西安交通大学
XI'AN JIAOTONG UNIVERSITY

安全事件处置管理平台

用户操作手册

网络信息中心

目录

一、系统简介

西安交通大学安全事件处置管理平台（以下简称安管平台）是进行校园网络安全事件通报、处置、复查的流程管理平台。平台规范了网络安全事件的提交、审核、通报和整改的要求，对日常网络安全巡查和发现的网络安全事件进行处置和追踪，形成完整的工作记录。

安管平台可以通过域名 http://sec.xjtu.edu.cn/event 直接访问，也可以在网络安全专题网（http://wlaq.xjtu.edu.cn/）首页右下角“安全管理平台”详情页看到平台的详细介绍和域名地址，到达平台登录页面。如果用户收到平台发送的短信，短信内容中包含平台域名地址。流程描述：

提交： 安全巡查人员或平台用户可通过平台提交自己发现的安全事件信息；

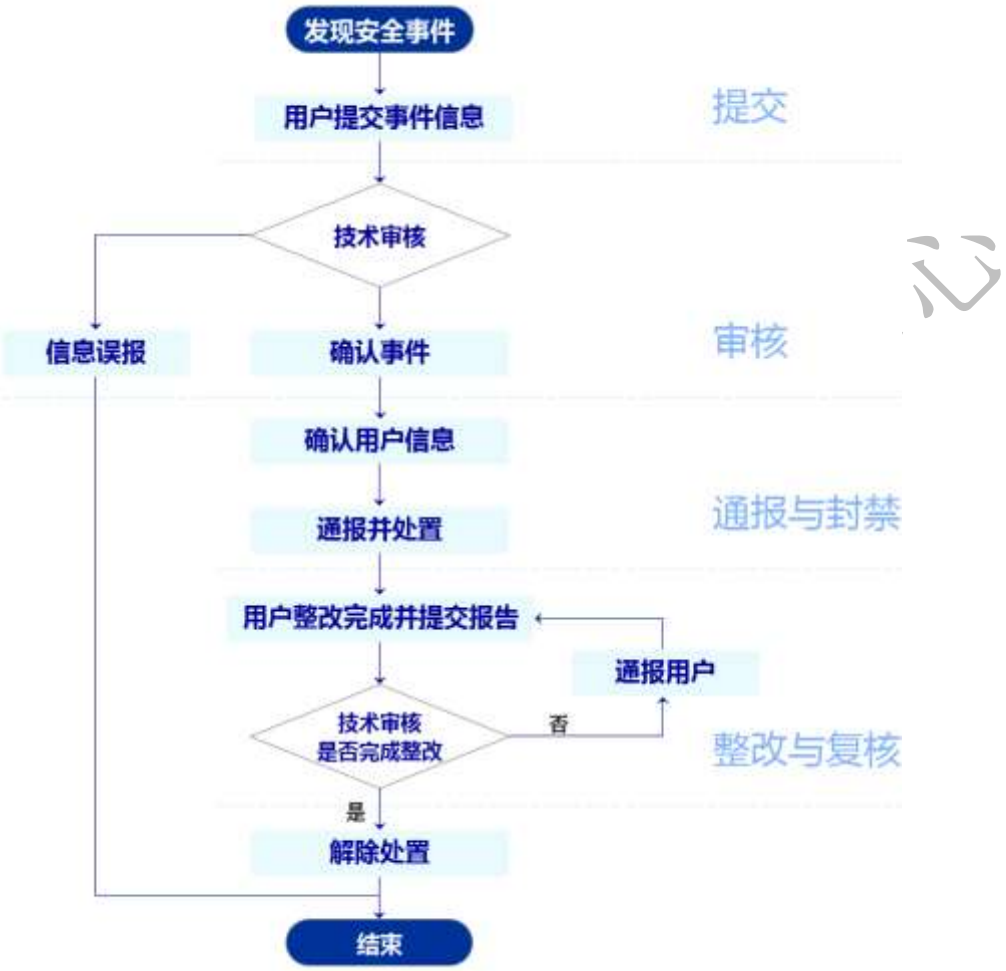
审核： 审核人员根据提交的信息确认网络安全事件是否有效；

通报： 如确认存在网络安全事件，提交处置意见后进入通报流程；

封禁： 根据安全事件的严重性，审核人员对通报账户或系统进行处置；

整改： 被通报用户收到短信后可以登录平台获取网络安全事件的相关信息，根据提示要求并完成整改后，将整改结果和整改报告上传平台；

