

ShinylogM 用户手册

1. 日志源日志搜索.....	1
1.1 功能描述.....	1
1.2 业务操作流程	2
2 安全可视化报表	3
2.1 功能描述.....	3
2.2 业务操作流程	3
3 安全规则.....	6
3.1 功能描述	6
3.2 业务操作流程.....	6
4 事件调查.....	9
4.1 功能描述	9

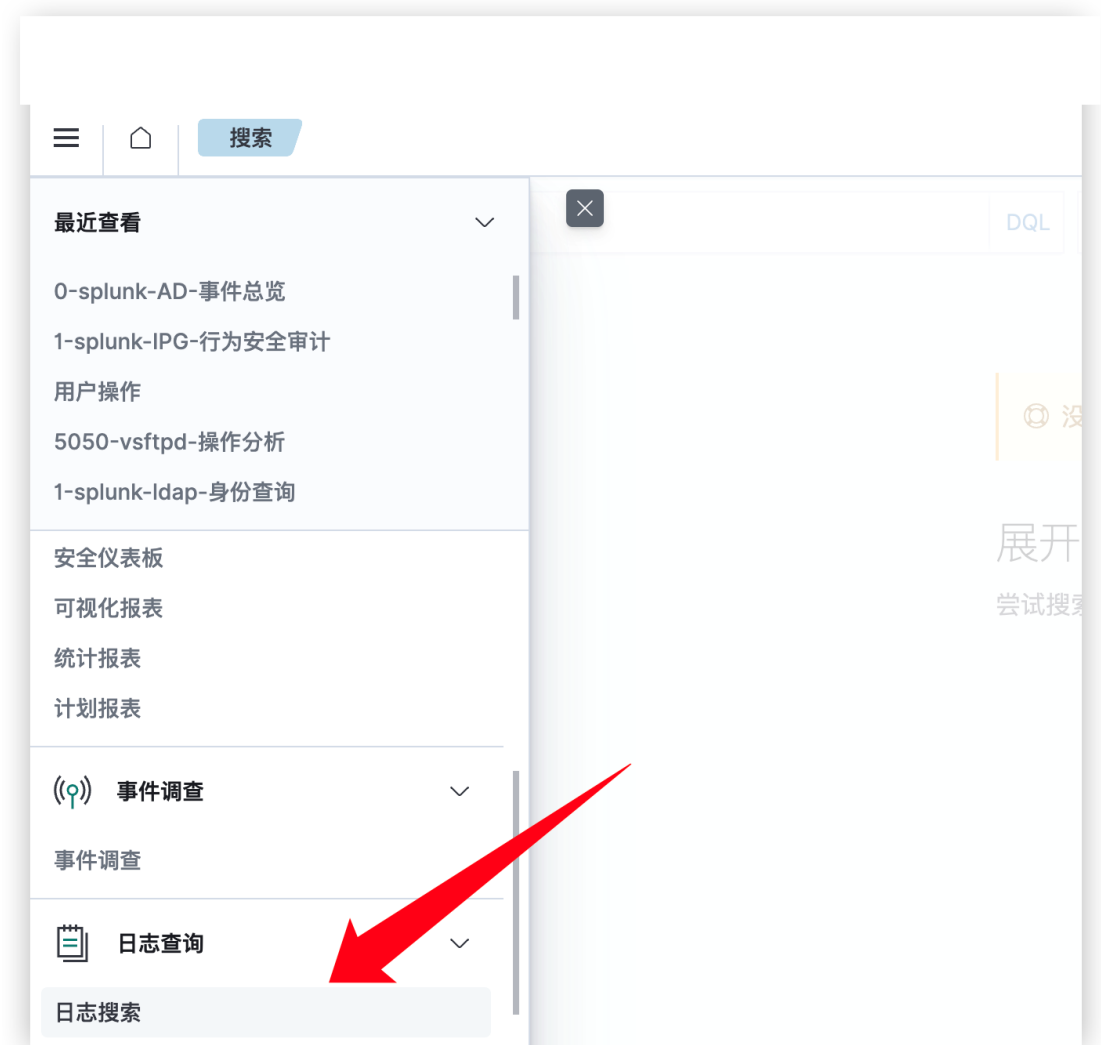
1. 日志源日志搜索

1.1 功能描述

ShinyLogM 日志平台提供内置日志搜索服务，使用人员可登录日志平台，选择日志搜索界面，根据需求可对任意索引中的日志进行搜索查询，搜索支持模糊匹配和关联查询（AND OR NOT 等）。

