

APISEC 安全平台

用户手册

版本 V2.5.8.1

2024-08-18

上海喜数信息科技有限公司

目录

1. APISEC 安全规范	3
1.1. 缩略术语.....	3
1.2. 应用程序接口安全级别.....	3
1.3. 风险等级定义.....	3
2. 登录	4
3. 首页	4
4. 资产管理.....	5
4.1. API	5
4.1.1. API 列表	5
4.1.2. 画像.....	7
4.2. 账号	10
4.2.1. 账号列表.....	10
4.2.2. 画像.....	10
4.3. 源 IP	11
4.3.1. 源 IP 列表	11
4.3.2. 画像.....	11
5. 应用分析.....	13
5.1. 第三方应用.....	13
5.2. 自主应用.....	13
5.2.1. 列表页.....	13
5.2.2. 画像.....	16
6. 漏洞分析.....	21
6.1. API 漏洞	21
6.1.1. 列表页.....	21
6.1.2. 详情.....	22
6.2. 漏洞扫描.....	24
7. 攻防态势.....	26
7.1. 应用情报.....	26
7.2. 攻防监控.....	27
8. 数据安全分析.....	27
8.1. 数据分析列表页.....	27
8.2. 数据详情.....	28
9. 数据流转分析.....	30
10. 安全报告	30
11. 安全审计	31
11.1. 事件审计.....	31
11.2. 行为记录.....	33
12. 安全配置	35
12.1. 资产策略.....	35
12.1.1. 源 IP 识别	35
12.1.2. 账号识别.....	36
12.1.3. API 分类	41

12.1.4. API 聚合	42
12.1.5. 应用拆分.....	43
12.1.6. 应用聚合.....	45
12.1.7. 账号生命周期.....	46
12.1.8. 网络配置.....	47
12.2. 异常行为策略.....	48
12.2.1. 风险检测模型.....	48
12.2.2. 自定义检测模型.....	50
12.2.3. 机器学习.....	52
12.3. 数据安全检测.....	53
12.3.1. 数据标签.....	53
12.3.2. 行业模板.....	54
12.3.3. 组合标签.....	57
12.4. 攻击靶标配置.....	58
13. 系统配置	59
13.1. 用户管理.....	59
13.2. 角色管理.....	60
13.3. 部门管理.....	61
13.4. 日志管理.....	62
13.4.1. 操作日志.....	62
13.4.2. 登录日志.....	63
13.5. 授权管理.....	63
13.6. 数据存储管理.....	64
13.7. 服务器监控.....	65

1. APISEC 安全规范

1.1. 缩略术语

API	Application Programming Interface	应用程序接口
JSON	JavaScript Object Notation	JavaScript对象表示法
REST	Representational State Transfer	表述性状态传递
SQL	Structured Query Language	结构化查询语言
XML	Extensible Markup Language	可扩展标记语言

1.2. 应用程序接口安全级别

由于随着业务需求的变化，应用程序接口本身也是在不断变化的，因此应用程序接口安全级别划分依据以下因素：

➤ 接口存在高危漏洞

根据漏洞影响风险，发现接口高危漏洞，所有涉及高危漏洞的应用程序接口，都应被视为高风险应用程序接口。

➤ 接口涉及高敏感数据

根据高敏感数据识别的原则，可梳理出高敏感数据，所有涉及高敏感数据的应用程序接口，都应被视为高风险应用程序接口，因为这些接口的数据安全风险都可能导致高风险数据事件。

➤ 接口操作数据方式

根据接口操作的方式可能影响应用程序接口风险发生的可能性，如接口仅为系统或设备间的自动化传输，在不涉及高风险数据时，该接口被利用或受攻击的可能性相对较小，面临的风险也相对较小。如接口涉及人员主动访问，则相应接口被非授权、超范围或出于非正常业务目的被人为访问的可能性就较高，应被列入高风险应用程序接口。

➤ 应用程序接口域

对应用程序接口的访问域即为访问的来源，如为组织内部访问，其风险可能相对较低，但如为通过互联网访问，则可能有超出组织管理边界的访问来源，可能存在较高风险，应被识别为高风险应用程序接口。如为跨国/地区的境外方位，应被识别为高风险应用程序接口，并进行全面风险监测。

➤ 应用程序接口用途

应用程序接口的用途，如用于身份认证、执行特定命令和操作、其风险相对较高。

1.3. 风险等级定义

➤ 高风险（Critical）

此等级适用于能够直接导致系统崩溃、数据泄露或非法访问的攻击行为，攻击者可以对系统进行完全控制。

➤ 中风险（Medium）

此等级适用于可能导致系统受损、数据泄露或部分控制的攻击行为，但不会立即造成严重影

响。

➤ 低风险（Low）

此等级适用于可能会对系统功能或性能产生轻微影响的攻击行为,但不会导致系统完全崩溃或重大数据泄露。

考虑因素:

➤ 攻击类型

考虑攻击是否属于已知的高风险攻击类型,如 SQL 注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）等。

➤ 攻击影响

评估攻击对系统的影响程度,包括数据泄露、系统崩溃、用户隐私泄露等。

➤ 潜在损失

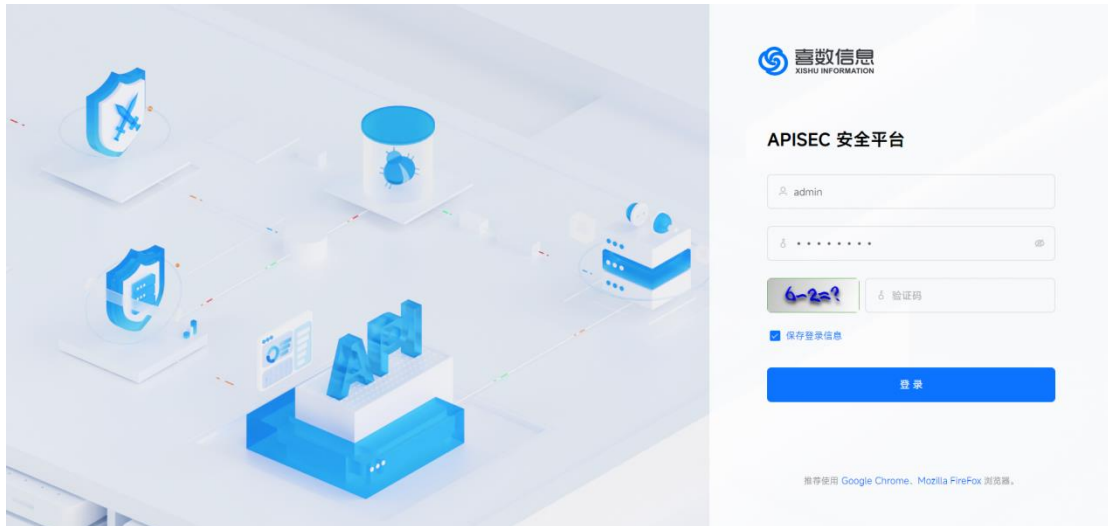
考虑成功攻击的潜在损失,包括财务损失、声誉损害等。

➤ 安全措施

评估系统已经采取的安全措施,如输入验证、身份验证、访问控制等对抗攻击的能力。

2. 登录

浏览器输入 <http://x.x.x.x:80> 输入用户名 admin 密码 Admin123,登录 APISEC 安全分析平台。



图：登录界面

3. 首页

首页部分,主要是对资产和风险事件不同维度的统计。显示三部分:资产及事件统计、各维度统计排行榜、风险事件动态。

- **资产统计**: 应用和 API 的数量和风险数的统计、漏洞统计、涉敏数据个数统计、访问统计;
- **排行榜**: 风险 API 访问热度 Top5、风险应用访问热度 Top5、API 漏的 Top5、涉敏数据 Top5、异常源 IP 访问热度 Top5、异常行为 Top5;
- **风险事件动态**: 形式最新 10 条未处置的风险事件简述 (分: 异常行为、漏洞、涉敏数据), 以及可以对事件进行处置。



风险事件动态		异常行为	漏洞	涉敏数据
2024-08-08 16:02:24	● 异常登录失败	源IP 110.166.100.223 使用账号: wshu 使用密码对 192.168.5.171:9990 应用下的 /prod-api/auth/login 进行登录,登录成功。		
2024-08-08 15:59:27	● 程序敏感信息泄露	192.168.1.86 访问 http://192.168.5.171:80 (/prod-api/code) 的响应信息中, 可能包含明文密码		
2024-08-08 15:28:35	● 程序敏感信息泄露	192.168.1.86 访问 http://192.168.5.171:80 (/prod-api/manager/dipl/query/DlpDataDetailsRespV2) 的响应信息中, 可能包含明文密码		
2024-08-08 15:28:35	● API 单次传输大量敏感数据	源IP 192.168.1.86 于 2024-08-08 15:28:33 对 http://192.168.5.171:80 (/prod-api/manager/dipl/query/DlpDataDetailsRespV2) API 访问时, 传输了大量敏感数据。		
2024-08-08 15:26:55	● 返回数据数据异常过多	源IP 192.168.1.86 在访问 http://192.168.5.171:80 (/prod-api/vulnerability/astra/showImpactInfoPageDetail) 时, 存在返回数据异常过多。		
2024-08-08 15:26:55	● API 单次传输大量敏感数据	源IP 192.168.1.86 于 2024-08-08 15:26:52 对 http://192.168.5.171:80 (/prod-api/vulnerability/astra/showImpactInfoPageDetail) API 访问时, 传输了大量敏感数据。		
2024-08-08 15:02:45	● API 单次传输大量敏感数据	源IP 192.168.1.86 于 2024-08-08 15:02:43 对 http://192.168.5.171:80 (/prod-api/manager/source/Network/page) API 访问时, 传输了大量敏感数据。		
2024-08-08 15:02:02	● 程序敏感信息泄露	192.168.1.86 访问 http://192.168.5.171:80 (/prod-api/vulnerability/astra/showImpactInfoPageDetail) 的响应信息中, 可能包含明文密码		
2024-08-08 15:01:53	● 程序敏感信息泄露	192.168.1.86 访问 http://192.168.5.171:80 (/prod-api/vulnerability/api/Loophole/loopholeDetail) 的响应信息中, 可能包含明文密码		
2024-08-08 15:01:53	● API 单次传输大量敏感数据	源IP 192.168.1.86 于 2024-08-08 15:01:51 对 http://192.168.5.171:80 (/prod-api/manager/project/v2/page?pageNum=1&pageSize=99999) API 访问时, 传输了大量敏感数据。		

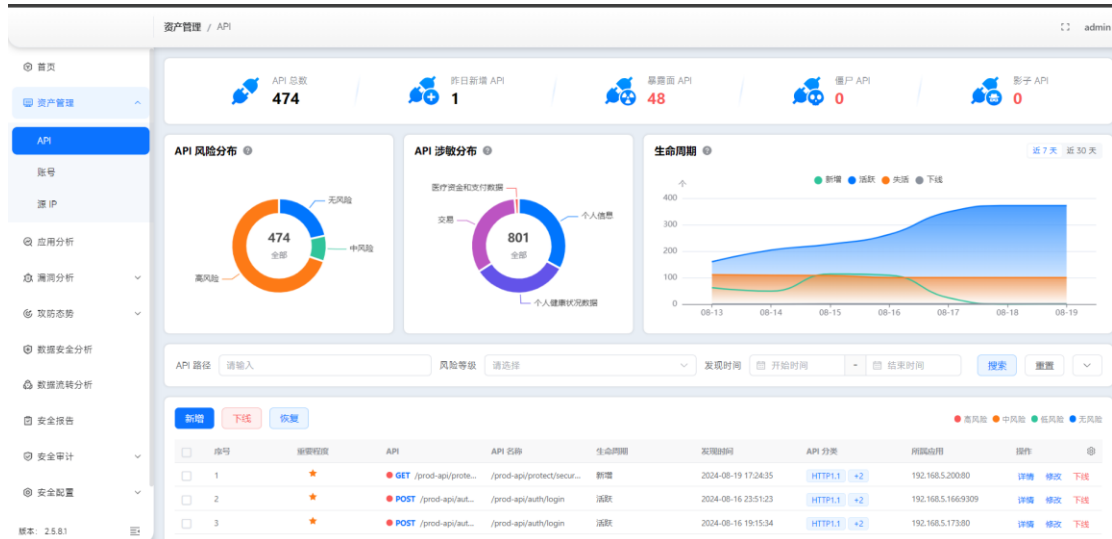
图: 首页

4. 资产管理

4.1. API

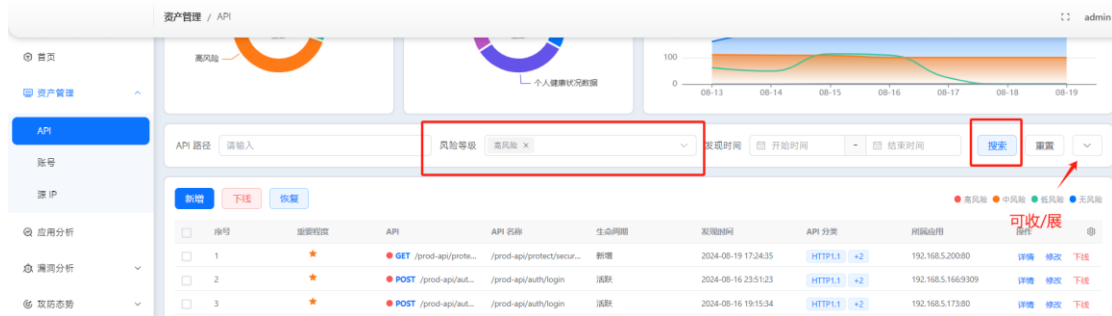
4.1.1. API 列表

显示 API 相关的数据, 包括统计数据、列表数据、拓展功能。



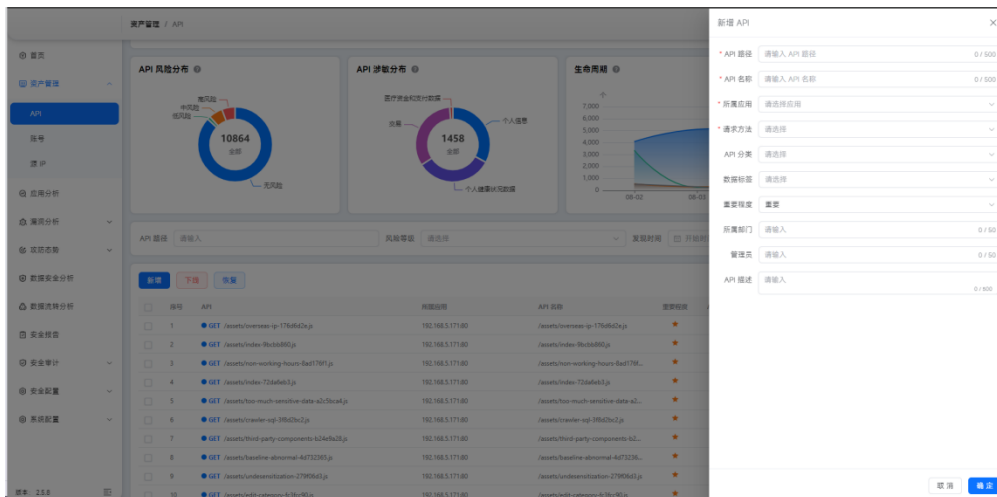
图：API 列表页

- **统计数据**包括：API 总数、昨日新增 API、暴露面 API、僵尸 API、影子 API、API 风险分布、API 涉敏分布、生命周期。
- **列表数据**：显示 API 的概要信息，一揽了解 API 的主要信息。
- **拓展功能**：根据整体的产品特点，提供一些拓展功能，方便特殊场景的操作。
【搜索】：支持根据选择的条件，筛选 API 信息。



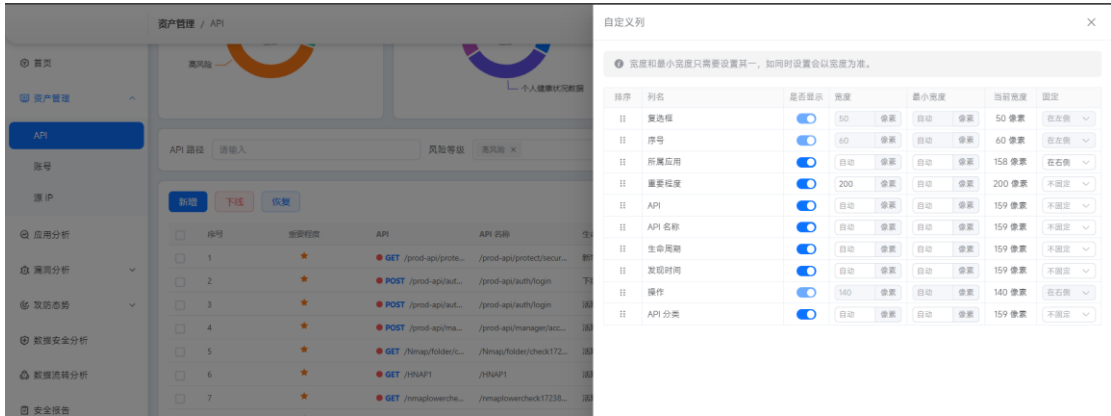
图：API 列表页 - 筛选

【新增】：支持自定义添加 API。



图：API - 新增

- 【修改】：支持修改 API 基本信息
- 【下线】：支持单个或者批量下线 API，API 的生命周期会流转为“下线”。
- 【恢复】：支持单个或者批量恢复 API，API 的生命周期流转为“活跃”
- 【自定义列表】：支持自定义列表显示的字段，并且调整字段的位置。

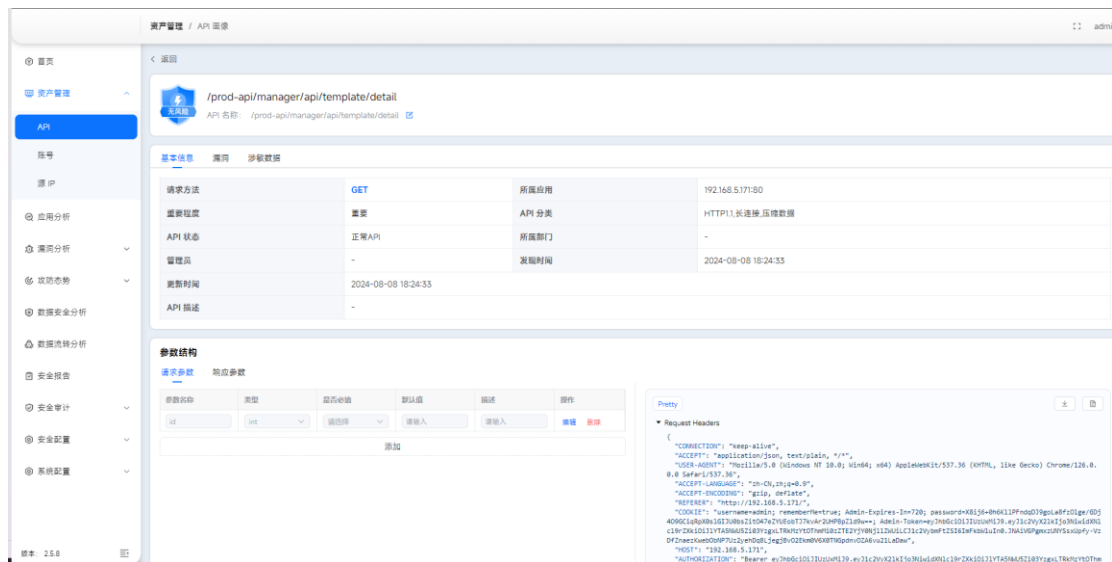


图：API - 字段自定义

4.1.2. 画像

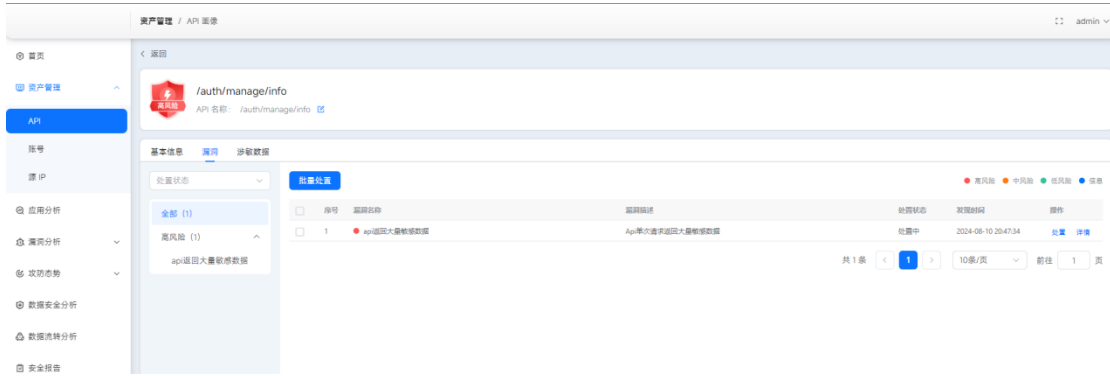
显示 API 的基本信息、漏洞列表和详情、涉敏数据和详情。

- **基本信息**：显示 API 被还原的基础信息，一般包括请求头、请求体、响应头、响应体的数据。



图：API - 画像 - 基本信息

- **漏洞**：显示 API 触发的漏洞信息，并且支持对事件的处置功能。
 【列表】显示该 API 触发的漏洞事件的概要信息。

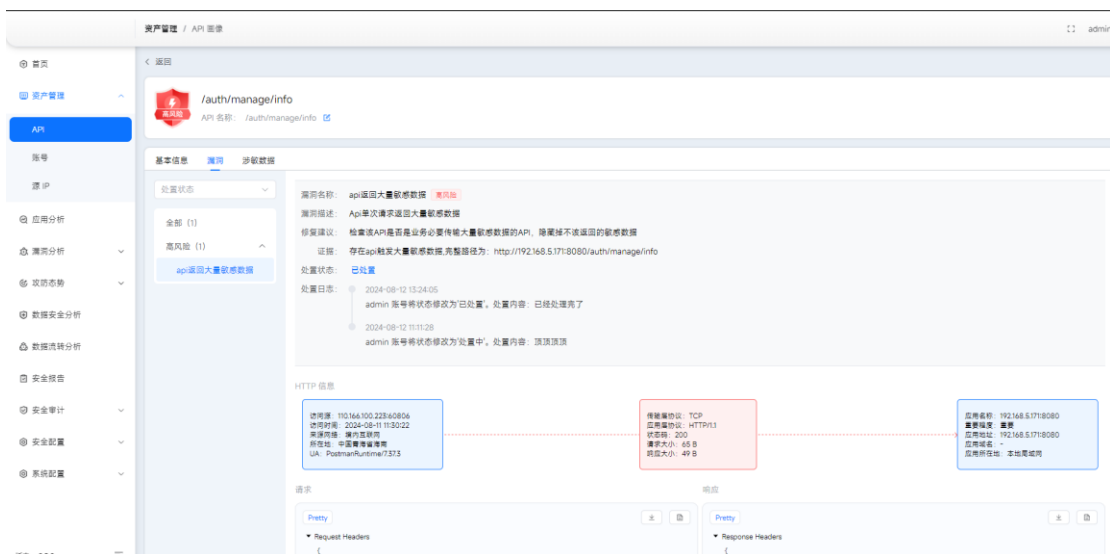


图：API - 画像 - 漏洞列表

【详情】：显示该 API 触发的漏洞事件的详细信息，包括：漏洞名称、漏洞描述、修复建议、证据、处置日志、HTTP 信息、请求、响应等。

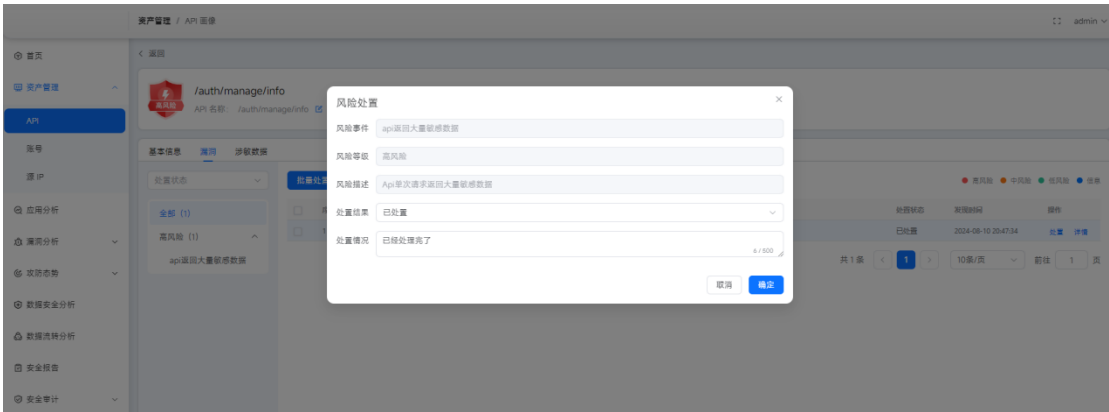


图：API - 画像 - 漏洞详情 A



图：API - 画像 - 漏洞详情 B

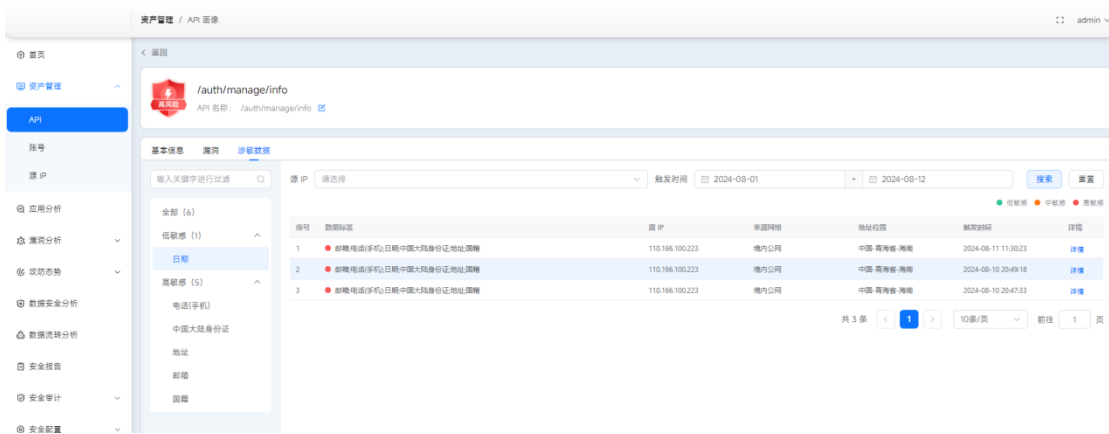
【处置功能】：支持对 API 的漏洞事件进行处置，分为：未处置、处置中、已处置。



