ShinylogM 用户手册

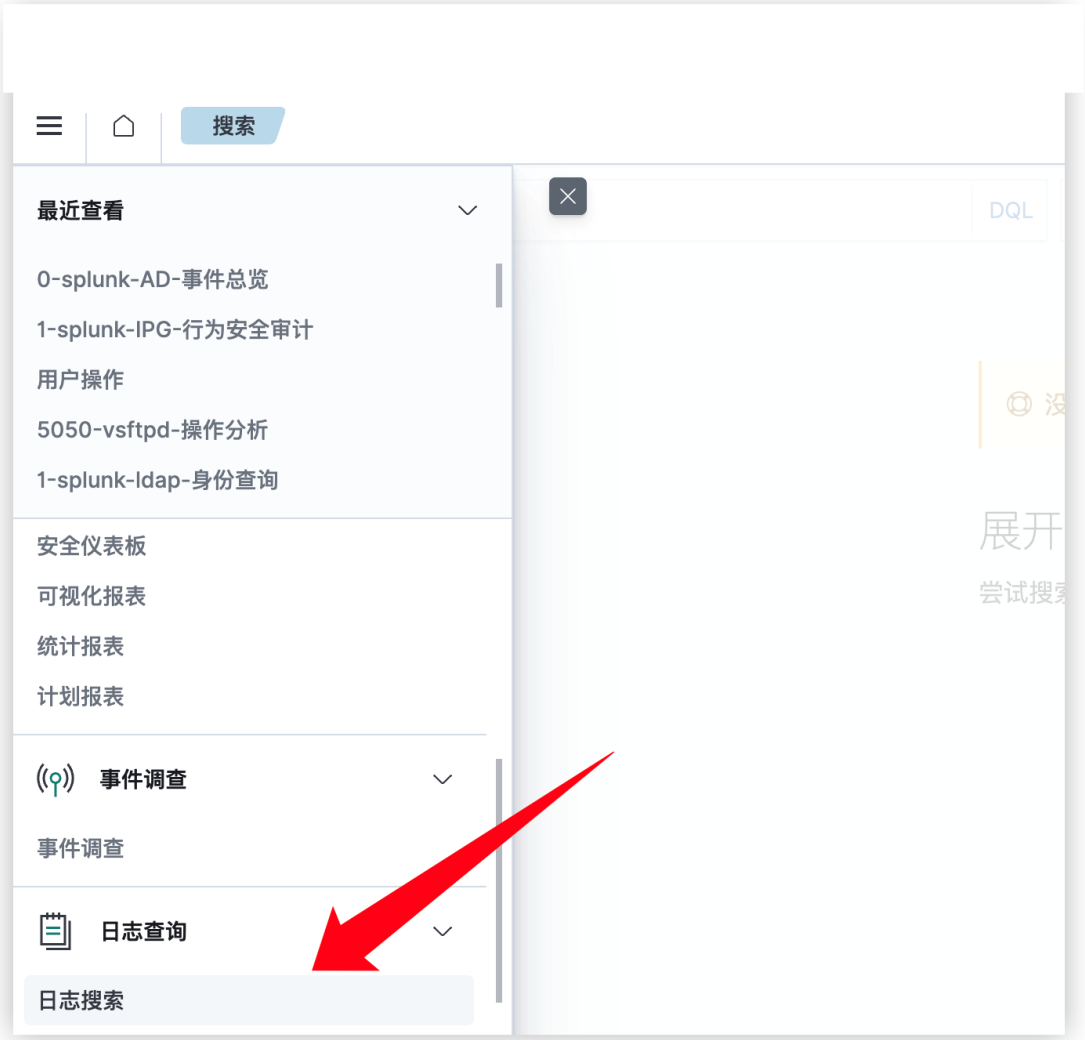
1. 日志源日志搜索

1.1 功能描述

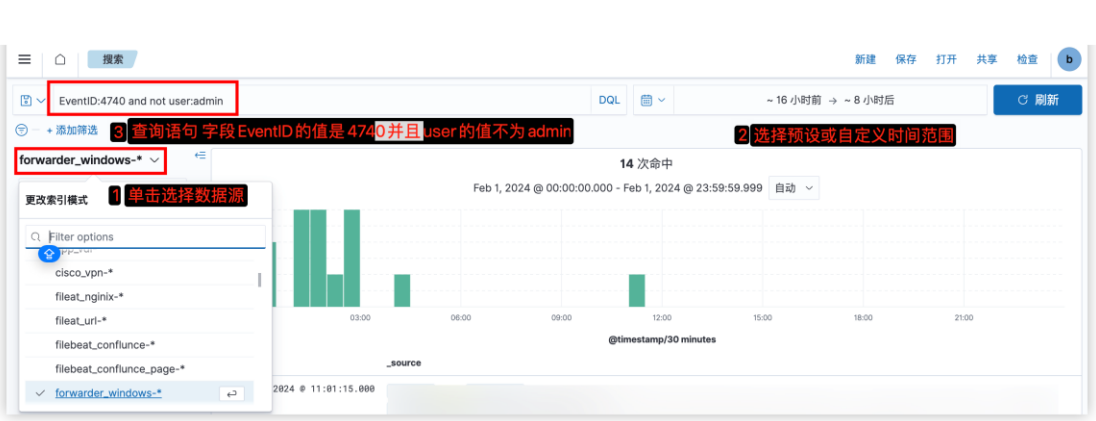
ShinyLogM 日志平台提供内置日志搜索服务，使用人员可登录日志平台，选择日志搜索界面，根据需求可对任意索引中的日志进行搜索查询，搜索支持模糊匹配和关联查询（AND OR NOT 等）。

