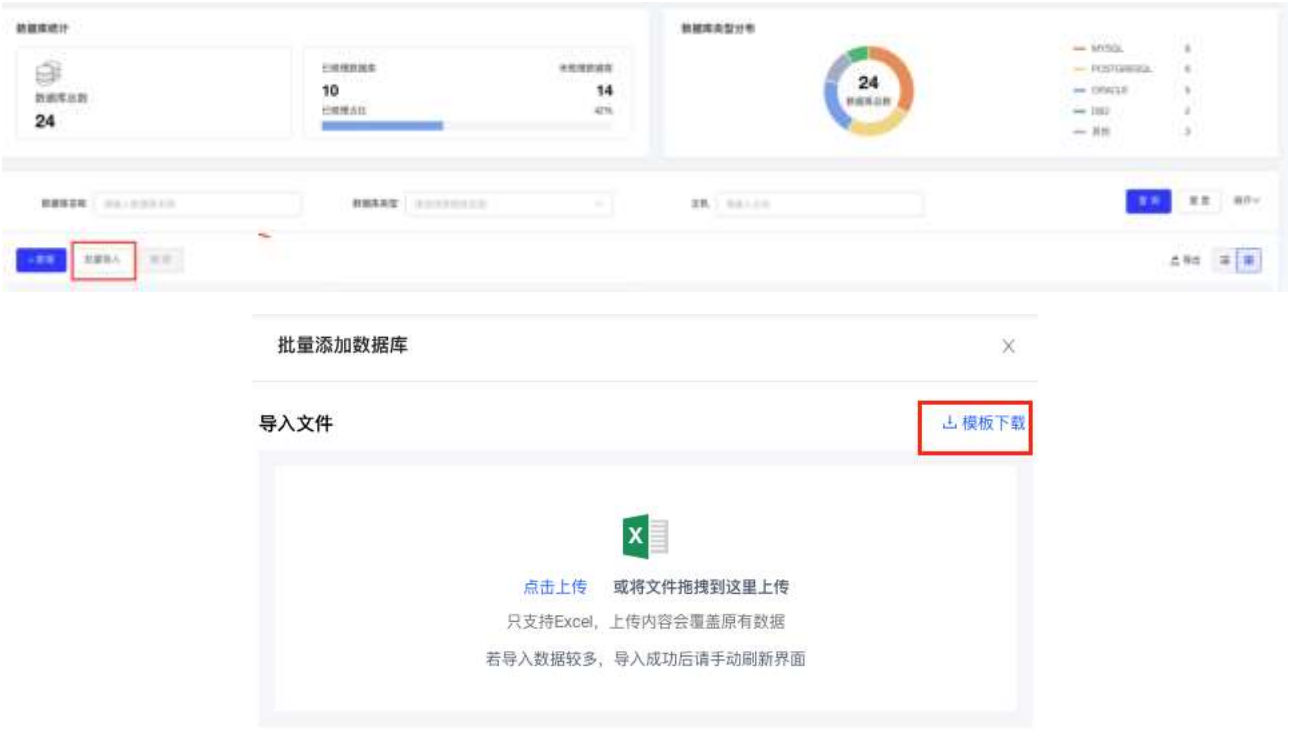
详细配置请参见下表。

配置项	说明
数据库名称	填写数据库名称。
数据库类型	选择数据库的类型，系统支持 Oracle、MySQL 和 SQL Server 等 9 种数据库类型。
主机/端口	填写该项数据库对应的主机 IP 地址/端口号。
版本号	填写该项数据库类型的版本号。
所属部门	选择该项数据库所属部门。
所属系统	选择该项数据库所属系统。
责任人	选择该项数据库的责任归属人。
标签	选择该项数据库所属标签，点击<**新增标签**>可以自定义增加标签类型。
库名/实例名	填写该数据库下的所有库名/实例名信息。
数据库主题信息	选择数据库相对应的主题信息，可添加自定义主题信息。

5.3.1.5 导入数据源

系统支持批量导入数据库。

步骤1.　在**数据库**页面，点击<**批量导入**>，再点击<**模板下载**>，模板将以 xlsx 格式导出至本地，根据模板格式进行填写。



步骤2.　继续点击<**点击上传**>将填写完成的模板拖拽或上传。

5.3.1.6　导出

支持根据查询筛选条件导出。导出字段如下：

5.3.1.7　查看数据库详情

在资产列表**操作**列点击<**详情**>，可以查看该项服务的基本信息、告警统计、库/实例信息。

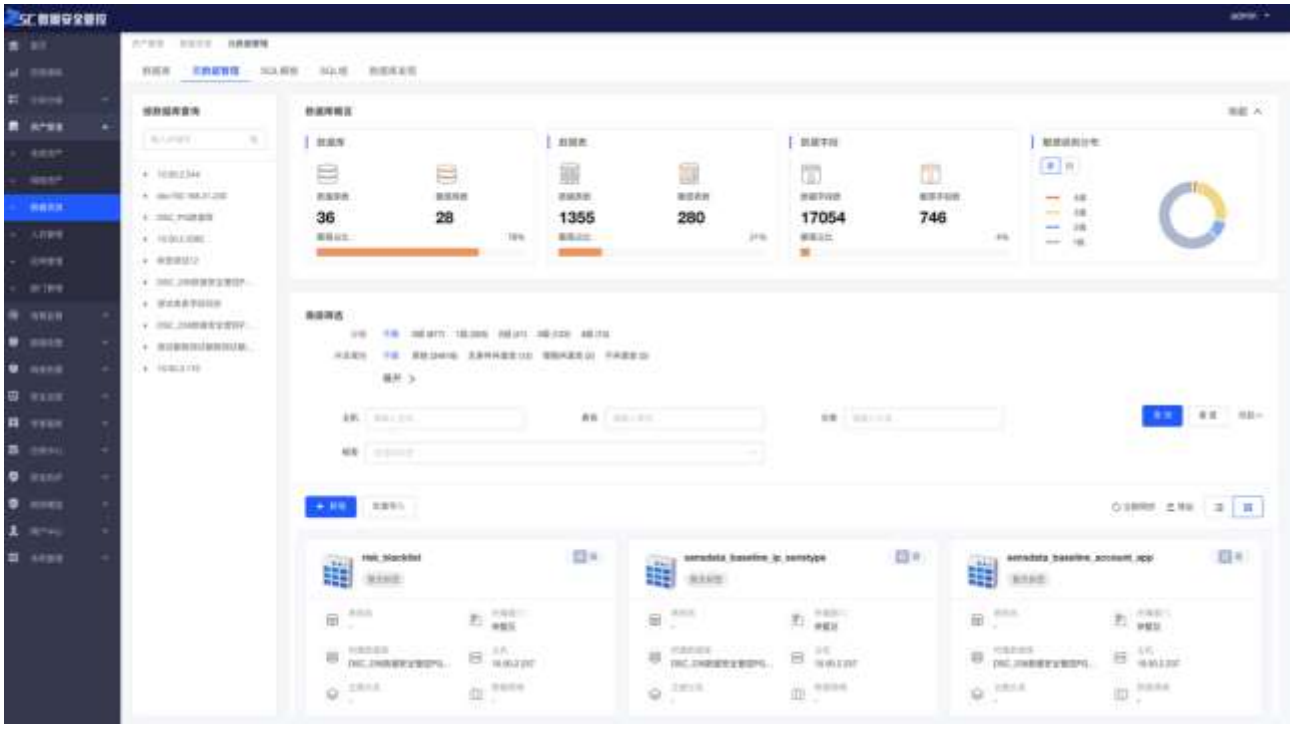
5.3.2 元数据管理

元数据是指描述数据的数据，包括数据源所包含的表和字段等信息，系统对这些数据进行统计和分析。

5.3.2.1 查询条件

可以通过数据库关键字、主机、表名、分类、标签查询数据服务，另外可以通过高级筛选区域过滤分级、共享属性、开放属性、数据领域、主题分类、更新周期等信息。

5.3.2.2 元数据卡片



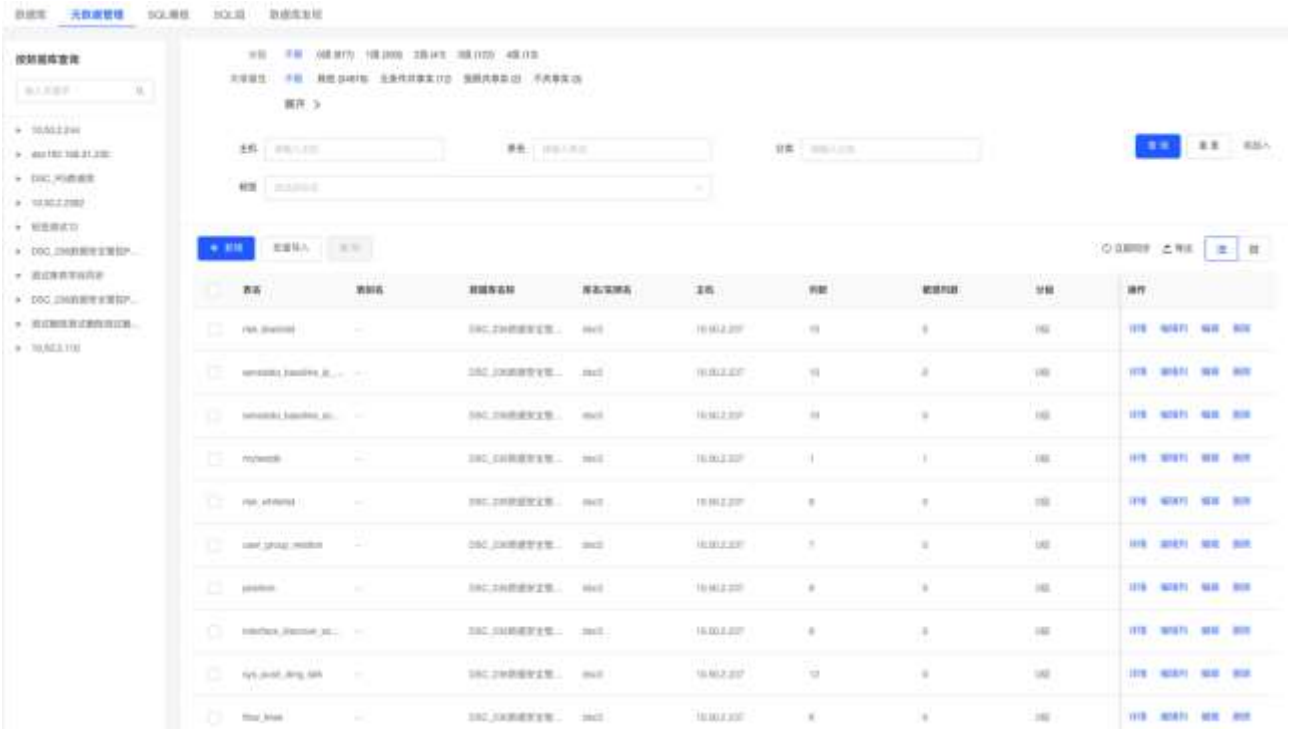
统计区域展示数据库数量、敏感库数量、敏感库占比、数据表数量、敏感表数、敏感表占比、数据字段数、敏感字段数、敏感字段占比、敏感表级别分布和敏感字段级别分布。

默认以卡片的形式展示数据表的基本信息，包括：数据表名称、表别名、所属部门、所属数据库、主机、分级、共享属性、开放属性、数据领域、主题分类、更新周期。且可在卡片页面进行查看详情、编辑和删除操作。

鼠标悬浮展示该数据表下数据列和告警统计情况。

5.3.2.3 元数据列表

点击  切换到列表页面，在列表页面展示字段包含表名、表别名、数据库名称、库名/实例名、主机、列数、敏感列数、分级、分类。且可在列表页面进行查看详情、编辑列、编辑和删除操作。



5.3.2.4 新增元数据

配置项	说明
数据表名称	填写数据表名称。
数据表别名	填写数据表别名。
所属数据库	选择该数据表所属的数据库。
数据库名/实例名	先选择所属数据库，再选择数据库名/实例名。
共享属性	选择该数据表的共享属性。
开放属性	选择该数据表的开放属性。
数据领域	选择该数据表的数据领域。
主题分类	选择该数据表的主题分类。
更新周期	选择该数据表的更新周期。
数据表描述	填写数据表的相关描述。

配置项	说明
标签	选择该项数据库所属标签，点击<**新增标签**>可以自定义增加标签类型。

5.3.2.5 导入元数据

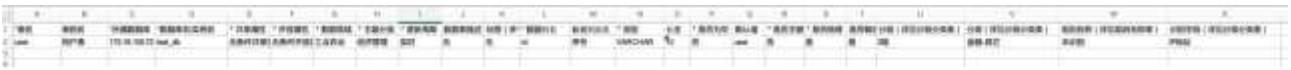
系统支持批量导入元数据。

步骤1. 在**元数据管理**页面，点击<**批量导入**>，再点击<**模板下载**>，模板将以 xlsx 格式导出至本地，根据模板格式进行填写。

步骤2. 继续点击<**点击上传**>将填写完成的模板拖拽或上传。

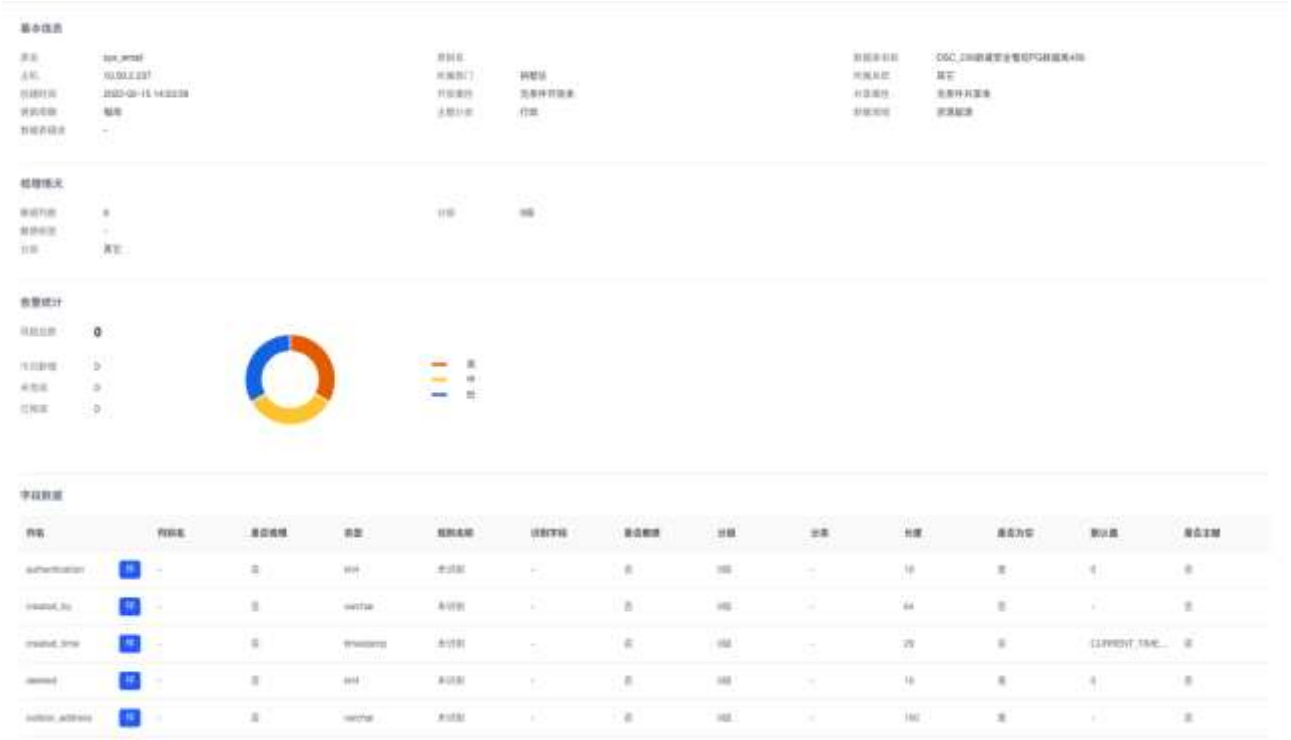
5.3.2.6 导出

支持根据查询筛选条件导出。导出字段如下：



5.3.2.7 查看元数据详情

在资产列表**操作**列点击<**详情**>，可以查看该元数据的基本信息、梳理情况、告警统计以及字段数据信息。



5.3.2.8 编辑列

元数据管理列表页面，点击操作列的 `···` ，再点击<**编辑列**>，可新增或编辑字段。

配置项	说明
列名	填写列名称。
列别名	填写列别名。
字段类型	选择该字段的类型。
长度	填写该字段的长度。
是否为空	选择该字段是否为空。
默认值	填写该字段的默认值。
是否主键	选择该字段是否是主键。
是否梳理	选择该字段是否进行梳理。
是否敏感	选择该字段是否敏感。
识别字段	选择该字段的识别字段。

配置项	说明
分级	选择该字段的分级。
分类	选择该字段的分类。
规则名称	选择识别该字段的规则名称。

5.3.3 SQL 模板

SQL（SQL Template）模板是去参数化的 SQL 语句，系统支持将访问数据库系统的 SQL 语句使用的模板信息提取并存储到磁盘中，用户可以通过 Web 页面查看 SQL 模板集合。

5.3.3.1 查询 SQL 模板

系统支持通过 SQL、所属组以及数据库进行条件查询和筛选。

5.3.3.2 新增 SQL 模板

步骤1. 在菜单栏选择“**资产档案➤数据资源**”进入**数据资源**页面，选择 **SQL 模板**页签，点击<**新增**>。

步骤2. 填写 SQL 语句并将其模板化以及描述信息，选择数据库、SQL 分组以及标签，点击<**保存**>。

详细配置请参见下表。

配置项	说明
SQL 语句	输入 SQL 语句并将其模板化。例如 select * from all。
数据库	选择 SQL 所属数据库，有关数据库详细信息请参考数据。
SQL 组	选择 SQL 语句所属 SQL 组，有关 SQL 组详细信息请参考 SQL 组。
描述	填写对于 SQL 语句的描述信息。
标签	选择该项元数据所属标签，点击<**新增标签**>可以自定义增加标签类型。

5.3.3.3 导入 SQL 模板

系统支持批量导入 SQL 模板。

步骤1. 在 **SQL 模板**页面，点击<**批量导入**>，再点击<**模板下载**>，模板将以 xlsx 格式导出至本地，根据模板格式进行填写。

步骤2.　继续点击<**点击上传**>将填写完成的模板拖拽或上传。

5.3.3.4　查看 SQL 模板详情

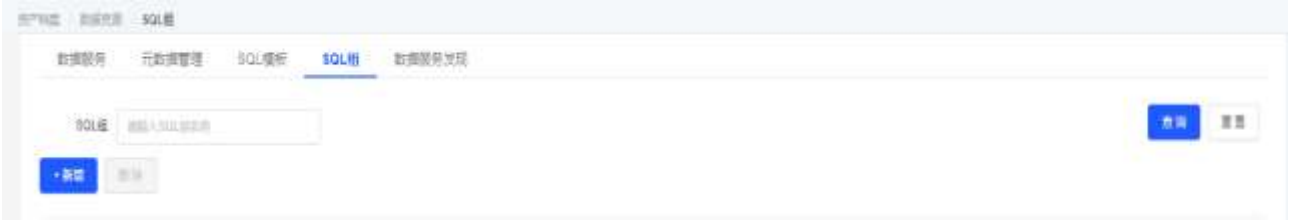
在 SQL 模板列表**操作**列点击<**详情**>，可以查看 SQL 模板的基本信息以及告警统计信息。

5.3.4 SQL 组

在很多应用场景时，需要对数据按照某条件进行分组统计其信息。

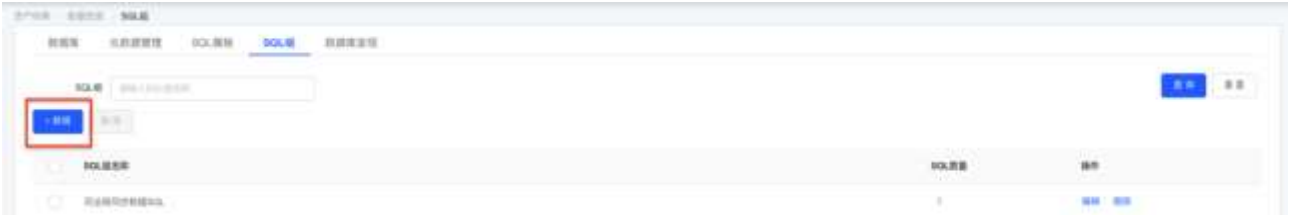
5.3.4.1 查询 SQL 组

系统支持通过 SQL 组名称的方式进行条件查询。



5.3.4.2 新增 SQL 组

步骤1. 在菜单栏选择“**资产档案➤数据资源**”进入**数据资源**页面，选择 **SQL 组**页签，点击<**新增**>。



步骤2. 填写 SQL 组名称以及描述信息，点击<**保存**>。

5.3.5 数据库发现

可以自动发现与系统对接的探针上的数据服务信息，并且可以自行决定添加至系统内或者删除服务。

在菜单栏选择“**资产档案➤网络资产**”进入**网络资产**页面，选择**网络资产发现**页签，可以对系统自动发现的网络资产进行统一管理和维护。

5.3.5.1 查询数据源

系统支持通过主机 IP 地址、数据源类型以及状态进行条件查询。

5.3.5.2 批量编辑数据源

步骤1. 选择所属部门、所属系统，在资产列表**操作**列点击<**批量编辑**>。

步骤2. 选择数据源所属部门和所属系统，点击<**保存**>可以批量编辑服务信息，一键添加时可以快速添加至系统内。

5.3.5.3 添加数据库

选择需要添加到平台管控范围的数据服务（需要编辑所属部门和所属系统），点击<**一键添加**>，或直接点击<**添加**>，状态变更为已添加，可以添加至系统，在数据库中可进行直接管理和维护。

5.3.5.4 同步数据库

点击<**立即同步**>，立即同步子探针上发现的数据库的信息。

5.3.5.5 删除数据源

- 在资产列表**操作**列点击<**删除**>，弹出**是否确认删除**对话框，点击<**确定**>，状态变成已删除。
- 选中需要删除的数据服务，点击<**批量删除**>，弹出**是否确认删除**对话框，点击<**确定**>，删除数据服务。

5.3.5.6 恢复已删除的数据源

在资产列表**操作**列点击<**恢复**>，可以将该项资产恢复至列表内。

5.4 应用管理

采用自动发现、手工录入以及批量导入等方式，对用户的应用服务和接口进行统一梳理。对应用服务（如 API 接口服务、应用服务等）的流量和日志进行监测，并对接口访问进行统计，结合业务规则对高频的访问行为进行及时的告警。

同时对接口的健康状况进行实时监测，包括高延时、返回报错、404 异常访问进行监测、记录以及及时告警。应用和接口可以获取探针信息，接口也可以进行分组管理。

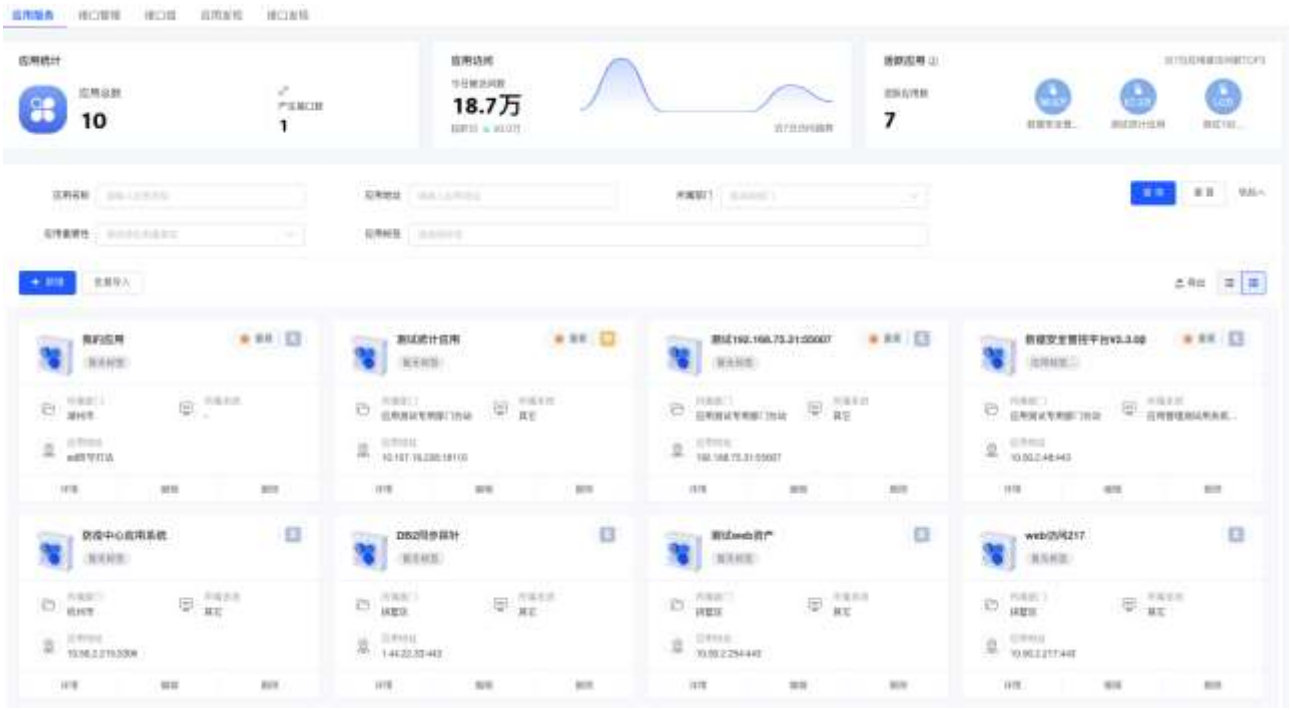
5.4.1 应用服务

服务是具有一定特征的信息流，如具有相应的应用名称、应用地址、所属部门以及所属系统等等。例如：欣欣小区所属部门为市数据资源局，所属系统为共享交换平台，其对应的应用域名为 www.xinxin.com，此应用服务需要重点关注。

