解决方案实践

顶象业务安全解决方案实践

文档版本	1.0
发布日期	2024-03-01

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述

应用场景

- **银行全行级反欺诈系统**

  客户的痛点：

  a. 随着欺诈案件多发，行内需要打造一体化全流程反欺诈体系，建成集交易事前防范、事中监控及事后分析的风险监控体系，有效防范电信网络诈骗、银行卡欺诈、互联网交易欺诈等，全面提升反欺诈能力。

  b. 传统人工审核方式无法应对越来越多的贷款类业务，效率低、成本高昂、且风险控制效果差。

  解决方案：

  基于顶象能力搭建全行级的风控反欺诈中台，服务于客户全部业务线，能够结合具体业务需求配置针对金融业务领域的风控策略。

  客户价值：

  全面实现全渠道、跨产品、各种关联方式的欺诈风险的实时防控。为行方构建了有效的全行级反欺诈体系，获得亚洲银行家大奖。

- **电商公司反营销作弊智能风控系统**

  业务痛点：

  a. 难以确保活动的公平公正性，防范黑灰产用户，保障正常用户的体验和权益。

  b. 难以识别渠道引流中的无效流量，识别优劣质渠道商。

  c. 平台商家的广告投放因为作弊，恶意竞争等导致效果较差。

  解决方案：

  提供了全套风控产品，为电商平台多个业务场景提供黑灰产的识别与拦截能力。可视化、易操作的风险管理平台，大幅提升了电商平台在高频次活动中调整营销策略的效率。

  客户价值：

  在多个业务场景进行了布控。针对免费试用退单风险，拦截比例达到了20-25%，相比厂家的要求提升了一倍效果。广告反作弊在风险发生时，可拦截90%以上作弊单击。在拉新场景能够识别5%以上无效流量，为电商平台在跟渠道结算时提供了依据。

- **互联网公司反营销作弊智能风控系统**

  业务痛点：

  客户的业务运营已经成为黑灰产的重点关注目标，黑灰产通过养号、使用虚假设备等手段对业务运营进行攻击，常年持续投入的巨大营销费用面临极高的薅羊毛风险。

  解决方案：

  部署顶象智能风控系统，一方面通过识别客户端运行环境、操作行为等异常信息，为风控系统提供决策依据；另一方面通过决策引擎配置应对策略，自动化解决流程中的问题，减少人工介入，提升决策效率，降低人为操作风险。

  客户价值：

  具体以某网约车客户为例，每日识别10万+风险设备，注册场景每月有效用户增加120万+，营销活动降损150万+元/月，提升营销投放效率20%+，降低逃单坏账50%+。

- **航空公司票务系统反爬反占座**

  客户的痛点：

  a. 航空公司线上销售渠道，比如官网、app、H5、小程序等，长期面临黑灰产爬虫和薅羊毛。黑灰产或者其他OTA渠道使用爬虫技术，批量获取航空公司官网航班和票价等信息，造成航空公司系统压力很大。
  b. 用户在航空公司官网提交订单后，一般有半小时左右等待支付时间，这期间座位会被临时’占用’。黑灰产利用这一特点，通过自动化工具大批量下单但不支付，导致航空公司无法正常售票。
  c. 航空公司官网推出的低价票，优惠券等营销活动被黑灰产大量薅羊毛，造成严重资损。

  解决方案：

  构建一栈式风控系统，覆盖端安全、人机验证、设备指纹、风控系统，对业务场景下各个环境进行风险控制。

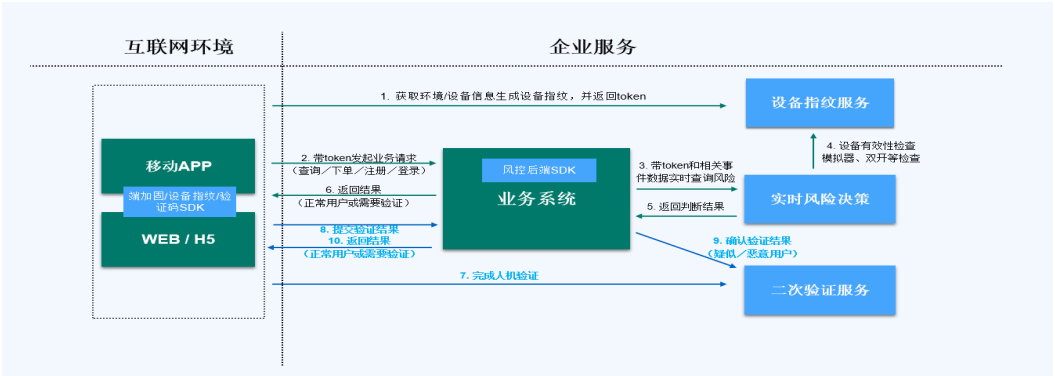
  客户价值：

  通过顶象业务安全解决方案，为航空公司提供全方位的安全防护，能够有效从线上业务流量中识别出风险，有效阻断各类业务风险请求。

方案架构

图 1-1 顶象业务安全解决方案逻辑架构

图 1-2 方案实施架构图



架构说明：

1. App/H5 加固，防止客户端业务逻辑被逆向破解。
2. 集成设备指纹/终端安全态势感知，识别终端设备各种风险，对抗黑灰产各种作弊工具。
3. 集成人机验证，阻断各业务场景中的机器攻击。
4. 集成风控系统，通过安全策略对不同业务场景，比如查询，订单，注册，营销活动等请求进行识别和控制。

方案优势

- **实践场景丰富：**已在超过4000家客户业务场景实践，覆盖24类行业，剖析92个场景 ，洞悉181大类风险，
- **策略配置灵活高效：**系统支持最复杂策略制定，单机每秒60万+个规则、指标和逻辑运算，30秒快速配置，60秒策略生效。
- **风险识别风控精准度高：**业务安全防御云已沉淀超过5903个模型策略，18859条规则，让防控精准度>99.9%。
- **支持全生命周期业务安全管理：**业务风险全生命周期自动化管理，从采集风险到策略生成最快3小时。
- **系统部署灵活可扩展：**从人机防控，安全策略，终端风险识别策略各方面，顶象业务安全方案提供高灵活度，高扩展性的产品。应对线上风险时，无需业务和系统的代码调整，通过顶象业务安全平台即可调整应对各类业务风险。

2 资源和成本规划

以电商，互联网，金融等客户案例为例，每日支撑百万以内业务数据量的情况下，提供资源和成本规划参考。

表 2-1 资源和成本规划

云资源	规格	数量	每月费用（元）
VPC	网段选择172.16.0.0/16，其他采用默认配置	1	00.00
Subnet	网段选择172.16.0.0/24，其他采用默认配置	1	00.00
安全组	根据需要开通入方向3306等端口	1	00.00
ECS	初级版 | 8核 16 GB | 100G 数据盘	3	2,250.00
CSS	规格: X86计算 | 计算密集型 | ess.spec-8u16g | 8核 | 16GB|高IO | 500GB	1	1,800.00
DCS	产品类型: 基础版 | 5.0 | Cluster 集群 | X86 | DRAM | 1 | 16 GB	1	1,500.00
DDS	社区版 | 副本集 | 通用型 | 4核16GB | 超高IO | 200GB	1	2500.00
RDS	MySQL | 5.7 | 单机 | 通用型 | 4核8GB | SSD云盘 | 40GB	1	400.00
ELB	共享型负载均衡| 全动态BGP| 流量 | 400GB	1	564.00
OBS	100G	1	13
总计：9027.00			

部署说明：

1. 用户现在华为云平台购买方案套餐和华为云资源，具体规格根据自身业务数据量评估后选择。

2. 所有软件模块均为java应用，docker方式部署，交付镜像包。华为云资源准备好以后由顶象实施人员部署。
3. 系统部署完成后，由顶象实施人员进行调试和验证，验证完成后交付用户接入集成。

3 实施步骤

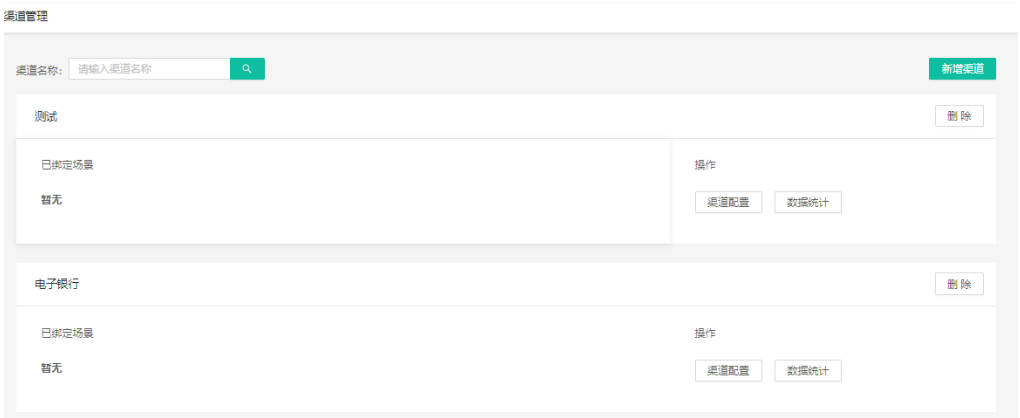
3.1 无感验证

当有无感验证授权时，才有权限访问无感验证下相关模块，否则不可见。

渠道管理

渠道管理模块供给用户对当前所有渠道应用的管理功能，主要包括新增、删除、已绑定业务场景展示、功能跳转(应用配置和数据统计)。

图 3-1 渠道管理



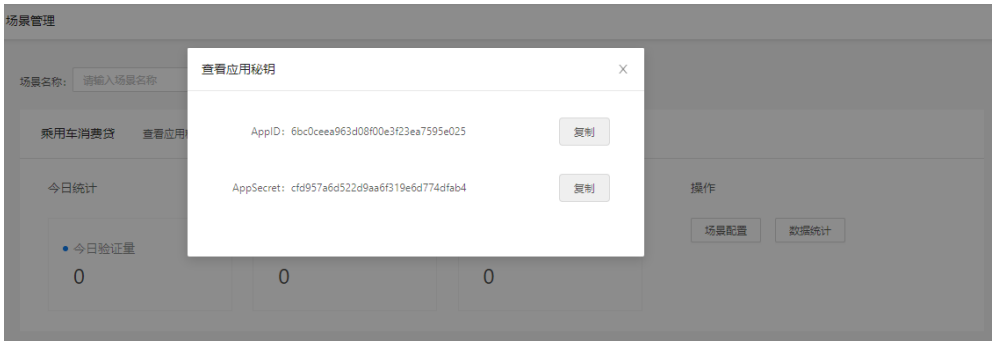
场景管理

每个业务场景都会展示今日 3 项数据指标的展示，包括今日验证量、今日验证成功量、 今日验证拦截量。

图 3-2 场景管理

用户接入无感验证应用时需要相应的密钥，每个业务场景在创建的时候系统会自动分配 一对密钥，用户可在业务场景管理界面单击【查看应用密钥】按钮进行查看。

图 3-3 查看应用密钥



外观管理

系统提供内置的默认图集和自定义图集供用户进行自主选择。默认图集中会内置系统提供的部分图片，自定义图集主要供用户自主上传自身企业风格符合的图片内容。

图 3-4 定制背景图片

用户可以自主定制验证码右上角的显示 Logo 和对应的超链接。

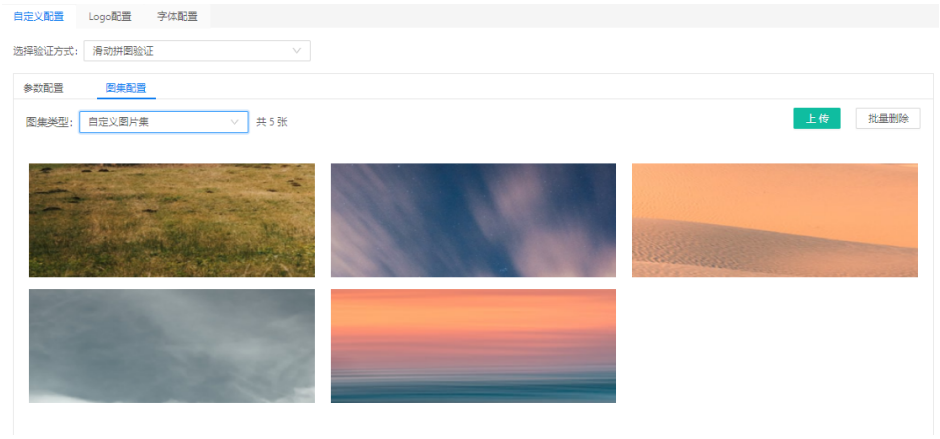
用户单击【上传文件】，上传需要的 Logo 文件，也可以调整 Logo 跳转链接;

图 3-5 外观管理-自定义配置-参数配置

图 3-6 外观管理-Logo 配置

用户单击【立即保存】，即可更新成功，系统更换 Logo 图片存在一定延时约 5 分钟。

图 3-7 外观管理-自定义配置-图集配置

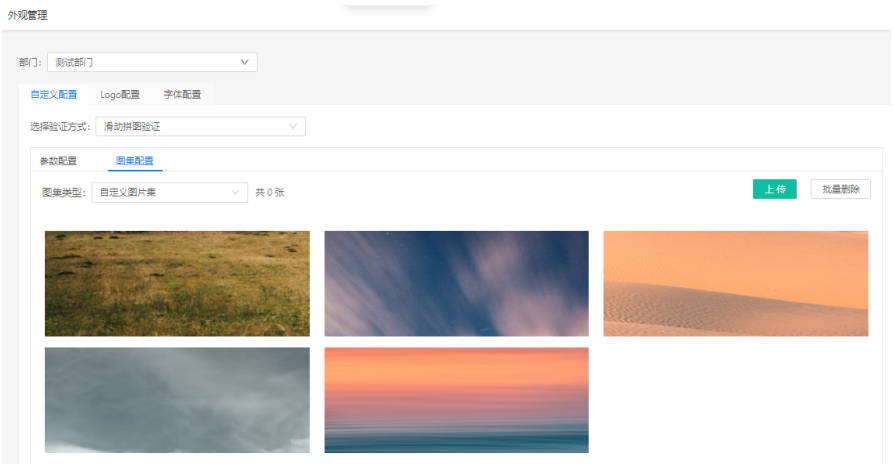


单个图片上传用户单击【上传】按钮并选择需要上传的图片；用户进入自定义页面进行裁剪编辑，完成后单击【确定】按钮。

图 3-8 自定义背景图片

批量图片上传 用户单击【批量上传】按钮;

图 3-9 批量图片上传



用户单击选择对应图片或将图片拖拽到区域内，系统会及时上传，完成后关闭上传窗口。

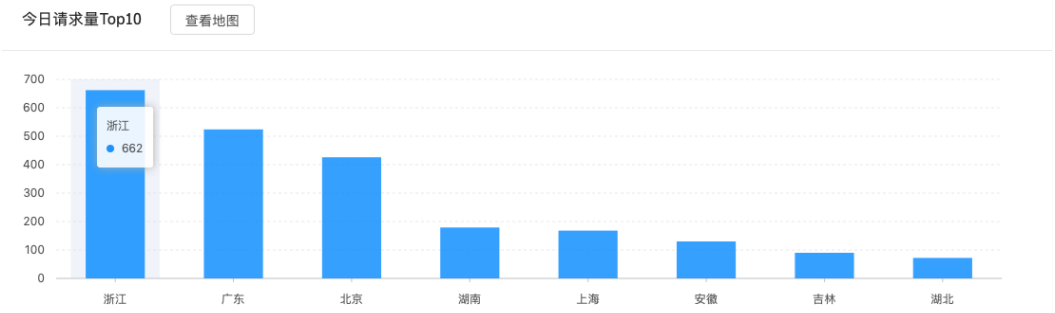
数据统计

切换渠道应用&业务场景： 用户可对所需查看的数据统计进行切换，支持渠道应用和业务场景两个维度进行切换。

查看今日指标：支持用户查看今日指标，主要包括今日请求量、今日验证量、今日验证成功量、今日验 证拦截量、今日验证通过率、今日验证占比、今日请求量 TOP10、今日请求量地图。

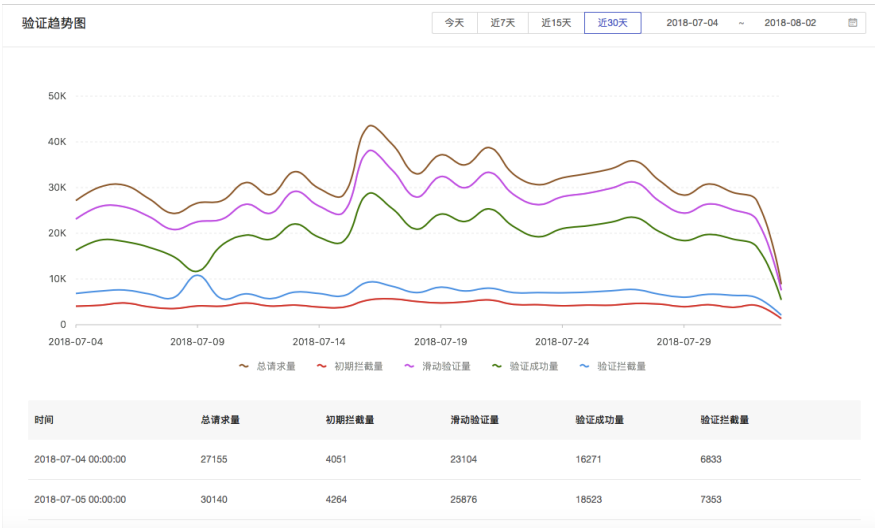
图 3-10 今日指标

图 3-11 今日请求量 TOP10



查看验证趋势图：支持用户查看验证趋势图以及验证统计数据，用户可自主选择所需要查看的时间区间。

图 3-12 验证趋势图



模型升级

支持用户自主上传新的模型文件进行更新。

图 3-13 上传升级文件

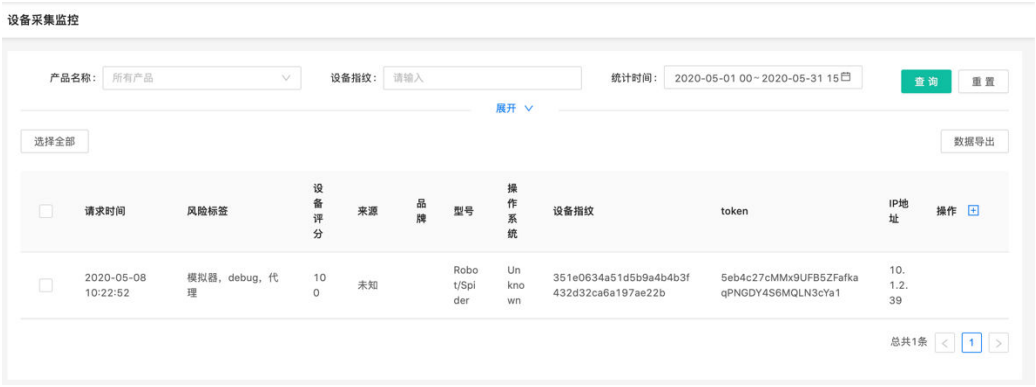
3.2 设备指纹

设备采集监控

在接入设备指纹之后，可以在设备采集监控模块通过不同的查询条件查询设备指纹请求的明细数据及风险标签、设备评分等信息。

- 条件查询：支持通过“设备指纹”“来源”“token”“风险标签”“IP地址”“请求时间”来查询。
- 列表数据：“设备指纹”“token”“操作系统”“品牌”“型号”“来源”“最近访问时间”“IP地址”“风险标签”“设备评分”。

