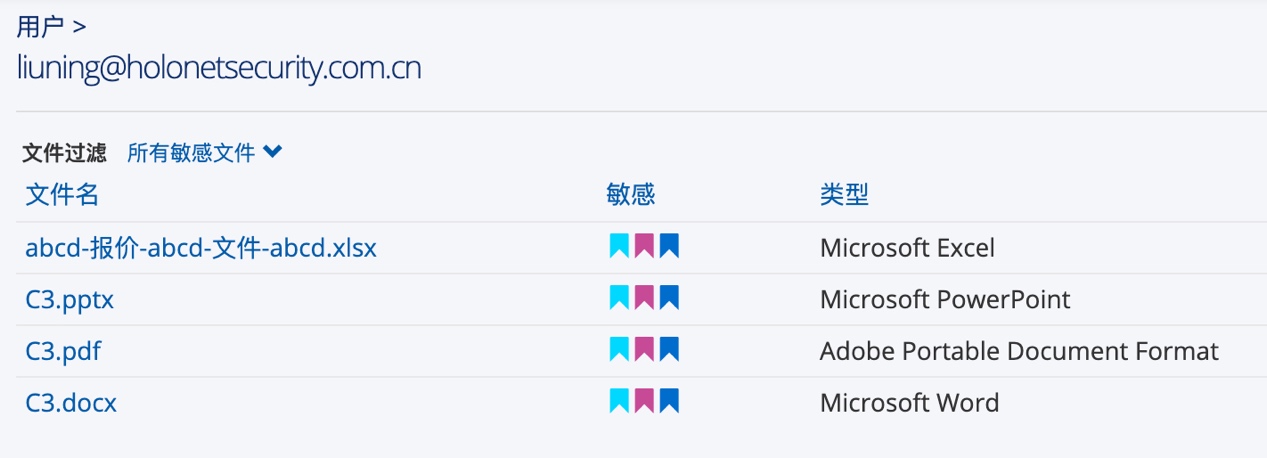
4.0内部测试

1. 敏感级别标签



C1信息：包含：身份证，电话号码

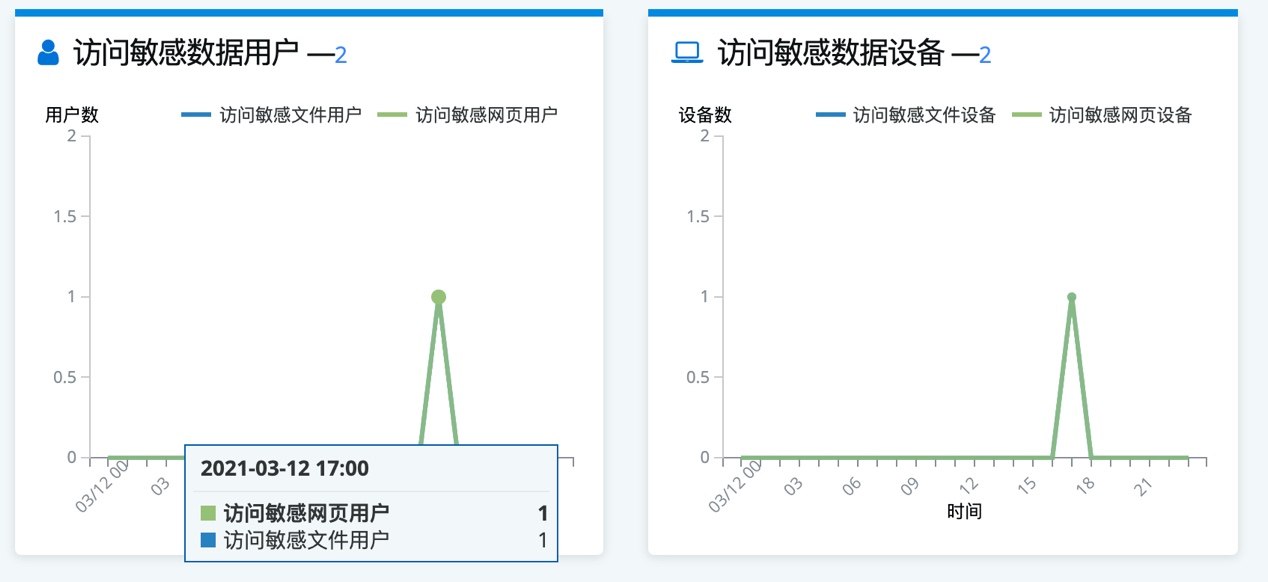
C2信息：包含：身份证，电话号码，银行卡

C3信息：包含：身份证，电话号码，银行卡，交易信息（匹配关键字“金额”）

结果C3文件有3个敏感标记

需求已记录，后面会讨论解决

1. 敏感数据

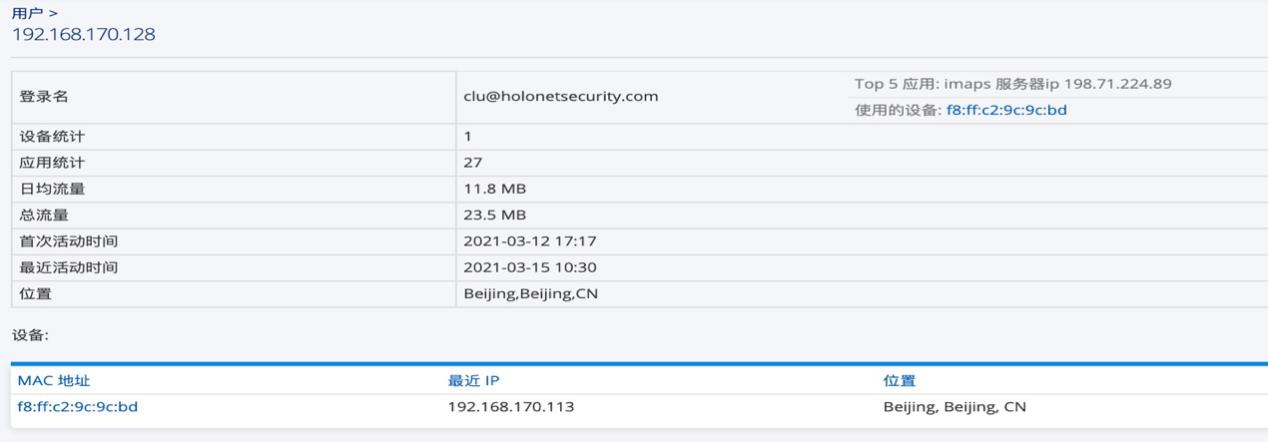


访问敏感文件和网页的用户都是1，在统计图上二者曲线重叠。

已记录属于需求优化，后面会讨论解决

1. 用户账号关联

3.1 非公司邮箱账号不与IP关联



之前发现的那个BUG，发现的用户账号域名与HF注册域名不一致，不把这个用户账号与用户关联。

如果在用户多域名情况，这个问题比较大。

最新4.0.1版本已修复

3.2 用户账号不更新

用户通过DHCP获取IP地址192.168.170.127，HV把这个IP做为用户账号。之后，该用户通过DHCP获取了其他IP地址192.168.170.111，这个用户账号仍然是原来的IP地址：（如下图所示）



192.168.170.127这个用户，登录阿里网页Web mail，用公司邮箱发送邮件，HV能够抓到用户行为，但是用户账号不更新：



已知问题，未触发登录行为时，如果ip变更会出现上述情况，已记录

1. 规则报警
   1. 数据外泄告警测试未通过
2. 定义策略



1. 上传文件



在HV上能够看到我上传了文件C3.pptx，但问题是HV把这个行为与企业账户关联，而我在告警规则里写的非企业账户，但事实是我登录百度网盘的账号是cyberbird0212

1. 没有告警



无告警规则测试3的告警。

1. 问题分析

HF没有抓到我的百度网盘账号，是因为我登录百度网盘是通过cookie，没有login动作。从百度网盘主动注销后再登录，可以看到HF抓到我的账号：cyberbird0212。

1. 向百度云盘上传文件c3.pdf，没有告警
2. 在规则里定义一个具体的非企业账号：cyberbird0212



保存后，提交。出了2个问题：

1. 通过百度网盘上传C3.xls，没有告警。
2. 查看测试3告警规则，发现不显示添加的非企业账号：cyberbird0212，无法判断是什么问题导致没有告警。