图：API - 画像 - 漏洞 - 处置

● **涉敏数据**：显示 API 触发的所有数据标签概要信息及详情信息。

【涉敏数据列表】 显示该 API 触发的敏感词列表，展示概要信息。



图：API - 画像 - 敏感数据列表

【涉敏数据详情】 显示 API 触发数据标签的详细显示，便于定位问题所在。

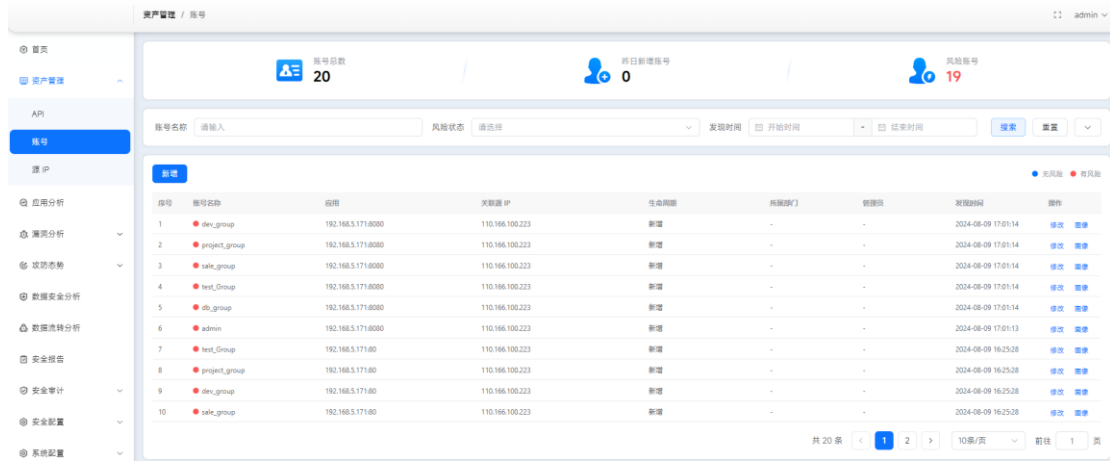


图：API - 画像 - 敏感数据详情

4.2. 账号

4.2.1. 账号列表

显示系统识别出的账号概要信息、相关的统计数据、拓展功能。

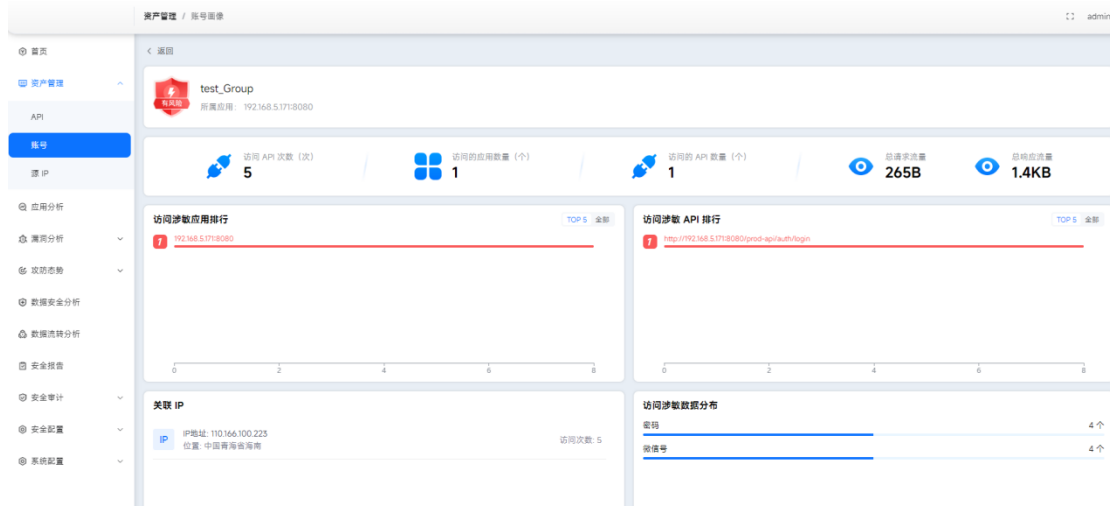


图：账号 - 列表页

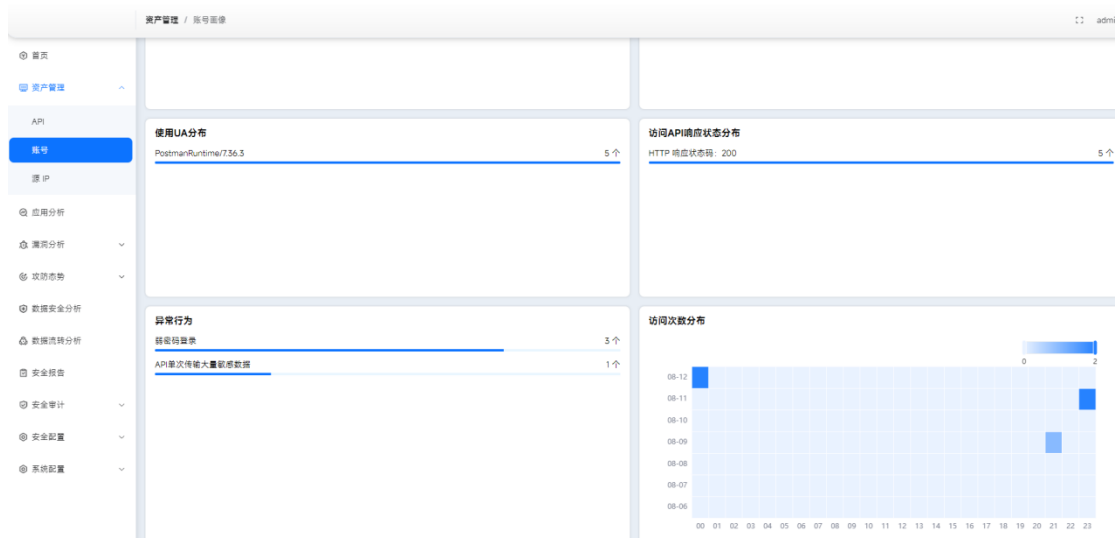
- **账号统计数据：** 账号总数、昨日新增账号、风险账号。
- **账号概要信息：** 显示账号信息。
- **拓展功能**
 - 【搜索】：根据选择的条件，筛选账号信息
 - 【新增】：自定义添加账号。
 - 【修改】：自定义添加账号。

4.2.2. 画像

显示当前账号的状态、访问行为、是否存在风险等。



图：账号 - 画像 1

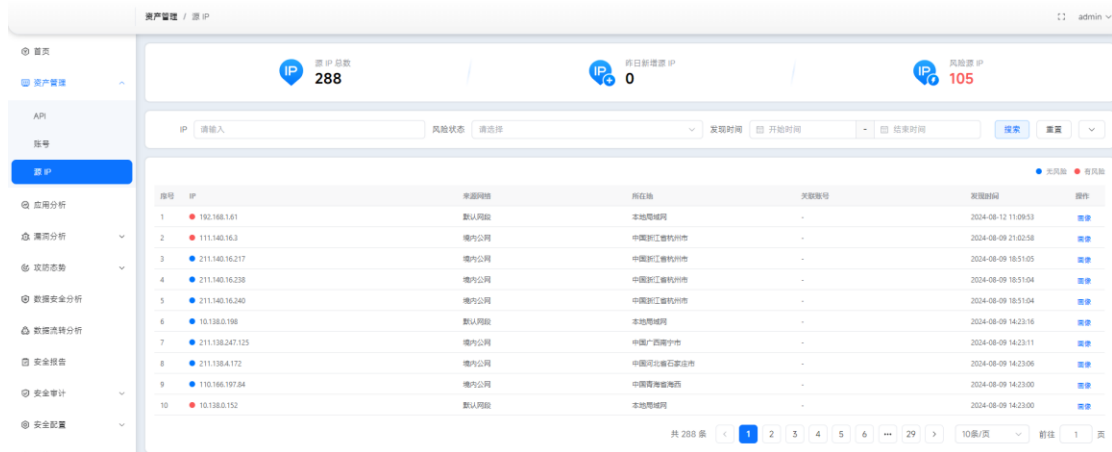


图：账号 - 画像 2

4.3. 源 IP

4.3.1. 源 IP 列表

显示识别出的源 IP 和对源 IP 的数据统计。

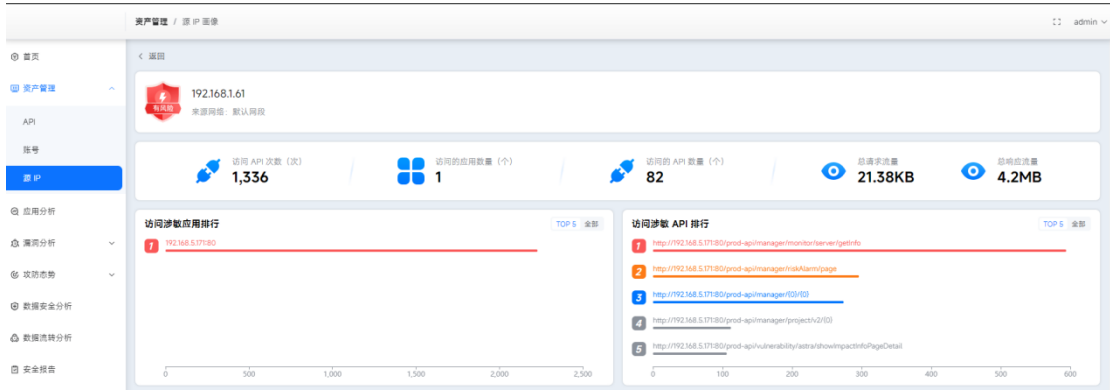


图：源 IP - 列表页

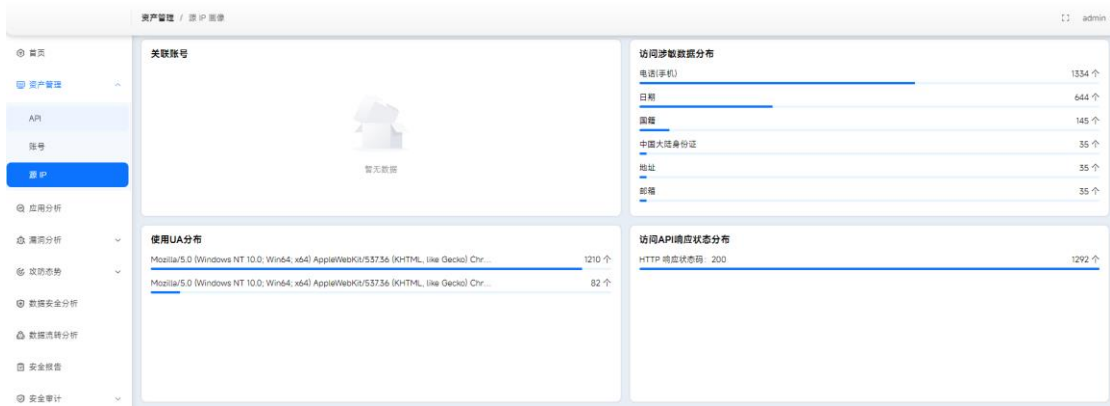
- **源 IP 数据统计：** 根据不同维度统计源 IP 的数量。
- **源 IP 列表：** 显示的概要数据。
- **筛选功能：** 根据选择的条件，筛选出对应的源 IP 信息。

4.3.2. 画像

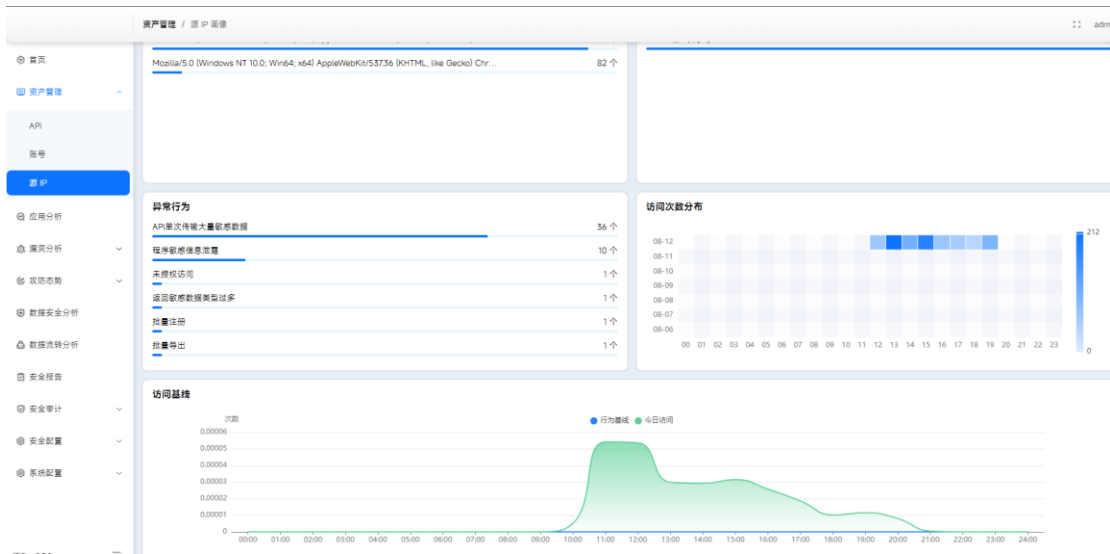
显示当前源 IP 的状态、访问行为、是否存在风险行为等



图：源 IP - 画像 1



图：源 IP - 画像 2



图：源 IP - 画像 3

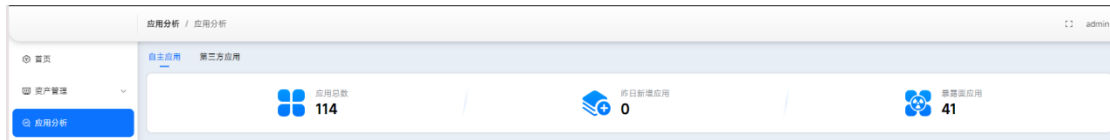
5. 应用分析

5.1. 自主应用

5.1.1. 列表页

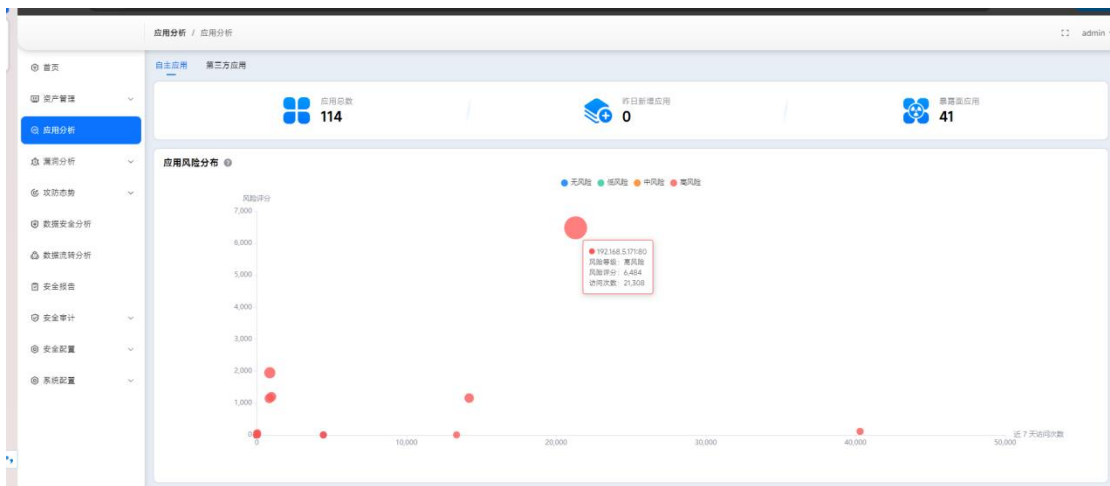
显示系统识别的自主应用，并且对识别到的数据进行统计和聚合展示。

- **头部统计:** 主要统计不同维度的应用数，分为：应用总数、昨日新增应用、暴露面应用。



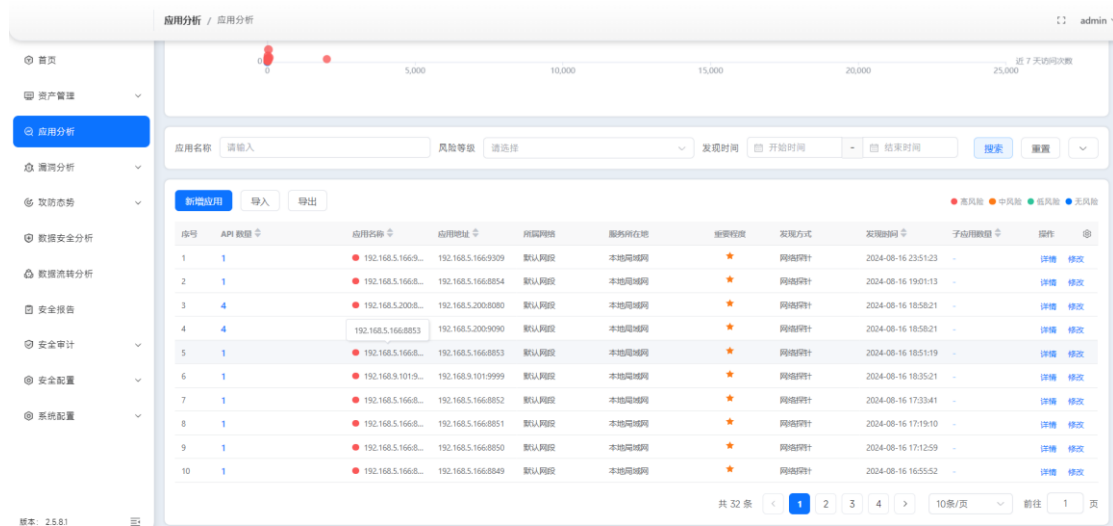
图：自主应用 - 头部统计

- **应用风险分布:** 根据 API 的风险等级计算出应用的风险评分，此处是根据风险评分和近七日的访问次数来显示，主要展示了一个应用的：风险评分、访问次数、风险等级。



图：自主应用 - 应用风险分布

- **列表:** 显示自主应用的关键信息。



图：自主应用 - 列表

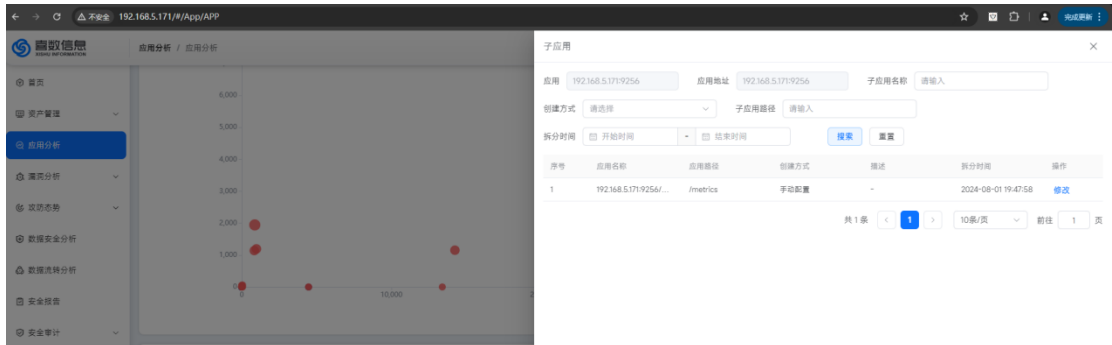
● 拓展功能

【筛选】：根据选择的条件，筛选自主应用信息。

【跳转子应用】：显示拆分的应用数，点击后显示子应用内容。

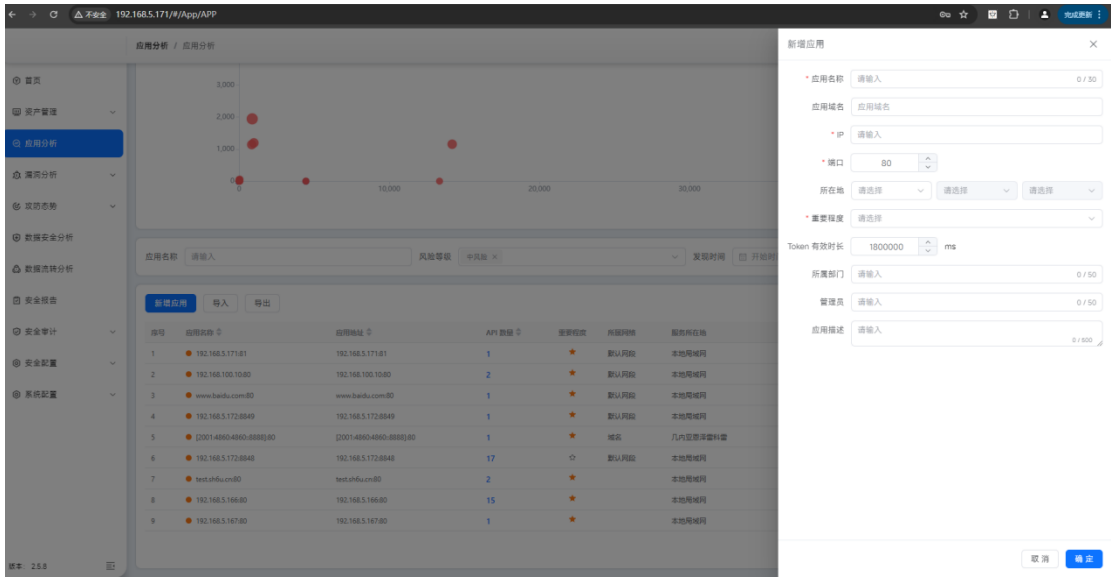


图：自主应用 - 列表



图：自主应用 - 子应用页面

【新增应用】：自定义新的应用。



图：自主应用 - 新增应用

【导入】：选择导入方式“文件”，选择要上传的文件，点击确定，上传成功后，应用列表将会显示对应数据。



图：自主应用 - 导入 - 文件

选择导入方式 swagger，输入 swagger 地址，点击确定，上传成功后，应用列表将会出现对应数据。

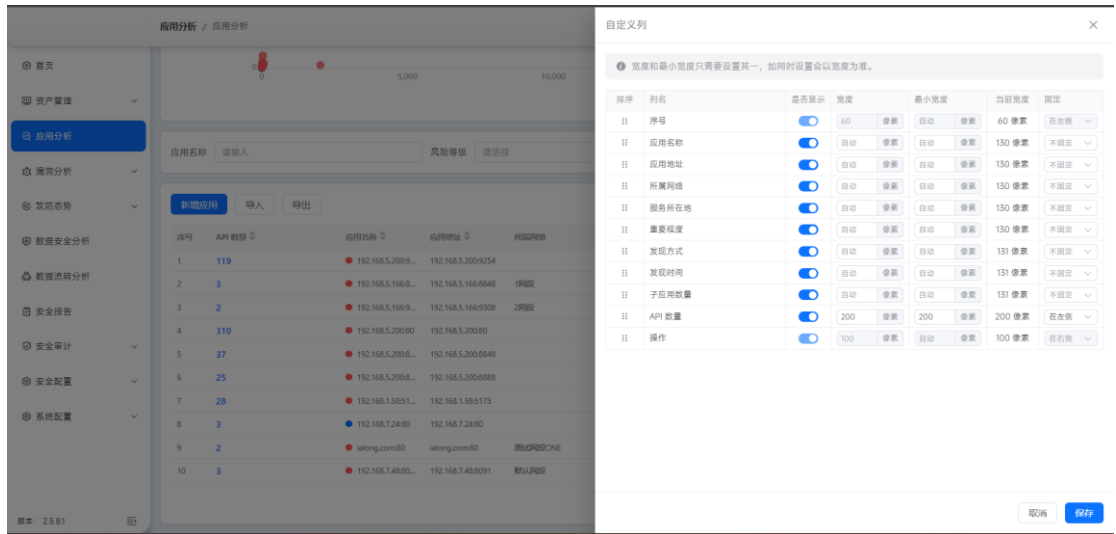


图：自主应用 - 导入 - swagger

【导出】：选择想要导出的应用和资源类型，点击确定，即可导出成功。

【修改】：可修改应用名称等基本信息，也可根据业务重要程序修改应用是否需要重点关注。

【自定义列表】：支持列表自定义功能，可以根据需求选择显示的字段和字段的排序。

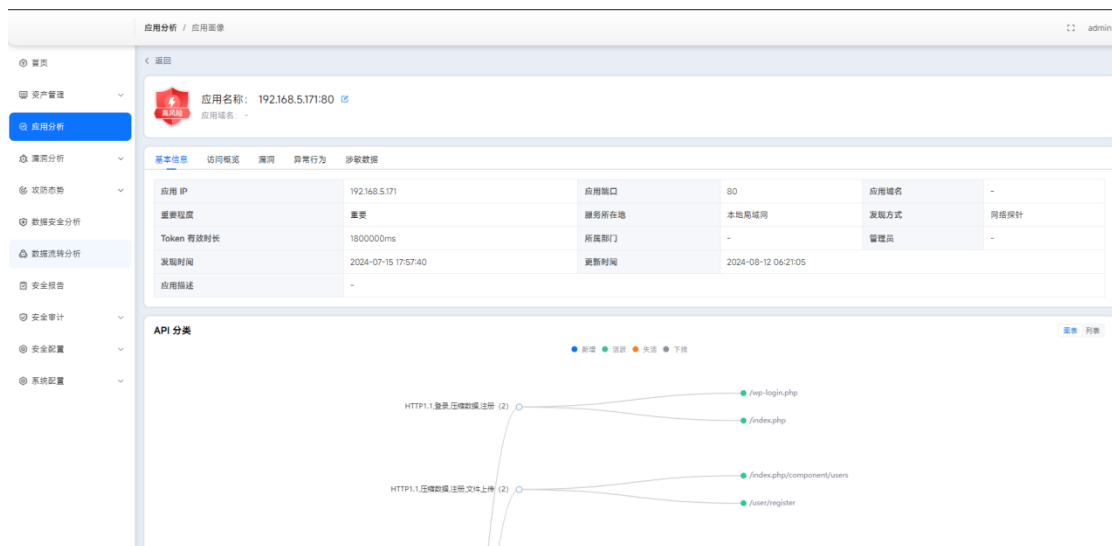


图：自主应用 - 自定义列表

5.1.2. 画像

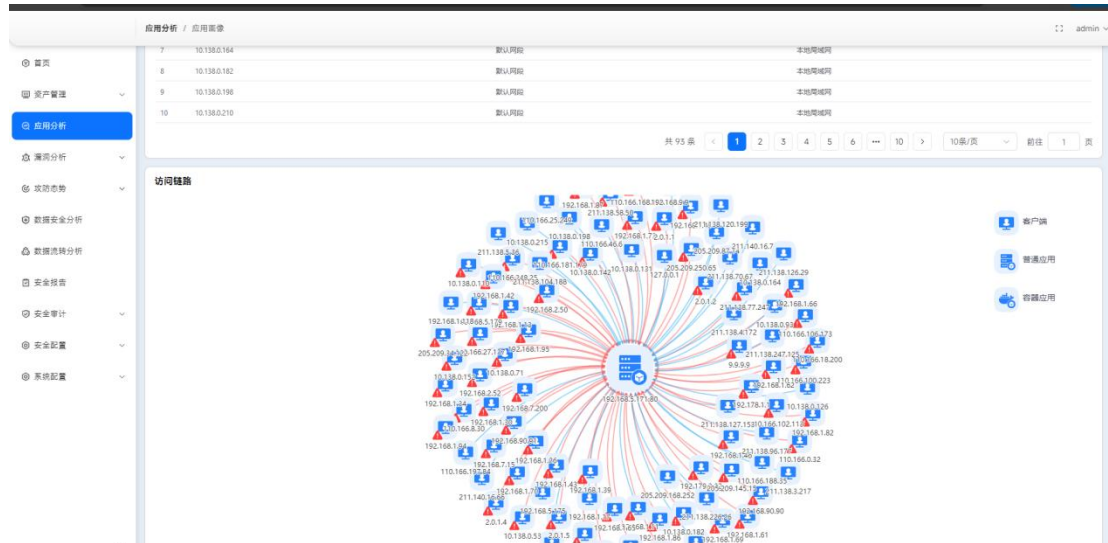
显示应用的基本信息，根据 API 的流量数据的统计和分析，显示访问概览、漏洞、行为记录、涉敏数据。