5.4.1.1 查询应用服务

系统支持通过应用名称、应用地址以及所属部门进行条件查询。

5.4.1.2 应用服务卡片



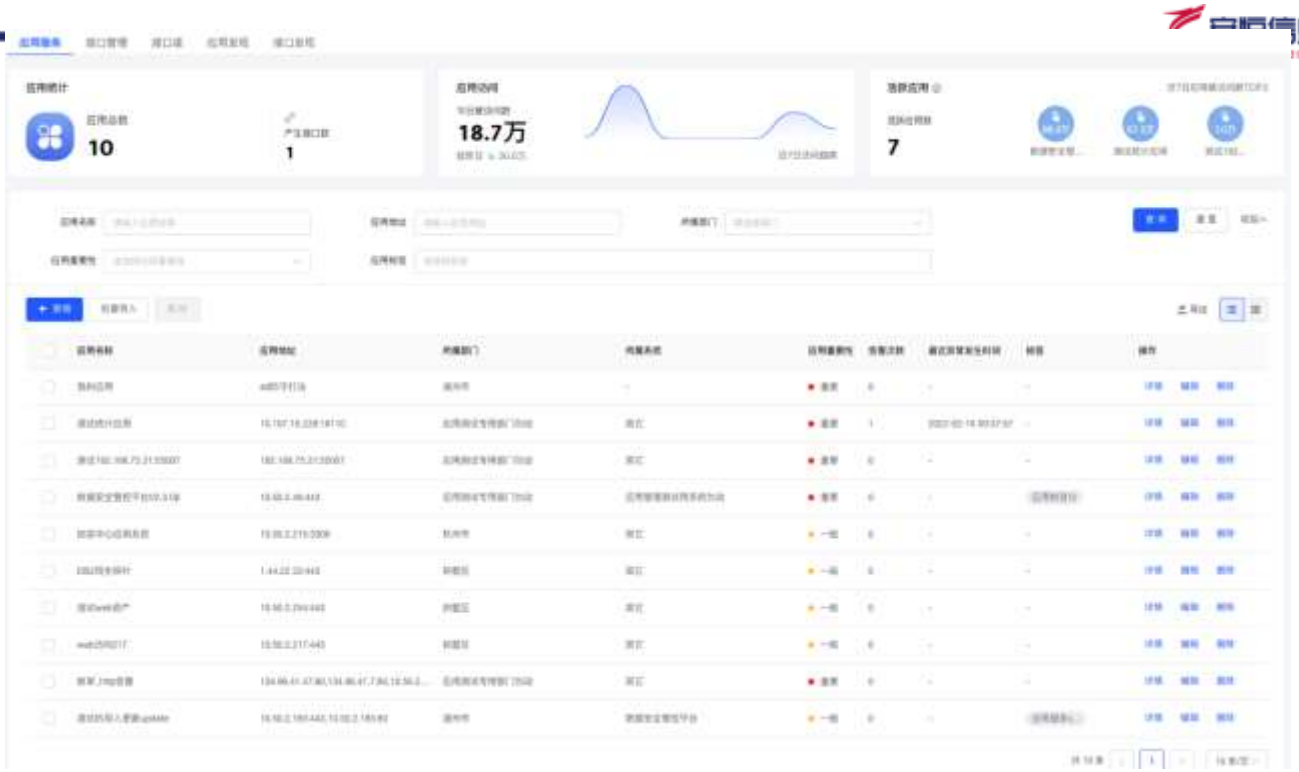
统计区域展示当前权限下应用总数以及产生的接口数;展示应用的今日被访问数量和近 7 日的被访问趋势;展示活跃应用数以及近 7 日应用被访问数 TOP3 的应用。

默认以卡片的形式展示应用的基本信息，包括：应用名称、标签、应用风险等级、所属部门、所属系统、应用地址。且可在卡片页面进行查看详情、编辑和删除操作。

鼠标悬浮展示该应用下告警统计情况。

5.4.1.3 应用服务列表

点击  切换到列表页面，在列表页面展示字段包含应用名称、应用地址、所属部门、所属系统、应用重要性、告警次数、最近异常发生时间、标签。且可在列表页面进行查看详情、编辑和删除操作。



5.4.1.4 新增应用服务

步骤1. 在菜单栏选择“**资产档案➤应用管理**”进入**应用管理**页面，选择**应用服务**页签，点击<**新增**>。

步骤2. 填写基本信息和应用服务实例，点击<**保存**>。

详细配置请参见下表。

配置项	说明
基本信息	
应用名称	填写需要添加的应用名称。
所属部门	选择此项应用所属的部门。
应用域名	填写应用对应的域名。
责任人	填写此项应用对应的责任归属人。
应用重要性	选择此项应用需要关注的重要性。
所属系统	选择此项应用的所属系统。

配置项	说明
系统架构	填写此项应用的系统架构。
描述	填写此项应用的描述信息。
标签	选择该项应用所属标签，点击<**新增标签**>可以自定义增加标签类型。
开发商信息	
开发商名称	填写此项应用的开发商名称。
开发商联系人	填写此项应用的开发商联系人。
联系电话	填写此项应用的开发商联系人联系电话。
应用服务实例	
IP/端口	填写应用下对应所包含的 IP 地址和端口信息，点击<**添加**>可以添加实例，便于统一管理。

5.4.1.5 导入应用

支持批量导入应用。

步骤 1. 在应用服务页面，点击<**批量导入**>，再点击<**模版下载**>，模版将以 xlsx 格式导出至本地，根据模板格式进行填写。

步骤 2. 继续点击<**点击上传**>将填写完成的模版拖拽或上传。

5.4.1.6 导出

支持根据查询筛选条件导出。导出字段如下：

*应用名称	应用域名	IP(多个ip以逗号分割，与端口一	端口(多个端口以逗号分割，1	*所属部门	所属系统	*应用重要性	责任人	描述	标签（多个标签请用英文逗号分割）
测试应用	www.111.com	0.0.0.0		0 市域乡建设委员	不填的话默认为其它	重要	admin	描述	无

5.4.1.7 查看应用详情

在应用列表操作列点击<**详情**>，可以查看该元数据的基本信息、应用服务实例、告警统计信息。

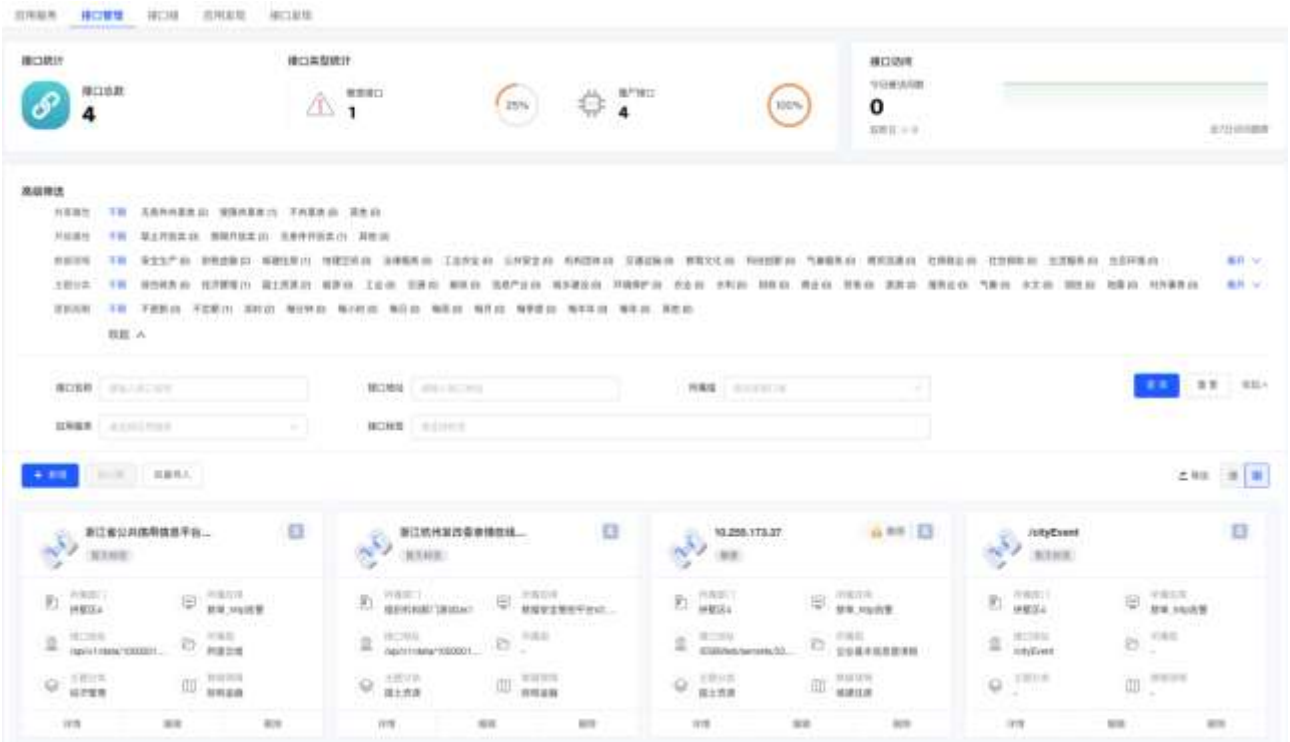
5.4.2 接口管理

系统支持对所访问的应用接口进行统一管理和维护。

5.4.2.1 查询接口

系统支持通过接口名称、接口地址以及所属组进行条件查询。

5.4.2.2 接口卡片



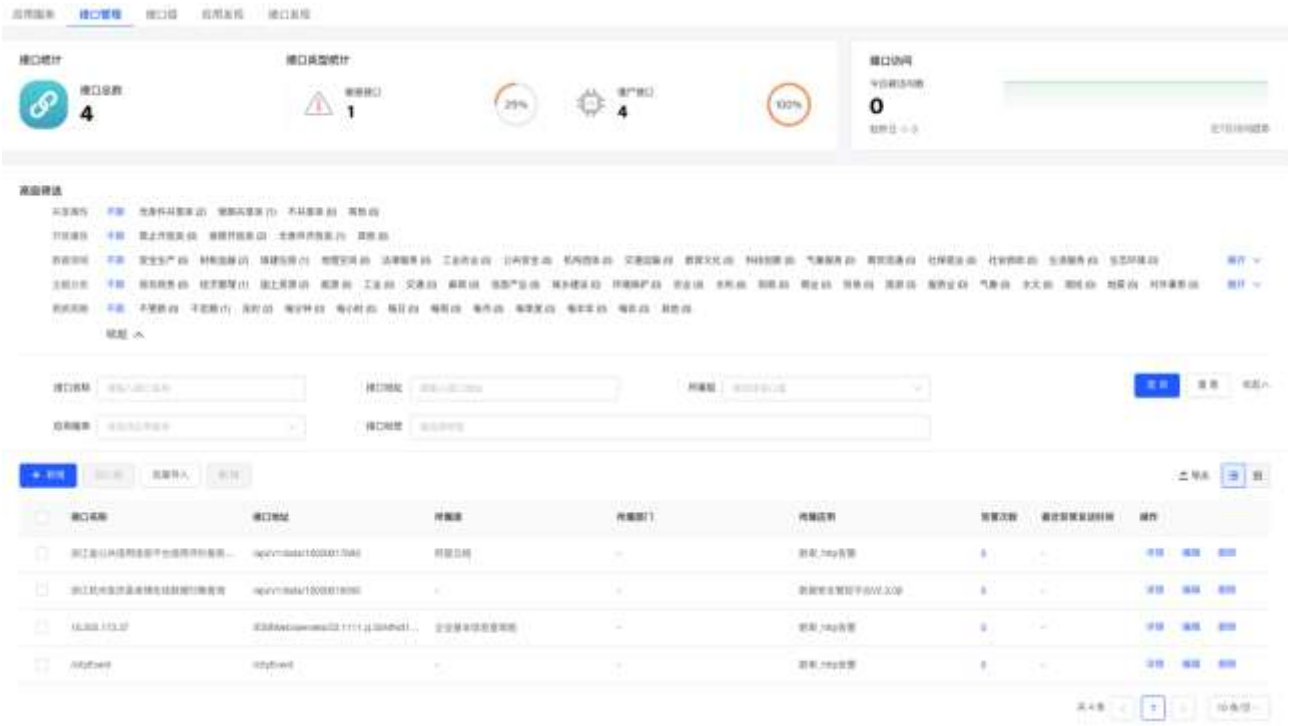
统计区域展示当前权限下接口总数；展示敏感接口数量和僵尸接口数量以及对应的占比；展示接口今日被访问总数和近 7 日被访问的趋势图。

默认以卡片的形式展示应用的基本信息，包括：接口名称、接口共享属性、接口开放属性、接口更新周期、接口风险等级、所属部门、所属应用、接口地址、所属组、主题分类、数据领域。且可在卡片页面进行查看详情、编辑和删除操作。

鼠标悬浮展示该接口的告警统计情况。

5.4.2.3 接口列表

点击  切换到列表页面，在列表页面展示字段包含接口名称、接口地址、所属部门、所属组、所属应用、告警次数、最近异常发生时间。且可在列表页面进行查看详情、编辑和删除操作。



5.4.2.4 新增接口

步骤1. 在菜单栏选择“**资产档案➤接口管理**”进入**接口管理**页面，选择**接口管理**页签，点击〈**新增**〉。

步骤2.　填写基本信息和应用服务实例，点击<**保存**>。

详细配置请参见下表。

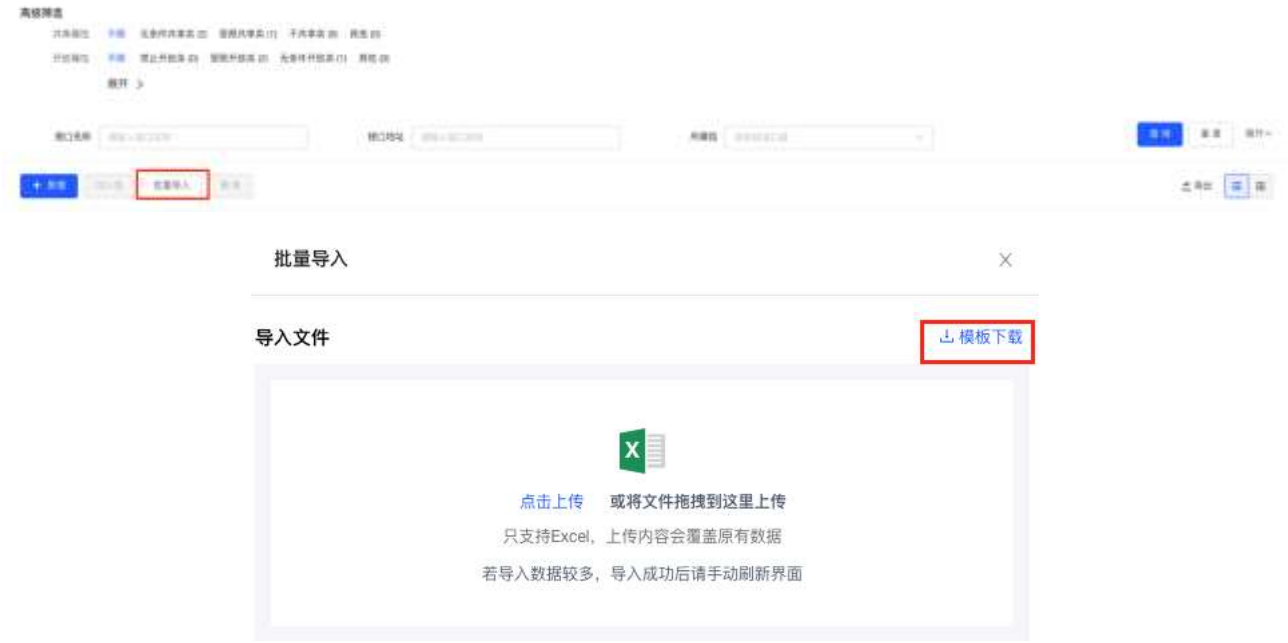
配置项	**说明**
接口名称	填写需要添加的接口名称。
所属部门	选择该接口的所属部门。

配置项	说明
请求方式	选择需要添加的接口的访问请求方式。
接口地址	填写需要添加的接口地址。
应用服务	选择接口对应的应用服务，有关服务的详细信息请参考应用服务。
接口组	选择该接口所属的接口组
共享属性	选择该接口的共享属性。
开放属性	选择该接口的开放属性。
数据领域	选择该接口的数据领域。
主题分类	选择该接口的主题分类。
更新周期	选择该接口的更新周期。
描述	填写此项接口的描述信息。
标签	选择该项应用所属标签，点击<**新增标签**>可以自定义增加标签类型。

5.4.2.5 导入接口

支持批量导入接口。

步骤 1. 在接口管理页面，点击<**批量导入**>，再点击<**模版下载**>，模板将以 xlsx 格式导出至本地，根据模板格式进行填写。



步骤 2. 继续点击<**点击上传**>将填写完成的模板拖拽或上传。

5.4.2.6 查看接口详情

支持根据查询筛选条件导出。导出字段如下：

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	*接口名称	*请求方式	*所属部门	*接口地址	*应用服务	接口组名	标签（多个标签用英文	描述	* 共享属性	* 开放属性	* 数据领域	* 主题分类	* 更新周期
2	企业基本信息查询	GET	公积金中心	api/v1/data/100000	共享平台	企业基本信息查询组	无	查询企业基本信息	受限共享类	无条件开放	财税金融	能源	每月
3													

5.4.2.7 导出

在接口列表操作列点击<**详情**>，可以查看该接口的基本信息以及告警统计信息。

5.4.3 接口组

在很多应用场景时，需要对接口按照某条件进行分组统计其信息。

- 系统支持按照接口组名称进行条件查询。
- 点击<**新增**>，填写接口组名称和描述信息，点击<**保存**>。
- 点击**接口数量**列下的数字链接，将跳转至接口管理，可以查看该接口下的接口数量和详细信息。

5.4.4 应用发现

可以自动发现与系统对接的探针上的应用发现信息，并且可以自行决定添加至系统内或者删除服务。

操作入口：在菜单栏选择“**资产档案➤应用管理**”进入**应用管理**页面，选择**应用发现**页签。

有关应用发现模块的操作与数据库发现类似，此处就不再一一赘述。

5.4.5 接口发现

可以自动发现与系统对接的探针上的接口发现信息，并且可以自行决定添加至系统内或者删除服务。

操作入口：在菜单栏选择“**资产档案➤应用管理**”进入**应用管理**页面，选择**接口发现**页签。

有关接口发现模块的操作与数据库发现类似，此处就不再一一赘述。

5.5 人员管理

对数据库、应用以及主机账号进行集中管理，并对账号权限进行梳理，明确人员尤其是开发测试人员的数据操作权限范围。并且建立了人员账号（关联到自然人）—业务系统（业务系统账号）—数据服务—数据资产的访问关系。

通过数据库审计、堡垒机日志以及 VPN 日志等信息进行关联分析，对其数据访问操作行为进行监督审核，确保相关人员的操作及行为在权限范围内，操作合理合规，同时可对越权行为及高危操作进行告警和记录。针对一些特权账户的使用，监管团队会定期进行审计，判断特权账户使用的必要性和合理性。

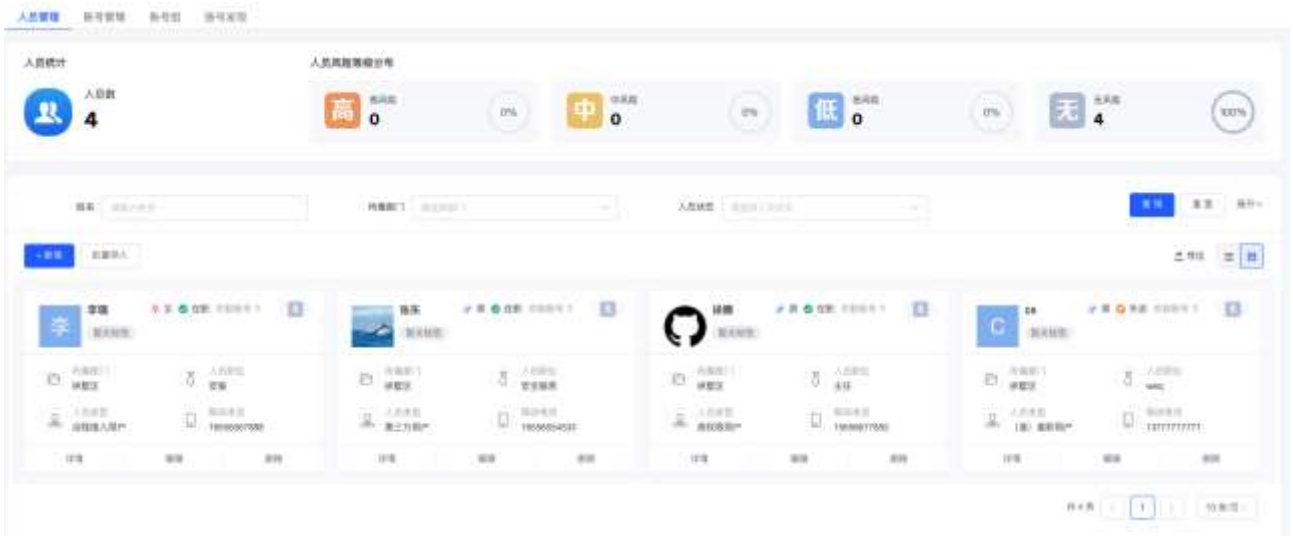
5.5.1 人员管理

系统对人员信息进行统一管理和维护。

5.5.1.1 查询人员

支持通过人员姓名、所属部门、人员状态、人员标签、人员类型进行条件查询。

5.5.1.2 人员卡片

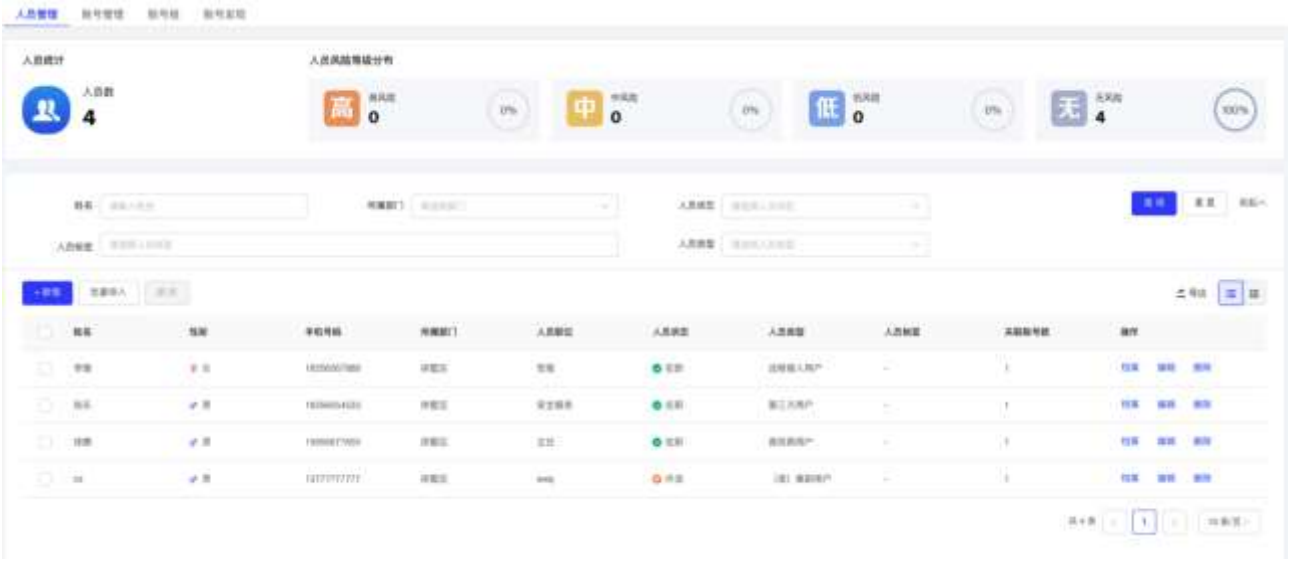


统计区域展示当前权限下人员总数；展示人员的高风险、中风险、低风险以及无风险的分布情况。

默认以卡片的形式展示人员的基本信息，包括：人员名称、性别、所属部门、移动电话、人员职位、人员状态、人员类型。且可在卡片页面进行查看详情、编辑和删除操作。

5.5.1.3 人员列表

点击  切换到列表页面，在列表页面展示字段包含人员姓名、性别、手机号码、所属部门、人员职位、人员状态、人员管理、人员标签、关联账号数。且可在列表页面进行查看详情、编辑和删除操作。