复核： 审核人员确认安全事件是否完成处置，根据处置结果对通报账户或系统进行解封或驳回等操作。



二、用户登录

平台提供两种登录方式，用户可以通过统一身份认证或手机验证码的方式登录进入安管平台（http://sec.xjtu.edu.cn/event）。

三、处置事件信息

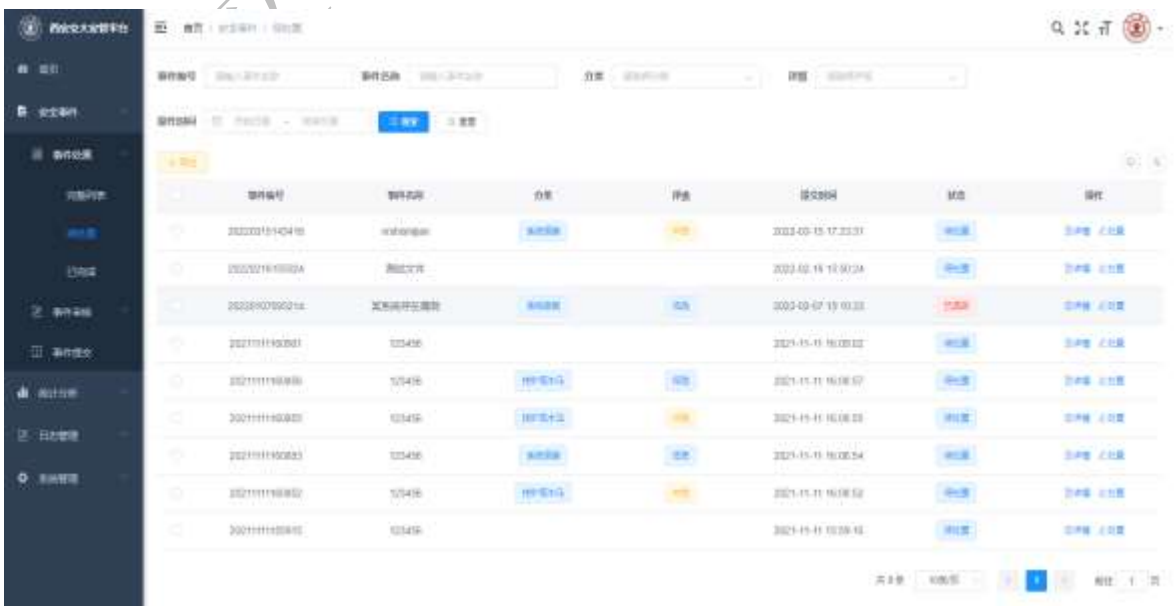
安管平台制定了规范化的处置流程，用户根据流程能够准确地处置通报给自己的安全事件。

1. 查看处置事件

（1）首页快速进入

在首页可以看到与自己相关的处置中事件和我的提交的事件信息数量。“待处置事件”显示的是与自己资产相关的安全事件数量，需要用户处置。“我的提交”是用户在日常工作中发现了安全事件或网站内容错误，可以提交到处置平台上，这里显示的是用户提交安全事件的数量。

通过点击首页的待处置事件可以直接跳转到处置中事件页面，查看与自己相关的处置中事件信息。



（2）侧边栏查看

用户点击左侧侧边栏中的**安全事件**，所有与自己相关的事件都在这里；再次点击**事件处置**，出现下图所显示。

2. 处置中页面

该页面显示所有与自己相关的“待处置”、“待确认”和“已退回”事件；

“待处置”事件需要用户尽快处置；“待确认”事件是用户已经提交了处置信息，等待管理员的审核；“已退回”事件是用户提交了处置信息，管理员审核未通过的状态，需要用户重新提交处置内容。