- **基本信息**：识别流量中应用的基础数据，回显到页面，主要有基本信息、API 分类的对应 API 数据（分为图标、列表两种形式）。



图：应用-画像-基本信息

- **访问概览**：显示访问该应用的源 IP 信息及访问链路。



图：应用-画像-访问概览-访问链路

- **漏洞：**显示应用下的 API 触发的所有漏洞信息。
【列表】：以漏洞名作为类型，显示有漏洞的 API 简要信息。

序号	API	漏洞名称	危险状态	漏洞描述	发现时间	操作
1	/prod-api/system/dict/data/type/sys_config_type	api返回大量敏感数据	未处置	Api单次请求返回大量敏感数据	2024-08-09 16:33:58	处置 详情
2	/prod-api/system/dict/data/type/matching_method	api返回大量敏感数据	未处置	Api单次请求返回大量敏感数据	2024-08-09 16:13:04	处置 详情
3	/prod-api/manager/faq	服务器敏感数据	未处置	服务器敏感数据	2024-08-08 14:19:10	处置 详情
4	/prod-api/manager/home	参数可遍历	未处置	参数可遍历	2024-08-09 10:16:11	处置 详情
5	/prod-api/analysis/attack/exception/exception/event/sp...	api返回大量敏感数据	未处置	Api单次请求返回大量敏感数据	2024-08-10 19:00:47	处置 详情
6	/admin/faq	参数可遍历	未处置	参数可遍历	2024-08-08 12:18:21	处置 详情
7	/prod-api/manager/element/sensitiveProjectCount	服务器敏感数据	未处置	服务器敏感数据	2024-08-08 18:18:22	处置 详情
8	/prod-api/system/dict/data/type/response_status	api返回大量敏感数据	未处置	Api单次请求返回大量敏感数据	2024-08-09 16:26:28	处置 详情
9	/prod-api/manager/home/v2/risk/event/list	返回测试信息	未处置	返回测试信息	2024-08-10 20:33:24	处置 详情
10	/prod-api/manager/home/v2/risk/event/list	api返回大量敏感数据	未处置	Api单次请求返回大量敏感数据	2024-08-09 16:01:27	处置 详情

图：应用-画像-漏洞-列表 1

漏洞名称: api返回大量敏感数据 **高风险**

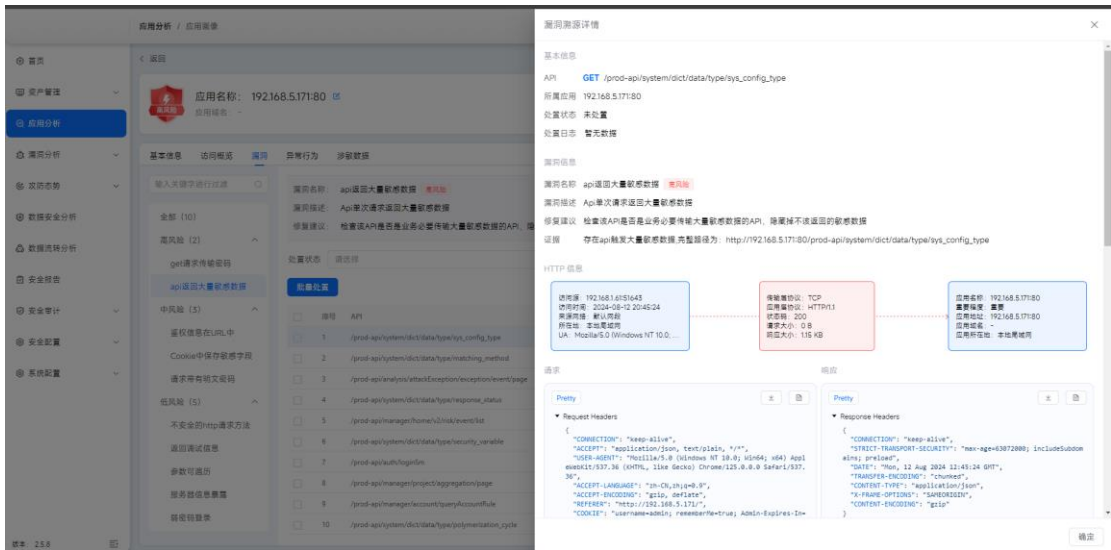
漏洞描述: Api单次请求返回大量敏感数据

修复建议: 检查该API是否是业务必要传输大量敏感数据的API, 确需该不该返回的敏感数据

序号	API	危险状态	发现时间	操作
1	/prod-api/system/dict/data/type/sys_config_type	未处置	2024-08-09 16:33:58	处置 详情
2	/prod-api/system/dict/data/type/matching_method	未处置	2024-08-09 16:13:04	处置 详情
3	/prod-api/analysis/attack/exception/exception/event/page	未处置	2024-08-10 19:00:47	处置 详情
4	/prod-api/system/dict/data/type/response_status	未处置	2024-08-09 16:26:28	处置 详情
5	/prod-api/manager/home/v2/risk/event/list	未处置	2024-08-09 16:01:27	处置 详情
6	/prod-api/system/dict/data/type/security_variable	未处置	2024-08-09 16:21:40	处置 详情
7	/prod-api/auth/loginSm	未处置	2024-08-09 16:01:27	处置 详情

图：应用-画像-漏洞-列表 2

【详情】显示 API 的漏洞溯源详情，分为基本信息、漏洞信息、HTTP 信息、请求、响应。

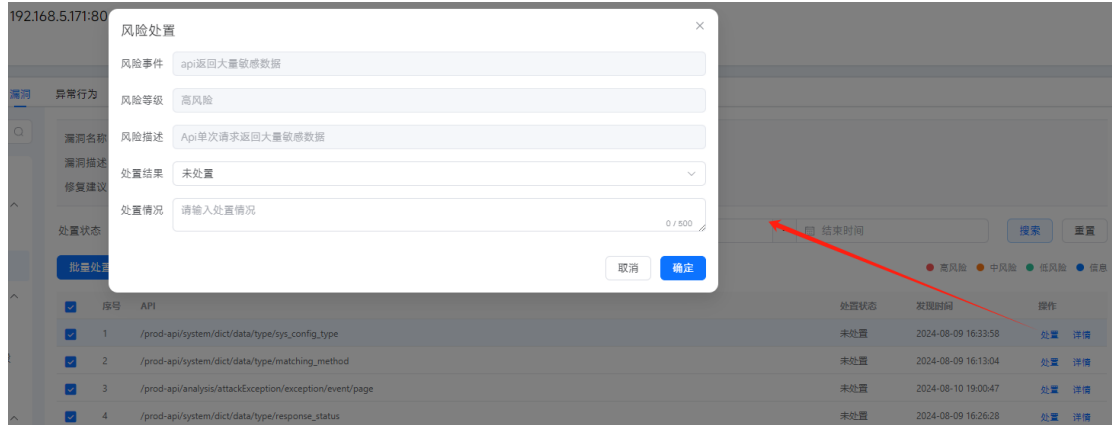


图：应用-画像-漏洞-溯源详情

【处置】：可以根据实际情况，对漏洞进行做“处置”动作，可以是单条处理，也可批量处理，处置的间断分为：未处置、处置中、已处置。



图：应用-画像-漏洞-批量处置



图：应用-画像-漏洞-单条处置

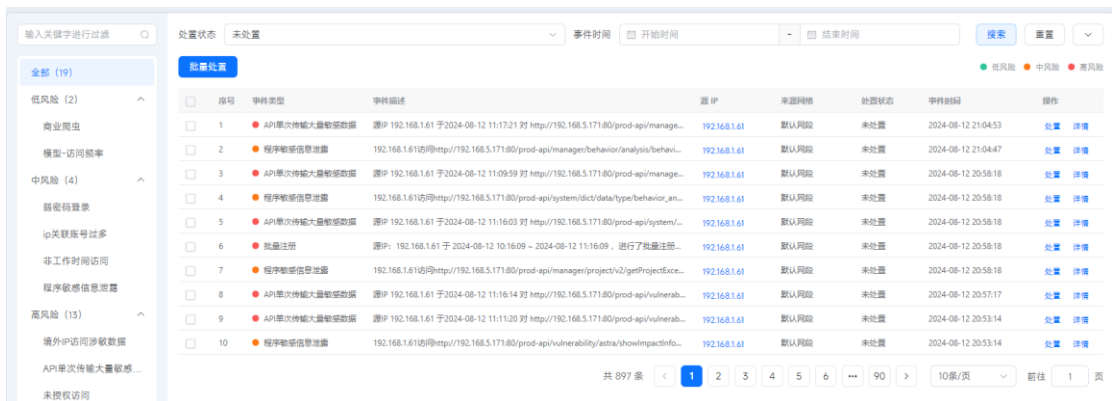
【筛选】：根据选择的筛选结果，搜索 API 的漏洞信息。

● 异常行为：显示应用下 API 触发的异常行为及相关的统计内容。

【统计-风险等级分布】：统计每个风险等级的 API 数量。

【统计-处置状态统计】：统计每个处置状态的 API 数量。

【异常行为列表】：显示应用下 API 触发的所有异常行为，并且以事件名分组。



图：应用-画像-异常行为-事件列表（全部）

【详情】：跳转到对应的“事件审计”的详情页。

【处置】：可以根据实际情况，对异常行为做“处置”动作，可以是单条处理，也可批量处理，处置的间断分为：未处置、处置中、已处置。

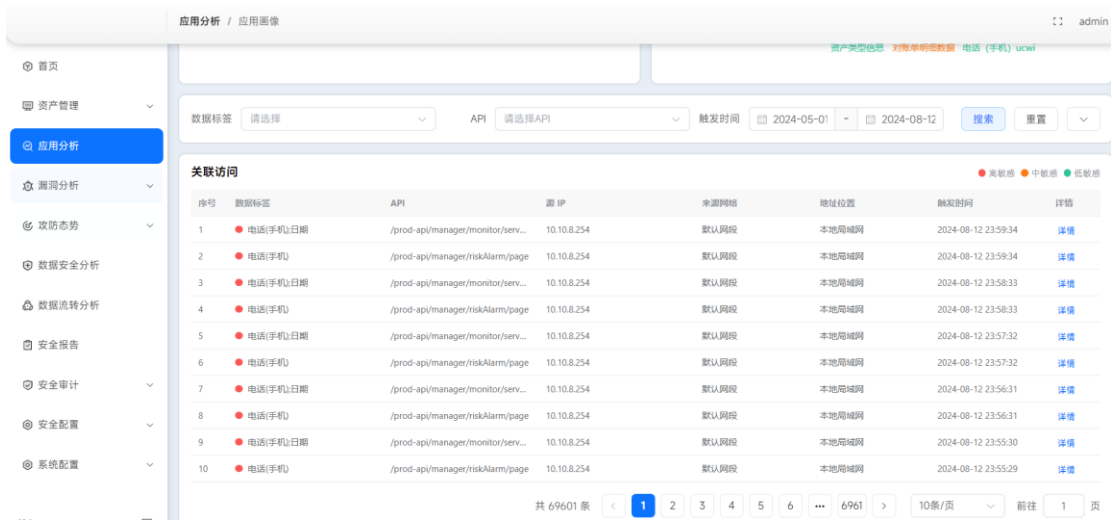
【筛选】“事件名筛选”：根据填写的内容模糊筛选事件名；异常行为事件筛选：根据事件类型，显示事件的概要信息。

● 涉敏数据：显示应用下 API 触发的数据标签及相关的统计内容。

【敏感等级分布】：根据风险等级统计应用命中过的数据标签个数。

【涉敏数据标签】：统计应用每个 API 触发的标签个数，根据等级用不同颜色标注。

【数据标签列表】：显示应用下的 API 每次触发的数据标签概要信息。



图：应用-画像-涉敏数据-关联访问

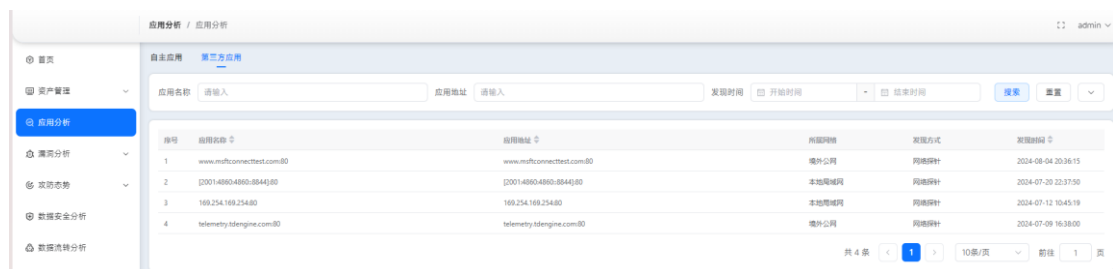
【数据标签详情】：显示数据泄露的详情信息。



图：应用-画像-涉敏数据-数据标签详情

【筛选】：根据选择的条件，筛选出标签记录。

5.2. 第三方应用



图：第三方应用

- 【列表】：显示识别出的所有第三方应用概要信息。
- 【筛选】：根据选择的条件，筛选第三方应用数据。

6. 漏洞分析

API 漏洞主要针对的是服务端可能含有的代码漏洞、错误配置、供应链漏洞等，对于这些具有一定风险的 API 本页面会对其进行统计以及详细的记录。漏洞分析主要分为：主动扫描和被动扫描。

6.1.API 漏洞

显示已经触发的所有漏洞的详细信息，从不同维度统计漏洞相关的数据。



图：API 漏洞-列表页

6.1.1. 列表页

该页面主要显示漏洞统计数据（头部统计、漏洞风险分布、API 漏洞 TOP5）、漏洞的概要信息、以及搜索功能。

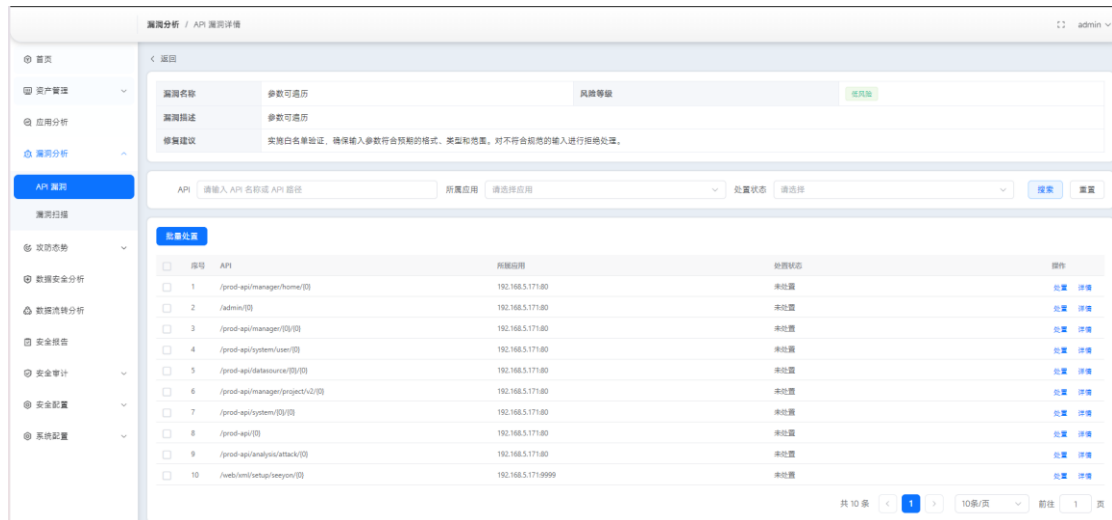


图：API 漏洞-列表页

- 头部统计：统计不同风险等级的 API 数、不同处置状态的 API 数。
- 漏洞风险分布：统计各风险等级漏洞对应的 API 个数。
- API 漏洞 TOP5：统计排名前 5 的漏洞涉及的 API 个数，按风险等级优先进行排序。
- 漏洞列表：以漏洞名的维度显示概要信息以及涉及应用统计数、涉及 API 统计数。
- 搜索：根据选择的条件，筛选漏洞信息。

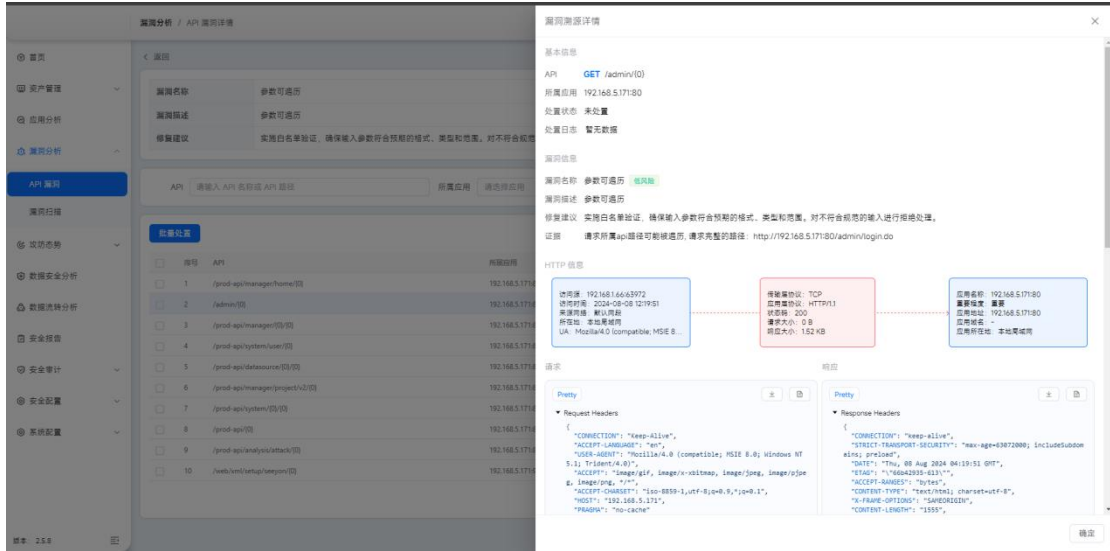
6.1.2. 详情

显示漏洞的描述信息、触发的 API 信息、API 触发漏洞的详情，以及处置功能。



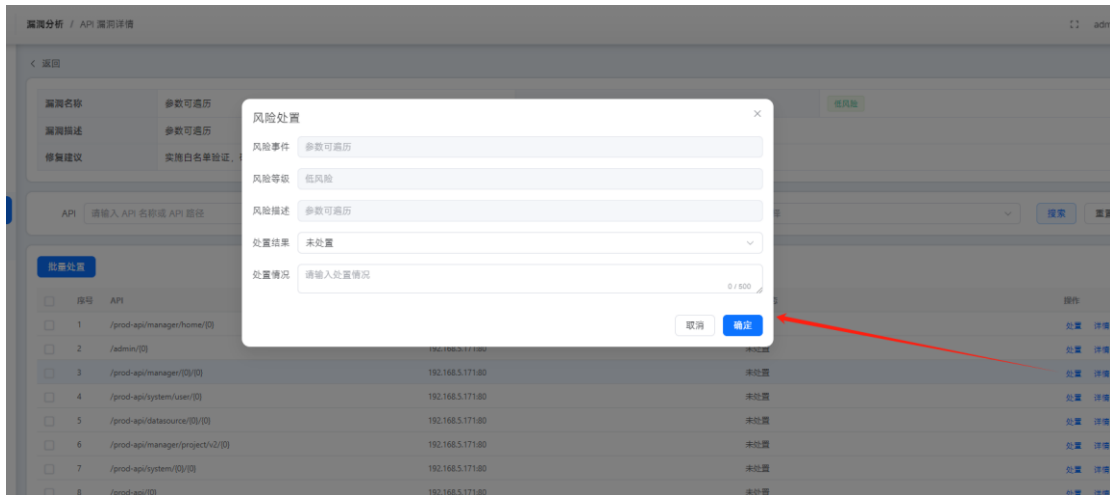
图：API 漏洞-详情

- API 漏洞概要信息：简要显示漏洞的名称、风险等级、描述、修复建议。
- API 列表：显示所有触发该风险事件的 API 数据。
- API 触发漏洞详情：显示 API 的基础信息、漏洞信息（包括证据）。

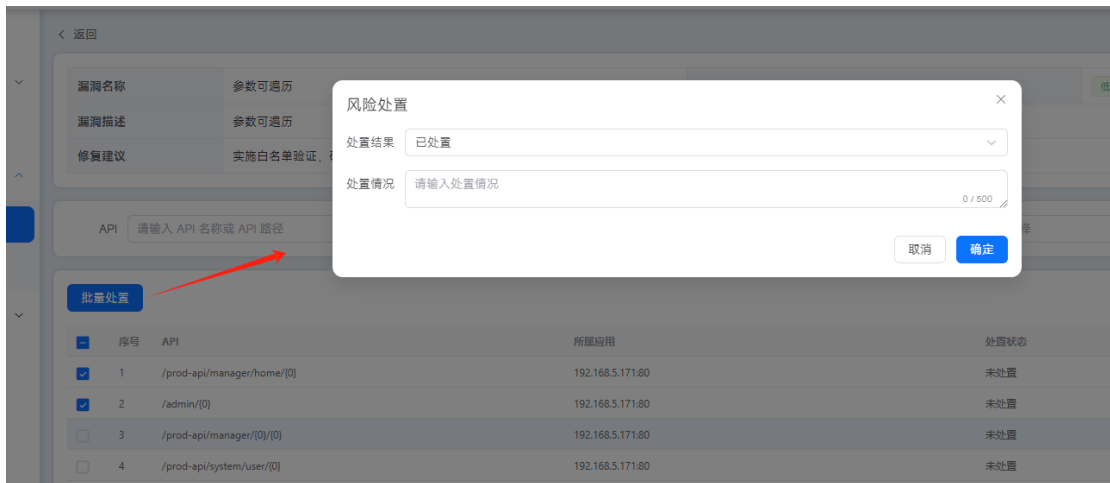


图：API 漏洞-详情-漏洞溯源详情

- 搜索：根据选择的条件，筛选 API 数据，回显在 API 列表部分。
- 处置：可以根据实际情况，对漏洞进行做“处置”动作，可以是单条处理，也可批量处理，处置的间断分为：未处置、处置中、已处置。



图：API 漏洞-详情-单条“处置”



图：API 漏洞-详情-批量“处置”

