阿里云
IoT安全运营中心

用户操作指南

文档版本：20190905

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

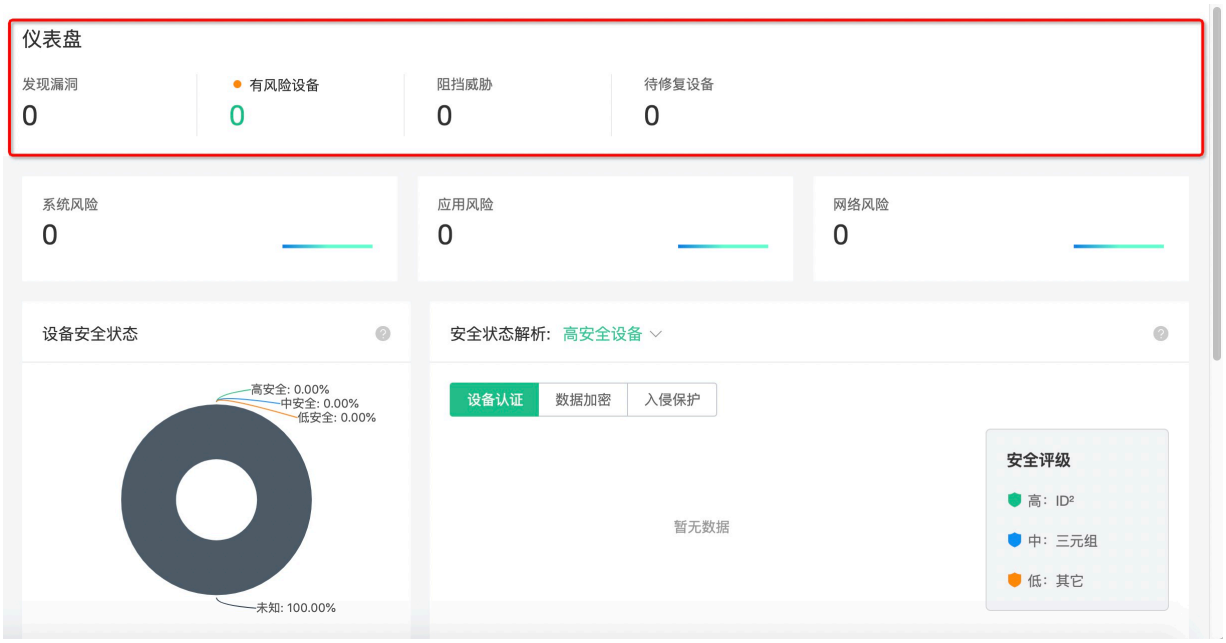
1 仪表盘

仪表盘实时展示IoT系统的安全状态，从多个维度对不同安全等级设备进行综合的安全评估和历史记录信息。

仪表盘

仪表盘面板展示了累计检测到的威胁、风险数量。

- 发现漏洞：累计所有设备上发现的漏洞数量。
- 有风险设备：累计所有存在未修复漏洞风险、异常行为风险的设备数量。
- 阻挡威胁：累计SOC为IoT系统接入设备已阻止的异常行为数量。
- 待修复设备：整个系统中存在未修复漏洞风险的设备数量。



风险统计

风险统计从不同维度对整个IoT系统面临的风险进行统计，分为系统风险、应用风险、网络风险三大类。

- 系统风险：系统中异常的应用执行或对象的未知改动，常见典型的风险：执行文件改动。
- 应用风险： 应用中异常的执行行为，常见典型的风险：文件访问等。
- 网络风险：设备异常的网络通信行为，常见典型的风险：对未知目标发送数据。

设备安全状态

设备安全状态展示了不同安全等级的设备占整体的比例。等级状态解析是以某个安全等级为集合，统计了不同维度的设备数量在该集合的占比。当前纳入安全评级的维度是：

- 设备认证：对设备的唯一合法身份认证的方式。
- 数据加密：数据传输过程中采用的数据加密方式。
- 入侵保护：检测和阻止攻击者对设备发起入侵活动的方式。

异常风险趋势

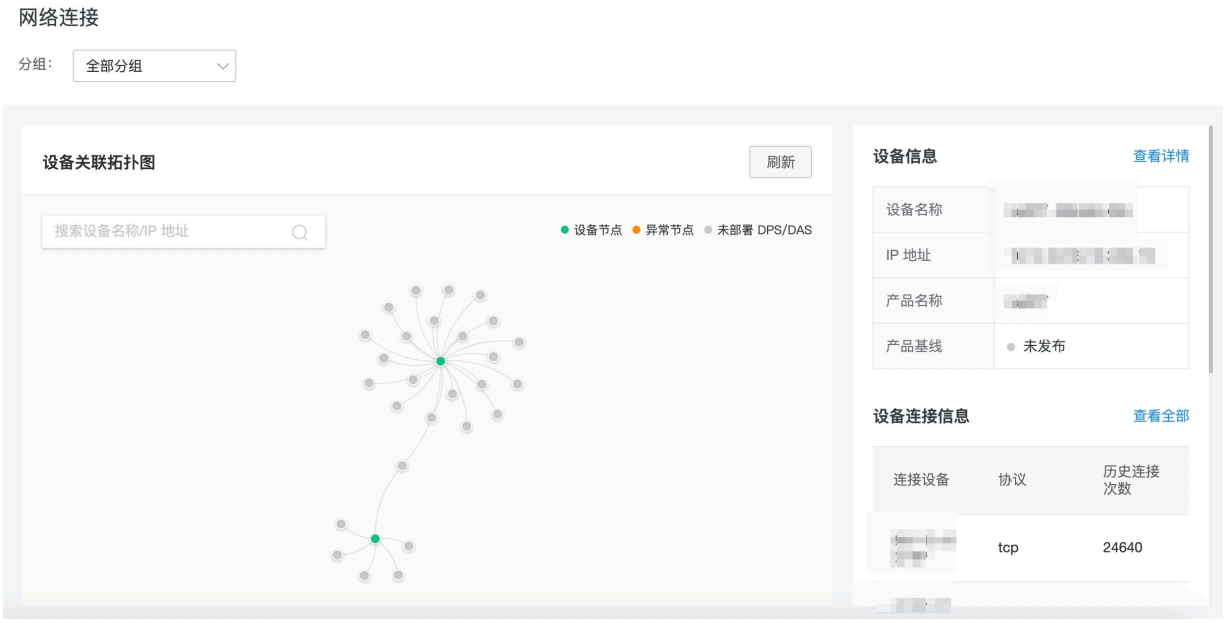
以事件轴的方式展现最近15天内每天异常事件的数量和受影响设备的数量，可以直观的反映设备安全运行的历史记录。通过异常风险趋势图便于发现潜在的风险或缩小攻击溯源的排查范围，在事件密集的时间段发生攻击入侵的事件概率较高。