用户可以根据上方的多个搜索框快速查询自己要处置的事件信息，搜索内容包括事件编号、事件名称、分类、评级和时间。

分类包括：弱口令、挖矿或木马、系统报错、网站真伪和其他漏洞等。

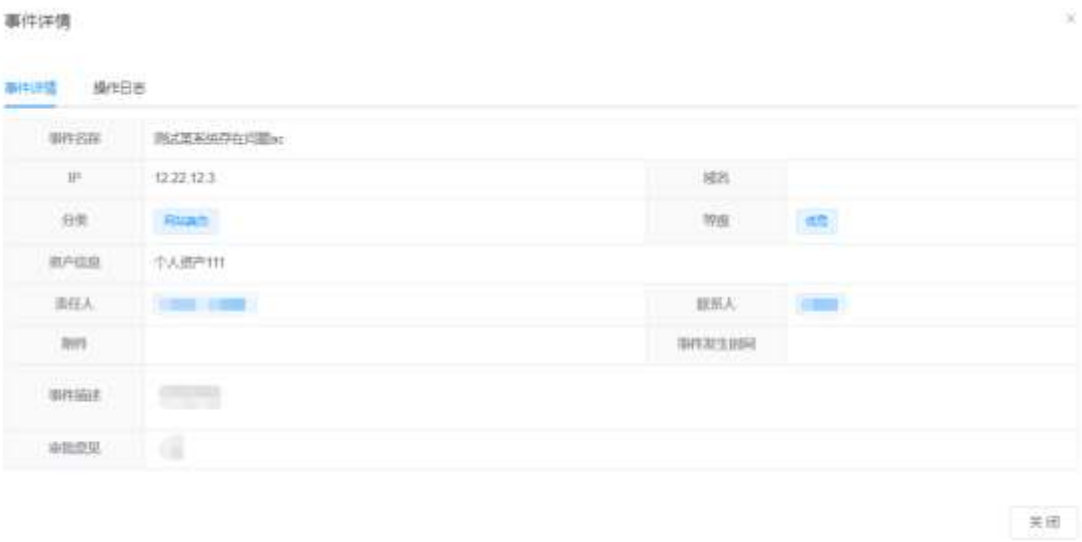
评级包括：低危、中危、高危、严重四个等级。

搜索功能下方有导出按钮，用户可以通过导出按钮将所有安全事件信息导出成 Excel 文件。

再下方是列表信息，信息包括：事件编号、事件名称、分类、评级、提交时间、状态等信息。

列表中的安全事件操作有详情和处置两个功能。

“详情”按钮：

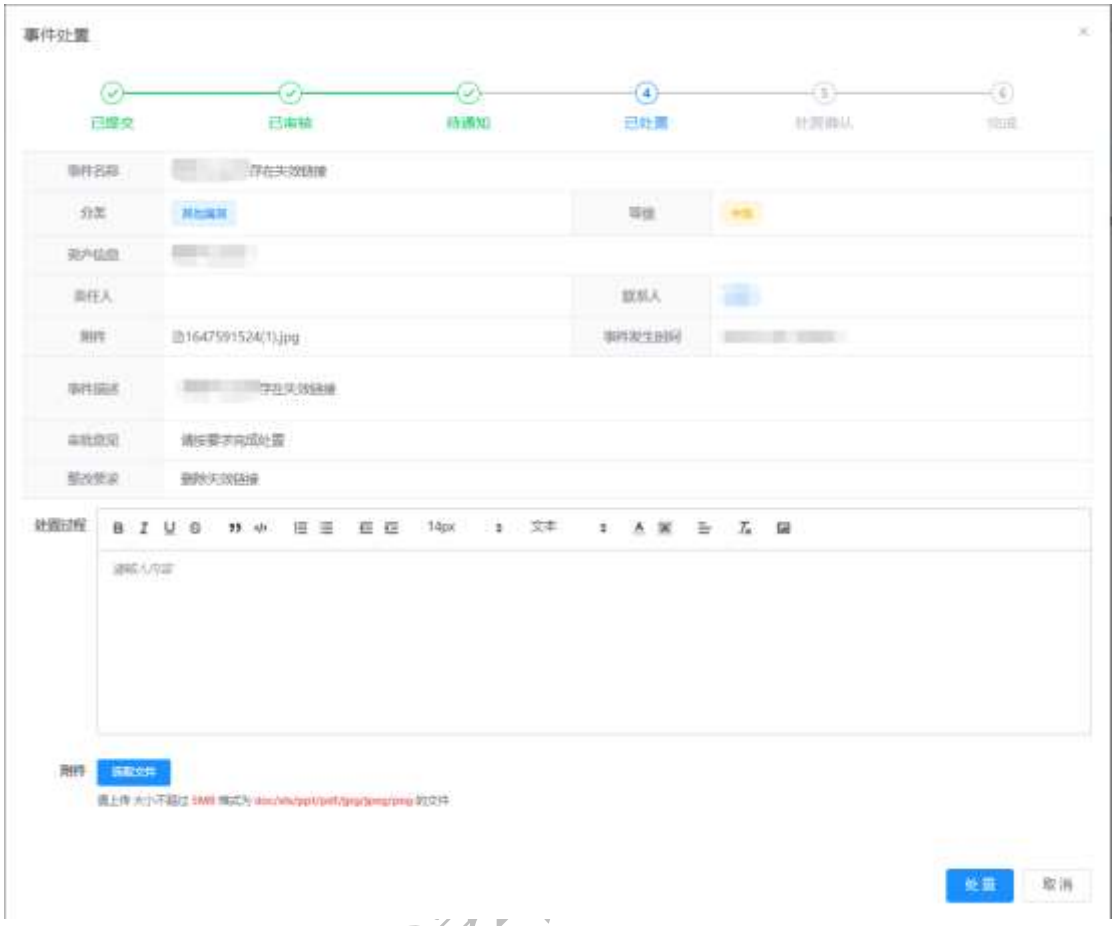


用户可以通过详情按钮查看该事件的详细内容，包括事件编号、事件名称、IP、域名、分类、评级、要求处置时间、事件描述和审批意见等信息。查看是否存在附件，如果有，可以点击文件名称下载附件文件。

详情页面还包括操作日志列表，能够查看所有操作该事件的日志信息，包括操作用户、时间、状态和内容。

“处置”按钮：

用户根据处置页面上方的表格中“审批意见”和“整改要求”完成事件处置的要求，可以在“处置过程”中填写详细的处置内容并在下方的附件中提供文件证明和详细信息，文件格式包括 word、PPT、excel、jpg、png。填写完成后点击右下角“处置”按钮提交处置信息，安全事件进入“待确认”状态，等待管理员审核。