5.5.1.4 新增人员

步骤 1. 在菜单栏选择“**资产档案➤人员管理**”进入**人员管理**页面，选择**人员管理**页签，点击<**新增**>。

步骤 2. 进入新增人员页面，填写人员姓名等相关信息，点击<**保存**>。

详细配置请参见下表。

配置项	说明
基本信息	

配置项	说明
姓名	填写需要添加的人员姓名。
性别	勾选人员的性别。
身份证	填写人员的身份证。
手机号码	填写人员的手机号码。
固定电话	填写人员的固定电话。
常用邮箱	填写人员的常用邮箱。
所属部门	选择人员所属的部门。
人员职位	填写人员的职位。
人员状态	选择人员的状态。
人员类型	选择人员的类型。
上传头像	上传人员头像，图片不能超过 5M。
扩展信息	
标签	选择该人员所属标签，点击<**新增标签**>可以自定义增加标签类型。
描述	填写该人员的描述信息。
关联信息	
关联账号名	选择该人员相关联的账号。点击<**添加**>可添加多个账号。
关联资产	选择账号后，自动为其匹配对应资产。

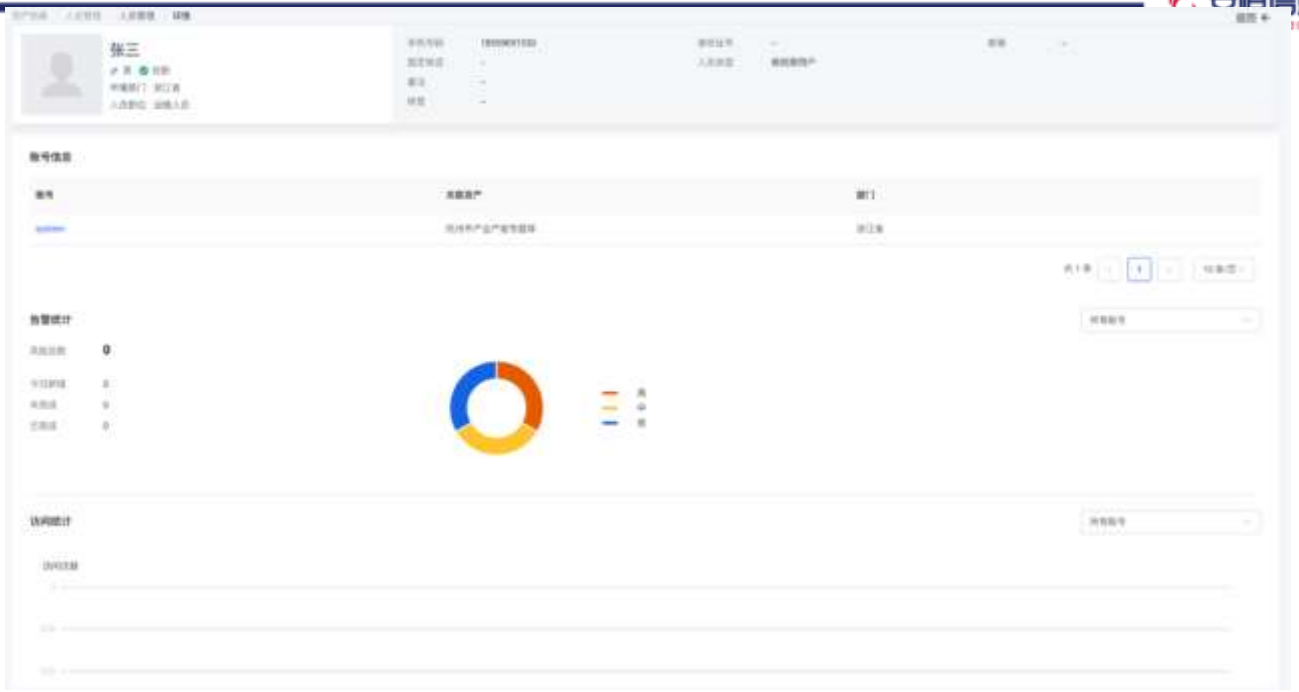
5.5.1.5 导出

支持根据查询筛选条件导出。导出字段如下：

A	B	C	D	E	F	G	H	I	J	K	L
*姓名	*性别	身份证	*手机号码	固定电话	常用邮箱	*所属部门	*人员职位	*人员状态	*人员类型	标签（多个标签用英文逗号隔开）	描述
张三	男	330621997110987OO	13676767776	0575-09898876	xxxx.uuuu@yahoo.com	市国资委	主任	离职	第三方用户	安全运维人员	无

5.5.1.6 查看人员详情

在人员列表操作列点击<详情>，可以查看该账号的基本信息，账号信息，告警统计一级访问统计等信息。



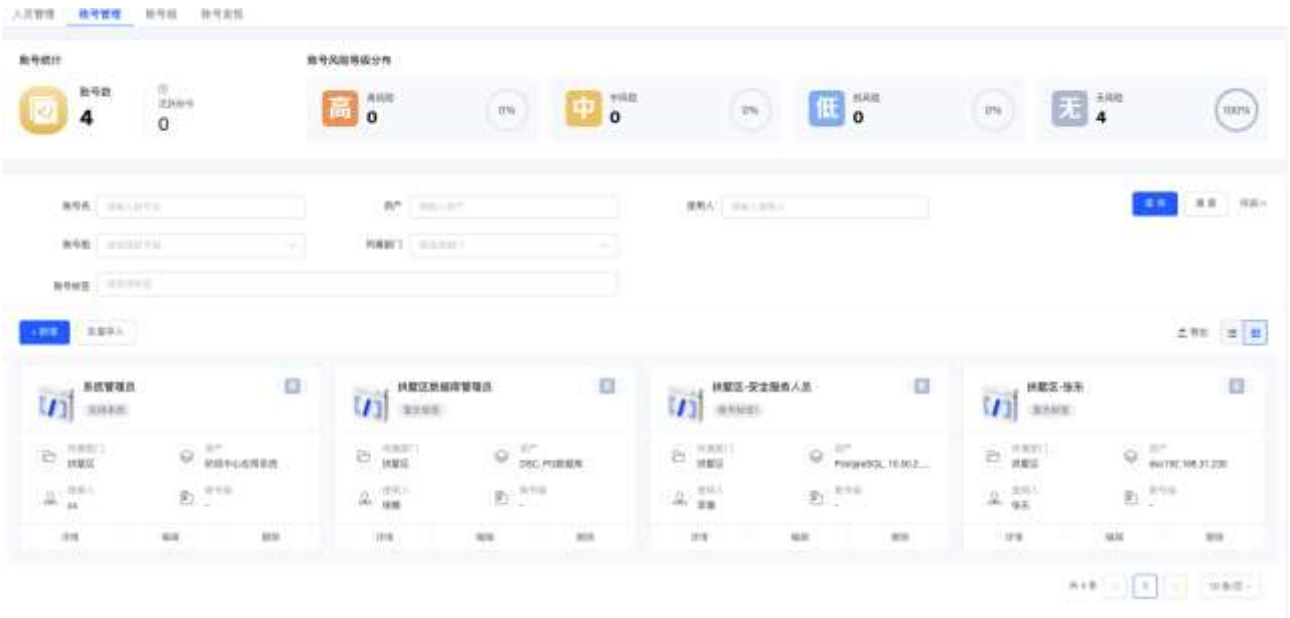
5.5.2 账号管理

系统对账号信息进行统一管理和维护。

5.5.2.1 查询账号

支持通过账号名、资产、使用人、账号组、所属部门和账号标签进行条件查询。

5.5.2.2 账号卡片



统计区域展示当前权限下账号总数和活跃账号数量；展示账号的高风险、中风险、低风险和无风险的分布情况。

默认以卡片的形式展示应用的基本信息，包括：账号名称、资产、使用人、账号组、所属部门、告警次数、异常时间、标签。且可在卡片页面进行查看详情、编辑和删除操作。

鼠标悬浮展示该账号的告警统计情况。

5.5.2.3 账号列表

点击  切换到列表页面，在列表页面展示字段包含账号名、资产、使用人、账号组、所属部门、告警次数、异常时间、标签。且可在列表页面进行查看详情、编辑和删除操作。

5.5.2.4 新增账号

步骤1. 在菜单栏选择“**资产档案➤账号管理**”进入**账号管理**页面，选择**账号管理**页签，点击<**新增**>。

步骤2. 进入**新增账号**页面，填写账号名等相关信息，点击<**保存**>。

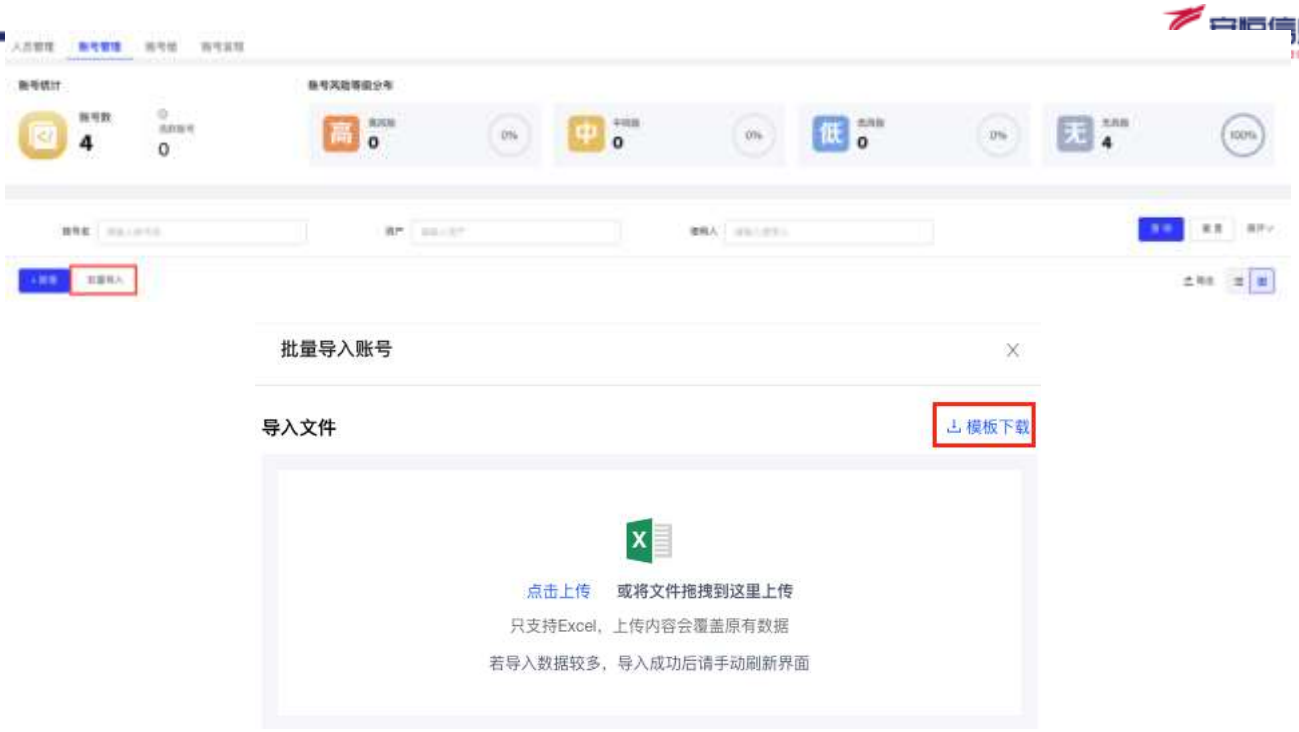
详细配置请参见下表。

配置项	说明
账号名	填写需要添加的账号名。
使用人	填写使用人姓名。
资产	选择账号所管理的资产，包含数据库、应用服务和主机。有关数据库、应用服务和主机的相关信息请参考网络资产、数据、应用管理。
拥有权限	填写账号所拥有的权限。
禁止权限	填写账号所禁止的权限。
描述	填写账号的描述信息。
标签	选择该账号所属标签，点击<**新增标签**>可以自定义增加标签类型。

5.5.2.5 导入账号

支持批量导入账号。

步骤 1. 在账号管理页面，点击<**批量导入**>，再点击<**模板下载**>，模板将以 xlsx 格式导出至本地，根据模板格式进行填写。



步骤 2. 继续点击<**点击上传**>将填写完成的模板拖拽或上传。

5.5.2.6 导出

支持根据查询筛选条件导出。导出字段如下：

	A	B	C	D	E	F	G	H
1	*账号名	*资产类型	*资产	使用人	拥有权限	禁止权限	描述	标签（多个标签用英文逗号隔开）
2	sys	database	数据资源局前置机数据库	徐佳	无	无	无	无
3								

5.5.2.7 查看账号详情

在账号列表操作列点击<**详情**>，可以查看该账号的基本信息、告警统计以及来源 IP 等信息。

5.5.3 账号组

在很多应用场景时，需要对账号按照某条件进行分组统计其信息。

- 系统支持按照账号组名称进行条件查询。
- 点击<**新增**>，填写账号组名称和描述信息，可以新增账号组。

5.5.4 账号发现

可以自动发现与系统对接的探针上的账号发现信息，并且可以自行决定添加至系统内或者删除服务。

操作入口：在菜单栏选择“**资产档案➤人员管理**”进入**人员管理**页面，选择**账号发现**页签。

有关接口发现模块的操作与数据库发现类似，此处就不再一一赘述。

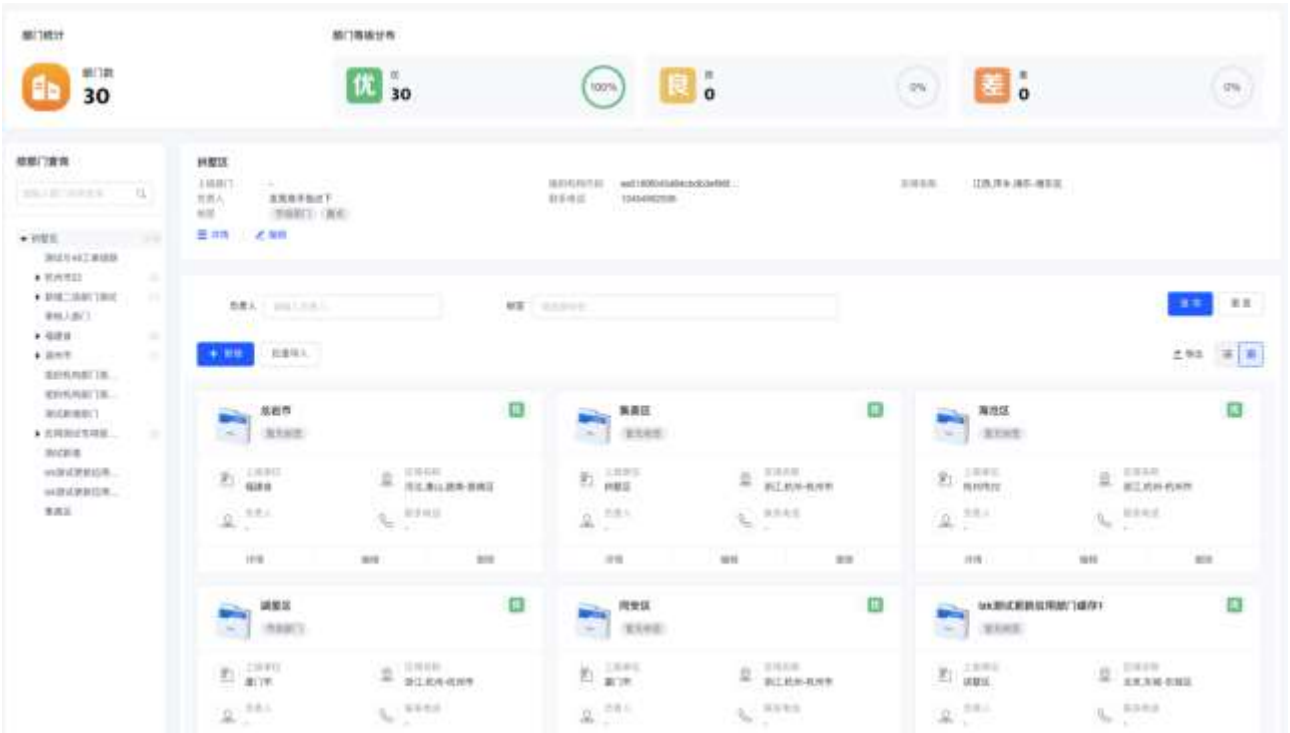
5.6 部门管理

部门管理模块主要提供对部门组织架构的管理，与用户的部门或者机构对应，用于实现对用户的分组归类管理，部门具有上下级关系，可以实现无限极的子节操作，同时可以查看部门下的人员。

5.6.1 查询部门

系统支持对部门、负责人和标签的条件查询。

5.6.2 部门卡片



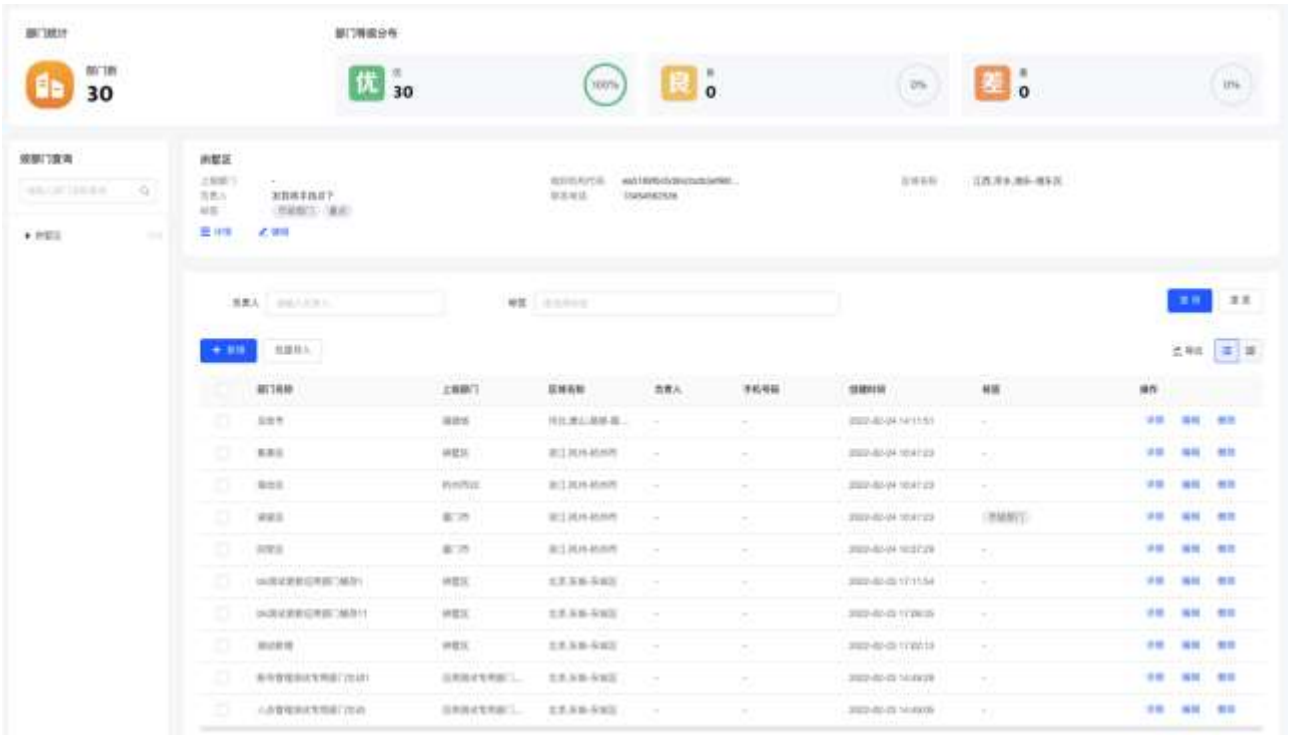
统计区域展示当前权限下部门总数；展示部门优秀、良好、差的等级分布情况。

默认以卡片的形式展示部门的基本信息，包括：部门名称、部门标签、部门等级情况、上级部门、区域名称、负责人、联系电话。且可在卡片页面进行查看详情、编辑和删除操作。

鼠标悬浮展示该部门下的系统情况、资产情况和安全运营情况。

5.6.3 部门列表

点击  切换到列表页面，在列表页面展示字段包含部门名称、上级部门、区域名称、负责人、手机号码、创建时间、标签。且可在列表页面进行查看详情、编辑和删除操作。



5.6.4 新增部门

操作步骤如下。

步骤1. 在菜单栏选择“**资产档案➤部门管理**”进入**部门管理**页面，点击<+>或<**新增**>。

步骤2. 进入**新增部门**页面，填写部门信息和组织机构代码，选择上级部门、区域划分以及有无独立平台，点击<**确定**>。

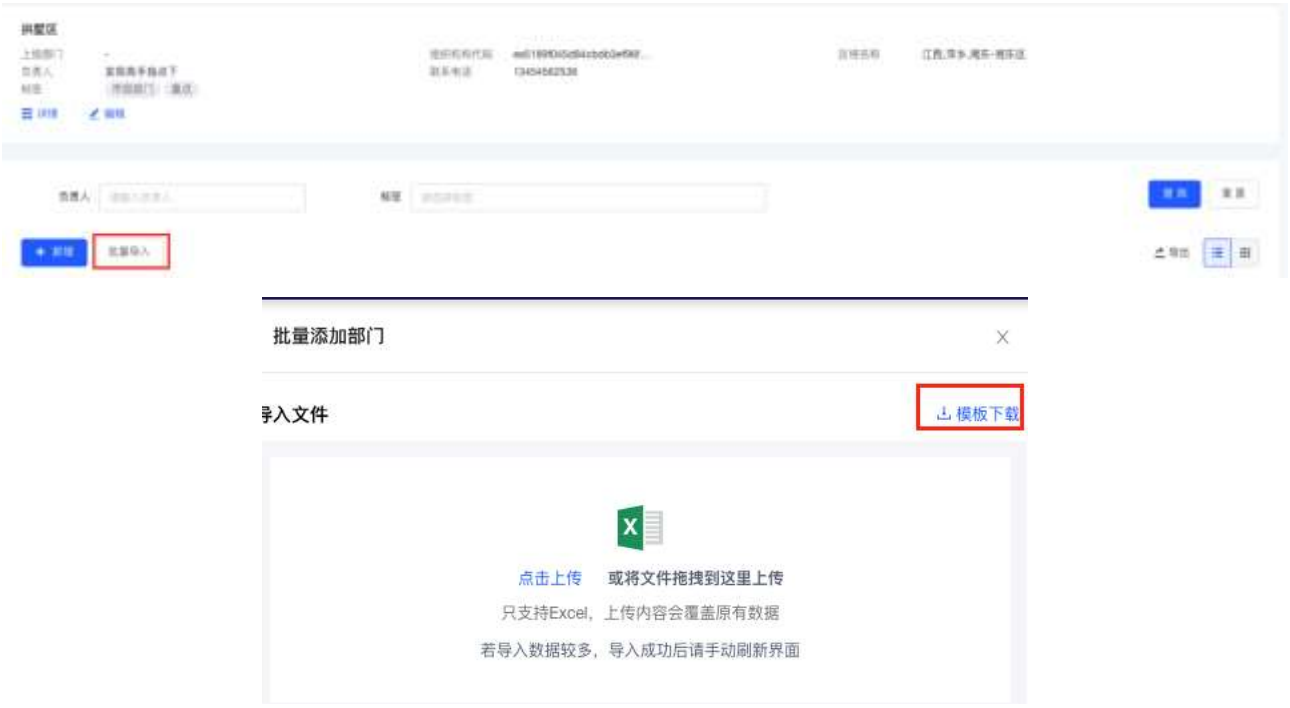
详细配置请参见下表。

配置项	**说明**
部门名称	填写需要添加的部门名称。
上级部门	选择该部门的上级部门。
组织机构代码	填写该部门的组织机构代码。
区域划分	选择该部门的所属的区域。
部门类型	选择该部门所属的部门类型。
有无独立平台	勾选该部门是否有独立平台，如果选择独立平台探针。
标签	选择该部门所属标签，点击<**新增标签**>可以自定义增加标签类型。