2 网络连接

网络连接基于历史的网络通信行为，以可视化的方式生成终端设备与终端设备之间、终端设备与网关节点之间、终端设备/网关节点与其他网络服务的连接关系。

设备关联拓扑图

与物理的网络拓扑不同，SOC的网络连接仅展示有实际通信行为的连接关系。



- 设备节点的颜色代表了该设备当前的安全状态，具体安全状态请查看拓扑图右上角的图例。
- 网络连接拓扑是基于所有设备的历史通信数据生成，您可以通过切换分组来查看更小范围的网络拓扑信息。
- 您可以通过点击拓扑图中的某个节点、搜索某个设备的名称/IP地址，选中一台设备。拓扑图右侧展示被选中设备的相关信息。
-

设备信息

被选中节点的详细信息。

- 设备名称：该设备在阿里云物联网平台、IoT安全运营中心（SOC）定义的设备名称。
- IP地址：该设备的网络地址，设备有可能有多个IP地址。
- 产品名称：该设备在阿里云物联网平台、IoT安全运营中心（SOC）所属的产品。
- 产品基线：该设备所属的产品是否已经发布了基线。
- 操作-查看详情：跳转到”设备详情“页，查看该设备更多的信息。

网络连接信息

被选中节点的历史信息汇总统计。

- 展示网络连接次数为TOP5的信息，包括：对端连接的设备、连接协议、历史连接的次数。
- 操作-查看全部：被选中节点所有的历史通信信息。

产品风险信息

与被选中节点同一产品的所有设备的风险信息汇总。

- 包括异常事件、组件漏洞，以及处理状态。
- 操作-查看详情：跳转到”异常事件“页面，可以查看到该产品不同类型的安全风险详情。

3 风险管理

风险管理通过持续监控所有设备并识别出风险行为，便于管理员及时控制和消除潜在风险。风险管理主要包括：

- 异常事件
- 组件漏洞
