幻阵-高级威胁检测系统

用户手册（超级管理员）

杭州默安科技有限公司

浙江省杭州市余杭区余杭塘路 2616 号正勤·美培创意园 3 号楼

0571-5789 0068

www.moresec.cn

默安科技

企业信赖的安全伙伴

文档说明文档说明

文档负责人	秦梓豪	文档版本编号	V3.0.0
起草人	秦梓豪	文档起草日期	2022.4.29
复审人	王哲	复审日期	

版本控制

版本号	版本日期	创建/修订人	说明
V2.10.0	2021-6-10	陈诗梦	创建
V2.10.1	2021-9-30	崔芙蓉	更新
V2.11.0	2022-1-14	黄澜	更新
V3.0.0	**2022-4-29**	**秦梓豪**	**更新**
V3.1.0	2022-8-19	秦梓豪	**更新**
V3.2.0	**2022-11-9**	**秦梓豪**	**更新**
V3.2.1	**2022-12**	**秦梓豪**	**更新**
V3.2.2	**2023-01**	**秦梓豪**	**更新**

版本申明

目录

一、 概述

1.1 产品概述

默安幻阵是默安科技首创的一款基于攻击混淆与欺骗技术的威胁情报产品。通过在黑客必经之路上构造陷阱，混淆其攻击目标，精确感知黑客攻击的行为。可阻断和隔离攻击，并溯源黑客身份及攻击意图，形成黑客攻击情报。该产品可用于保护易受黑客入侵攻击的业务系统，特别在金融、证券、运营商等包含大量用户数据、资金等敏感信息的业务环境中。通过构建用户威胁情报体系，实现从安全事件的被动响应到安全威胁的积极应对，帮助企业控制安全风险。

1.2 公司简介

杭州默安科技有限公司是由来自 BAT 等知名互联网安全团队资深专家及业内精英组建成立的一家安全公司，致力于用创新技术解决企业安全问题的高新企业。将威胁情报技术和人工智能技术融入企业真实安全防御体系，提供企业在云计算和 IOT 时代的安全整体解决方案。默安科技将不断创新、积极探索，用专业服务成为企业信赖的安全伙伴。

二、 系统维护

2.1 账号维护

超级管理员密码如果忘记，请联系默安科技，安排工程师重置密码。

2.2 重新启动系统

如果遇到需要重启系统的情况应注意:在重启设备前停用所有已经启动沙箱,重启之后,重新启动沙箱即可。

三、 Web 管理界面

3.1 登录界面

默安幻阵云端 Web 管理界面的登录方法:

1) 确保设备已被正确配置。

2) 打开浏览器 Google Chrome（支持以下浏览器: Google Chrome、firefox、IE11、

360 浏览器、Edge、搜狗浏览器），用 HTTPS 方式连接默安幻阵的 IP 地址，如：https://192.168.100.80

3） 回车后进入如下图所示的登录页面，输入正确的用户名、密码和验证码。

4） 子账户可选择认证登录方式，包括 radius 认证和 ldap 认证

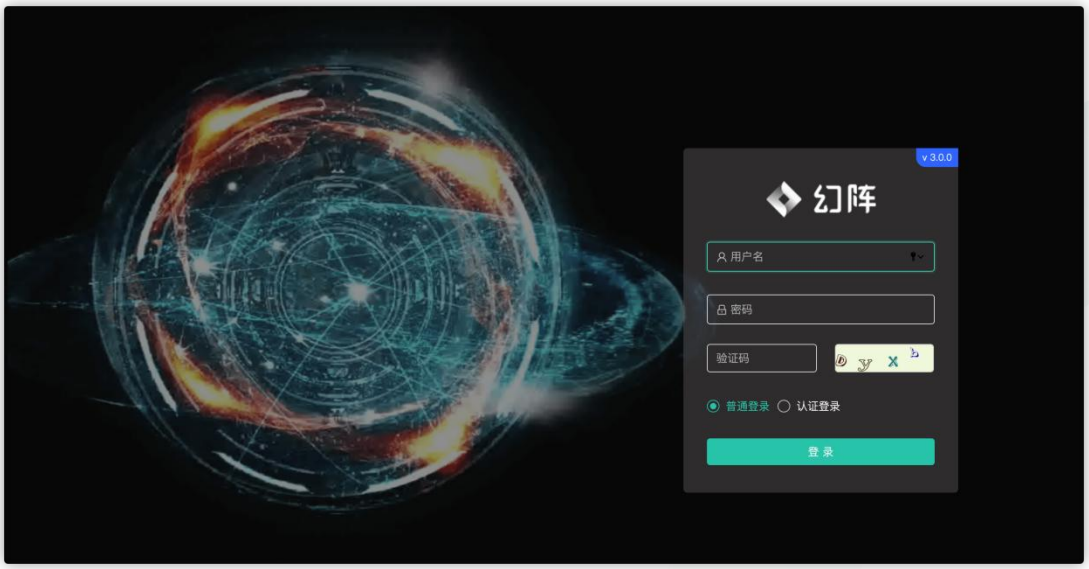


图 3-1-1 默安幻阵云端 Web 管理登录界面

当用户未在规定时间修改密码时，系统会弹出强制修改密码弹窗，如下图所示，修改密码后便可重新登陆。

图 3-1-2 密码过期强制修改密码弹窗

3.2 风险大盘

风险大盘主要记录目前用户环境所面临的威胁情况。具体包括攻击事件和入侵事件趋势，受攻击目标 top5，受攻击沙箱 top5，事件威胁统计。

3.2.1 数据统计

图 3-2-1 默安幻阵云端 Web 风险大盘界面

如上图上方前四个展示框，分为资产防护、探测事件、入侵事件、威胁人员四项，其中资产防护即为当前的伪装代理数量，探测事件、入侵事件、威胁人员即为前用户环境某一段指定时间内（默认是最近 7 天）的数据统计。

威胁风险量化值是默安幻阵基于当前发现攻击事件行为和威胁人员数目以及时间和威胁程度量化出来的一个分值，分值越高，表示系统的风险越高。企业威胁级别分为低危、中危、高危、重度高危和 APT 攻击五个级别，分值小于等于 20 企业威胁级别为低危，分值 20--50 企业威胁级别为中危，分值 50--80 企业威胁级别为高危，分值 80--90 企业威胁级别为重度高危，分值大于 90 企业威胁级别为 APT 攻击。

3.2.2 受攻击 IP

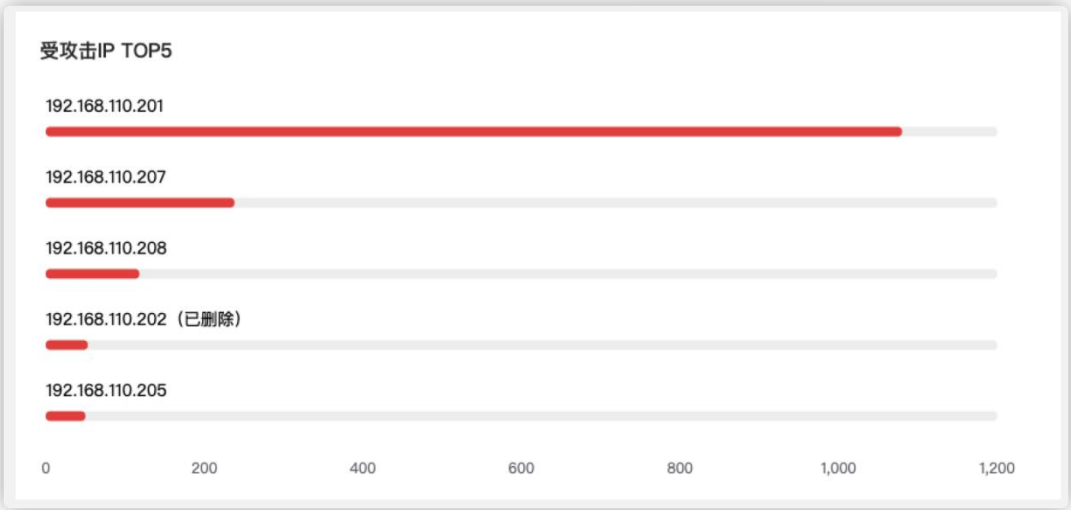


图 3-2-2 默安幻阵云端 Web 风险大盘受攻击 IP top5 界面

如上图所示， 受到攻击状态图以横向柱状图显示。分别取受到攻击最多的五个资产作为展示。

3.2.3 攻击和探测事件趋势

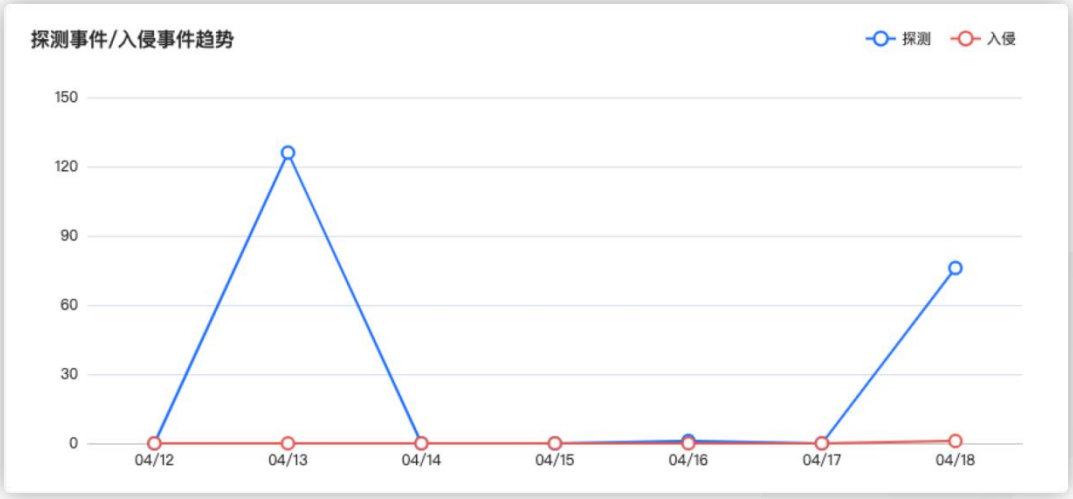


图 3-2-3 默安幻阵云端 Web 风险大盘探测/入侵趋势界面

如是上图所示，系统记录了目前用户环境某一段指定时间内（默认是最近 7 天）的数据统计探测和入侵事件数，并根据用户选择时间分析出用户环境在这段时间内所遭受的攻击事件趋势。

3.2.4 受攻击沙箱 top5 和事件威胁等级分布

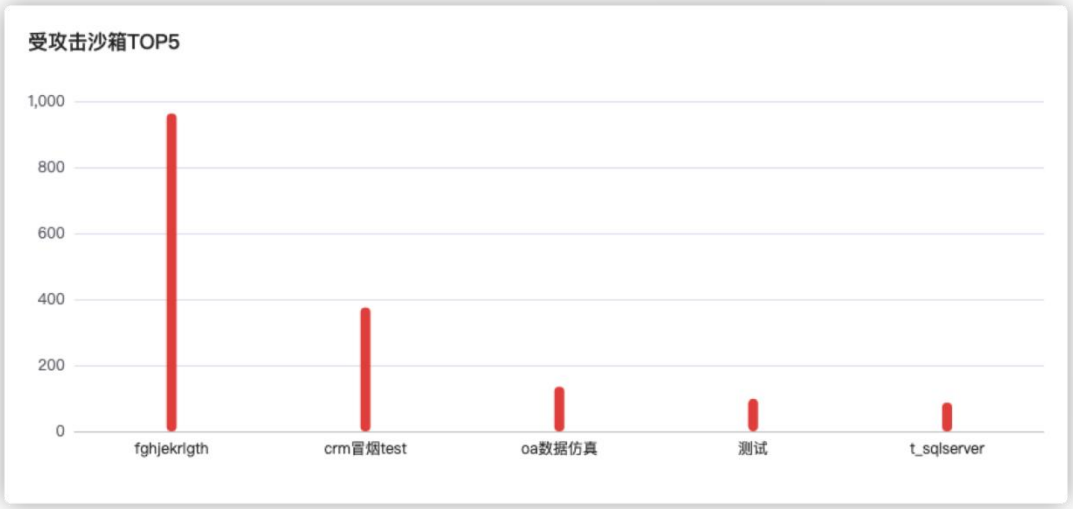


图 3-2-4 受攻击沙箱 top5 和事件威胁等级分布

3.3 安全大屏

安全大屏是实时显示目前用户环境的威胁情况。主要显示当前状态：动态显示当前网络拓扑图和受攻击实时动态展示，如图：

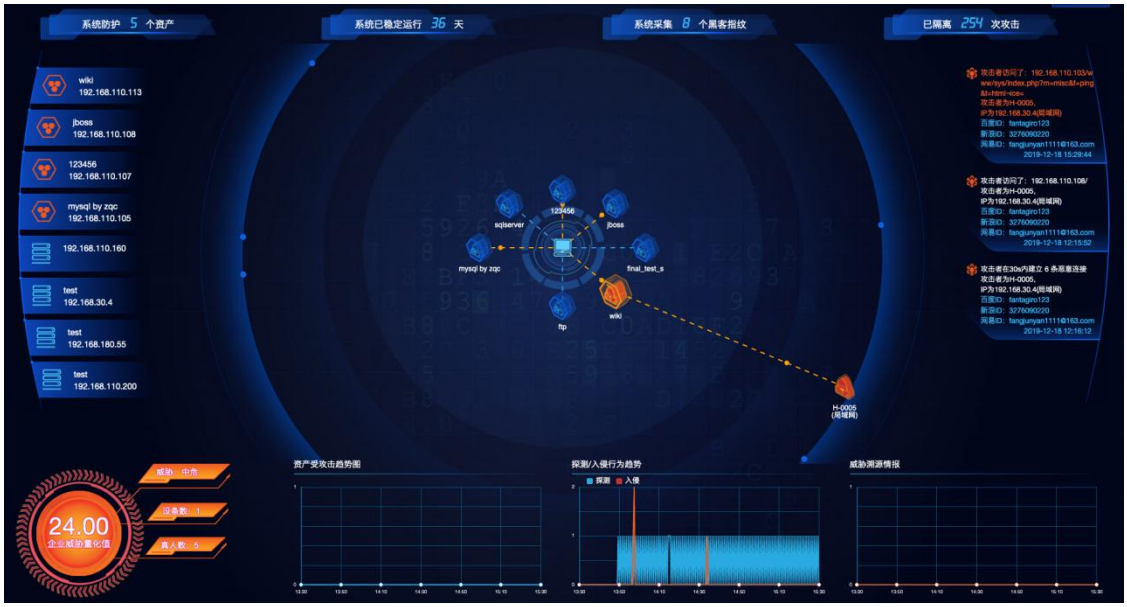


图 3-3-1 默安幻阵云端 Web 安全大屏页面

3.4 威胁情报管理

3.4.1 黑客溯源

黑客溯源页面主要统计攻击过目前用户环境的攻击者，以图表形式显示攻击者名称、攻击源 IP、内网 IP、公网 IP、物理地址、开始攻击时间-最近攻击时间、攻击次数，可对攻击者添加白名单，当攻击为扫描器时将会显示出扫描器类型，现能获取的扫描器类型有：AWVS、Netsparker、WebInspect、NSFOCUS RSAS、Nessus、WebReaver、Sqlmap。如图：

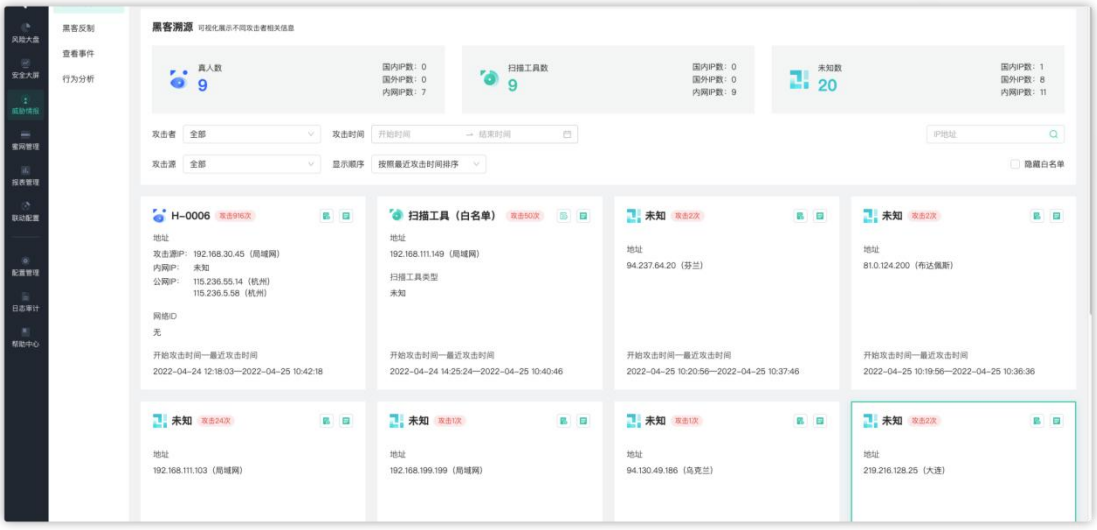


图 3-4-1 黑客溯源

点击查看详情图标‘ ’，会跳转到黑客画像分析界面，里面会以图表和列表两种方式显示攻击者的详细信息，包括攻击了哪些资产以及被隔离到哪个沙箱等信息，点击生成报告可单独生成该攻击者的攻击报告。

情报联动模块会根据攻击者的设备指纹信息进行碰撞，如果有相匹配的指纹信息，将会从情报中心同步相关数据，以达到丰富黑客画像目的。

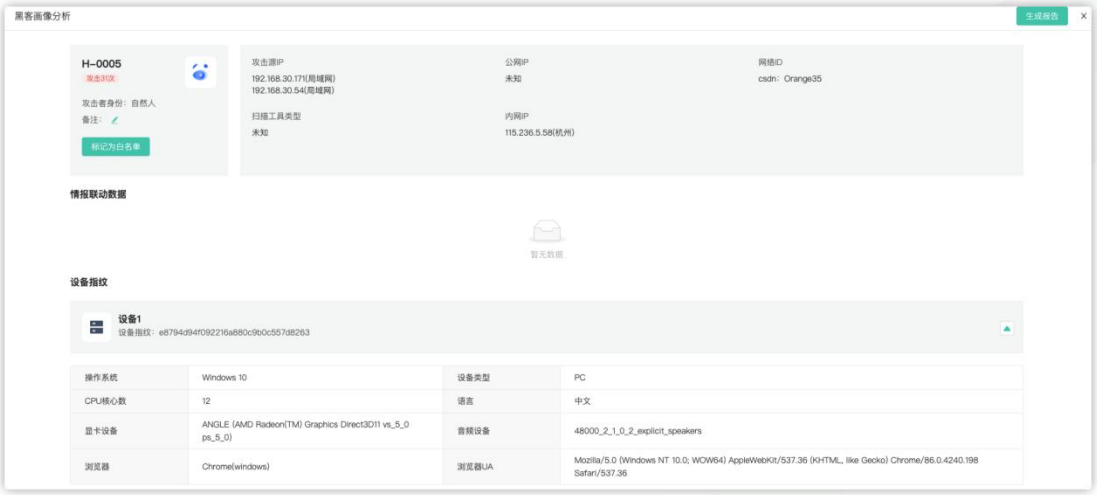


图 3-4-2 黑客画像分析

同时黑客画像分析页面还可自动归并攻击者的攻击链，展示攻击者的攻击路径，反向探测攻击源所开放的端口和服务。

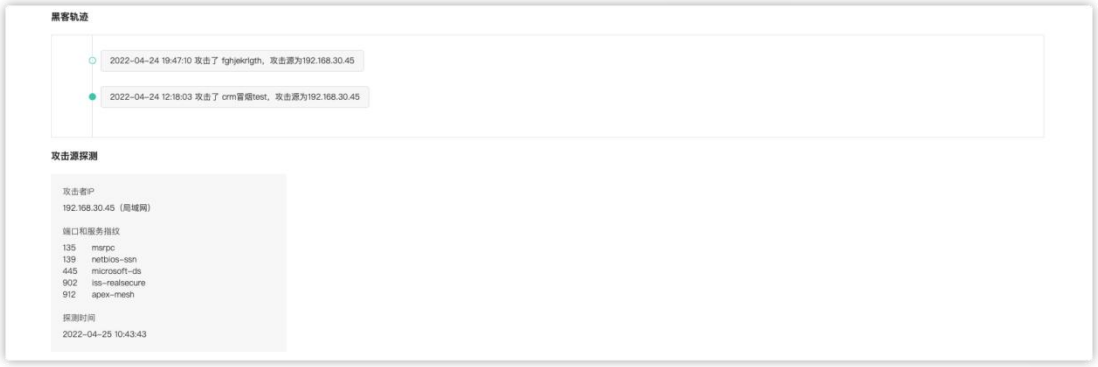


图 3-4-3 黑客画像攻击路径

黑客反制页面主要显示反制的攻击者，在页面上会具体的显示出反制类型，攻击者 IP，在线状态，初次上线时间以及最近上线时间。可根据在线状态、IP 位置、最近上线时间等进行精确搜索，攻击反制如下图所示：