5.6.5 导入部门

支持批量导入部门。

步骤 1. 在部门管理页面， 点击<**批量导入**>，再点击<**模板下载**>，模板将以 xlsx 格式导出至本地，根据模板格式进行填写。



步骤 2. 继续点击<**点击上传**>将填写完成的模板拖拽或上传。

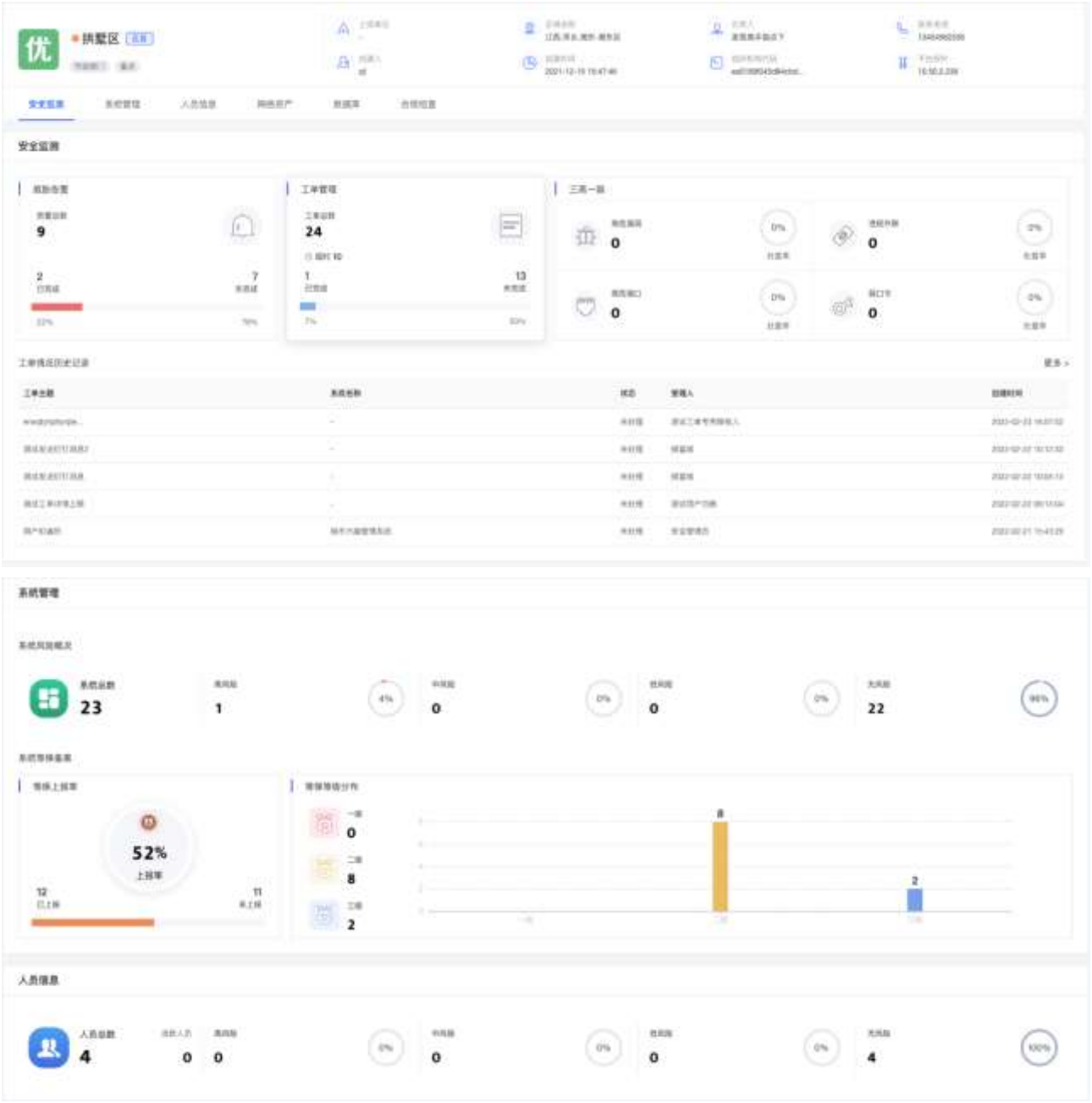
5.6.6 导出

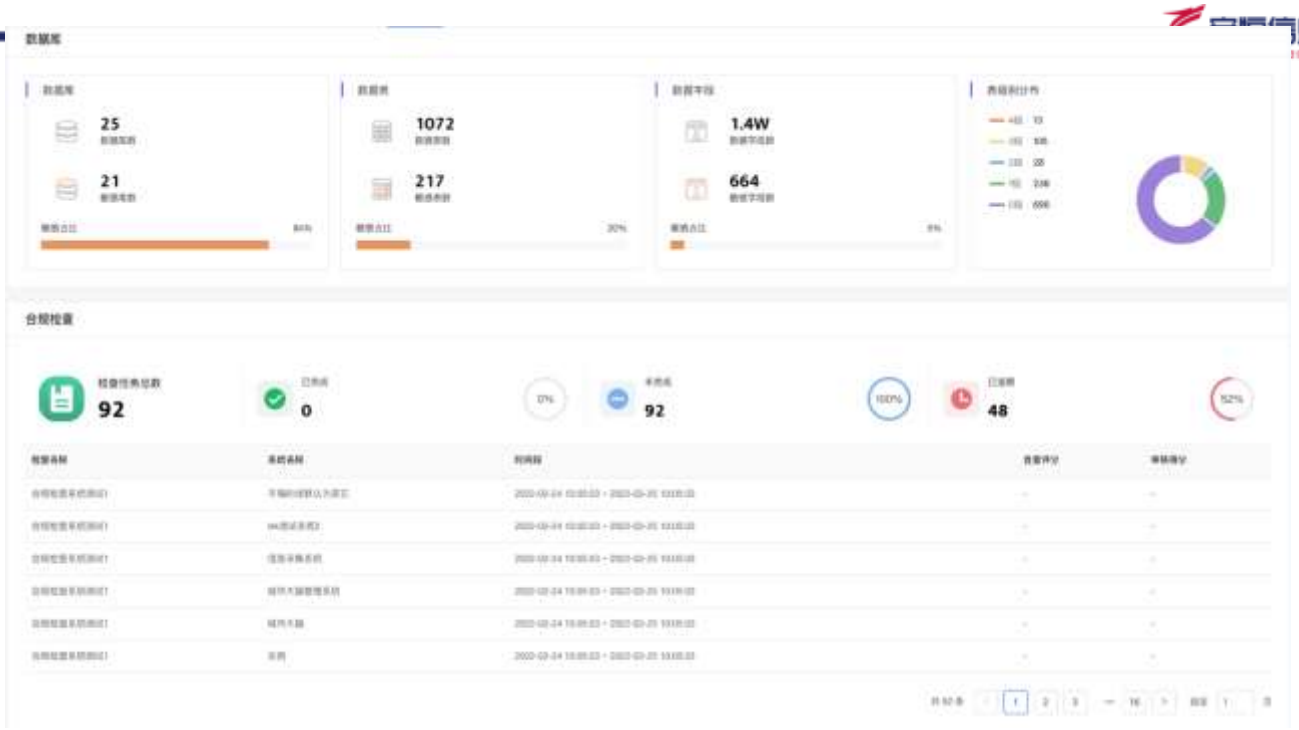
支持根据查询筛选条件导出。导出字段如下：

	A	B	C	D	E	F
1	*部门名称	*上级部门	机构组织代码	*区域划分（详见区域划分对照表）	*部门类型	标签（多个标签请用英文逗号分隔）
2	杭州市	市城乡建设委员会	3a6050b4d34f4032b2ee3550b4d9dd71	浙江,杭州,滨江	委办局	无
3						

5.6.7 查看部门详情

展示了该部门的基本信息、安全监测、系统管理、人员信息、网络资产、数据库、合规检查等情况。




数据库
25
21
1072
217
1.4W
664
合规检查
92
0
92
48

系统支持半自动化可视化拓扑建模。

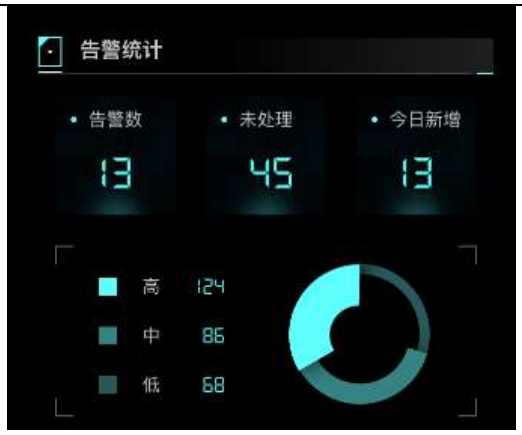
6.1 业务场景

根据业务建模生成业务数据流程大屏，可直观查看业务数据流转情况及其风险情况。

点击业务建模大屏，可在另一个页面全屏查看大屏。

各模块详细说明如下。

展示项	说明	其他
业务流程图	显示业务建模时配置的业务流程图。	
应用服务	选中应用服务显示： ◆ 基本信息：应用名称、应用地址、系统重要性、所属部门、所属系统、标签、描述以及创建时间。 ◆ 接口：显示该应用的接口。 ◆ 访问趋势：最近 7 天的访问次数。	

展示项	说明	其他
数据服务	选中数据服务显示： ◆ 基本信息：数据服务：数据源名称、数据源类型、主机、端口、库名/实例名、版本号、所属部门、所属系统、标签以及创建时间。 ◆ 表：显示该数据服务用到的表。 ◆ 访问趋势：最近 7 天的访问次数。	
告警统计	统计告警数、未处理告警数、今日新增告警数、（高、中、低）等级告警数。	

展示项	说明	其他
告警信息	最近 20 条告警轮播。	

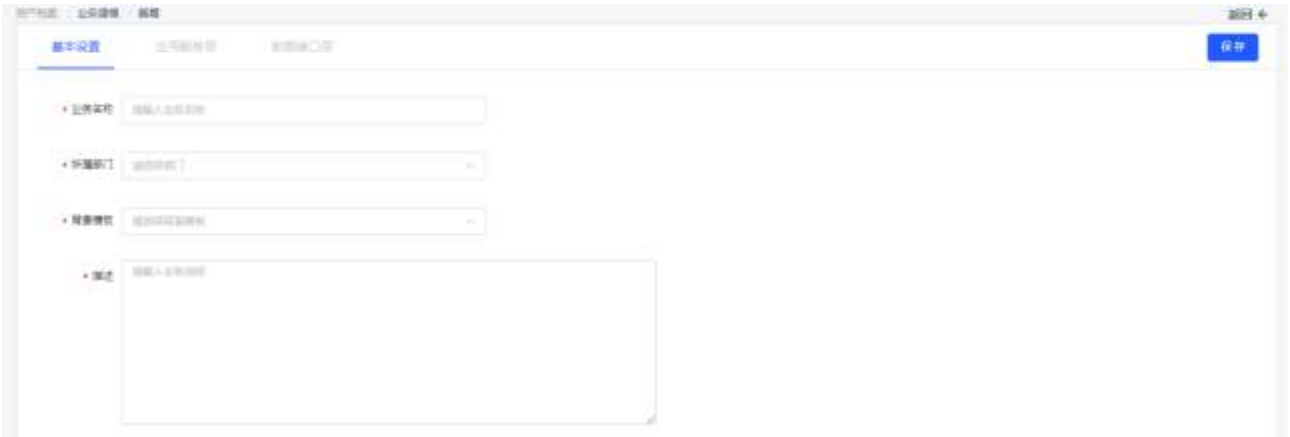
6.2 业务建模

面向多部门协同的业务场景或复杂的数据流转场景，根据数据的流向，利用数据流节点，采用简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑配置和统一管理。同时，基于业务需求对其节点及节点之间的数据流转设置监控策略。基于业务的数据流转拓扑作为数据、业务和人员安全监控的参考基线，包括节点对象的访问量、访问流量、访问速率、请求延时、异常访问和敏感数据访问的监控，同时支持对特定数据的全网数据流转拓扑自动梳理。

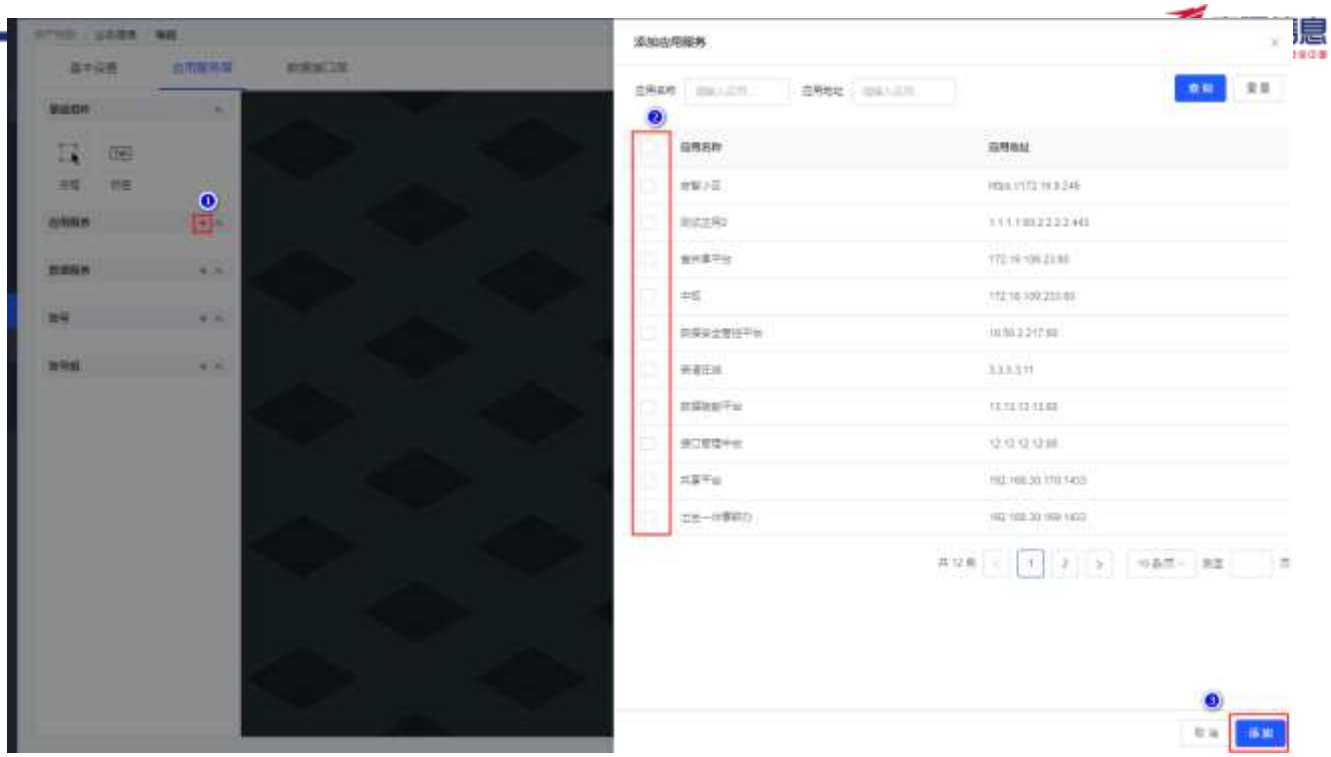
6.2.1 新增建模

步骤1. 在菜单栏选择“**资产档案➤业务建模**”进入**业务建模**页面，点击<**新增**>。

步骤2. 输入业务名称、所属部门、背景模板以及描述等账号组信息，点击<**保存**>。



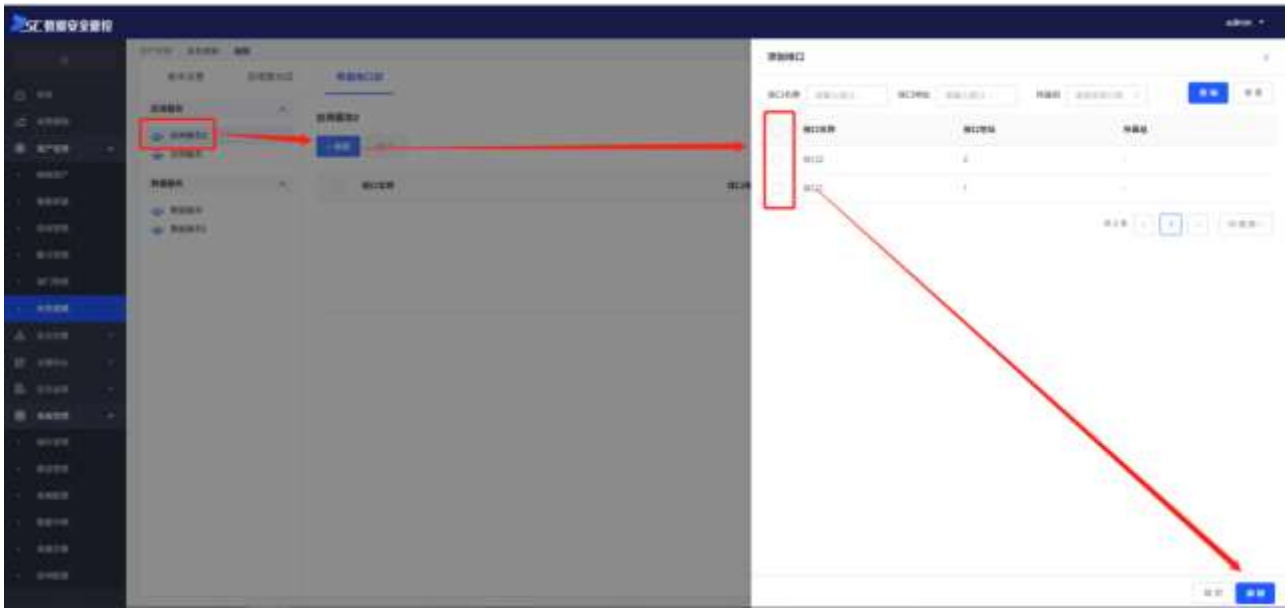
步骤3. 填写完基本信息后，跳转至**应用服务层**页签，进行应用服务、数据服务、账号组、账号的添加。点击+，勾选需要添加的账号组（应用服务、数据服务、账号），点击<**添加**>。此处仅以应用服务为例展开介绍。



步骤4.　应用服务层、数据服务、账号、账号组添加完后可组建业务建模。选中左边的基础组件、应用服务以及数据服务等往右边拖可组成业务建模大屏，点击<**保存**>，完成业务建模的组建。

步骤5.　保存业务建模后可进行预览，点击<**预览**>，进行大屏的查看。

步骤6. 应用服务层添加应用服务和数据服务后，选择**接口数据层**页签进行应用服务的接口、数据服务的表的添加。点击某个应用，点击<**添加**>，选择要添加的应用服务的接口，点击<**添加**>添加应用服务接口。

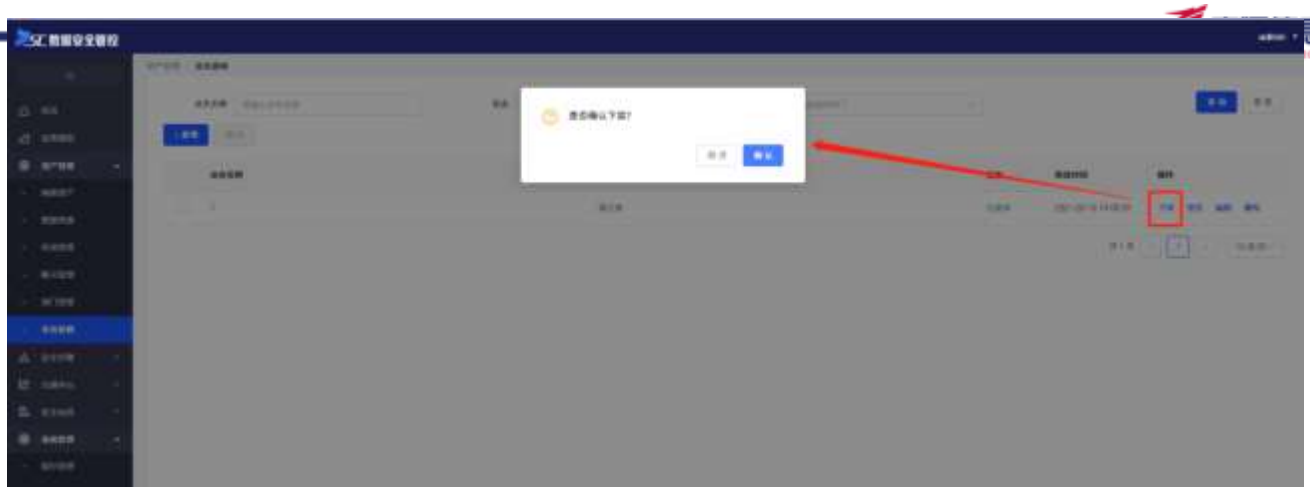


6.2.2 发布建模

点击建模列表**操作**列的<**发布**>，可以在态势感知进行查看。

6.2.3 下架建模

点击建模列表**操作**列的<**下架**>，已发布的业务建模才能下架，可将已发布到态势感知的业务建模进行下架。



7. 数据告警

系统支持从数据告警管理和安全隐患管理两个维度查看和管理告警和隐患信息。

7.1 数据原始告警

对探针发现的告警事件进行统一管理并提供各维度的查询功能。

7.1.1 查询告警信息

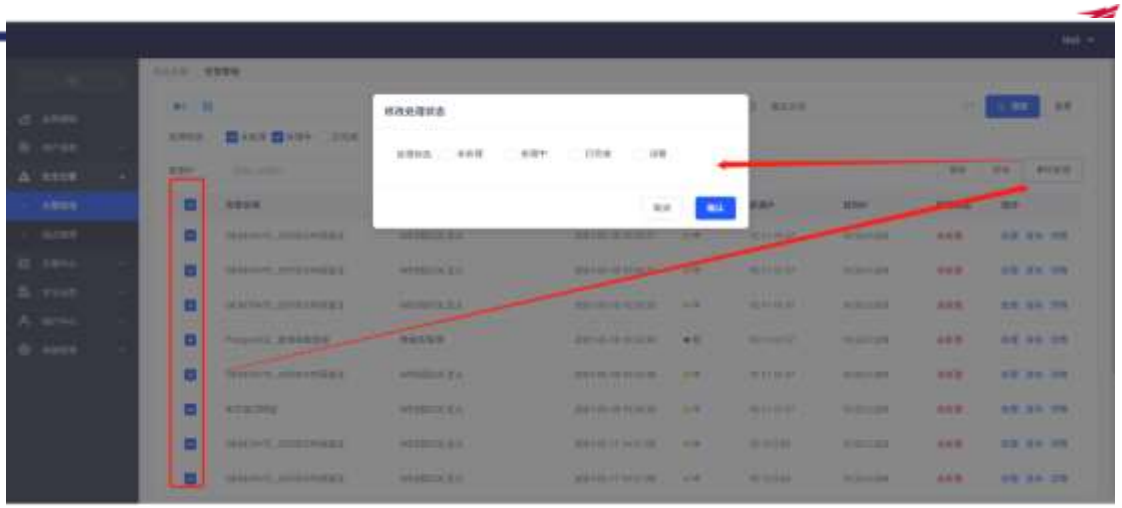
在菜单栏选择“数据告警➤**数据原始告警**”进入**数据原始告警**页面，设置查询条件（时间、处理状态、告警等级、来源 IP 以及目的 IP），点击<**搜索**>即可查询相关告警信息。