- 安全日志

3.1 异常事件

异常事件展现了每一个异常事件的详细信息，针对每一个异常事件提供了操作处置选项。

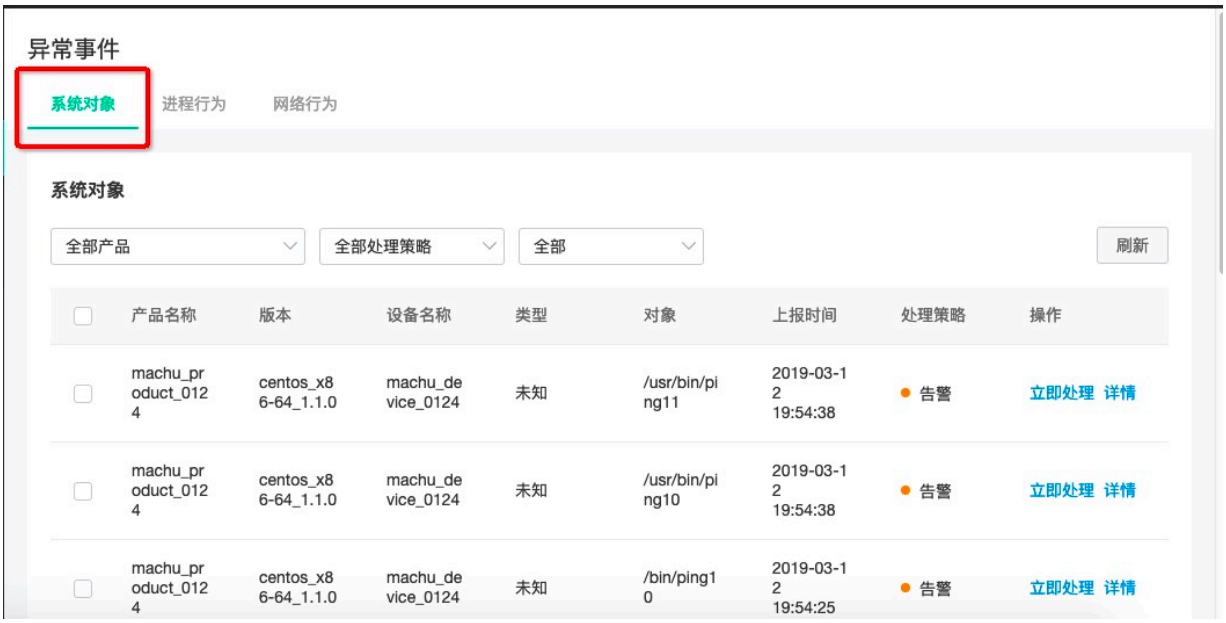
- 系统行为
- 进程行为
- 网络行为

事件处理

管理员可以根据实际应用场景进行处理，包括告警、阻止、允许。

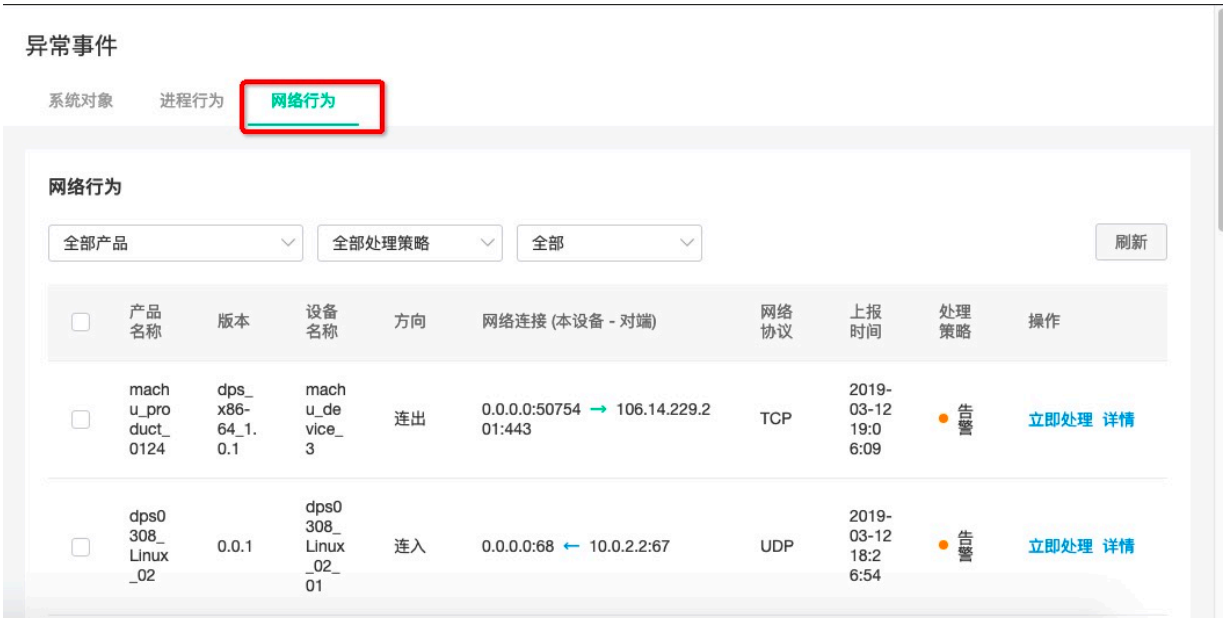
- 告警：本次不处理，后续再发生仍然会上报为异常事件。
- 阻止：后续同样的事件发生时，SOC会进行阻断操作。
- 允许：后续同样的事件发生时，SOC不做阻断处理且不再上报为异常事件。

异常事件-系统对象



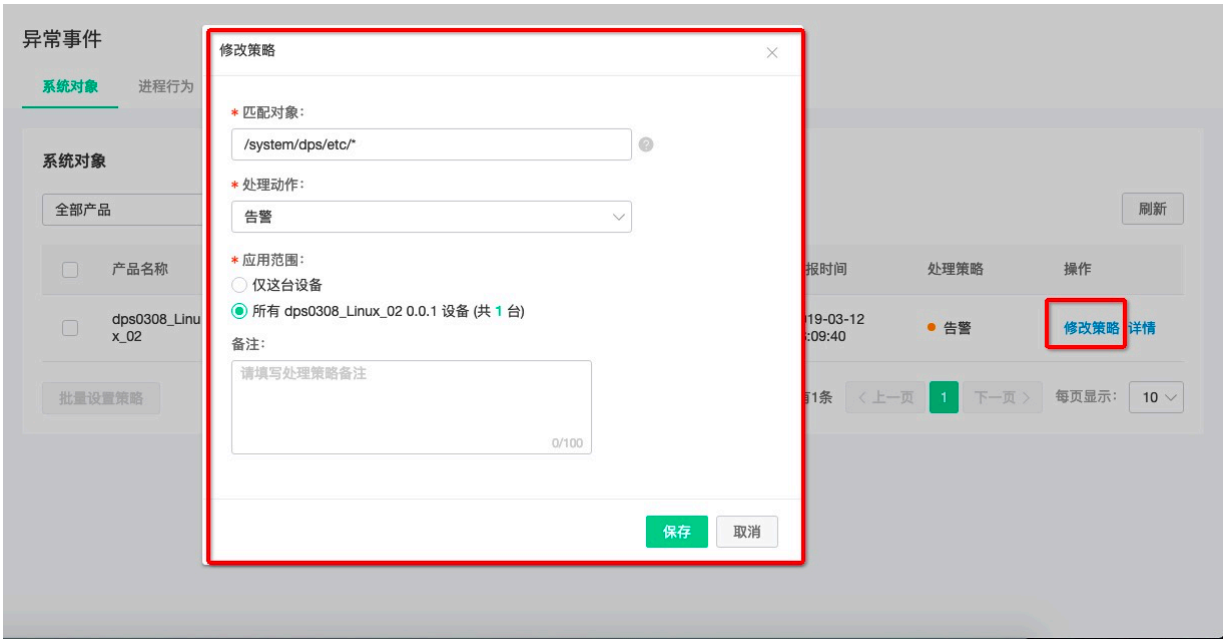
异常事件-进程行为

异常事件-网络行为



修改策略

异常事件上报后初始操作为”立即处理“，无论您在“立即处理”中执行了哪些操作，都可以通过“修改策略”重新设定针对某类事件（符合策略匹配对象、应用范围）的处理动作。



匹配对象支持通配符操作：

匹配对象	支持的通配符	示例
文件路径或进程	· 单个字符用?表示； · 同一个路径内的任一字符用*表示； · 任意层路径用**表示；	/system/dps/etc/*
IP地址	· 支持子网掩码； · 多个IP/IP段用逗号,分隔； · 一组连续的IP用短横线-连接。	192.168.1.0/24,192.168.2.1-192.168.2.100

操作项状态：

操作项	说明
立即处理	该事件上报之后，管理员未做处理（没有配置相应的策略）
修改策略	管理员已经做了处理，并配置了相应的策略，可以通过“修改策略”重新调整策略。