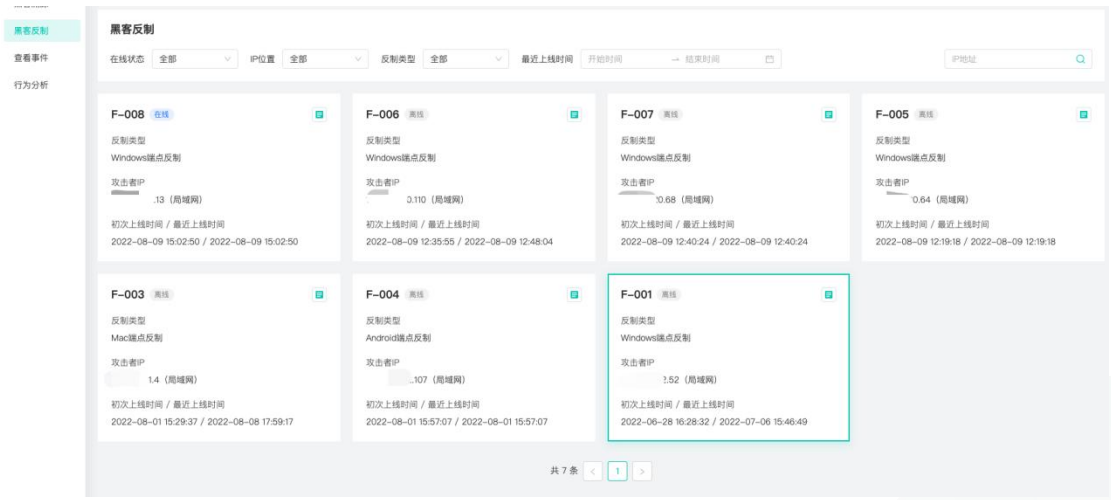


图 3-4-4 攻击反制

点击 进入 Windows 反制详情页面，可以看到具体的反制信息，包括反制对象、设备精确信息，以及高级反制。攻击反制中木马可以抓取 wechat, qq, cs, navicat, xshell 连接信息，支持将数据以列表的形式下载。如下图所示。

图 3-4-5 攻击反制

反制对象包括反制的类型（当被反制者状态为离线时，高级反制仅可进行历史命令的查询），反制 IP 以及与所关联的攻击者。

设备精确信息包括基本信息、网卡信息、IP 信息、用户信息、进程信息、系统信息以及桌面文件。

基本信息包括操作系统的类型、设备类型、主板序列号、硬盘序列号、cpu 类型、BLOS、GPU 类型、IDE、显示器、声卡、内存条、硬盘、主机品牌、物理机接口、当前路径以及当前用户，如下图所示。

图 3-4-6 基本信息

网卡信息包括组策略配置文件、接口 WLAN 上的配置文件等信息，如下图所示。

图 3-4-7 网卡信息

IP 信息包括用户的网络配置信息，例如 Windows 配置、vlan、以太网配置等信息，如下图所示。

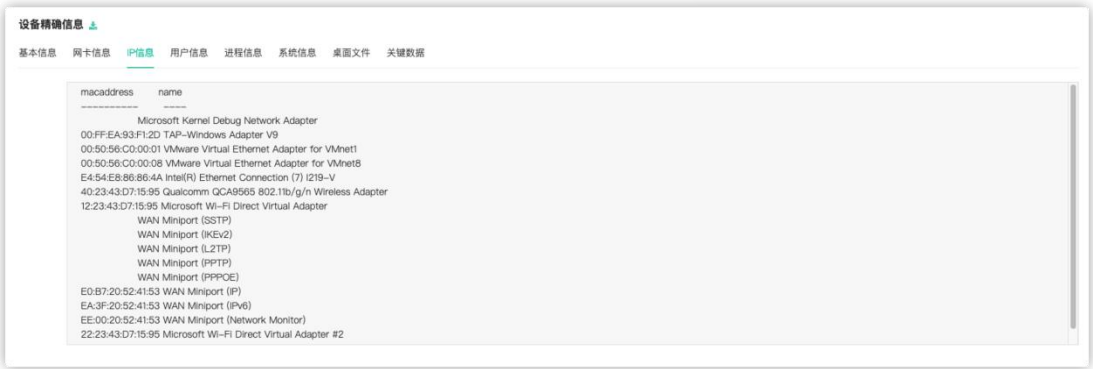


图 3-4-8 IP 信息

用户信息包括用户的账户信息等内容，如下图所示。

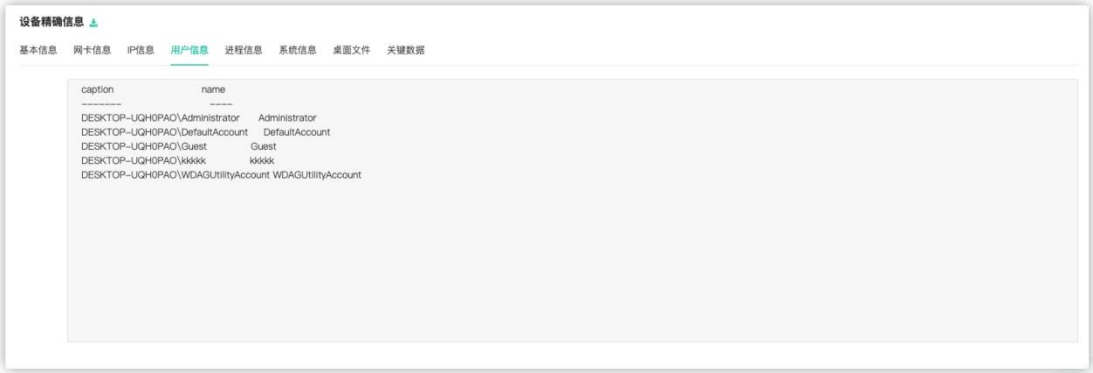


图 3-4-9 用户信息

进程信息包括映像名称、PID 会话名、内存使用情况等。如下图所示。

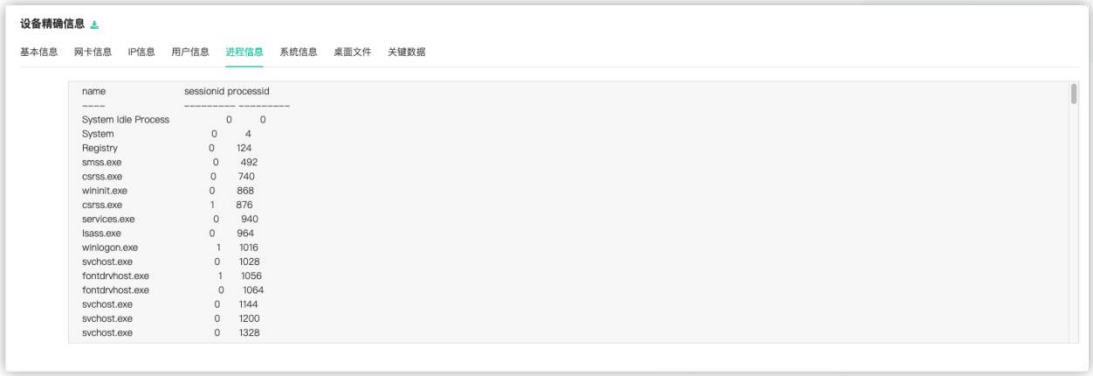


图 3-4-10 进程信息

系统信息包括攻击者系统的一些信息，例如主机名，os 名，os 版本等信息，如下图所示。

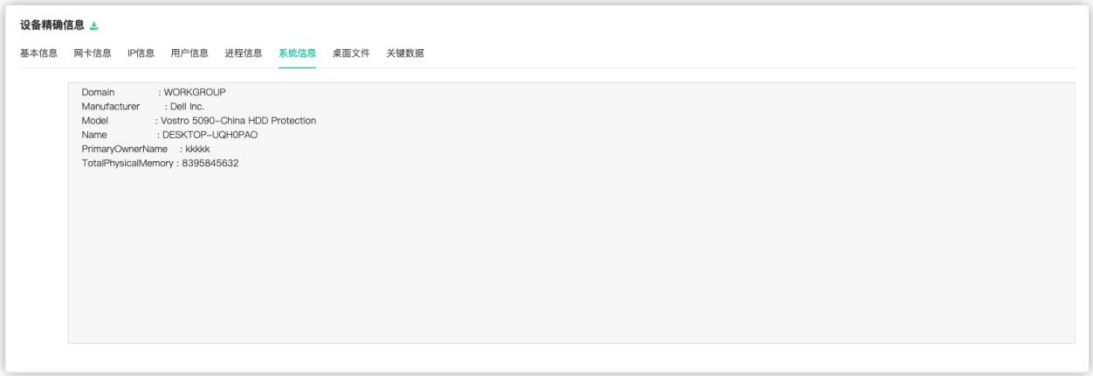


图 3-4-11 系统信息

桌面文件为攻击者的桌面信息，如下图所示。

图 3-4-12 桌面文件

关键数据，展示手机号、iPhone（IMEI、MEID、序列号）、Git、Email、域名|用户名等信息，如下图所示。

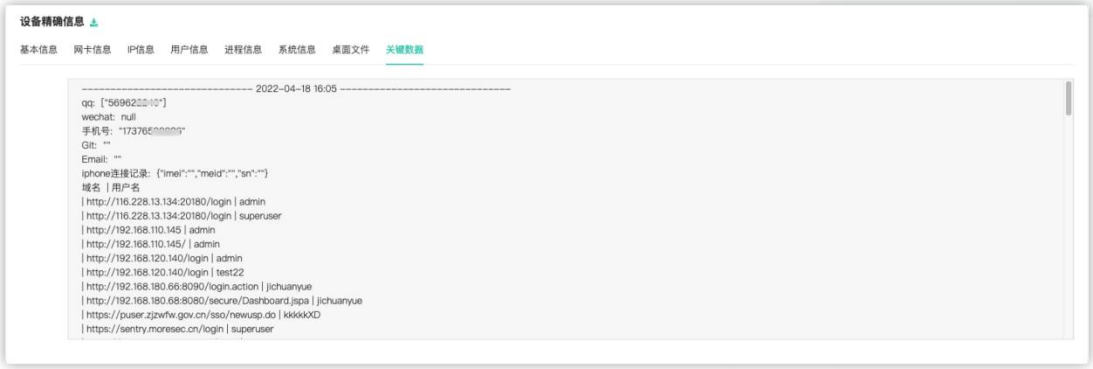


图 3-4-13

高级反制，当攻击者在线时（攻击者离线时除历史命令查询保存，其余均隐藏），幻阵可对其进行一系列的操作，包括交互 shell、文件上传、文件下载、电脑截屏、历史命令查询，如下图所示。

图 3-4-14 高级反制

交互式 shell，幻阵使用者可以在攻击者电脑上进行一些操作，且攻击者电脑不会显示出来，如下图所示。

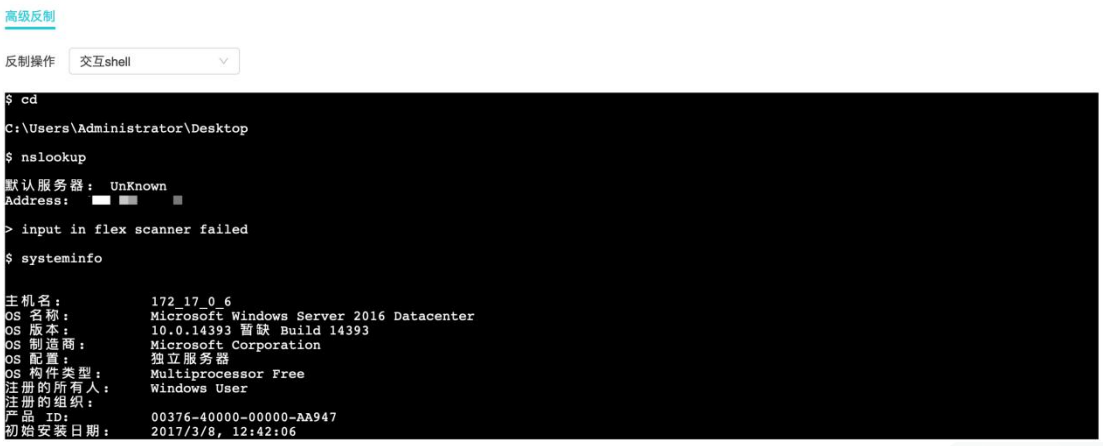


图 3-4-15 交互式 shell

文件上传，使用者指定上传到攻击者电脑的地址以及文件，点击上传显示上传成功即可，此时攻击者电脑对应的地址便会有幻阵使用者上传的文件，如下图所示。

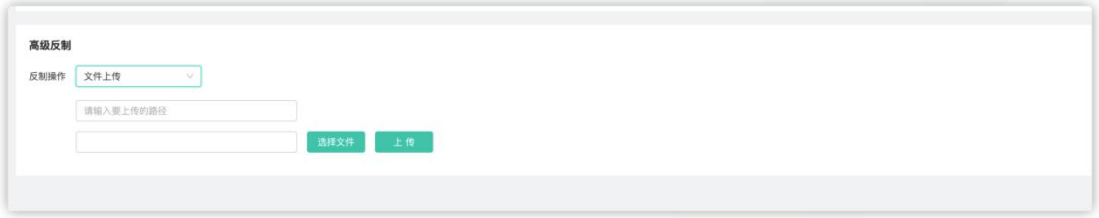


图 3-4-16 文件上传

文件下载，幻阵使用者指定下载的内容在攻击者电脑上的地址，点击下载即可下载即可。如下图所示。

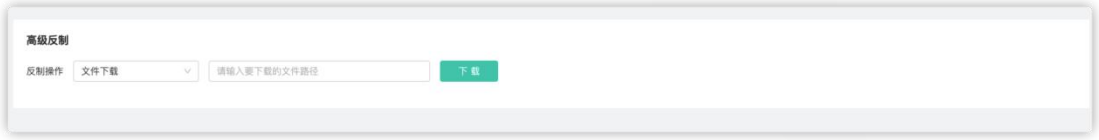


图 3-4-17 文件下载

电脑截屏，点击执行即可截取攻击者电脑当前的图片，如下图所示。

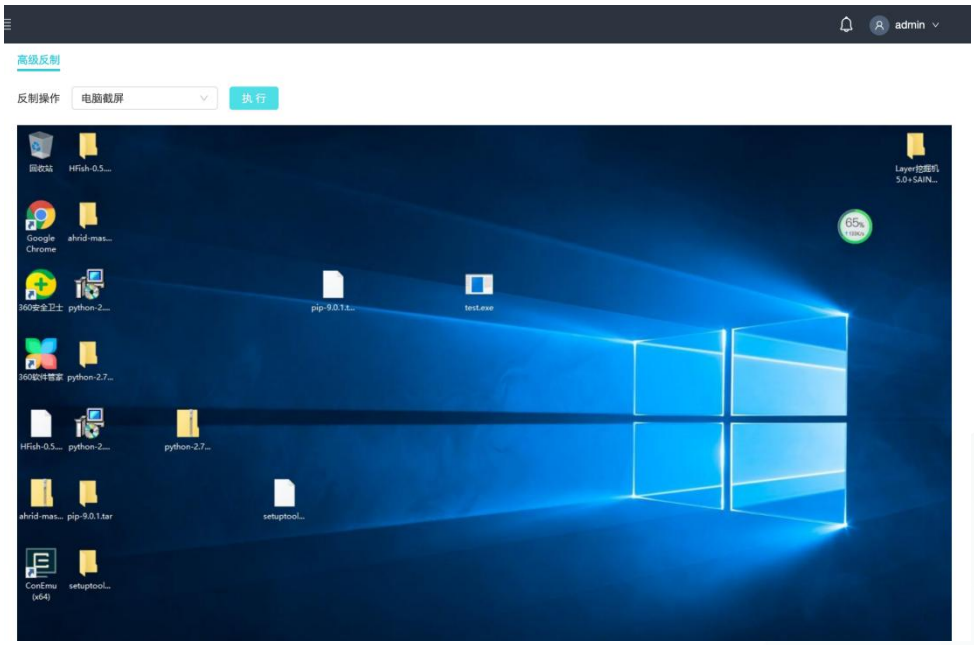
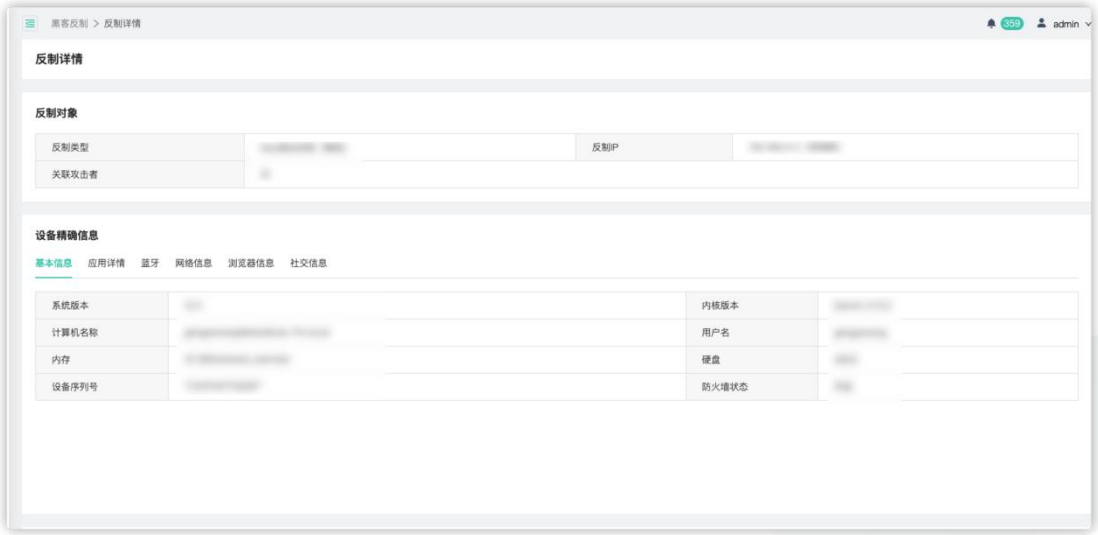