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

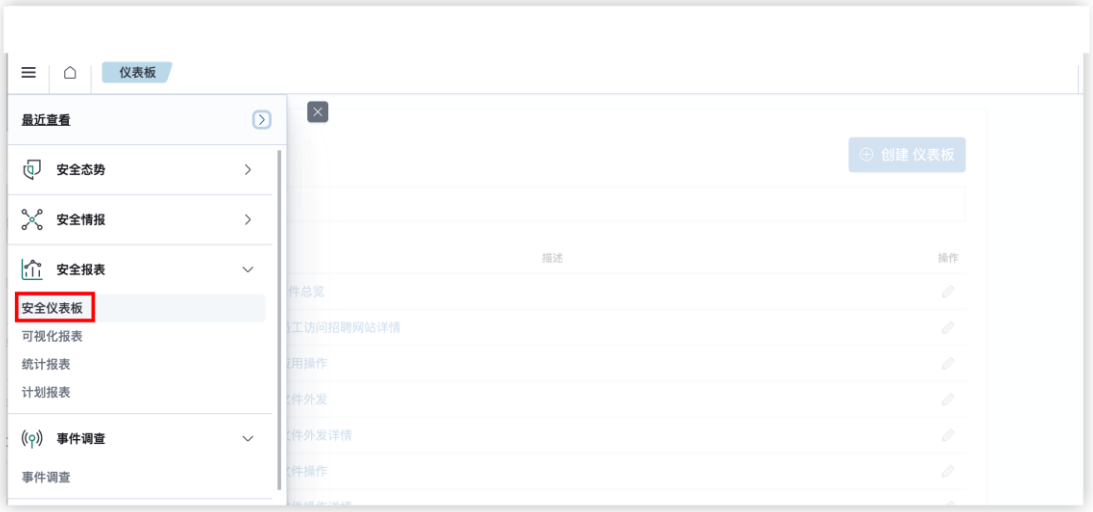
2.1 功能描述

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

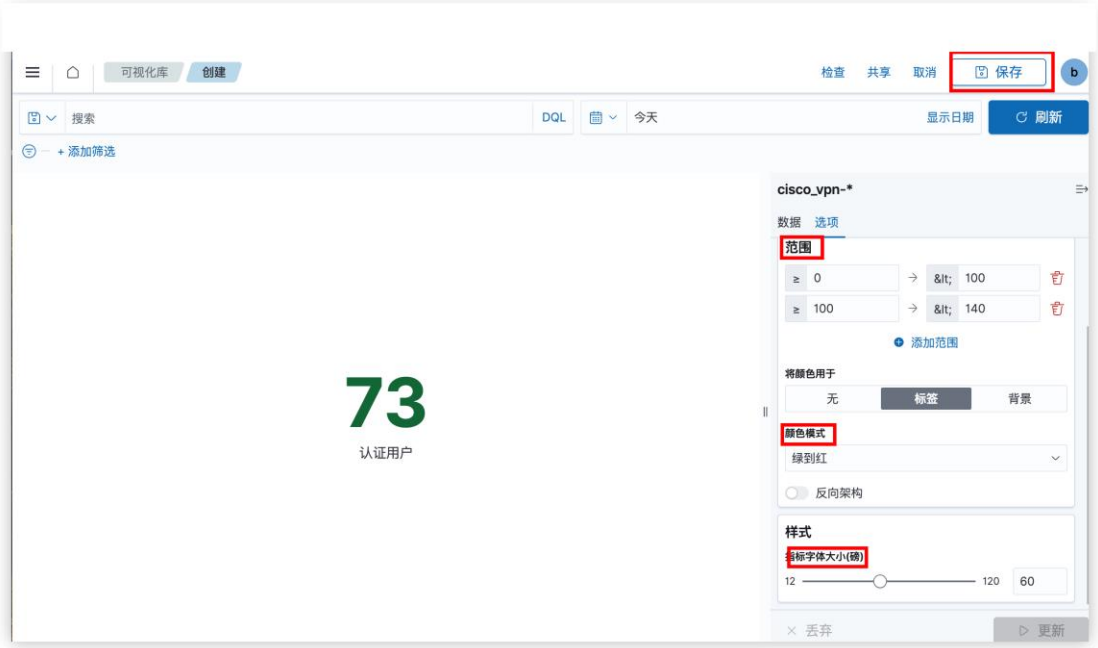
3　选择报表类型，这里演示报表的类型为”指标”


新建可视化
Filter
Markdown
TSVB
Timeline
Vega
仪表盘
区域
区域地图
单杠
坐标图
垂直条
指标
控件
实
数据表
标签云图
热图
目标图
选择一个可视化类型
通过为该可视化选择类型开始创建您的可视化.