详情

通过“详情”查看该异常事件的详细信息：

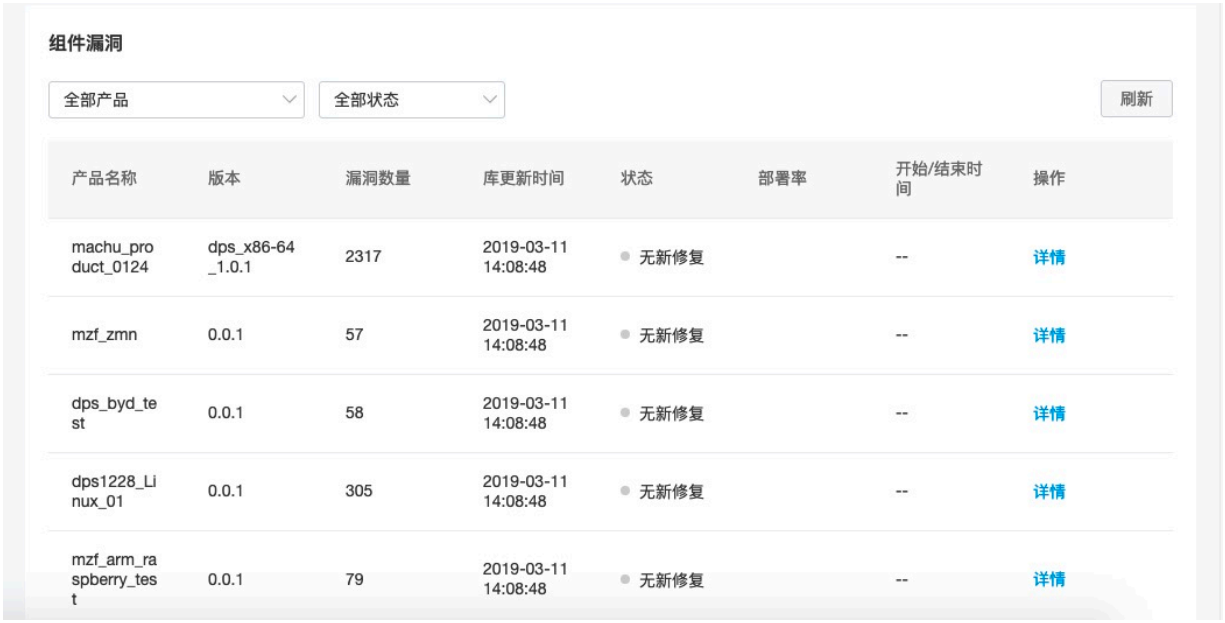
信息	说明
产品名称	产生该事件的设备是属于哪一个产品
ProductKey	该产品的ProductKey值
DeviceName	产生该事件的设备的DeviceName，标识一台唯一的设备
生产商	该设备的生产厂商

信息	说明
产品版本	该产品的版本
首次上报时间	该事件第一次发生的时间点
处理策略	针对该事件的处理方式（后续同样事件发生时，按照处理方式自动执行）
描述	提供更多的事件信息，帮助管理员配置合适的处理策略
最近10条异常上报	该事件最近10次发生的时间点，以及每次发生时的处理结果

3.2 组件漏洞

组件漏洞展示了每一型号产品中所有组件存在的漏洞数量。漏洞数量是该产品所有组件存在的漏洞（基于安全运营中心的漏洞库扫描结果）的总和。管理员通过漏洞修复功能将指定的补丁或者系统镜像部署到指定的型号产品中。

组件漏洞

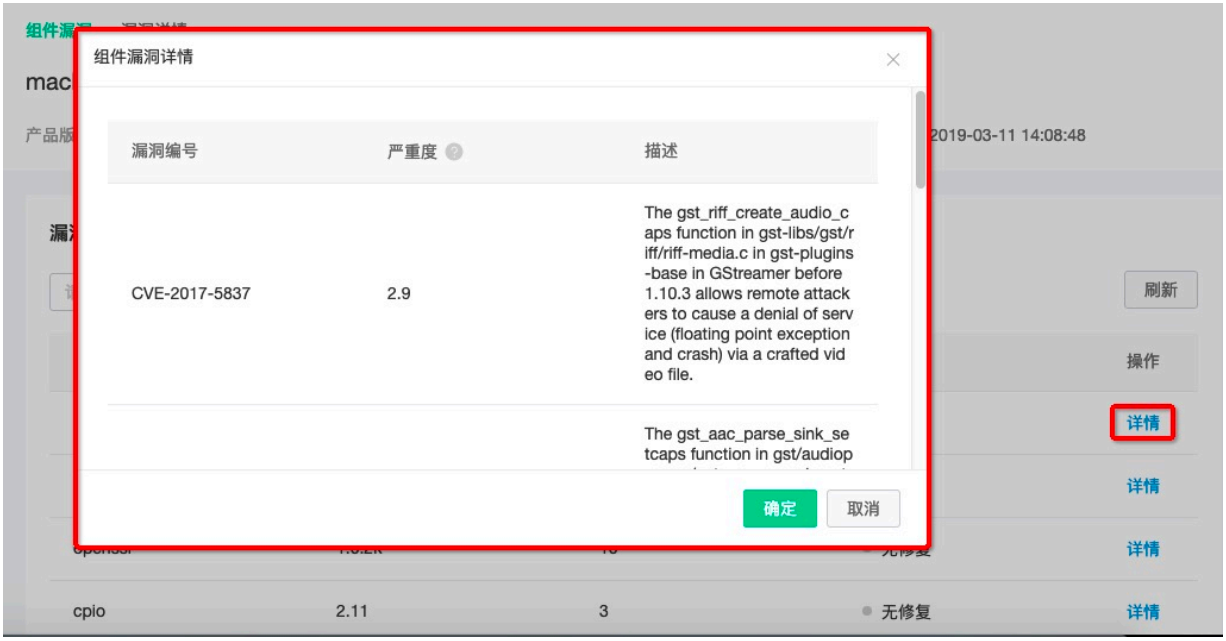


漏洞列表

基于某个产品，以组件为序列罗列出每个组件存在的漏洞数量。

漏洞详情

查看某个组件下，所存在的漏洞列表，描述每一个漏洞的漏洞编号、严重度、描述。严重度越高，代表该漏洞被攻击者利用时造成的安全风险越大。



部署修复

部署修复以产品为单位，对该产品下所有的设备执行修复，修复范围：存在修复补丁的组件。

3.3 安全日志

安全日志提供设备取证和其他安全操作历史记录的列表和查看的功能，方便了解设备周期取证的执行结果，和单个设备实际响应情况。在复查设备侵入事件时可以帮助缩小调查范围。

4 设备管理

本章主要描述设备管理中的安全基线、基线详情和设备状态的管理。

如果还没有接入设备，那么您需要在物联网平台上创建产品和设备，集成安全开发组件之后，即可进行安全基线的检测。

安全基线

安全基线指的是特定的IoT产品维持其正常业务功能所需要的基准行为，包括网络、设备访问、进程间IPC通信、文件访问等。

安全基线包含两类：

- 一类是静态文件取证，通过扫描系统中已有的二进制文件，计算文件hash并上报云端。该功能的主要作用是后续如果有未知的程序侵入，可以及时被发现和阻止。
- 另一类是动态行为采集，相对静态文件取证来说，动态行为采集可以捕获系统中进程在动态运行过程中所做的操作，例如访问网络、打开设备驱动、进程间IPC通信等。