图 3-14 设备采集监控



数据统计

数据统计展示昨日设备指纹的请求量，昨日有风险的设备请求量及设备请求趋势图，同时支持对近7天、近30天等时间范围的查询。

图 3-15 数据统计

在页面下方对查询时间内的数据通过列表的方式进行了详细的展示，包括总请求量、Web、iOS、Android请求量及各端的风险量情况。

图 3-16 数据统计列表

时间	总请求量	Web请求量	iOS请求量	Android请求量	总风险量	Web风险量	iOS风险量	Android风险量
2019-07-11 09:00	1	1	0	0	0	0	0	0
2019-07-11 10:00	9	9	0	0	0	0	0	0
2019-07-11 11:00	40	40	0	0	0	0	0	0
2019-07-11 12:00	1	1	0	0	0	0	0	0
2019-07-11 14:00	19	19	0	0	0	0	0	0
2019-07-11 15:00	6	6	0	0	0	0	0	0

设备分析

设备分析模块默认展示当前自然日的设备请求趋势、风险命中排行、异常占比、风险请求分布，支持按不同应用、请求时间查询。

图 3-17 设备分析

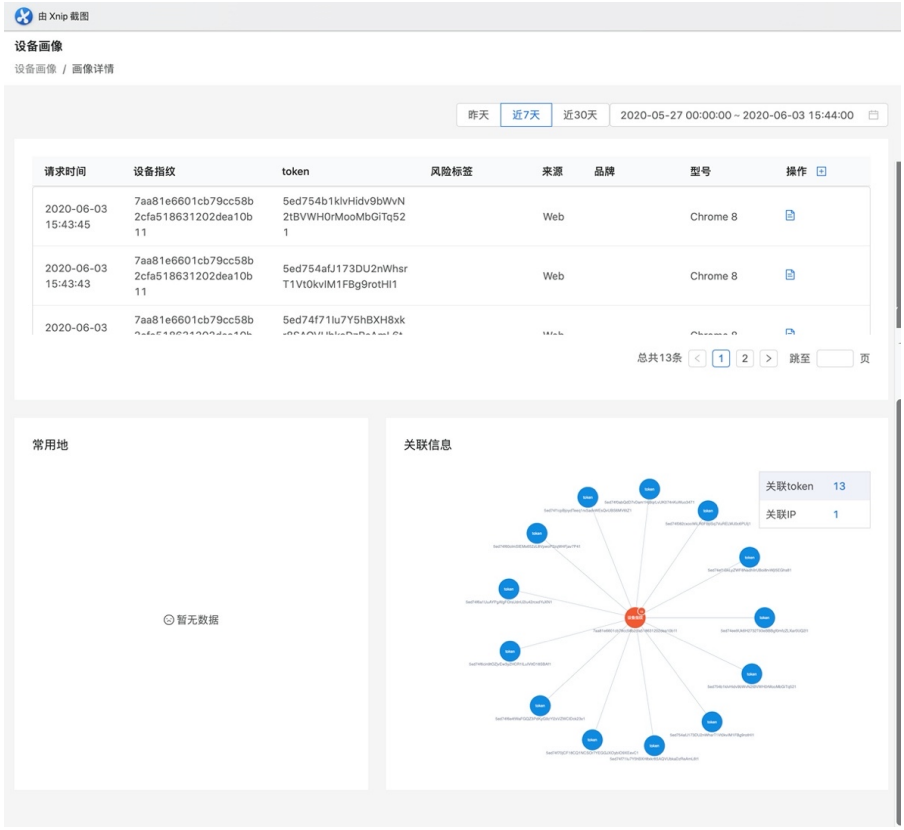
在页面下方以列表的形式展示每个时间段内不同风险标签的命中情况。

图 3-18 设备分析数据列表

设备画像

在设备画像模块支持按设备指纹、设备指纹token来查询设备的画像，设备画像包括设备的基础属性、近期行为属性、近七日常用地，近七日关联信息。

图 3-19 设备画像



3.3 风控引擎

风险大盘

风险大盘展示当前自然日的风险请求数据，风险大盘共包含两屏。

页面右上角为风险大盘入口。风险大盘展示当前自然日的实时风险数据。

图 3-20 风险大盘入口

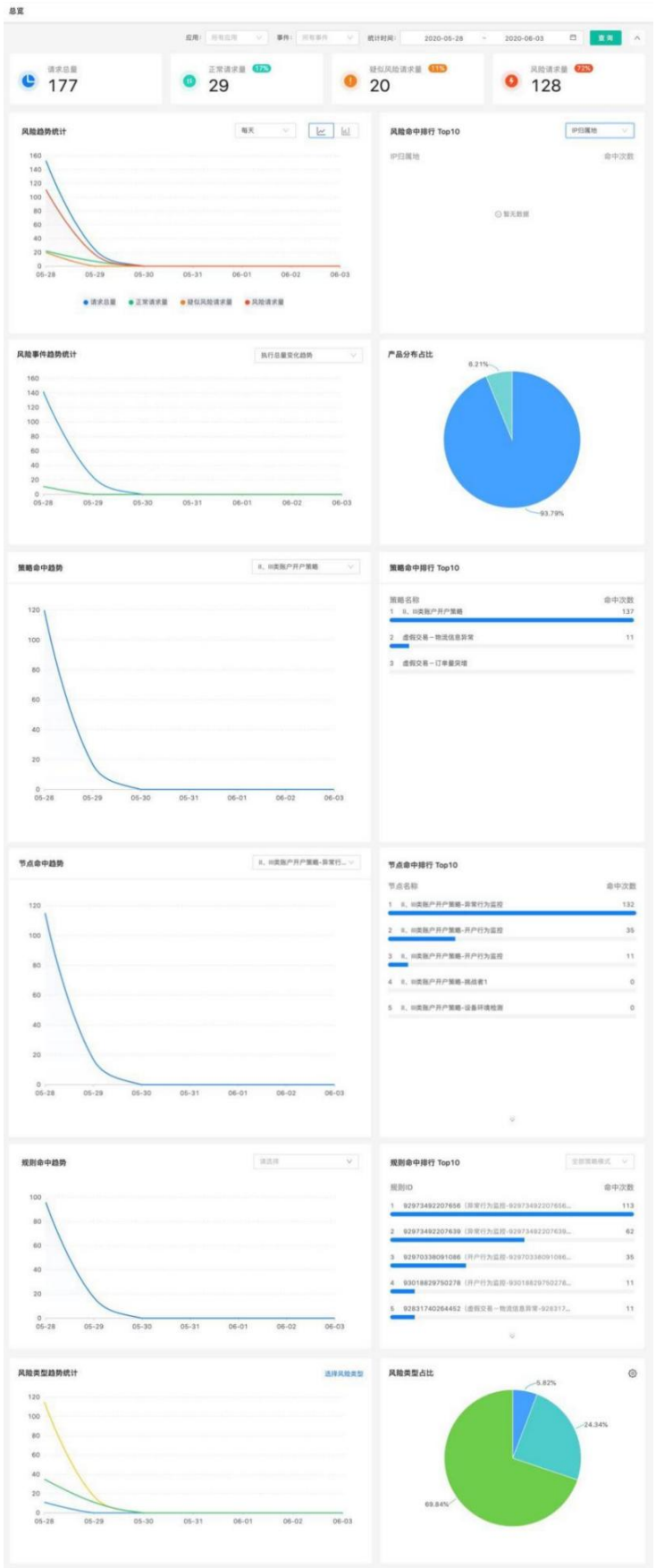
风险大盘分为首屏、次屏和设备屏，可自定义设置首、次屏的展示数据、刷新频率和切换频率。

总览展示

总览模块默认展示近7天的风险数据，包括请求趋势、策略、规则趋势、风险事件等维度报表。特别是策略命中排行等维度数据可以为业务人员提供策略调优数据依据。

支持通过“产品”、“事件”和“统计时间”查询风险请求、风险命中情况、产品/事件命中情况、策略命中情况、节点命中情况、规则命中情况、风险类型命中情况多个维度的统计报表。

图 3-21 总览



监控中心

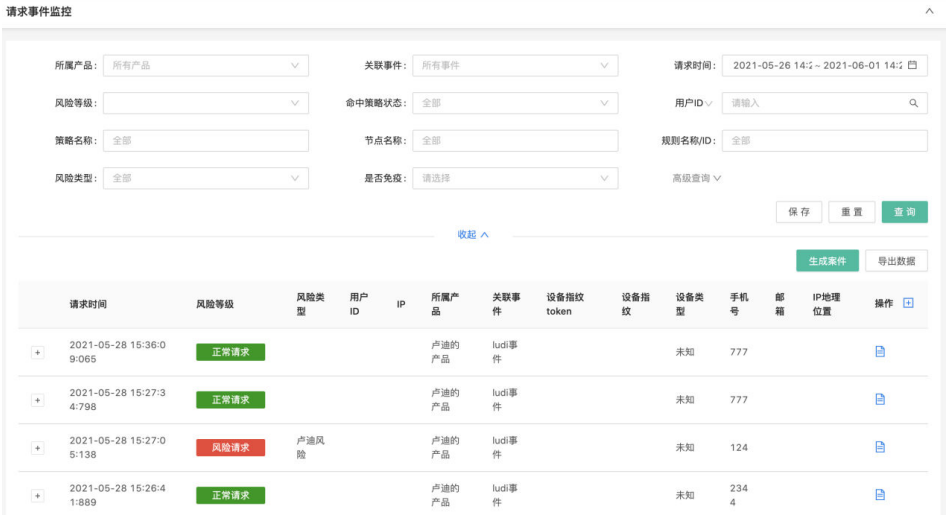
- **业务监控**

  a. 请求事件监控

  查询系统的风控引擎风险识别日志，及时了解业务系统的风险情况和定位风险源头及数据回放，查看策略的执行结果，支持通过各类查询条件组合进行筛选。

  通过设置查询条件，可从不同维度对请求结果进行筛选，查询结果列表的展示会随查询条件的维度而变化，可从请求、策略、节点、规则等维度展示列表信息，也支持设置高级查询条件。

  图 3-22 请求事件监控



  查询结果列表中可查看每笔请求对应的事件详情信息，包括风险等级、风险类型、各类参数等信息

  b. 数据报告管理

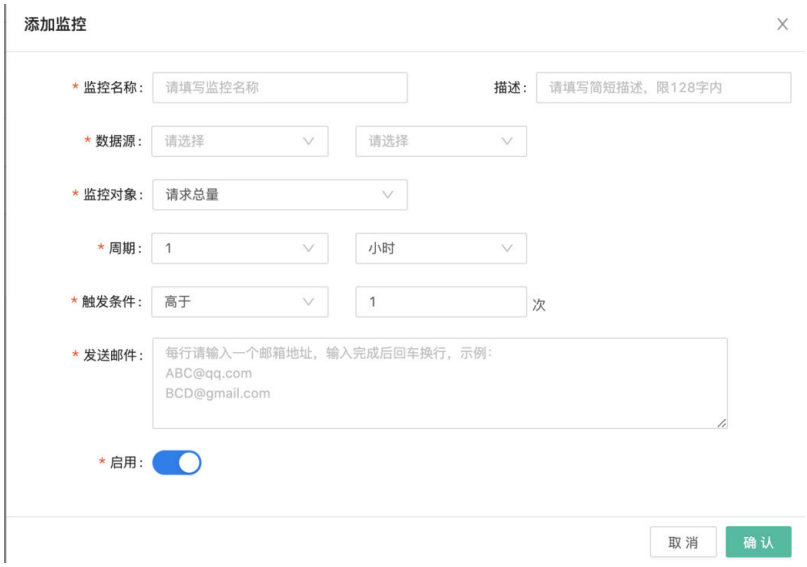
  系统可以自动发送设置周期内的风险报告邮件，可以不通过访问总览，通过邮件了解日常风险情况，报告的维度包括风险趋势、风险分类占比、每日风险详情。

图 3-23 添加数据报告

c. 风险监控管理

该功能支持对不同产品、事件下的业务情况进行监控，包括请求总量、正常请求量、风险请求量、疑似风险请求量进行监控，可以按分钟、小时、天进行高于、低于等百分比进行监控设置，超过设定的条件后，系统将发送报警通知到设定的邮箱。