1.2 业务操作流程

1 通过侧边栏进入数据查询界面



2 数据查询界面功能介绍



2 安全可视化报表

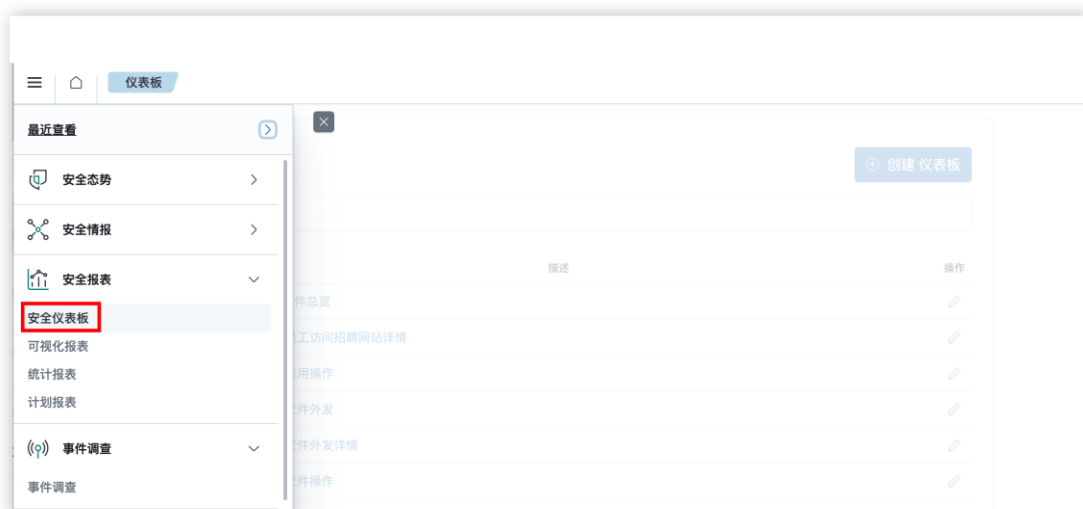
2.1 功能描述

ShinyLogM日志平台内置日志的可视化展示服务，可以将任意完成日志建模的日志进行可视化展示，支持用户自定义可视化仪表板。

2.3

2.2 业务操作流程

1 单击侧边栏安全仪表板进入安全仪表板界面



2 在安全仪表板界面单击创建仪表板



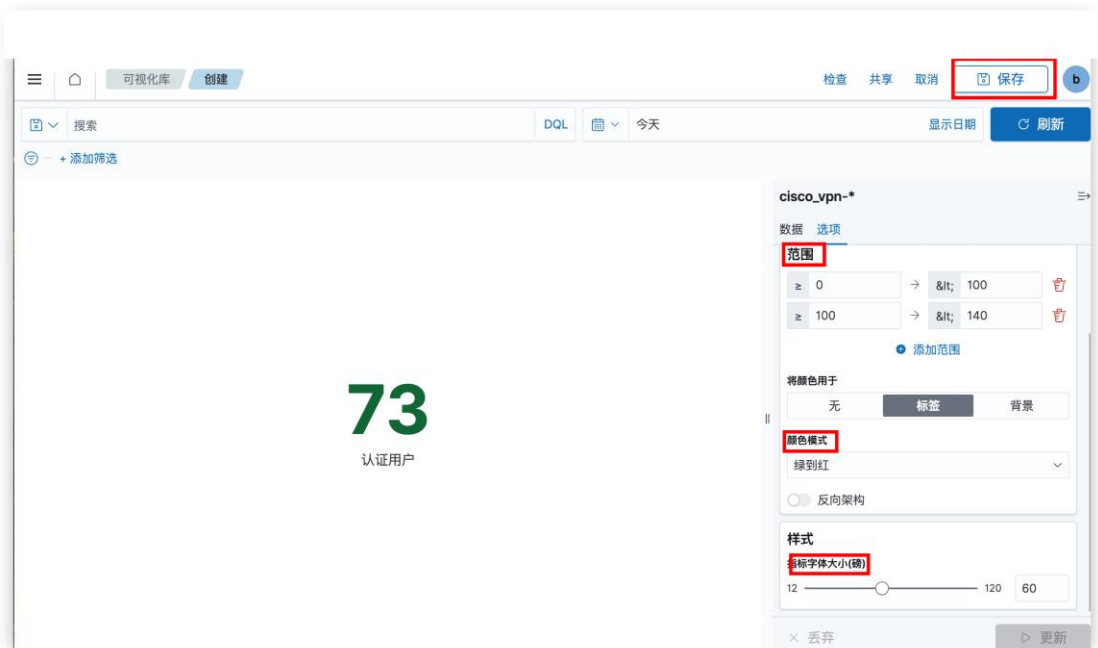
3 选择报表类型，这里演示报表的类型为“指标”