6.2. 漏洞扫描

漏洞扫描主要是针对一些可能含有的代码漏洞、错误配置、逻辑漏洞等数据进行扫描，并在脆弱性分析页面显示出可能存在问题的数据。

注：漏洞无入侵检测配置。

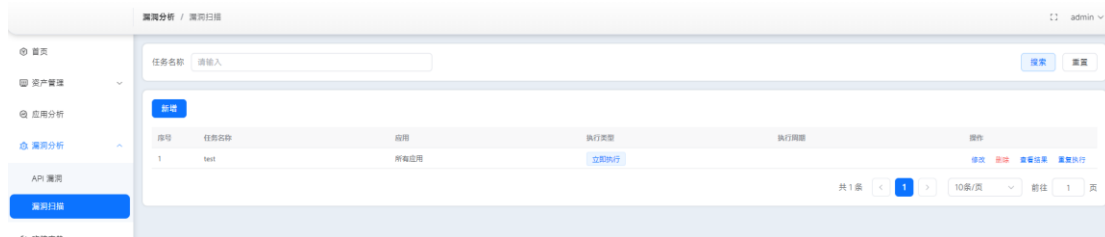
关闭防火墙：systemctl stop firewalld

浏览器访问 http://IP:8848/nacos

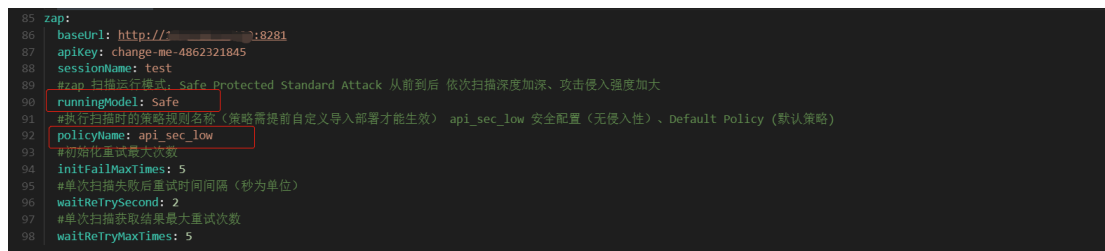
输入用户名/密码：nacos/nacos

修改脆弱性配置文件 xishu-cloud-vulnerability-dev.yml, xishu-cloud-job-dev.yml, 详细配置如下图

同时配置运行模式 runningModel 为 Safe、扫描策略使用 api_sec_low 时,可安全无侵入扫描。



图：漏洞扫描



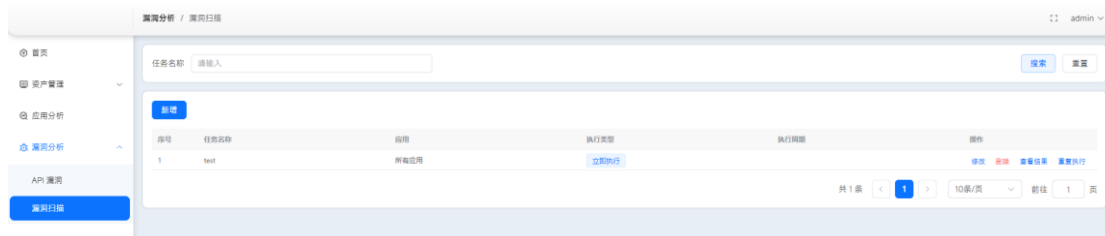
图：nacos 配置

修改后，点击【发布】

开启防火墙：systemctl start firewalld

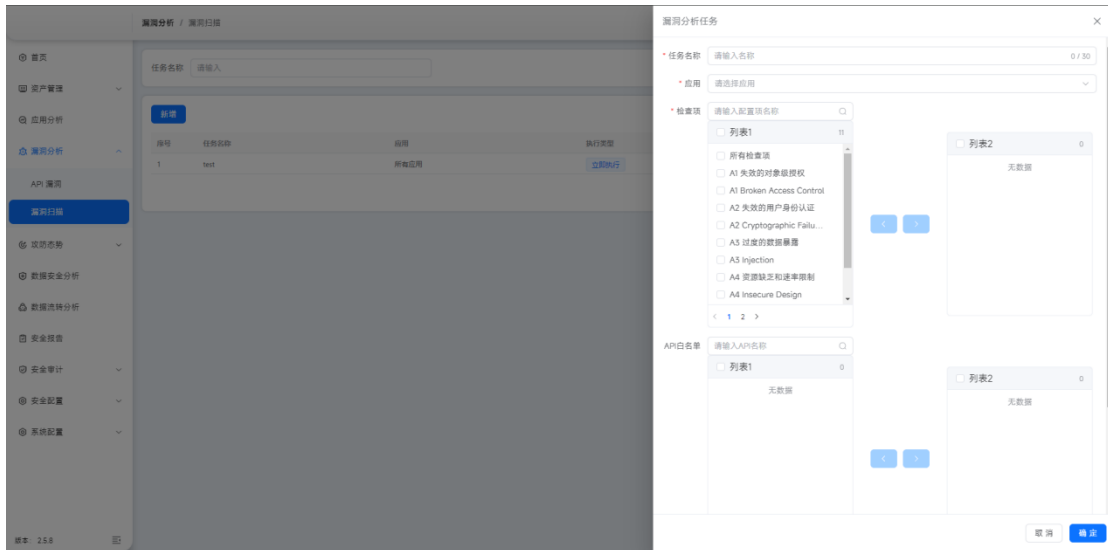
无入侵检测配置配置完成。

点击【漏洞扫描】，显示配置列表，可按照配置名称查询列表



图：漏洞扫描-列表

点击【新增】可添加新的脆弱性配置，可多选和单选以及全选



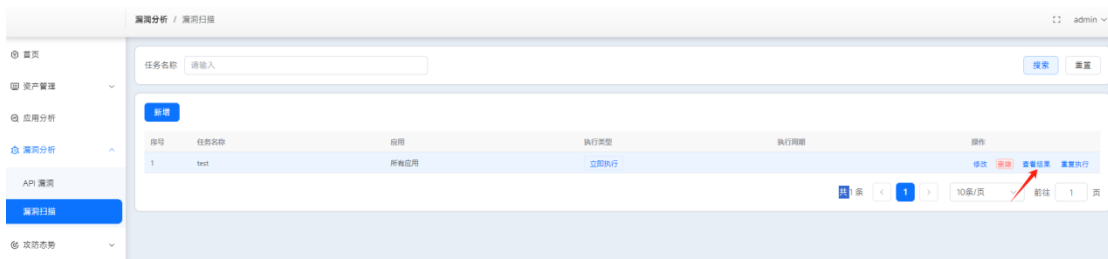
图：漏洞扫描-新增

点击【修改】可修改配置信息

点击【重复执行】可对配置重复执行扫描一次

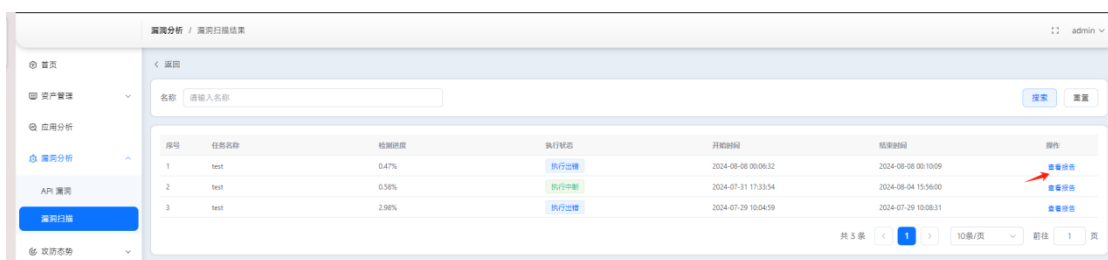
点击【删除】，提示是否删除该配置

点击【查看结果】跳转到【检测结果】页面，显示检测结果列表，可按照名称查询列表



图：漏洞扫描-查看结果-1

点击列表中【查看报告】跳转到【检测报告】页面，显示检测报告列表，包括应用地址以及危险数量和信息数量。



图：漏洞扫描-检测报告-1

漏洞分析 / 漏洞扫描报告

应用: 请选择应用

序号	地址	应用	高危数量	中危数量	低危数量	任意数量
> 1	/nacos/console-ui/public/js/jquery.js	192.168.5.171-8848	0	0	1	1
> 2	/nacos/console-ui/public/js/codemirror/addon/fullscreen.js	192.168.5.171-8848	0	0	1	0
> 3	/nacos/console-ui/public/js/vs/editor/editor.main.css	192.168.5.171-8848	0	0	1	0
> 4	/nacos/console-ui/public/js/loader.js	192.168.5.171-8848	0	0	1	1
> 5	/nacos/instance/catalog/instances	192.168.5.171-8848	0	0	0	1
> 6	/nacos/console-ui/public/css/bootstrap.css	192.168.5.171-8848	0	0	2	0
> 7	/nacos/console-ui/public/css/font-awesome.css	192.168.5.171-8848	0	0	1	0
> 8	/nacos/instance/catalog/service	192.168.5.171-8848	0	0	0	1
> 9	/nacos/console-ui/public/js/vs/editor/editor.main.nls.zh-cn.js	192.168.5.171-8848	0	0	1	0
> 10	/nacos/console-ui/public/css/icon.css	192.168.5.171-8848	0	0	2	0

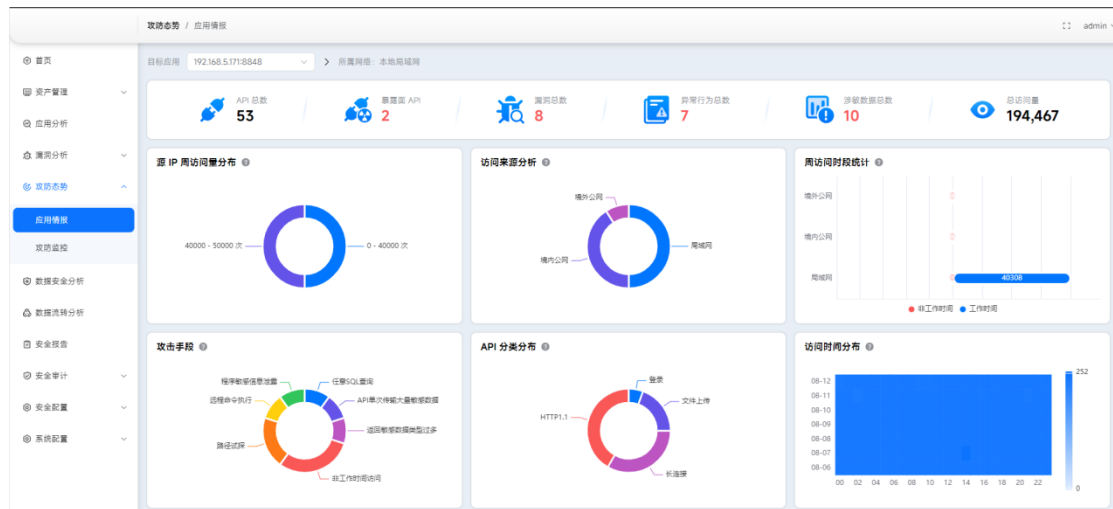
共 34 条 < 1 2 3 4 > 10条/页 前往 1 页

图：漏洞扫描-漏洞扫描报告

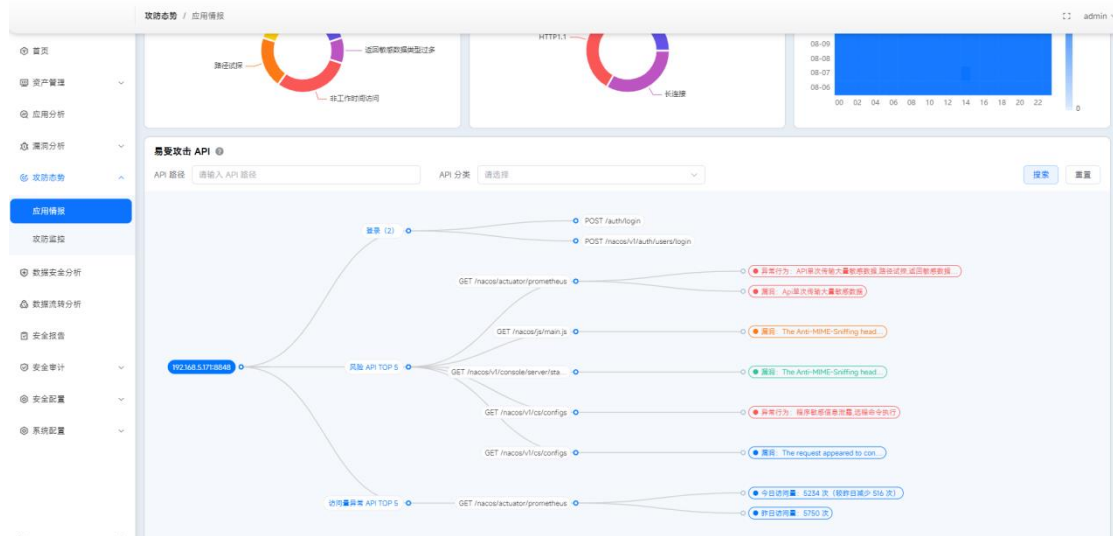
7. 攻防态势

7.1.应用情报

根据添加的靶标资产，统计资产数据、风险数据，并且根据显示不同维度的统计数据。



图：应用情报 1



图：应用情报 2

7.2. 攻防监控

根据不同维度统计资产的风险情况：受攻击 API 排行、受攻击应用排行、攻击源 IP；实时监控 QPS 和共计趋势；流量触发异常行为、脆弱性，进行实时播报。

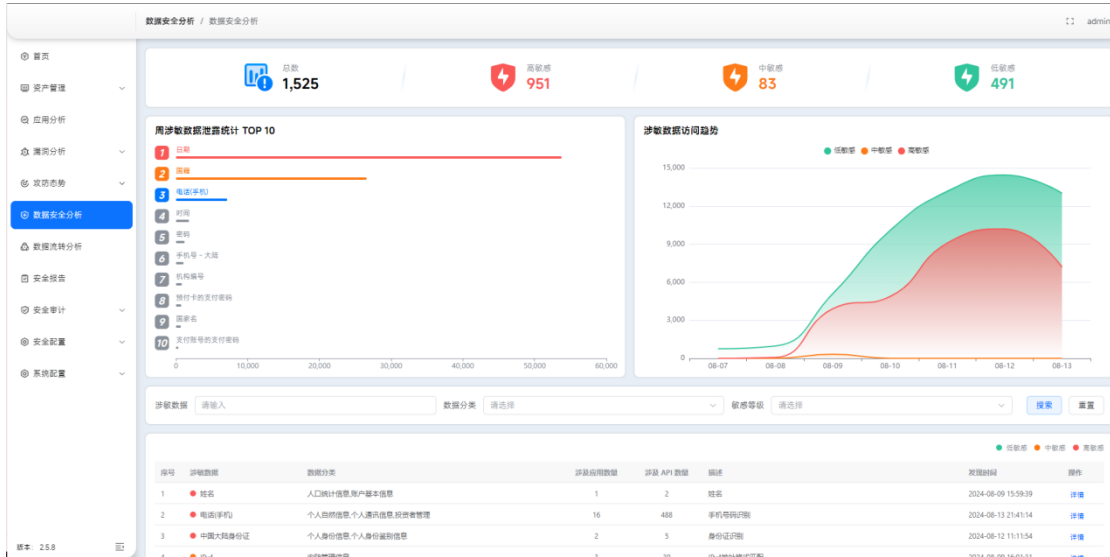


图：攻防大屏

8. 数据安全分析

8.1. 数据分析列表页

显示所有应用触发的数据标签，并且根据不同维度进行统计。

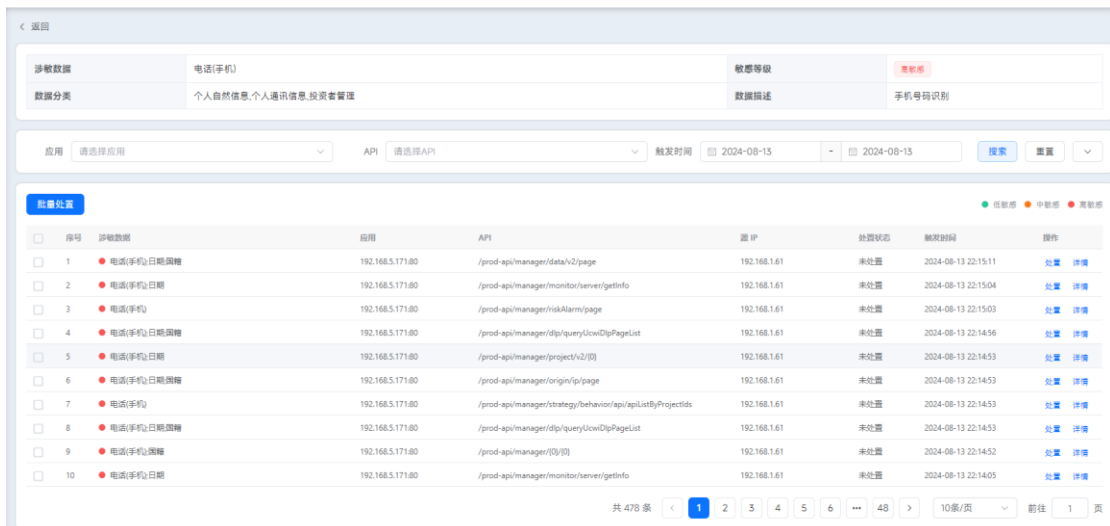


图：数据分析页

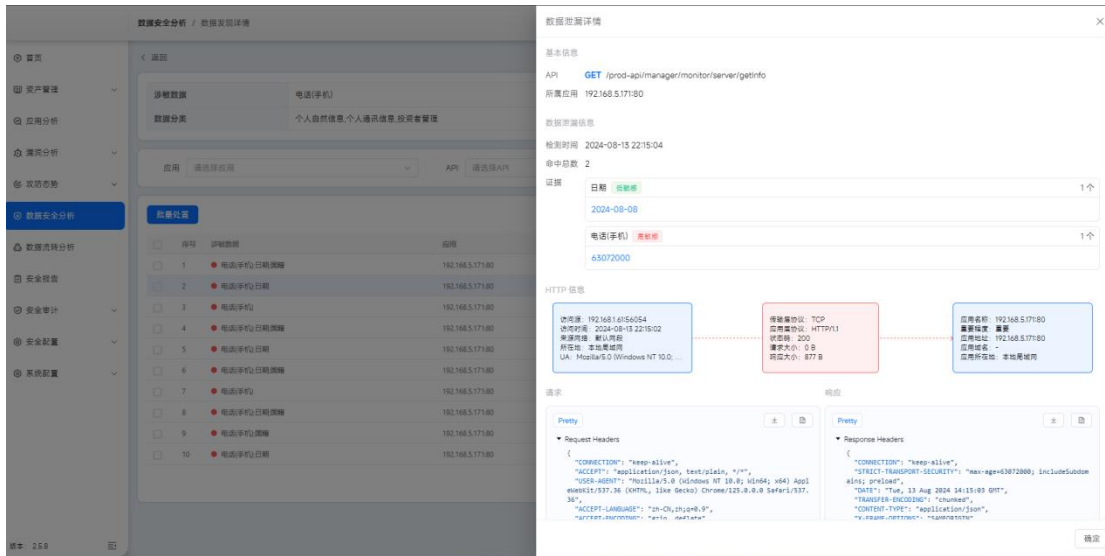
- 头部统计：统计触发标签的 API 总数、根据风险等级统计 API 数
- 周涉敏数据泄露统计 TOP10：统计近 7 日的涉敏数据触发次数排行表。
- 涉敏数据访问趋势：显示近 7 日各等级数据标签的触发次数趋势。
- 涉密数据列表：显示触发过的所有数据标签，并且统计涉及的应用数量、API 数量。
- 搜索：根据选择的条件，筛选出对应的数据标签。

8.2. 数据详情

显示数据标签的简要信息（涉敏数据、敏感等级、数据分类、数据描述），以及触发该数据标签的 API 数据、及溯源页。

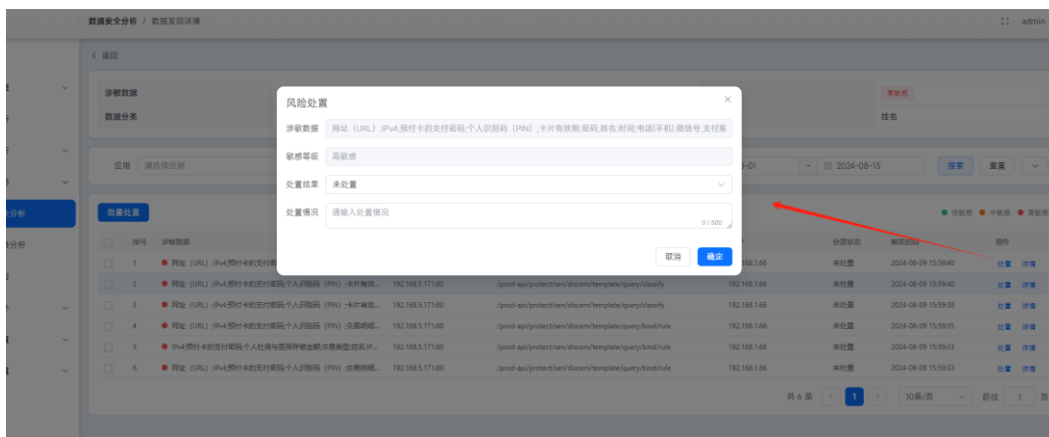


图：数据安全分析-详情

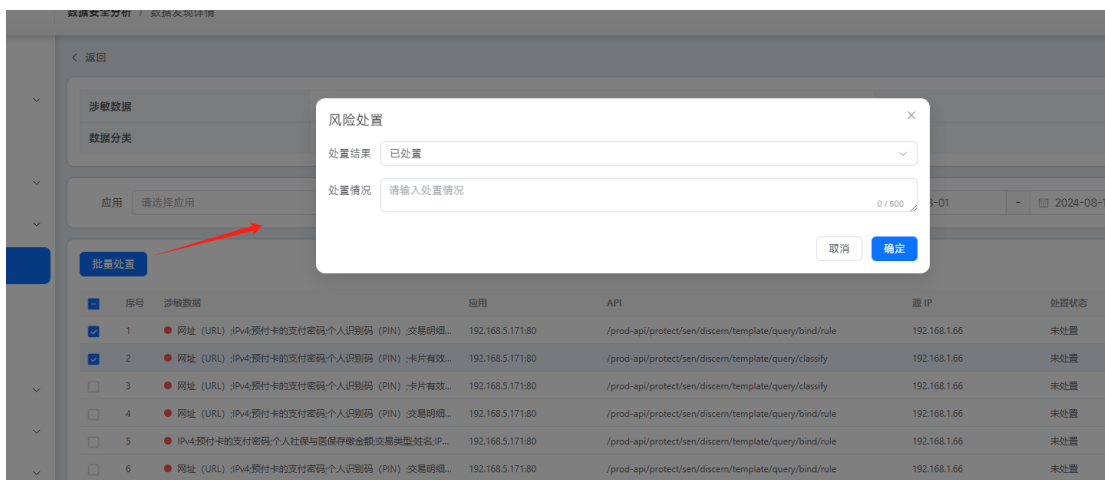


图：数据安全分析-详情-溯源页

- 点击【处置】，可以根据实际情况，对数据标签进行做“处置”动作，可以是单条处理，也可批量处理，处置的间断分为：未处置、处置中、已处置。



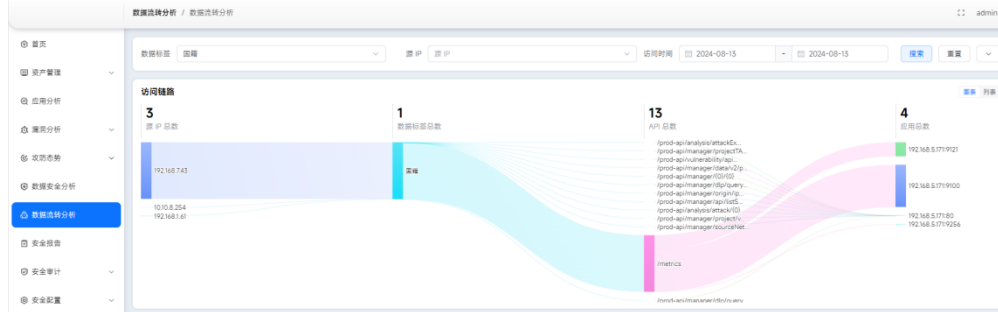
图：数据安全分析-详情-单条处置



图：数据安全分析-详情-批量处置

9. 数据流转分析

显示从源 IP 到应用的数据流转分析，主要流转链路是：源 IP -> 数据标签 -> API -> 应用。



图：数据流转分析

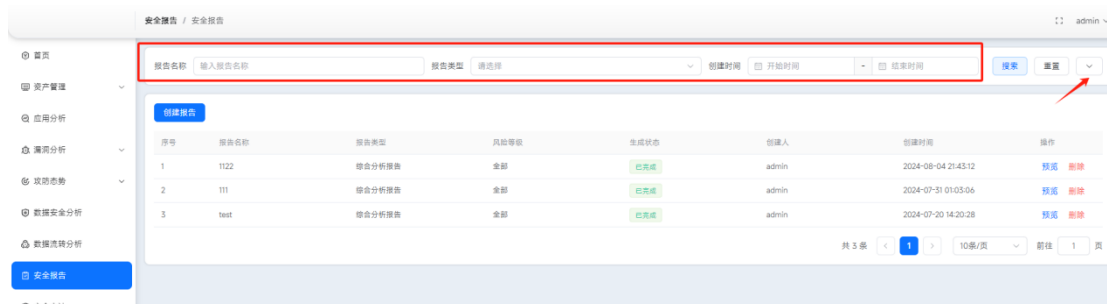
10. 安全报告

可自定义选择应用生成报告，不同维度分析报告：综合报告、资产漏洞报告、攻击风险报告、数据安全报告等。



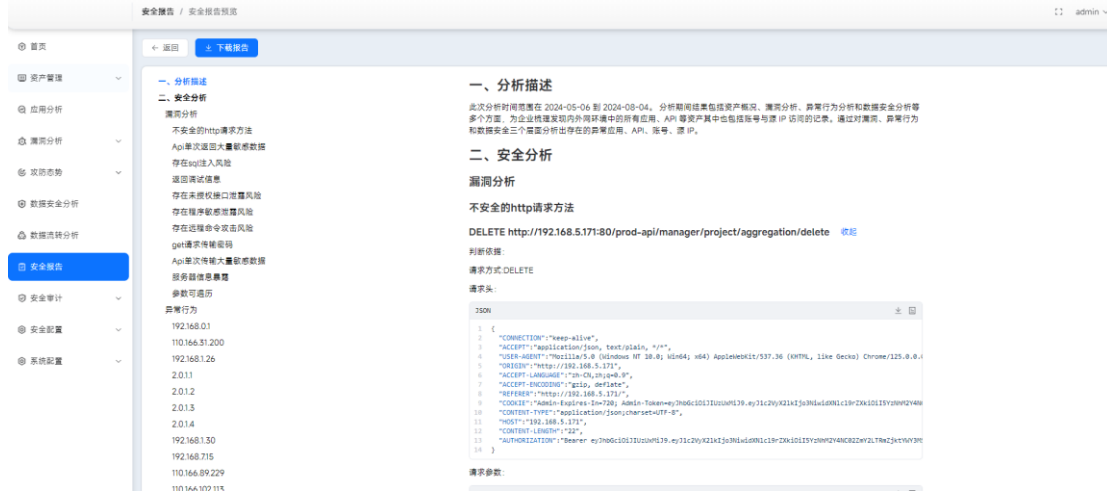
图：创建安全报告

点击【搜索】，可通过条件进行筛选



图：安全报告列表-搜索

点击【预览】可查看报告结果



图：安全报告-预览

点击【下载】，可将生成的报告以 PDF 的形式下载至本地



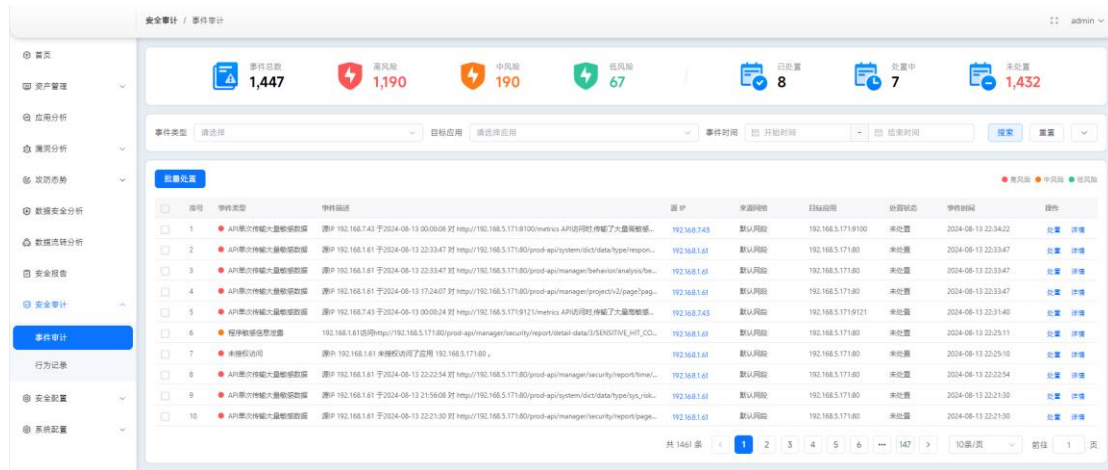
图：安全报告-下载报告

11. 安全审计

11.1. 事件审计

事件审计主要是用来统计用户的访问记录、记录访问 IP、根据访问频率判断是否是正常访问并统计异常 IP。

点击【事件审计】显示事件总数、高风险事件数、中风险事件数、低风险事件数，根据处置状态统计事件数量、事件列表。



图：安全审计 - 事件审计

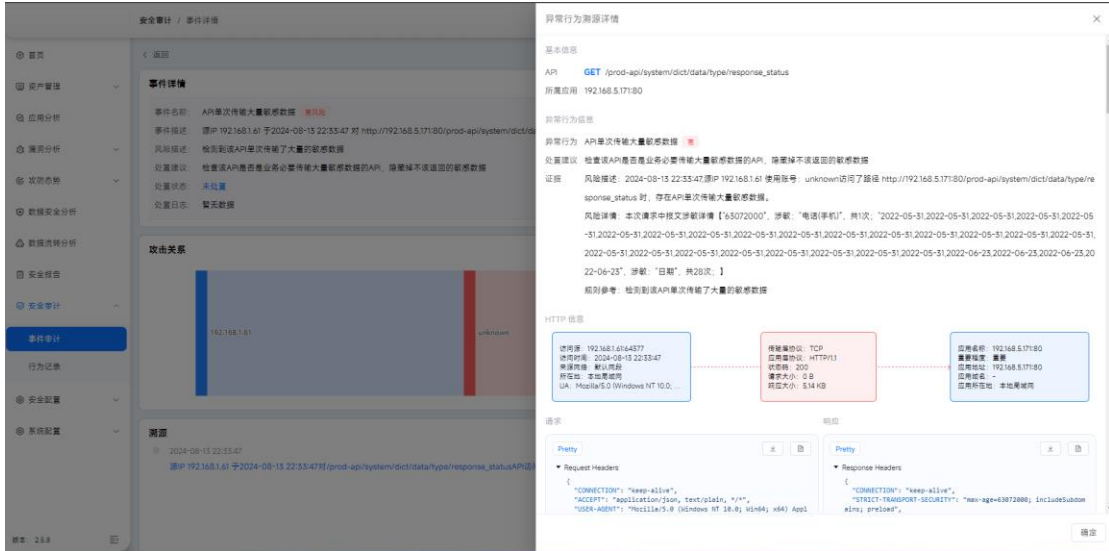
点击【搜索】，可根据事件类型、目标应用、事件时间、风险等级、源 IP、来源网络、处置状态进行查询。