图 3-24 添加监控



- **系统监控**

a. 应用节点监控

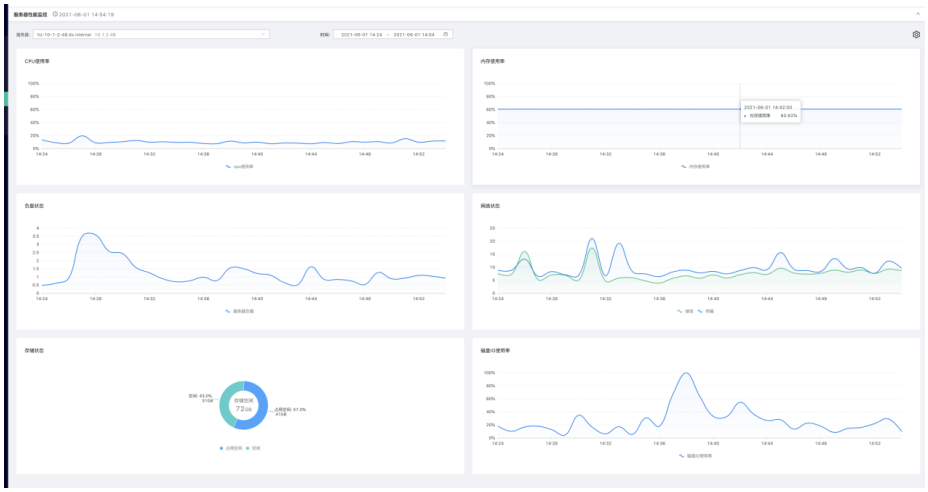
监控指标、设备指纹、引擎的节点状态，支持对近7天的监控情况进行查询。

图 3-25 应用节点监控

b. 服务器性能监控

监控服务器的CPU使用率、内存使用率、负载状态、网络状态、存储状态、磁盘IO使用率。

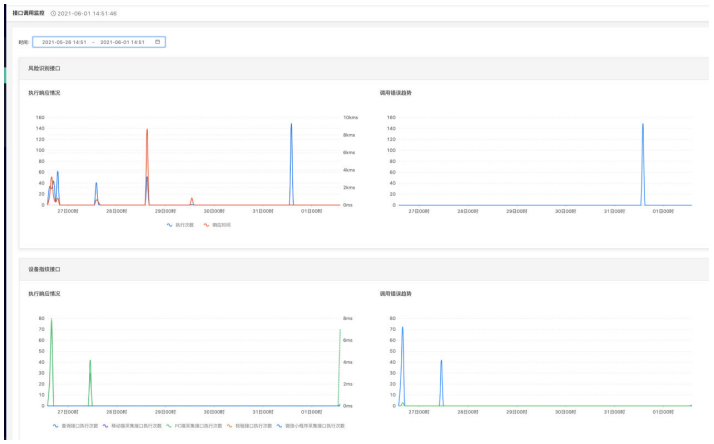
图 3-26 服务器性能监控



c. 接口调用监控

监控引擎的风险识别接口执行情况和调用错误趋势，设备指纹接口执行响应情况和调用错误趋势，指标接口的执行响应情况，支持对近7天的监控情况进行查询。

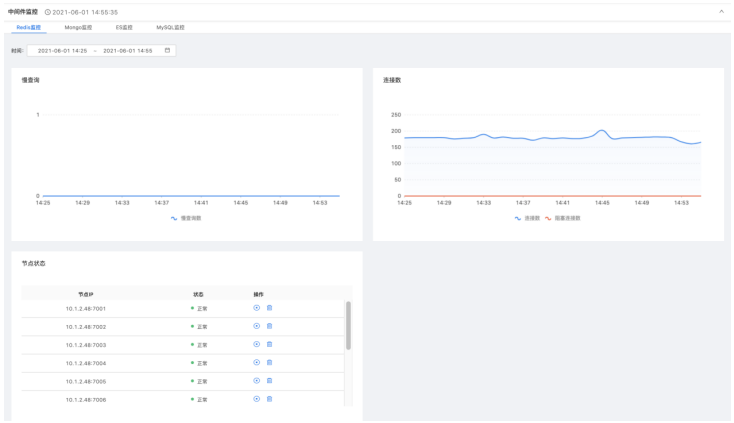
图 3-27 接口调用监控



d. 中间件监控

系统展示Redis、Mongo、ES、MySQL的监控，包括慢查询、连接数、节点状态等；

图 3-28 中间件监控

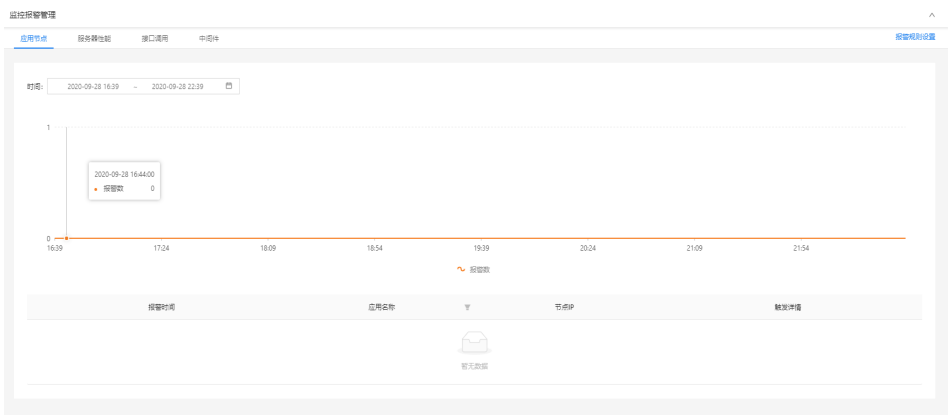


e. 监控报警管理

该功能可以查询到应用节点、服务器性能、接口、中间件触发的报警，触发后以折线图及列表的形式展示报警信息及出发详情。

单击“监控报警管理”，进入页面后，系统会默认近6个小时的情况。

图 3-29 监控报警管理



变量管理

- **字段管理**

字段是用于判断和识别风险的最小单位，例如ID、IP地址、 账号、设备指纹等，配置指标、策略时都将用到字段。

字段分成系统字段和自定义字段，系统字段不可以编辑和删除。

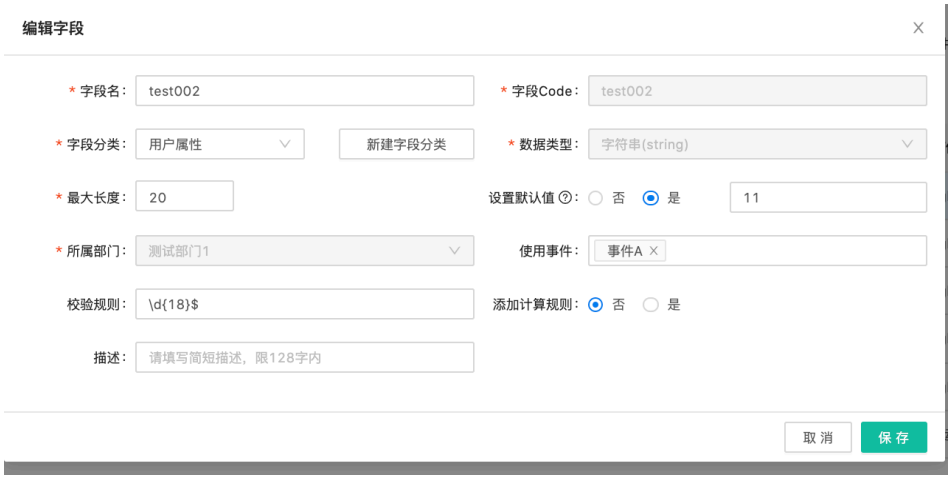
a. 新增

支持批量导入或手动新增字段，手动新建/编辑字段时，可使用函数计算公式，使用复杂表达式定义函数字段。

系统内已有预置分类，也可单击“字段分类管理”创建自定义分类，在规则中使用字段时可通过分类筛选字段，方便选择。

在字段管理页面单击“添加字段”按钮，弹出添加字段页面，如下图所示：

图 3-30 手动新增字段



依次填写字段的信息，信息填写完整后，单击“确定”按钮即可新增字段信息，并提示“新增成功”信息；

图 3-31 新增字段成功

b. 编辑

单击字段管理列表中的操作列的编辑“ ”按钮，即可进入“编辑字段”页面（未审核通过字段不可编辑），如下图所示：

字段信息中除了“字段code”、“数据类型”、“所属部门”不可编辑，其它信息都可以编辑，单击“提交”按钮即可编辑成功；

图 3-32 编辑字段

c. 删除

在字段管理列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“确定删除该字段吗？”

图 3-33 删除字段 1

单击“取消”按钮，该数据不做任何操作，单击“确定”按钮，页面上方提示“您的操作已提交审核，审核通过后生效”；并在该产品数据的最左侧有“待审核”标签。

图 3-34 删除字段 2

- **名单管理**

  用户可以自定义名单并上传数据，名单数据支持增删改查的操作，在风控策略中可以使用名单数据。

  a. 新增

  添加名单：单击名单管理列表右上方的“添加名单”，弹出“添加名单”页面，如下图所示

图 3-35 添加名单

相关信息填写完整好，单击“提交”，弹出“新增成功”信息；新增的字段默认为“生效”状态；

图 3-36 名单新增成功

添加名单数据-文件上传：根据“模板文件”示例，添加名单数据在文件中，并导入到系统中即可批量上传名单数据；

图 3-37 添加名单数据-文件上传

添加名单数据-手动录入：可手动逐条添加名单数据信息，并可约束名单数据的效期；

图 3-38 添加名单数据-手动录入

b. 编辑

在名单管理列表中，单击操作列的编辑“ ”按钮，即可进入“编辑名单”页面，名单的编辑支持对名单的“基本信息”和“名单数据”的编辑，如下图所示：

图 3-39 基本信息

图 3-40 名单数据

c. 删除

在名单管理列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“确定删除该字段吗？”

图 3-41 名单删除警告

单击“取消”按钮，该数据不做任何操作，单击“确定”按钮，页面上方提示“名单删除成功”；

图 3-42 名单删除提示

- **函数管理**

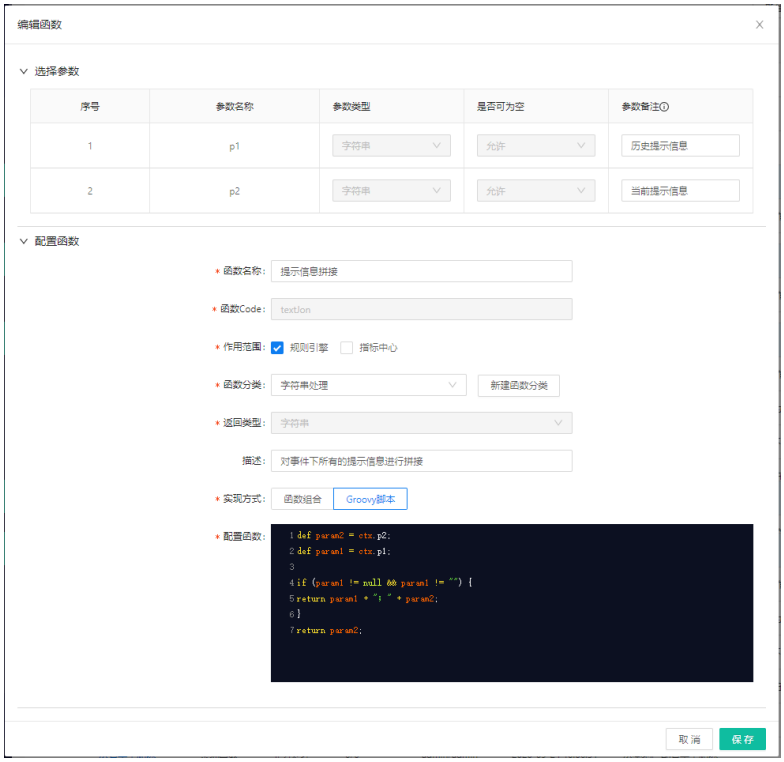
  可管理风控系统中的函数，支持增、删、改、查操作。

  a. 新增

  单击函数管理列表右上方的“新建函数”，弹出“新增函数”页面，如下图所示：

图 3-43 新增函数

图 3-44 编辑函数



所有函数为全部部门可见，添加函数时无需选择函数的所属部门;
单击“提交”按钮，函数新增成功，单击“取消”按钮，数据无变化；

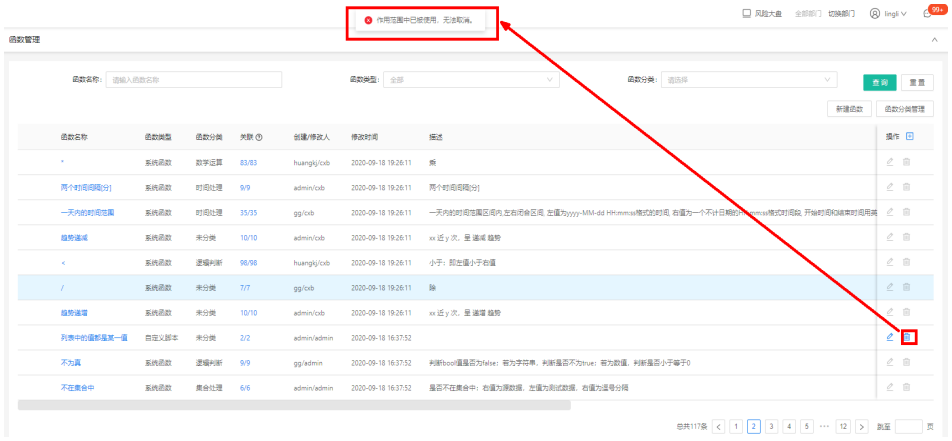
图 3-45 函数管理

b. 编辑

在函数管理列表中，单击操作列的编辑“ ”按钮，即可进入“编辑函数”页面，函数的编辑支持对函数的“基本信息”和“名单数据”的编辑，如下图所示：

图 3-46 函数基本信息

图 3-47 函数名单列表



c. 删除

图 3-48 删除函数

- **风险类型管理**

  根据业务场景定义不同的风险类型并在策略中使用，命中后可在总览里根据风险类型来查询风险分类趋势。可管理风控系统中的风险类型，支持增、删、改、查操作。

  a. 新增

  在风险类型管理，单击“添加风险类型”按钮，输入分类名称后即可自定义风险分类；

图 3-49 添加风险

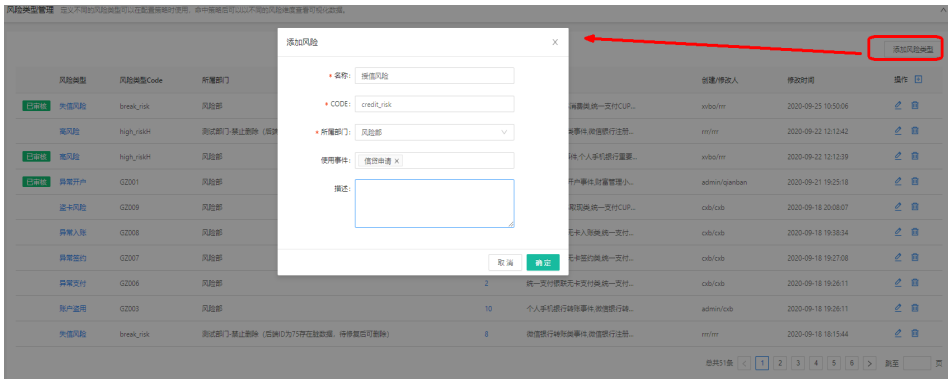
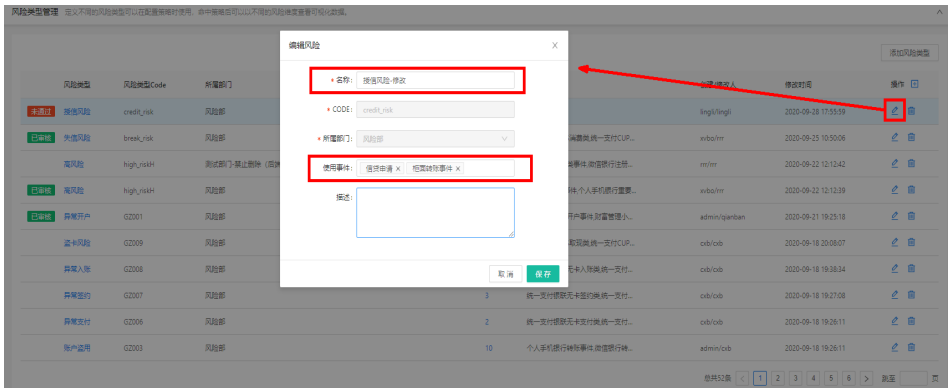


图 3-50 风险类型管理

b. 编辑

单击风险类型管理列表中的操作列的编辑“ ”按钮，即可进入“编辑风险”页面，支持对风险的“名称”“使用事件”“描述”进行编辑，不支持“CODE”和“所属部门”的编辑；

图 3-51 编辑风险



单击“确定”按钮，编辑成功的风险类型需要“审核”通过后才能生效；

图 3-52 编辑风险提示

c. 删除

在风险类型管理列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“您确定删除该风险类型吗？”

图 3-53 删除风险类型警告

单击“确定”按钮，删除的数据需要提交审核，根据审核的状态来决定该条数据是否删除；

图 3-54 删除风险类型提示

- **指标中心**

  可管理风控系统中的指标，查看指标的调用统计，新建指标计算方式。

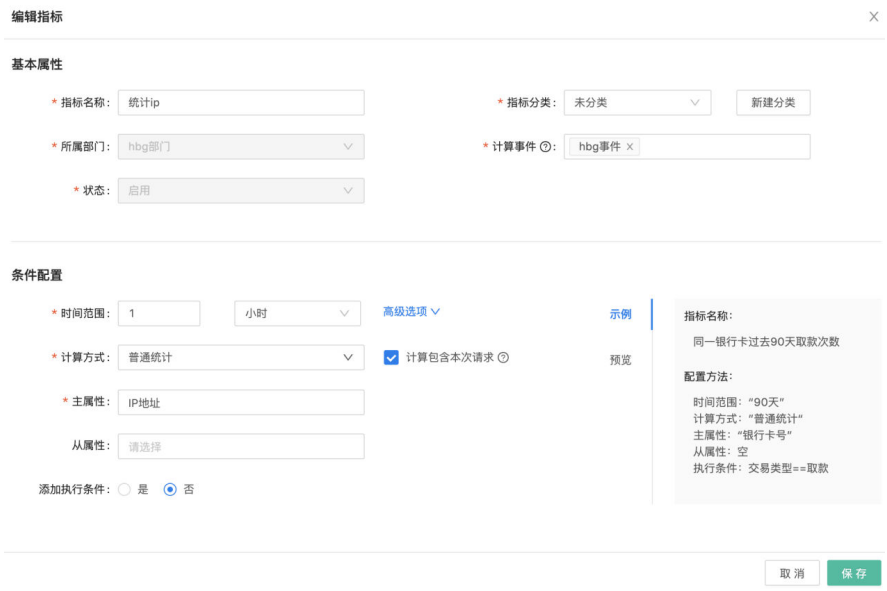
  a. 指标调用统计

  定义完成的指标有数据接入后，在此模块就可以看到指标的调用统计信息，包括指标调用趋势图、调用排行、接口调用量等信息。

  b. 指标定义

  新增：在指标定义页面，单击“添加指标”按钮，弹出“添加指标”页面；新建指标时，需选择指标的计算事件；

图 3-55 添加指标



编辑：单击指标定义列表中的操作列的编辑“ ”按钮，即可进入“编辑指标”页面，除了指标的“所属部门”无法编辑，其他字段都支持编辑；

图 3-56 编辑指标

删除：在指标定义列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“您确认执行删除操作吗？”

单击“取消”按钮，该指标数据无变化；单击“确定”按钮，指标，待删除的数据需要提交审核，审核通过，则删除成功；审核拒绝，则删除失败；

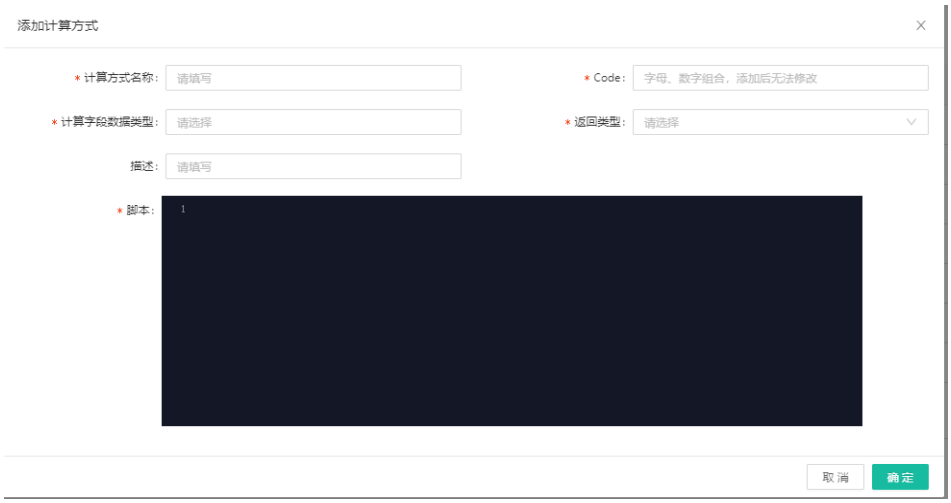
图 3-57 删除指标

c. 计算方式管理

计算方式是指标里使用到的，系统里内置了常用的关联、统计、方差等计算方式，在此功能模块可以对系统内置的计算方式和新建的计算方式来查询。

新增：计算方式是指标里使用到的，系统里内置了常用的关联、统计、方差等计算方式，也支持自定义计算方式，在“计算方式管理”界面，单击“添加计算方式”按钮，弹出如下图：