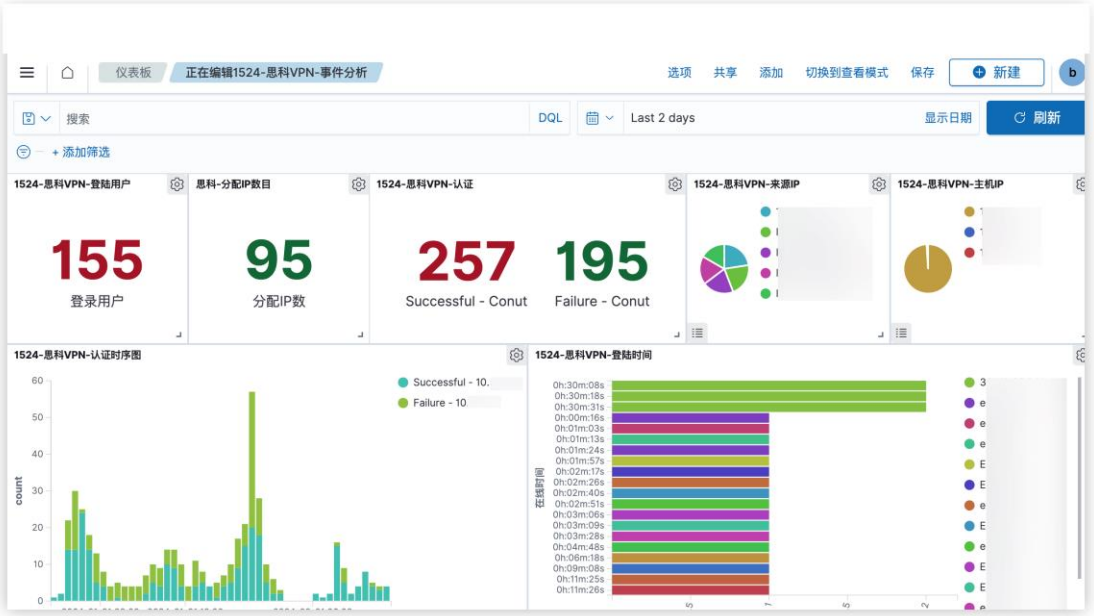
4 选择数据源


新建指标 / 选择源
搜索.....
排序
类型
2
cisco_vpn-*
1 2 3 4 5 6 7 ... 14

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