点击【详情】，可以查看异常行为的详细信息，事件名称、等级、描述、攻击关系等。



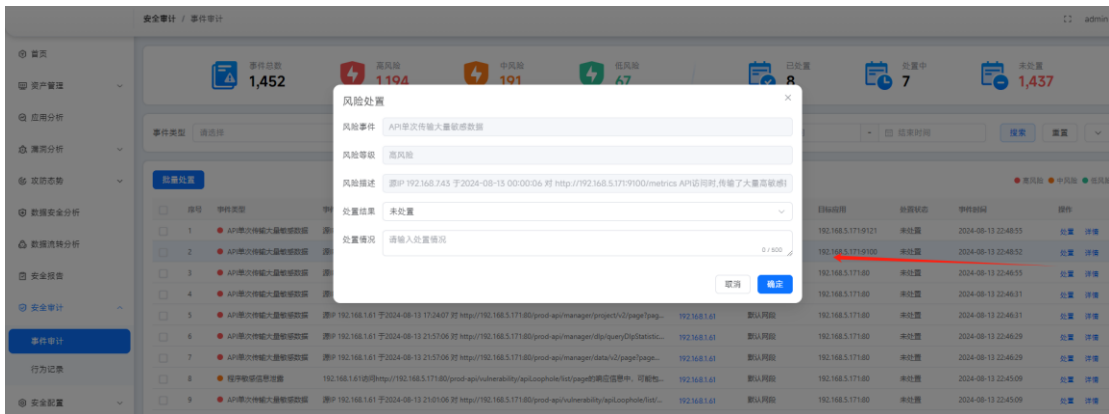
图：事件审计-溯源

点击溯源记录，可以查看详细的记录数据。



图：事件审计-溯源-详情

点击【处置】，可以根据实际情况，对事件进行做“处置”动作，可以是单条处理，也可批量处理，处置的间断分为：未处置、处置中、已处置。



图：事件审计-处置-单条



图：事件审计-处置-批量

11.2. 行为记录

点击【行为记录】，默认显示为最近一小时的数据；可按照源 IP、应用 IP、目标应用、API、响应状态进行搜索，点击列表右侧【详情】右侧弹出访问记录详细信息，包含源 IP、源 IP

的端口、客户端类型、地理位置、请求数据大小、目标应用、目标 API 名称、应用 IP、响应状态、响应数据大小、访问时间以及请求头、请求体、响应头和响应体。

序号	源 IP	目标应用	目标 API	状态码	访问时间	操作
1	192.168.7.43	192.168.5.171:8048	/metrics/actuator/prometheus	404	2024-08-13 22:50:25	详情
2	192.168.7.43	192.168.5.171:9121	/metrics	200	2024-08-13 22:50:25	详情
3	192.168.7.43	192.168.5.171:9100	/metrics	200	2024-08-13 22:50:22	详情
4	192.168.7.43	192.168.5.171:9256	/metrics	200	2024-08-13 22:50:19	详情
5	192.168.7.43	192.168.5.171:8048	/metrics/actuator/prometheus	404	2024-08-13 22:50:10	详情
6	192.168.7.43	192.168.5.171:9308	/metrics	200	2024-08-13 22:50:09	详情
7	192.168.7.43	192.168.5.171:9100	/metrics	200	2024-08-13 22:50:07	详情
8	192.168.7.43	192.168.5.171:9256	/metrics	200	2024-08-13 22:50:04	详情
9	192.168.1.61	192.168.5.171:80	/prod-api/manager/hikAlarm/page	200	2024-08-13 22:50:02	详情
10	192.168.1.61	192.168.5.171:80	/prod-api/manager/monitor/server/getInfo	200	2024-08-13 22:50:02	详情

图：行为记录-列表

点击【搜索】，可以源 IP、目标应用、目标 API、响应状态、访问时间进行查询。

图：行为记录-搜索

点击【详情】，显示记录的具体信息。

行为记录详情

基本信息

API GET /metrics

所属应用 192.168.5.171:9308

HTTP 信息

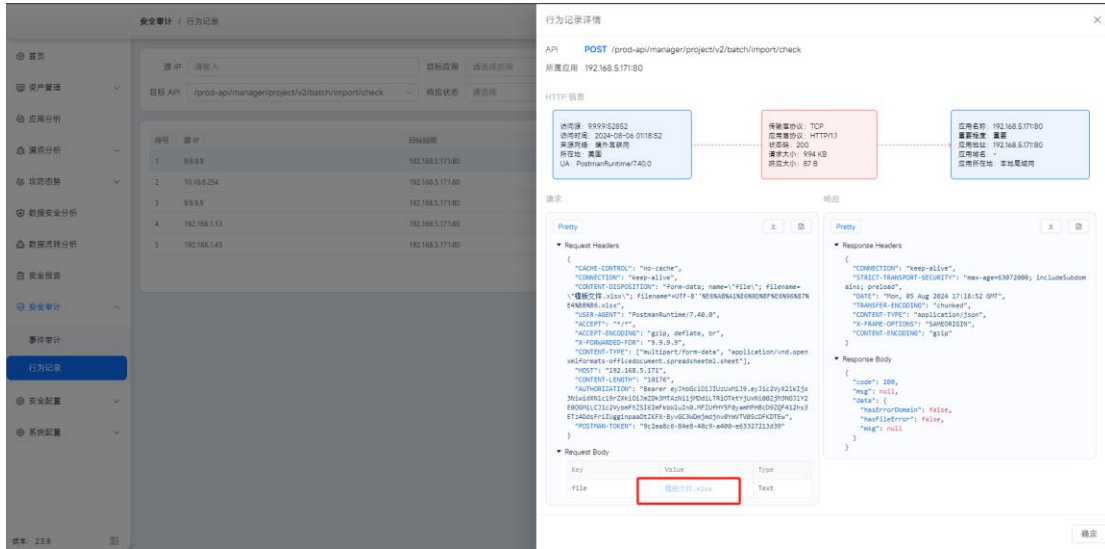
请求

```
Request Headers: {"USER-AGENT": "Prometheus/2.45.1", "ACCEPT": "application/openmetrics-text;version=1.0.0,application/openmetrics-text;version=0.1.0;q=0.75,text/plain;version=0.0.4;q=0.5,*/*;q=0.1", "ACCEPT-ENCODING": "gzip", "X-PROMETHEUS-SAMPLE-TIMEOUT-SECONDS": "30", "HOST": "192.168.5.171:9308"}
```

响应

```
Response Headers: {"DATE": "Tue, 13 Aug 2024 14:50:09 GMT", "TRANSFER-ENCODING": "chunked", "CONTENT-TYPE": "text/plain; version=0.0.4; charset=utf-8", "CONTENT-ENCODING": "gzip"}
```

图：行为记录-详情-无文件



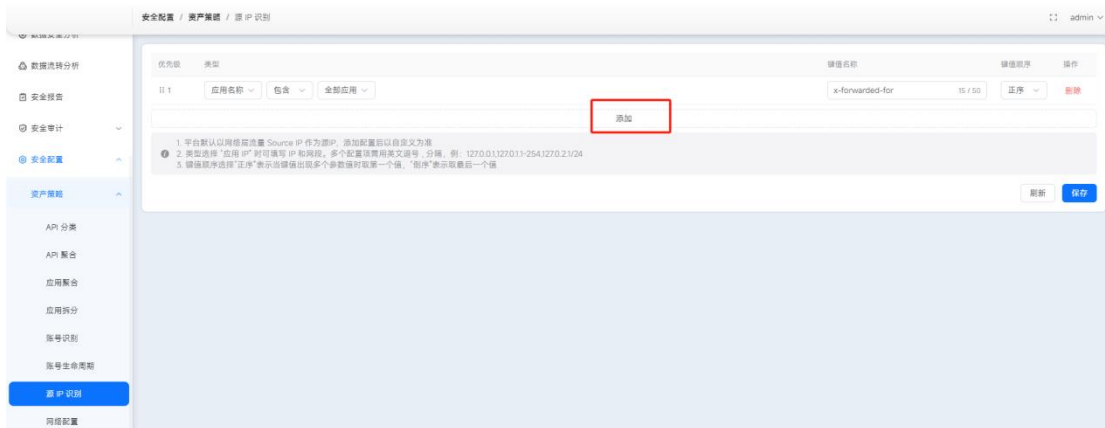
图：行为记录-详情-有文件

12. 安全配置

12.1. 资产策略

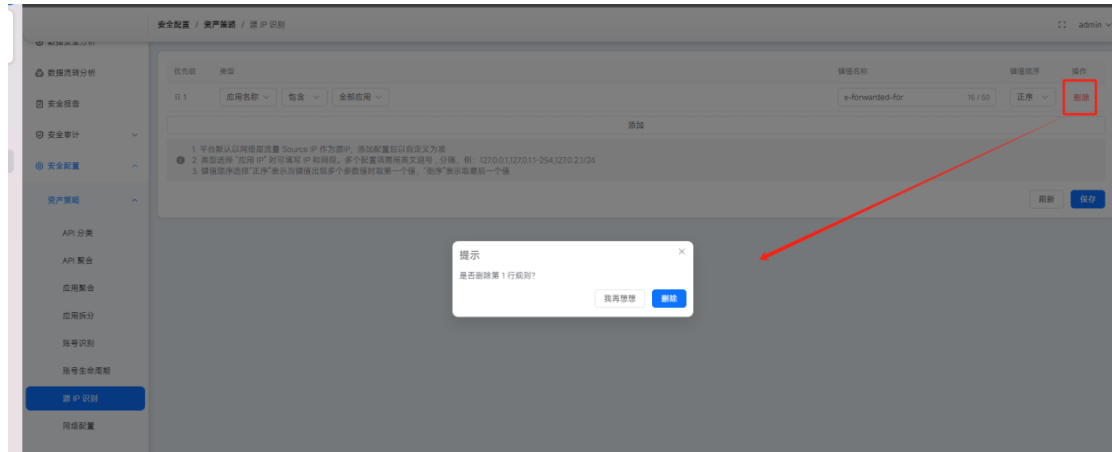
12.1.1. 源 IP 识别

点击【添加】，可新增识别源 IP 的规则，根据不同维度（应用名称、应用 IP、应用域名）和参数（比如 x-real-ip,可自定义）



图：源 IP 规则添加

点击【删除】，可对配置项进行删除操作



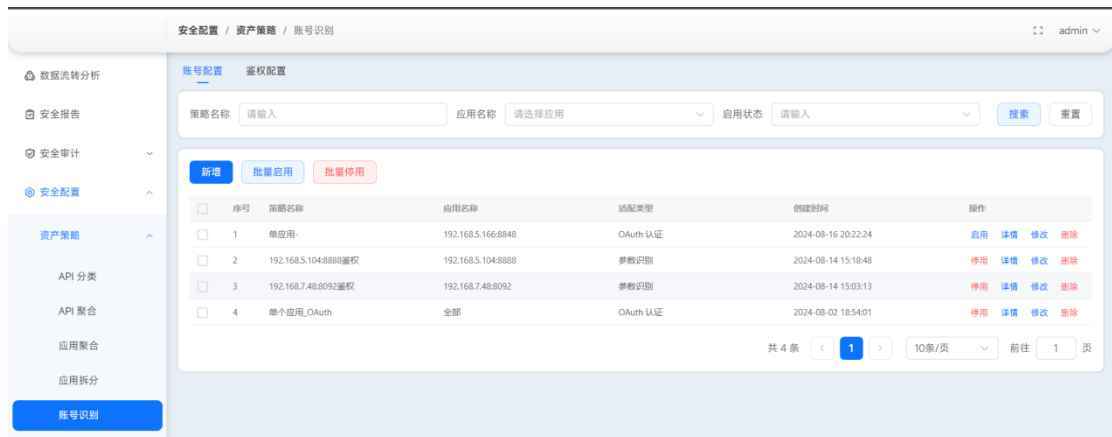
图：源 IP 规则-删除

12.1.2. 账号识别

账号识别主要用于识别流量中的账号，并且通过账号信息识别一些风险事件。账号识别根据使用场景，分为账号配置、鉴权配置两种。

- 账号配置

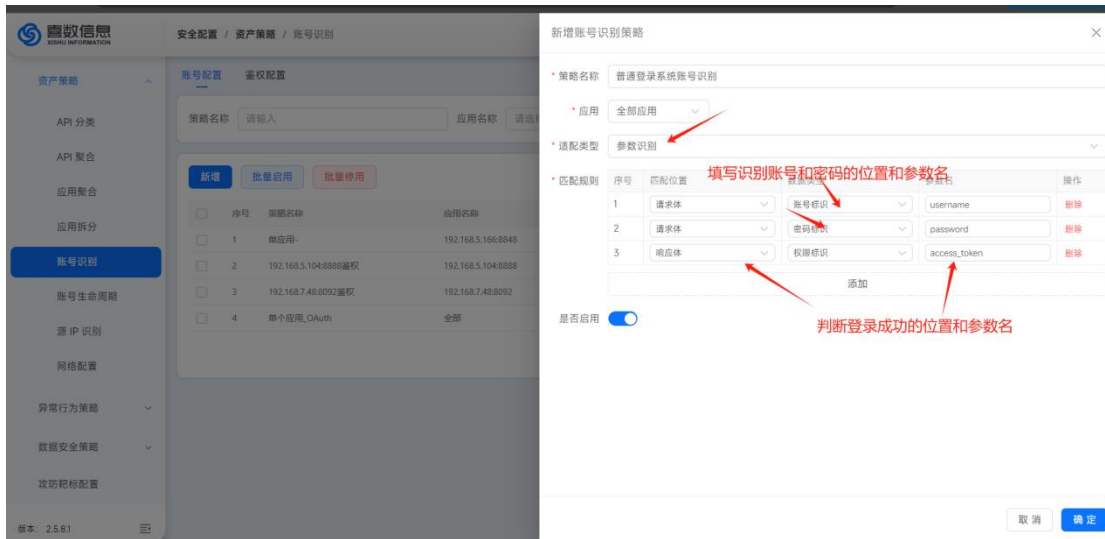
点击【账号配置】，打开识别账号的配置页，此处支持普通的登录和 SSO 登录。



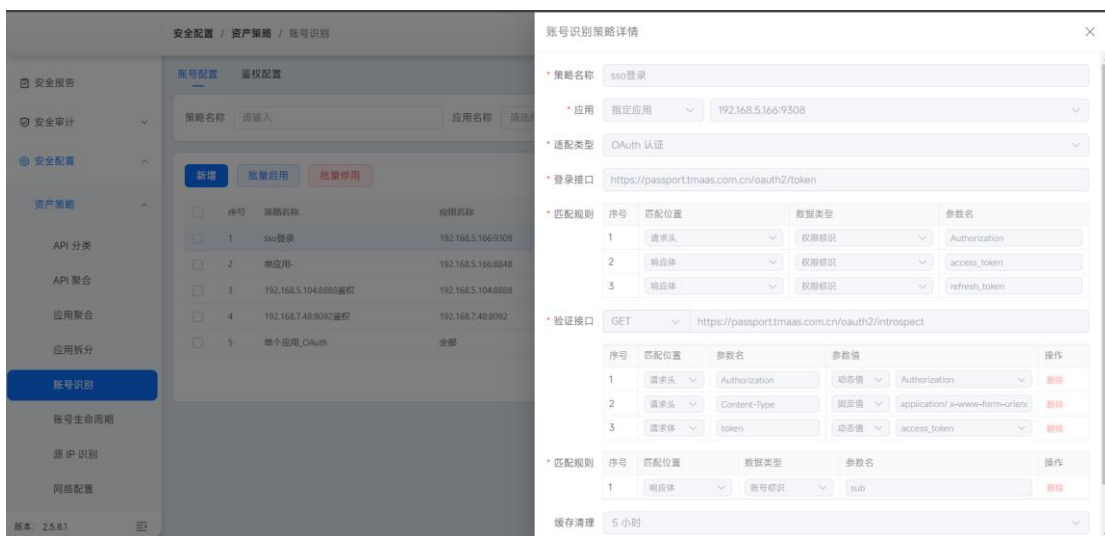
图：账号识别-账号配置

点击“搜索”，根据选择的筛选条件，搜索出账号配置对应的数据。

点击【新增】按钮，根据接入的系统登录类型，配合账号识别的规则。

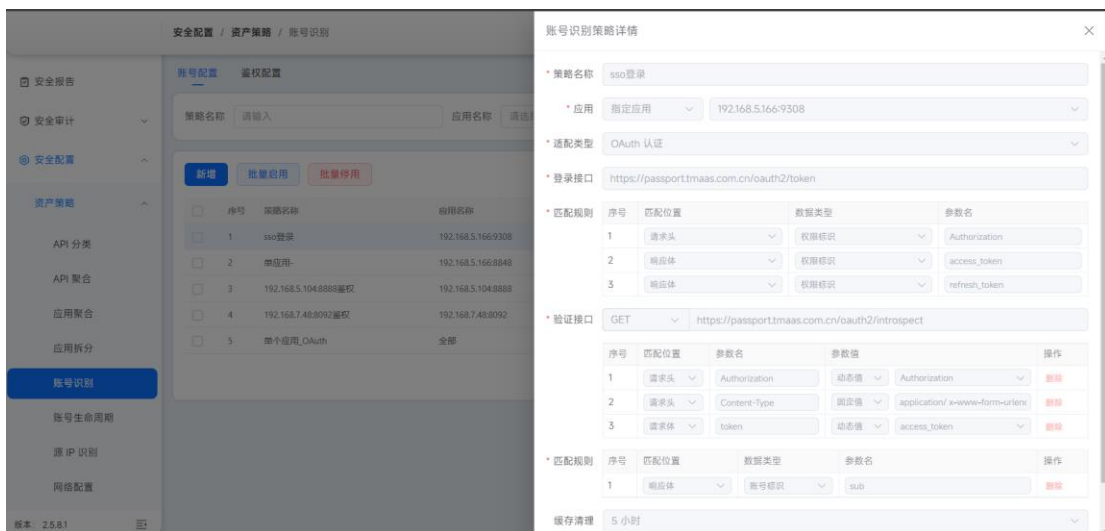


图：账号识别-账号配置-新增普通登录账号识别



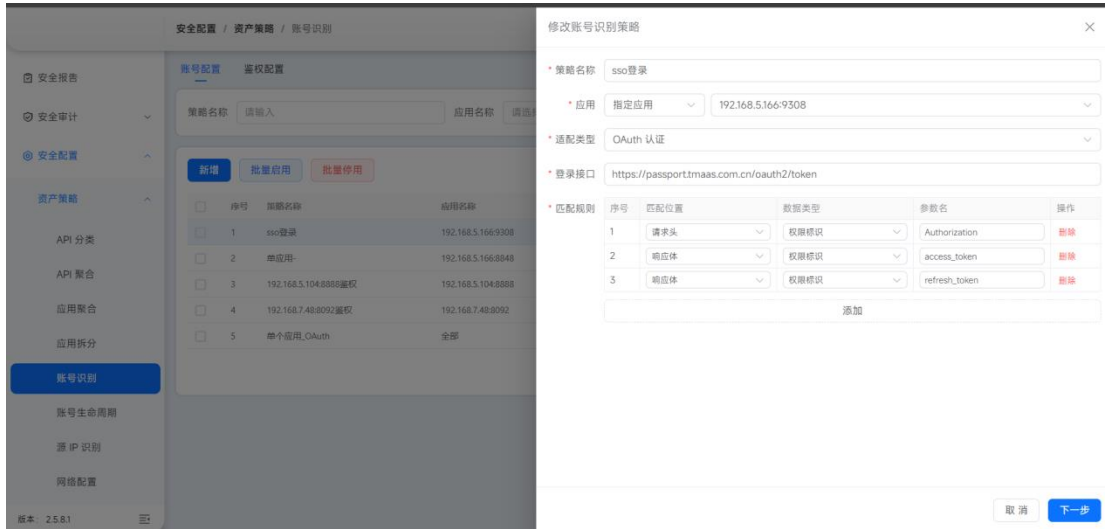
图：账号识别-账号配置-新增 SSO 登录账号识别

点击【详情】，可查看账号识别详情菜单。



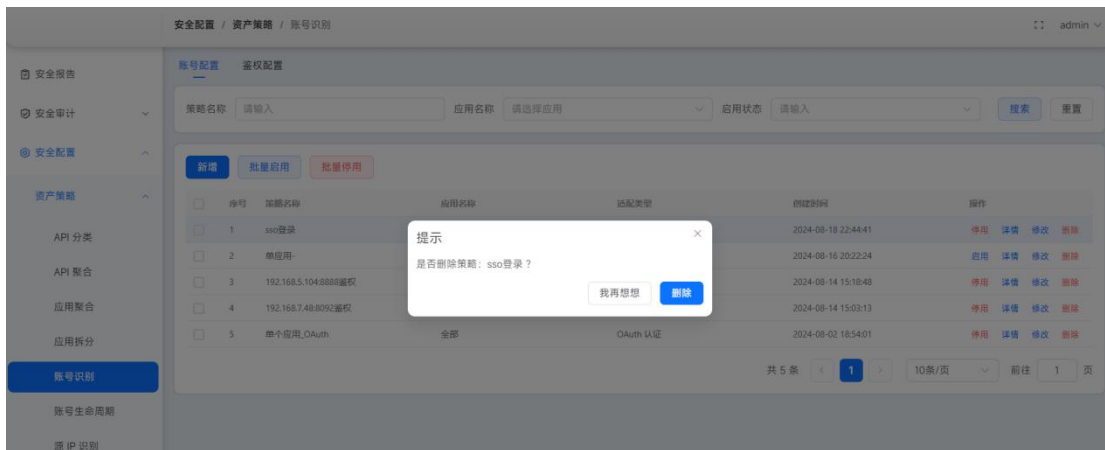
图：账号配置-详情

点击【修改】，可以修改账号识别信息。



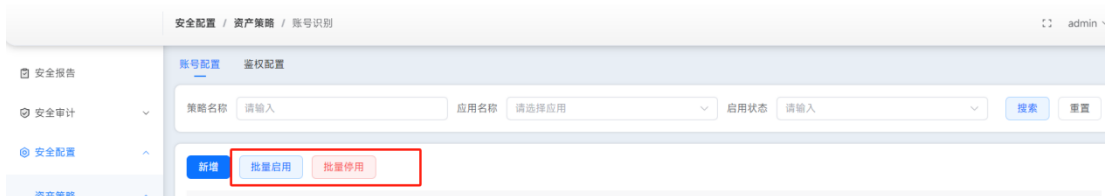
图：账号配置-修改

点击【删除】提示是否删除所选数据，点击确认则删除成功，点击取消则取消本次删除。



图：账号配置-删除

点击【批量启用/批量停用】，批量处理账号配置规则。



图：账号配置-批量启用/停用

点击【启用/停用】，单个处理账号配置规则。

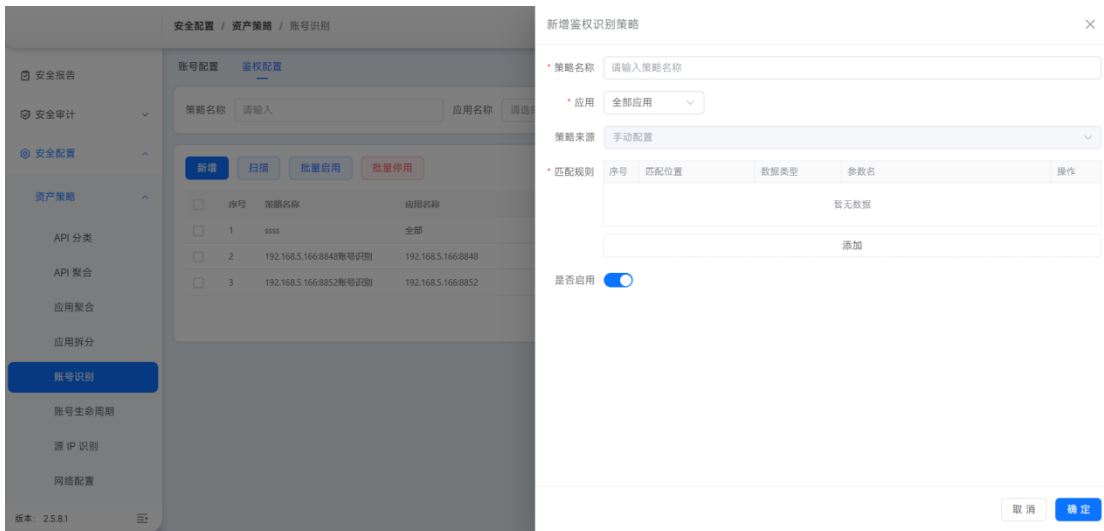
序号	策略名称	应用名称	适配类型	创建时间	操作
1	sso登录	192.168.5.166-9308	OAuth 认证	2024-08-18 22:44:41	停用 详情 修改 删除
2	单应用-	192.168.5.166-8848	OAuth 认证	2024-08-16 20:22:24	启用 详情 修改 删除
3	192.168.5.104-8888鉴权	192.168.5.104-8888	参数识别	2024-08-14 15:18:48	停用 详情 修改 删除
4	192.168.7.48-8092鉴权	192.168.7.48-8092	参数识别	2024-08-14 15:03:13	停用 详情 修改 删除
5	单个应用_OAuth	全部	OAuth 认证	2024-08-02 18:54:01	启用 详情 修改 删除