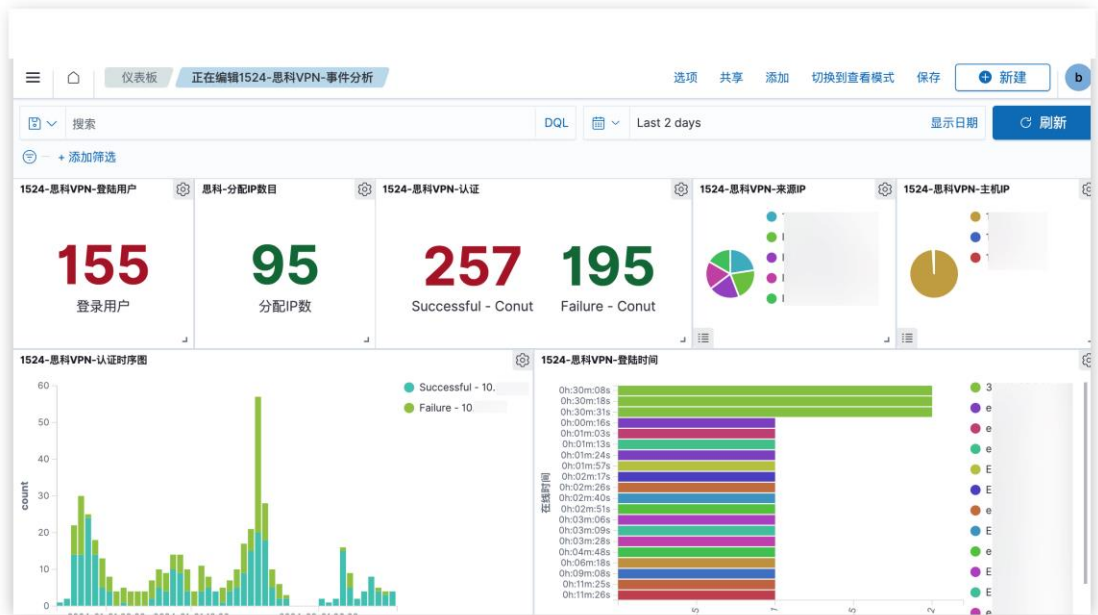
4 选择数据源



5 编辑可视化内容，点击保存。



6 查看仪表板内容



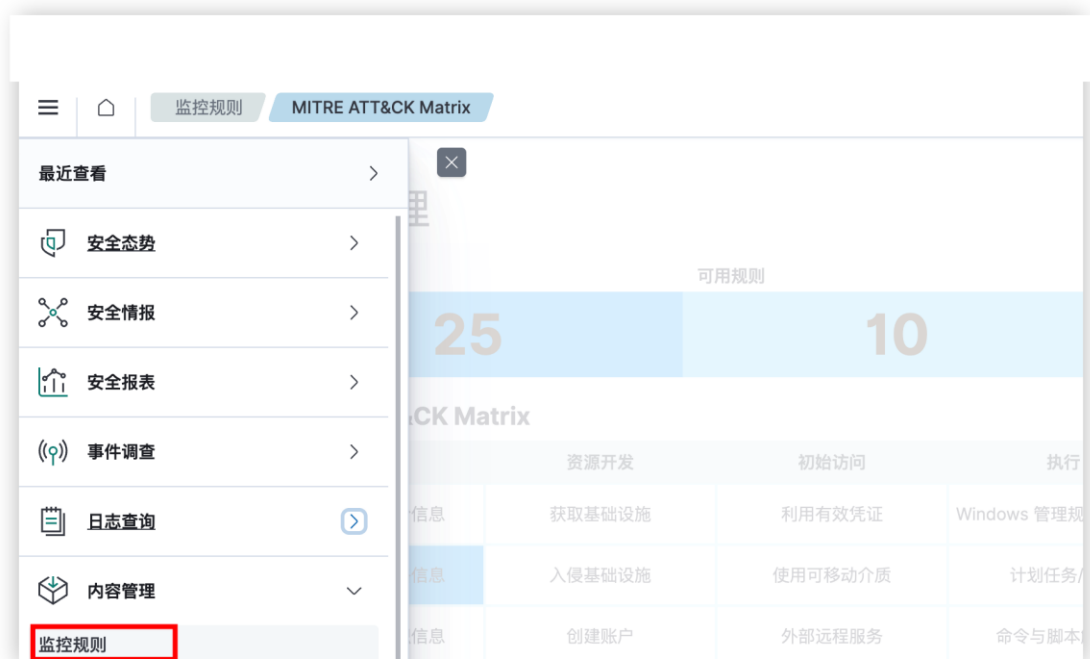
3 安全规则

3.1 功能描述

ShinyLogM 日志平台支持客户自定义告警功能，能够对于任意指定事件，潜在高危安全事件，异常用户行为，事件统计结果，关联分析结果等实现告警和通知。

3.2 业务操作流程

1 单击侧边栏进入监控规则进入监控规则界面



2 点击规则库新建规则



3 填入告警名称，描述及规则语句



4 点击计划任务，配置计划任务及触发条件