此时用户提交的处置信息，能够在详情中看到“处置详情”，包括用户提交的附件和处置内容。

3. 已完成页面

该页面显示与自己相关的“已完成”安全事件，方便用户追溯历史事件信息。

页面中包括搜索功能、导出功能和查看详情。

搜索功能能够快速定位安全事件信息。

搜索下方的是导出功能，能够将所有安全事件信息导出为 Excel 文件。

列表中的操作列表能够通过“详情”按钮查看该事件的详细信息、处置详情和操作日志。

4. 完整列表

完整列表，该页面显示与自己相关的所有安全事件，包括“待处置”、“待确认”、“已完成”和“已退回”事件的信息。

5. 处置安全事件

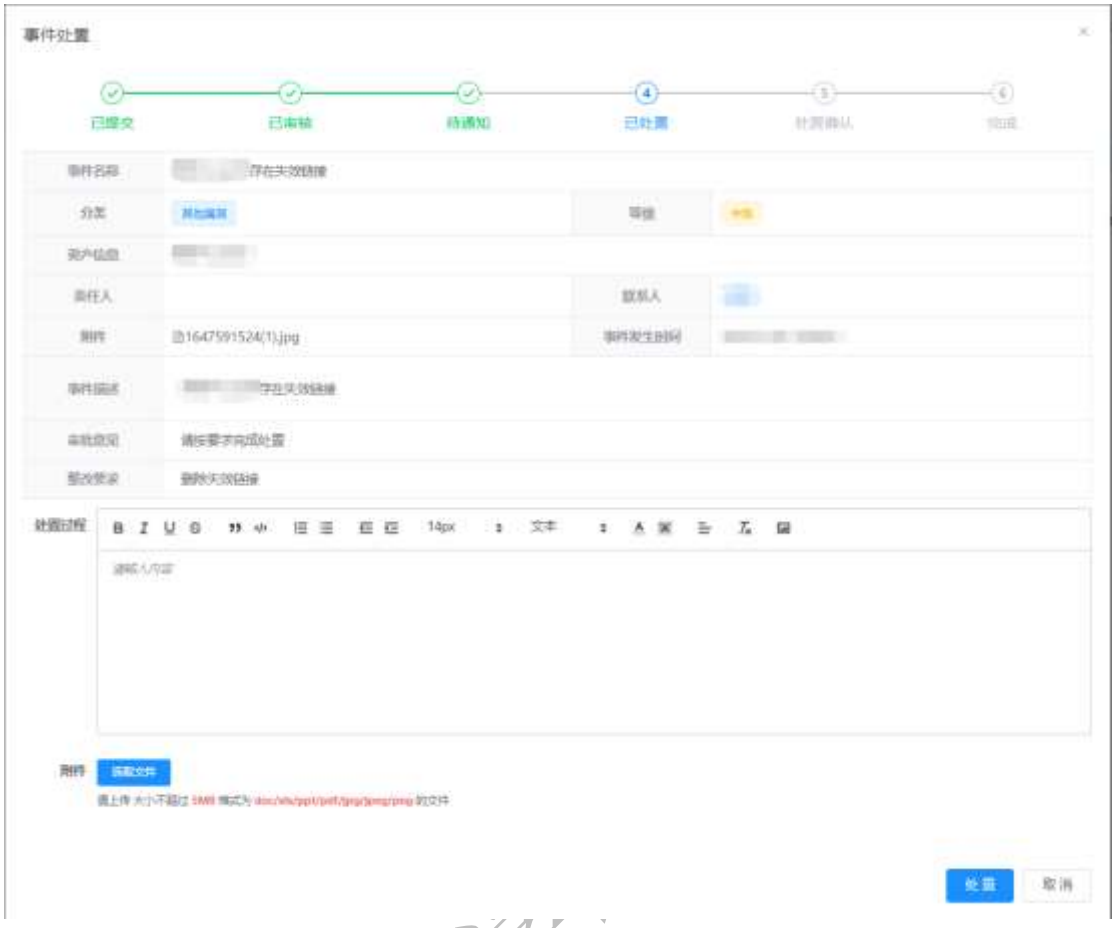
用户收到短信，包含事件名称、风险编号、以及整改要求时间和网站域名信息。

用户进入平台后，通过首页快速查看或者侧边栏查看进入“处置中”页面。

根据短信信息中事件编号和事件名称，使用页面上方搜索功能，快速定位事件信息。

点击事件的操作栏中的**处置**按钮。

进入处置操作页面。



（1）资产不属于自己

如果用户发现安全事件详情中的 IP、域名或者事件描述中的详细信息包含的 Mac 地址等信息不是自己的资产或者资产责任人已经变更，可以在处置页面的“处置过程”中填写：“该资产不属于我”或“该资产归属权已变更”等描述信息。右下角“提交”按钮提交反馈给管理员；也可以通过电话或微信等方式反馈给网络信息中心。

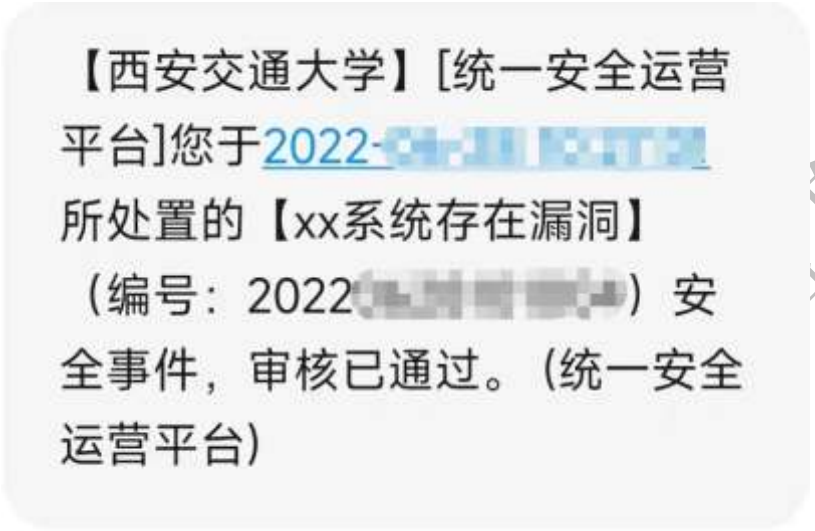
（2）资产属于自己

用户确定事件详情中的 IP、域名等信息是自己的资产，查看安全事件的详细信息和“整改要求”，下载事件附件。根据“整改要求”