7.1.2 处理告警信息

点击告警信息列表**操作**列的<**处理**>，弹出**修改处理状态**对话框，设置处理状态，可以对事件进行处理。

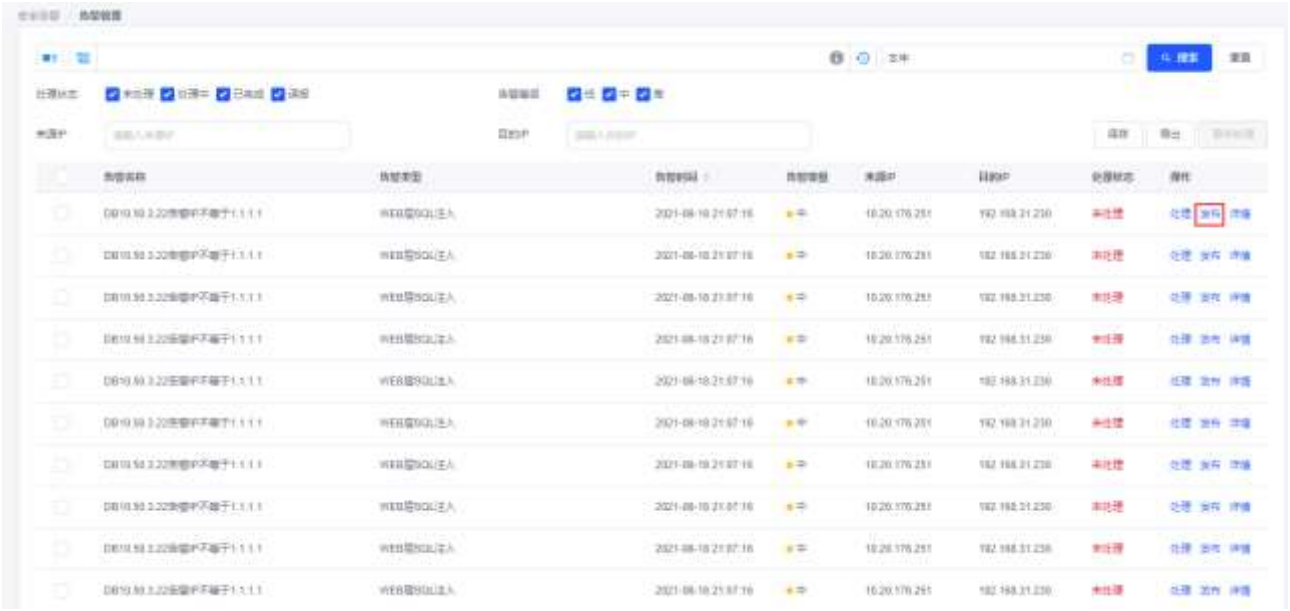
7.1.3 批量处理告警信息

选中需要处理的业务建模，点击<**批量处理**>，弹出**修改处理状态**对话框，设置处理状态，可以对事件进行处理。点击<**确定**>，可以批量处理告警事件。



7.1.4 发布工单

步骤1. 点击告警信息列表**操作**列的<**发布**>。

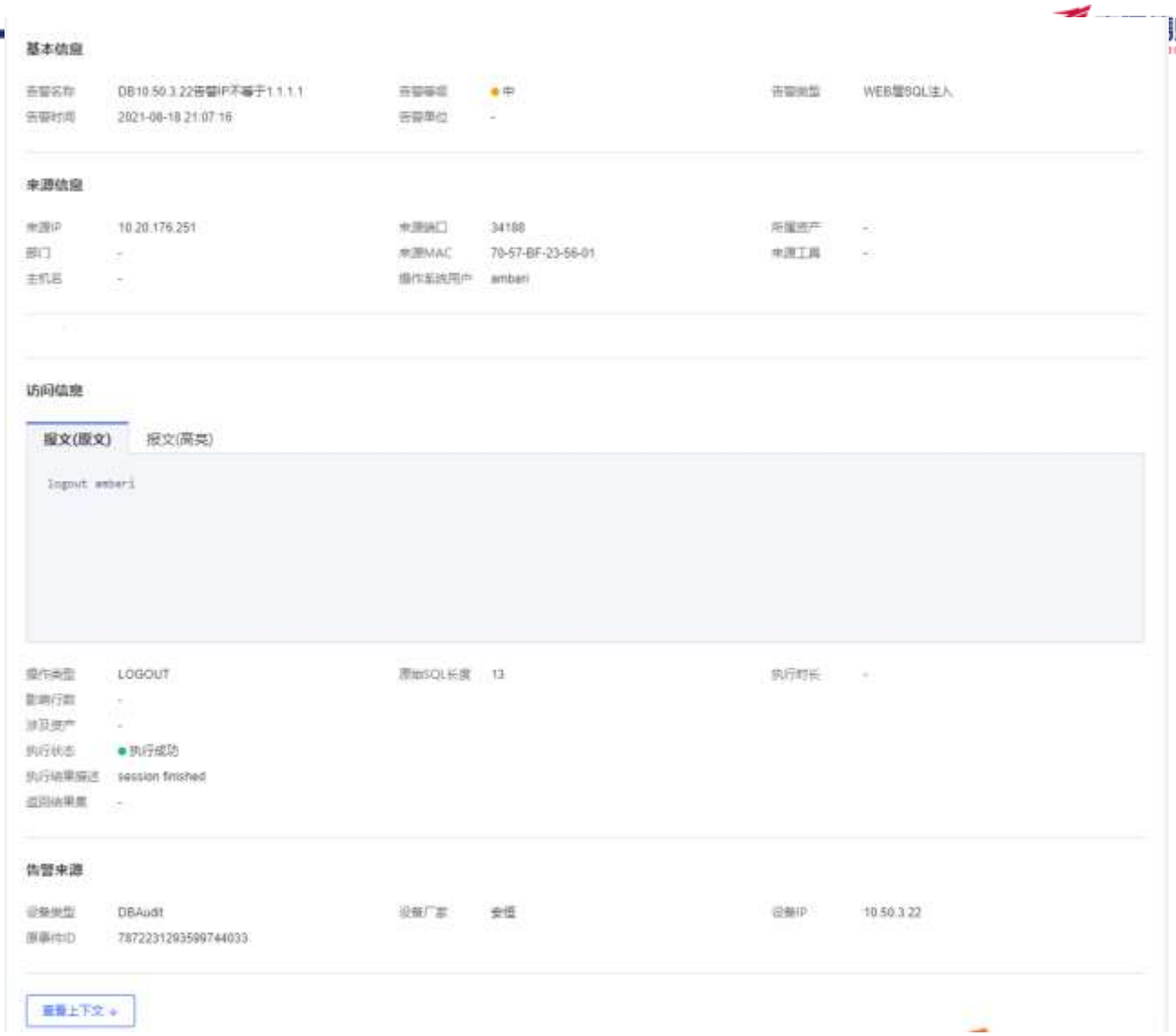


步骤2. 跳转至一键生成工单页面，填写工单主题、受理部门以及受理人等信息，点击<**保存**>发布工单。

7.1.5 查看告警详细信息

点击告警信息列表**操作**列的<**详情**>，可以查看告警管理详细信息。

- 显示基本信息：告警名称、告警等级、告警类型、告警时间以及告警单位。
- 显示来源信息：来源 IP、来源端口、所属资产、部门、来源 MAC、来源工具、主机名以及操作系统用户。
- 显示目的信息：目的 IP、目的端口、所属资产、部门、目的 MAC、数据库类型、数据库/实例名以及数据库账号。
- 显示访问信息、告警来源以及上下文。

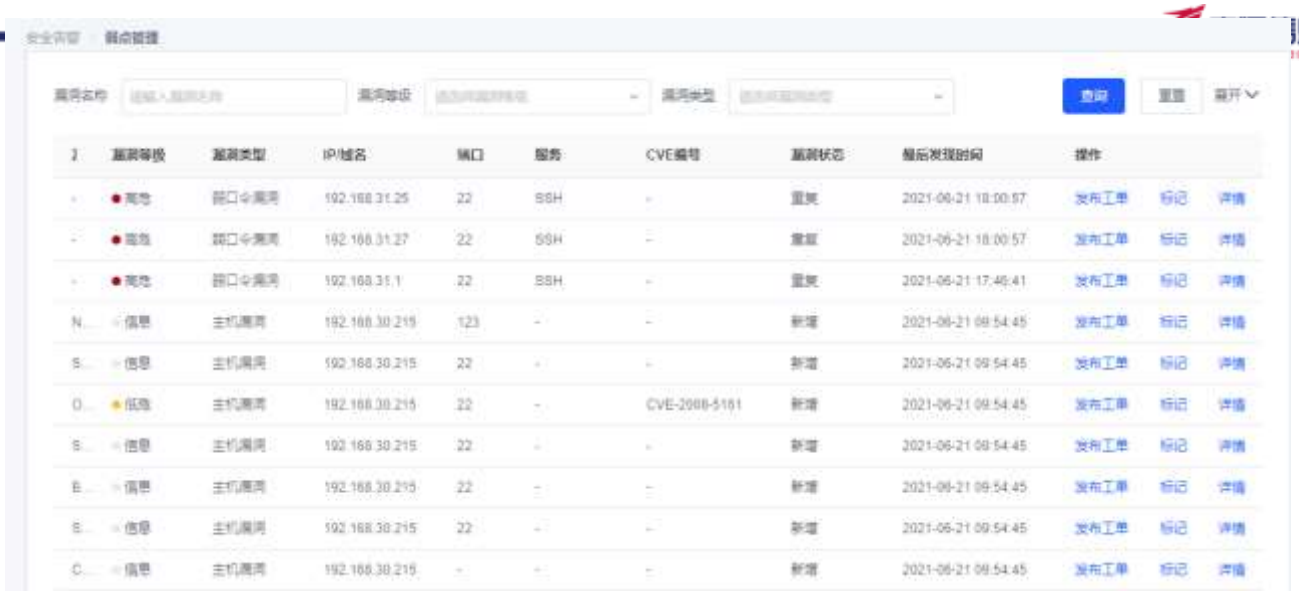


7.2 安全隐患事件

以资产和漏洞为视角，结合内部管理制度和流程，通过内置工单系统，实现资产弱点的全生命周期管理。通过弱点标准化引擎，资产对扫描器扫描发现漏洞、安全服务人工渗透漏洞、内部运维人员运维发现漏洞以及互联网公布漏洞等不同的漏洞进行统一管理。

7.2.1 查询漏洞信息

在菜单栏选择“数据告警➤**安全隐患事件**”进入**安全隐患事件**页面，设置查询条件（漏洞名称、漏洞等级、漏洞类型），点击<**查询**>即可查询相关漏洞信息。



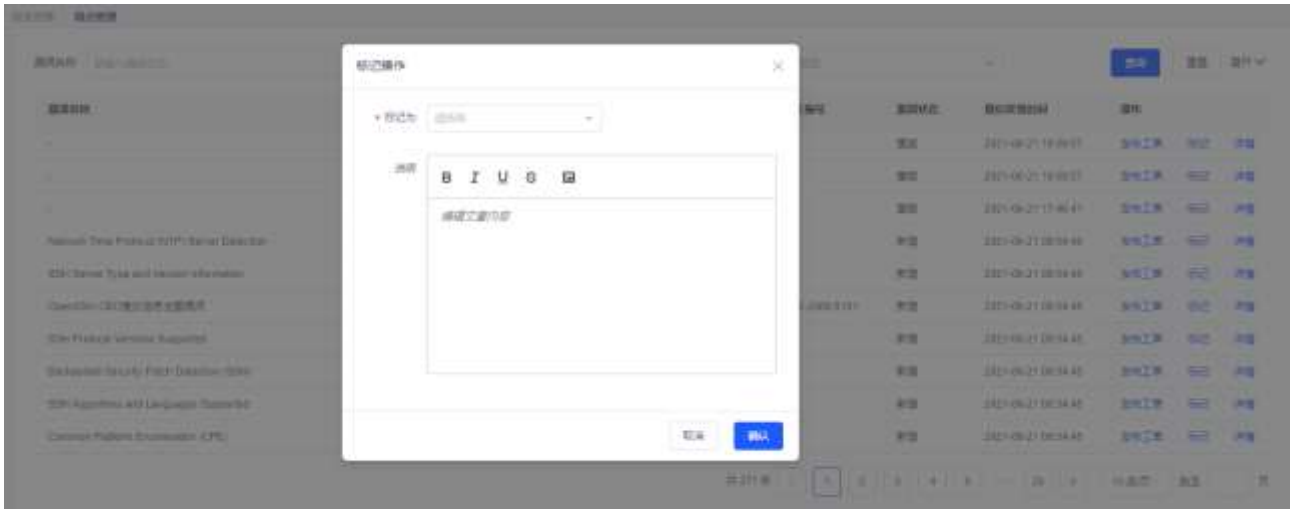
7.2.2 发布工单

步骤1. 点击告警信息列表**操作**列的<**发布工单**>。

步骤2. 跳转至一键生成工单页面，填写工单主题、受理部门、受理人、优先级、工单详情、关联风险等信息，点击<**保存**>发布工单。

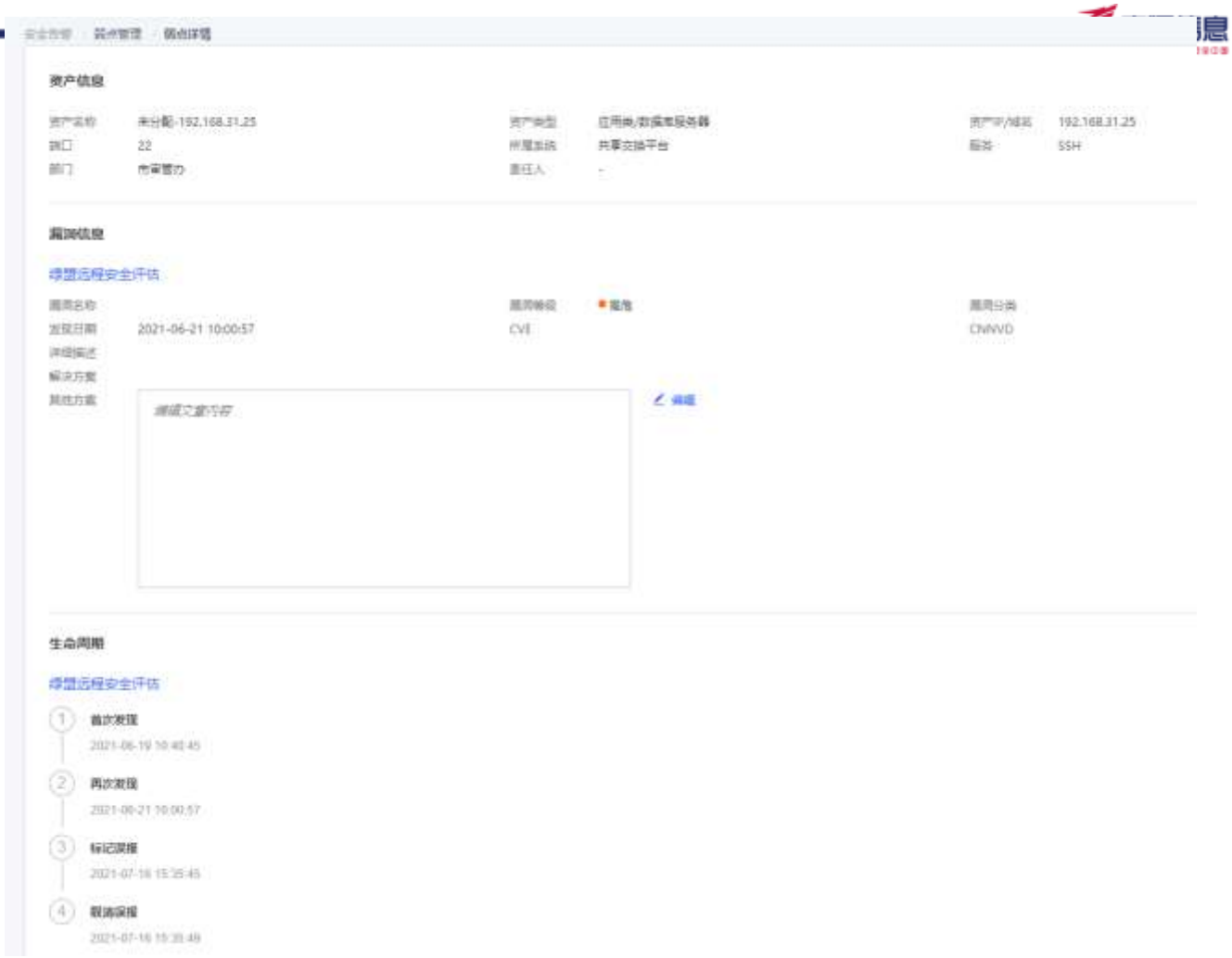
7.2.3 标记漏洞

点击告警信息列表**操作**列的<**标记**>，弹出**标记操作**对话框，选择标记状态和填写说明，点击<**确认**>，漏洞标记成功。



7.2.4 查看漏洞详细信息

点击告警信息列表**操作**列的<**详情**>，可以查看漏洞详细信息。



7.3 数据告警聚合

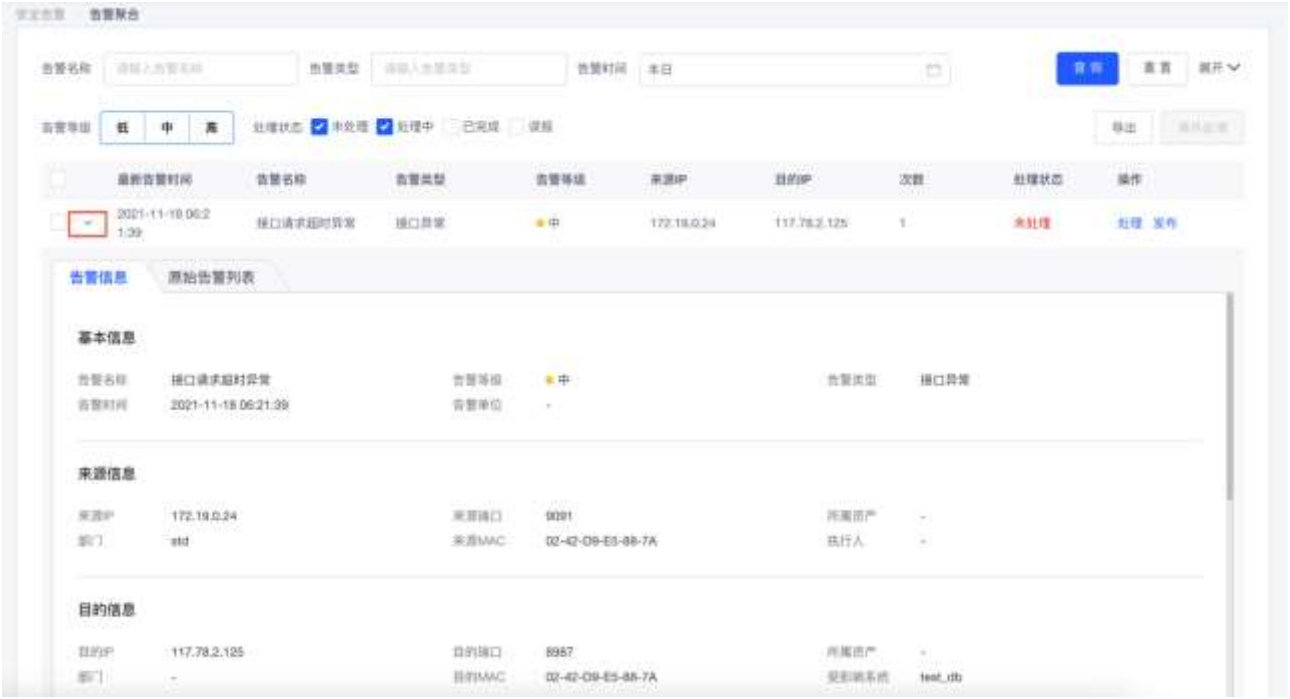
对告警名称、告警类型、来源 IP 和目的 IP 相同的重复告警事件进行聚合，并支持不同维度的查询功能。

7.3.1 查询告警信息

在菜单栏选择“**数据告警➤数据告警聚合**”进入**数据告警聚合**页面，设置查询条件（告警名称、告警时间、告警类型、告警等级、处理状态、来源 IP 以及目的 IP），点击<**搜索**>即可查询相关告警信息。

7.3.2 展开告警信息

点击“ ˅ ”图标，展开告警详细信息和原始告警列表。



7.3.3 处理告警信息

和告警管理的处理告警信息一致，详见告警管理。

7.3.4 批量处理告警信息

和告警管理的批量处理告警信息一致，详见告警管理。

7.3.5 发布工单

和告警管理的发布工单一致，详见告警管理。

8. 合规中心

针对系统资产档案可以配置合规检查任务和合规自查任务，并且可以制定对应的检查标准，同时针对各地下发的政策形成系统的知识库。

8.1 检查总览

检查总览统计分析了所有检查的整体情况，主要包括了不同状态（已结束、进行中、未开始）的检查数量统计；已结束的检查任务的完成率以及检查任务完成率的排名情况；各项检查任务的得分情况包括了排在前五的部门自评得分和审核得分情况。

8.2 合规检查

平台内置数据安全检查模版和检查要求，可自行配置形成数据安全检查表，下发至各级部门（子平台），并支持在平台完成检查项确认和材料上传，形成检查一体化、标准化和自动化。

8.2.1 查询合规检查任务

在菜单栏选择“**合规中心➤合规检查**”进入**合规检查**页面，设置查询条件（合规检查、状态），点击<**查询**>即可查询相关合规检查。

8.2.2 新增合规检查任务

步骤1. 在菜单栏选择“**合规中心➤合规检查**”进入**合规检查**页面，点击<**新增**>。

步骤2. 填写合规检查名称以及备注信息，选择检查标准、检查时间以及被检单位，点击<**保存**>。

详细配置请参见下表。

配置项	说明
合规检查	填写此次合规检查的任务名称。
检查标准	选择此次合规检查的检查标准，有关检查标准的详细信息请参考检查标准。
检查类型	选择此次合规检查的检查类型是部门和系统。选择系统是检查该部门下所有的系统。
检查方式	选择检查的方式，包括合规检查和现场检查两种。
检查时间	选择此次合规检查的开始时间和结束时间。
被检单位	选择此次合规检查的被检单位，有关被检单位的详细信息请参考部门管理。
备注	填写此次合规检查的备注信息。

8.2.3 审核合规检查

在检查列表操作列点击<**审核**>，可以审核被检查部门的上传的自查情况，并为其评分。

8.2.4 查看检查详细信息

在检查列表操作列点击<**查看**>，可以查看被检查部门的任务执行情况、得分情况以及提交时间情况。

点击<**下载全部**>可以将各部门详细执行情况信息以 zip 压缩包的形式导出至本地。

点击对应部门操作列下的<**查看**>，可以查看该部门的任务执行情况，针对组织建设、管理制度、应急管理、风险评估及等级测评、安全技术检查、服务外包检查六个部门中的详细检查内容进行评分和填写备注信息和佐证。