图：账号配置-单个启用/停用

● 鉴权配置

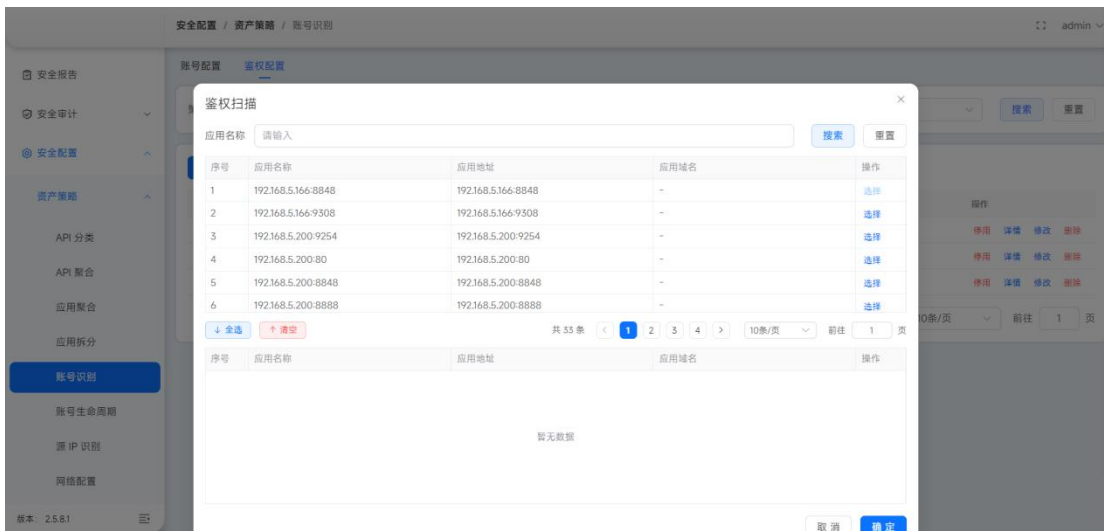
支持配置鉴权的规则，便于系统识别出风险事件。

点击【新增】，添加鉴权的规则。



图：鉴权配置-新增

点击【扫描】，选择要扫描的应用，点击开始扫描，扫描成功后页面会出现本次选择。扫描应用的信息且匹配类型为业务。



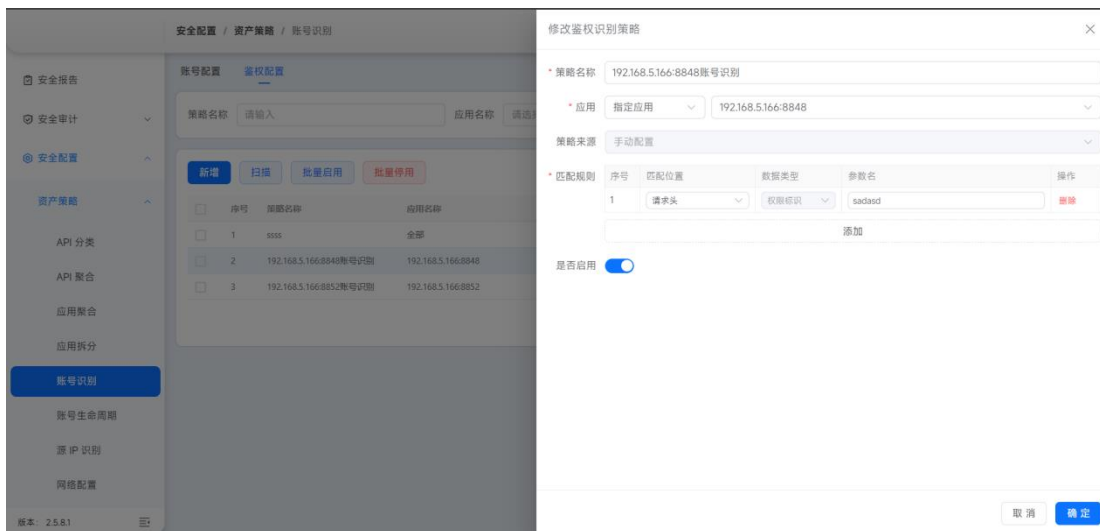
图：鉴权配置-扫描

点击【详情】，显示鉴权规则的详细信息。



图：鉴权配置-详情

点击【修改】，修改鉴权规则的内容。



图：鉴权配置-修改

点击【搜索】，根据选择的筛选条件，搜索出对应的鉴权规则。



图：鉴权配置-搜索

点击【批量启用/停用】，批量开启/停用鉴权配置规则。



图：鉴权配置-批量启用/停用

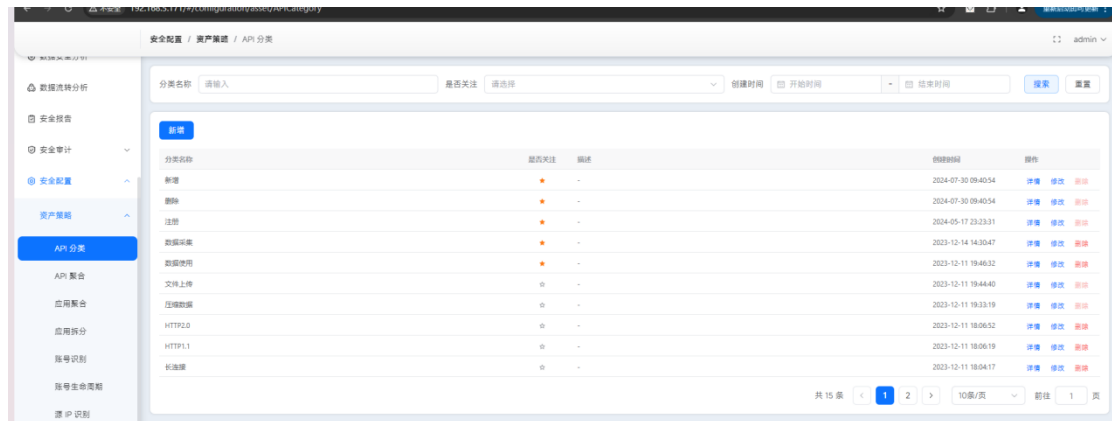
点击【单个启用/停用】，单个开启/停用鉴权配置规则。



图：鉴权配置-单个启用/停用

12.1.3. API 分类

点击【API 分类】，显示已经添加好的 API 类型名称，系统根据标签里添加的规则识别 API 类型，对 API 打标签。



图：API 分类-列表

点击【新增】，自定义添加 API 分类标签，输入类型名称，选择匹配规则，匹配规则根据不同的数据进行选择添加，点击确定。



图：API 分类-新增

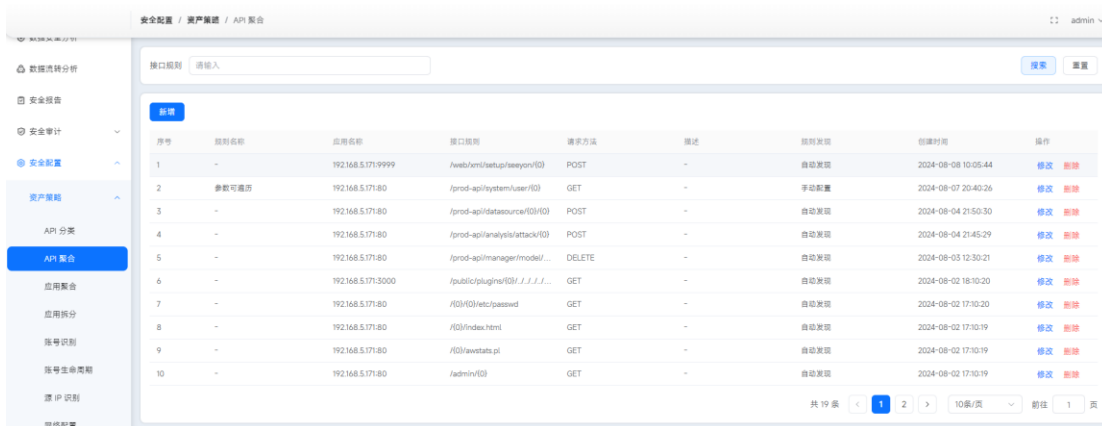
点击【详情】，显示已配置好的数据类型。

点击【修改】，可以修改已配置好的数据类型。

点击【删除】，弹出对话框，点击删除，可以删除已配置好的数据类型，点击取消返回。

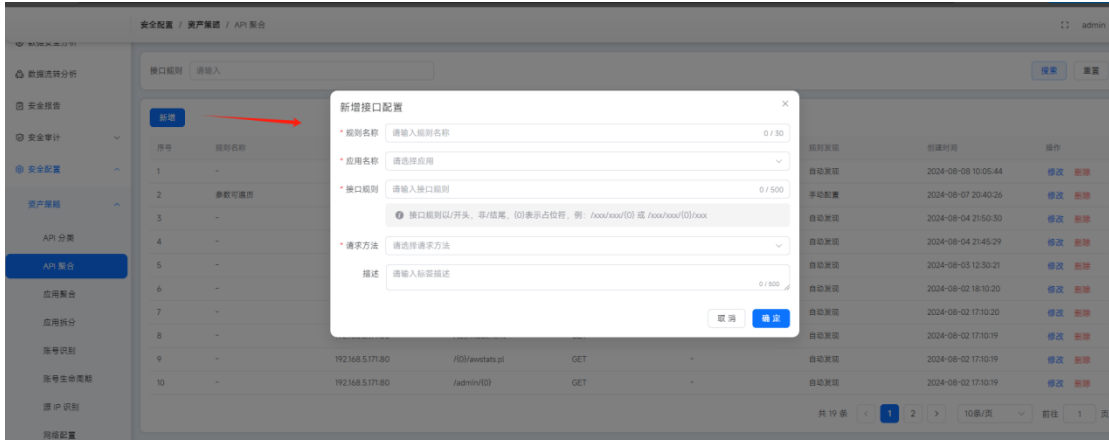
12.1.4. API 聚合

点击【API 聚合】，显示接口配置信息，可以根据接口规则进行模糊查询数据



图：API 聚合-列表

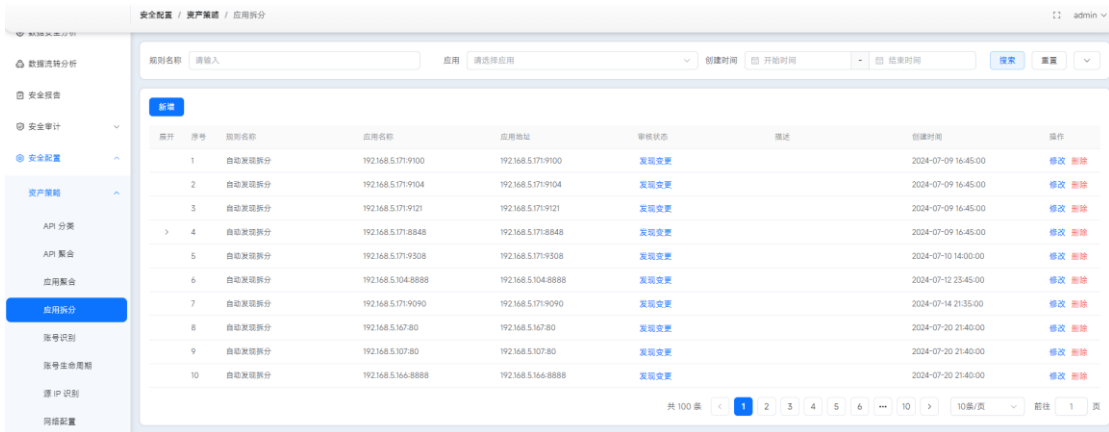
点击新增，可以添加新的接口规则，可以将符合规则的接口进行合并，其规则分为自动发现和手动发现，手动发现是指手动的去配置接口配置信息，配置完成之后如果是规则相同的接口则不会显示多条 API 记录了



图：API 聚合-新增

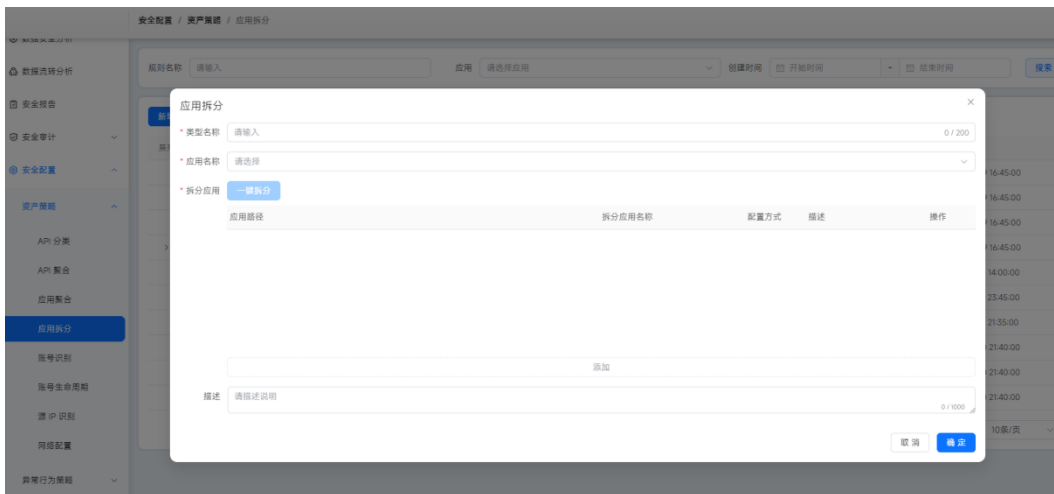
12.1.5. 应用拆分

内置机器学习自动拆分应用功能，每天执行定时任务对未拆分的原始应用进行分析，自动生成待确认的拆分规则记录，人工确认后拆分规则生效；也可新增自定义拆分规则。



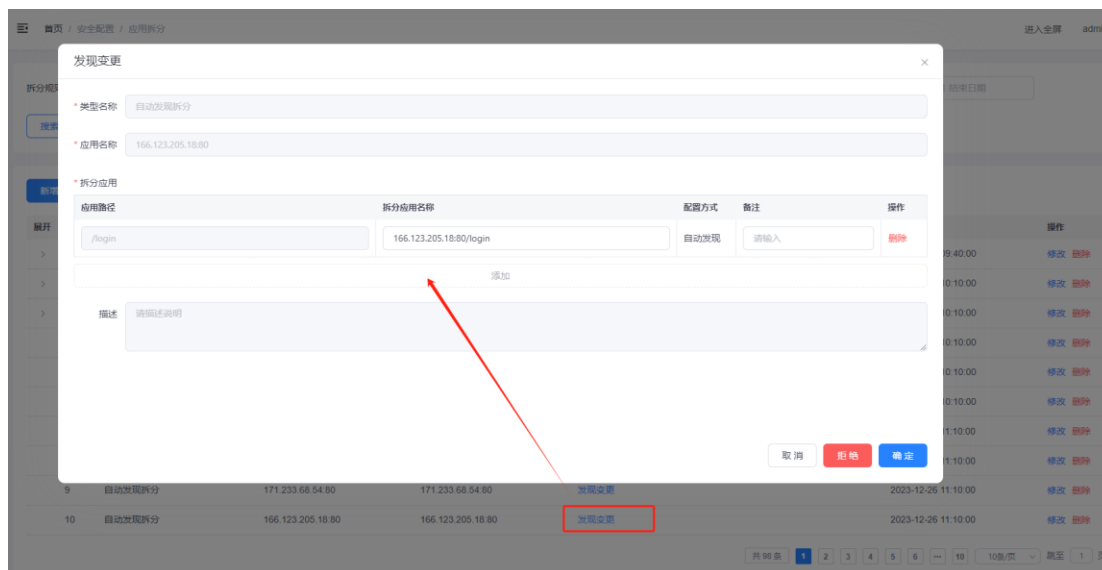
图：应用拆分-规则列表

点击【新增】，可选择应用及应用路径进行拆分



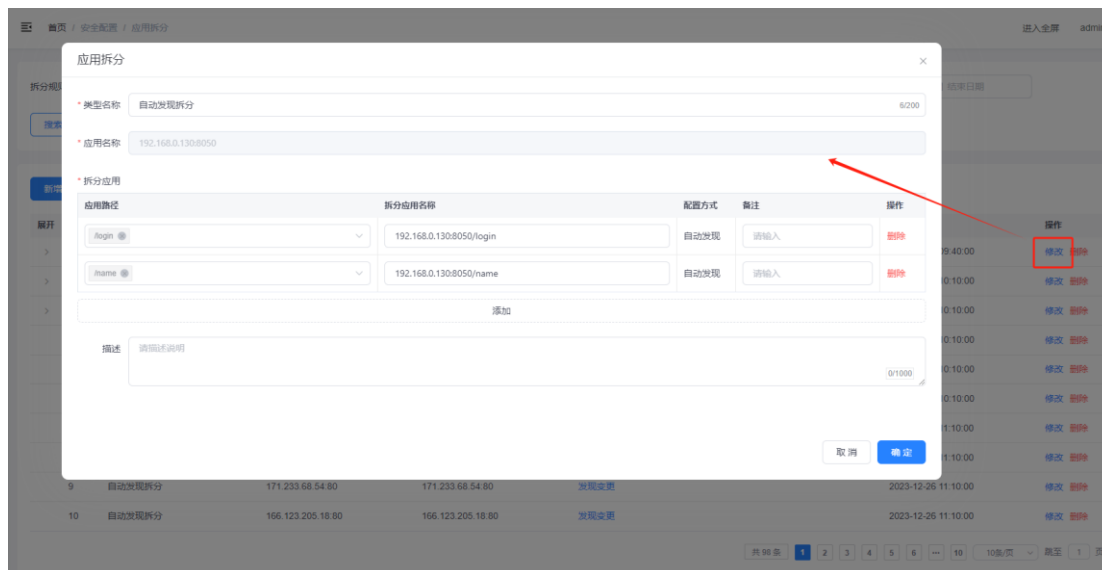
图：应用拆分-新增规则

点击【发现变更】，可查看机器学习自动拆分的应用列表，点击【确定】将进行拆分，点击【拒绝】则不拆分



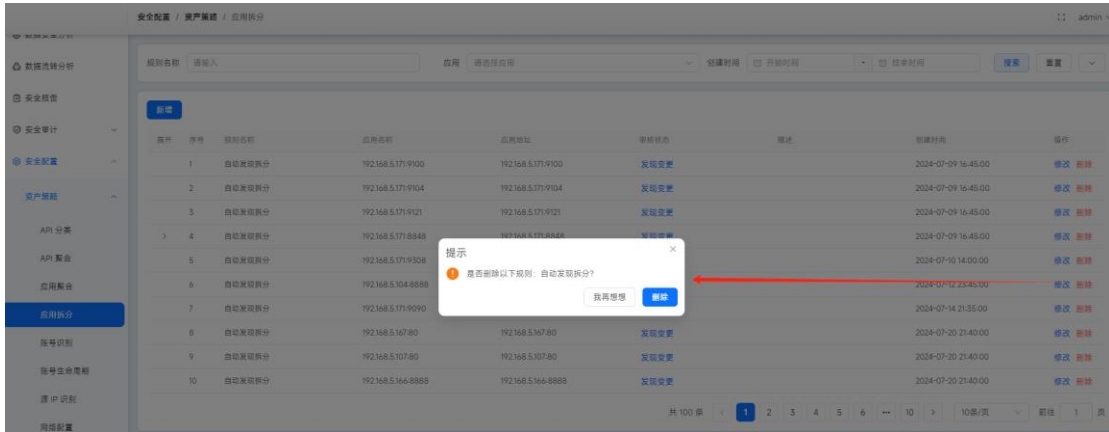
图：应用拆分-确认/拒绝规则

点击【修改】，可对类型名称，拆分应用及描述等进行修改操作



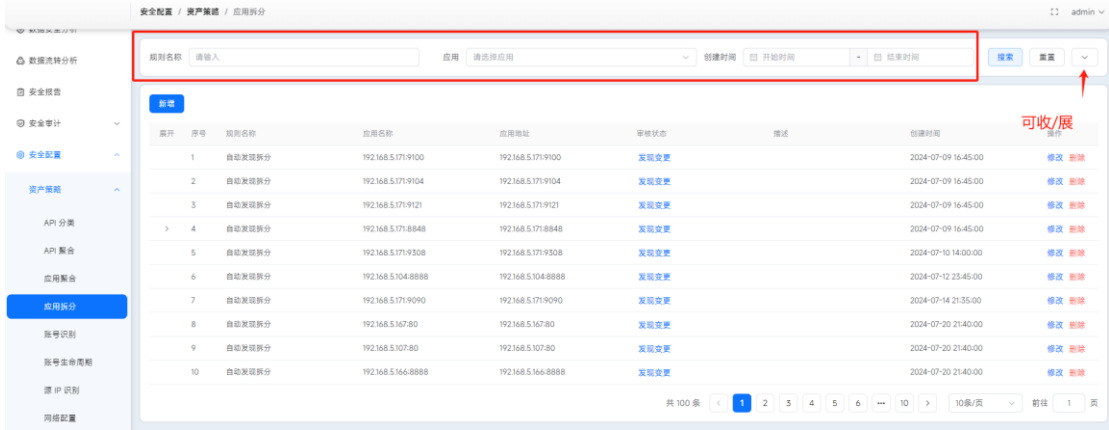
图：应用拆分-规则修改

点击【删除】，弹出确认弹窗，点击【删除】删除该条配置，点击【我再想想】撤销本次删除操作



图：应用拆分-规则删除

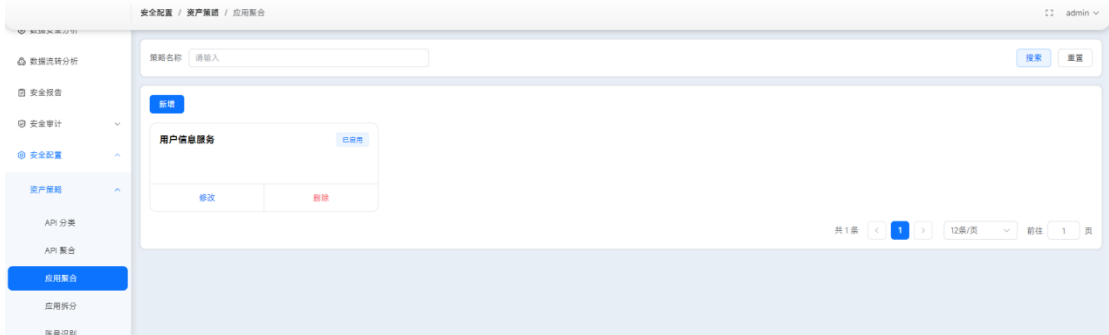
点击【搜索】，可输入搜索条件对列表进行检索



图：应用拆分-搜索

12.1.6. 应用聚合

点击【应用聚合】，显示已经添加好的聚合策略，系统根据所选的应用进行聚合。



图：应用聚合

点击【新增】，自定义添加聚合策略，输入策略名称、应用名称，选择所需要聚合的应用，已经聚合过的应用不能再次选择。



图：应用聚合-新增

点击【修改】，可以修改自定义的配置

点击【搜索】，输入策略名称，可以进行模糊查询。

点击【删除】，弹出对话框，点击删除，可以删除已配置好的自定义应用聚合，该配置下的应用将不会以聚合状态显示，点击取消返回。

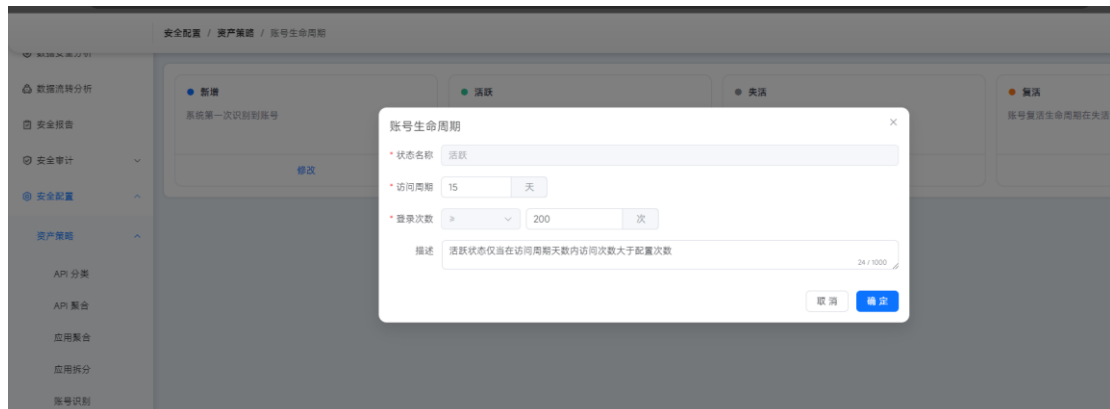
12.1.7. 账号生命周期

系统内置生命周期规则，每日进行定时任务对系统已识别的账号更新其生命周期；可自定义修改参数



图：账号生命周期

点击【修改】，可自定义访问周期以及登录次数阈值

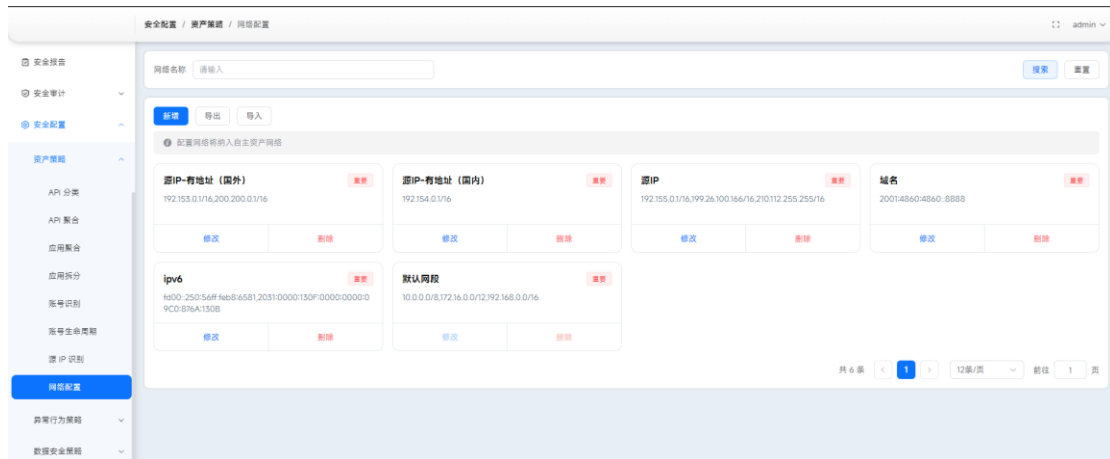


图：账号生命周期-修改

12.1.8. 网络配置

该部分的网络配置，主要用于识别自主应用，并且源 ip 的所属网络和所在地亦是根据此处的网络进行判断。

【网段列表】显示有效的网络配置信息



图：网络配置-列表

【筛选】根据网络名称，模糊匹配

点击【新增】，填写配置名、网段地址、所在地、重要程度，确定后新增配置



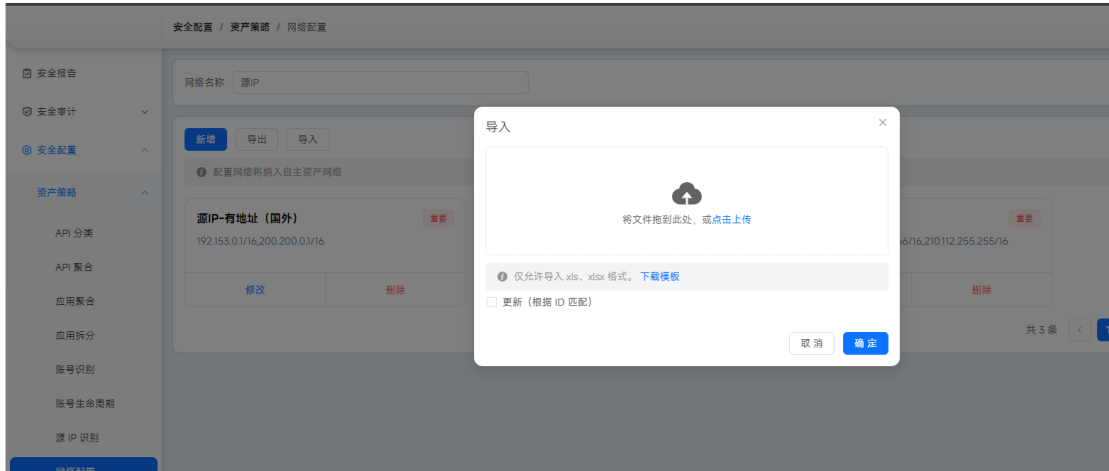
图：网络配置-新增

点击【修改】，可以对自定义的配置进行修改信息

点击【删除】，删除自定义的配置信息

点击【导出】，以 excel 形式导出现有的配置信息

点击【导入】，可以将需要导入的文件拖至图标处，也可以点击上传选择文件导入，勾选下方框内，可导入更新已有的数据，点击下载模版，可下载 Excel 格式的来源分类模版