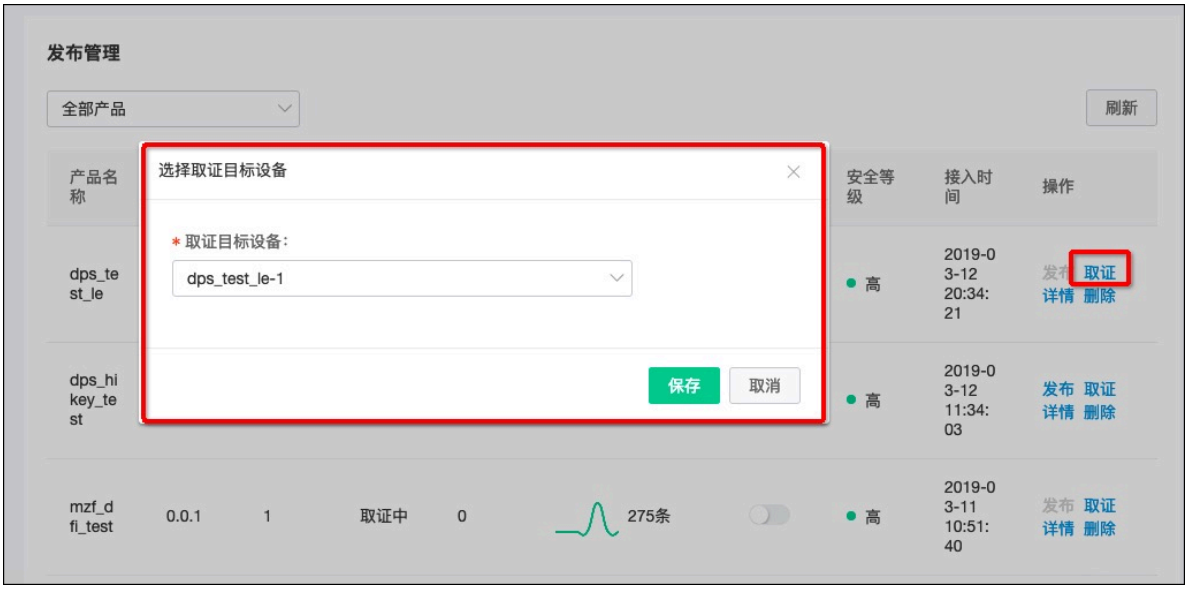
一切不在基准行为规则里面的操作和程序运行都被视为是风险行为而被拦截。SOC基于阿里云IoT安全团队沉淀的安全能力，通过持续感知设备正常运行期间的行为生成多个安全维度的行为基线，管理员可以按需修正后发布该基线作为后续设备运营阶段的安全监控参考基线。安全基线可以有效拦截攻击者远程入侵和未知风险文件的运行，从而保证IoT设备的安全。

SOC为每一款产品生成的安全基线均为未发布状态，需要用户执行发布。发布后的基线会对设备的行为进行安全基线检查，按照既定的策略进行自动处理。

生成安全基线

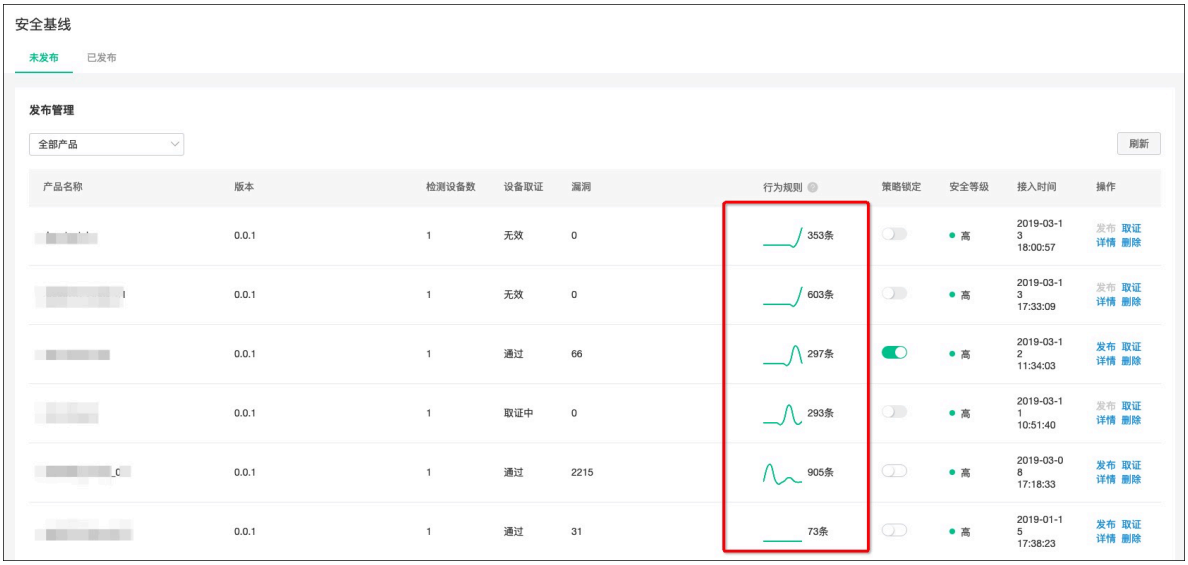
- **设备取证（静态文件取证）**

  需要用户手动执行“取证”操作。



- 行为规则

  安全基线的动态行为采集由SOC SDK全自动完成，无需人工干预。



> **说明:**
>
> 行为规则曲线波动较小后再发布基线，能够获得更好的安全防护效果和更精确的风险事件预警。

- 策略锁定

  - 开启了策略锁定：允许安全基线允许的行为发生，安全基线以外的行为将会产生告警。
  - 未开启策略锁定：只允许安全基线允许的行为发生，安全基线以外的行为将会被阻止。