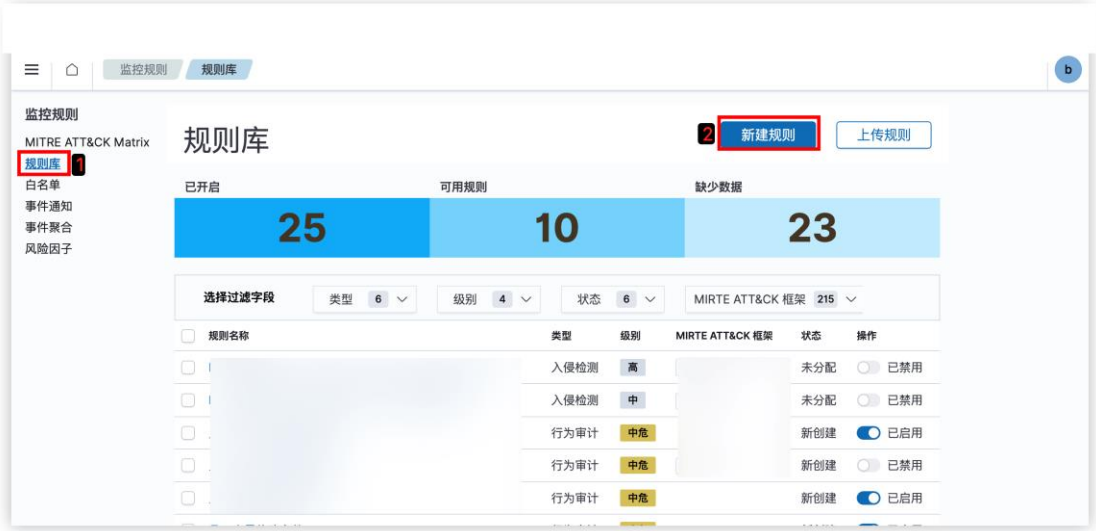
3.1 功能描述

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

5 为规则添加告警注释

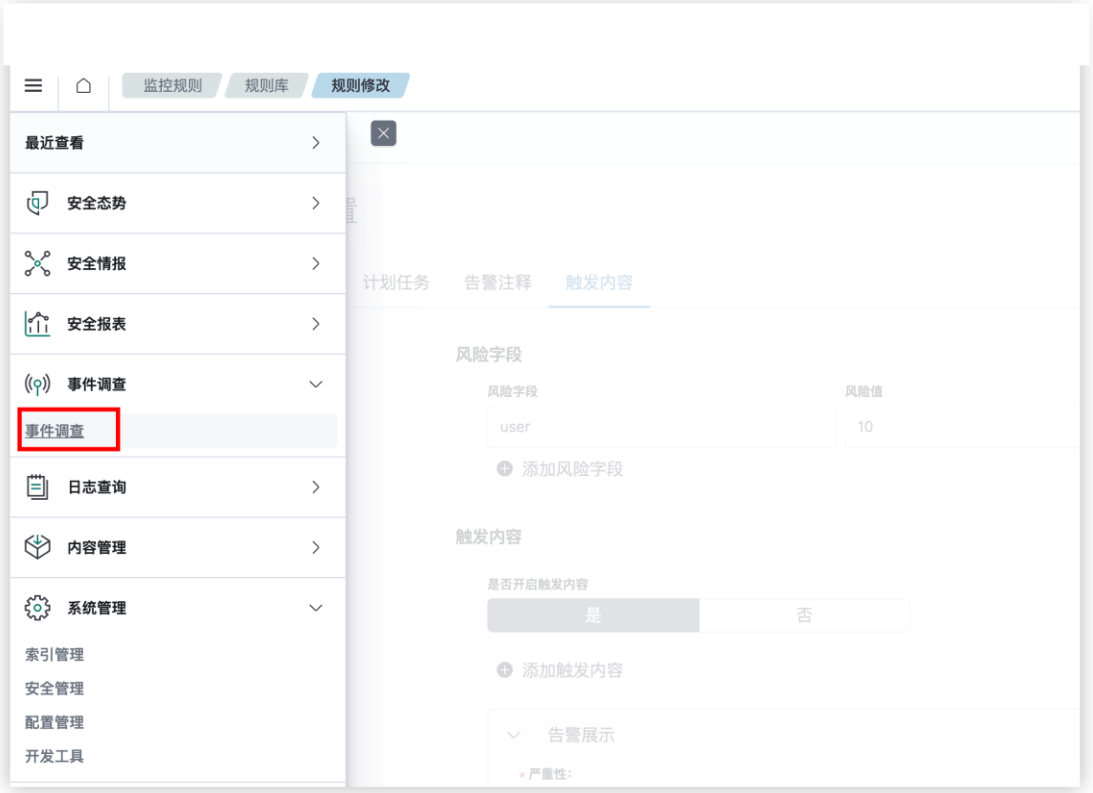