点击对应部门操作列下的<**下载**>，可以以 zip 格式下载该部门的任务执行信息至本地。

8.2.5 现场检查

步骤 1. 在**合规检查**页面，点击<检查>按钮。

步骤 2. 进入到检查页面，再点击<检查>按钮，主管单位对被检查单位进行现场检查。

8.3 合规自查

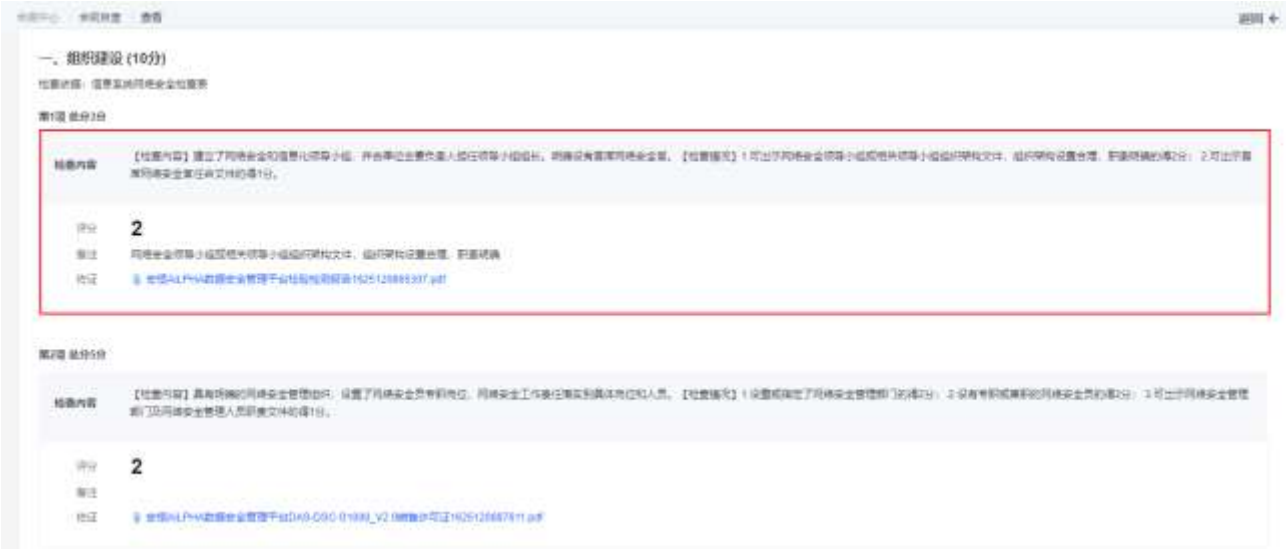
被检单位可以填写模块进行自查，填写上报信息。

8.3.1 查询合规自查任务

在菜单栏选择“**合规中心➤合规自查**”进入**合规自查**页面，设置查询条件（合规检查、状态、完成进度），点击<**查询**>即可查询相关合规自查任务。

8.3.2 查看检查详细信息

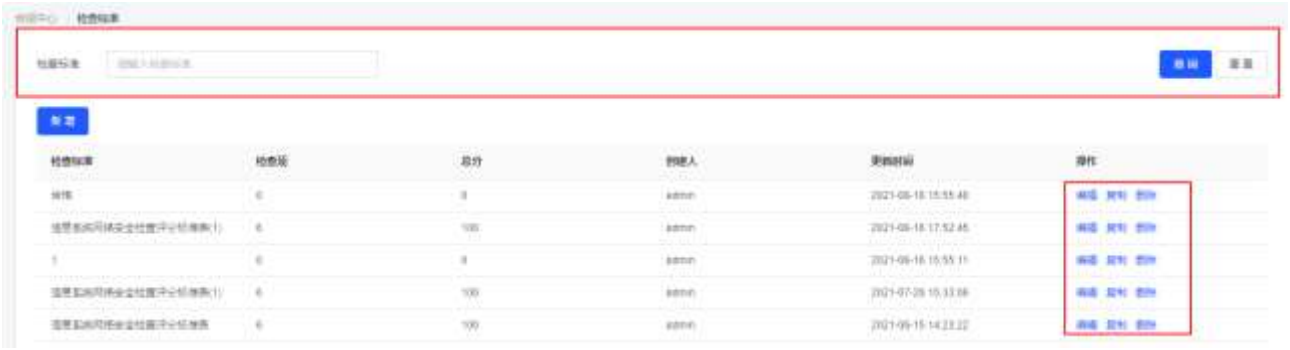
在检查列表操作列点击<**查看**>，可以查看该部门的任务执行情况，针对组织建设、管理制度、应急管理、风险评估及等级测评、安全技术检查、服务外包检查六个部门中的详细检查内容进行评分和填写备注信息和佐证，佐证以 PDF 的形式，点击文件链接可以进行下载。



8.4 检查标准

针对合规检查和合规自查任务，可以制定相应的检查标准。

- 系统支持通过检查标准进行条件查询。
- 在检查标准列表操作列点击<**编辑**>，可以对已编辑完成的信息进行修改。
- 在检查标准列表操作列点击<**复制**>，可以复制一条一样的检查标准。
- 在检查标准列表操作列点击<**删除**>，可以删除此条检查标准。

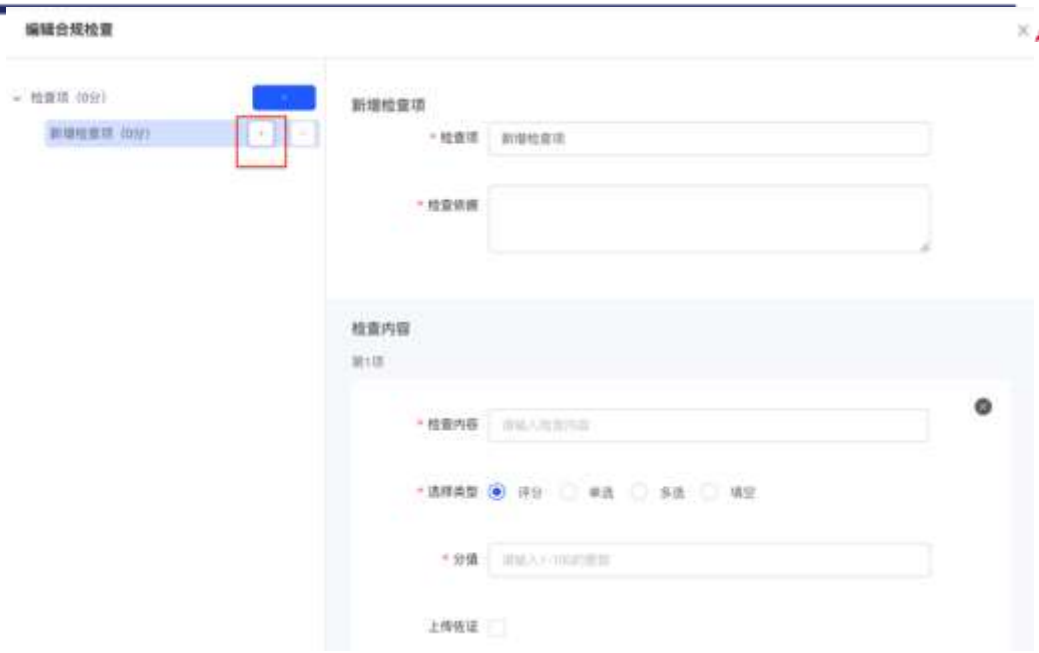


新增检查标准的操作步骤如下。

步骤1.　点击<**新增**>，进入**新增检查标准**页面，填写检查标准和检查说明，点击<**下一步**>。

步骤2.　点击“+”可以新增检查项目，填写检查项和检查依据。

步骤 3.　点击“+”可以在该检查项目下新增检查内容，支持自定义检查类型为评分、单选、多选和填空。



8.5 知识库

帮助用户建立一个安全知识库，管理和维护安全相关的标准和指导性文件等，平台支持上传、下载和在线阅读，同时支持通过文件名对进行条件查询。

在菜单栏选择“**合规中心➤知识库**”进入**知识库**页面，可以查看知识库管理的文件信息。

点击<**新建文件夹**>，填写文件夹名称，选择文件权限，上传文件，点击<**保存**>。

点击<**查看**>，查看该文件夹下所有的文件。

文件夹下的内容：

点击<**上传文件**>，填写文件名称，选择文件权限，上传文件，点击<**保存**>。

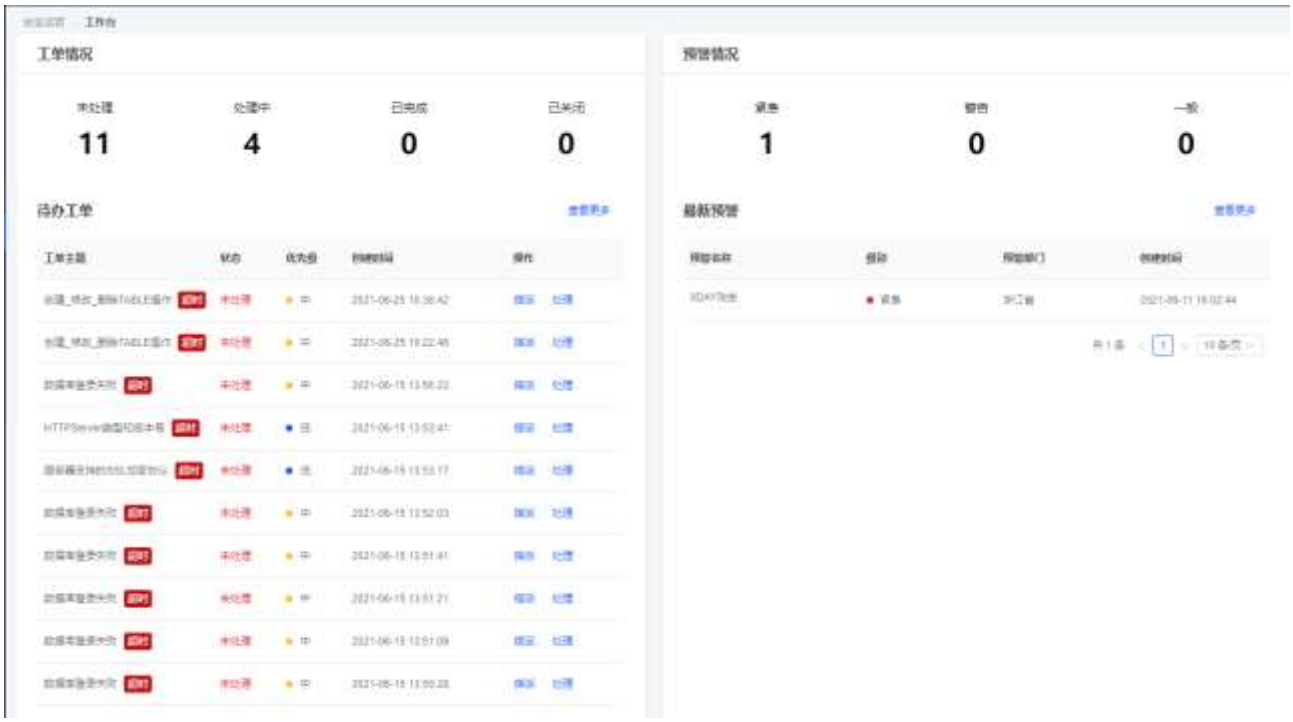
勾选文件列表前面的复选框，点击<**下载文件**>可以将文件批量导出至本地。

9. 安全运营

安全运营通过工单处理流程，将风险和预警快速安排至具体人员进行跟踪处理，形成风险闭环，并且通过通报预警功能将各单位需要注意的风险快速下发至具体单位，下级单位负责人可以快速查看存在的风险，针对风险进行快速处理，同时形成安全报告以供下载和留存。

9.1 工作台

工作台提供了工单以及预警情况快速查看和处理工单功能，主要包括工单的各状态情况统计，各级别预警单情况统计，待办工单快速处理和最新预警查看通道。



各模块说明请参见下表

模块	说明
工单情况	可以查看工单未处理、处理中、已完成以及已关闭的数量统计。
待办工单	可以查看待办工单列表详细信息，点击<**查看更多**>将跳转至处理工单和指派工单。
预警情况	可以查看预警状态为紧急、警告和一般的任务情况，点击<**查看更多**>将跳转至预警管理。
最新预警	可以查看最新预警信息，可以快速进行处置。

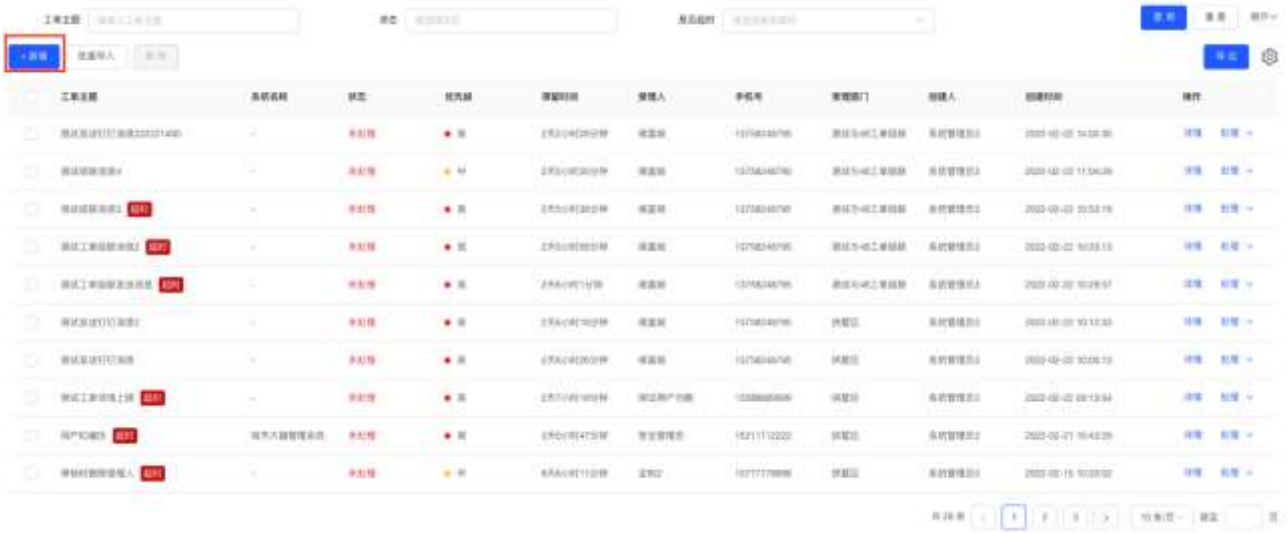
9.2 工单管理

平台可通过工单处理流程，将风险快速安排具体人员进行跟踪处理，实现责任到人，形成风险闭环。

9.2.1 一键生成工单

支持对风险事件（安全告警、弱点管理）一键生成工单，使其进入工单处理流程，同时支持通过工单名称、状态以及优先级进行条件查询。

步骤1. 在菜单栏选择“**安全运营➤工单管理**”进入**工单管理**页面，点击<**新增**>。



步骤2. 进入**新建工单**页面，填写基本信息以及关联风险，点击<**保存**>。

详细配置请参见下表

配置项	说明
工单主题	填写工单主题。
受理部门	选择工单受理部门，有关受理部门的详细请参考部门管理。
受理人	选择工单受理人。
抄送人	选择工单抄送人。

配置项	说明
优先级	选择工单处理优先级。
工单类型	选择工单的类型。
工单类型明细	先选择工单的类型，再选择具体的工单类型明细。
对象	输入工单处理对象。
咨询人姓名	填写咨询人姓名。
咨询人手机号	填写咨询人手机号码。
工单详情	填写工单详细信息，可以通过点击<**附件上传**>进行上传。
标签	通过点击标签对公单进行分类。
超时日期	选择工单处理的截止日期。
关联风险	选择工单类型和唯一 ID 进行绑定，关联风险。点击<**添加**>可以新增关联信息。

9.2.2 查看工单详细信息

在工单列表**操作**列点击<**详情**>，可以查看工单详细信息。

9.2.3 处理工单

从“未处理-处理中-已完成-已关闭”，可对所有工单状态进行跟踪处理，实现责任到人，形成风险闭环。

步骤1. 在工单列表**操作**列点击<**处理**>或者在工单详细信息页面点击<**处理**>，弹出**确认开始处理工单**对话框，可以对工单进行处理。

步骤2. 若状态显示为“处理中”，填写处理备注信息，点击操作列中的<**完成**>可以完成对表单的处理流程。

步骤3. 若状态显示为“已完成”，填写关闭备注信息，点击操作列中的<**关闭**>可以关闭表单流程，完成风险闭环。

9.2.4 指派工单

在工单列表**操作**列点击<**指派**>或者在工单详细信息页面点击<**指派**>，可以将工单指派给其他工单管理人，填写工单信息，详情请参考一键生成工单。填写完成后，工单将指派给需要处理的管理人。

9.2.5 备注

在工单详情页面点击<备注>，可以对该工单进行备注。

9.3 预警管理

通过通报预警功能将各单位需要注意的风险快速下发到具体的单位，同时系统支持通过预警名称、级别以及所属部门进行条件查询。

9.3.1 新增通报预警任务

步骤1. 在菜单栏选择“**安全运营➤预警管理**”进入**预警管理**页面，点击<**新增**>。

步骤2. 进入**新增预警**页面，填写预警名称以及预警详情，选择预警级别和预警范围，点击<**保存**>可以保存配置信息，点击<**保存并发布**>可以保存并发布配置信息。

详细配置请参见下表

配置项	说明
预警名称	填写预警任务名称。
预警级别	选择预警任务级别。
预警范围	选择预警任务的执行范围，详情请参见部门管理。
预警详情	填写预警详细信息，支持通过上传附近形式。

9.3.2 查看任务详情

在预警任务列表**操作**列点击<**详情**>，可以查看预警任务详细信息，点击<**下载**>，可以将信息导出至本地。

9.4 安全报告

主要用于生成综合性数据安全评估报表，提供 Word 格式下载功能。

在菜单栏选择“**安全运营➤安全报告**”进入**安全报告**页面，可以查看数据安全管控评估报告，同时系统支持通过所属部门和时间范围进行查询安全报告。

- 点击<**订阅**>，将跳转至报告订阅页面，报告将以订阅策略的设置进行触发。
- 点击<**导出**>，可以以 Word 格式将安全报告导出至本地。

9.5 报告订阅

针对安全报告，可以制定相应的策略，定时（如日报、周报、月报）自动发送至收件者邮箱内。

使用前需要配置邮件服务器地址，详细信息请参考邮件服务器配置，否则会发送失败。

步骤1. 在菜单栏选择“**安全运营➤报告订阅**”进入**报告订阅**页面，点击<**新增**>。

步骤2. 填写任务名称、收件人邮箱、报表类型、报表格式，选择部门、任务周期以及发送时间，点击<**保存**>。

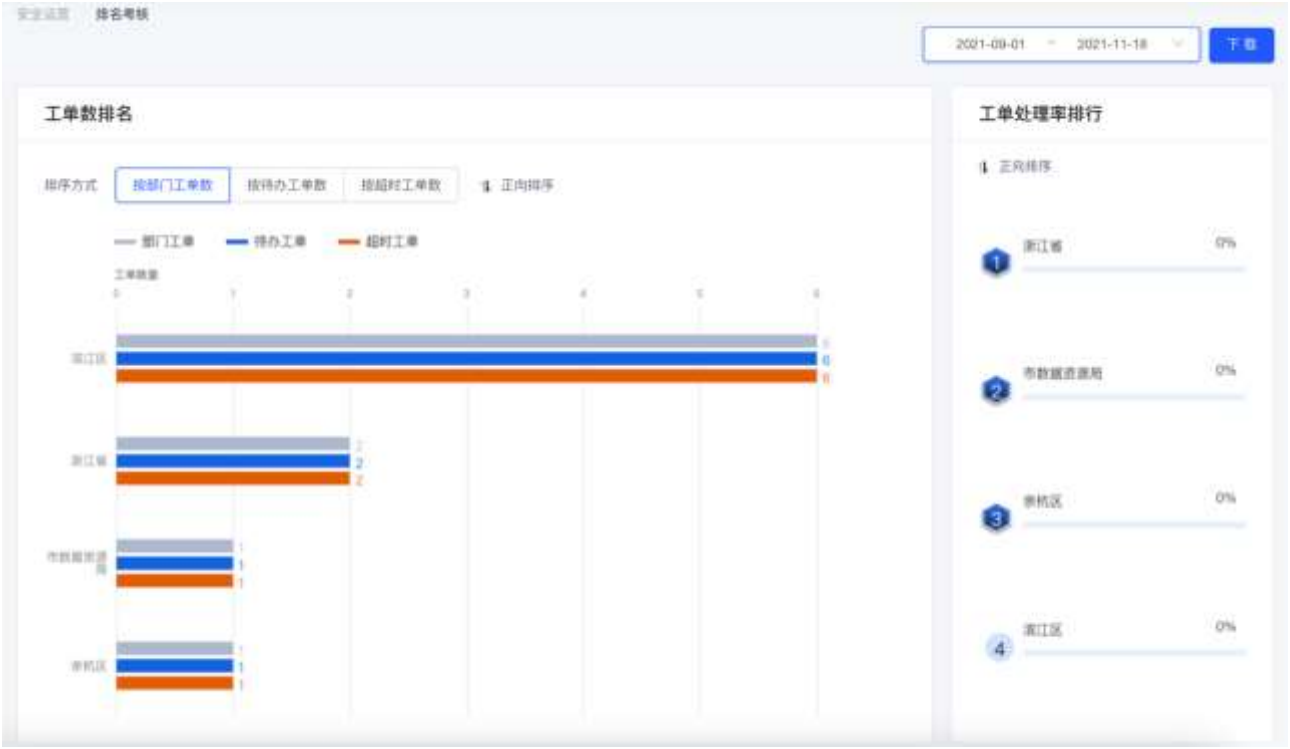
详细配置请参见下表。

配置项	说明
任务名称	填写订阅任务名称。

配置项	说明
收件人邮箱	填写收件人邮箱地址。
报表类型	选择订阅任务报表类型。
报表格式	报告将以 Word 格式保存至系统内，同时可以将报告导出至本地。
部门	选择订阅任务的所属部门。
任务周期	系统支持每天（日报）、每周（周报）、每月（月报）以及每年（年报）。
发送时间	选择报告发送时间，报告将按照固定时间发送至收件人邮箱。

9.6 排名考核

对各部门进行统计排名，主要包括统计按部门排名的工单总数、待办工单数、超时工单数、工单处理率等排名情况。

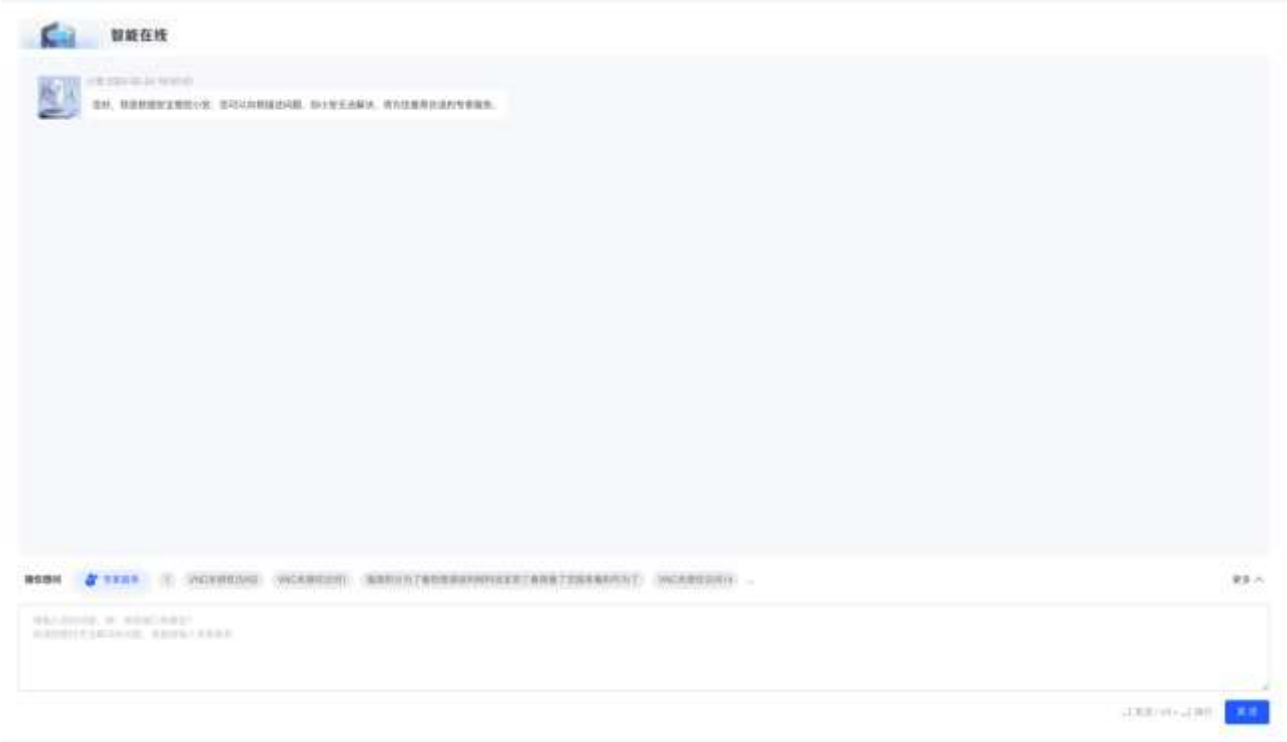


10. 专家服务

专家服务模块提供智能在线和问题库功能，方便用户快速查询常见问题，并给予相应的修复建议。

10.1 智能在线

系统提供智能在线服务，对用户遇到的问题可为其自动匹配其答案，给予链接跳转到问题解决的详情页。倘若匹配不到的，可为其推荐云端专家，并提供专家的手机号、浙政钉号，方便用户向专家直接提问。另外用户可以直接在工单详情页面点击专家服务按钮跳转到智能在线模块，使得专家能够快速了解工单相关的信息并对其对症下药。