发布安全基线

- 全局基线：安全基线覆盖了设备的所有行为。
- 系统基线：安全基线仅覆盖了设备的部分行为，不包含后续安装的其他应用（不阻止新应用/组件的安装和执行，但是会生成告警上报给管理员）。

说明：

已发布的安全基线，不允许修改任何配置。如果需要重新配置安全基线，需要执行“撤销发布”，恢复为 未发布的安全基线。

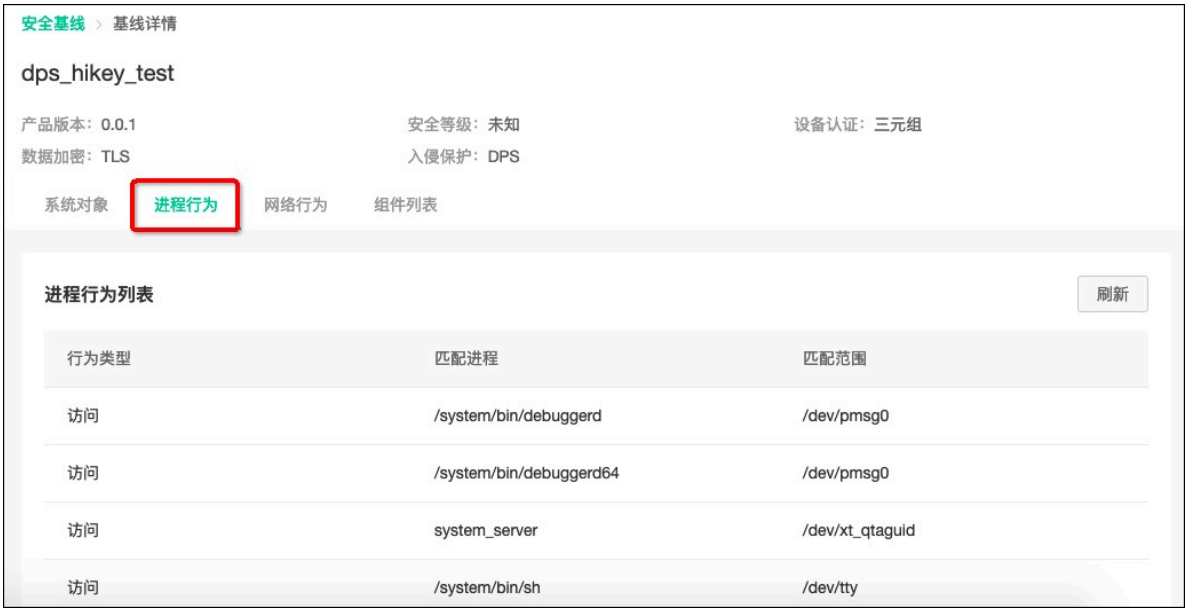
安全基线详情

无论安全基线是否发布，都可以通过基线详情查看指定产品的安全基线，包括如下。

- **系统对象**


安全基线 > 基线详情
dps_hikey_test
产品版本：0.0.1
安全等级：未知
设备认证：三元组
数据加密：TLS
入侵保护：DPS
系统对象
进程行为
网络行为
组件列表
系统对象列表
刷新
对象类型
对象
可加载库
/system/bin/dps/lib/libdl.so
可加载库
/system/bin/dps/bin/logd
可加载库
/system/bin/dps/bin/linker64
可加载库
/system/bin/dps/bin/linker

- **进程行为**

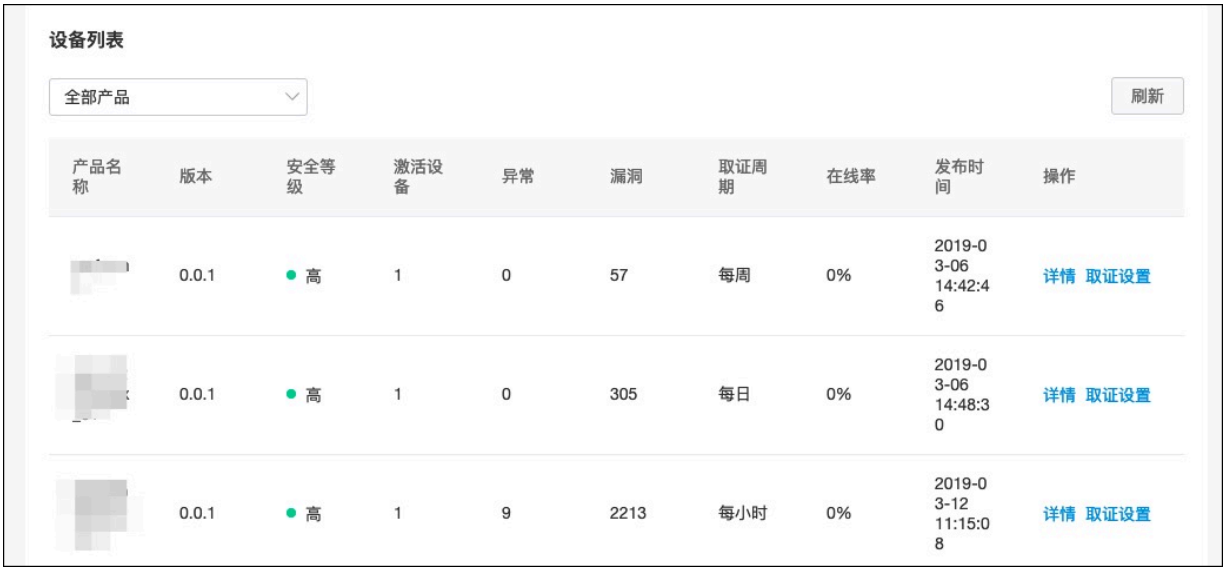

安全基线 > 基线详情
dps_hikey_test
产品版本：0.0.1
安全等级：未知
设备认证：三元组
数据加密：TLS
入侵保护：DPS
系统对象
进程行为
网络行为
组件列表
进程行为列表
刷新
行为类型
匹配进程
匹配范围
访问
/system/bin/debuggerd
/dev/pmsg0
访问
/system/bin/debuggerd64
/dev/pmsg0
访问
system_server
/dev/xt_qtaguid
访问
/system/bin/sh
/dev/tty