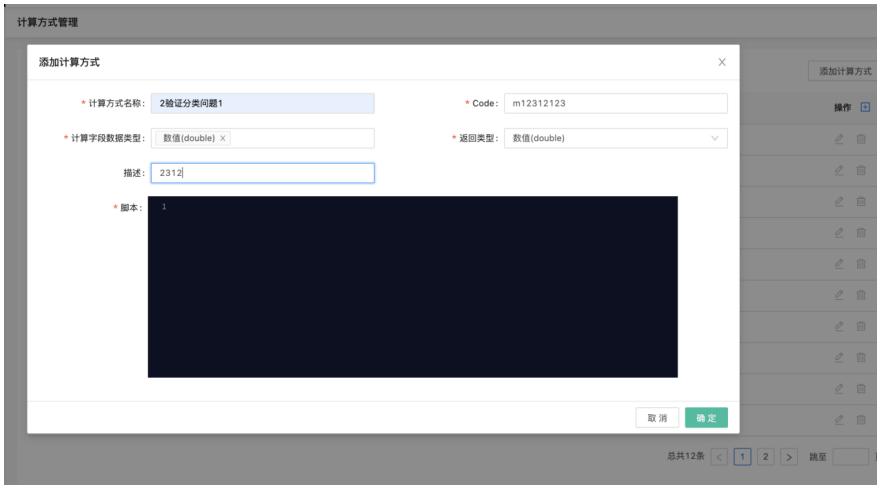
图 3-58 添加计算方式



在页面弹出框，依次填写计算方式名称、Code、数据类型、返回类型、描述、脚本，单击“确定”按钮完成指标的定义，添加后即时生效。

编辑：在“计算方式管理”界面，在每条计算方式数据的操作栏，编辑“ ”按钮，弹出“编辑计算方式”页面，支持对计算方式的名称、数据类型、描述、脚本进行修改，如下图：

图 3-59 编辑计算方式



删除：在计算方式管理列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“您确认执行删除操作吗？”

图 3-60 删除计算方式

- **数据聚合**

  可管理外部数据和管理外部数据映射，支持对外部数据及其映射进行增、删、改、查的操作。

  a. 三方数据源

  列表展示已添加的所有三方数据源，支持查看、编辑、删除和添加新的三方数据源。

  新增：在“三方数据源”的列表中，单击【添加三方数据源】按钮，可设置数据源的基本信息、计费方式、费用和参数等。

图 3-61 添加三方数据源 1

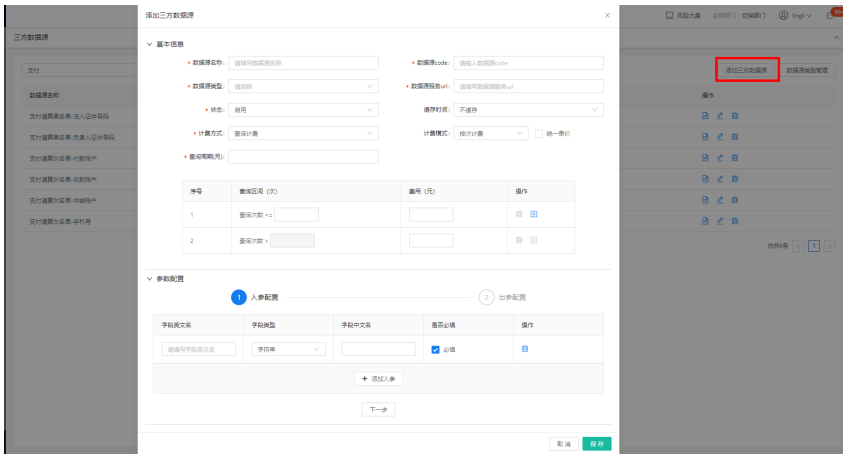
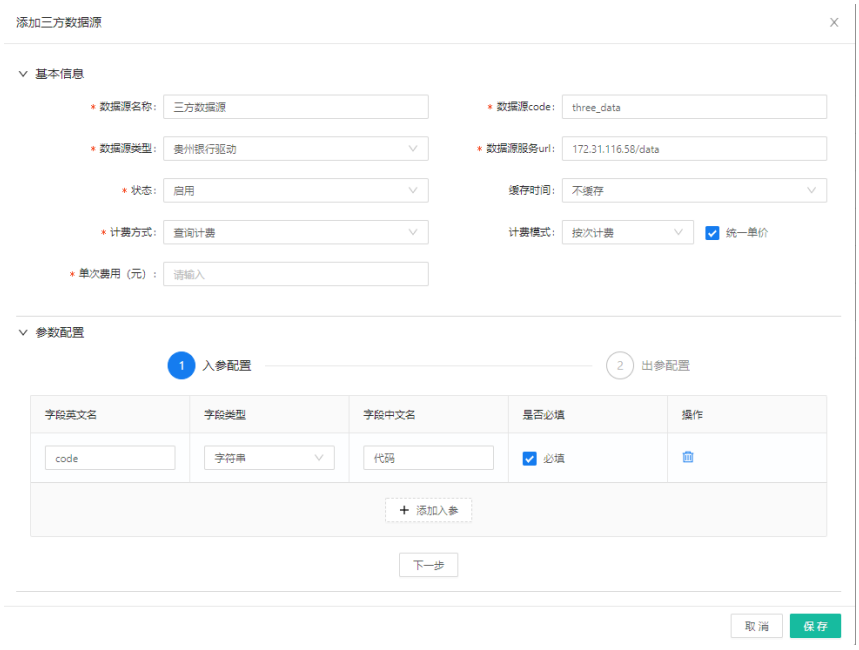


图 3-62 添加三方数据源 2



外部数据创建完成后可添加映射，将外部数据的入参与风控系统内的字段进行映射，映射完成后可在策略中使用此外部数据。

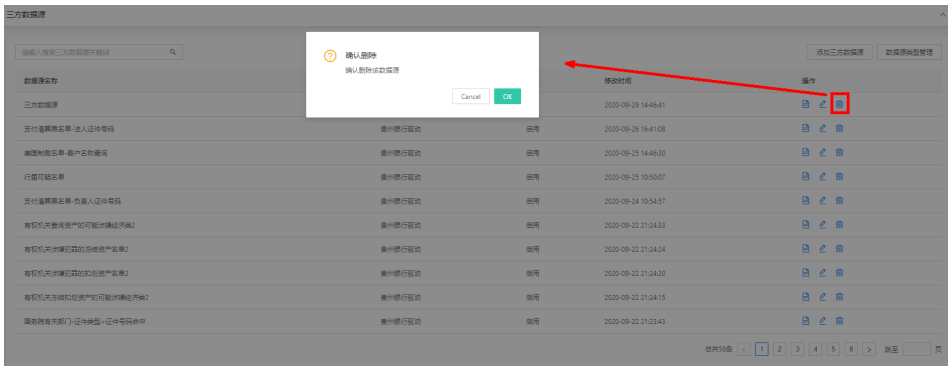
编辑：在三方数据源列表中，单击操作列的编辑“ ”按钮，弹出“编辑三方数据源”页面，除“数据源code”无法编辑，其他数据都可以进行编辑；

图 3-63 编辑三方数据源

单击【确定】，数据提交审核，审核通过后修改的数据方可生效，否则数据不生效。

删除：在“三方数据”列表界面，单击操作列的删除“ ”按钮，弹出提示页面，如下图：

图 3-64 删除三方数据源



单击【确定】删除成功，单击【取消】数据无变化；

b. 行内数据源

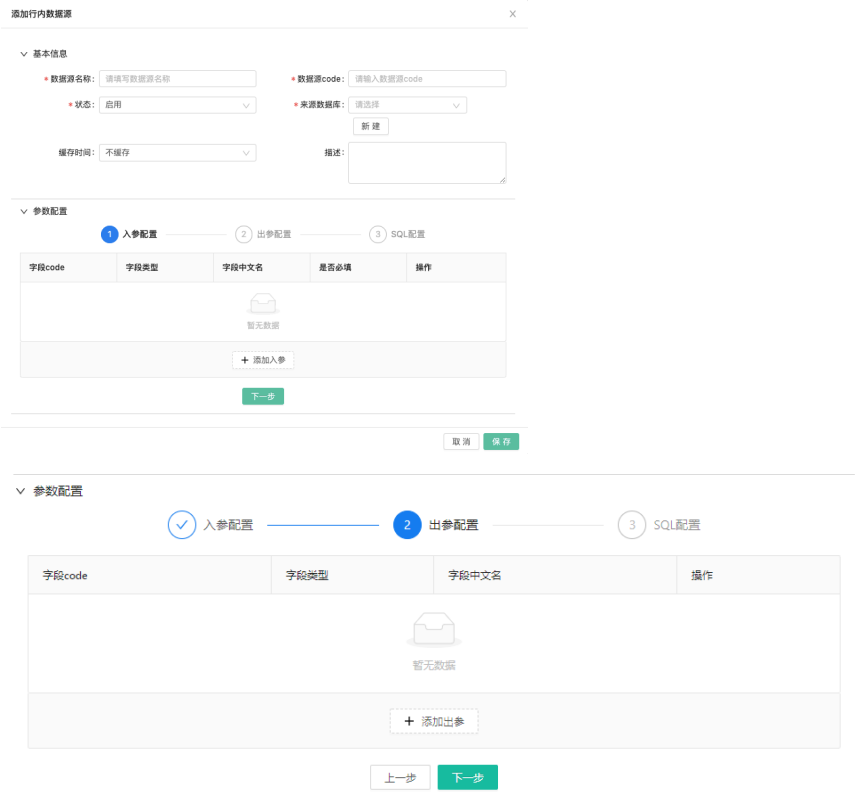
列表展示已添加的所有行内数据源，支持查看、编辑、删除和添加新的行内数据源。

新增：行内的数据源可以通过添加数据源的方式与风控对接。

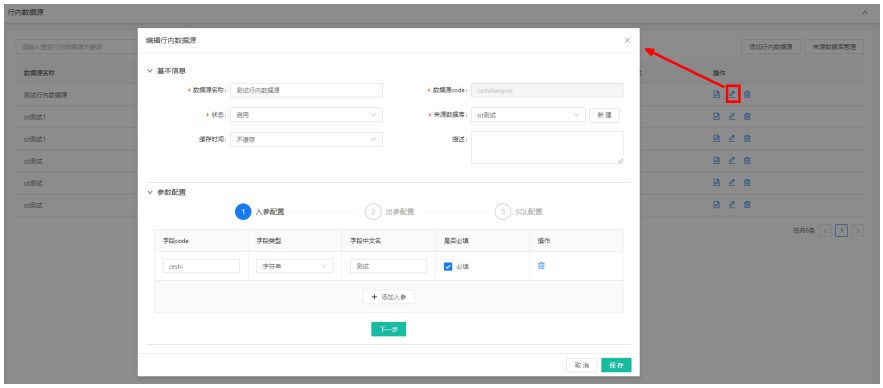
行内数据源的添加分为两部分，一部分为基本信息的输入；第二部分需要设置三方数据源的入参和出参，设置完即可在策略中使用。

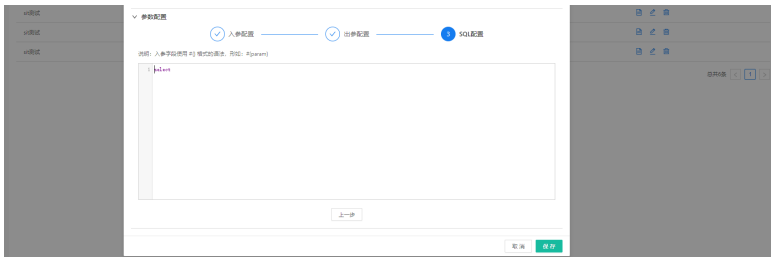
单击“行内数据源”菜单，进入页面，单击页面右上角“添加行内数据源”按钮；

在页面弹出框，依次填写数据名称、Code，选择状态、来源数据库、缓存时间，设置入参；



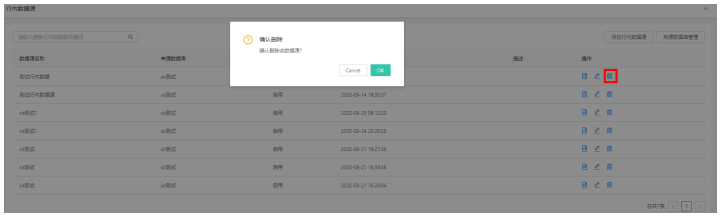
编辑：在行内数据源列表中，单击操作列的编辑“ ”按钮，弹出“编辑行内数据源”页面，除“数据源code”无法修改，其他数据都可以进行修改；





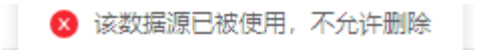
删除：在“行内数据”列表界面，单击操作列的删除“ ”按钮，弹出提示页面，如下图：

图 3-65 删除确认



单击【确定】删除成功，单击【取消】数据无变化；

如果该数据源已经被使用，则无法删除；需要解除该数据源的使用才可以删除；



c. 映射管理

无论是SAAS数据源还是行内数据源，在数据源添加到系统后，需要将数据源的入参与风控的字段做映射后才可使用。

新增映射：单击“映射管理”菜单，进入页面；列表中每条数据源的最右侧有操作栏，单击操作栏的“添加映射”操作，弹出“添加映射”页面；

添加映射时需设置映射名称、映射可见范围，将数据源的入参和系统字段进行映射，映射完成后即可在策略中使用此数据源；

依次输入“映射名称”，选择“所属部门”，选择“使用事件”，列表下方显示事件下的字段，选择字段后，单击“确定”按钮，完成字段映射。

图 3-66 字段映射 1

图 3-67 字段映射 2

编辑映射：在“映射管理”列表中，单击操作列的编辑“ ”按钮，弹出“编辑行内数据源”页面，除“数据源”和“所属部门”无法修改，其他数据都可以进行修改；

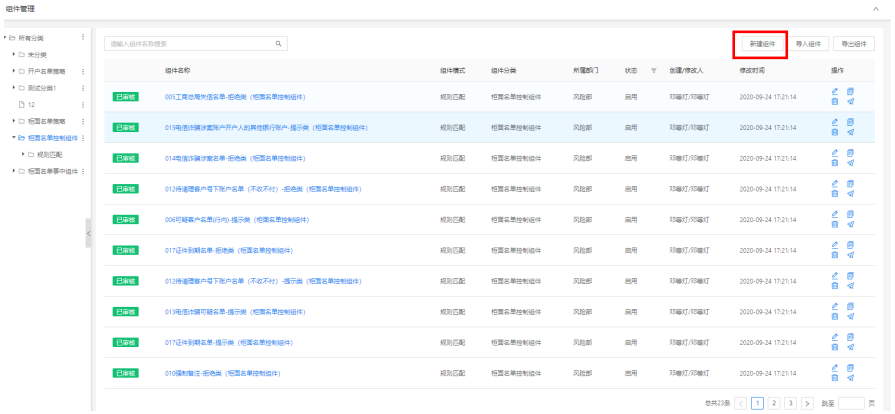
图 3-68 编辑映射

- **删除映射组件管理**

  组件可以在策略的条件、动作中使用，提升策略的配置效率，提高复用性。支持对组件进行新建、编辑、删除、复制、导入导出等操作。

  a. 新增：在“组件管理”列表界面，单击【新建组件】按钮，跳转到“新建组件”界面，如下图所示：

图 3-69 新建组件 1



依次输入组件名称，选择组件模式、组件分类、状态，配置条件与动作，最后单击“确定”按钮完成组件的创建。

图 3-70 新建组件 2

组件模式包括规则匹配、风险权重、自定义规则、评分卡、基础决策表、决策矩阵、决策树、规则、动作多种类型，操作员可根据业务需要选择对应的组件模式进行配置。

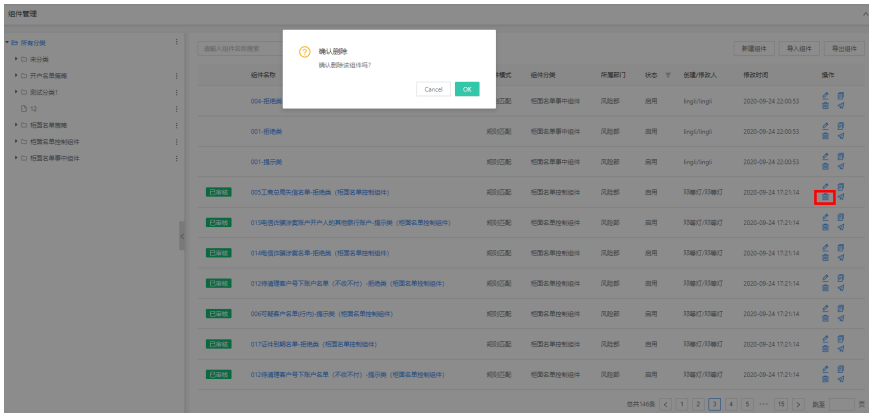
图 3-71 新建组件 3

b. 编辑：在“组件管理”列表中，单击操作列的编辑“ ”按钮，弹出“编辑组件”页面，除“组件模式”和“所属部门”无法修改，其他数据都可以进行修改；

图 3-72 编辑组件

c. 删除：在“组件管理”列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“您确认删除该组件？”

图 3-73 删除组件



- **策略管理**

  用户可根据业务需求自定义策略并对策略信息进行维护，支持按目录管理策略，可查看产品、事件、策略的层级关系，支持通过目录快速定位到策略及策略节点查看详情。

图 3-74 策略管理

新建策略时，可设置策略名称、所属产品和关联事件、优先级、状态、策略模式等基本信息和策略配置详情。也可通过复制功能复制已有的策略并在原策略的基础上进行修改生成新的策略。

图 3-75 开户策略

a. 新增策略

在“策略管理”列表界面，单击“新建策略”按钮，跳转到“新建策略”页面，如下所示：

图 3-76 策略管理-新建策略

图 3-77 新建策略

b. 编辑策略

在“策略管理”列表界面，每条策略数据的右侧，单击操作栏的编辑“ ”按钮，跳转到策略的编辑页面，如下所示：

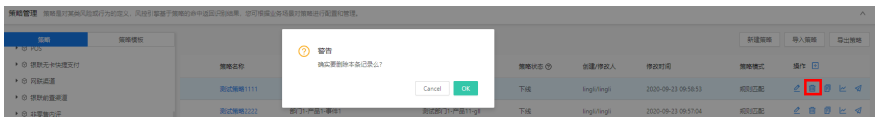
图 3-78 编辑策略 1

图 3-79 编辑策略 2

c. 删除策略

在“策略管理”列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“您确认删除该组件？”