10.2 问题库

系统支持批量导入、新增、编辑的方式更新和维护问题库中的常见问题，对所有的问题和答案按照问题漏洞的类型进行分类，确保用户们在常见问题页面可以快速获取信息。

10.2.1 查询问题

系统支持对问题名称、问题分类、标签进行查询。

10.2.2 新增问题

步骤 1. 在菜单栏选择“**专家服务➤问题库**”进入**问题库**页面，点击<**新增**>。

步骤 2. 进入**新增问题库**页面，填写**问题**相关信息，点击<**保存**>。

详细配置请参见下表。

配置项	说明
问题名称	填写问题名称。
问题分类	选择问题的分类。
问题描述	填写该项问题的描述。
修复建议	填写该项问题的修复建议。
备注	填写该项问题的备注。
标签	选择该项问题所属标签，点击<**新增标签**>可以自定义增加标签类型。

10.2.3 导入问题

系统支持批量导入问题。

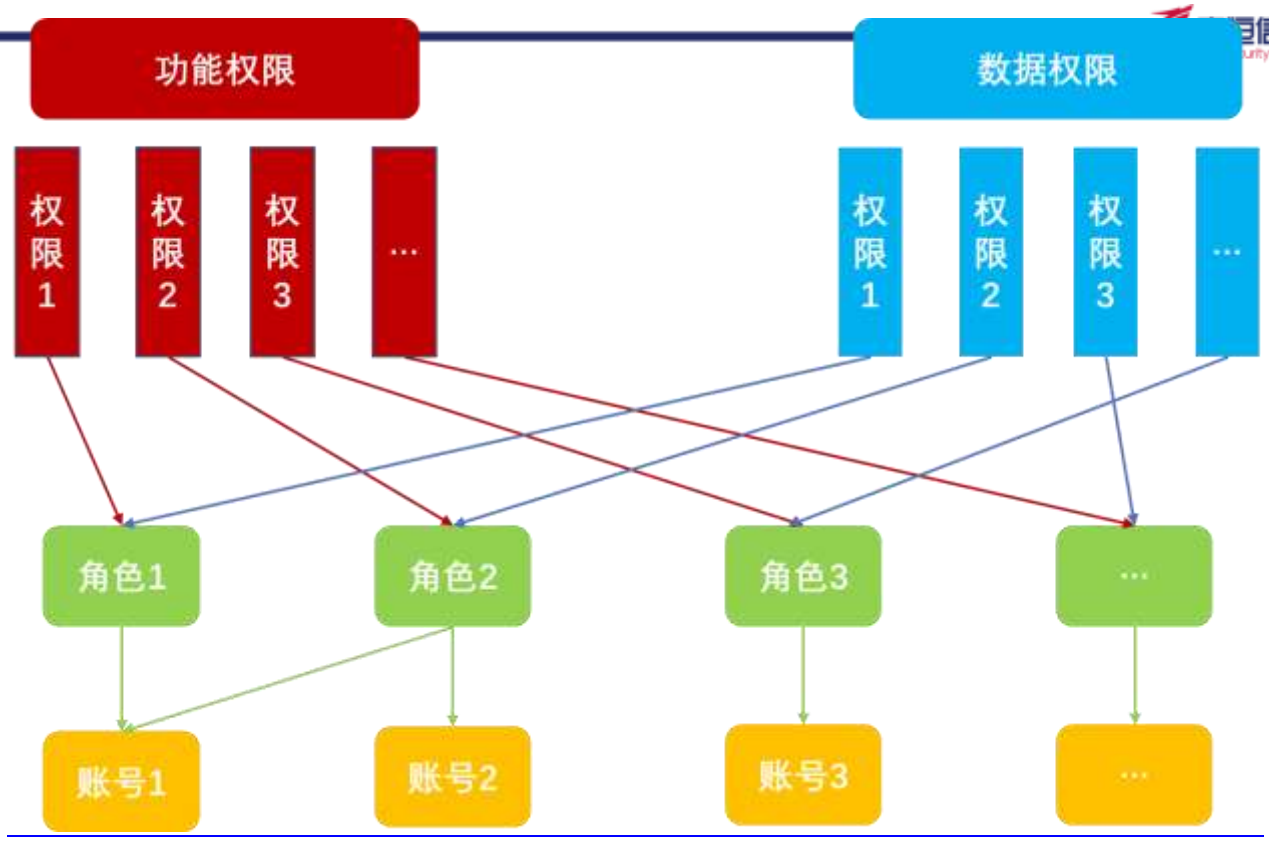
步骤 1. 在**问题库**页面，点击<**批量导入**>，再点击<**模板下载**>，模板将以 xlsx 格式导出至本地，根据模板格式进行填写。

步骤 2. 继续点击<**点击上传**>将填写完成的模板拖拽或上传。

10.2.4 查看问题详情

11. 用户中心

平台提供细粒度的权限分配和控制，分为功能权限管理和数据权限管理。除了功能菜单权限分配和授权给角色外，数据权限同样具备权限的分配和授权。不同的单位组角色的用户只能看到赋予给该单位组的数据，包括网络基础资产清单、数据资产、业务场景拓扑、告警信息、预警和工单等等。



11.1 用户管理

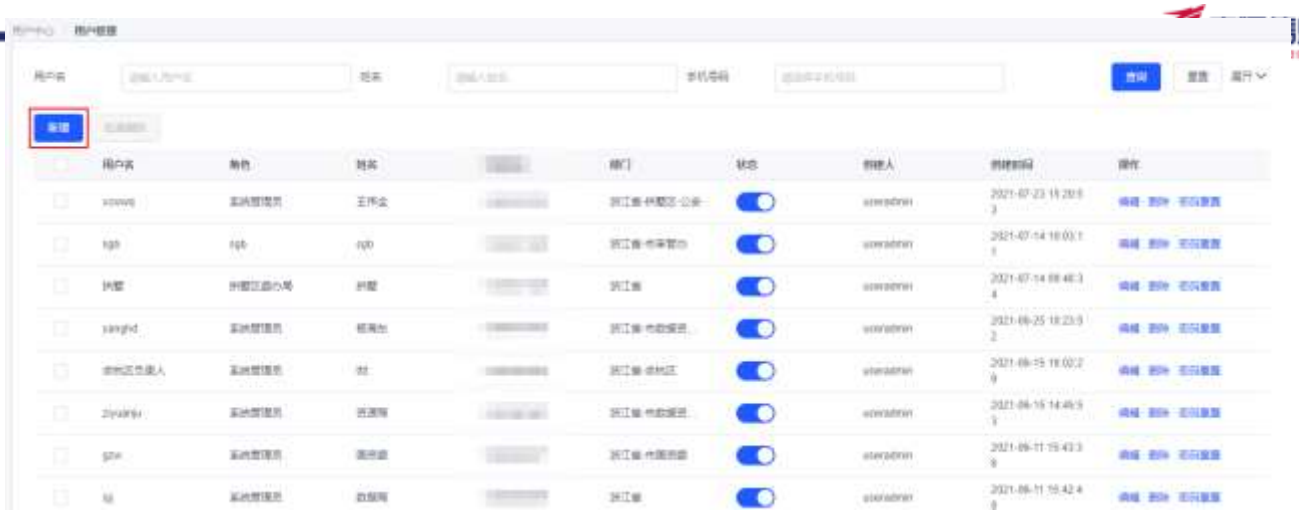
用户是系统中的一项重要资源，用户必须隶属于部门，不同部门之间的资源是隔离的（如部门 A 的用户只能对部门 A 中具有权限的资产进行管理），因此在创建用户前必须创建部门，有关部门管理的操作请参考部门管理。

11.1.1 查询用户

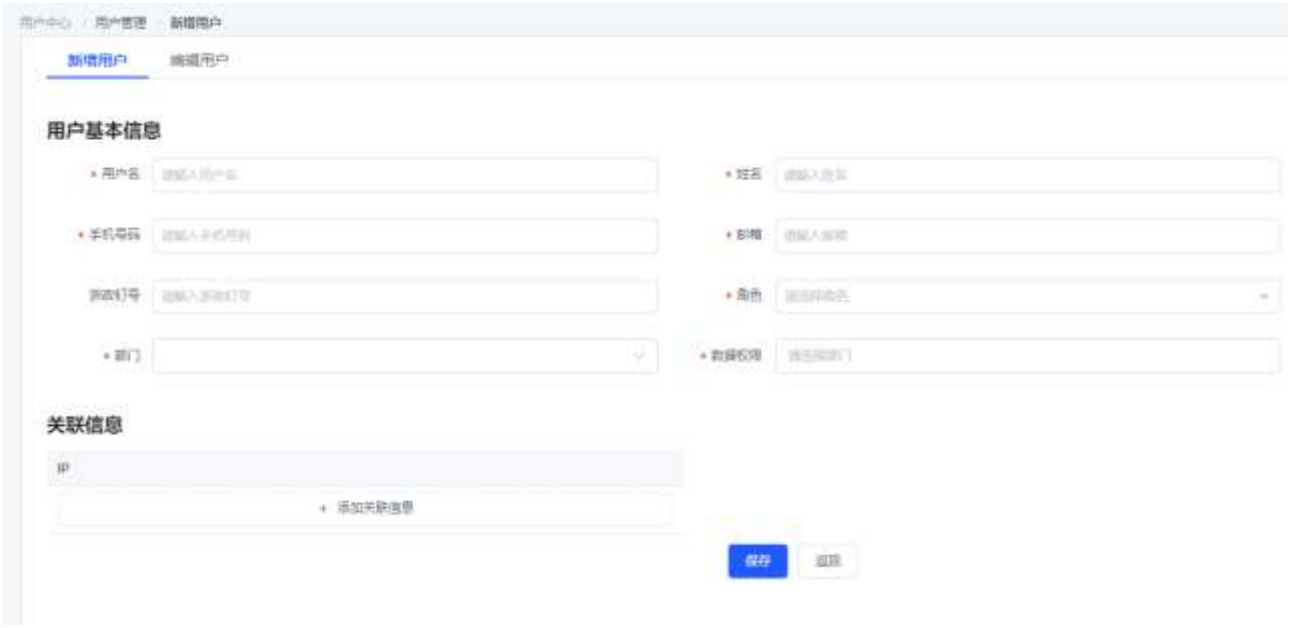
系统支持通过用户名、姓名以及手机号码进行条件查询。

11.1.2 新增用户

步骤1. 在菜单栏选择“**用户中心➤用户管理**”进入**用户管理**页面，点击<**新增**>。



步骤2.　进入**新增用户**页面，填写用户基本信息和关联信息，点击<**保存**>。



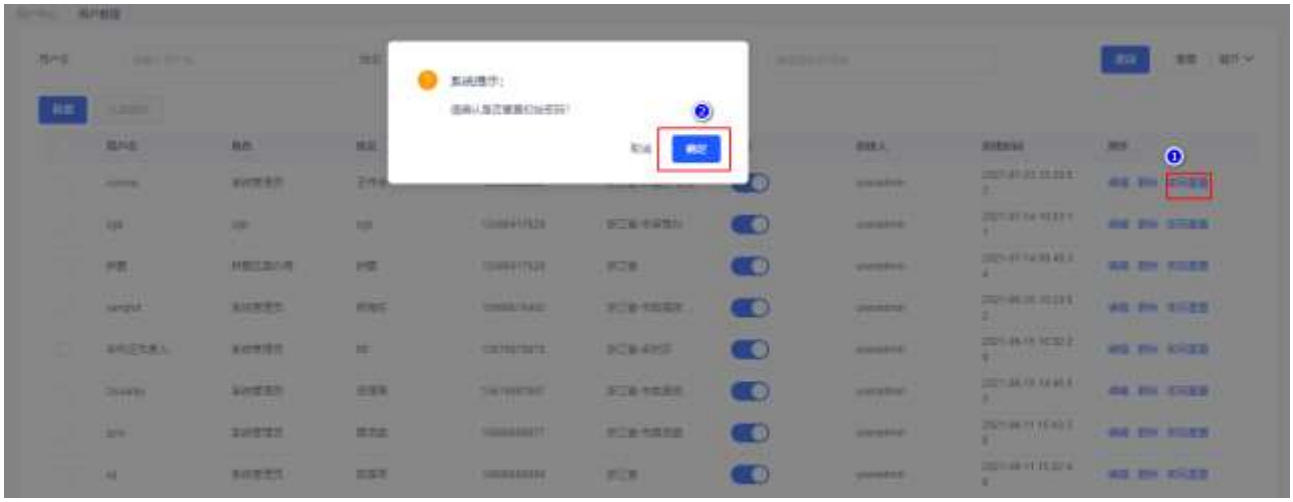
详细配置请参见下表

配置项	说明
用户基本信息	
用户名	填写用户名称。
姓名	填写新增用户真实姓名。
手机号码	填写用户手机号码。
邮箱	填写用户邮箱地址。
浙政钉号	全省统一的政府系统掌上协同办公平台的钉钉号。
角色	选择新增用户的系统角色。

配置项	说明
用户基本信息	
部门	选择新增用户的部门，有关部门管理相关信息请参考部门管理。
数据权限	选择新增用户的数据权限。
关联信息	
IP	填写 IP 地址与账号进行关联。

11.1.3 密码重置

在用户列表**操作**列点击<**密码重置**>，弹出**请确认是否重置初始密码**对话框，点击<**确定**>，重置用户密码为随机密码。用户可以复制密码，重新登录后同样也可以重新设置密码。



11.1.4 解锁用户

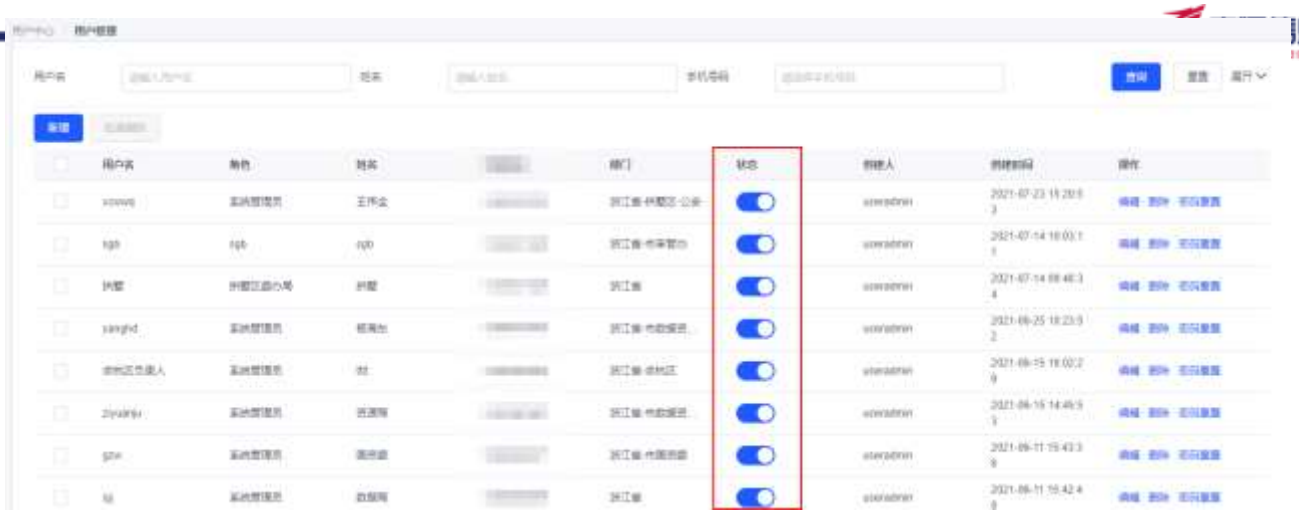
当用户被安全策略（有关安全配置详细信息请参考**错误!未找到引用源。**）锁定用户时，登录提示“您的账号已被安全锁定，请联系系统管理员!”

在用户列表**操作**列中，系统管理员点<**解锁**>，弹出**请确认是否解锁用户**对话框，点击<**确定**>，解锁用户。

11.1.5 启用/禁用状态

启用状态时，点击可切换成禁用状态，禁用状态下，用户无法登录。

禁用状态时，点击可切换成启用状态，启用状态下，用户可登录。



11.2 角色管理

新增角色操作步骤如下。

步骤1. 在菜单栏选择“**用户中心➤角色管理**”进入**角色管理**页面，点击<**新增**>。

步骤2. 进入**新增角色**页面，填写角色名称以及勾选功能权限，同时填写角色描述，点击<**保存**>。

11.3 安全配置

在菜单栏选择“**用户中心➤安全配置**”进入**安全配置**页面，配置用户安全设置、用户锁定设置以及密码策略，点击〈**保存**〉。

各模块说明请参见下表。

模块	说明
用户安全设置	
登录超时	设置用户登录超时时间，当用户超过设定值时长无操作时，再次操作需要重新登录系统。取值范围为 1~43200 分钟，默认值是 5 分钟，可根据需要进行设置。
验证码	勾选启用数字验证码，当用户登录时，将生成数字验证码，用户需要填写正确方可进入系统。
IP 验证	启用 IP 验证功能，当用户登录时，需要进行 IP 验证。若不正确，将不能进入系统。
登录方式	默认勾选 IDaaS，主要用于统一身份认证和多因子强认证。
用户锁定	
密码尝试次数	设置用户登录系统尝试密码次数，若超过设置时，用户将被锁定，需要系统管理员进行解锁。有效值是 0~999 次，默认值是 5，若不设置为 0，则不锁定用户。
锁定时长	设置用户登录系统被锁定后的锁定时间。有效值是 0~10080 分钟，默认值是 30。
重置计数器	登录尝试密码失败之后，将登录尝试失败计数器重置为 0 次所需要的时间。有效值是 0~10080 分钟，默认值是 5。
密码策略	
密码强度	设置强密码时，8-64 个可见字符，必须包含以下 4 项：1、大写字母 A-Z；2、小写字母 a-z；3、数字 0-9；4、非字母符号如@,#,$。 设置中密码时，8-64 个可见字符，必须包含以下 2 项：1、大写字母 A-Z；2、小写字母 a-z；3.数字 0-9；4、非字母符号如@,#,$。

模块	说明
密码使用期限	设置密码使用期限。有效值是 0~999 天，默认值是 0。如果设置为 0，则密码不过期。

12. 规则模型

规则模型是指系统提供通用的告警规则引擎，安全运营人员可以在其基础上根据现场的风控场景来自定义规则。

12.1 查询规则

支持通过规则名称、风险等级、规则分类、规则分组、规则类型和规则标签条件过滤查询。

12.2 新增规则

步骤 1. 在规则管理页面，点击<新增>，新增规则。

步骤 2. 进入新增规则页面，填写规则名称等相关信息，点击<保存>。

详细配置请参见下表。

配置项	说明
规则名称	填写需要添加的规则名称。
规则分类	选择规则的类型。
风险等级	选择风险等级。
规则分组	选择规则分组。
规则说明	填写规则的说明。
策略状态	勾选策略的状态。
标签	选择该规则所属标签，点击<**新增标签**>可以自定义增加标签类型。

可以通过以下步骤自定义添加匹配规则、抽取规则、统计规则、判断规则。

步骤 1. 添加匹配规则

【1】下拉单项选择，支持函数：strequ、strnotequ、strstr、strnotstr、strregex、strlength、strinclude

函数名	参数	说明
strequ	2 个(string1,string2)	判断两个字符串是否完全相等
strnotequ	2 个(string1,string2)	判断两个字符串是否不相等 （一般用于某个规则对少数网站有误报）
strstr	2 个(string1,string2)	判断 string1 是否含有第 string2
strnotstr	2 个(string1,string2)	判断 string1 是否不含有第 string2(一般用于某个规则对少数网站有误报)
strregex	2 个(string1,string2)	判断 string1 是否含有第 string2(Google RE2 正则匹配)
strlength	3 个(string1,int1,int2)	判断 string1 的长度与 int1 的关系,int2 表示大于小于的匹配模式,string1 为 key 取的是 key 对应的 value 的长度 int2 =1 代表大于 =0 代表小于
strinclude	2 个(string1,string2)	判断 string2 是否含有 string1 如果规则 string1 设计是固定字段，则需要这条规则，如果不固定则无需（建议参考 beaver，固定）
支持&&和||逻辑		

【2】 参数 1，选择匹配字段

【3】 参数 2，输入匹配值

【4】 参数 3，strlength 的 int2， int2 =1 代表大于，int2 =0 代表小于

【5】 操作：⊕：加一行；⊖：删除这行；⊙：上移一行；⊙：下移一行

步骤 2: 添加抽取规则

基础功能	
函数	**说明**
attr(string1,string2,string3) => string4	**string1** 的取值支持字段 **string2** 定义待取值的 key 值，若为【re】模式，则为对应的正则表达式 **string3** 定义 string1 解析模式，当前支持： • json • xml • k-v（支持分号和&符号） • re **string4** 定义将抽取到的值赋值给变量,变量名为string4 规则举例： attr(postdata,'(?<phone>\d+)', re) => phone
多条规则间使用【;】进行分隔，抽取出来的数据最后封装成 JSON，之后通过 MQ 传递到下一个节点	

步骤 3. 添加统计规则

【1】参数 1：时间间隔，hour：24 小时

【2】参数 2：下拉单选框，时间间隔粒度，可取值如下：

- hour
- minute

【3】参数 3：函数，下拉单项选择，支持函数：groupby、groupbycount、groupbysum、count、distinct、nop

【4】参数：groupby、groupbycount、groupbysum，下拉多项选择；count、distinct，下拉单项选择；nop，

无

【5】参数：用户变量，将结果赋值为一个字段

统计完成后，将统计结果通过 MQ 发送给其他引擎进行处理

步骤 4. 添加判断规则

用于对接收到的 MQ 消息进行数值&逻辑判断，判断结果通过 MQ 发送给对应的 APP（攻击事件产出）

【1】函数，下拉单项选择，支持函数：stdev、cycle_stat

项目	举例	备注
stdev	stdev(string1, string2, string3...)	计算标准差
cycle_stat	cycle_stat(string1, int1, string2)	统计指定时间间隔内的数据 string1：待统计数据的变量名 int1：时间间隔 string2：时间间隔粒度，可取值如下： • hour • minute
自定义	随便填	

stdev 函数：

【2】参数 1：下拉多选框，可选择内置变量、用户变量（前一个规则定义的）、全局变量

【3】参数 2：逻辑判断：> 、>= 、<、 <=、==

【4】参数 3：数字

cycle_stat 函数：

【2】参数 1：下拉单选框，可选择内置变量、用户变量（前一个规则定义的）、全局变量

【3】参数 2：时间间隔

【4】参数 3：下拉单选框，时间间隔粒度，可取值如下：hour、minute

【5】参数 4：逻辑判断：> 、>= 、<、 <=、==

【6】参数 5：数字

12.3 查看规则

在规则管理页面，点击<查看>按钮查看规则详情。

详情：

12.4 上/下线规则

点击<下线>，该规则将处于禁用状态，且该状态下，可进行编辑、测试和删除。

12.5 测试规则

在规则列表页，点击<测试>，可对规则进行测试。

13. 系统管理

系统管理是指系统管理员对系统运行参数进行设置，以及对资源进行维护，使系统更好地适配实际业务场景。系统管理主要包括探针管理、推送管理、系统配置、数据字典、系统告警以及菜单配置六个部分。

13.1 探针管理

对与本平台存在数据交互的子探针进行管理。系统支持与明御数据库审计与风险控制系统、明御综合日志审计平台、外网流量探针 AiNTA、AiLPHA 资产弱点管理平台、数据安全分级与风险评估系统以及数据安全管控平台共 6 个。

13.1.1 新增探针

步骤3. 在菜单栏选择“**系统管理➤探针管理**”进入**探针管理**页面，点击<**新增**>。

步骤4. 填写探针名称、探针 IP 地址以及探针端口，选择探针厂家和探针类型，点击<**保存**>。

详细配置请参见下表

配置项	说明
探针名称	填写新增探针名称。
探针厂家	选择探针所属厂家，目前仅支持安恒信息一个。
探针类型	选择探针类型，系统支持明御数据库审计与风险控制系统、明御综合日志审计平台、外网流量探针 AiNTA、AiLPHA 资产弱点管理平台、数据安全分级与风险评估系统以及数据安全管控平台共 6 个。
探针 IP/端口	填写探针 IP 地址/端口。