- 网络行为

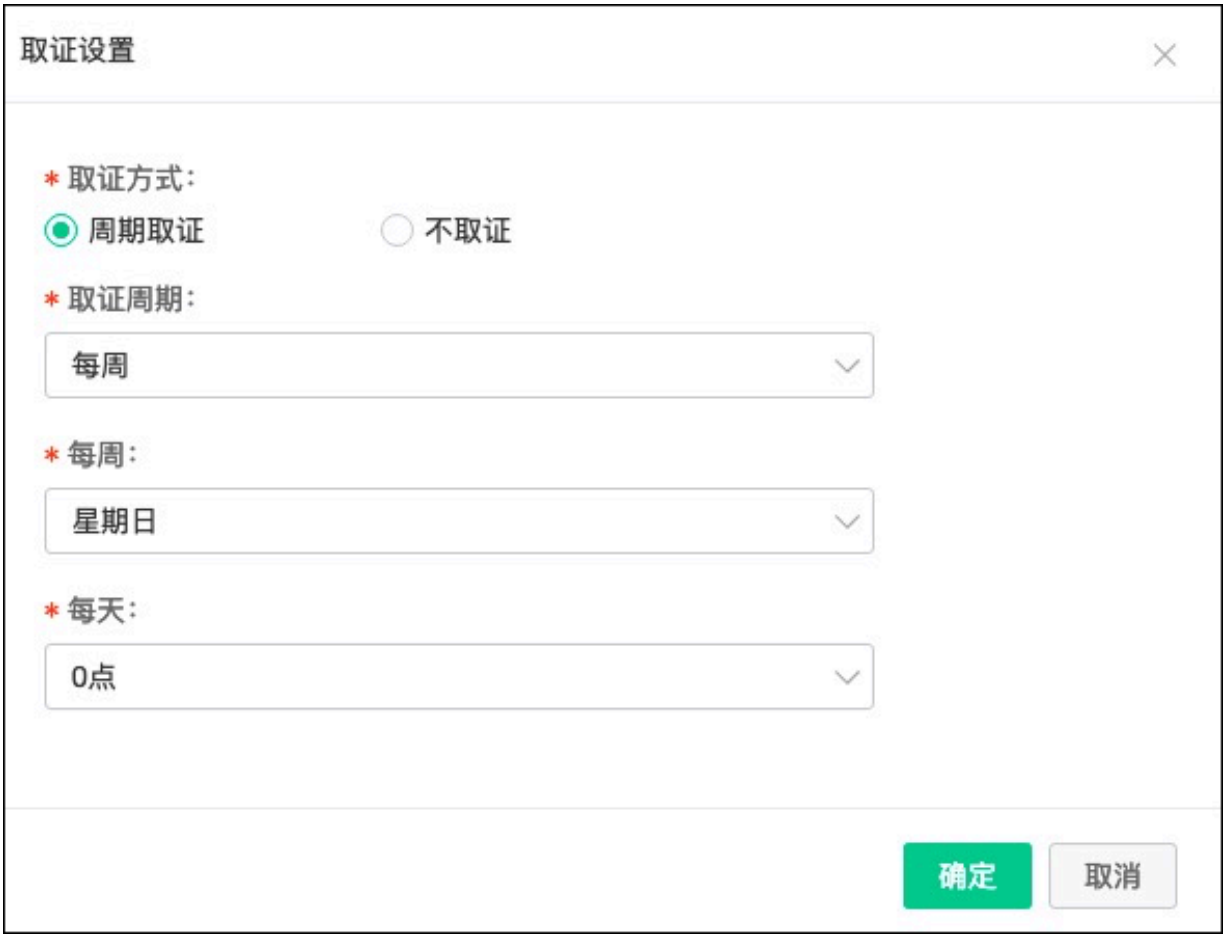
- 组件列表

设备状态

在设备安全发布后，针对每一型号设备的状态汇总和取证周期的设置需要在状态管理完成。管理员可以在该界面进行设备状态查询和调整取证周期。



您也可以单击取证设置，设置取证方式。



5 运营托管

运营托管是将您账号下所有物联网设备（仅部署了 SOC SDK 的设备）完全托管给 SOC，托管期间您随时可以通过自己的阿里云账号登录并查看所有风险事件、设备信息、运营托管任务的进展。

使用运营托管功能有如下注意事项：

- 公测期间，可以免费试用。
- 同一时间内，只有一个托管任务有效。
- “安全运营托管”期间SOC只会执行该产品能的安全风险检测、安全风险防护、设备管理、安全基线管理等功能，没有权限也不会去执行/处理其他云产品的功能/事件。
- “安全运营托管”期间阿里云IoT安全运营中心不会自动执行如下操作。
  - 修复安全漏洞
  - 修改预留的联系方式/邮箱
  - 修改阿里云账号的信息资料
- 您有权利随时终止运营托管。