图 3-80 删除策略警告



单击【取消】按钮，该指标数据无变化；单击【确定】按钮，指标，待删除的数据需要提交审核，审核通过，则删除成功；审核拒绝，则删除失败；

图 3-81 删除策略提示

d. 导入导出

支持将系统内的策略导出后进行同系统/跨系统导入。

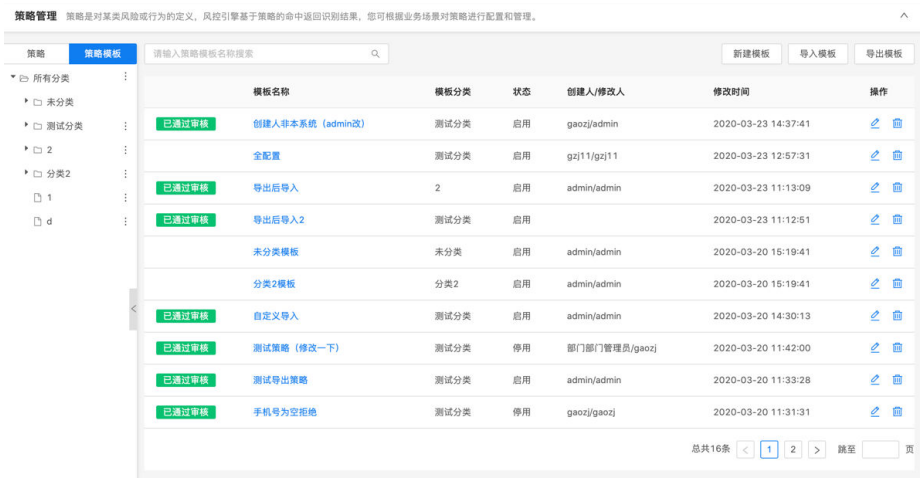
图 3-82 导出策略

导入时需上传导入文件、选择文件导入的产品和事件，确认导入数据（包括策略、字段、指标、外部数据、名单、函数、模型等）并审核通过后即可在系统中查看策略。

e. 策略模板

支持创建策略模板并对策略模板进行分类管理，支持单条、批量导入和导出策略模板。

图 3-83 策略模板

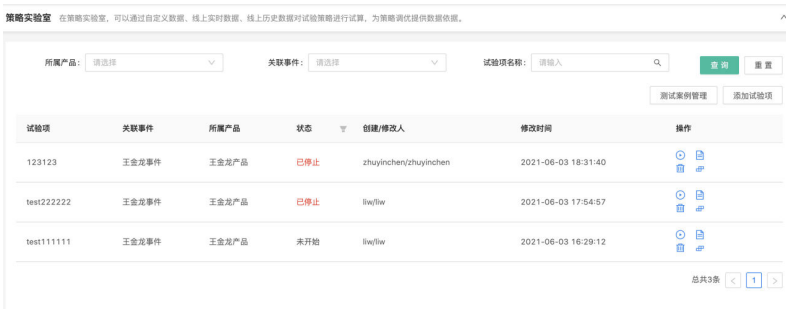


新建策略模板时，模板基本信息为必输项，规则信息和流程概览中的内容无需配置完整。在创建策略时可引用策略模板后，在此基础上进行完善，将策略配置完整。

- **策略实验室**

  策略实验室主要用于策略调优，实验室的策略支持用户手动新建，也可引用线上策略。调优后的策略可复制到线上去运行。

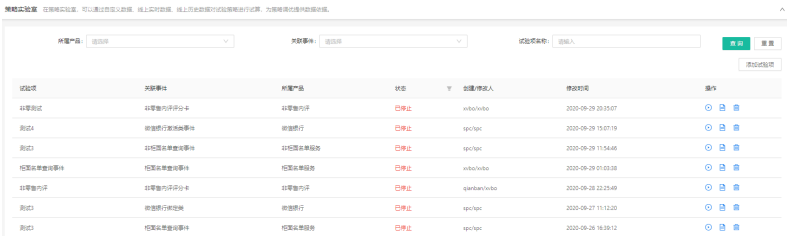
图 3-84 策略实验室



a. 查看实验

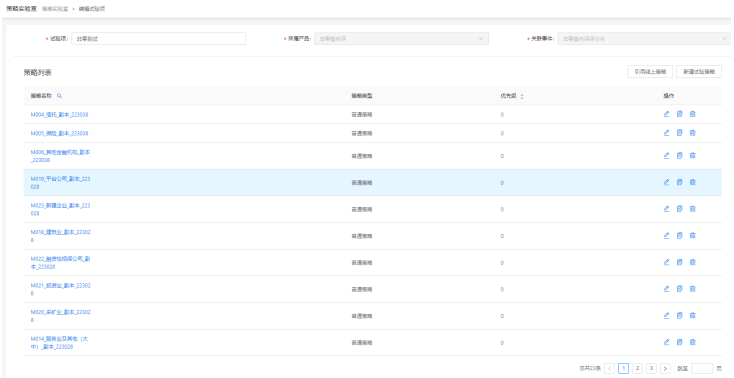
在“策略实验室”界面，支持根据策略的“所属产品”、“关联事件”、“试验项名称”条件进行筛选查询试验项；

图 3-85 试验项列表



在每条试验项的操作栏，单击“ ”按钮，可支持查看试验项下策略的详细信息；并支持查看、编辑和删除每条策略；也可支持“引用线上策略”和“新建试验策略”；

图 3-86 策略列表

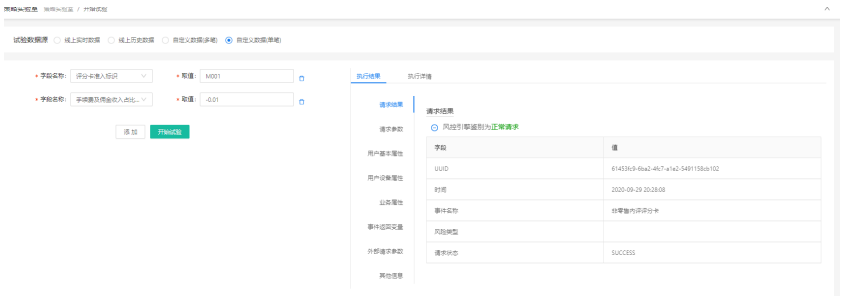


b. 开始实验

可在“策略实验室”界面，在试验列表中选择需要执行的试验项，并单击操作列的“ ”按钮，跳转到配置“试验数据源”页面；

支持选择线上实时数据、线上历史数据或自定义数据（多笔、单笔）、测试案例管理多种数据源对策略进行试验。查看试验结果时，操作员可选择不同的查询维度（策略、节点）查看不同的报表项，也支持查看试验策略的执行详情和决策结果。

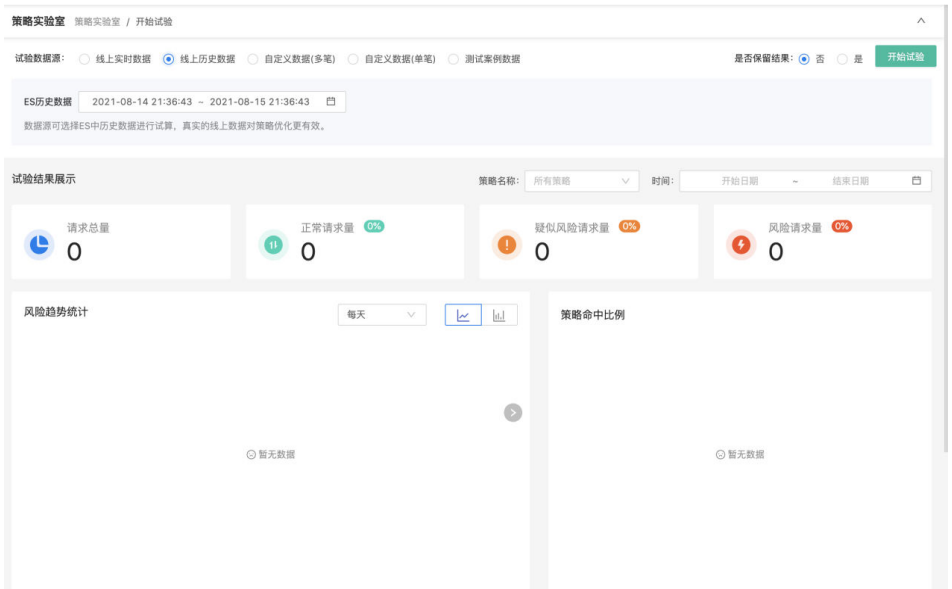
图 3-87 自定义数据



如果选择“线上数据”，单击【开始试验】按钮，即可查看线上数据在该试验项下的“风险趋势统计”和“执行详情”的情况；

选择是否保留结果（线上实时数据除外），可以保留本次结果的报告。在试验室列表可以查看试验结果。

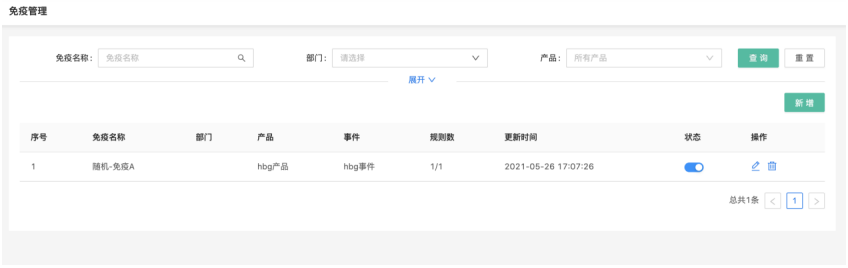
图 3-88 线上历史数据



免疫管理

对于已经风险较小的对象如名单、对公账号、事业单位账号等，在特定的策略和场景下，可以做免疫处理，减少无效预警，灵活适用于各业务场景，提高风控质量。目前免疫的结果是对流程退出以及节点退出动作进行免疫，可以让请求继续匹配其他风控策略。

图 3-89 免疫管理



单击新增，可以增加一条免疫信息。

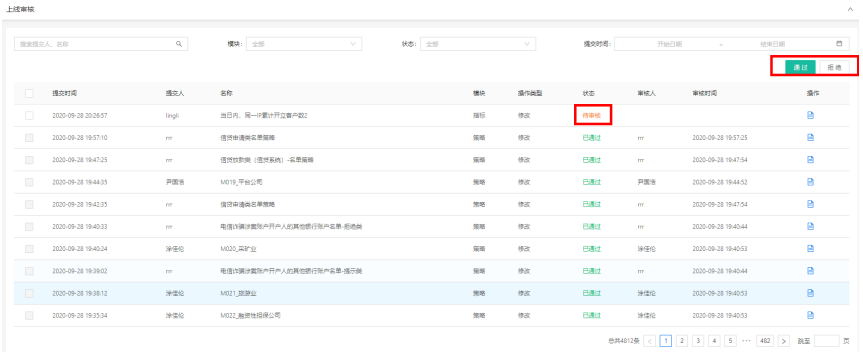
录入规则的基本信息，配置免疫规则，以及筛选出同事件下的免疫规则。

上线审核

为了保证线上业务的安全，所有策略在增删改的操作都需管理员审核通过后才能生效，如未通过则不予上线。

审核流程：单击“上线审核”菜单，进入页面；可以查看需要当前用户审核的数据；

图 3-90 上线审核



选择“待审核”的事件，勾选后，单击页面右上角【通过】，该数据状态变为“已审核”，完成审核操作；单击【拒绝】按钮，该数据的状态变为“未通过”，完成审核操作。

图 3-91 待审核处理

数据报表

- **请求趋势统计**

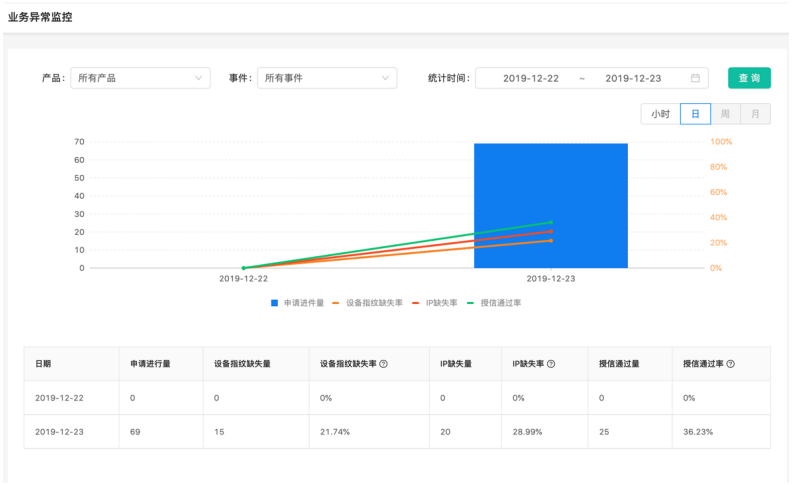
  展示总请求量、正常请求量、疑似请求量、风险请求量的趋势统计，最多可查询近180天的数据。支持不同时间段的请求趋势的对比和数据报表的导出操作。

图 3-92 请求趋势统计

- **业务异常统计**

  可查看请求总量、设备指纹缺失情况、IP缺失情况和策略通过情况。

图 3-93 业务异常监控



- **事件策略统计**

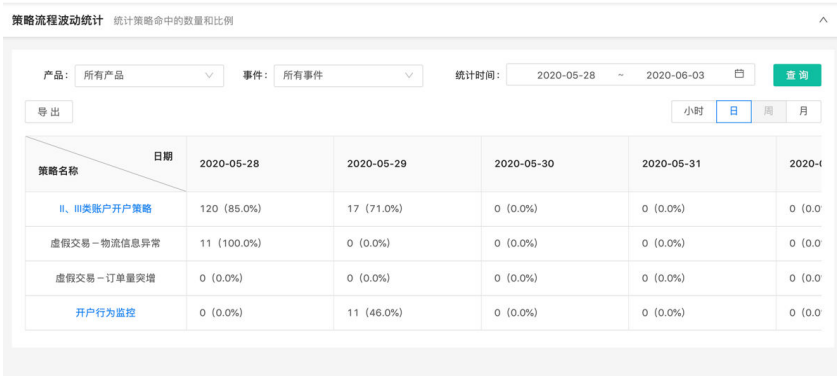
  可按事件查询近180天的请求分布情况，包括请求数、疑似风险数及占比，风险数及占比情况；也可从策略维度查询策略的触发率、命中情况、疑似风险、风险数等信息。查询结果支持导出。

图 3-94 事件策略统计

- **策略流程波动统计**

统计每个策略或策略节点的执行请求量，可按同事件下策略的执行顺序查看每个策略的执行量，也可按流程策略中节点的执行顺序查看每个节点的执行量；查询结果支持导出。

图 3-95 策略流程波动统计



- **规则命中统计**

  可查看每条规则的执行总量、通过总量、命中总量和命中率，查询结果支持导出。

图 3-96 规则命中统计

- **风险类型统计**

  统计风险请求对应的风险类型的命中情况，查询结果支持导出。

图 3-97 风险类型统计

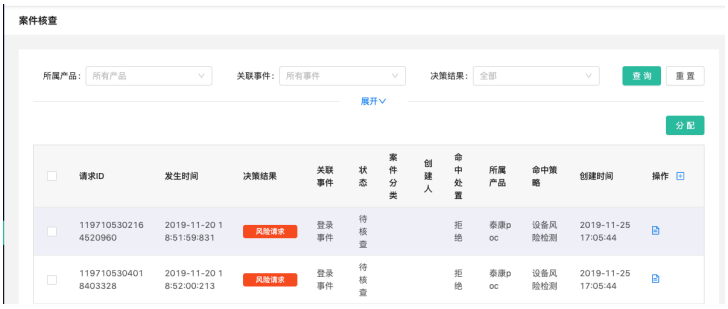
案件中心

在案件中心可以对风险请求进行人工核查，核查后可自动归档分类。

- **案件核查**

  反欺诈预警交易能够被有权用户领取或分配、风险审核全流程的管理。在发起事件审查申请时，经办人员可以审查页面填写审查意见、上传附件（佐证材料）。经办人员领取或接收到分配的审查任务后，在系统中可以在任务中查看待办任务。

图 3-98 案件核查



- **任务中心**

  他人分配给自己处理的案件，可以在任务中心查看。任务中心存放待办任务和已办任务。

- **风险案件库**

  经过结案的请求会自动归档到风险案件库，在风险案件库里可以看到结案的明细，包括分配人、分配时间、结案人、结案意见等信息。

图 3-99 风险案件库

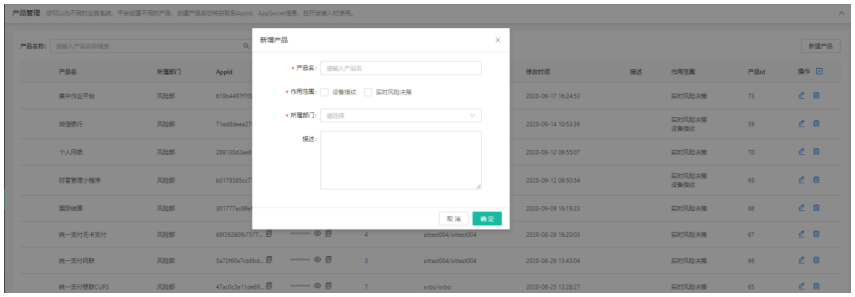
系统管理-产品管理

接入全景式业务风控系统的前提是需要先创建产品，系统会分配 appId和appSecret. 这两个参数标识一个应用，也贯穿整个风控体系，包括事件，字段，指标，策略等，就算是调用风控任何一个接口都需要对appId和appSecret进行鉴权。