三 监控规则 规则库 规则修改

白名单
事件通知
事件聚合
风险因子

规则配置

告警规则 计划任务 告警注释 触发内容

计划任务

开始时间: 2 时间单位: 小时前

结束时间: 1 时间单位: 小时前

Cron计划: 0 * / 1 * * * 输入 cron 样式计划

触发条件

触发: 一次 针对每个结果

5 为规则添加告警注释

三 监控规则 规则库 规则修改

MITRE ATT&CK Matrix
规则库
白名单
事件通知
事件聚合
风险因子

规则配置

告警规则 计划任务 告警注释 触发内容

类型: 访问认证

MIRTE ATT&CK 框架: 选择MIRTE ATT&CK 框架

上一步 下一步

6 配置风险字段及告警触发后动作，保存规则

三 监控规则 规则库 规则修改

风险字段

风险字段: user 风险值: 10

添加风险字段

触发内容

是否开启触发内容: 是 否

添加触发内容

告警展示

* 严重性: 高危

* 默认所有者: admin

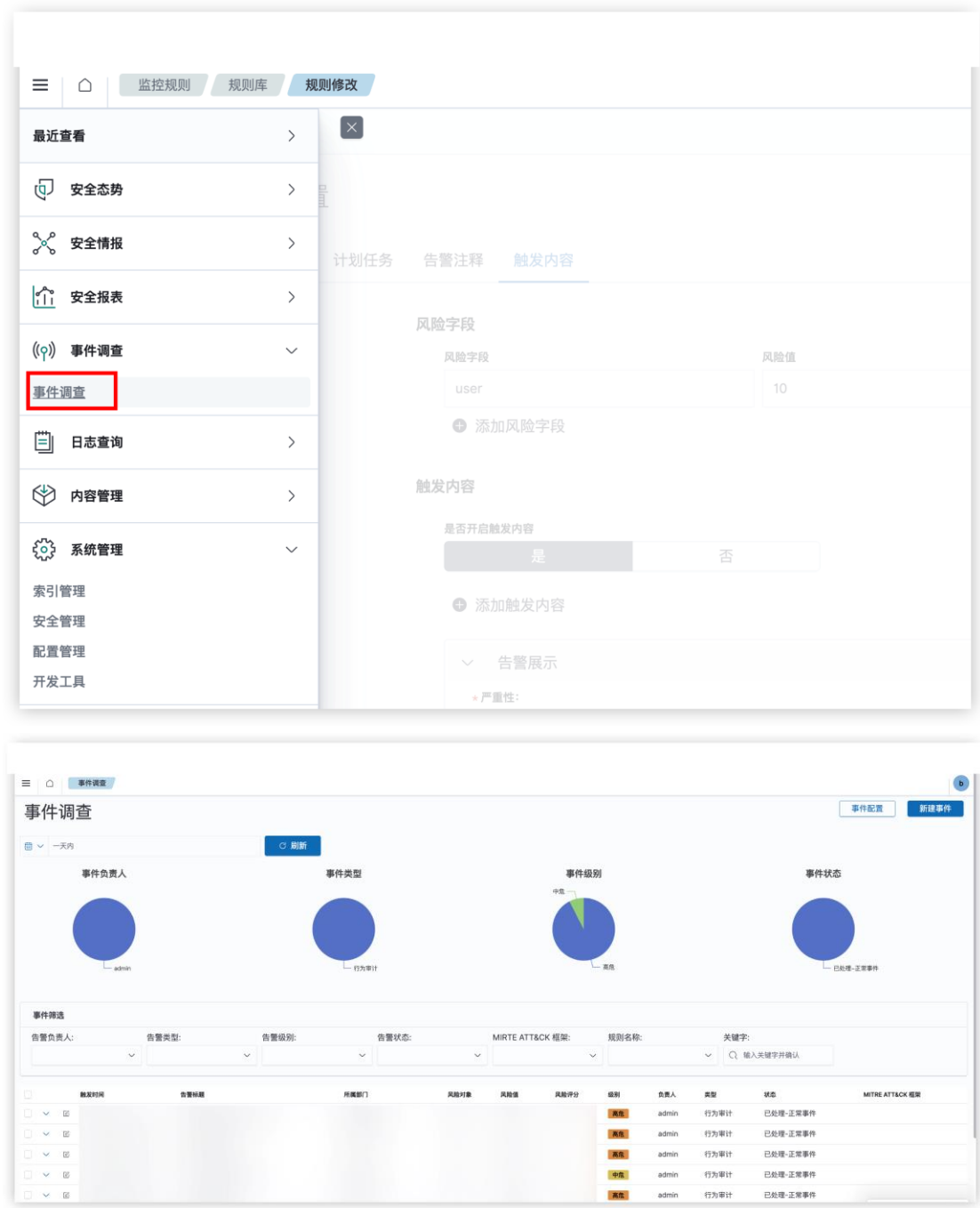
* 默认状态: 新创建

4 事件调查

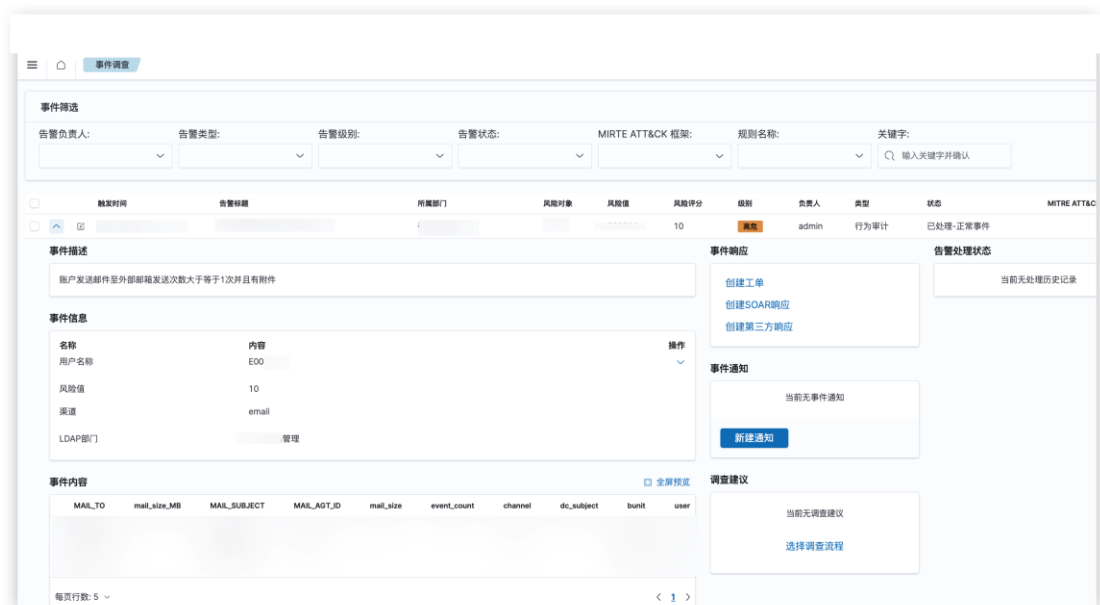
4.1 功能描述

流程编排

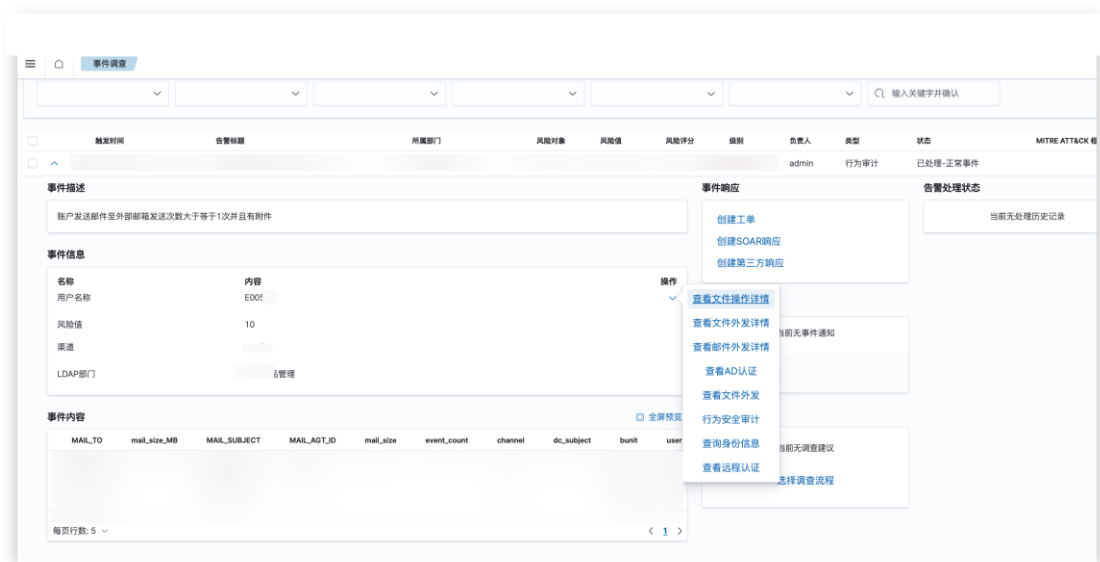
1 点击侧边栏，事件调查，进入事件调查界面