13.1.2 编辑探针

系统支持对已增加的探针进行修改信息。

步骤1. 在探针列表操作项点击<**编辑**>。

步骤2. 进入**编辑探针**页面，修改探针名称等信息，点击<**保存**>。

13.1.3 删除探针

系统支持删除已增加的探针。

在探针列表操作项点击<**删除**>，弹出**是否确认删除**对话框，点击<**确定**>。

13.1.4 查询探针

系统支持通过探针名称、探针 IP、探针类型以及状态对探针进行条件查询。

13.1.5 查看探针

在探针列表操作项点击<**详情**>，可以查看系统信息（包括 CPU、内存以及数据磁盘等）以及探针信息。

13.1.6 同步探针

在探针列表操作项点击<**同步**>，弹出**是否确认同步**对话框，点击<**确定**>。

13.2 推送管理

推送管理是指对与平台对接的邮件服务器、短信服务器以及钉钉服务器进行配置，及时发送推送消息。

13.2.1 邮件服务器配置

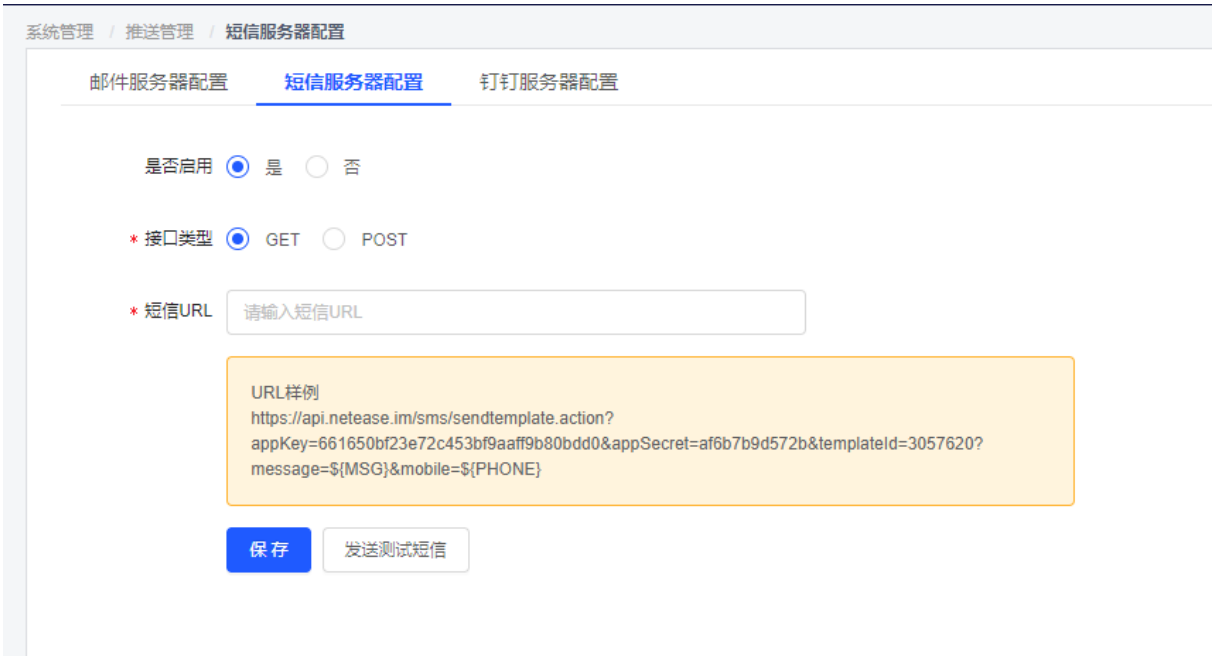
在菜单栏选择“**系统管理➤推送管理**”进入**推送管理**页面，选择**邮件服务器配置**页签，配置邮件服务器相关信息。点击<**发送测试邮箱**>可以与邮箱进行连通性测试，点击<**保存**>对已配置完成的信息进行保存。

详细配置请参见下表

配置项	说明
是否启用	选择是否启用邮件服务器。
邮件服务器	配置邮件服务器的地址，建议使用域名形式。
端口	配置邮件服务器的端口。
加密方式	可以选择不加密、SSL 以及 TLS 三种加密方式。
需要验证	选择是否需要进行验证，如果选择“否”，可以不需要输入密码。
发件箱地址	配置发送邮箱的地址。
请输入密码	如果需要验证选择“是”，则需要填写邮件服务器密码。

13.2.2 短信服务器配置

在菜单栏选择“**系统管理➤推送管理**”进入**推送管理**页面，选择**短信服务器配置**页签，配置短信服务器相关信息。点击<**发送测试短信**>可以与短信服务器进行连通性测试，点击<**保存**>对已配置完成的信息进行保存。



详细配置请参见下表

配置项	说明
是否启用	选择是否启用短信服务器。
接口类型	选择接口类型，包括 GET 和 POST 两种。
短信 URL	填写短信服务器 URL 地址。

13.2.3 钉钉服务器配置

在菜单栏选择“**系统管理➤推送管理**”进入**推送管理**页面，选择**钉钉服务器配置**页签，配置钉钉服务器相关信息。点击<**发送测试消息**>可以与钉钉服务器进行连通性测试，点击<**保存**>对已配置完成的信息进行保存。

详细配置请参见下表

配置项	说明
是否启用	选择是否启用钉钉服务器。
webhook	填写钉钉服务器 webhook 地址。

13.3 系统配置

主要用于对平台进行系统维护和管理，以适应实际应用场景。

13.3.1 网络配置

主要对默认网关、策略路由信息以及网口信息进行配置和管理。

13.3.1.1 网口配置

为了适配实际的网络环境，需要对平台进行网络配置。

在菜单栏选择“**系统管理➤系统配置**”进入**系统配置**页面，选择**网络配置**页签，点击<**编辑**>可以对网口信息进行修改。

修改网口配置后，需要使用修改后的管理 IP 地址重新登录系统 Web 管理平台。

13.3.1.2 默认网关及策略路由配置

点击<**编辑**>，系统支持对默认网关地址、DNS 服务器地址以及备选 DNS 服务器地址信息进行修改。

13.3.2 许可证

许可是安恒信息授权给用户正常使用产品功能的证书文件，在产品使用许可期限即将到期时，请及时联系安恒信息客服热线 400-059-110，向产品服务人员申请许可。

步骤1. 在菜单栏选择“**系统管理➤系统配置**”进入**系统配置**页面，选择**许可证**页签，点击<**许可延期**>。

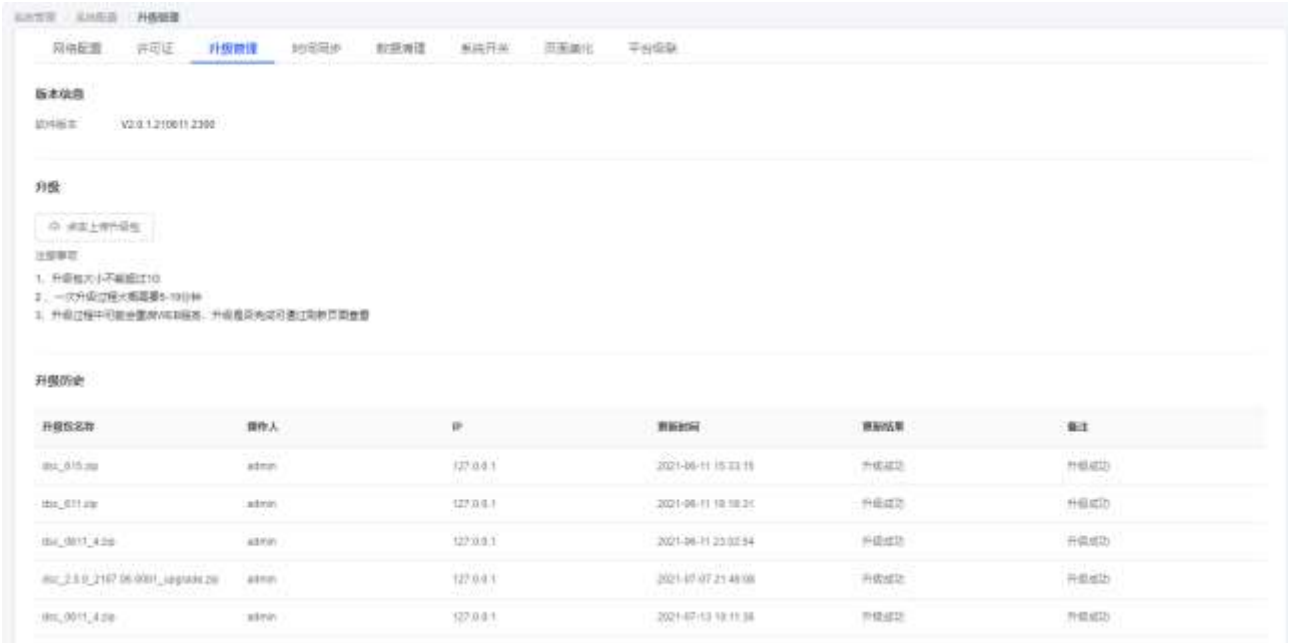
步骤2. 点击<**导出**>可以导出许可证申请文件，将导出的申请文件发送至安恒信息技术服务工程师制作新的授权文件。

步骤3. 获取到新的授权文件后，点击<**导入**>重新导入许可证。

13.3.3 升级管理

系统支持通过离线升级方式进行系统升级，同时可以在页面中查看版本信息以及历史升级信息。

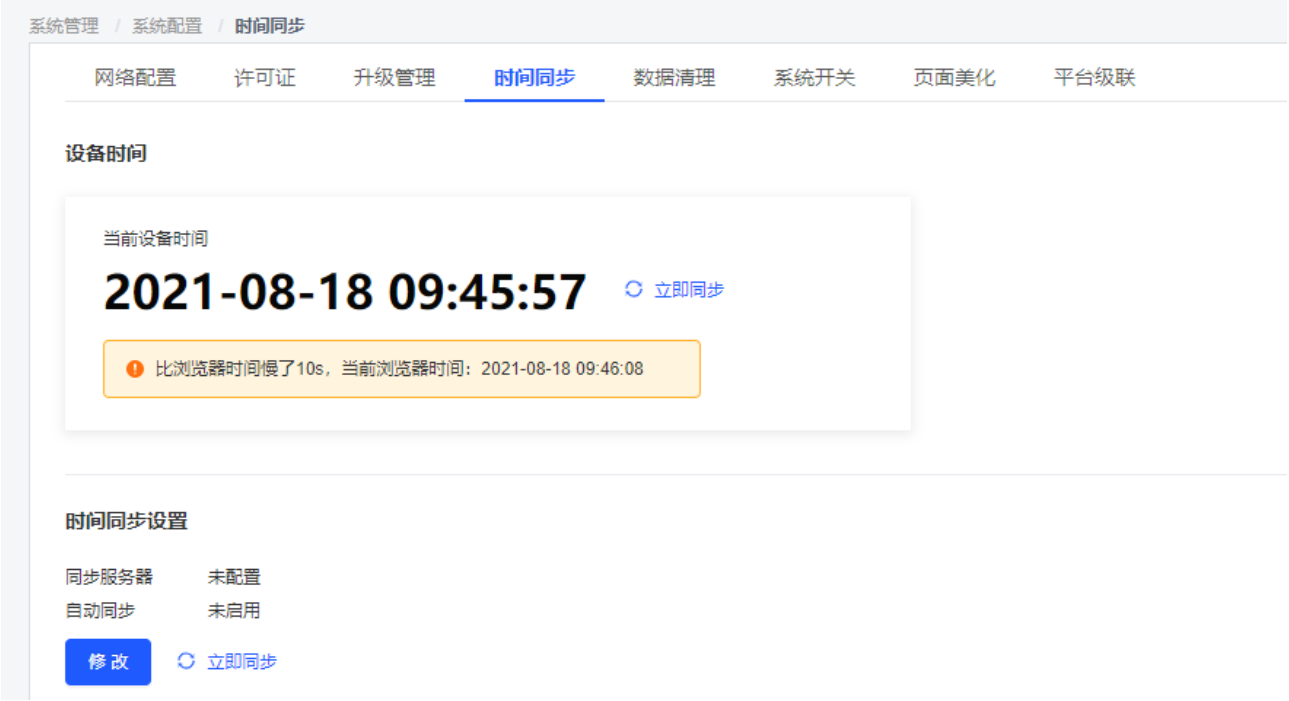
在菜单栏选择“**系统管理➤系统配置**”进入**系统配置**页面，选择**升级管理**页签，点击<**点击上传升级包**>，选择需要的升级包进行上传。



- 升级包大小不能超过 1G
- 一次升级过程大概需要 5-10 分钟。
- 升级过程中可能会重启 Web 服务器，升级是否完成可通过刷新页面查看。

13.3.4 时间同步

用户可对系统时间进行设置，设置方式分为手动设置系统时间以及通过网络获取系统时间。在**系统配置**页面，选择**时间同步**页签。



点击<**立即同步**>，可以将系统时间与浏览时间进行同步。

点击<**修改**>，填写同步服务器地址以及启用自动同步功能，点击<**确认**>。

如果设备事件晚于同步服务器时间，同步时间后，设备将会重启。

13.3.5 数据清洗

通过设置策略，设备磁盘空间小于设定值时将会自动开始清理数据。

在菜单栏选择“**系统管理➤系统配置**”进入**系统配置**页面，选择**数据清理**页签，设置相关信息，点击<**保存**>。

- 选择数据满策略，系统支持满覆盖和满停止两种。
  - 满覆盖：数据达到设定值时，新增数据将覆盖之前的数据。
  - 满停止：数据达到设定值时，新增数据将不再保存。
- 当磁盘剩余空间小于等于设置值开始清理，磁盘空间大于等于设置值停止清理。
- 当磁盘剩余空间小于等于设置值低等级告警，磁盘空间大于等于设置值中级告警。

13.3.6 系统开关

在菜单栏选择“**系统管理➤系统配置**”进入**系统配置**页面，选择**系统开关**页签，点击<**关闭服务**>可以关闭 SSH 服务，重新点击<**开启**>可以再次开启与服务器之间的 SSH 服务。

13.3.7 页面美化

默认展示系统的名称信息以及 Logo 信息。

在菜单栏选择“**系统管理➤系统配置**”进入**系统配置**页面，选择**页面美化**页签，点击<**修改信息**>，重新填写产品名称，上传产品 Logo 以及页卡 Logo。

13.3.8 平台级联

默认展示用户唯一的 Key 信息，做为用户的唯一标识 ID。

在菜单栏选择“**系统管理➤系统配置**”进入**系统配置**页面，选择**平台级联**页签，填写上级平台 IP 地址以及填写上级平台的唯一 APIKey，点击<**保存**>，出现保存成功提示则证明与上级平台建立连接。

13.4 数据字典

是指对字段 ID、字段名称、字段类型等信息进行字典分组，主要用于进行告警管理。

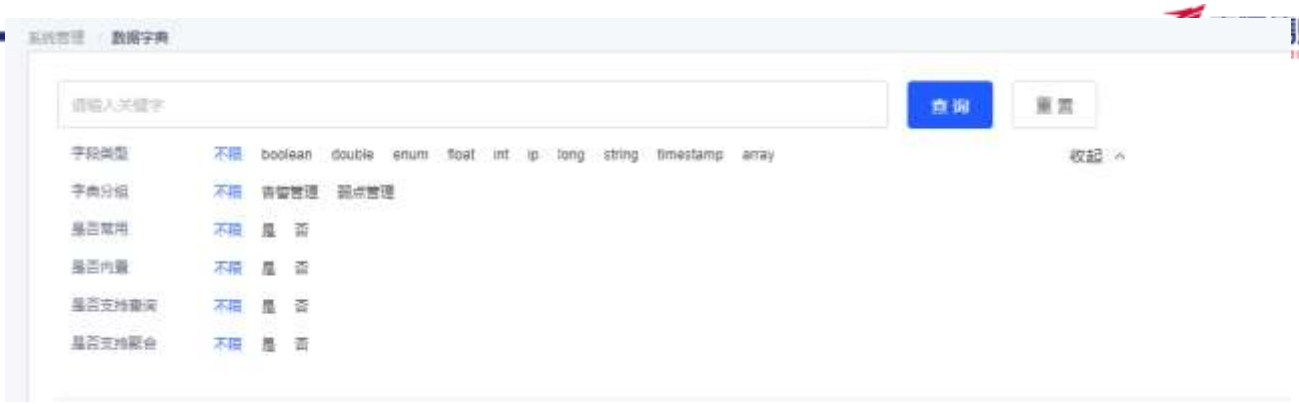
13.4.1 新增字段

步骤1. 在菜单栏选择“**系统管理➤数据字典**”进入**数据字典**页面，点击<**新增**>。

步骤2. 填写字段 ID 以及字段名等相关信息，点击<**保存**>可以新增自定义数据字典。

13.4.2 查询字段

系统支持通过输入关键字或者点击对应标签进行条件查询和筛选。

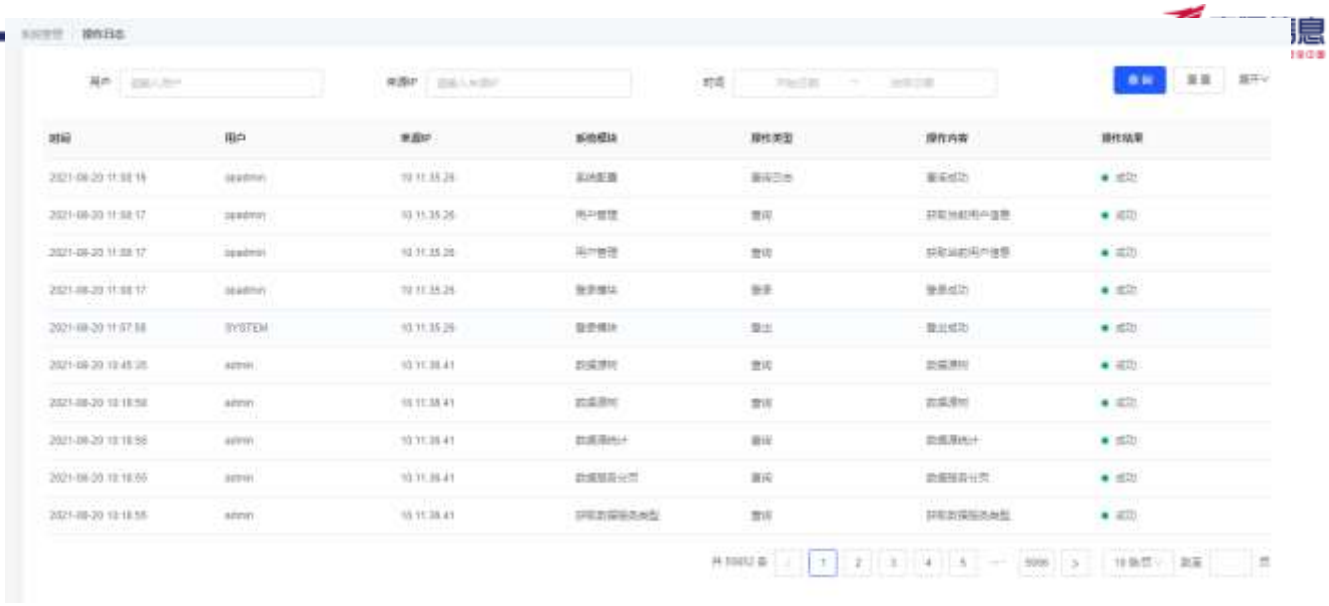


13.4.3 查看字段

点击字段列表**操作**列的<**查看**>，可以查看该条字段的详细信息。

13.5 操作日志

在菜单栏选择“**系统管理➤操作日志**”进入**操作日志**页面，可以查看系统的操作日志，并且支持按照时间、用户和来源 IP 进行条件查询。

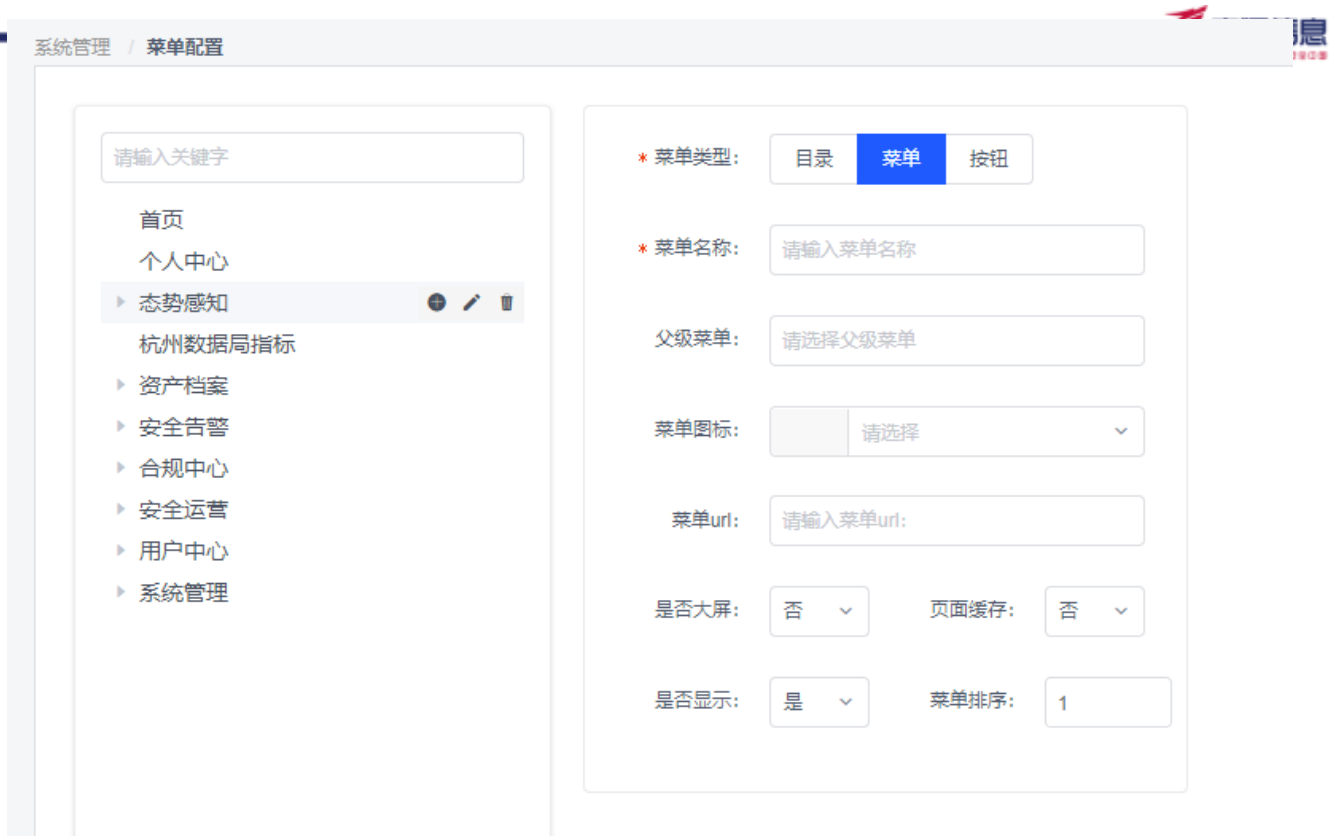


13.6 系统告警

在菜单栏选择“**系统管理➤系统告警**”进入**系统告警**页面，用于展示系统告警日志，同时系统支持通过告警类型、告警级别以及时间进行条件查询。

13.7 菜单配置

在菜单栏选择“**系统管理➤菜单配置**”进入**菜单配置**页面，主要用于对系统菜单栏、目录栏以及按钮进行配置和显示，同时系统支持通过输入关键字进行条件查询。


系统管理 / 菜单配置
请输入关键字
首页
个人中心
态势感知
杭州数据局指标
资产档案
安全告警
合规中心
安全运营
用户中心
系统管理
* 菜单类型:
目录
菜单
按钮
* 菜单名称:
请输入菜单名称
父级菜单:
请选择父级菜单
菜单图标:
请选择
菜单url:
请输入菜单url:
是否大屏:
否
页面缓存:
否
是否显示:
是
菜单排序:
1

14. 附录-术语

术语	解释
浙政钉	为规范浙政钉整体架构体系，按照统分结合原则，由省政府办公厅统一设计整体工作界面和系统框架，统筹指导全省统建应用建设，各单位根据自身业务特点分别建设自建应用，最终形成全省统一的政府系统掌上协同办公平台。