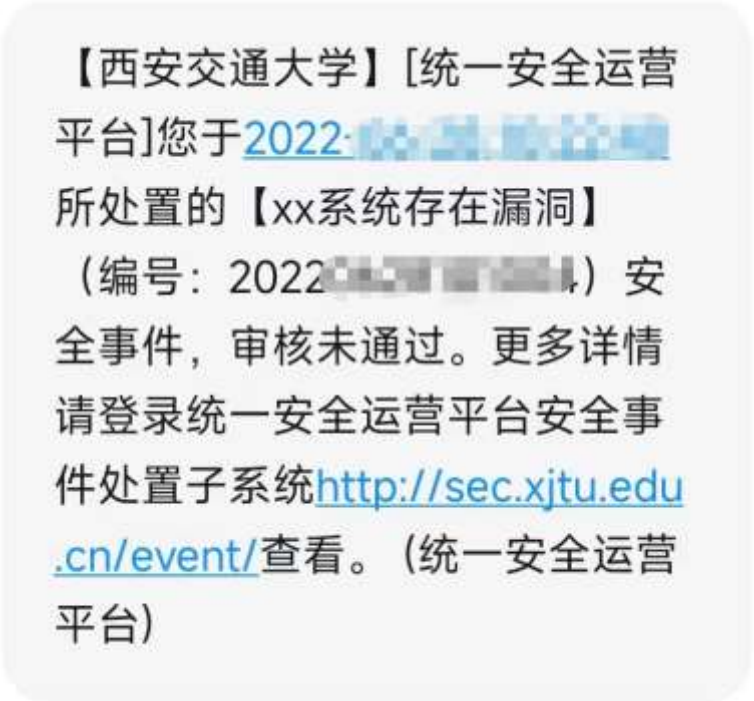
完成处置后，用户处置页面填写“处置过程”，并上传处置结果附件。

点击右下角“处置”按钮后，事件状态转变为待确认状态，等待审核员进行审核。

如果管理员审核通过，事件进入“已完成”状态，则该事件处置流程完成，用户会收到该事件审核通过的短信提醒用户。



如果审核员审核未通过，则该事件再次进入“已退回”状态，相关用户会收到事件审核未通过短信。



等待相关用户重新处理事件后，点击“处置中”页面的“处置”按钮，打开处置页面再次提交处置完成的“处置过程”和附件信息，点击右下角“处置”按钮，提交处置信息，等候审核员审核，直至审核通过，事件进入已完成状态，则事件处置流程完成并收到事件处置审核已通过的短信通知。

四、我的提交

安管平台处置系统不仅支持用户处置自己系统的安全事件，也支持用户举报在日常工作中发现的安全事件：如来自校内的网络攻击、网站内容错误等其他安全事件。

1. 进入提交页面

（1）首页快速进入

用户登录成功后，进入首页，点击**我的提交**，可以直接跳转到提交页面。

（2）侧边栏进入

通过左侧侧边栏，安全事件下的**事件提交**，进入提交安全事件页面。

2. 事件提交

用户进入提交页面，页面中包含**搜索**功能、**新增**安全事件功能、**导出**安全事件功能以及列表中操作列的**修改、删除、详情**和**重新生成**按钮。

搜索功能：

用户通过页面上方的搜索框查询相关的安全事件信息。包括事件编号、IP、域名、事件名称等信息。

新增按钮：

搜索框下方第一个按钮是“新增”按钮，点击进入添加安全事件信息页面。

用户提交的事件信息包括：事件名称、网站名称、IP、域名、分类、评级、事件发生的时间、附件和事件详细描述，其中有红※的项为必填项。用户点击右下角“提交”按钮，增加一条安全事件信息，等待管理员的审核。

“导出”按钮：

第二个按钮是“导出”按钮；用户点击“导出”按钮可以将全部事件信息导出为 Excel 文件。

列表信息包括：事件编号、事件名称、IP、域名、网站名、分类、

评级、状态和提交时间。

列表中的事件操作包括：修改、删除、详情和重新生成。

用户点击“修改”按钮，打开修改页面，用户能够修改提交的安全事件信息。管理员审核后，用户不能修改。

用户点击“删除”按钮，可以删除该事件信息，管理员审核过，用户不能删除。

如果提交的事件被管理员驳回，该事件进入“已驳回”状态，用户可以重新新增一个安全事件信息，也可以直接点击列表的操作列中“重新生成”按钮再次生成一个相同的安全事件，用户点击“修改”按钮，修改信息后，点击右下角“修改”，再次提交安全事件信息。

用户点击“详情”按钮，打开详情页面，可以查看提交的安全事件详细信息和操作日志。

五、平台使用技术支持

何柯楠

电话：88968989　18191124356