图 3-4-18 电脑截屏

历史命令查询可以看到在攻击者电脑上执行的命令，该内容在攻击者上线和离线状态下均存在，如下图所示。

图 3-4-19 历史命令查询

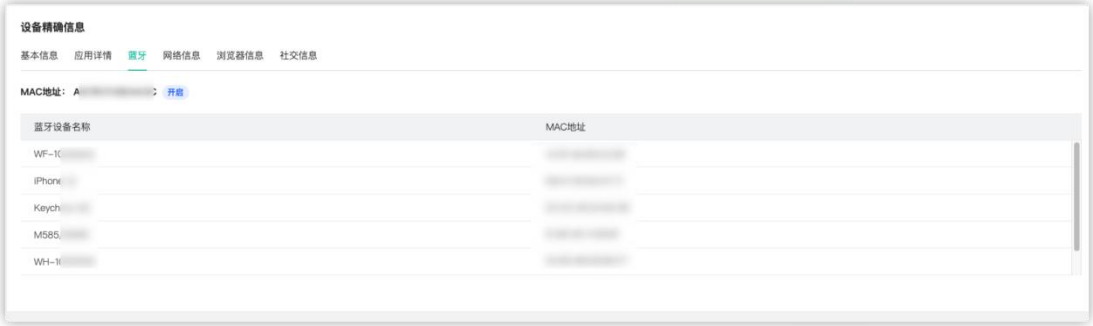
Mac 反制详情：点击 进入 Mac 反制详情页面，可以看到具体的反制信息，包括反制对象、设别精确信息，以及高级反制，如下图所示：



设备精确信息包括基本信息、应用详情、蓝牙、网络信息、浏览器信息、以及社交信息；基本信息包括系统版本、内核版本、计算机名称、用户名、内存、硬盘、设备序列号、防火墙状态等；

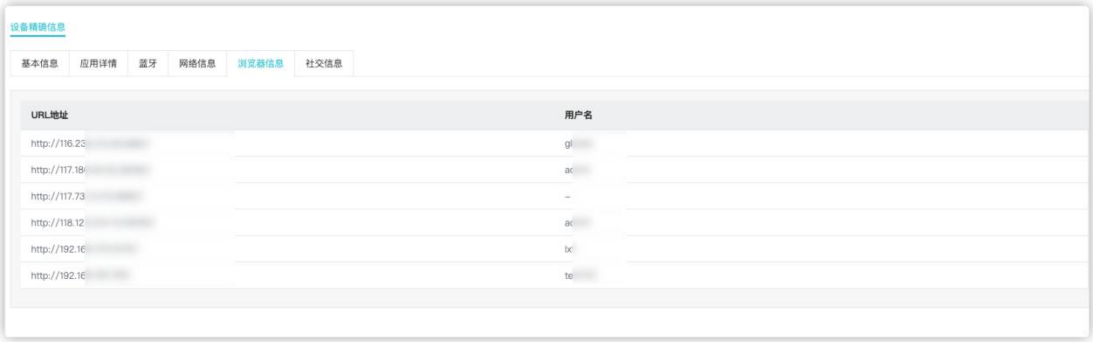
应用详情包括应用名称、应用版本、最后一次使用时间

蓝牙包括 mac 地址、启用状态、蓝牙设备名称、Mac 地址等



网络信息包括 wifi Mac 地址、当前网络信息、剩余网络信息等

浏览器信息包括浏览器 URL 和用户名



社交信息包括微信账号、手机号、邮箱；钉钉手机号、邮箱

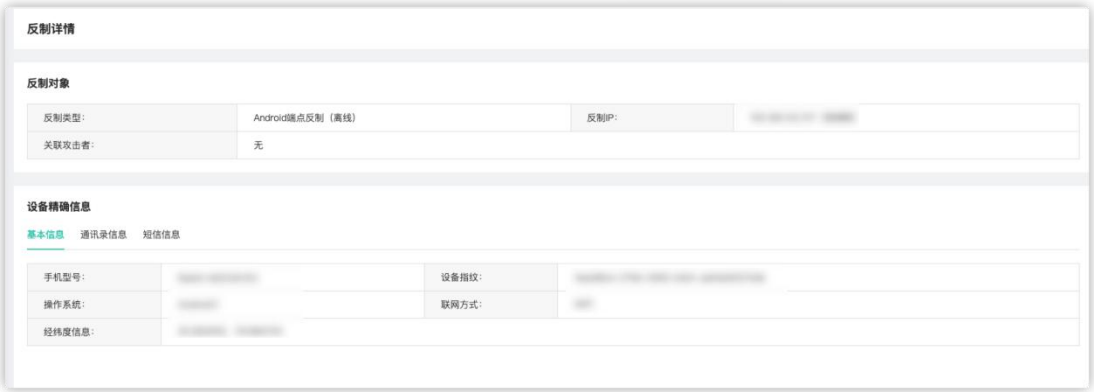
当攻击者在线时（攻击者离线时除历史命令查询保存，其余均隐藏），幻阵可对其进行一系列的操作，包括命令执行、文件上传、文件下载、历史命令查询

命令执行，幻阵使用者可以在攻击者电脑上进行一些操作，且攻击者电脑不会显示出来，如下图所示。

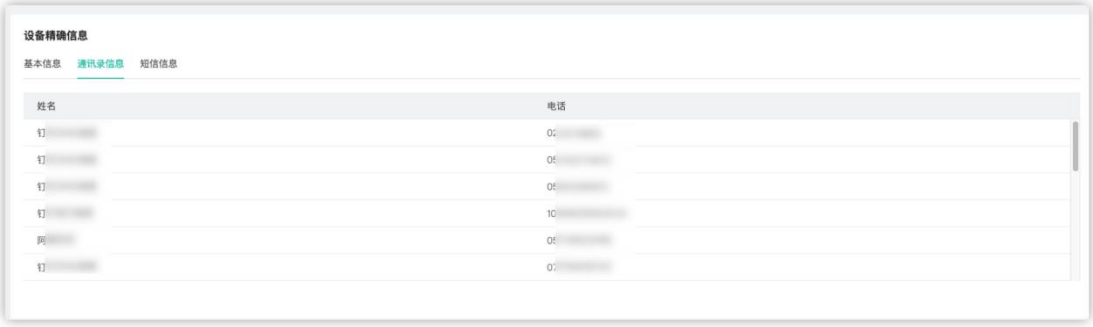
文件上传，使用者指定上传到攻击者电脑的地址以及文件，点击上传显示上传成功即可，此时攻击者电脑对应的地址便会有幻阵使用者上传的文件，如下图所示。

文件下载，幻阵使用者指定下载的内容在攻击者电脑上的地址，点击下载即可下载即可。如下图所示。

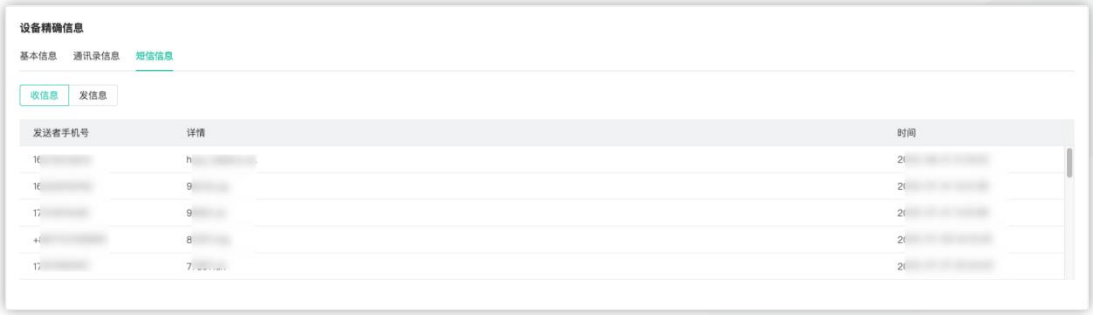
Android 反制详情：点击 进入 Android 反制详情页面，可以看到具体的反制信息，包括反制对象、设别精确信息，以及高级反制，如下图所示：



设备精确信息包括基本信息、通讯录信息、短信信息等；
其中基本信息包括手机型号、设备指纹、操作系统、联网方式、经纬度信息等
通讯录信息包括姓名和电话



短信信息包括收发短信的手机号、详情和时间



当攻击者在线时（攻击者离线时除历史命令查询保存，其余均隐藏），幻阵可对其进行一系列的操作，包括命令执行、文件上传、文件下载、历史命令查询

命令执行，幻阵使用者可以在攻击者电脑上进行一些操作，且攻击者电脑不会显示出来，如下图所示。

文件上传，使用者指定上传到攻击者电脑的地址以及文件，点击上传显示上传成功即可，此时攻击者电脑对应的地址便会有幻阵使用者上传的文件，如下图所示。

文件下载，幻阵使用者指定下载的内容在攻击者电脑上的地址，点击下载即可下载即可。如下图所示。

3.4.2 查看事件

查看事件列表详细记录威胁事件攻击者、攻击源、攻击目标、开始攻击时间、最后攻击时间和事件的风险等级。同时记录攻击者的详细操作步骤，对 SSH，RDP 操作记录进行视频展示，对攻击者上传文件进行下载可分析，逃逸检测功能，当发生逃逸时也会在事件列表进行记录，并且支持隔离沙箱对高管邮件、机密文件、疑似逃逸、高敏沙箱的筛选。默安幻阵采用先进的指纹智能识别技术，能有效区分攻击者身份，用户可主动添加 IP 到白名单中，避免扫描器产生的大量告警。如下图事件列表所示。

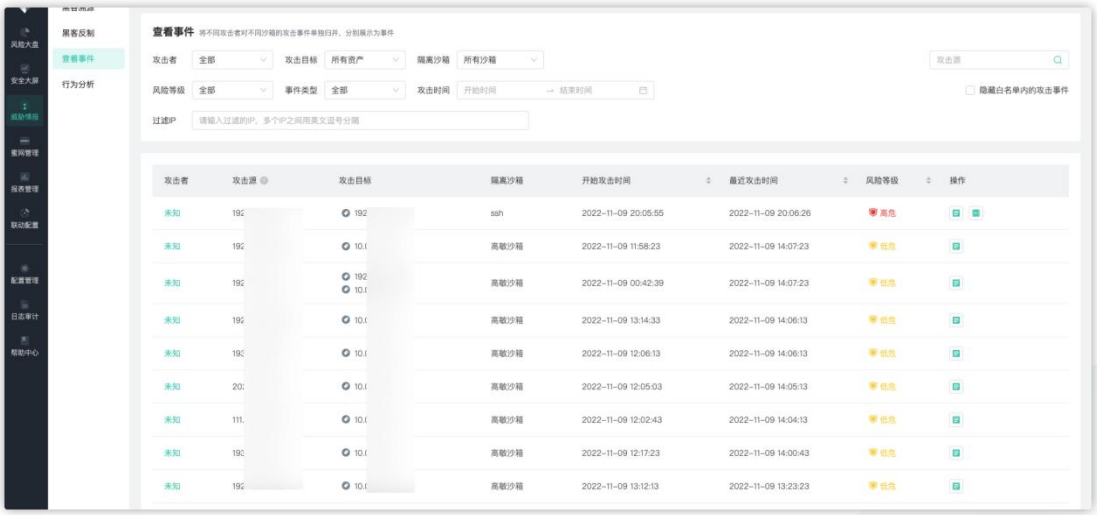


图 3-4-20 事件列表

事件列表的攻击目标筛选框和攻击目标列表中，均会展示中继节点标签以及伪装代理的 IP 标签，如下图所示。

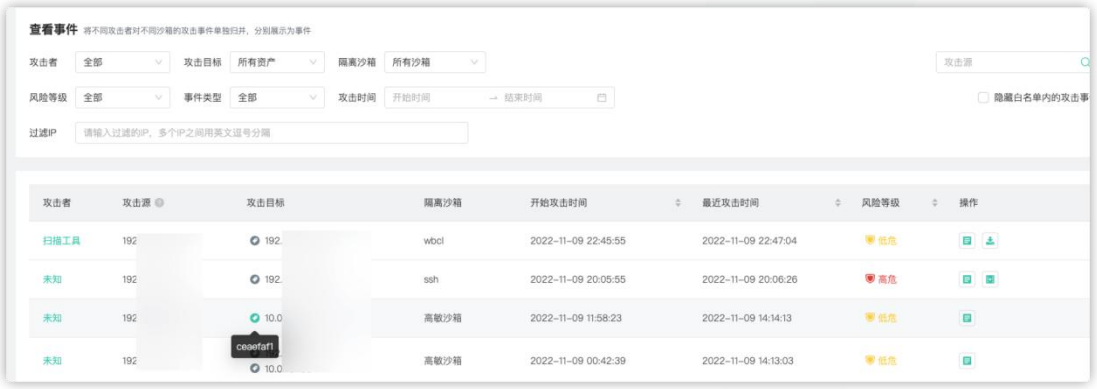


图 3-4-21 事件列表

事件列表有事件回放按钮、恶意文件分析按钮以及入侵视频回放按钮。点击事件回放按钮，如下图攻击事件回放，可看到攻击者的基本信息以及攻击者的入侵记录，以及攻击者的 mac 地址以及对扫描器的识别。同时支持对攻击手法进行筛选，通过时间轴的方式展示重点攻击手法及事件。

图 3-4-22 攻击事件回放

在事件回放显示页面中点击攻击者的网络 ID，会跳转至黑客画像分析页面。如下图内容所示，用户可查看攻击者的详细身份信息，包括攻击源 IP、攻击者真实 IP、内网 IP、公网 IP、网络 ID（包括 163、新浪、百度等）、设备指纹、使用的操作系统、浏览器。如果配置了联动配置-威胁情报中心联动相应内容，对于匹配到相同设备指纹的真人，会在情报联动数据模块显示相应信息。进一步丰富黑客画像内容。

图 3-4-23 黑客画像分析

点击恶意文件分析按钮“ ”即可跳转到攻击文件分析页面，详细的展示了攻击上传的文件名称、文件类型、文件 md5、virustotal 鉴定、AntlVirus 鉴定，并且可以对恶意文件进行下载，如下图上传文件分析所示。

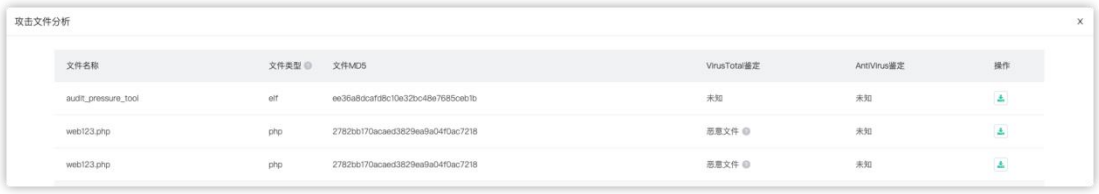


图 3-4-24 恶意文件分析

入侵视频支持 ssh 攻击事件回放和 rdp 攻击事件回放，点击‘ ’即可弹出入侵视频回放界面，展示出了视频名称、开始事件、视频大小以及操作，以 rdp 为例，如下图 RDP 入侵视频回放所示。

图 3-4-25 RDP 入侵视频回放

点击‘ ’即可播放入侵视频，如下图 rdp 入侵视频回放

图 3-4-26 rdp 入侵视频回放

3.4.3 行为分析

该页面按照时间轴排序展示所有被监控沙箱的详细攻击行为记录，可根据攻击者、攻击源、攻击目标、隔离沙箱、攻击时间、攻击类型、攻击者手法等信息更加快速定位攻击者；

在攻击行为处增加对扫描工具的判别展示和对进程逃逸的展示。同时支持对伪装代理、中继节点的半开连接、UDP 扫描等事件的记录（此功能需要打开半连接感知开关）。集成了内部编码转义功能，用户可以直接在页面内贴入需要转换的 URL，点击转义输出转义结果。同时引入了 ATT&CK 能力，支持用户通过 ATT&CK 进行筛选。上述功能如下图所示：

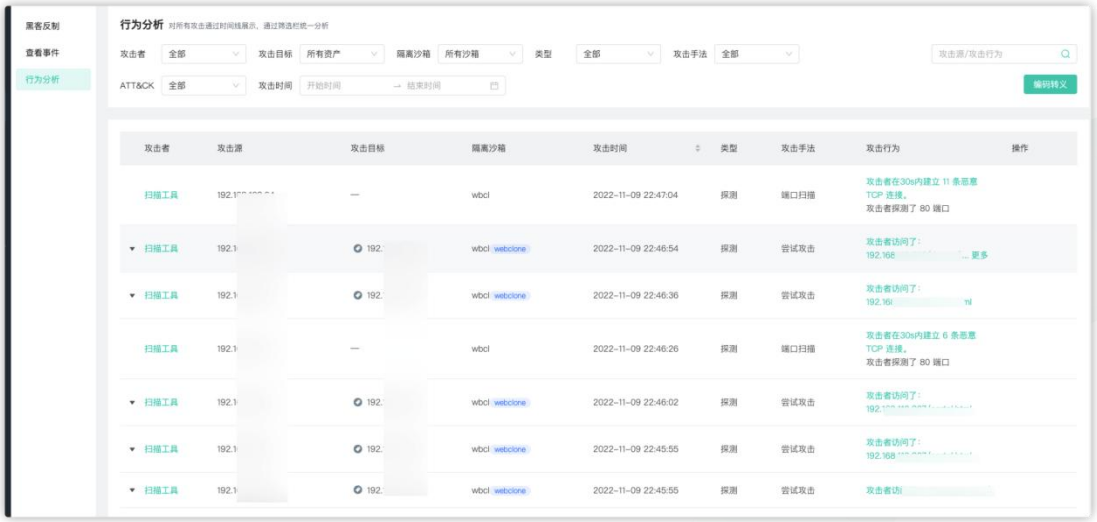


图 3-4-27 行为分析

在页面中可点击攻击者跳转至黑客画像分析页面，查看该攻击者详细信息；点击单条攻击手法可跳转至攻击事件回放页面，显示该条记录关联的完整事件。

3.5 蜜网管理

3.5.1 蜜网导图

默安幻阵支持集群管理，一个云端管理多台客户端。幻阵智能蜜网系统，通过一键检测企业内现有服务，加以安全算法编排，将中继节点、伪装代理迅速关联沙箱，同时实现自适应业务场景。在节省人力部署成本的前提下，以安全人员的视角迅速张开蜜网，真正实现快速、自动化智能部署。（如下图 3-5-1-1 所示）

基于探测及扫描结果，密网导图将显示幻阵设备、中继节点设备、沙箱信息，并围绕相关内容，展开显示伪装代理 IP、中继节点 IP 等绑定沙箱的情况，同时也将显示探测的客户资产 IP、未存活 IP 的相关内容。