- **新增**

  单击“新建产品”按钮，即可看到如下图所示的“新增产品”页，如下图所示：

  图 3-100 新增产品

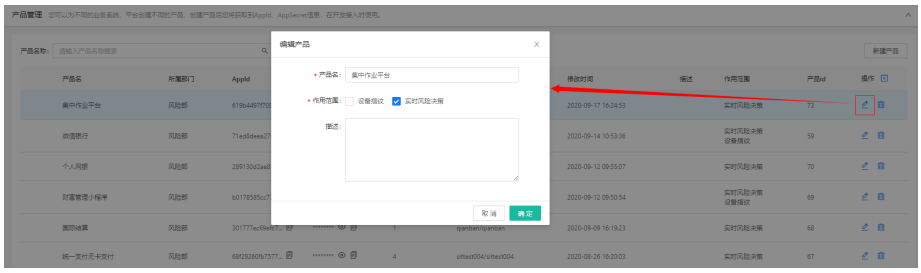
  

  依次填写产品的信息，单击“确定”按钮即可新增产品信息。

- **编辑**

  单击产品管理列表中的操作列的编辑“ ”按钮，即可进入“编辑产品”页面：

  图 3-101 编辑产品

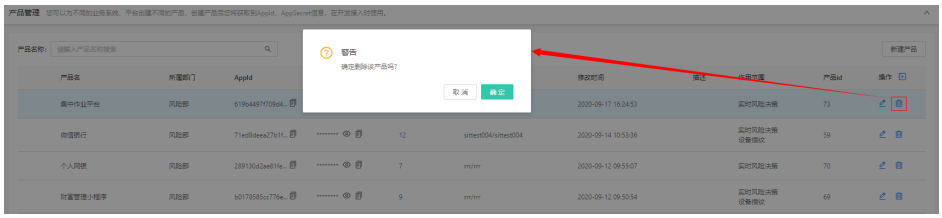
  

  在此页面中可对产品名、作用范围、描述进行编辑，单击“确定”即可将信息更新到该产品信息中，单击“取消”数据无变化。

- **删除**

在产品管理列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“确定删除该产品吗？”

图 3-102 删除产品



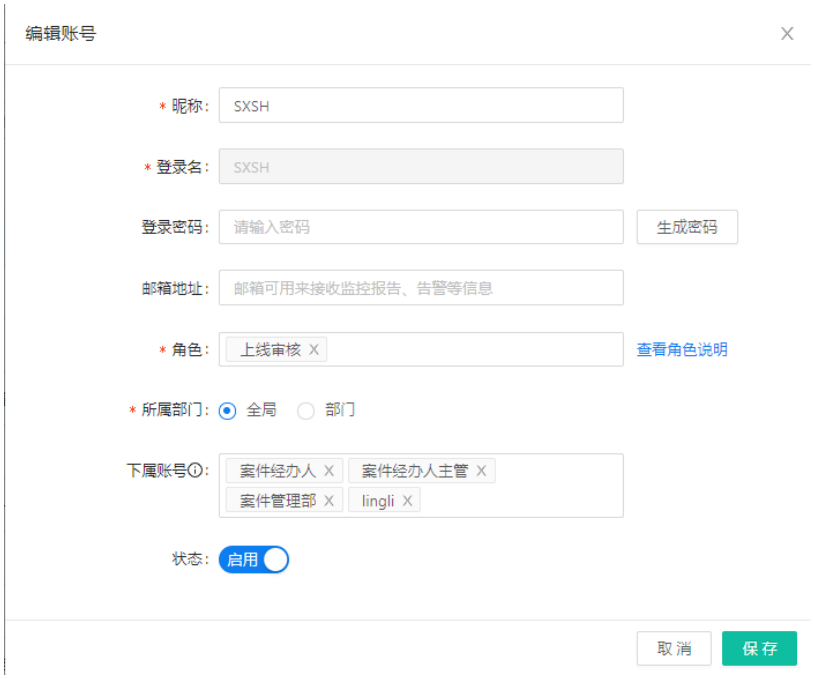
账号管理

- **查询：**账号管理列表默认按照最后登录时间倒序排序，可根据“账号昵称”、“所属部门”、“角色”进行查询；
- **新增：**系统管理员可以添加不同角色的账号，以方便不同业务部门登录风控平台进行相关操作。新增的账号默认为“启用”状态；

图 3-103 添加帐号

- **编辑：**在账号管理列表，单击操作列的编辑“ ”按钮，弹出编辑账号页面，可支持编辑昵称、登录密码、角色、所属部门、状态（启用/停用）等信息；其中登录名不可以编辑。单击“提交”按钮即可编辑成功；

图 3-104 编辑帐号



权限管理

在系统管理菜单下单击权限管理，打开权限管理列表页面，列表内容默认按照角色创建时间排列，可根据角色名称进行查询，支持对角色进行增、删、改、查的操作。

图 3-105 权限管理

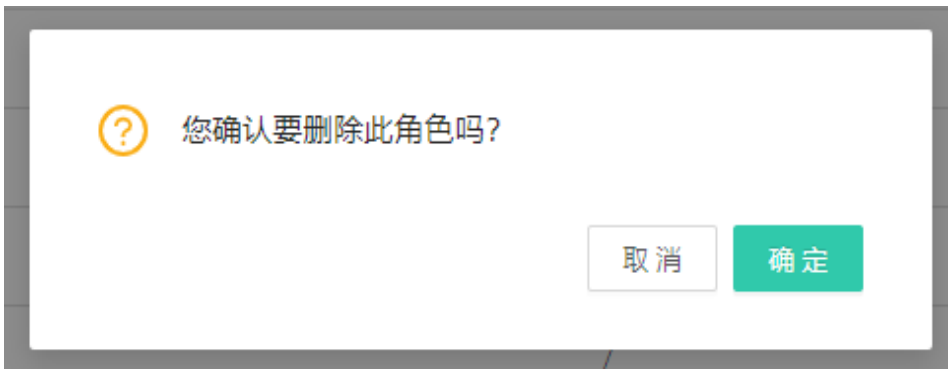
- **新增：**系统可内置角色，管理员可根据业务需要自定义新角色；
  a. 单击【添加角色】按钮，打开添加角色弹窗，输入角色名称并设置此角色的功能权限后，单击提交按钮即可成功创建角色；
  b. 角色名称为必输项且全局唯一，提交时需校验角色名称的唯一性，如果角色名称已存在，则提示“该角色名称已存在”；
  c. 角色的功能权限划分至页面按钮级别；

图 3-106 添加角色

一级菜单	子菜单	操作权限
总览	—	☐查看
监控中心	请求事件监控	☐查看
	设备采集监控	☐查看
	数据报告管理	☐查看 ☐添加 ☐编辑 ☐删除 ☐下载
	风险监控管理	☐查看 ☐添加 ☐编辑 ☐删除
	接口调用监控	☐查看
	应用节点监控	☐查看 ☐应用节点管理
	服务器性能监控	☐查看 ☐服务器管理
	中间件监控	☐查看
	监控报警管理	☐查看 ☐报警规则设置
案件中心	案件核查	☐查看 ☐分配 ☐结案
	任务中心	☐查看 ☐结案
	风险案件库	☐查看 ☐新增 ☐编辑 ☐删除
变量管理	字段管理	☐查看 ☐添加 ☐编辑 ☐删除 ☐批量导入 ☐分类管理
	名单管理	☐查看 ☐添加 ☐编辑 ☐删除 ☐导出
	函数管理	☐查看 ☐添加 ☐编辑 ☐删除 ☐分类管理
	风险类型管理	☐查看 ☐添加 ☐编辑 ☐删除
	指标调用统计	☐查看
	指标定义	☐查看 ☐添加 ☐编辑 ☐删除 ☐分类管理
	计算方式管理	☐查看 ☐添加 ☐编辑 ☐删除
	模型仓库	☐查看 ☐导入 ☐调试 ☐编辑 ☐删除 ☐下载 ☐服务器管理
	模型仪表盘	☐查看
	模型映射	☐查看参数 ☐查看映射 ☐添加映射 ☐编辑映射 ☐删除映射
	三方数据源	☐查看 ☐添加 ☐编辑 ☐删除 ☐数据源类型管理
	行内数据源	☐查看 ☐添加 ☐编辑 ☐删除 ☐来源数据库管理
	映射管理	☐查看参数 ☐查看映射 ☐添加映射 ☐编辑映射 ☐删除映射
	数据调用统计	☐查看
策略中心	事件管理	☐查看 ☐添加 ☐编辑 ☐复制
	组件/动作模板管理	☐查看 ☐添加 ☐编辑 ☐删除 ☐复制 ☐导入导出 ☐分类管理 ☐版本管理
	策略管理	策略：☐查看 ☐添加 ☐编辑 ☐删除 ☐复制 ☐导入导出 ☐版本管理 ☐趋势图 策略模板：☐添加 ☐编辑 ☐删除 ☐导入导出 ☐分类管理
	策略实验室	☐查看 ☐添加 ☐编辑 ☐删除 ☐开始试验 ☐复制
上线审核	—	☐查看 ☐审核
数据报表	请求趋势统计	☐查看 ☐导出
	业务异常统计	☐查看 ☐导出
	事件策略统计	☐查看 ☐导出
	策略流程波动统计	☐查看 ☐导出
	规则命中统计	☐查看 ☐导出
	风险类型统计	☐查看 ☐导出
设备指纹	数据统计	☐查看
	设备分析	☐查看
	设备画像	☐查看
无感验证	渠道管理	☐查看 ☐添加 ☐编辑 ☐删除 ☐场景配置 ☐数据统计
	场景管理	☐查看 ☐场景配置 ☐数据统计
	外观管理	☐查看 ☐外观自定义 ☐图集管理
	数据统计	☐查看
系统管理	产品管理	☐查看 ☐添加 ☐编辑 ☐删除
	账号管理	☐查看 ☐添加 ☐编辑 ☐删除
	权限管理	☐查看 ☐添加 ☐编辑 ☐删除
	部门管理	☐查看 ☐添加 ☐编辑 ☐删除
	许可授权	☐查看
	邮箱服务	☐查看

- **编辑：**单击角色列表中操作列的【 编辑 】按钮，可打开角色编辑弹窗，支持修改角色名称和调整功能权限；
- **删除：**单击角色列表中操作列的【 删除 】按钮，弹窗提示“您确认要删除此角色吗？”，单击确定后判断是否有账号正在使用此角色，如果有账号正在使用此角色则提示“有账号正在使用该角色，暂时无法删除”，如果账号正在使用此角色则可成功删除；

图 3-107 删除角色确认



说明

系统内置的角色不允许删除

许可授权

许可授权页面可以查询决策引擎的有效期，以及更新相关的授权文件。

图 3-108 许可授权

邮箱服务

权限管理模块只对系统里的监控告警、数据报告等模块具有发送告警邮件、发送数据报告邮件等功能，在使用前需对邮箱服务器进行设置，在此模块可对邮箱进行设置。

图 3-109 邮箱服务器设置

部门管理

超级管理员可访问此模块，创建不同的部门。不同部门的产品、事件、字段、指标、策略等数据，相对独立，仅限于本部门员工可见，但名单、风险类型、函数、模型等数据所有部门可以共享。

图 3-110 部门管理

- **新增：**单击“添加部门”按钮，即可看到如下图所示的“添加部门”页，如下图所示：

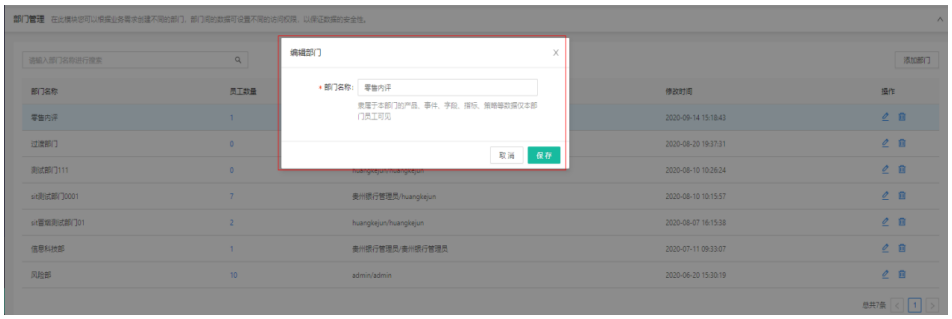
  图 3-111 添加部门

  填写部门名称信息，单击“确定”按钮即可新增部门信息。

- **编辑：**单击部门管理列表中的操作列的编辑“ ”按钮，即可进入“编辑部门”页面：

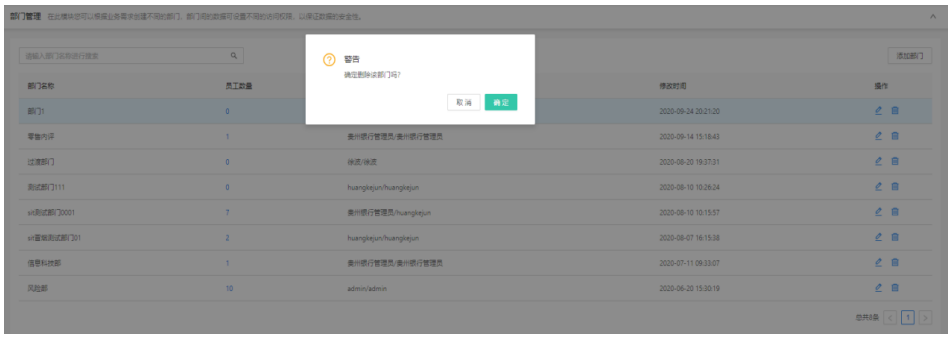
图 3-112 编辑部门



在此页面中可对部门名进行编辑，单击“确定”即可将信息更新到该产品信息中，单击“取消”数据无变化。

- **删除：**在产品管理列表中，单击操作列的删除“ ”按钮，弹出警告，并给出提示“确定删除该部门吗？”单击“取消”按钮，该数据不做任何操作，单击“确定”按钮，删除该部门信息，并给出提示“删除成功”；

图 3-113 删除部门

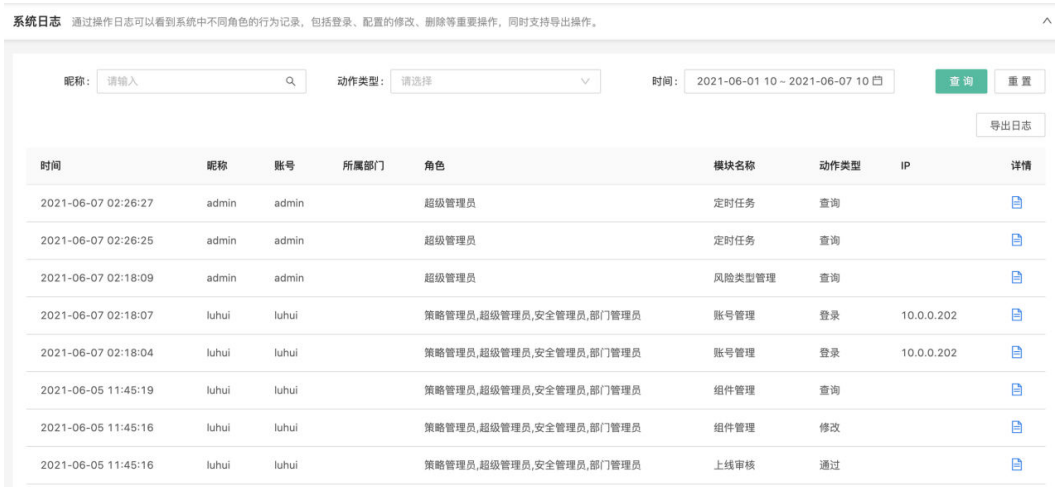


系统日志

系统日志记录了各角色在系统上的操作记录。

可以查看详情和导出日志。

图 3-114 系统日志



3.4 态势

大盘

威胁感知大盘展示当前自然日的威胁感知数据，威胁感知大盘分为首屏、次屏和设备屏，可自定义设置首、次屏的展示数据、刷新频率和切换频率。

图 3-115 风险大盘设置

态势概览展示

态势概览模块默认展示近7天的风险数据，包括请求趋势、策略、规则趋势、风险事件等维度报表。特别是策略命中排行等维度数据可以为业务人员提供感知策略调优数据依据。

支持通过“产品”、“事件”和“统计时间”查询风险请求、风险命中情况、产品/事件命中情况、策略命中情况、节点命中情况、规则命中情况、风险类型命中情况多个维度的统计报表。

监控中心-态势监控

- **态势请求监控**
  a. 查询：查询系统的风险识别日志，及时了解业务系统的风险情况和定位风险源头及数据回放，查看策略的执行结果，支持通过各类查询条件组合进行筛选。

     通过设置查询条件，可从不同维度对请求结果进行筛选，查询结果列表的展示会随查询条件的维度而变化，可从请求、策略、节点、规则等维度展示列表信息，也支持设置高级查询条件。
  b. 导出数据：在态势请求监控页面，单击【 导出数据 】按钮，可批量或单个导出请求事件；

     勾选事件后，再次单击【 导出数据 】按钮，可以选择需要到导出数据的明细，根据实际业务需要，勾选需要导出的数据信息；

- **态势报告管理**

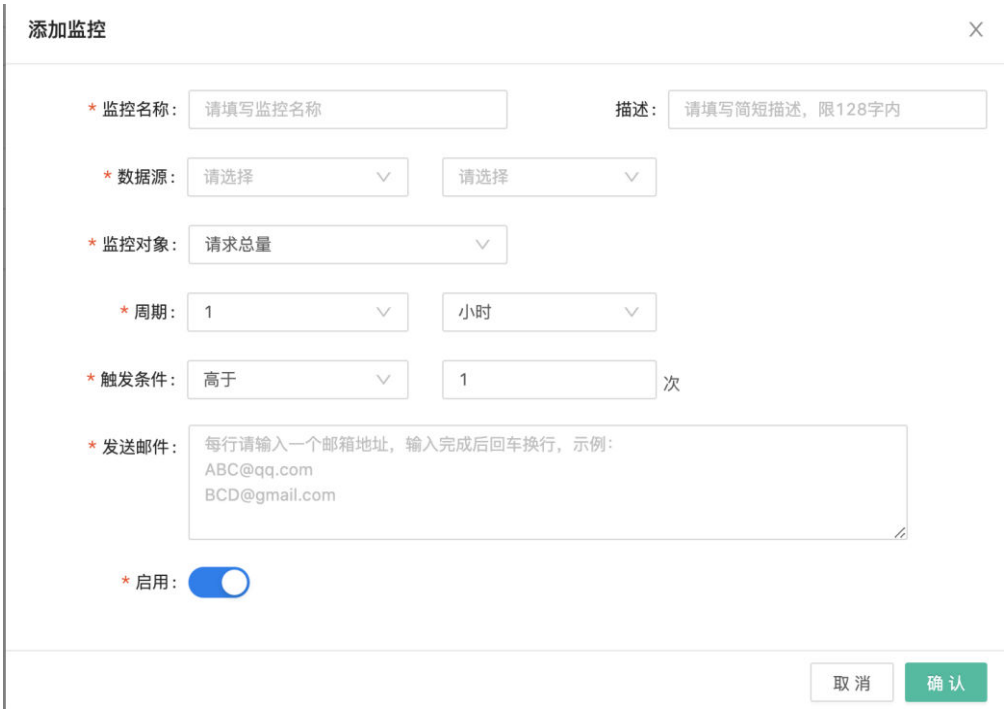
  系统可以自动发送设置周期内的风险报告邮件，可以不通过访问态势概览，通过邮件了解日常风险情况，报告的维度包括风险趋势、风险分类占比、每日风险详情。