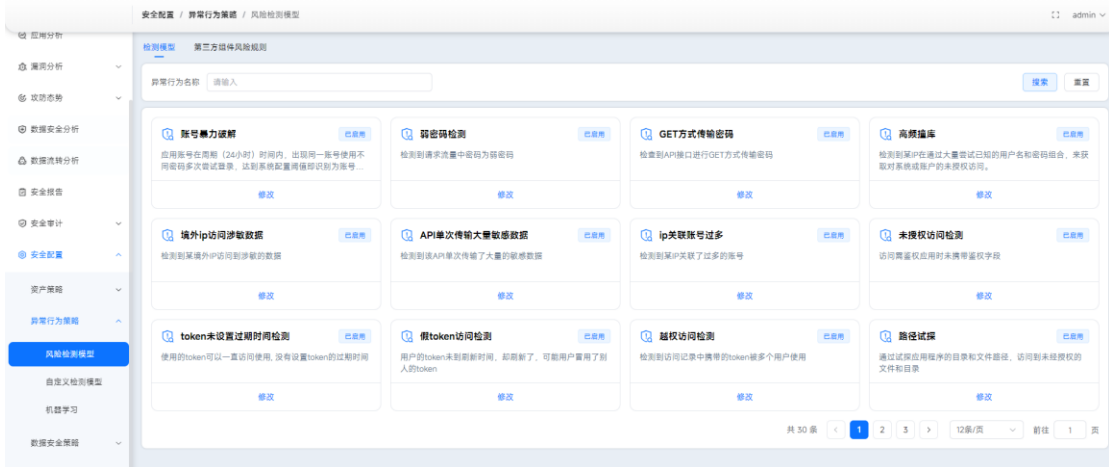


图：网络配置-导入

12.2. 异常行为策略

12.2.1. 风险检测模型

风险模型检测是用于识别应用下的异常行为和脆弱性配置页面，配置不同策略，可以对数据进行不同规则的防护。



图：风险检测模型

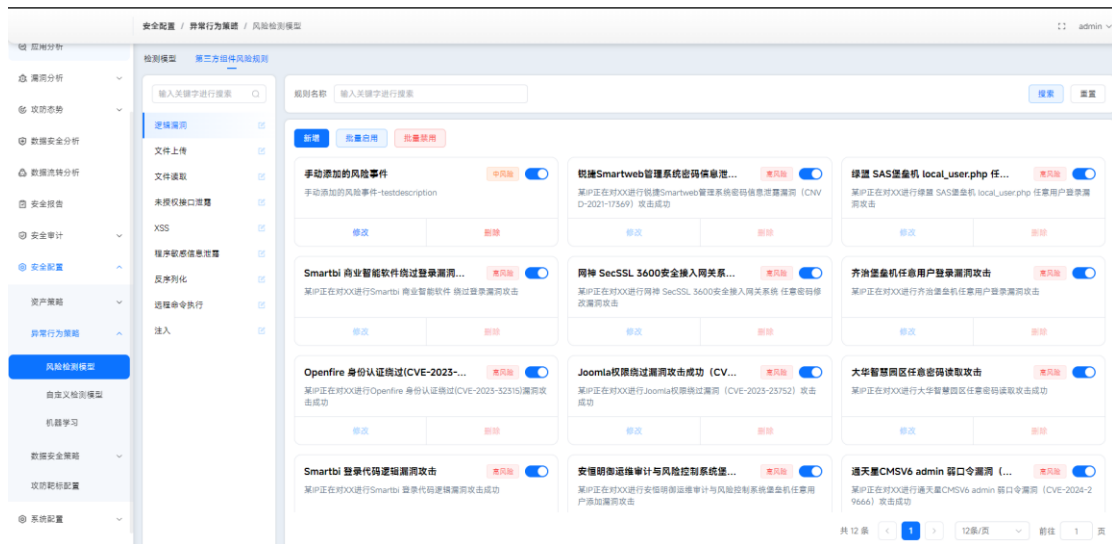
点击【修改】，显示规则详细信息，可以根据模型调整对应的参数阈值、处理建议、白名单、启用状态等，点击修改即修改成功，点击取消放弃本次修改。



图：账号暴力破解-修改

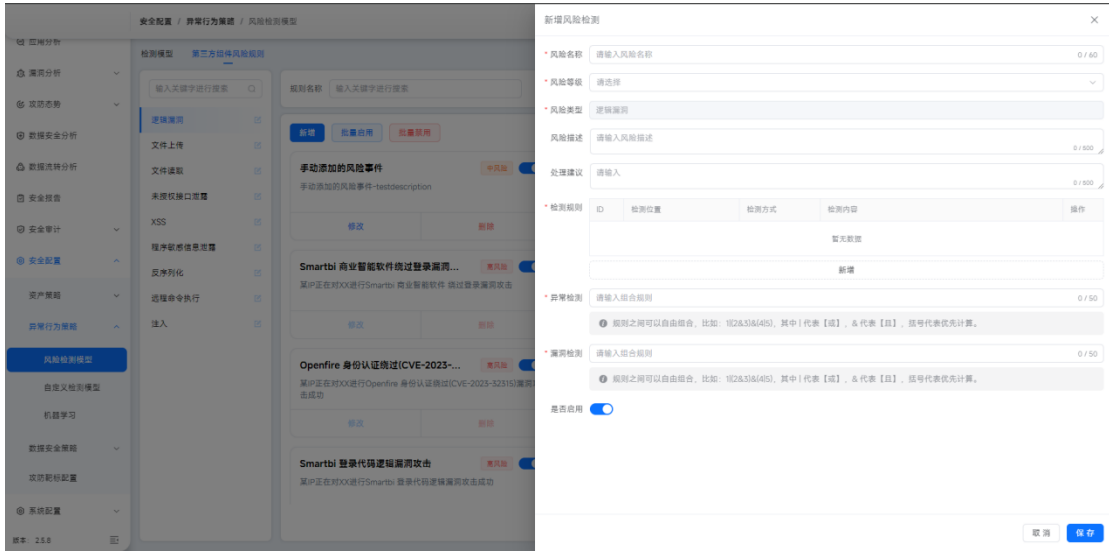
点击【搜索】，输入规则名称，点击搜索，可以进行模糊查询。

点击【第三方组件风险规则】，分类展示漏洞配置信息，左侧以列表形式展示漏洞分类，点击后右侧以卡片形式加载子项漏洞配置信息



图：风险检测模型-第三方组件风险规则

点击【新增】，可新增对应规则



图：风险检测模型-第三方组件风险规则-新增

可对规则进行【批量启用】【批量禁用】的操作

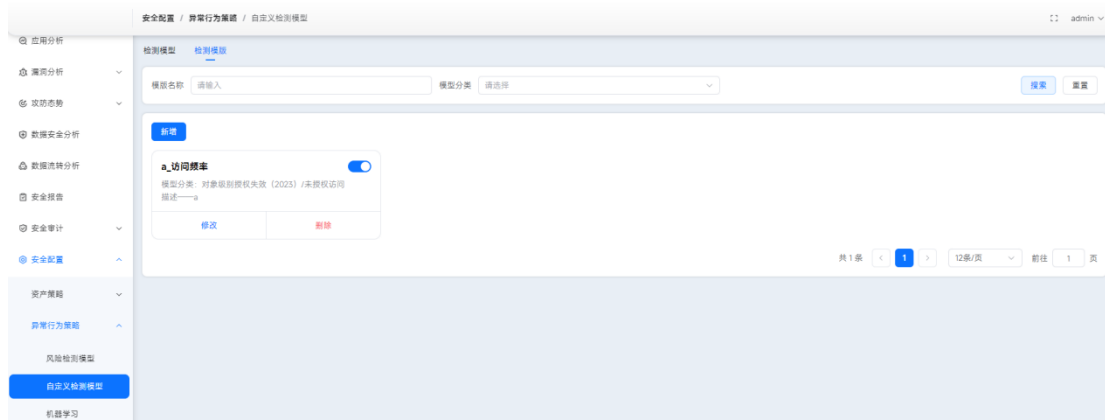


图：风险检测模型-第三方组件风险规则-批量启用/禁用

12.2.2. 自定义检测模型

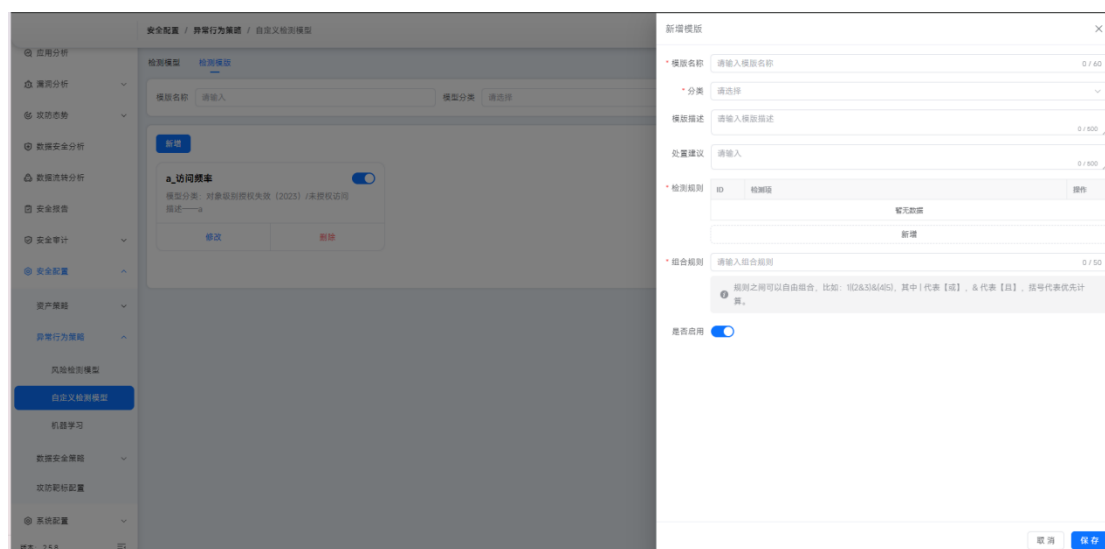
● 检测模版

系统支持的内置检测项有：访问频率、请求大小（单次）、响应大小（单次）。本模块是自定义组合内置检测项组成一个模板。



图：检测模版 - 列表

点击【增加】，可以选择不同的内置检测项，并且设置不同的组合规则，生成新的模版。



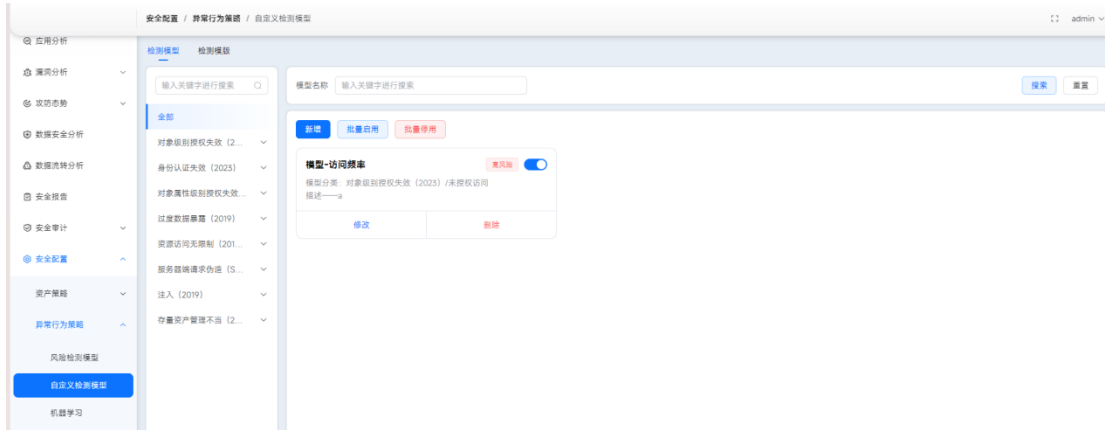
图：检测模版 - 新增

点击模版部分的【修改】，可以修改模版的基本信息。

点击【删除】，即可删除模版。

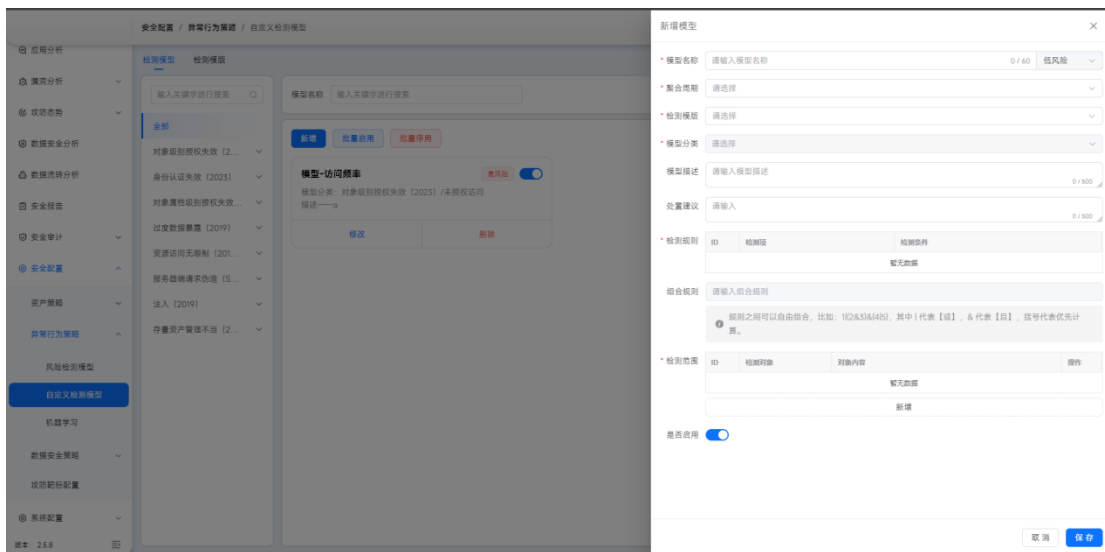
● 检测模型

根据创建的检测模版，创建不同的模型，流量会根据模型的参数进行分析，触发后结果会同步到“安全审计-事件审计”部分。



图：检测模型-列表

点击【新增】，选择检测模型，设置参数，创建出新的模型。



图：检测模型-新增

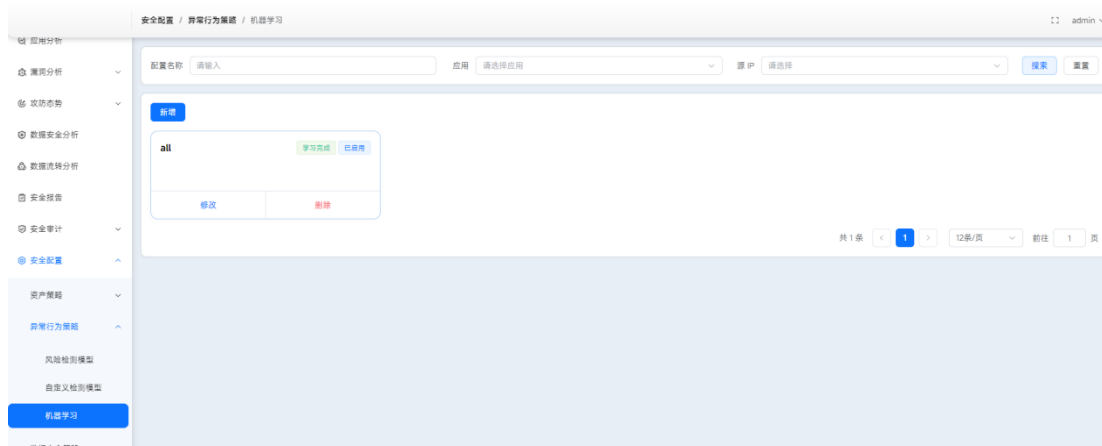
点击【修改】，可以修改模型的基础信息（比如：周期、阈值、检测范围）。

点击【删除】，删除现有的检测模型，并且失效。

点击【开启/关闭】控件，设置模型的开启状态，若关闭，流量分析时该模型则不会生效。

12.2.3. 机器学习

根据自定义访问周期对应用或源 IP 进行基线学习



图：机器学习-列表

点击【新增】，自定义学习配置



图：机器学习-新增

点击【修改】，可对配置项进行编辑操作

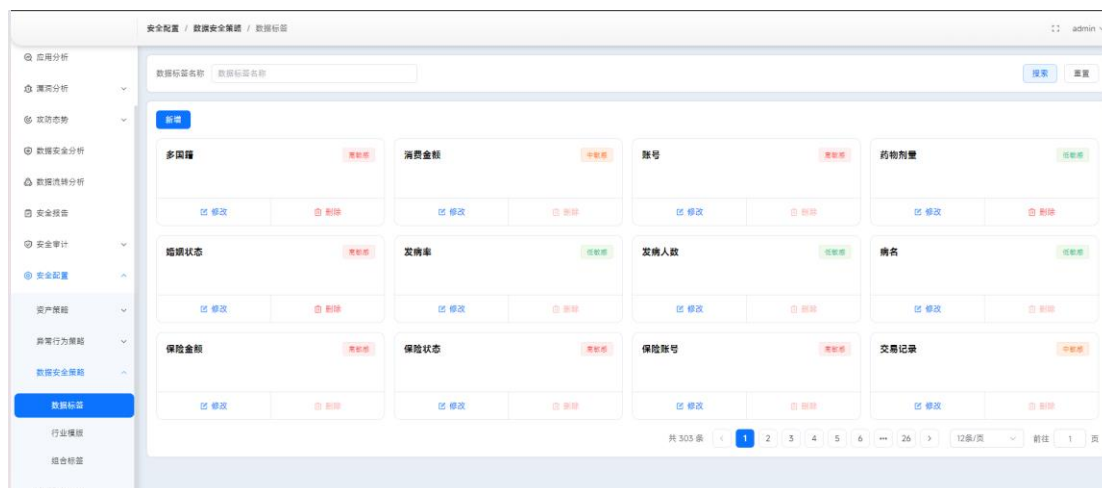
点击【删除】提示是否删除所选数据，点击确认则删除成功，点击取消则取消本次删除。

点击【搜索】，可根据自定义条件进行匹配

12.3. 数据安全检测

12.3.1. 数据标签

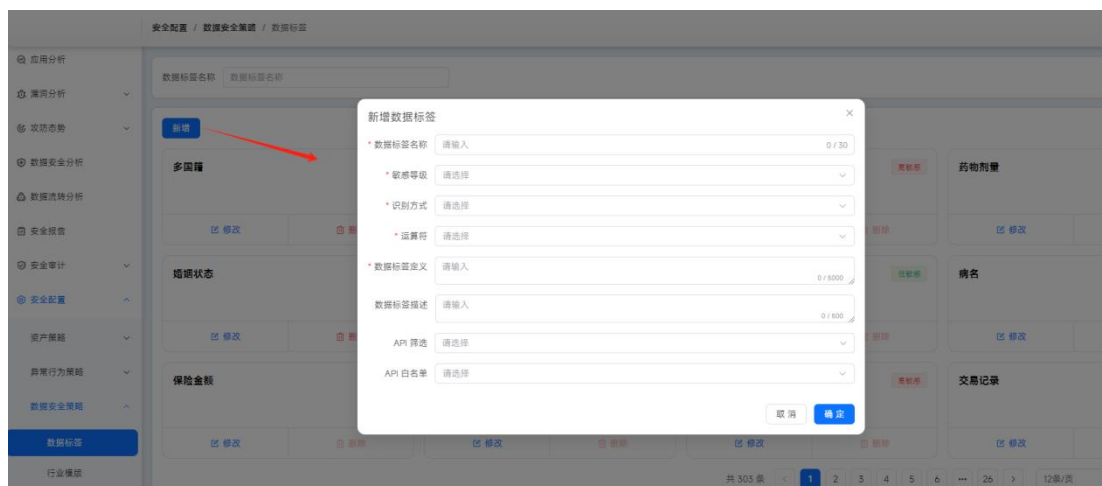
点击【数据标签】，查看敏感数据规则分类，支持自定义



图：数据标签-列表

点击【搜索】，输入分类名称，即可进行模糊查询。

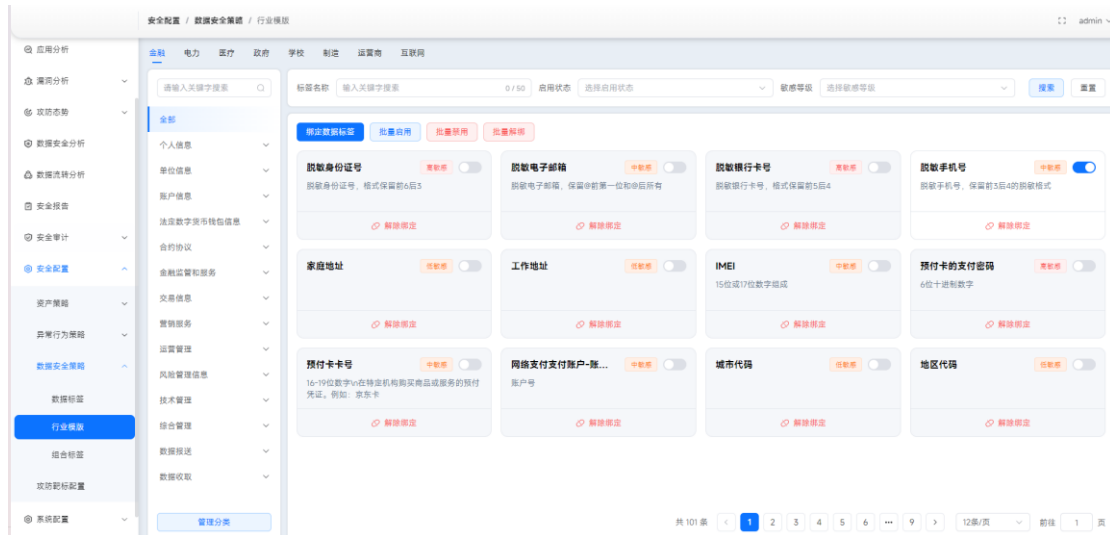
点击【新增】，可以新增规则，点击确定，即可新增成功



图：数据标签-新增

12.3.2. 行业模板

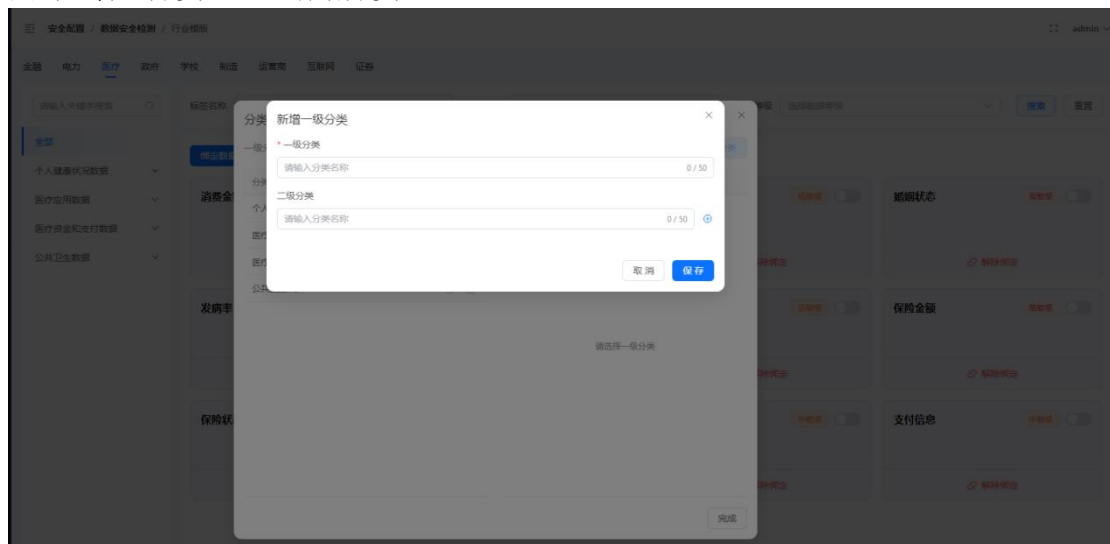
点击【行业模版】查看标签分类



图：行业模版-列表

点击页面上方的分类，可查看不同行业的数据标签

点击【管理分类】，可新增分类



图：行业模版-管理分类-1

自定义的一级二级分类可进行修改删除等操作

分类管理



























✕

一级分类

新增一级分类

二级分类

新增二级分类

分类	操作	分类	操作
一级分类	 	今日测试	 
金融监管和服务	 		
交易信息	 		
营销服务	 		
运营管理	 		
风险管理信息	 		
技术管理	 		
综合管理	 		
数据报送	 		
数据收取	 		
aaaa	 		
一级分类test	 		