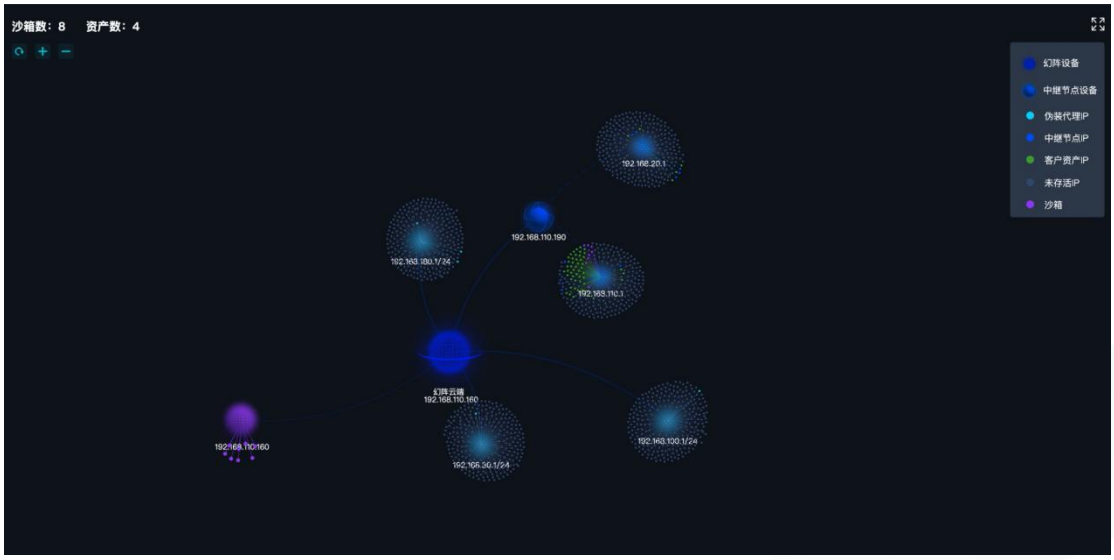


图 3-5-1-1 蜜网导图

3.5.2 智能蜜网

智能蜜网是在贴合现有业务场景的前提下，将欺骗能力赋予各个业务单元。通过智能自动化的方式快速部署形成欺骗密网。

用户可以勾选一键探测模块下的中继节点或者伪装代理发起探测，发起探测过程中，将会对不同 vlan 或子网信息进行扫描。并以图形化的方式统计相应的端口分布情况、系统分布情况信息。探测完成后需要用户手动刷新页面，查看最新页面信息。如图 3-5-2-1 所示。

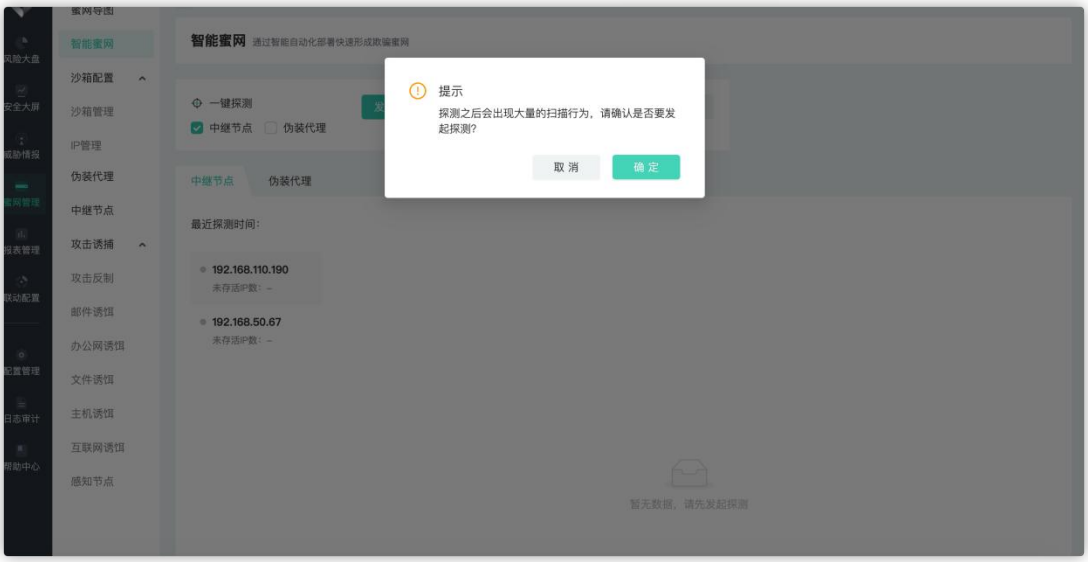


图 3-5-2-1 蜜网导图

对于中继节点模块，对于扫描到的未存活 IP，用户可以进行选择，并将其添加至 IP 管

理中。如图 3-5-2-2 所示。成功添加后，可以在中继节点-IP 管理页面查看所添加的 IP。

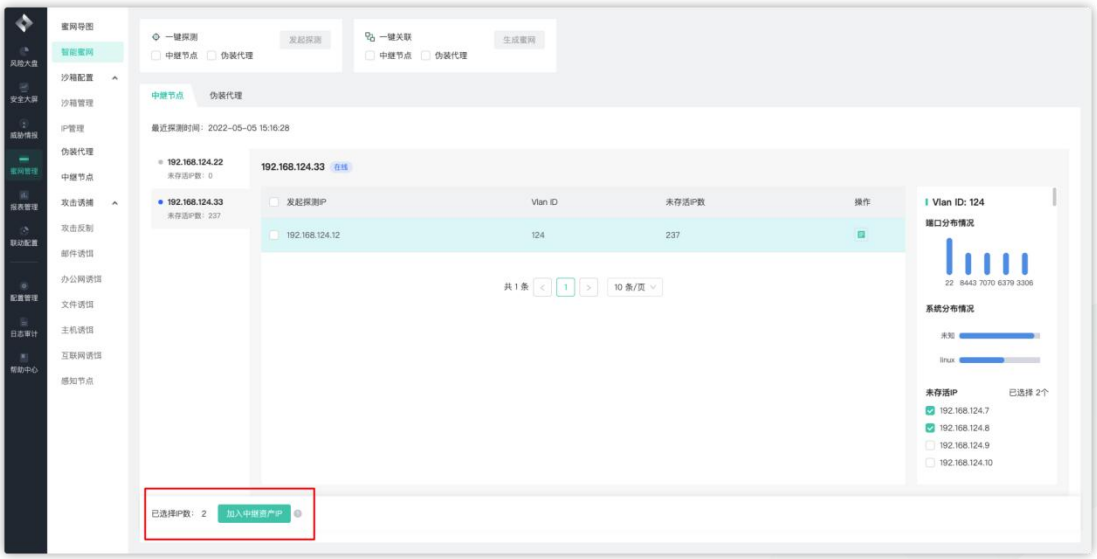


图 3-5-2-2 中继节点添加未存活 IP

中继节点模块可以查看不同 VLANID 下自动关联沙箱的情况。点击“ ”图标，即可带 VLANID、关联方式的方法跳转到中继节点-节点详情-IP 管理界面。

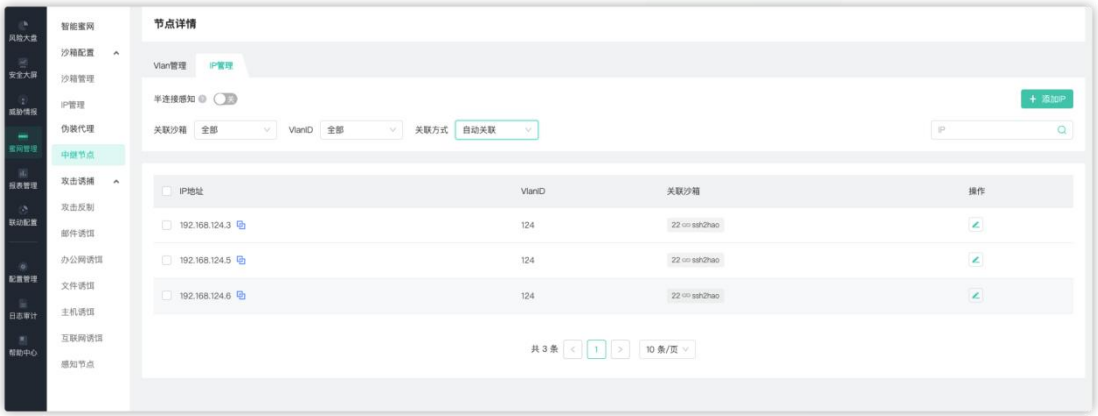


图 3-5-2-3 中继节点带筛选跳转

伪装代理模块，针对子网信息进行扫描，点击查看详情按钮，可以带关联方式筛选跳转至伪装代理-IP 管理模块。

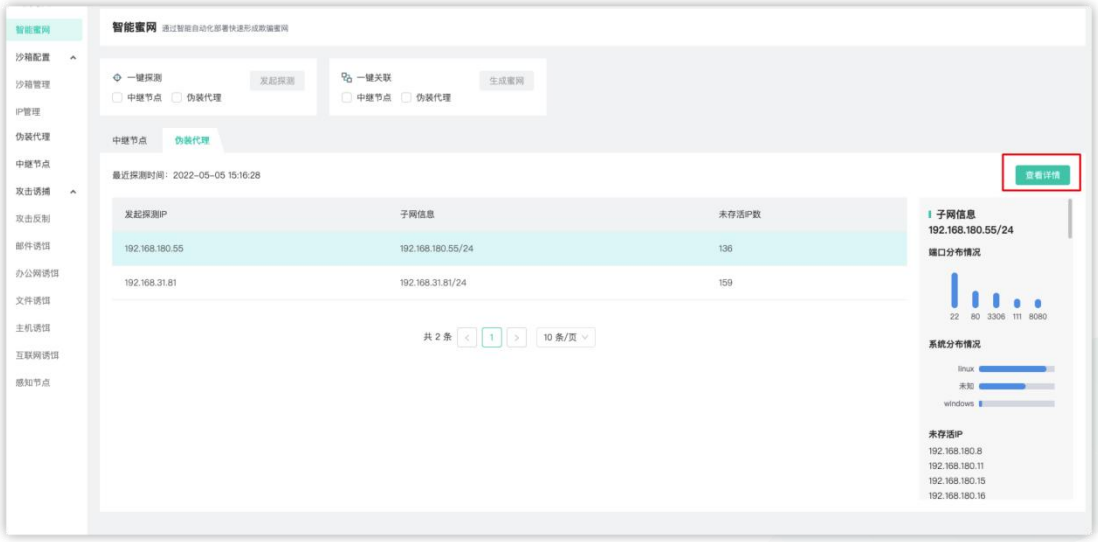


图 3-5-2-4 伪装代理带筛选跳转

探测并完成绑定沙箱之后（伪装代理及中继节点绑定沙箱方式可查看伪装代理、中继节点模块说明），用户可以点击智能蜜网页面顶部——一键关联模块，选择中继节点或伪装代理，生成密网，即可将最新的关联信息更新至密网导图页面。如图 3-5-2-5 所示。

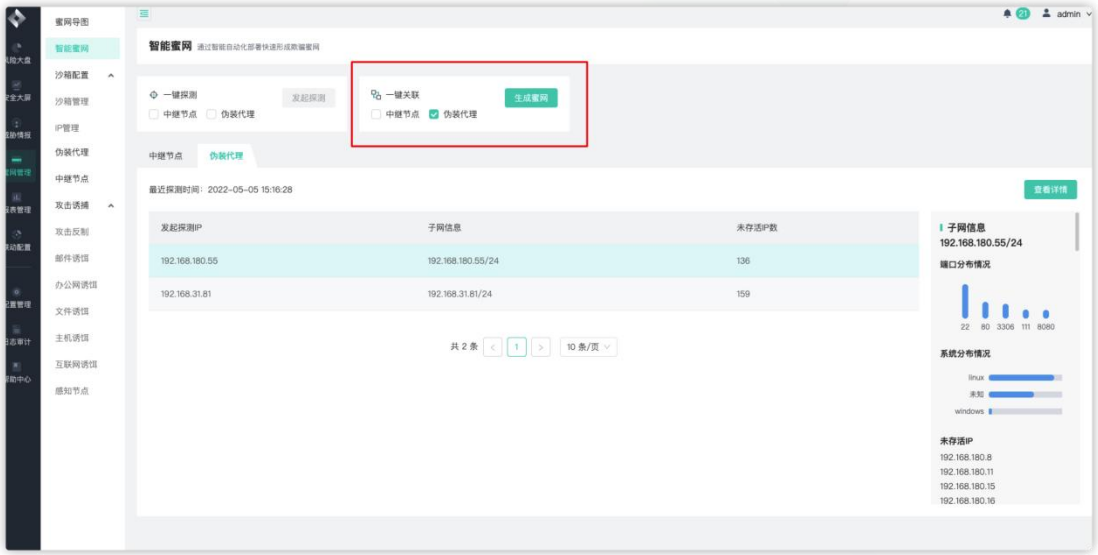


图 3-5-2-5 一键关联智能蜜网生成

3.5.3 沙箱管理

沙箱主要用于吸引攻击者入侵；普通用户权限只能看到相关沙箱基本信息，不能对沙箱进行操作，比如新建沙箱，重启沙箱、停用沙箱等相关操作。管理员权限不能删除沙箱。

用户可根据实际需求，对沙箱设置事件灵敏度，事件灵敏度设置分为高、中、低三个级别，事件灵敏度设置为'高'时：系统会上报该沙箱的所有相关事件，包括所有攻击事件和所有探测事件，事件灵敏度设置为'中'时：系统会上报该沙箱的所有入侵事件和高危探测事件，

事件灵敏度设置为‘低’时：系统会上报该沙箱的所有入侵事件。

沙箱管理页面主要用于展示所有沙箱信息以及对沙箱的相关操作，展示的信息包括沙箱类型、关联 IP、沙箱状态，其中关联 IP 可上浮展示所有。支持按照设备、沙箱类型和运行状态进行查询；沙箱信息默认按照图标形式展示，也可以点击页面右边‘ ’按钮切换至列表模式。如下图：

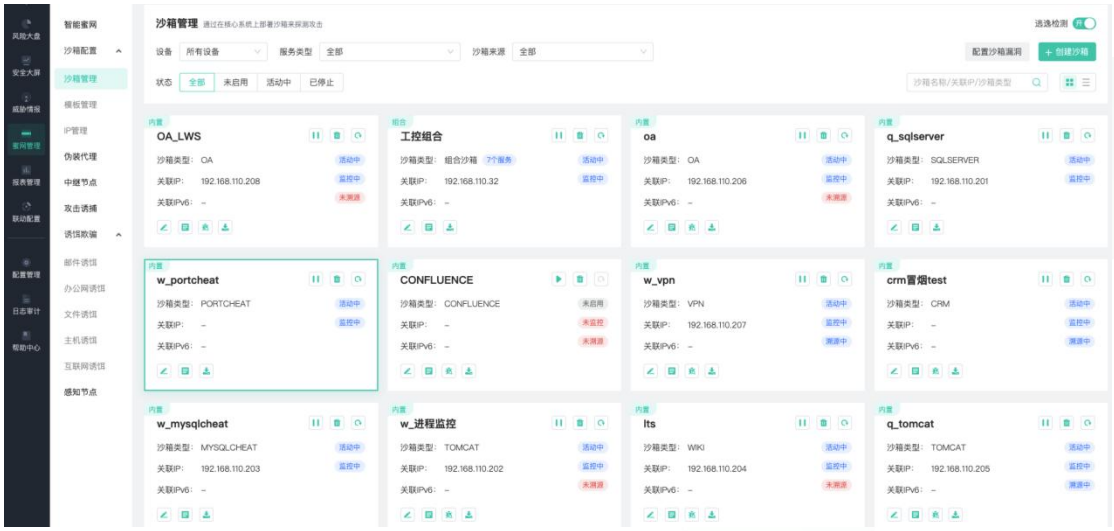


图 3-5-3-1 沙箱管理

在漏洞设置后增加下载 pcap 功能，如下图所示。

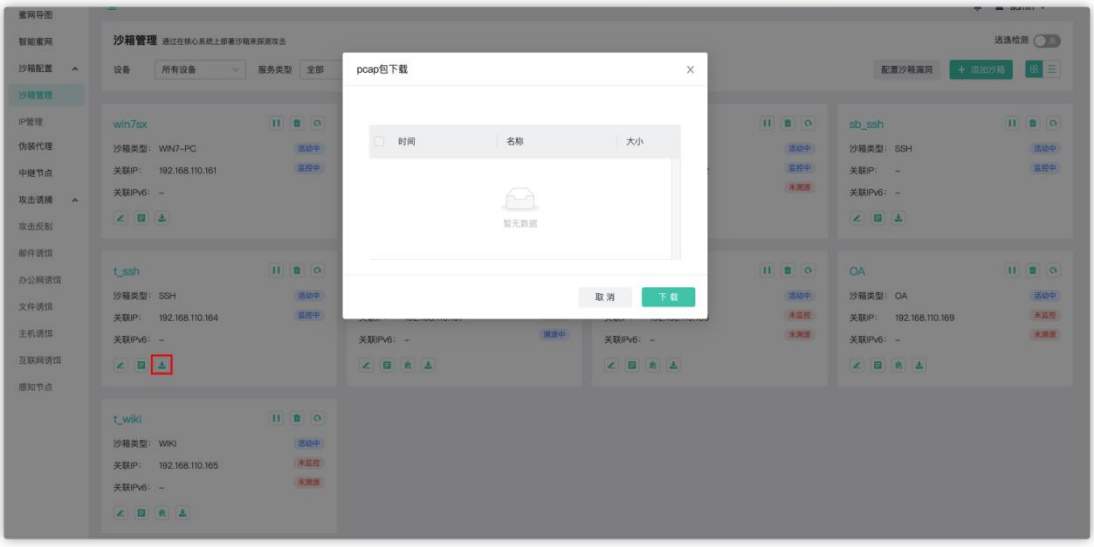


图 3-5-3-2 pcap 下载

注：为了保证性能，根据性能对设备的沙箱数量做了相应限制。低配设备启动 windows 沙箱数量最多为 1 个。中配设备启动 windows 沙箱数量最多为 2 个。高配设备 windows 沙箱数量最多为 3 个。（仅标准版支持）

1) 应用服务沙箱

wiki 沙箱为例

创建 wiki 沙箱，蜜网管理-->沙箱管理-->创建沙箱-->服务类型（应用服务）-->选择 WIKI：

“沙箱配置”中输入沙箱名称、选择端口（可设置，默认 80 端口）、可选设备；

“告警设置”选择邮件告警选择（全部/严重/高危及以上/中危及以上），完成告警设置；

“HTTPS 证书设置”，用户可自定义选择是否开启此开关来启用 HTTPS。如果决定启用，用户需要将证书文件（*.crt/cer/pem）和私钥文件（*.key）打包成 zip 格式后再导入。

选择 确定添加/取消，完成添加沙箱操作。

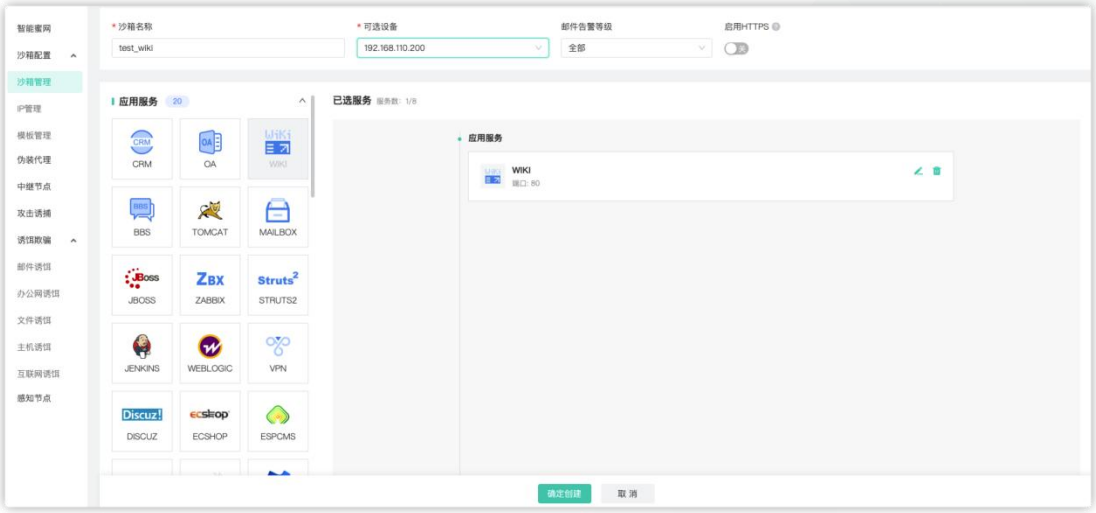


图 3-5-3-3 wiki 沙箱

添加沙箱完成后，会跳转到沙箱管理页面，新建的沙箱默认是未启用和未监控状态。设置完成之后，沙箱管理页面-->启用沙箱 （所有应用服务沙箱启用沙箱、验证沙箱操作步骤一致）如图所示：