  图 3-116 添加数据报告

- **态势监控报警**

  该功能支持对不同产品、事件下的业务情况进行监控，包括请求总量、正常请求量、风险请求量、疑似风险请求量进行监控，可以按分钟、小时、天进行高于、低于等百分比进行监控设置，超过设定的条件后，系统将发送报警通知到设定的邮箱。

图 3-117 添加监控



数据赋能管理

- **字段管理**

  字段是用于判断和识别风险的最小单位，例如ID、IP地址、 账号、设备指纹等，配置指标、策略时都将用到字段。

  支持批量导入或手动新增字段，手动新建/编辑字段时，可使用函数计算公式，使用复杂表达式定义函数字段。

  系统内已有预置分类，也可单击“字段分类管理”创建自定义分类，在规则中使用字段时可通过分类筛选字段，方便选择。

  手动新增字段：在字段管理页面单击“添加字段”按钮，弹出添加字段页面，依次填写字段的信息。

- **名单管理**

  用户可以自定义名单并上传数据，名单数据支持增删改查的操作，在策略中可以使用名单数据。

  a. 添加名单

  单击名单管理列表右上方的“添加名单”，弹出“添加名单”页面，如下图所示：

  图 3-118 添加名单

图 3-119 添加名单成功提示

名单中的数据可选择手动录入或批量上传，名单数据具有有效期的属性，可根据实际需求设置某些数据的有效起止日期。

b. 添加名单数据-文件上传

根据“模板文件”示例，添加名单数据在文件中，并导入到系统中即可批量上传名单数据；

图 3-120 本地上传名单数据

c. 添加名单数据-手动录入

可手动逐条添加名单数据信息，并可约束名单数据的效期；

图 3-121 手动录入名单数据

- **函数管理**

可管理系统中的函数，支持增、删、改、查操作。

单击函数管理列表右上方的“新建函数”，弹出“新增函数”页面，实现方式为函数组合：通过常量、函数和参数的组合配置生成新函数;

图 3-122 新建函数

实现方式为groovy脚本：输入脚本生成新函数；脚本语言可使用java语言进行实现；

所有函数为全部部门可见，添加函数时无需选择函数的所属部门;

单击“提交”按钮，函数新增成功，单击“取消”按钮，数据无变化；

图 3-123 新建函数提交

- **风险类型管理**

  根据业务场景定义不同的风险类型并在策略中使用，命中后可在态势概览里根据风险类型来查询风险分类趋势。可管理系统中的风险类型，支持增、删、改、查操作。

  在风险类型管理，单击“添加风险类型”按钮，输入分类名称后即可自定义风险分类；

- **指标特征**

  可管理系统中的指标，查看指标的调用统计，新建指标计算方式。

  a. 指标调用统计：

  定义完成的指标有数据接入后，在此模块就可以看到指标的调用统计信息，包括指标调用趋势图、调用排行、接口调用量等信息。

  单击“指标调用统计”菜单，进入页面，系统默认展示进7天的数据；

  在页面上可支持对指标的“统计时间”、“产品名称”、“事件名称”筛选条件进行查询；

  其中筛选条件如果不选择，则“统计时间”默认本周的数据，“产品名称”和“事件名称”默认所有；

  指标的调用统计包括：指标调用总量、指标计算量、指标取值量，调用趋势图，指标调用排行等数据。

  b. 指标特征定义

  在指标特征定义页面，单击“添加指标”按钮，弹出“添加指标”页面；

  新建指标时，需选择指标的计算事件；

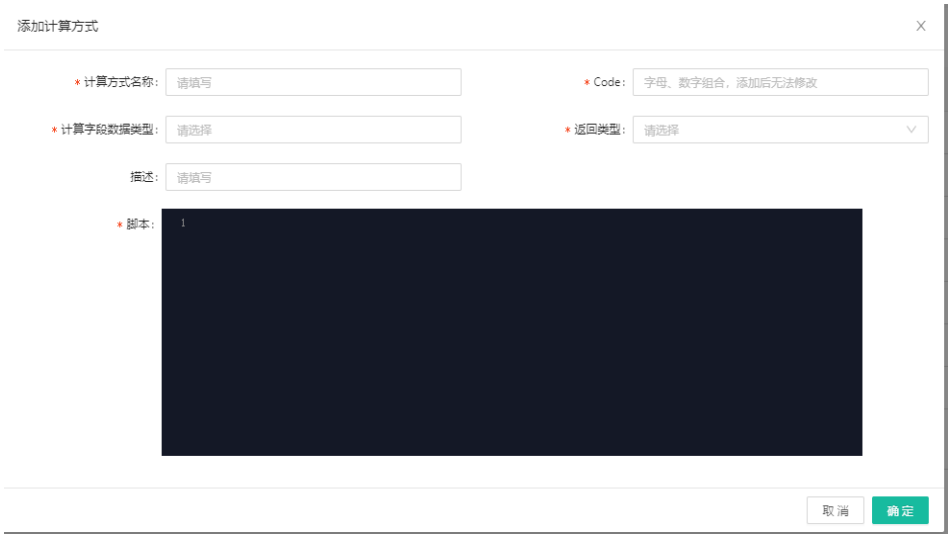
  目前系统内置了统计、求和、求平均、求关联、历史指标、最大值、最小值、标准差、频次排行等计算方式，可根据业务场景在配置时进行选择。

  c. 计算方式管理

  计算方式是指标里使用到的，系统里内置了常用的关联、统计、方差等计算方式，在此功能模块可以对系统内置的计算方式和新建的计算方式来查询。

  计算方式是指标里使用到的，系统里内置了常用的关联、统计、方差等计算方式，也支持自定义计算方式，在“计算方式管理”界面，单击【添加计算方式】按钮，弹出如下图：

图 3-124 添加计算方式



在页面弹出框，依次填写计算方式名称、Code、数据类型、返回类型、描述、脚本，单击“确定”按钮完成指标的定义，添加后即时生效。数据聚合可管理外部数据和管理外部数据映射，支持对外部数据及其映射进行增、删、改、查的操作。

- **数据聚合**

  a. 三方数据源

  列表展示已添加的所有三方数据源，支持查看、编辑、删除和添加新的三方数据源。

  在“三方数据源”的列表中，单击【添加三方数据源】按钮，可设置数据源的基本信息、计费方式、费用和参数等。

  外部数据创建完成后可添加映射，将外部数据的入参与系统内的字段进行映射，映射完成后可在策略中使用此外部数据。

图 3-125 入参配置

图 3-126 出参配置

b. 行内数据源

列表展示已添加的所有行内数据源，支持查看、编辑、删除和添加新的行内数据源。

图 3-127 行内数据源

新增行内的数据源可以通过添加数据源的方式与系统对接。

行内数据源的添加分为两部分，一部分为基本信息的输入；第二部分需要设置三方数据源的入参和出参，设置完即可在策略中使用。

单击“行内数据源”菜单，进入页面，单击页面右上角“添加行内数据源”按钮；

在页面弹出框，依次填写数据名称、Code，选择状态、来源数据库、缓存时间，设置入参；

图 3-128 添加行内数据源

c. 映射管理

无论是SAAS数据源还是行内数据源，在数据源添加到系统后，需要将数据源的入参与系统的字段做映射后才可使用。

单击“映射管理”菜单，进入页面；列表中每条数据源的最右侧有操作栏，单击操作栏的“添加映射”操作，弹出“添加映射”页面；

添加映射时需设置映射名称、映射可见范围，将数据源的入参和系统字段进行映射，映射完成后即可在策略中使用此数据源；

依次输入“映射名称”，选择“所属部门”，选择“使用事件”，列表下方显示事件下的字段，选择字段后，单击“确定”按钮，完成字段映射。

图 3-129 字段映射

在数据源添加到系统后，需要将数据源的入参与系统中字段做映射后才可使用；每个数据源下可能有多个映射。

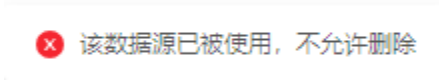
编辑映射：在“映射管理”列表中，单击操作列的编辑“ ”按钮，弹出“编辑行内数据源”页面，除“数据源”和“所属部门”无法修改，其他数据都可以进行修改；

删除映射：在列表中每条“数据源”的最右侧有操作栏，单击操作栏的“ ”按钮，再单击每条“映射数据”操作栏的删除“ ”按钮；，如下图：

图 3-130 删除映射警告

单击【取消】数据无变化，单击【确定】，该数据提交到“上线审核”流程，审核通过，则删除成功；审核拒绝，则删除失败；

如果该数据源已经被使用，则无法删除，并弹出提示信息，如下图：



d. 数据调用统计

支持查看数据调用情况，查看调用次数、查得率、调用成本等统计图及数据调用详情的列表展示。

单击“数据调用统计”菜单，进入页面；

页面上默认展示近30天的数据，同时可以通过统计范围、数据源名称、统计时间查询三方数据源、行内数据源的调用情况。

防御策略管理

- **事件管理**

  单击“事件管理”菜单，进入页面；在页面右上角，单击“添加事件”按钮，弹出“添加事件”页面；

  依次选择所属产品，输入事件名、Code，填写描述，设置事件下的关联字段、指标、风险类型、外部数据映射、模型映射。

  最后单击“确定”按钮完成事件的创建。

- **策略配置**

  用户可根据业务需求自定义策略并对策略信息进行维护，支持按目录管理策略，可查看产品、事件、策略的层级关系，支持通过目录快速定位到策略及策略节点查看详情。

  新建策略时，可设置策略名称、所属产品和关联事件、优先级、状态、策略模式等基本信息和策略配置详情。也可通过复制功能复制已有的策略并在原策略的基础上进行修改生成新的策略。

  执行条件：满足条件时才会执行策略。

- **策略实验室**

策略实验室主要用于策略调优，实验室的策略支持用户手动新建，也可引用线上策略。调优后的策略可复制到线上去运行。

开始实验：

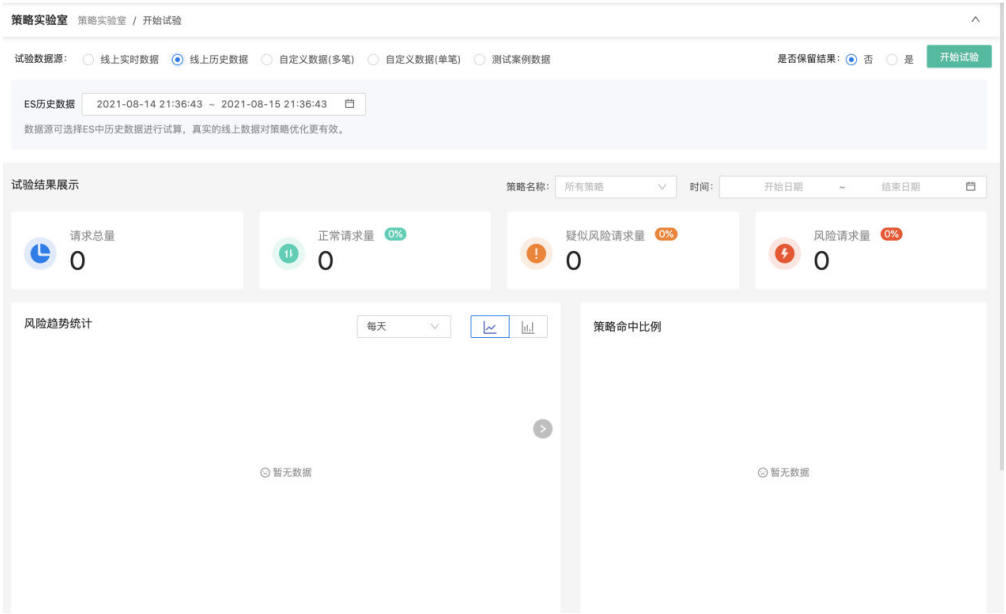
可在“策略实验室”界面，在试验列表中选择需要执行的试验项，并单击操作列的“ ”按钮，跳转到配置“试验数据源”页面；

支持选择线上实时数据、线上历史数据或自定义数据（多笔、单笔）、测试案例管理多种数据源对策略进行试验。查看试验结果时，操作员可选择不同的查询维度（策略、节点）查看不同的报表项，也支持查看试验策略的执行详情和决策结果。

如果选择“线上数据”，单击【开始试验】按钮，即可查看线上数据在该试验项下的“风险趋势统计”和“执行详情”的情况；

选择是否保留结果（线上实时数据除外），可以保留本次结果的报告。在试验室列表可以查看试验结果。

图 3-131 策略实验室



统计报表

- **态势请求统计：**展示总请求量、正常请求量、疑似请求量、风险请求量的趋势统计，最多可查询近180天的数据。支持不同时间段的请求趋势的对比和数据报表的导出操作。
- **策略命中统计：**统计每个策略或策略节点的执行请求量，可按同事件下策略的执行顺序查看每个策略的执行量，也可按流程策略中节点的执行顺序查看每个节点的执行量；查询结果支持导出。
- **风险类型统计：**统计风险请求对应的风险类型的命中情况，查询结果支持导出。

设备指纹

- **数据统计**

  数据统计展示昨日设备指纹的请求量，昨日有风险的设备请求量及设备请求趋势图，同时支持对近7天、近30天等时间范围的查询。

图 3-132 数据统计

在页面下方对查询时间内的数据通过列表的方式进行了详细的展示，包括总请求量、Web、iOS、Android请求量及各端的风险量情况。

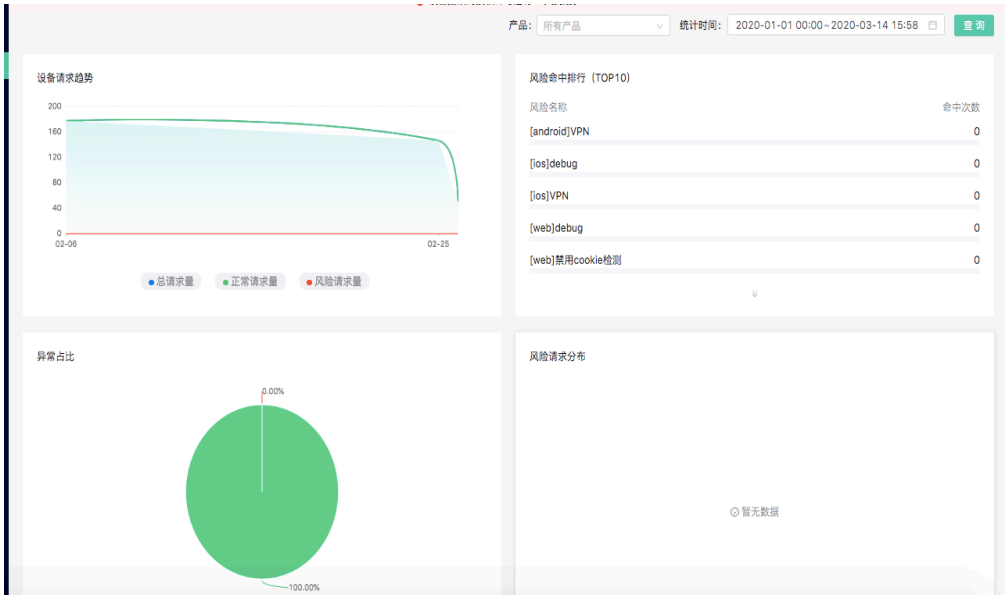
图 3-133 数据统计列表

时间	总请求量	Web请求量	iOS请求量	Android请求量	总风险量	Web风险量	iOS风险量	Android风险量
2019-07-11 09:00	1	1	0	0	0	0	0	0
2019-07-11 10:00	9	9	0	0	0	0	0	0
2019-07-11 11:00	40	40	0	0	0	0	0	0
2019-07-11 12:00	1	1	0	0	0	0	0	0
2019-07-11 14:00	19	19	0	0	0	0	0	0
2019-07-11 15:00	6	6	0	0	0	0	0	0