6 配置风险字段及告警触发后动作，保存规则

4 事件调查

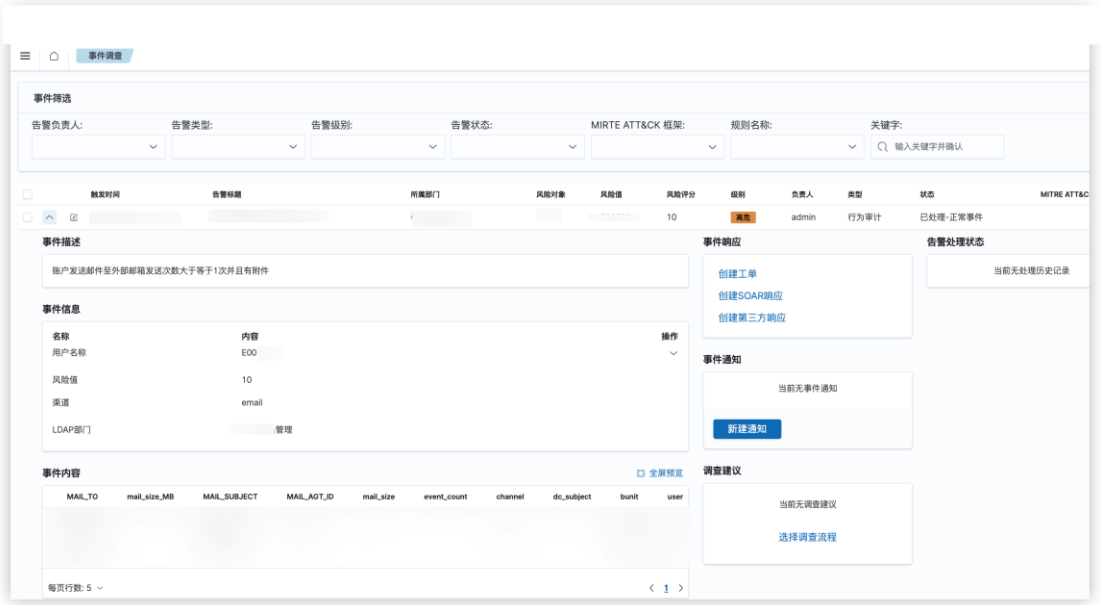
4.1 功能描述

流程编排

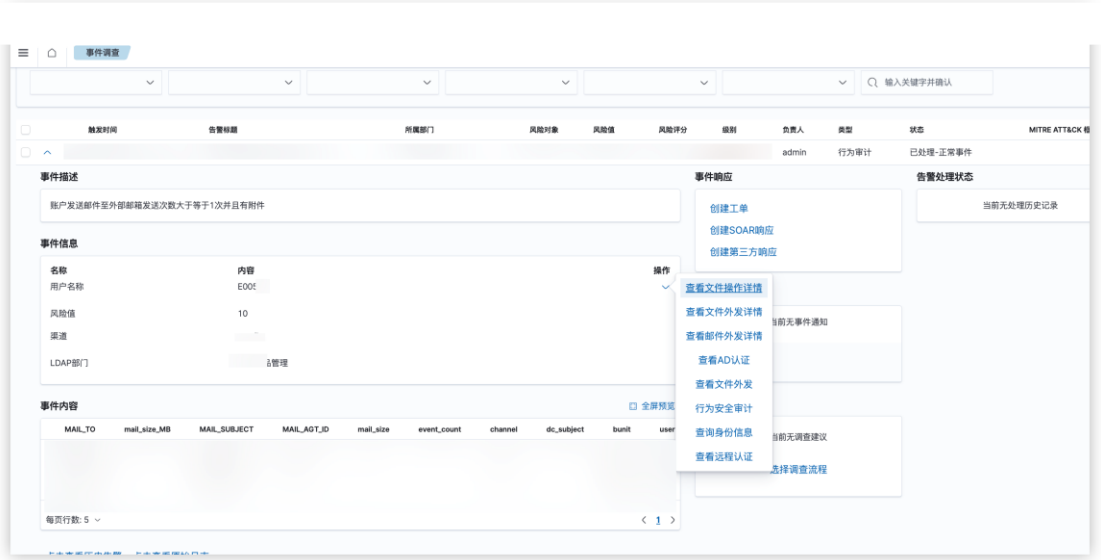
1 点击侧边栏，事件调查，进入事件调查界面

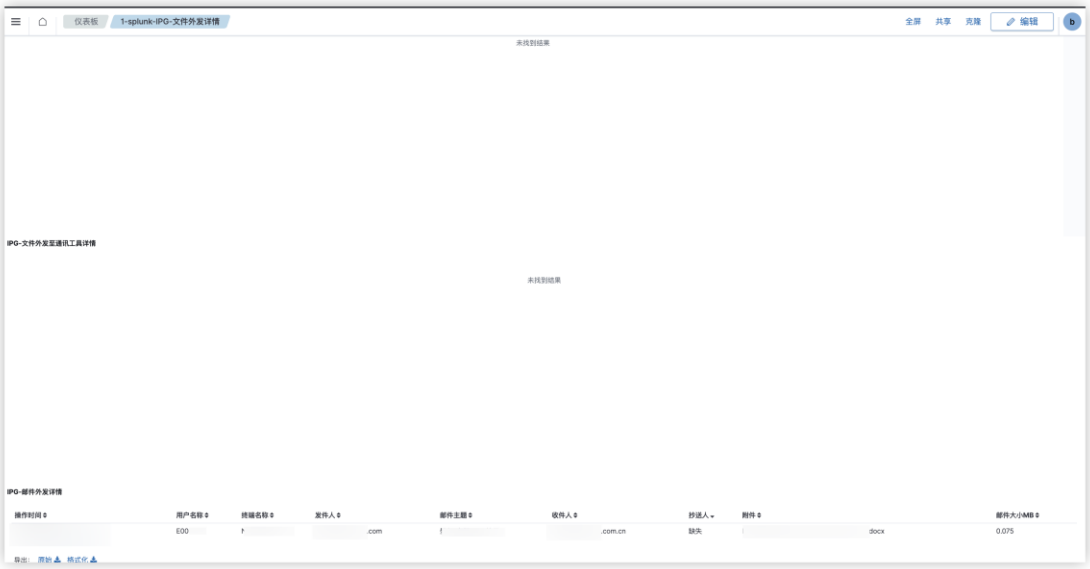