图 3-5-3-4 启用沙箱页面

wiki 沙箱是半自定义沙箱，编辑沙箱-->可以对沙箱名称、行为灵敏度（选择 高/中/低）、流量阻断（开启/关闭）、日志监控、邮件告警等级、沙箱关联 IP、溯源设置、网站 url_path 路径、漏洞类型进行调整；事件灵敏度默认设置为'高'，流量阻断默认为开启，日志监控默认'关闭'状态，日志监控是对该沙箱所产生事件是否上报进行设置。“溯源设置”选择 是否开启溯源开关，完成溯源设置配置和浏览器反制配置；“网站 url_path 路径”支持自定义添加路径、特征字符串、替换方式（替换/向前追加/向后追加），完成指定在特定 URL 下插入 JS 设置。 对于半自定义 wiki 沙箱，用户可在 wiki 沙箱里面设置一些类似企业内部敏感信息的文档等（比如其他沙箱的信息，让攻击者在蜜罐之间跳转），建议用户在对沙箱里面内容调整设置时，可关闭日志监控，避免用户操作事件上报，操作设置完成之后，开启日志监控；如下图沙箱设置。漏洞设置可对沙箱关联的漏洞进行修改。

图 3-5-3-6 沙箱设置

沙箱状态变为‘活动中’监控状态变为‘监控中’时，沙箱成功启动，可以关联 ip，在关联 ip 上开放了 80 端口，浏览器通过关联 IP 访问，显示 wiki 界面，如下图 wiki 页面。

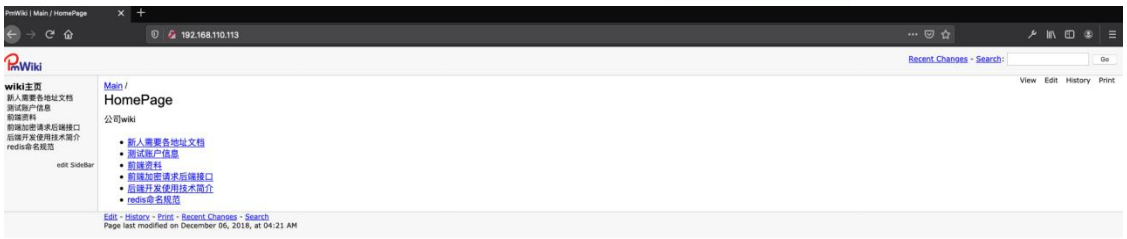


图 3-5-3-7 wiki 页面

在沙箱管理界面上选择要停用的沙箱点击‘’，沙箱状态变为‘未启用’，表示已停用；点击‘’，即删除沙箱；点击‘’，即将沙箱恢复到沙箱初始状态。如下图操作沙箱。

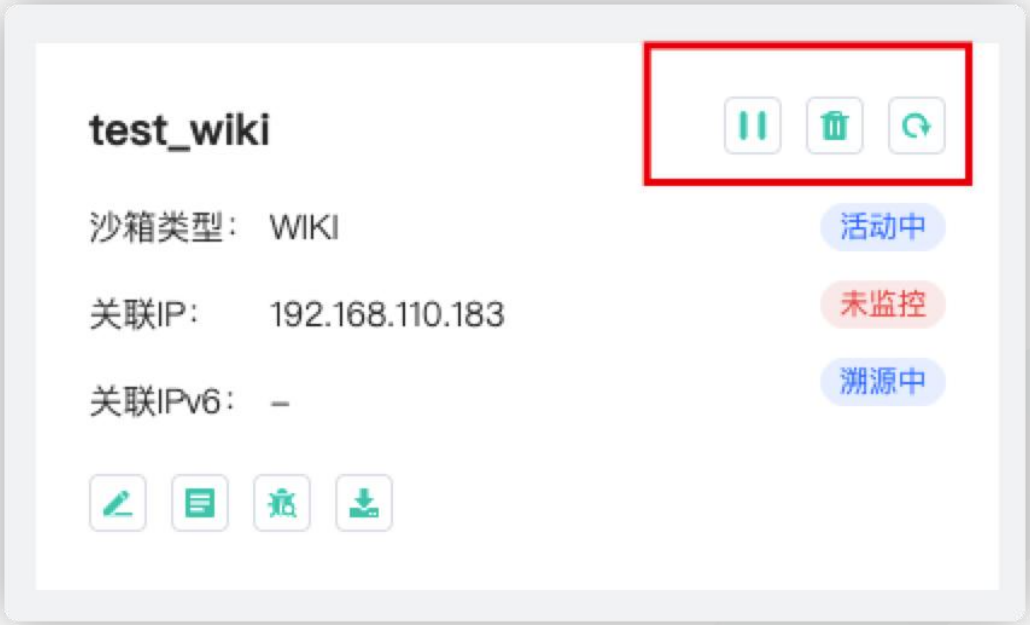


图 3-5-3-8 操作沙箱

查看沙箱->可以查看当前沙箱基本信息和服务配置信息；沙箱基本信息包括：沙箱 ID，沙箱类型，沙箱名称，设备 IP，沙箱状态，运行时间，行为灵敏度，办公网诱饵数、伪装代理个数、关联中继节点 IP 数等；服务配置信息包括服务名，服务图标，端口，服务配置，WEB 漏洞数，溯源状态，浏览器反制，git 泄露反制，svn 泄露反制，goby 反制等，如下图查看沙箱页面：

图 3-5-3-9 查看沙箱页面

web 漏洞设置页面，可对漏洞进行添加、编辑、修改，删除操作，漏洞、诱饵、伪装代理的详细操作参考 3.5.4 伪装代理模块）漏洞设置和 3.5.6 诱饵设置（**所有应用服务沙箱伪装代理、漏洞设置、诱饵管理操作步骤一致**）。

图 3-5-3-10 web 漏洞设置页面

注：应用服务类沙箱支持类型包括（CRM、OA、WIKI、BBS、TOMCAT、MAILBOX、JBOSS、ZABBIX、STRUTS2、JENKINS、WEBLOGIC、VPN、DISCUZ、ECSHOP、ESPCMS、WEBSPHERE、PHYPMYADMIN、CONFLUENCE、JOOMLA、HADOOP）

2) 系统服务沙箱

SSH 沙箱为例

创建 ssh 沙箱，蜜网管理-->沙箱管理-->创建沙箱-->服务类型（系统服务）-->选择 ssh：

“沙箱配置”中输入沙箱名称、可选设备、SSH 登录名、SSH 登录密码、确认密码，其中密码长度为 5 到 18 之间的字符串，并支持特殊字符，如@，#等。如图所示

“告警设置”选择邮件告警选择（全部/严重/高危及以上/中危及以上），完成告警设置；

选择 确定添加/取消，完成添加沙箱操作。

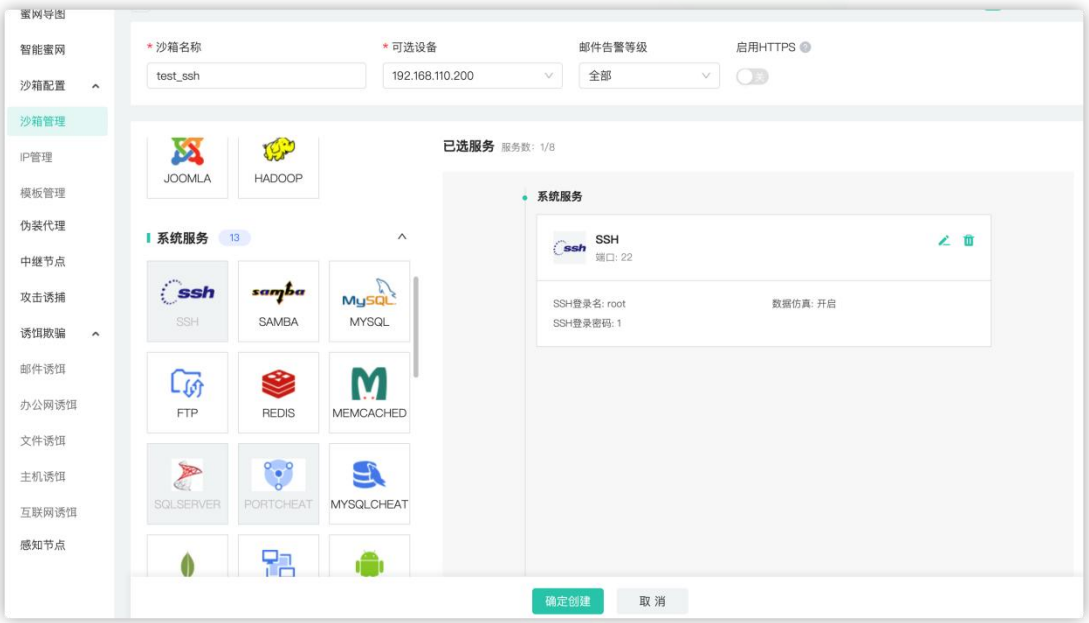


图 3-5-3-11 SSH 沙箱

SSH 沙箱被创建并启用后，用 SSH 连接上去，成功登陆后，执行任意命令，在威胁情报管理-->查看事件处，如果看到入侵则表示 ssh 沙箱运行正常，如下图事件列表。

点击查看攻击事件回放便可看到详细信息，如下图所示

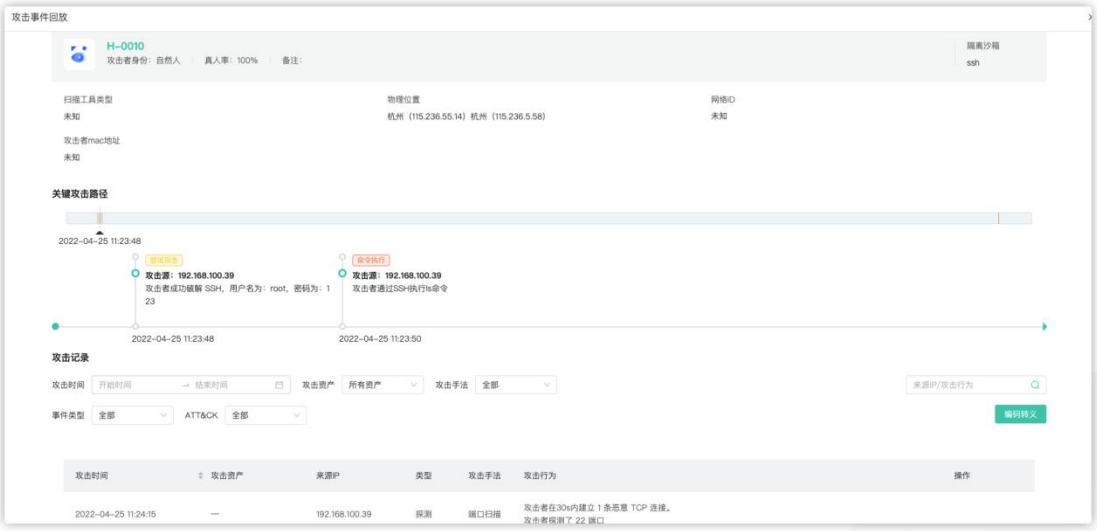


图 3-5-3-13 攻击事件回放

- **注：**系统服务类沙箱支持类型包括(SSH、SAMBA、MYSQL、FTP、REDIS、MEMCACHED、SQLSERVER、PORTCHEAT、MYSQLCHEAT、MONGODB、TELNET、ADB、POSTGRESQL）；SSH 沙箱事件支持视频回放。

3) Windows 沙箱（仅标准版支持）

WIN7-PC 沙箱为例

创建 win7-pc 沙箱，蜜网管理-->沙箱管理-->创建沙箱-->服务类型（windows）-->选择 WIN7-PC:

“沙箱配置”中配置中输入沙箱名称、可选设备、登录用户名、登录密码、确认密码，其中密码长度为 5 到 18 之间的字符串，并支持特殊字符，如@，#等。

“告警设置”选择邮件告警选择（全部/严重/高危及以上/中危及以上），完成告警设置；选择 确定添加/取消，完成添加沙箱操作，如图所示:

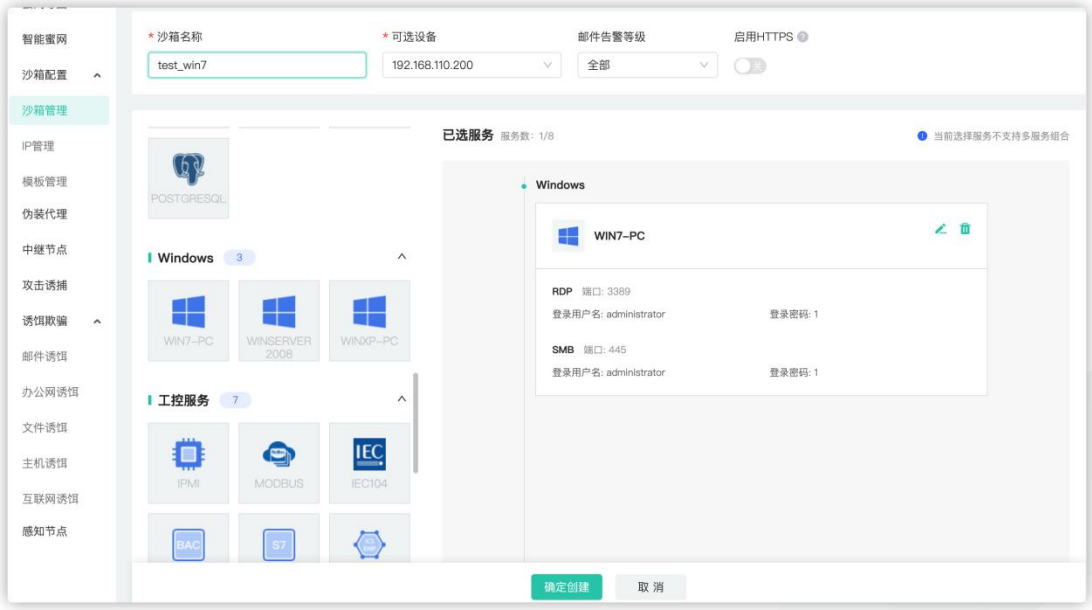


图 3-5-3-14 win7-pc 沙箱

◆ **win7-pc** 沙箱被创建并启用，假如沙箱 IP 是 192.168.199.227，win7-pc 验证方式如下：

a. 3389 远程桌面连接，

b. mysql 远程连接，账户名密码为沙箱启动设置的账户名密码

c. ipc连接，net use \\ip\c$ "pass" /user:"username"spsexec \\ip cmd.exe

验证之后，在威胁情报管理-->查看事件处，有事件记录表示沙箱运行正常.

◆ **WIN2008-SERVER** 沙箱被创建并启用， win2008-server 验证方式如下：

a. 3389远程桌面连接

b. sqlserver弱口令连接

c. ipc连接，net use \\ip\c$ "pass" /user:"username"spsexec \\ip cmd.exe

验证之后，在威胁情报管理-->查看事件处，有事件记录表示沙箱运行正常。

d. 利用 nmap 工具执行命令：nmap --script smb-vuln-ms17-010.nse ip

验证之后，在威胁情报管理-->查看事件处，有事件记录表示沙箱运行正常

◆ **Winxp-pc** 沙箱被创建并启用，检测 ms08067 漏洞。

利用 nmap 工具执行命令：nmap --script smb-vuln-ms08-067.nse -p445 <host>

在威胁情报管理-->查看事件处，有事件记录则表示沙箱运行正常。

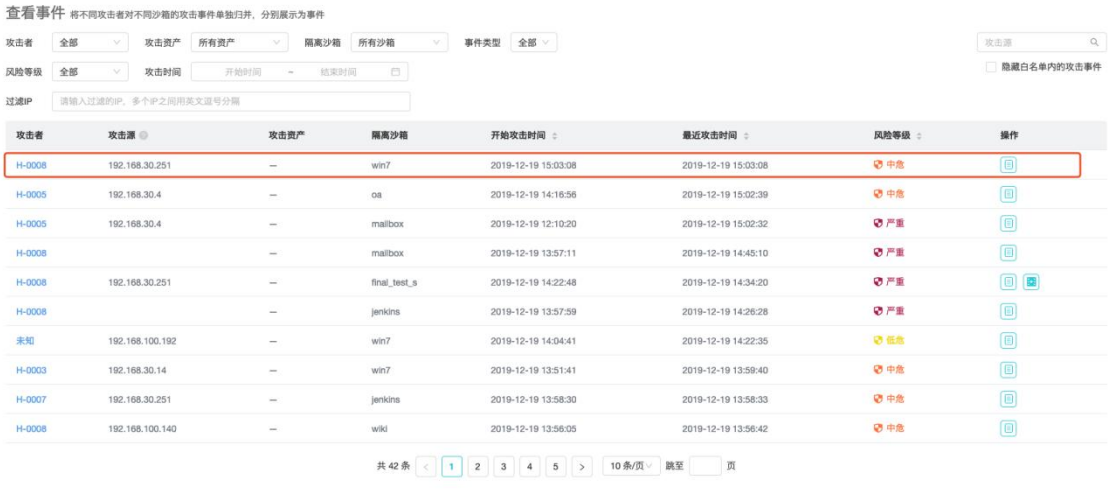


图 3-5-3-15 事件列表

- **注：windows** 类沙箱支持类型包括（WIN7-PC、WIN2008SERVER、WINXP-PC）

4) 工控沙箱

IPMI 沙箱为例

创建 ipmi 沙箱，蜜网管理-->沙箱管理-->创建沙箱-->服务类型（工控沙箱）-->选择 ipmi：

“沙箱配置”中输入沙箱名称、选择端口、可选设备、IPMI 用户名、IPMI 密码、确认密码，其中密码长度为 5 到 18 之间的字符串，并支持特殊字符，如@，#等；