3. 在原有规则上指定源网段地址：192.168 .0.0/16，通过百度网盘上传文件，仍然没有告警；

注释：

1. 上面两种情况，上传文件行为，HF侧是无法获取到百度云盘（客户端）用户登录名称(可通过客户端邮箱上传外网测试)。
2. 登录web端下载时无法获取当前账号信息
3. 把规则中的账号选项，改为任意账号，同时源IP网段不变，再次测试，告警出现：



告警有效：



* 1. 用户登录业务系统失败告警——未通过

1. 定义告警规则



1. 访问公司OA域名和IP地址，登录失败多次，均未触发告警。

注释：该功能未做 HF抓取不到内网应用登录失败日志。

* 1. 同一账号在多个设备上登录告警

1. 企业内部账号登录外网系统（公司邮件）通过

问题：我的两个设备（笔记本和手机）登录公司邮件服务器会触发告警，并且这个告警没有bypass机制。注释：bypass需求需要确认，V4.0暂无实现。

1. 非企业账号登录外部系统（百度网盘）——未通过

我的两个设备用百度网盘账号登录百度网盘，HV可以看到不同设备登录行为，但是没有触发报警。

注释：当前测试场景只支持本企业账号，非企业账号无法触发。

1. 企业账号登录企业内部系统（OA）——未通过

我使用两个设备（Macbook，ThinkPad）使用OA账号liuning登录192.168.157.135 OA系统，HV可以看到ThinkPad登录OA行为，但是没有触发告警。

注释：同一账户在多设备登录行为中的账户信息是针对企业账号情况，而OA系统的账号为非企业账号，无法触发告警。

* 1. 规则报警的逻辑优化

1. 同一账号在多个设备上登录：

* HV已经把我的Macbook，手机，Thinkpad关联在我的帐号下，我在这三个设备上访问邮件系统，会触发报警，这个逻辑是否可以优化：
  + 属于一个用户的多个设备，使用该用户账号访问系统，不触发告警；

注释：这种情况还是bypass需求，如果规则配置的告警次数为1的话，当前并未对告警事件进行报警次数限制，即每次都报警。

1. 规则告警有个处理状态（待处理，处理中，已处理）的功能不完善，不能只是显示一个状态，至少要有以下功能：
2. 有过滤和分类显示：过滤已处理日志；把待处理和处理中日志分开显示
3. 日志的处理机制：白名单/例外（可以忽略的事件不再出发告警）

注释：需求已记录，后续讨论