- **风险分析**

  风险分析模块默认展示当前自然日的设备请求趋势、风险命中排行、异常占比、风险请求分布，并支持按不同应用、请求时间来查询。

图 3-134 风险分析



在页面下方以列表的形式展示每个时间段内不同风险标签的命中情况。

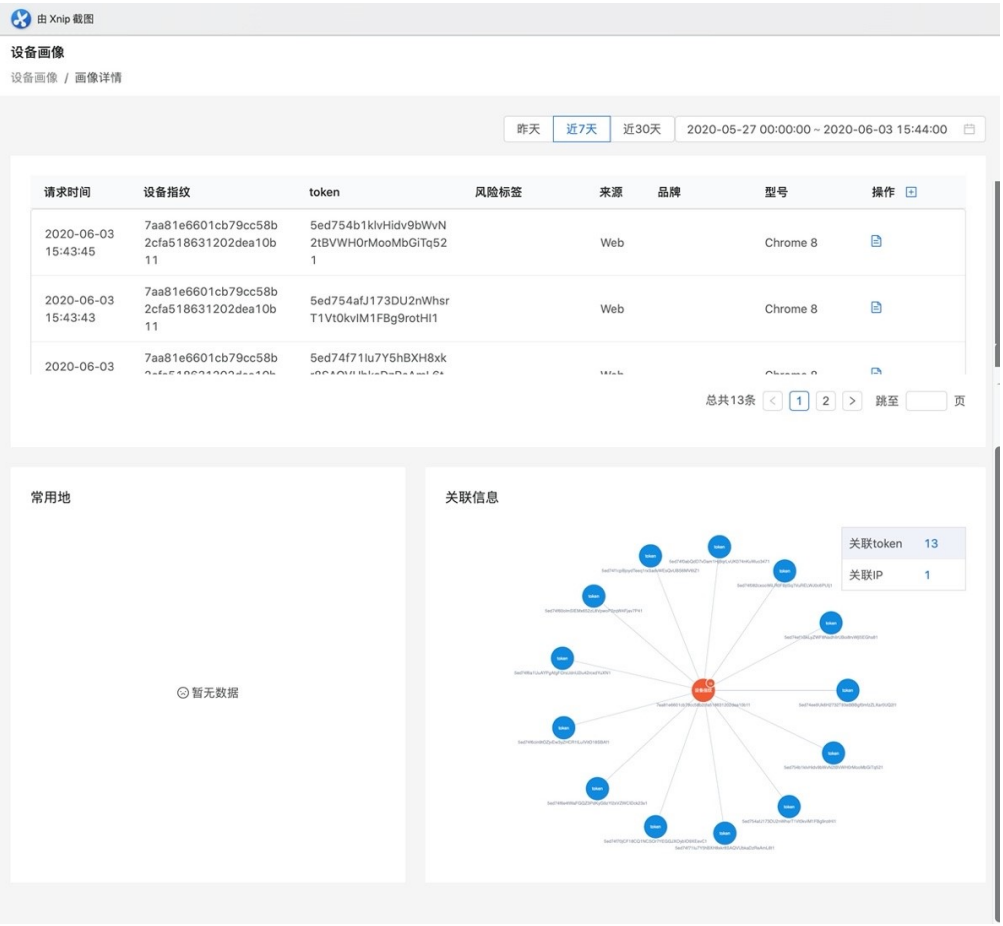
图 3-135 风险命中数据列表

时间	总请求数	正常请求数	风险请求数	模拟器	调试	越狱/root	代理IP	操作
2020-02-06 00:00:00	177	177	0	Android：0 iOS：0 web: 0	Android：0 iOS：0 web: 0	0/0	Android：0 iOS：0 web: 0	
2020-02-25 00:00:00	146	146	0	Android：0 iOS：0 web: 0	Android：0 iOS：0 web: 0	0/0	Android：0 iOS：0 web: 0	
2020-02-26 00:00:00	50	50	0	Android：0 iOS：0 web: 0	Android：0 iOS：0 web: 0	0/0	Android：0 iOS：0 web: 0	
汇总	373		0	Android: iOS: web:	Android: iOS: web:	undefined/undefined	Android: iOS: web:	

- **设备画像**

  在设备画像模块支持按设备指纹、设备指纹token来查询设备的画像，设备画像包括设备的基础属性、近期行为属性、近七日常用地，近七日关联信息。

图 3-136 设备画像



系统管理

- **产品管理**

系统的前提是需要先创建产品, 系统会分配 appId和appSecret. 这两个参数标识一个应用, 如事件, 字段, 指标, 策略等, 就算是调用任何一个接口都需要对appId和appSecret进行鉴权。

根据产品名称可在搜索框中输入需要查询的产品，单击搜索图标或者按下键盘的“Enter”键进行搜索，产品支持模糊查询，如果在查询框不输入任何产品名称，默认加载所有产品记录。

在产品管理列表中，单击操作列的右侧的加号“ ”按钮，可以对产品的查询列表进行自定义设置，以便更清晰的查询产品的相关信息。

- **账号管理**

  账号管理列表默认按照最后登录时间倒序排序，可根据“账号昵称”、“所属部门”、“角色”进行查询；

  系统管理员可以添加不同角色的账号，以方便不同业务部门登录平台进行相关操作。新增的账号默认为“启用”状态；

  角色右侧单击“查看角色说明”可以查看所有角色对应的权限信息；

  角色支持选择多个，以多个角色的并集作为该账号的权限配置

  输入账号相关信息，其中“登录密码”的管理员可以自己设定也可以单击“生成密码”，系统自动生成密码；单击“提交”即可添加成功该账号信息；

- **权限管理**

  在系统管理菜单下单击权限管理，打开权限管理列表页面，列表内容默认按照角色创建时间排列，可根据角色名称进行查询，支持对角色进行增、删、改、查的操作。

- **部门管理**

  超级管理员可访问此模块，创建不同的部门。不同部门的产品、事件、字段、指标、策略等数据，相对独立，仅限于本部门员工可见，但名单、风险类型、函数、模型等数据所有部门可以共享。

- **系统日志**

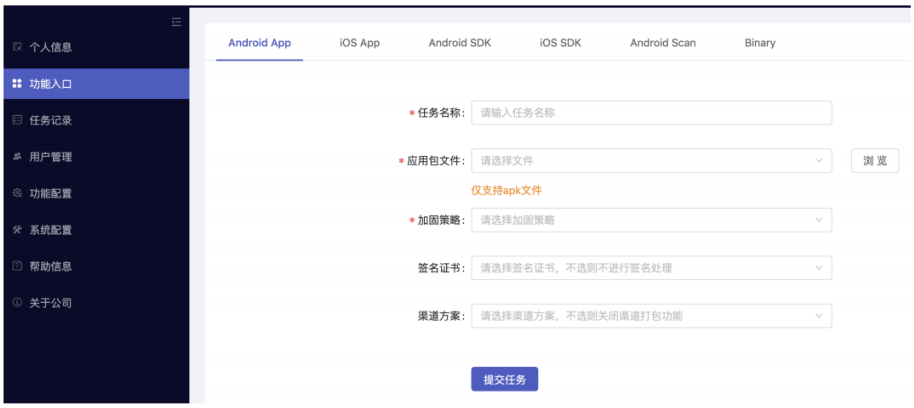
  系统日志记录了各角色在系统上的操作记录。可以查看详情和导出日志。

3.5 加固

功能入口

- **Android App加固**

图 3-137 Android App 加固



功能说明：

任务名称：输入可作为标识的字符，区别不同的任务；

应用包文件：APK文件；

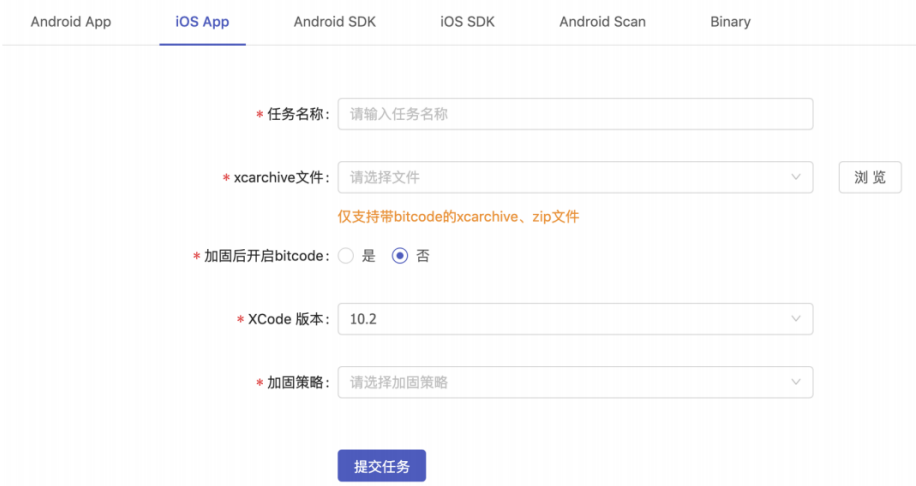
加固策略：选择指定的加固策略

签名证书：加固后，是否采用的特定签名证书进行签名（可选），详细的配置说明见后面章节；

渠道方案：加固后，是否使用指定的渠道方案进行多渠道打包输出（可选)，详细的配置说明见后面章节；

- **iOS App加固**

图 3-138 iOS App 加固



功能说明：

任务名称：输入可作为标识的字符，区别不同的任务；

xcarchive文件：带bitcode的xcarchive包；加固后是否开启bitcode：加固后是否带bitcode；

XCode版本：选择编译xcarchive的XCode版本；

加固策略：选择指定的加固策略

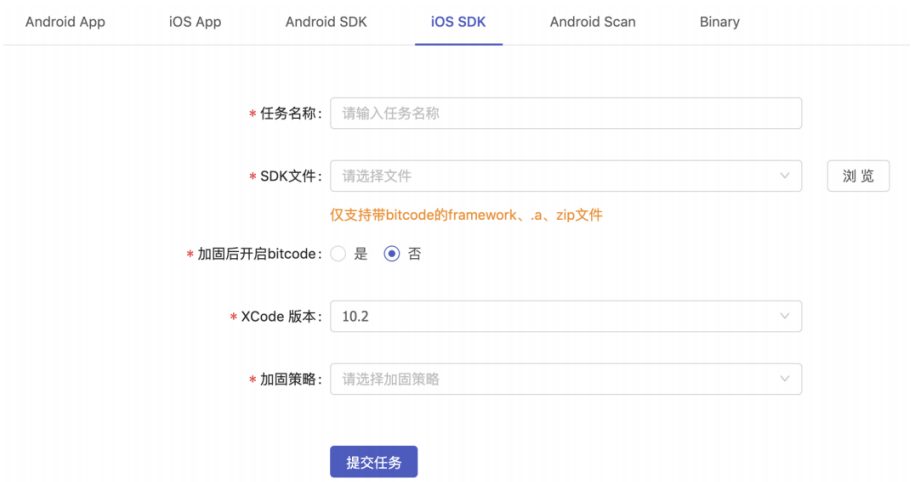
- **Android SDK加固**

图 3-139 Android SDK 加固

功能说明：
任务名称：输入可作为标识的字符，区别不同的任务；
SDK文件：AAR或JAR文件；
SDK关键类：选择需要保护的类范围；
SDK入口类: SDK最早被调用的类；
加固策略：选择指定的加固策略；

- **iOS SDK加固**

图 3-140 iOS SDK 加固



功能说明：
任务名称：输入可作为标识的字符，区别不同的任务；
xcarchive文件：带bitcode的xcarchive包；
加固后是否开启bitcode：加固后是否带bitcode；

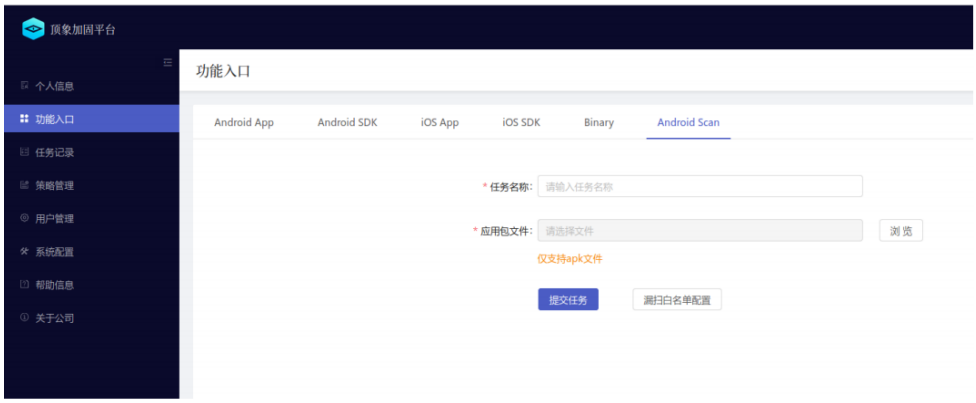
XCode版本：选择编译xcarchive的XCode版本；

加固策略：选择指定的加固策略

- **Android Scan 应用漏扫**

  系统支持Android应用漏洞自动化扫描功能，扫描完成后输出PDF格式的审计报告。 用户可以选择“Android Scan”选项卡，如下图所示

图 3-141 Android Scan 应用漏扫



功能说明：

任务名称：输入可作为标识的字符，区别不同的任务；应用包文件：APK文件；

- **Binary加固**

图 3-142 Binary 加固

功能说明：

任务名称：输入可作为标识的字符，区别不同的任务；

二进制文件：So, 或者包含So的压缩包，或者AAR包；

模式：指定Android还是Linux平台；

SDK入口类: SDK最早被调用的类；

防静态分析：对抗主流的静态分析工具，如IDA、readelf、objdump等；

防调试攻击：对抗主流的调试工具，如gdb、lldb、IDA等；

防动态攻击：对抗主流的动态攻击，如inject、hook等；

防文件篡改：对文件进行数据效验，防止文件被篡改；

任务记录

当完成任务提交后，在左侧“任务记录”功能里，可以查看当前各任务的状态，如下图所示：

图 3-143 任务记录

当任务状态为 “已完成” ，用户可下载加固后的应用包。当任务状态为 “内部程序异常” ，用户可下载相关的日志，

并发给技术人员排除问题。

用户管理

加固平台主要涉及两种角色: 管理员 和 普通用户 。两者的区别对比如下:

图 3-144 角色对比

角色	应用加固	用户管理	策略管理
管理员	有	有	有
普通用户	有	无	仅浏览

当以 管理员 身份登录系统，左侧会出现“用户管理”功能项，如下图所示：

图 3-145 用户管理

用户可以非常方便的添加和编辑每个用户，如下图所示：

图 3-146 添加用户

同时，用户可通过“个人信息”功能项，查看个人信息、修改登录密码等等。

图 3-147 个人信息

功能配置

所有功能的配置总入口，目前的功能模块分别是Android App、Android SDK、iOS App、iOS SDK、Android

Scan和Binary（实际情况视所购买产品会有所不同）。

- **Android App加固**
  a. 加固策略
     加固平台中有两种策略，一种是 预置加固策略 ，另一种是 定制加固策略 。预置加固策略 在首次登录系统，在“策
     略管理”功能项里就可以查看，如下图所示：

图 3-148 策略管理

预置加固策略 基本覆盖大部分的加固场景。当 预置加固策略 无法满足客户需求，则可由双方技术人员共同协商，

定制出满足客户场景的加固策略。管理员通过“策略管理”功能项，把定制的加固策略，添加到系统中。当下次创建加

固任务时，即可选择。

b. 签名证书

图 3-149 签名证书

加固后可以用指定的证书进Apk进行签名，该功能页可以新增/编辑证书的签名信息。

c. 渠道方案

图 3-150 渠道方案

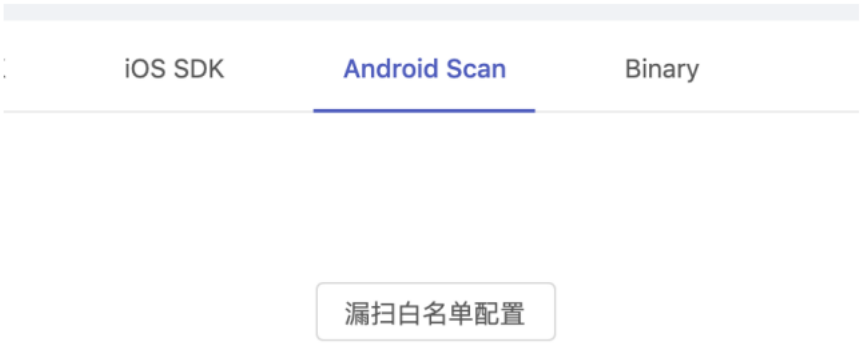
图 3-151 编辑渠道方案

加固后可以用指定的渠道方案进行多渠道打包，该功能页可以新增/编辑渠道方案信息。另外app需要集成顶象多渠道

SDK，详细见《 顶象应用加固平台多渠道打包使用说明 》帮忙文档。

- **iOS App加固**
  该功能页是针对iOS App加固的策略管理，功能跟Android App加固类似。
- **Android SDK加固**
  该功能页是针对Android SDK加固的策略管理，功能跟Android App加固类似。
- **iOS SDK加固**
  该功能页是针对iOS SDK加固的策略管理，功能跟Android App加固类似。
- **Android Scan 应用漏扫**

图 3-152 Android Scan 应用漏扫



可以针对第三方SDK进行过滤处理。

- **Binary加固**
  暂无可配置功能。

系统配置

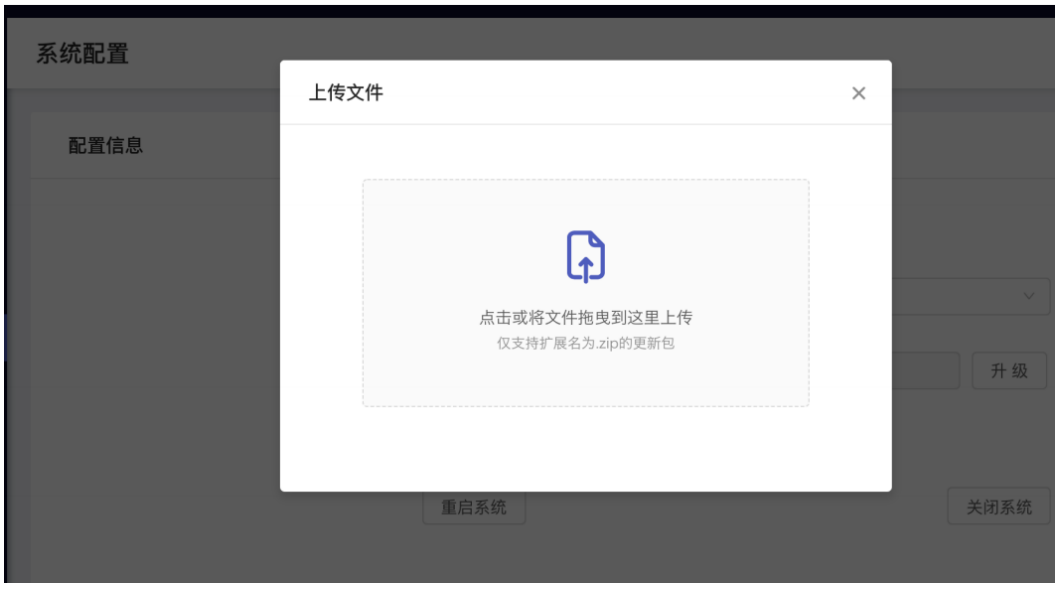
通过系统配置，可以完成系统版本查看、系统更新和系统停启的管理。如下图所示：

图 3-153 系统配置

注意：当要重启系统或关闭系统，请不要直接强制操作，正确的方式是通过系统配置

当系统需要更新，技术人员会提供对应的更新包。用户只要把更新包拖到指定位置即可完成更新，如下图所示：

图 3-154 上传文件



帮助信息

通过帮助信息，可以方便快捷查阅相关的使用说明，这里会不定期更新。如下图所示：

图 3-155 帮助信息

4 修订记录

表 4-1 修订记录

发布日期	修订记录
2024-03-01	第一次正式发布。