“告警设置”选择邮件告警选择（全部/严重/高危及以上/中危及以上），完成告警设置；如图所示

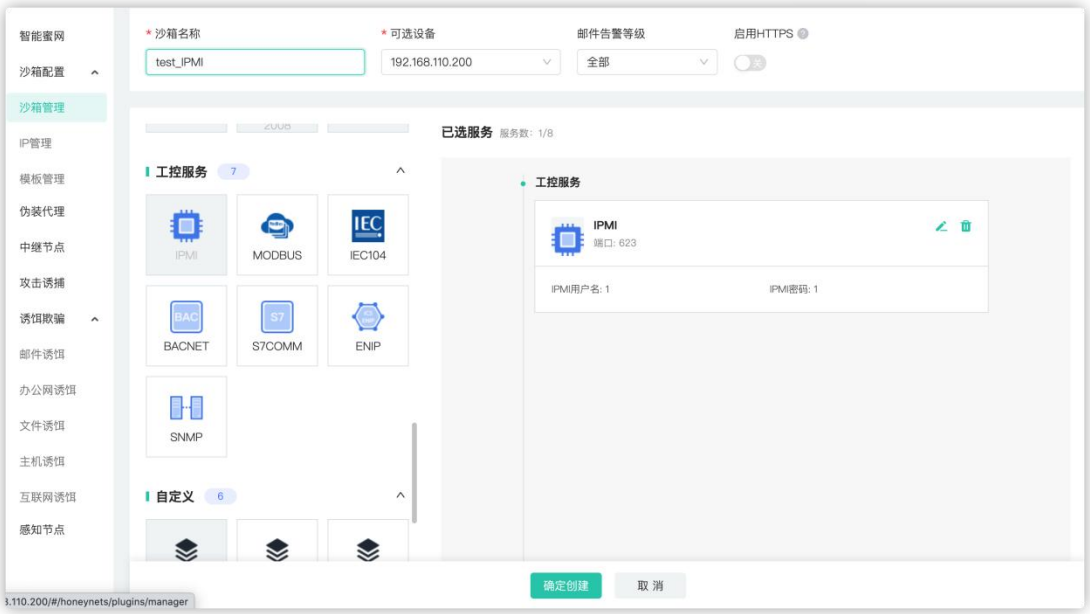


图 3-5-3-16 ipmi 沙箱

添加沙箱后，启动沙箱，当沙箱状态变为‘活动中’，监控状态变为‘监控中’时，表明沙箱已经在运作。

图 3-5-3-17 启用沙箱页面

这时可在主机或虚拟机上通过 apt-get install -y ipmitool 的命令，安装 ipmi 工具后，使用 ipmitool -I lan -H（ip 地址） -U （登录名）shell，输入 password,进入 IPMI 交互模式，或可以 shell 直接换成 bmc 命令。

```
root@ubuntu1:~# apt-get install ipmitool
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
ipmitool 已经是最新版 (1.8.16-3ubuntu0.2)。
升级了 0 个软件包，新安装了 0 个软件包，要卸载 0 个软件包，有
12 个软件包未被升级。
有 1 个软件包没有被完全安装或卸载。
解压缩后会消耗 0 B 的额外空间。
您希望继续执行吗？ [Y/n] y
正在设置 nginx-core (1.10.3-0ubuntu0.16.04.5) ...
root@ubuntu1:~# ipmitool -I lan -H 192.168.110.166 -P ipmi she
ll
root@ubuntu1:~# ipmitool -H 192.168.110.166 -I lanplus -U ipmi
 -P 123456  power status
Chassis Power is off
```

图 3-5-3-18 攻击 IPMI 沙箱

成功进入 IPMI 沙箱后，执行任意命令，在威胁情报管理-->查看事件处，如果看到入侵则表示 IPMI 沙箱运行正常，如下图事件列表。

攻击时间	攻击资产	来源IP	类型	攻击手法	攻击行为	操作
2022-01-13 16:02:33	—	[redacted]	探测	端口扫描	攻击者在30s内建立 11 条恶意 UDP 连接	
2022-01-13 16:02:02	—	[redacted]	探测	登出	攻击者断开60063端口与IPMI协议的连接	
2022-01-13 16:02:02	—	[redacted]	入侵	命令执行	攻击者通过60063端口使用IPMI协议，重新设置IPMI工控设备会话权限	
2022-01-13 16:02:02	—	[redacted]	入侵	命令执行	攻击者通过60063端口使用IPMI协议，IPMI工控设备接收到无法识别的命令	
2022-01-13 16:02:02	—	[redacted]	入侵	命令执行	攻击者通过60063端口使用IPMI协议，IPMI工控设备接收到无法识别的命令	
2022-01-13 16:02:02	—	[redacted]	入侵	命令执行	攻击者通过60063端口使用IPMI协议，IPMI工控设备接收到无法识别的命令	
2022-01-13 16:02:02	—	[redacted]	入侵	敏感信息探测	攻击者通过60063端口使用IPMI协议，对IPMI工控设备发送了指令：请求获取电源状态	
2022-01-13 16:02:02	—	[redacted]	入侵	登出	攻击者通过60063端口使用IPMI协议，关闭IPMI工控设备会话	
2022-01-13 16:02:02	—	[redacted]	探测	尝试访问	攻击者通过60063端口建立IPMI协议的访问	
2022-01-13 16:01:22	—	[redacted]	探测	端口扫描	攻击者在30s内建立 22 条恶意 UDP 连接	

图 3-5-3-19 幻阵告警

5) 漏洞设置

漏洞设置页面主要是在自定义沙箱、应用服务类沙箱中添加漏洞，根据沙箱的语言类型选择不同的语言类型（PHP、ASP、JSP）添加相应的漏洞，攻击者访问该 web 漏洞时，抓取攻击者的设备指纹，新建沙箱 web 漏洞默认为不添加。

通过沙箱管理界面点击“配置沙箱漏洞”，如图:

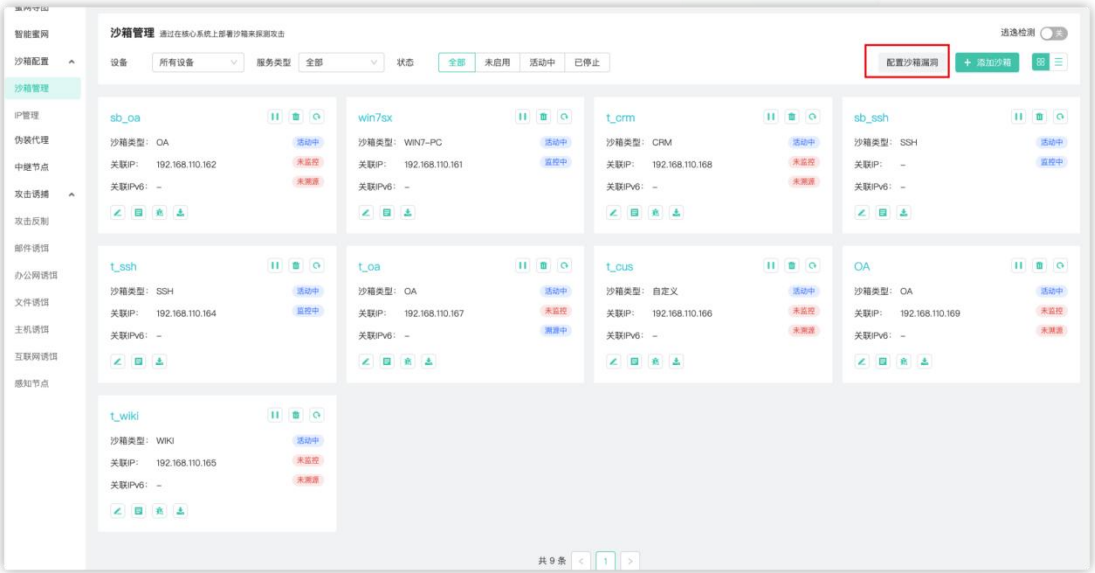


图 3-5-3-23 配置沙箱漏洞 1

通过沙箱列表点击“配置沙箱漏洞”，如图:

图 3-5-3-24 配置沙箱漏洞 2

添加 web 漏洞，点击沙箱右上角的‘  ’(漏洞设置)按钮，即跳转到漏洞设置页面，如下图。

图 3-5-3-25 漏洞设置

点击右上角添加 web 漏洞，漏洞类型可选漏洞包和单条漏洞，选择 web 漏洞的关联沙箱，如果关联沙箱是自定义沙箱，需要选择和自定义沙箱的仿真业务系统一致的网站语言，应用服务类沙箱可选取 PHP、ASP、JSP 三种语言的其中一种，如下图添加 web 漏洞页面：

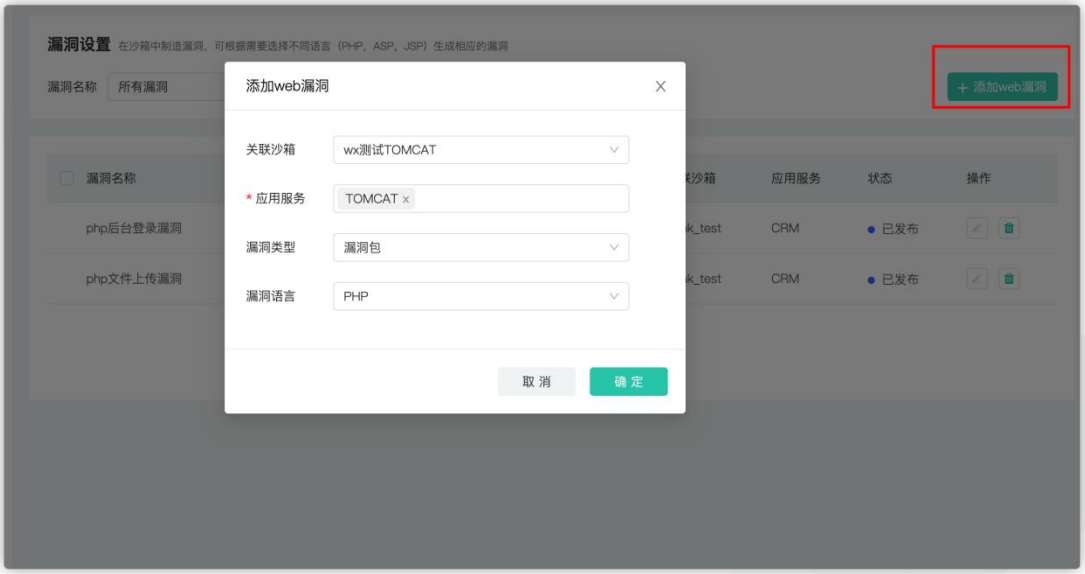


图 3-5-3-26 添加 web 漏洞页面

漏洞类型包含如下：文件上传漏洞、后台登录漏洞、数据库后台登录漏洞、服务器后台登录漏洞、安装信息泄露漏洞。

添加完成之后回到 web 漏洞设置界面，此时添加的 web 漏洞还未生效，还可对单条 web 漏洞进行编辑、删除操作；如下图 web 漏洞管理页面：

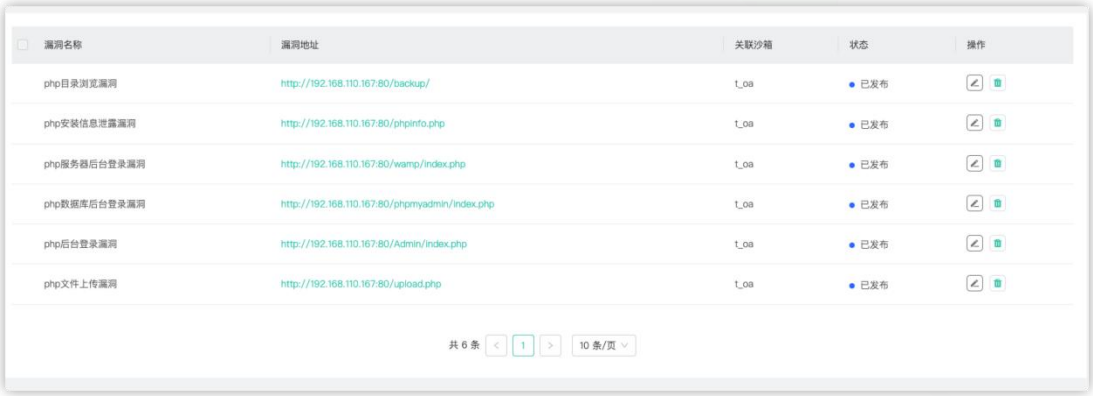


图 3-5-3-27 web 漏洞管理页面

选择需要发布的漏洞，点击‘发布’按钮，状态变为‘已发布’之后，几分钟后，规则下发到沙箱，访问漏洞列表‘已发布’的漏洞地址，能访问到漏洞页面表示该条 web 漏洞添加完成，如下图沙箱漏洞页面：

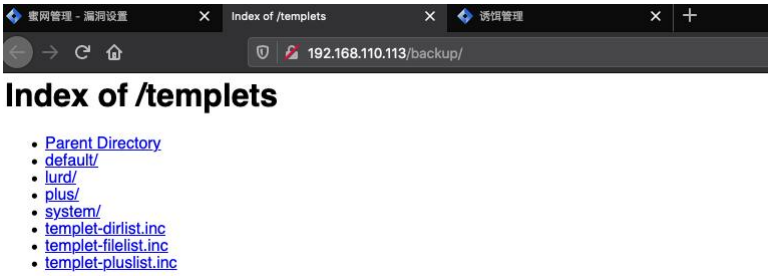


图 3-5-3-28 沙箱漏洞页面

3.5.4 IP 管理

IP 管理页面展示了 IP 地址、关联沙箱、关联设备、状态以及操作，并且可以根据关联类型和 IP 进行筛选，右侧有添加 IP 按钮可以进行 IP 的添加，如下图所示：

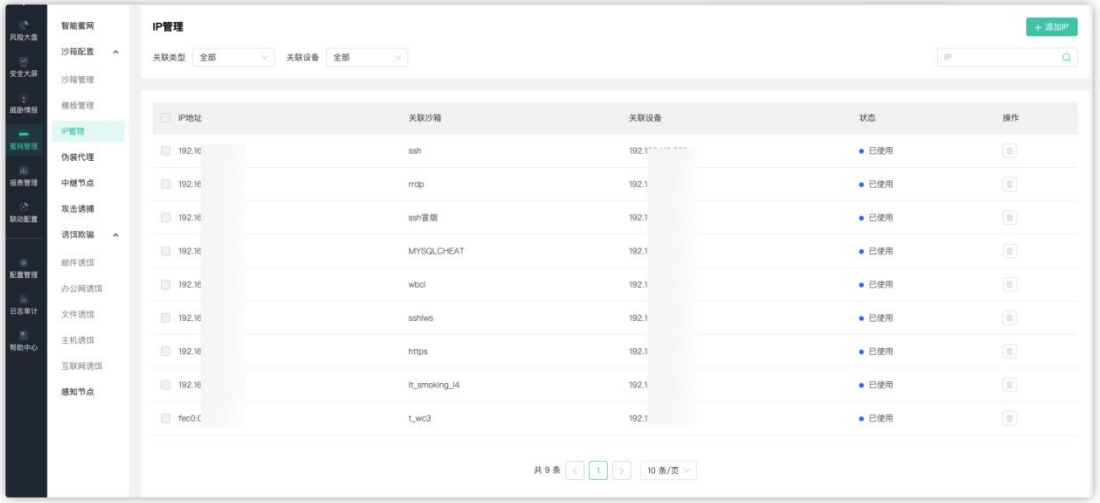
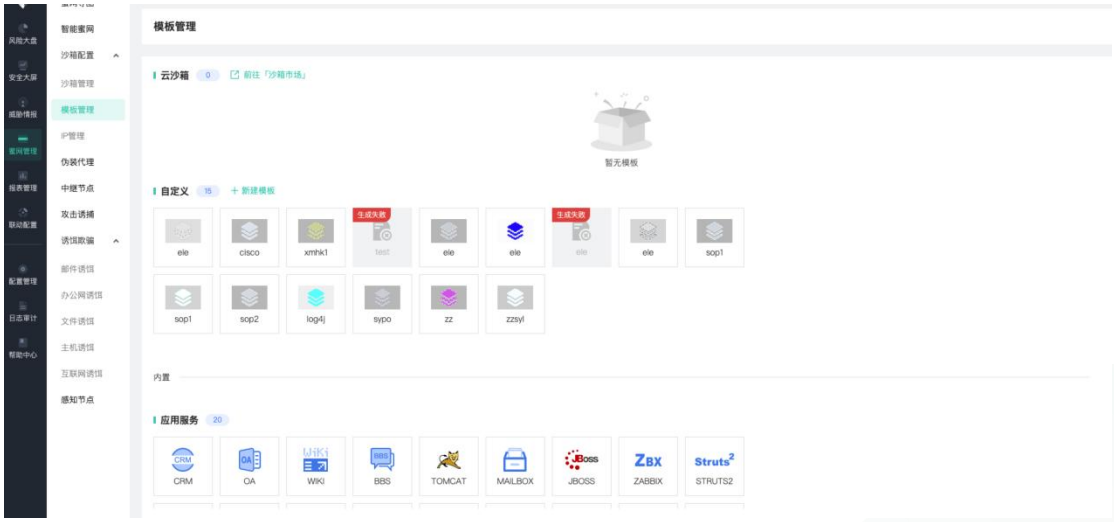


图 3-5-3-28 IP 管理页面

3.5.5 模板管理

模板管理页面展示云沙箱模板、自定义模板和内置模板；



「前往沙箱市场」:当与 MSS 安全运营平台完成注册后，可跳转至沙箱市场页面获取云沙箱。

新建模板：点击"新建模板",配置"模板图标"、"模板名称"、"模板介绍"、"模板文件"，点击【确定】，自定义栏中生成自定义模版对应的图标，如下图所示。

"沙箱文件" 仅支持上传 zip 文件，文件大小不能超过 1GB；
zip 包内的基础模板支持上传保活脚本：keepalive.sh；支持上传配置脚本：config.sh
zip 包内的高级模板必须包含 define.yml 以及 docker 镜像;

- **注：**

  1. 上传的 html 压缩包（.zip 文件）会自动解压，自动安装部署。
  2. 如果需要支持其他语言，可参考《附录 A 自定义沙箱部署说明》

◆ **说明**：自定义沙箱主要为了模拟用户的真实业务系统的，扰乱攻击者的攻击目标。

3.5.6 伪装代理

伪装代理部署在用户机器上，通过端口混淆，将黑客攻击诱导至沙箱。当系统 CPU 或内存占用率达到 80%时，伪装代理会自动停用，保证业务正常运行。其中，伪装代理的最大同

时存在的数量为沙箱数量的 5 倍。

1)　伪装代理安装

◆ **基础模式：**适用于网络直接可达的多个网段中安装（网络可达比如各网段中没有禁止对幻阵服务器 8888/udp 5555/tcp 端口的防火墙策略）

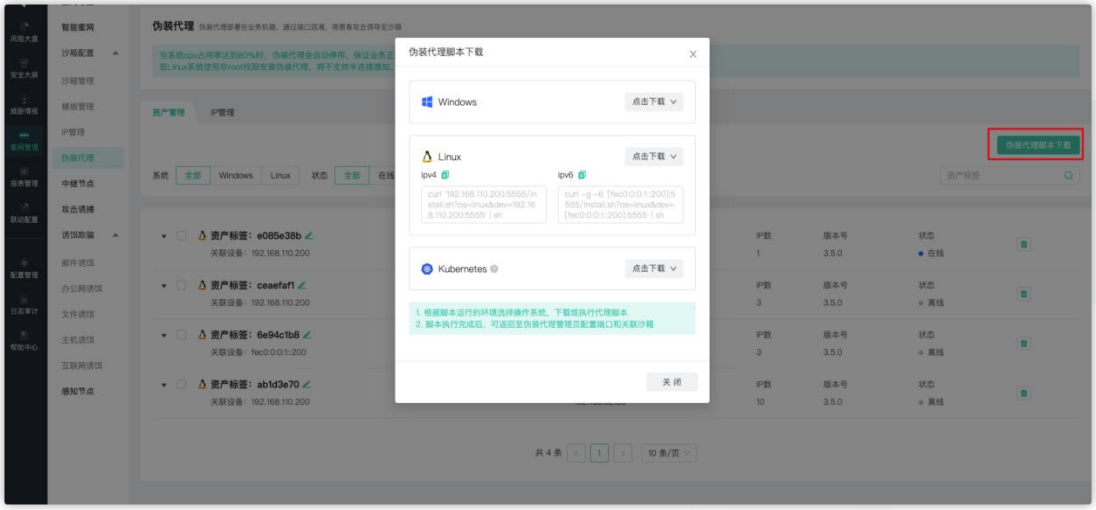


图 3-5-4-1 伪装代理下载

选择相应操作系统下载。Linux 和 windows 都需直接运行 install 文件(管理员权限)。目前 linux 端目前支持 centos6.4/centos6.5/centos6.6/centos7.0/centos7.1/centos7.2/ubuntu14.04/ubuntu16.04/redhat 6.5 进行一键部署(如需要支持其他操作系统，提供相关操作系统版本号联系默安科技工程师)。