完成

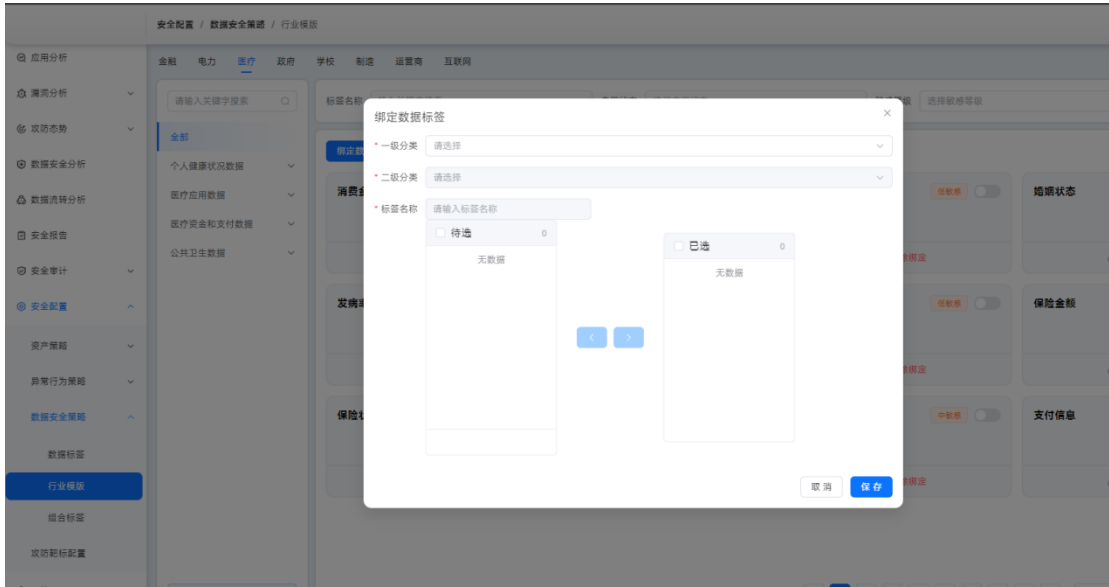
图：行业模版-管理分类-2

可根据关键字对分类名称进行模糊查询



图：行业模版-搜索

点击【绑定数据标签】，可对数据标签进行所属分类绑定

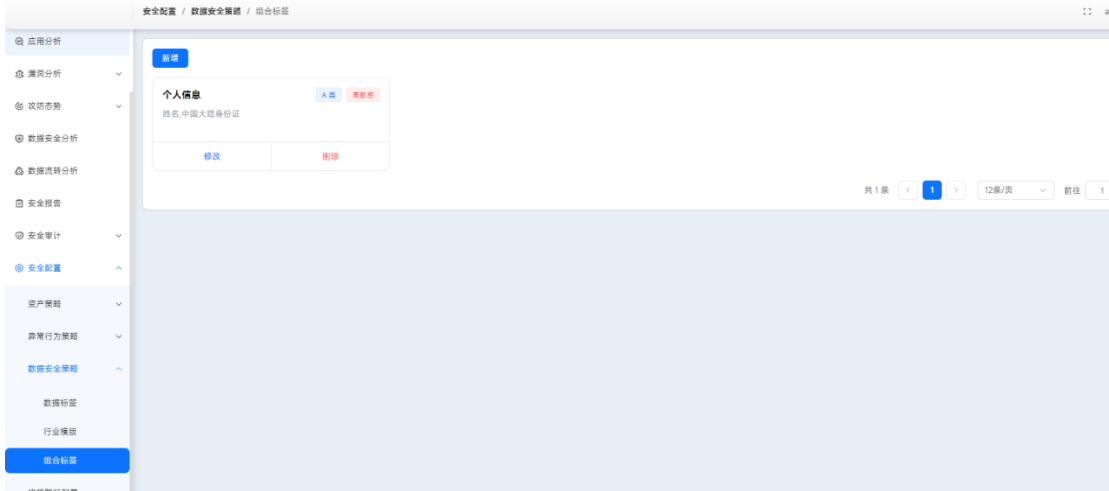


图：行业模版-绑定数据标签

点击【批量启用】，可对所选分类下的数据标签全部启用
点击【批量禁用】，可对所选分类下的数据标签全部禁用
点击【批量解绑】，可对所选分类下的数据标签全部解绑

12.3.3. 组合标签

点击【等级管理】，显示敏感数据等级分类，根据自定义的规则对敏感标签进行等级分类



图：组合标签

点击【新增】，输入名称、分级、敏感等级，选择需要分类的敏感标签，点击确定即可新增成功



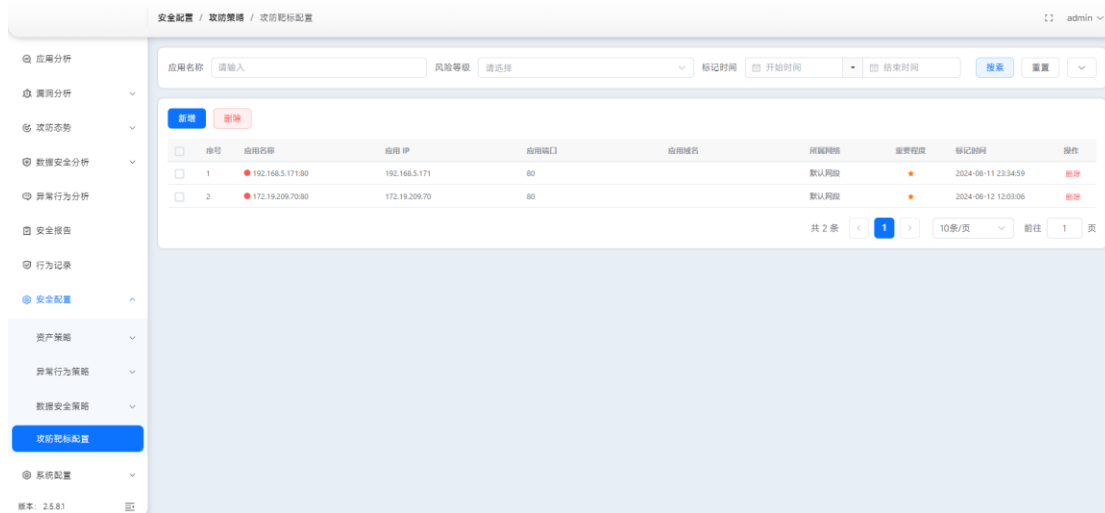
图：组合标签-新增

点击【修改】，可对已有的数据信息修改

点击【删除】，可删除已有数据，点击取消放弃本次删除

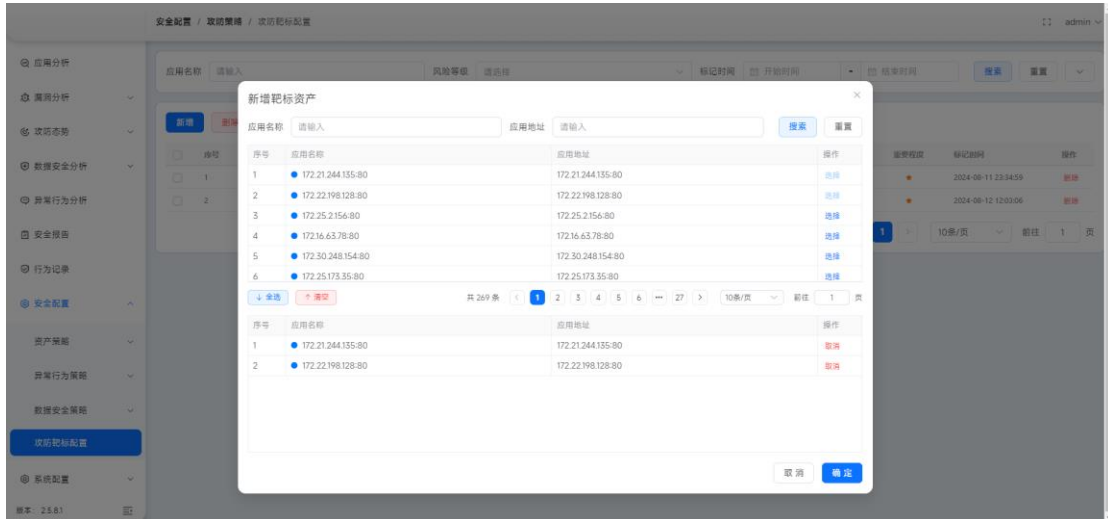
12.4. 攻防靶标配置

攻防靶标配置是用于标记攻防演练中的靶标应用和关注应用，标记的应用会在【攻防态势/应用情报】模块输出全面的应用分析，为用户加强攻击防范提供参考信息。



图：攻防靶标配置

点击【新增】可添加靶标应用。弹出对话框上方列表显示已识别的应用，支持按应用名称和应用地址进行筛选查询。在应用清单列表中点击【选择】可将当前应用添加入下方预选池，点击【全选】可将当前页的所有应用添加入预选池，在预选池中点击【取消】可清除当前应用选择，点击【清空】可清空预选池中已添加的所有应用。选择完目标应用点击【确认】将添加成功，点击【取消】放弃本次操作。



图：新增靶标资产

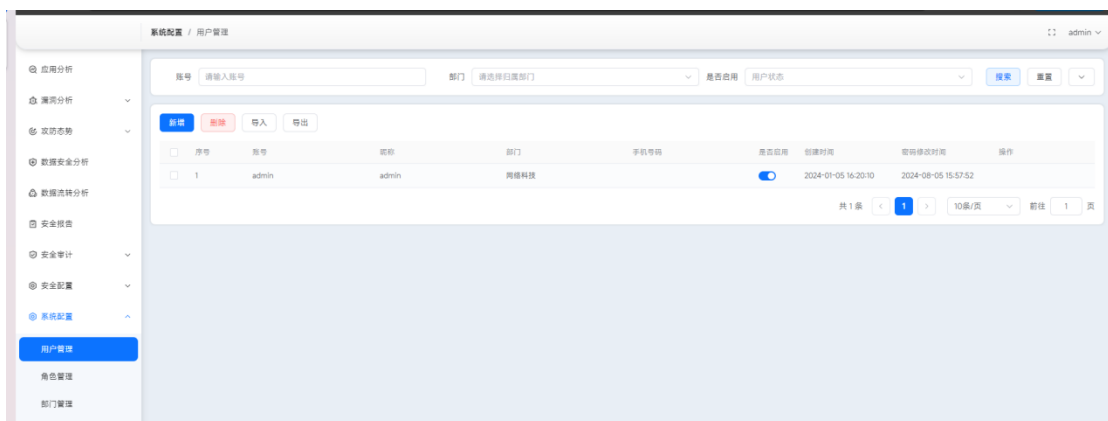
点击【搜索】，输入应用名称、应用 IP、应用域名点击搜索，可以进行模糊查询。输入风险等级、标记时间、所属网络、重要程度可进行精确搜索。

点击【删除】，提示是否删除，删除后列表不再显示已删除应用，应用情报中也不再分析已删除的靶标应用。列表上方删除按钮可批量删除列表中已勾选的应用，列表中的删除仅删除当前单条应用信息。

13. 系统配置

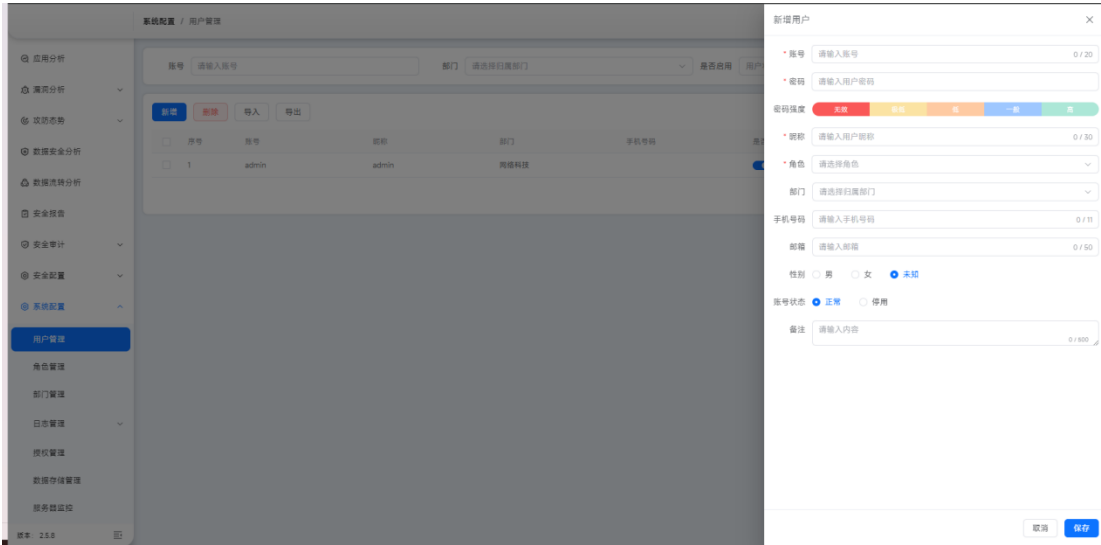
13.1. 用户管理

点击【用户管理】，显示用户列表，可以按照部分、用户名称、手机号、状态，日期查询列表（初始只显示 admin 账号）



图：用户管理-列表

点击【新增】，可以添加用户信息



图：用户管理-新增用户

- 点击列表【修改】，可以修改用户信息
- 点击列表【删除】，提示是否删除，删除后列表不显示该用户信息
- 点击【导入】，可以导入用户信息
- 点击【导出】，导出所有用户信息，可勾选导出部分用户
- 点击【重置密码】，提示输入新密码，修改后重新登录
- 点击【搜索】，可进行条件查询

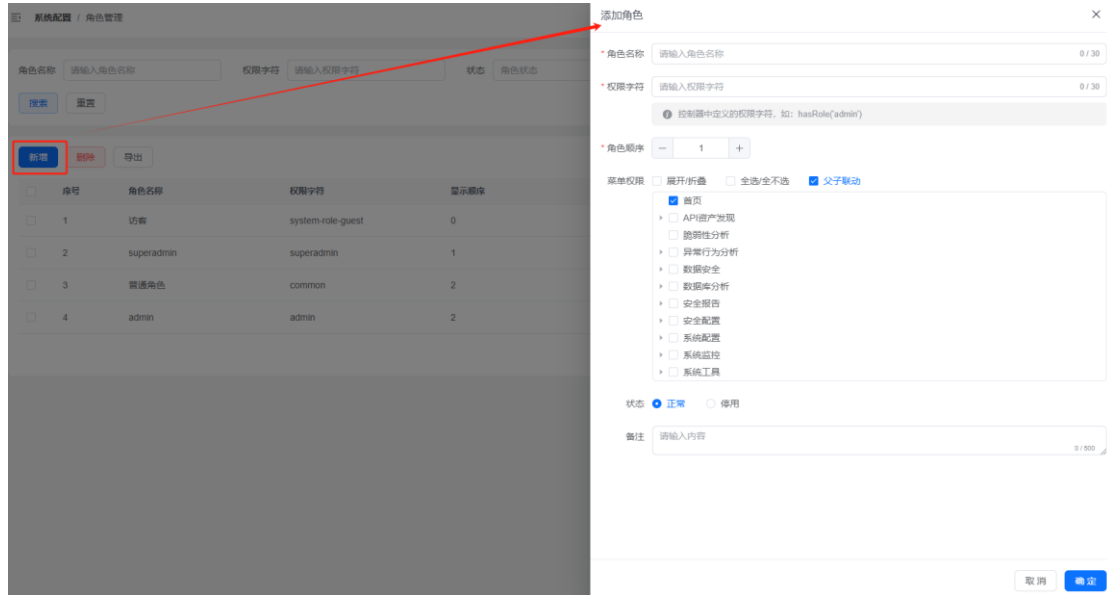
13.2. 角色管理

点击【角色管理】，显示角色列表，可以按照角色名称、权限字符、状态、时间查询列表（初始只显示 admin 角色）



图：角色管理-列表

点击【新增】，可以添加角色信息



图：角色管理-新增

点击列表【修改】，可以修改角色信息

点击列表【删除】，提示是否删除，删除后列表不显示该角色信息

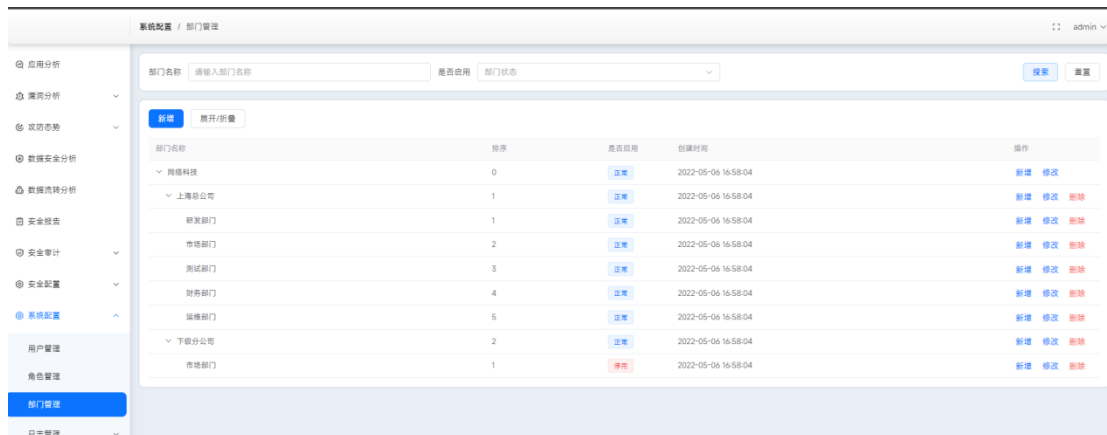
点击【导出】导出所有角色信息，或者勾选导出部分角色信息

点击【分配权限】，可对角色权限范围进行修改

点击【分配用户】，可对角色进行用户分配

13.3. 部门管理

点击【部门管理】，显示部门列表，可按照部门名称、状态查询列表



图：部门管理-列表

点击列表【新增】，在当前部门下新增部门或者点击列表上方【新增】自定义上级部门



图：部门管理-新增

点击列表上方【展开/折叠】，可以展开/折叠部门列表

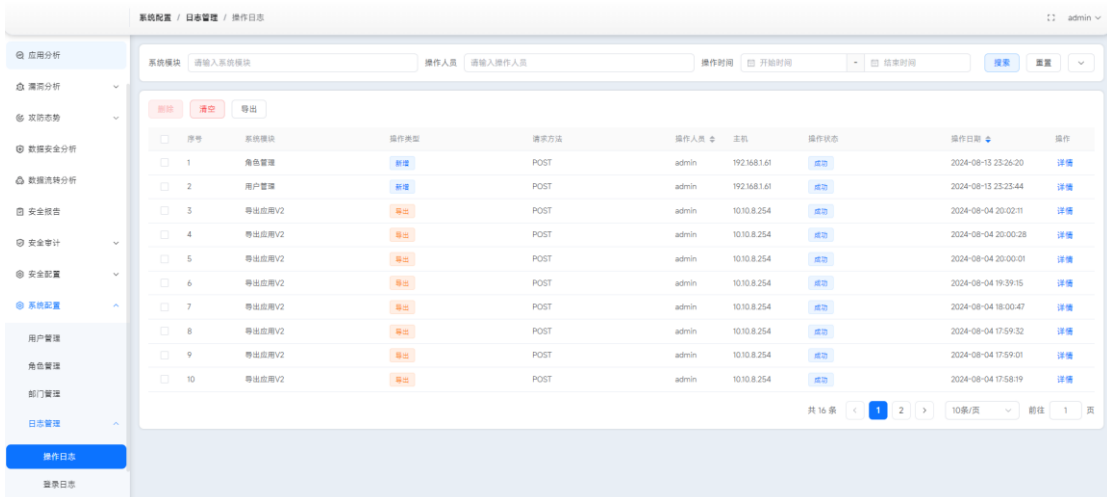
点击列表【修改】，可以修改当前部门信息

点击列表【删除】，提示是否删除，删除后列表不显示该部门信息

13.4. 日志管理

13.4.1. 操作日志

点击【操作日志】，显示操作日志列表，可按照系统模块、操作人员、类型、状态、时间查询列表（admin 账号不能查看 superadmin 的操作日志）



图：操作日志管理-列表

点击【清空】，提示是否清空，清空所有操作日志

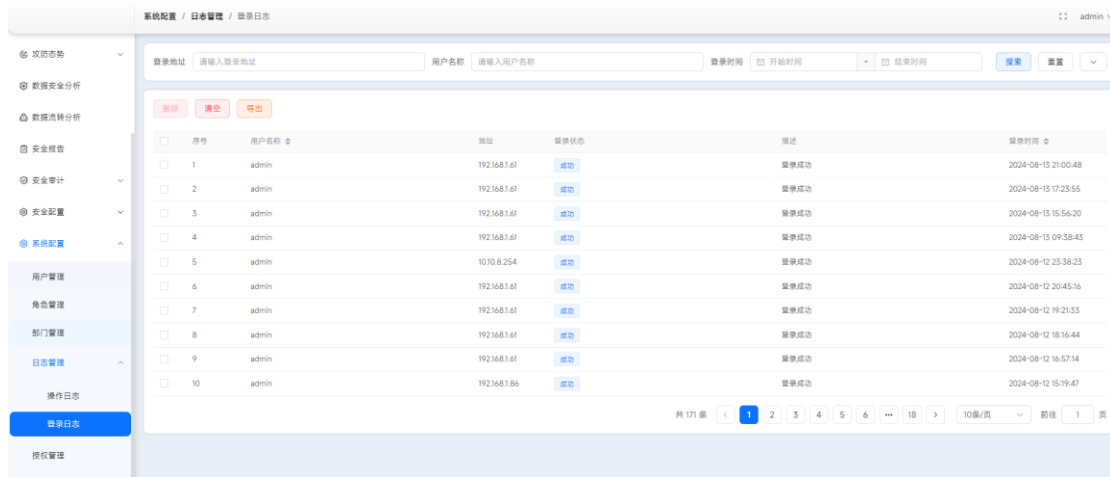
勾选日志点击【删除】，提示是否删除，删除后列表不显示该操作日志

点击【导出】，导出全部操作日志信息，或者勾选操作日志导出部分信息

点击【详细】，可查看当前操作日志详细信息

13.4.2. 登录日志

点击【登录日志】，显示登录日志列表，可按照登录地址、用户名称、状态、登录时间查询列表（admin 账号不能查看 superadmin 的登录日志）



序号	用户名	地址	登录状态	描述	登录时间
1	admin	192.168.1.61	成功	登录成功	2024-08-13 21:00:48
2	admin	192.168.1.61	成功	登录成功	2024-08-13 17:23:55
3	admin	192.168.1.61	成功	登录成功	2024-08-13 15:56:20
4	admin	192.168.1.61	成功	登录成功	2024-08-13 09:38:43
5	admin	10.10.0.254	成功	登录成功	2024-08-12 23:38:23
6	admin	192.168.1.61	成功	登录成功	2024-08-12 20:45:16
7	admin	192.168.1.61	成功	登录成功	2024-08-12 19:21:53
8	admin	192.168.1.61	成功	登录成功	2024-08-12 18:16:44
9	admin	192.168.1.61	成功	登录成功	2024-08-12 16:57:14
10	admin	192.168.1.86	成功	登录成功	2024-08-12 15:19:47

图：登录日志管理-列表

勾选登录日志点击【删除】，提示是否删除，删除后列表不显示该登录日志

点击【清空】，提示是否清空，清空所有登录日志信息

点击【导出】，导出全部登录日志信息，或者勾选导出部分信息

13.5. 授权管理

上传授权管理许可说明，支持 API 资产发现模块、脆弱分析模块、异常行为分析模块、数据安全分析模块的流量解析。



图：授权管理

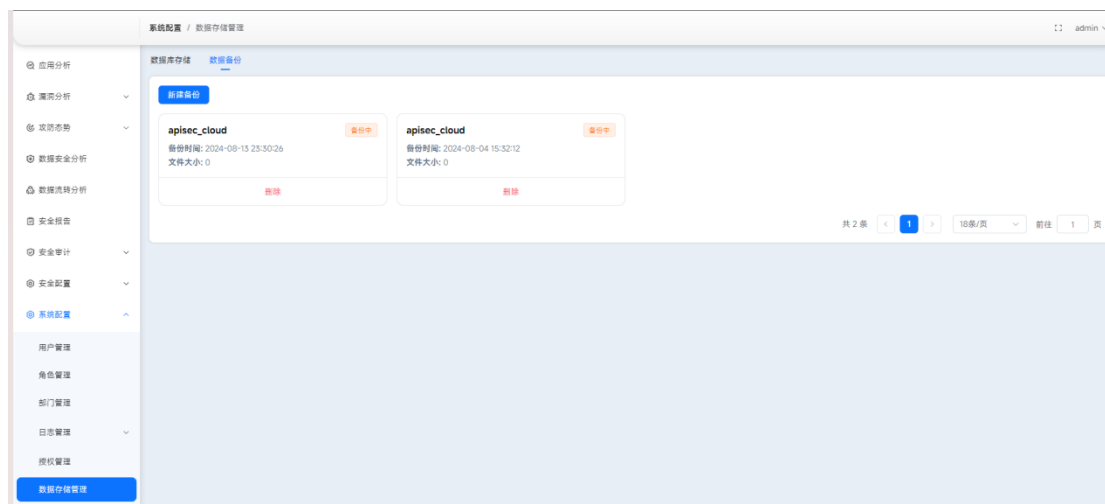
点击【上传】，选择要上传的文件，上传成功后，会显示授权许可以及许可有效期，支持API资产发现模块、脆弱分析模块、异常行为分析模块、数据安全分析模块的流量解析



图：授权管理-上传

13.6. 数据存储管理

点击【新建备份】，可以对数据进行备份，显示备份中



图：数据存储管理-数据备份

数据备份成功后，会显示备份成功，可以进行下载、删除操作



图：数据存储管理-数据库备份-列表

13.7. 服务器监控

监控 CPU、内存、磁盘、以及运行时长