开启托管任务

在物联网安全运营中心左侧导航栏选择设备管理 > 运营托管，单击开启托管，设置托管参数，启动托管任务。

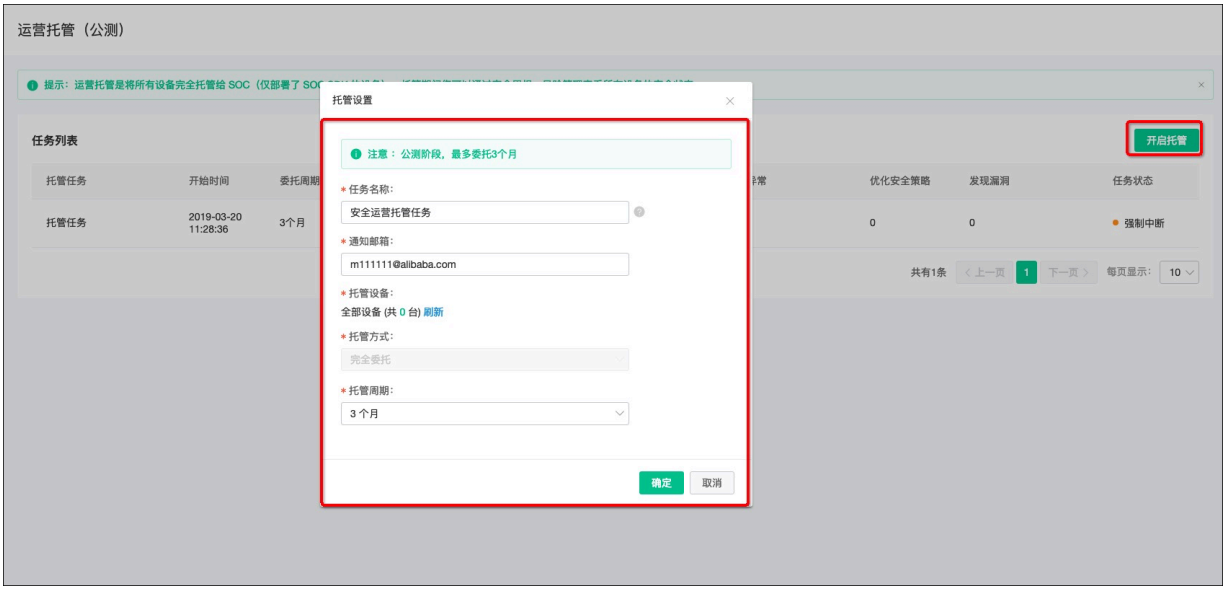


表 5-1: 参数说明

参数	说明
任务名称	通过任务名称来标记本次托管任务的目标、范围、作用等。
通知邮箱	用于接受托管报告、紧急风险事件的邮箱。默认采用通知设置中的邮箱，可以根据实际情况做修改。
托管方式	支持完全托管方式，将您账号下所有的物联网设备（部署了SOC SDK且能够连接到SOC的所有设备），都委托给IoT安全团队来做安全运营。
托管周期	IoT安全团队约定本次托管任务运行的时间，托管任务到期后自动撤销安全运营管理授权。

终止托管任务

托管任务进行期间，您可以选择随时终止托管任务。

在物联网安全运营中心左侧导航栏选择设备管理 > 运营托管，单击终止托管，来终止当前执行的托管任务。


终止托管
您确定立即终止托管任务吗?
持续运行
10天
发现风险
100个
优化策略
9个
保护设备
20台
处理异常
132个
发现漏洞
86个
立即终止
取消

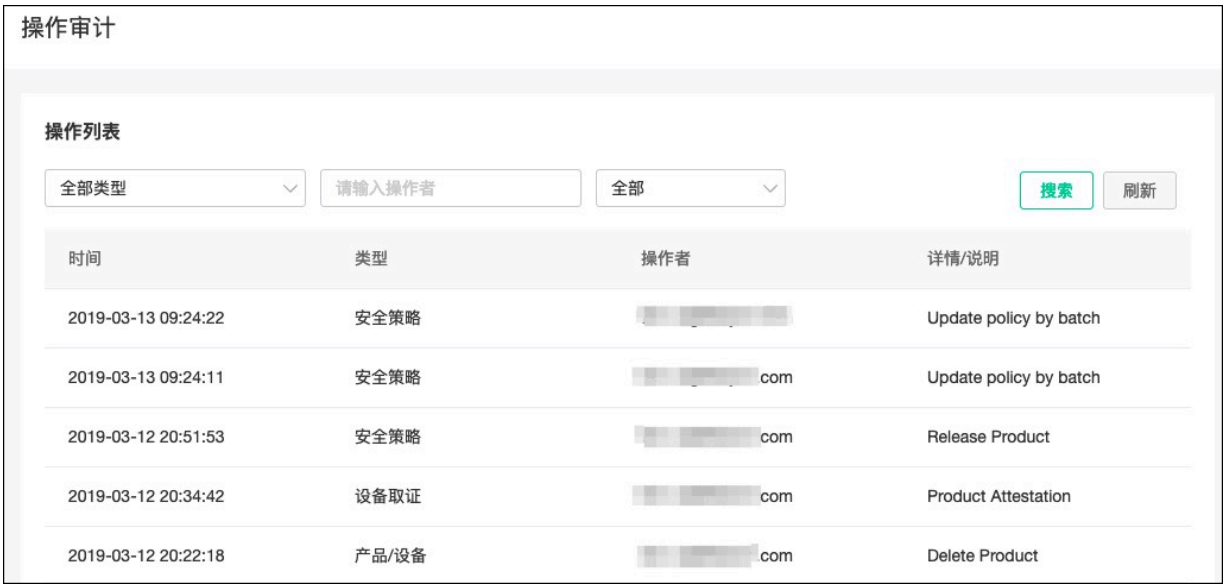
6 操作审计

操作审计记录了管理员在SOC上的所有配置操作。

操作审计包括：

- 账号管理
- 安全策略管理
- 产品/设备管理
- 设备取证
- 托管管理
- 漏洞检测
- 漏洞修复

管理员可以通过操作审计日志追溯某一个账号对某一类配置的变更动作。



7 通知设置

管理员可以根据实际要求选择需要通知的事件，并设置一个邮件地址实时接收相应的通知邮件。

- 异常风险通知：设置接收邮箱地址，默认每隔一小时收到一封异常风险汇总邮件。邮件中汇总的风险为近1小时产生的新风险。
- 漏洞库更新通知：设置接收邮箱地址，当检测到新的漏洞时，会定期收到一封漏洞汇总邮件。邮件中汇总的漏洞为近1小时产生的新漏洞。

发件人地址为：`linksecurity@service.aliyun.com`，请不要忽略或设置为垃圾邮件。