2 点击事件左侧下拉键，查看安全事件详情

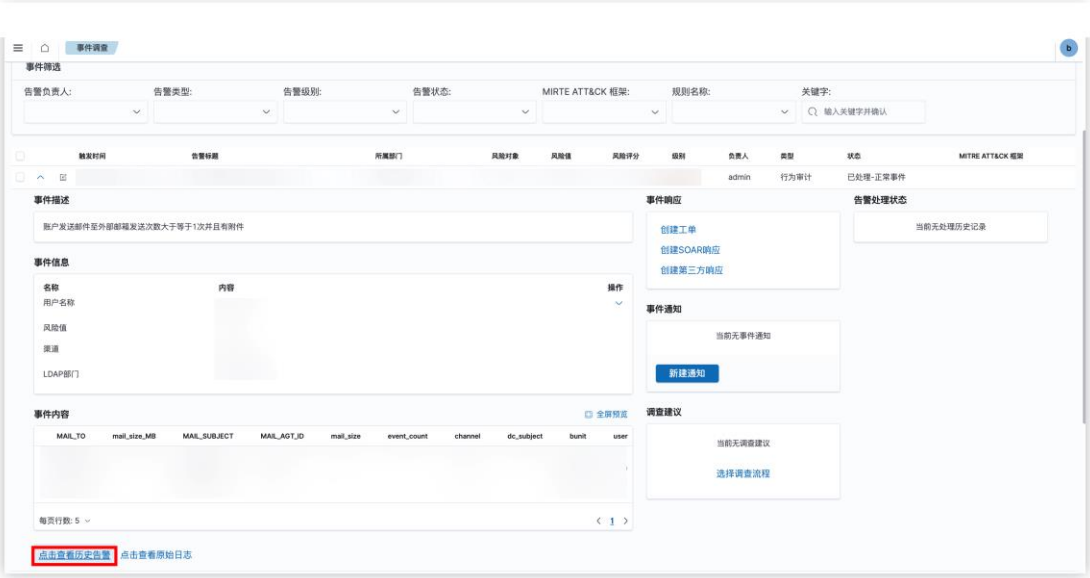


3 点击事件信息中操作列下拉键，查看字段关联面板





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