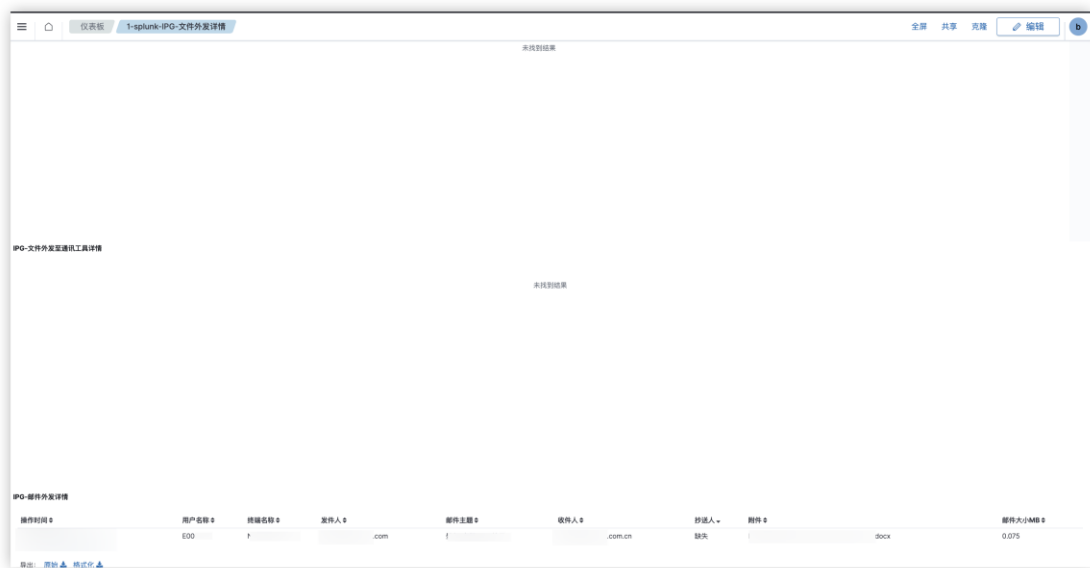


2 点击事件左侧下拉键，查看安全事件详情

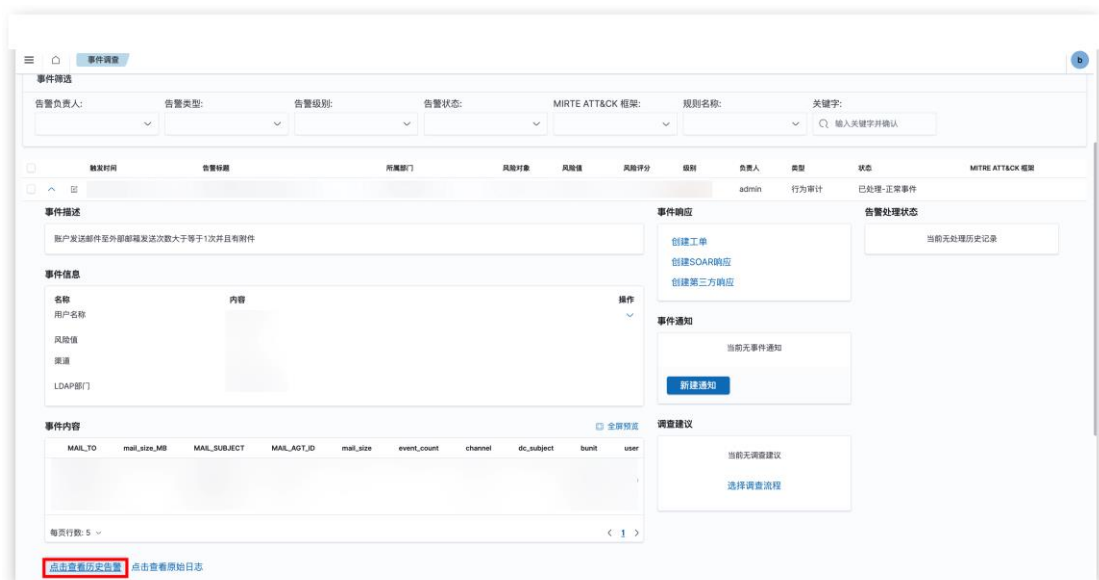


3 点击事件信息中操作列下拉键，查看字段关联面板





4 点击查看历史告警，查看该告警规则历史触发事件



5 事件通知中点击将安全事件发送通知

事件调查

admin

行为审计

高危

事件筛选

告警负责人: 告警类型: 告警级别: 告警状态: MIRTE ATT&CK 框架: 规则名称: 关键字: 输入关键字并确认

触发时间

告警标题

所属部门

风险对象

风险值

风险评分

级别

负责人

类型

状态

10

高危

admin

行为审计

已处理-正常事件

事件描述

客户发送邮件至外部邮箱发送次数大于等于1次并且有附件

事件信息

名称 内容 操作

用户名称

风险值

渠道

LDAP部门

事件响应

创建工单

创建SOAR响应

创建第三方响应

告警处理状态

事件通知

当前无事件通知

选择通知方式

新建通知

电子邮件通知

企业微信通知

钉钉通知

事件内容

MAIL_TO mail_size_MB MAIL_SUBJECT MAIL_AGT_ID mail_size event_count channel dc_subject

调查建议

当前无调查建议