例 linux:

Linux 下安装

解压已下载的压缩文件　tar -zvxf xxxxx.tar.gz

```
moresec          proxy_cli_linux_20170828083703.tar.gz  proxy_cli_linux_20170829133706.tar.gz  proxy_cli_linux.tar.gz
proxy_cli_linux  proxy_cli_linux_20170829125128.tar.gz  proxy_cli_linux_20170829203854.tar.gz
[root@localhost home]# tar -zvf proxy_cli_linux_20170829203854.tar.gz
tar: You must specify one of the `-Acdtrux' or `--test-label' options
Try `tar --help' or `tar --usage' for more information.
[root@localhost home]# tar -zxvf proxy_cli_linux_20170829203854.tar.gz
proxy_cli_linux/
proxy_cli_linux/src/
proxy_cli_linux/src/hp_route_cli/
proxy_cli_linux/src/hp_route_cli/hp_route_cli.py
proxy_cli_linux/src/hp_route_cli/hp_conf.json
proxy_cli_linux/src/base/
proxy_cli_linux/src/base/yg_util.py
proxy_cli_linux/src/base/yg_process.py
proxy_cli_linux/src/base/yg_time.py
proxy_cli_linux/src/base/__init__.py
proxy_cli_linux/src/base/yg_syshead.py
proxy_cli_linux/src/base/yg_log.py
proxy_cli_linux/src/base/yg_daemon.py
proxy_cli_linux/src/base/yg_net.py
proxy_cli_linux/src/base/yg_thread.py
proxy_cli_linux/src/base/yg_base_cfg.py
proxy_cli_linux/src/base/yg_daemon.pyc
proxy_cli_linux/src/base/yg_syshead.pyc
proxy_cli_linux/src/base/yg_base_cfg.pyc
proxy_cli_linux/src/base/yg_log.pyc
proxy_cli_linux/src/base/yg_util.pyc
proxy_cli_linux/src/base/yg_net.pyc
proxy_cli_linux/src/base/yg_process.pyc
proxy_cli_linux/src/base/yg_time.pyc
proxy_cli_linux/src/hp_route_base/
```

图 3-5-4-2 Linux 安装 1

进入该目录 cd xxxxxx

```
[root@localhost home]# ls
moresec          proxy_cli_linux_20170828083703.tar.gz  proxy_cli_linux_20170829133706.tar.gz  proxy_cli_linux.tar.gz
proxy_cli_linux  proxy_cli_linux_20170829125128.tar.gz  proxy_cli_linux_20170829203854.tar.gz
[root@localhost home]# cd proxy_cli_linux/
[root@localhost proxy_cli_linux]# ls
initd  install.sh  Makefile  Makefiles  src
[root@localhost proxy_cli_linux]#
```

图 3-5-4-3 Linux 安装 2

运行该目录下 install.sh 文件　sudo bash install.sh 即可安装完成

```
[root@localhost proxy_cli_linux]# sudo bash install.sh
CentOS Linux release 7.3.1611 (Core)
NAME="CentOS Linux"
ID="centos"
PRETTY_NAME="CentOS Linux 7 (Core)"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"
CENTOS_MANTISBT_PROJECT="CentOS-7"
CENTOS_MANTISBT_PROJECT_VERSION="7"
REDHAT_SUPPORT_PRODUCT="centos"
CentOS Linux release 7.3.1611 (Core)
CentOS Linux release 7.3.1611 (Core)
detect Centos!
deploy program ...
mkdir -p /usr/local/moresec
mkdir -p /usr/local/moresec/hpc_guiseproxy
cp -r ./src/* /usr/local/moresec/hpc_guiseproxy
cp ./initd/moresec-routeCli /etc/init.d
chmod a+x /etc/init.d/moresec-routeCli
install autostart
chkconfig --add moresec-routeCli
chkconfig --level 2345 moresec-routeCli on
service moresec-routeCli start
hp_route_cli start!
install done!
[root@localhost proxy_cli_linux]#
```

图 3-5-4-4 Linux 安装 3

卸载伪装代理命令：service moresec-routeCli uninstall(或者在伪装代理界面直接点击删除卸载)

```
[root@localhost proxy_cli_linux]# service moresec-routeCli uninstall
no hp_route_cli is running ...
uninstall done!
[root@localhost proxy_cli_linux]#
```

图 3-5-4-5 Linux 安装 4

停止伪装代理命令：service moresec-routeCli stop

启动伪装代理命令：service moresec-routeCli start

例 windows：

1. 下载 windows 版本伪装代理安装文件后进行解压

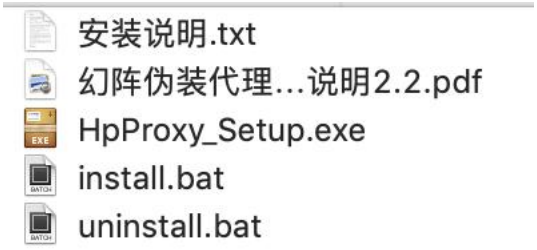


图 3-5-4-6 Windows 安装 1

2. 安装请右键以管理员权限运行 install.bat
3. 卸载请右键以管理员权限运行 uninstall.bat

例 Kubernetes：

1. 下载 Kubernetes 版本伪装代理安装文件
2. 将文件拷贝到 K8S 环境的 master 节点下
3. 解压已下载压缩包 tar zxvf xxxxx.tar.gz
4. 在 worker 节点将镜像加载到本地仓库 docker load -i hp_route.tar

```
root@kubernetes-master:~/test# ls
hp_route.tar  hp_route.yaml  route_cli_docker_1655285908.tar.gz
root@kubernetes-master:~/test# docker load -i hp_route.tar
11cccb4a9bac: Loading layer [==================================================>]  5.476MB/5.476MB
3789fb48b291: Loading layer [==================================================>]  6.414MB/6.414MB
Loaded image: hp_route:3.5.0
root@kubernetes-master:~/test#
```

5. 使用宿主机网络：修改 hp_route.yaml，将 hostNetwork 字段的值改为 true

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: route-cli-pod
  namespace: default
spec:
  containers:
    - name: route-cli
      image: hp_route:3.5.0
      imagePullPolicy: IfNotPresent
      env:
      - name: SERVER_IP
        value: 10.0.1.6:5555
  hostNetwork: true
~
```

6. 创建 pod：kubectl create -f hp_route.yaml

```
root@kubernetes-master:~/test# kubectl create -f hp_route.yaml
pod/route-cli-pod created
root@kubernetes-master:~/test#
```

```
root@kubernetes-master:~/test# kubectl create -f hp_route.yaml
pod/route-cli-pod created
root@kubernetes-master:~/test# kubectl get pod -A
NAMESPACE     NAME                                          READY   STATUS    RESTARTS   AGE
default       hp-route-5b7778df59-qxr7v                     1/1     Running   1          5d3h
default       route-cli-pod                                 1/1     Running   0          31s
kube-system   coredns-545d6fc579-2j6z2                      1/1     Running   1          13d
kube-system   coredns-545d6fc579-ksrr8                      1/1     Running   1          13d
kube-system   etcd-kubernetes-master                        1/1     Running   3          13d
kube-system   kube-apiserver-kubernetes-master              1/1     Running   16         13d
kube-system   kube-controller-manager-kubernetes-master     1/1     Running   8          13d
kube-system   kube-flannel-ds-amd64-d9975                   1/1     Running   1          13d
kube-system   kube-flannel-ds-amd64-khwmj                   1/1     Running   1          13d
kube-system   kube-flannel-ds-amd64-sz7jk                   1/1     Running   1          13d
kube-system   kube-proxy-hx25h                              1/1     Running   1          13d
```

7. 删除 pod：kubectl delete -f hp_route.yaml

◆ **高级模式：**适用于内网隔离状态或将伪装代理安装在外网情况下

● **路由器操作示例**:

A. 在路由器、防火墙等设备上将沙箱所在服务器的 IP 映射到需要安装伪装代理的服务器网络可达的 IP 地址(UDP8888 和 TCP5555 或全端口)，如下图:

图 3-5-4-7 路由器操作 1

● **幻阵页面操作**

A. 首先需要在幻阵管理页面的设备信息处添加虚拟 IP（沙箱所在服务器映射后的 IP）

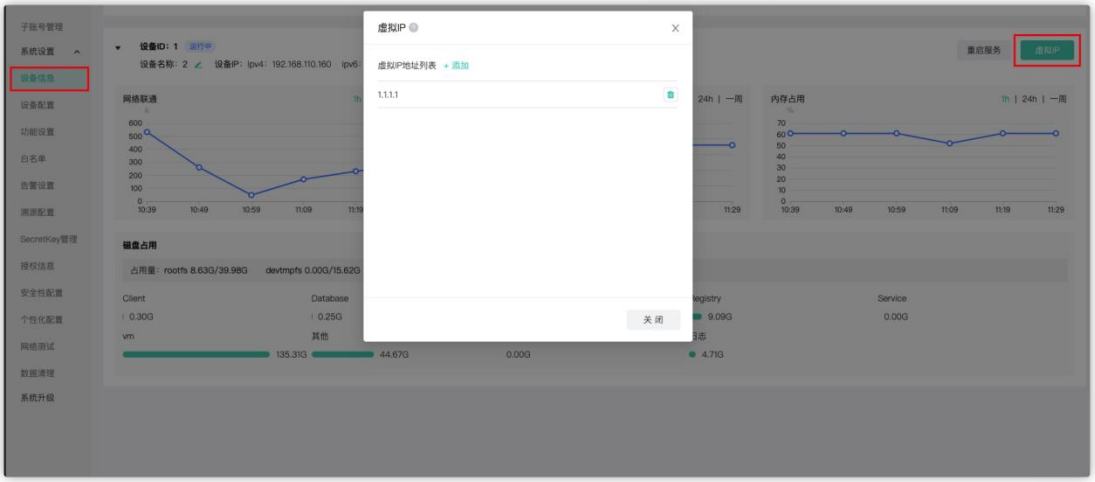


图 3-5-4-8 幻阵页面操作 1

B. 设置完成后进入伪装代理下载页面进入高级模式，在该页面选择需要安装伪装代理的真实 IP 或者虚拟 IP（多台设备可以多选），下载相应操作系统的伪装代理。

图 3-5-4-9 幻阵页面操作 2

✧ **注：**安装步骤和简单模式的安装步骤一致。

2) 伪装代理配置

伪装代理脚本安装好后会在默安幻阵的伪装代理页面显示出已经安装成功伪装代理的资产信息，点击编辑按钮即可对伪装代理进行编辑，并且可以选择批量编辑，批量删除，批量更新，输入标签（便于管理），选择资产本机需映射的端口和映射目标沙箱与服务关联。

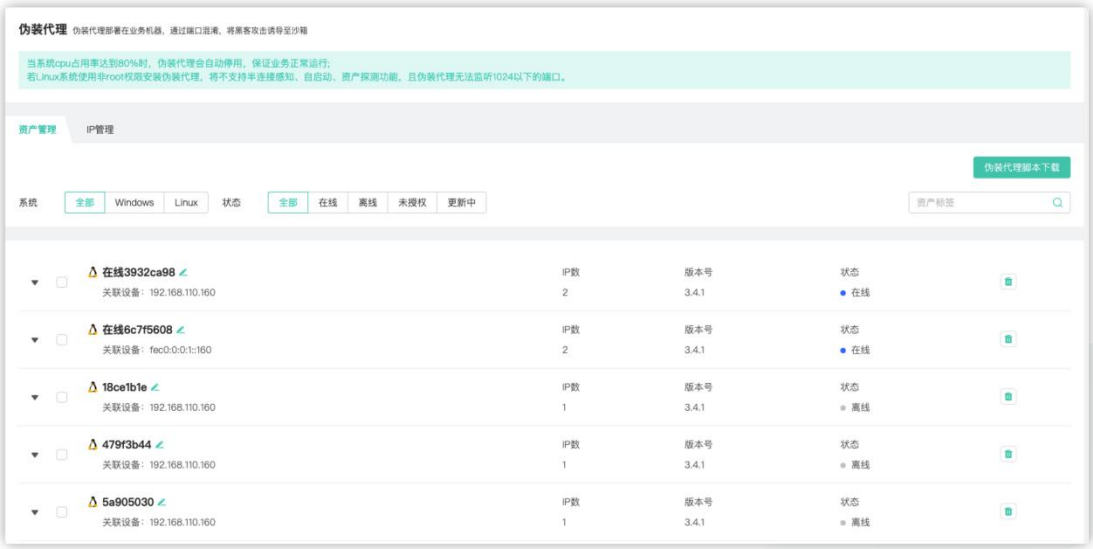


图 3-5-4-10 幻阵伪装代理页面

点击【伪装代理脚本下载】，进入下载页面，根据伪装代理安装的环境选择操作系统，“点击下载”按钮进行下载。下载后执行脚本完成，返回到伪装代理页面，可查看【资产管理】页面，会显示已经获取到的资产信息，以及相关 IP 信息；查看【IP 管理】页面，会自动显示获取到的伪装代理 IP 信息；在【IP 管理】页面，可以对伪装代理 IP 进行删除操作，如下图：

图 3-5-4-11 幻阵伪装代理-资产管理页面

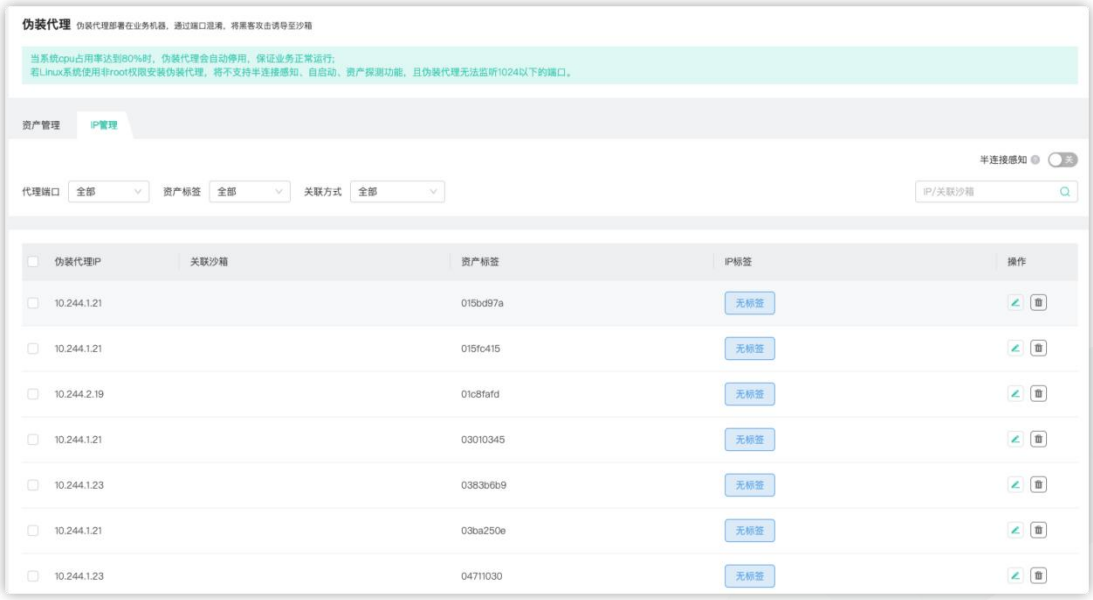


图 3-5-4-12 幻阵伪装代理-IP 管理页面

进入【IP 管理】页面，点击编辑按钮，即可编辑伪装代理，绑定沙箱。半连接开关支持用户自定义开启或者关闭，半连接感知开关开启后，关联沙箱的 IP 将可以感知 tcp、udp、icmp 等半连接扫描。编辑界面中的“标签”，“客户端端口”，“关联沙箱“等，客户可根据需要进行配置。点击“+”，选择关联的沙箱，会出现对应的关联服务和推荐的端口号，客户也可根据自己的需要修改端口号，每个伪装代理可关联多个沙箱。编辑伪装代理图示如下:

图 3-5-4-13 幻阵伪装代理-编辑代理页面

返回【资产管理】页面，即可查看关联信息。

图 3-5-4-14 幻阵伪装代理-沙箱关联

资产标签后面带有 标识，表示为精简版伪装代理，即非 root 权限下部署的伪装代理。用户可对伪装代理进行批量操作，如批量删除或批量编辑（被编辑的伪装代理的配置信息如果不一致，将清空原有配置），如下图：

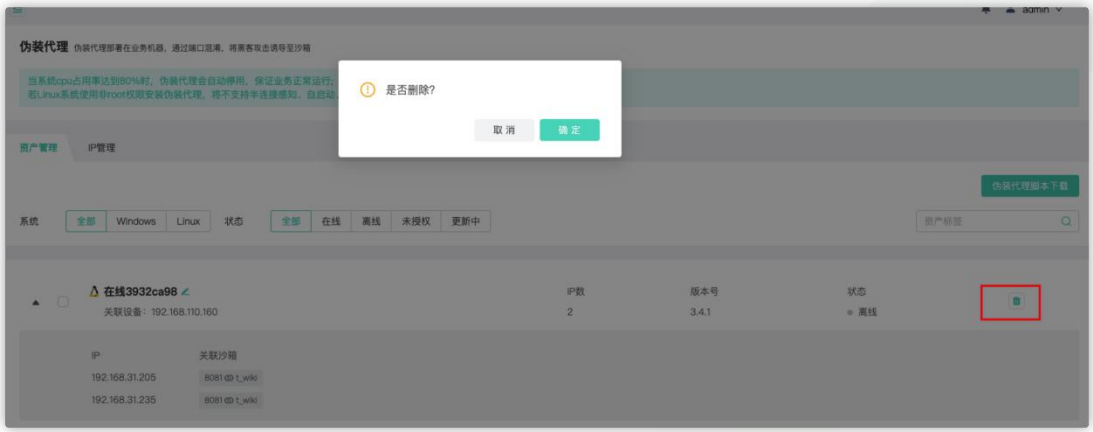


图 3-5-4-15 幻阵伪装代理-删除伪装代理页面

此外支持用户在【IP 管理】页面，对未编辑的 IP 自动绑定沙箱关系，关联成功后会在伪装代理 ip 旁用用“ ”标注。

图 3-5-4-16 幻阵伪装代理-自动关联沙箱服务页面

请勿设置被占用的端口，若资产端口和伪装代理端口冲突端口颜色会标红显示，需重新编辑。

图 3-5-4-17 伪装代理-端口冲突页面

在下发已停止的沙箱时，会有红色提示沙箱状态，但是并不影响伪装代理绑定沙箱。即沙箱无论是否运行都可编辑。

图 3-5-4-18 伪装代理列表

附录：沙箱关联规则

沙箱对应端口规则								
沙箱	端口		沙箱	端口		沙箱	端口
CRM	8080		WEBLOGIC	7001		SQLSERVER	1433
OA	81		VPN	10200		MYSQLCHEAT	3306
BBS	8000		DISCUZ	8085		MONGODB	27017
TOMCAT	8086		ECSHOP	8087		WIN7	3389
WIKI	8081		ESPCMS	8088		WIN2008	3389
MAILBOX	8890		WEBSPHERE	9043		WINXP	3389
JBOSS	8093		PHPMYADMIN	8090		自定义	80
ZABBIX	8069		MYSQL	3306		HaDoop	50070
STRUTS2	8083		REDIS	6379		Joomla	82
JENKINS	8089		MEMCACHED	11211		Confluence	8001
ADB	5555		Postgresql	5432		SSH（中继）	22
Telnet（中继）	23		Samba（中继）	445			

注:

1、当伪装代理出现“当前所建沙箱，不满足一键关联要求”提示，请查看配置是否存在如下情形:

（1）不在自动关联规则内的沙箱: SSH、Telnet、PortCheat、FTP、Samba、IPMI、MODBUS、IEC104、BACNET、S7COMM、ENIP、SNMP。

（2）只创建一个在自动关联规则里的沙箱或只创建了多个相同类型的沙箱。

（3）当前所建沙箱与安装伪装代理的主机两者操作系统不属于同一个平台，如 windows7 沙箱，与 Linux 伪装代理。

2、当伪装代理出现“没有可以一键关联的沙箱”提示，请查看配置是否存在如下情形:

(1)没有创建沙箱。

3、同一类型的沙箱不可重复关联。

4、应用服务类沙箱，若两个都是 web 容器，则只能关联其中一个。如: 同时存在 tomcat/struts2/weblogic/jboss/websphere 时，只取其中一个关联。

3.5.7 攻击诱捕

1.基础反制

Windows 反制:

反制诱饵包括文件诱饵和反制端点，可以加密上传的 office 文档，经过水印后的文件被打开时，可以被系统捕获到；反制端点为免杀型/不传染，用户可自行绑定其他应用，扩

散到企业中。同时如果攻击者踩中反制诱饵，消息中心会进行提醒，方便用户及时获取攻击者信息。如下图所示。

图 3-5-6-13 windows 基础反制

反制诱饵界面可以添加反制文件绑定，反制文件支持上传文件类型：doc/docx/rtf/exe，其中 exe 文件会自动关联到 vpn 沙箱，doc/rtf 文件会自动关联到 wiki 沙箱，原始木马文件自动关联到 Windows 沙箱不需用户上传。注意：同类沙箱只允许存在一个反制文件，多次上传会覆盖之前的上传记录，如图所示，查看感知节点跳转到感知节点 tab，下载反制文件以及删除反制文件，下载对应的诱饵，exe 的直接打开使用，doc 的需要对应的 office 版本打开，office 版本限定如下图所示。

图 3-5-6-14 添加反制文件

Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Word 2007 Service Pack 3
Microsoft Word 2010 Service Pack 2 (32-bit editions)
Microsoft Word 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)

图 3-5-6-15 支持的 office 版本

当攻击者打开反制诱饵后，在黑客溯源-攻击反制页面便可以找到上线的攻击者，当攻击者在线时可以进行高级反制，离线时可以查看历史记录，如下图所示。

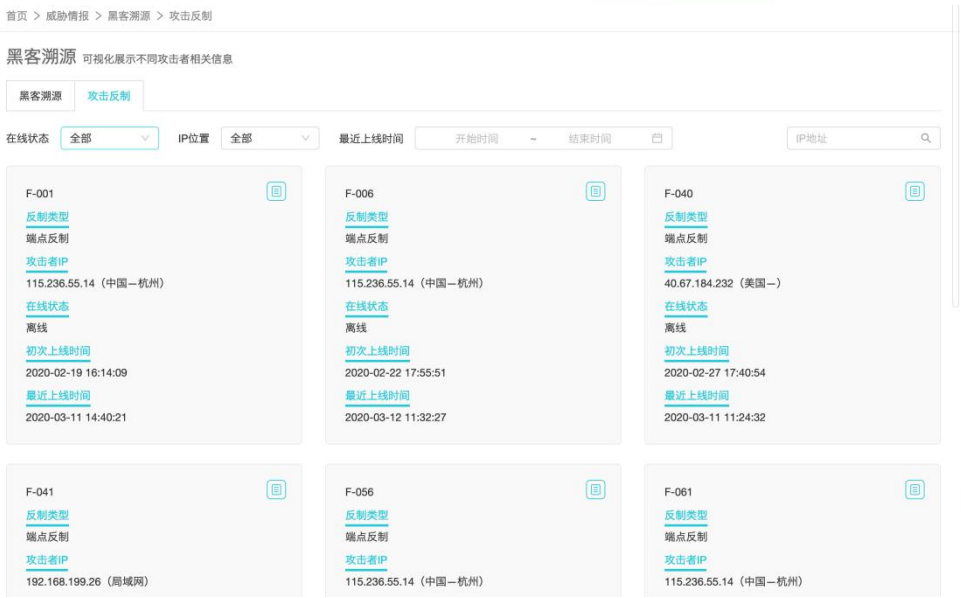


图 3-5-6-16 黑客溯源-攻击反制

Mac 反制：

反制诱饵界面可以添加反制文件绑定，反制文件支持上传文件类型：dmg/pkg/app，其中 dmg 文件会自动关联到 vpn 沙箱；注意：同类沙箱只允许存在一个反制文件，多次上传会覆盖之前的上传记录，如图所示，查看感知节点跳转到感知节点 tab，下载反制文件以及删

除反制文件，下载对应的诱饵，直接打开使用。

制作反制文件包括手动上传和自定义制作；其中自定义制作需要填写文件名称、url 地址、app 图标和文件格式；最多可制作 10 个自定义木马。

Android 反制：

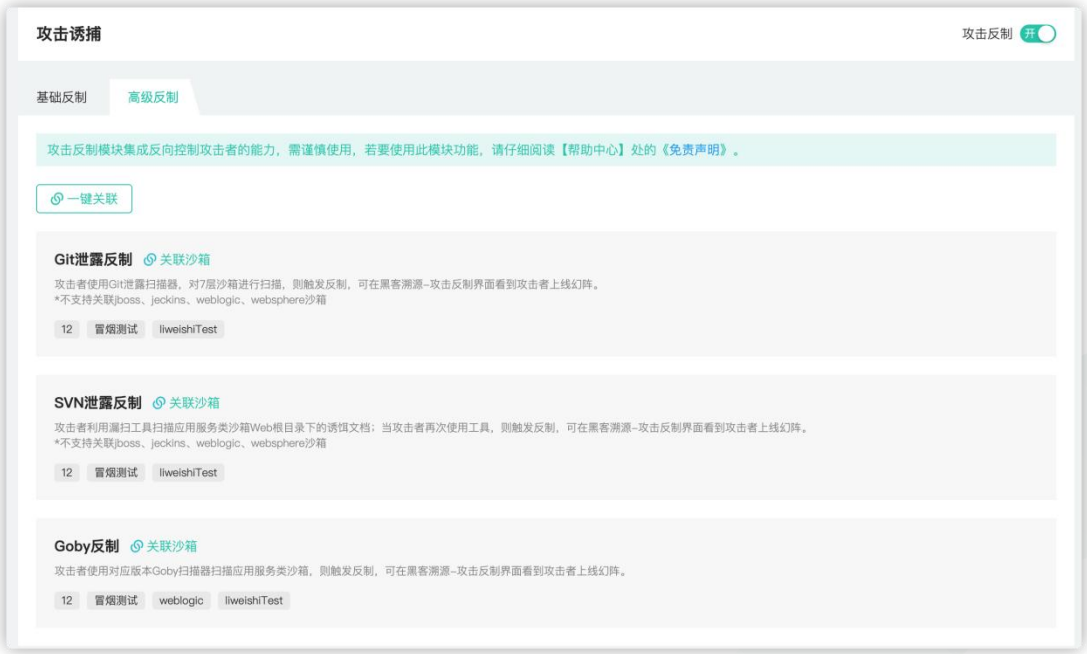
反制诱饵界面可以添加反制文件绑定，反制文件支持上传文件类型：apk，注意：同类沙箱只允许存在一个反制文件，多次上传会覆盖之前的上传记录，如图所示，查看感知节点跳转到感知节点 tab，下载反制文件以及删除反制文件，下载对应的诱饵，直接打开使用。

制作反制文件包括手动上传和自定义制作；其中自定义制作需要填写文件名称、url 地址、app 图标；最多可制作 10 个自定义木马。

2. 高级反制

高级反制模块包括 Git 泄露反制、SVN 泄露反制、Goby 反制、Git clone 反制等；

其中 Git 泄露反制、SVN 泄露反制、Goby 反制需要关联 7 层沙箱，其中 jboss、jeckins、weblogic、websphere 沙箱不支持关联；



Git clone 反制需要在 github 上发布项目，填写诱饵名称、选择模板、用户名、token 等，并点击发布项目。

3.5.8 诱饵欺骗

1) 邮件诱饵

邮件服务主要提供对高管邮箱的保护功能，通过向高管邮箱定期发送诱饵邮件，诱骗攻击者访问来发现邮箱入侵行为，可以和 VPN 等沙箱配合使用，邮件内容指向 VPN 沙箱。

添加邮件诱饵操作：蜜网管理-->诱饵管理--> 邮件诱饵-->添加邮件诱饵

点击【添加诱饵邮件】进入诱饵邮件详情的编辑页面，需要填写发送者用户名（例如发送者邮箱为 test@126.com，则用户名为 test）、密码（密码为邮箱里设置的发送密码）、服务器地址、服务器端口、是否进行证书校验、可选设备（可随机选择）、被保护的高管邮

箱（每个邮箱以行分割）、发送频率、邮件的标题、邮件日期前缀、邮件模版等信息，发送频率可以选择每周或每月，系统会根据配置的频率定期发送邮件到指定邮箱，邮件标题的前缀可以选择无或者日期，选择日期选项则会在发送邮件时将当天日期添加到邮件标题中（可以用于周报或月报等类型的诱饵邮件），邮件模板中可以选择系统默认提供的一些诱饵邮件模板，也可以自定义邮件内容，拥有添加附件功能，点击后支持上传 docx，xlsx，pptx 文件，支持上传多个文件，最多 5 个文件，每个文件最大 20M。点击【测试发送】会根据配置的邮件信息发送当前邮件到被保护者邮箱。如下图添加诱饵邮件:

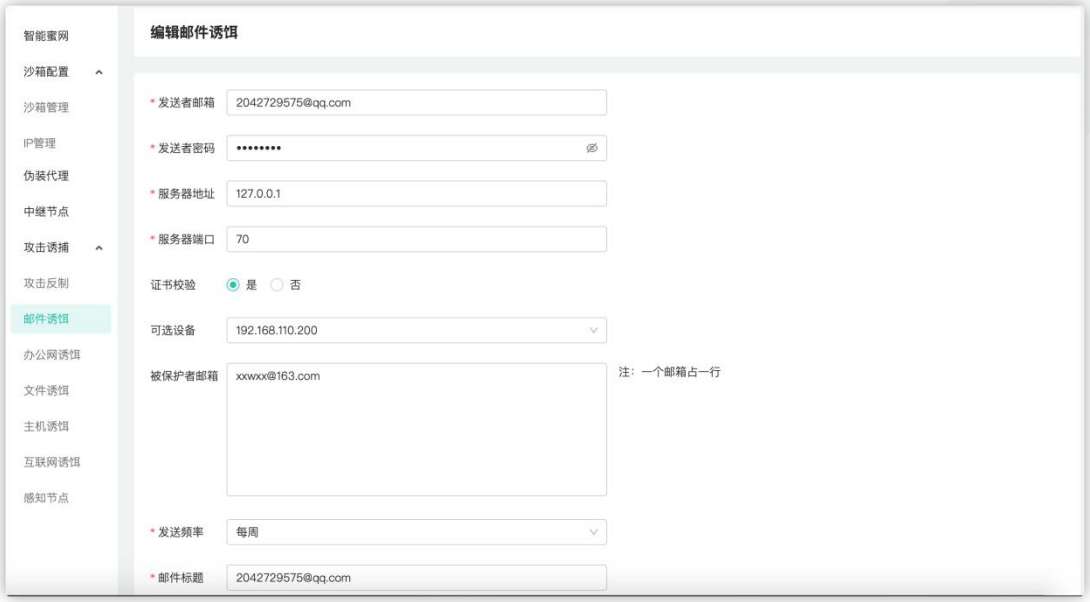


图 3-5-6-1 添加诱饵邮件

成功登陆被保护者邮箱后，查看所发送的诱饵邮件或打开邮件诱饵中的附件会被记录下来，在威胁情报管理-->查看事件处，如果看到相关事件且不是被保护者邮箱拥有者登陆则表示被保护者邮箱被入侵，如下图事件列表:

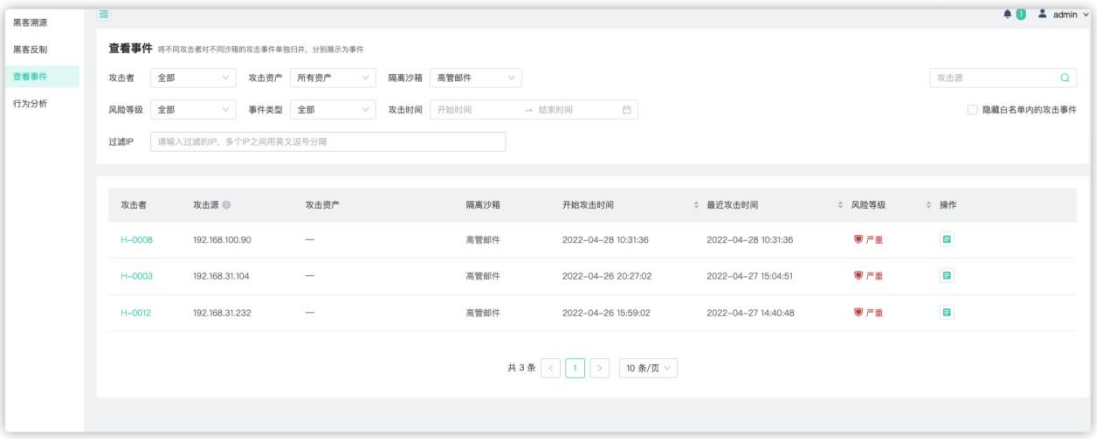


图 3-5-6-2 事件列表

测试发送事件列表查看到相应事件，说明设置正确，点击【保存】即可保存当前配置内容，在诱饵列表会生成相应的诱饵记录，状态为‘已发布’，表示该条诱饵已经发布成功，可以在操作栏‘取消发布’，状态变为‘未发布’。可以对单条记录进行‘编辑’和‘删除’操作。如下图邮件诱饵管理：

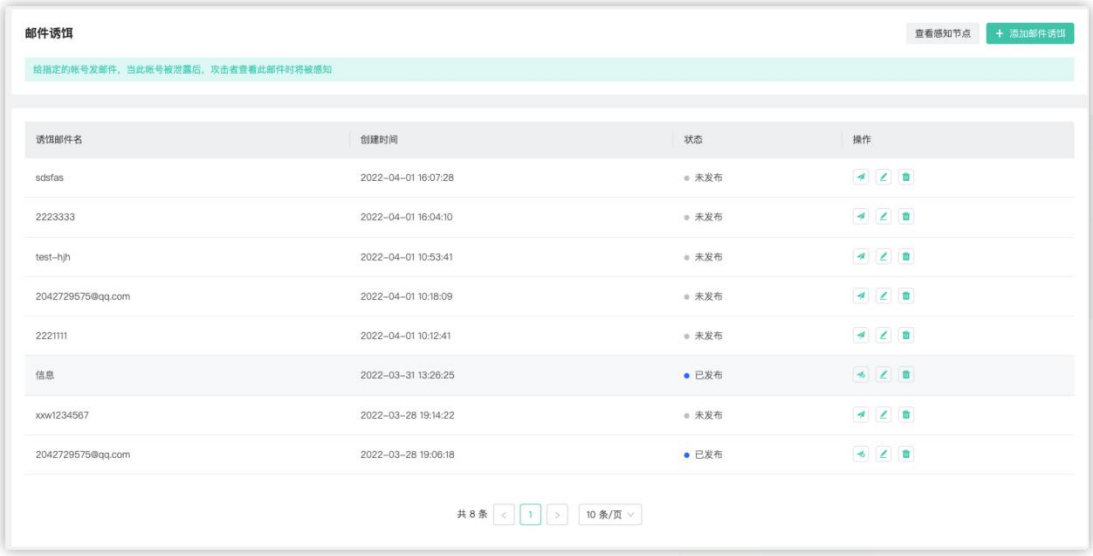


图 3-5-6-3 邮件诱饵管理

2) 办公网诱饵

办公网诱饵是在企业员工设备上分发诱饵，当攻击者入侵办公环境，诱饵会把攻击者引入默安幻阵沙箱中，从而发现攻击行为。

在办公网诱饵管理页面，有‘办公网诱饵客户端下载’链接，点击下载，下载完成之后按照下面步骤安装。

安装说明：HpfClient_Installer_1.0.0.0.exe 支持 win7，win10 系统；

办公网诱饵客户端是轻量级进程，5 分钟检查一次诱饵状态便进入睡眠。

安装方式：在 windows 机器上 cmd 中执行命令行：HpfClient_Installer_1.0.0.0.exe /u hr /i 192.168.xxx.xxx； **命令行中 IP 为默安幻阵设备客户端的 IP 地址。**

其中，/u 参数表示：用户组；比如，hr，staff 等员工组，请确保使用英文表示分组；

其中，/i 参数表示：ip； ip 为默安幻阵安装时用户提供的物理机 IP 安装地址；安装完成之后，在客户端列表会生成对应的客户端记录，如下图：

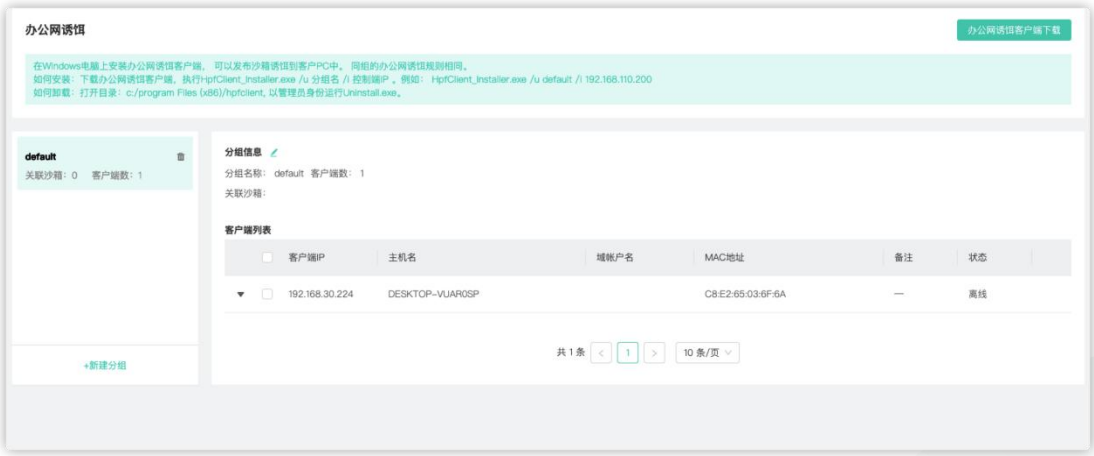


图 3-5-6-4 办公网诱饵客户端

办公网诱饵客户端安装完成之后，点击‘编辑’按钮给指定的客户端组的所有客户端分发诱饵。

添加办公网诱饵操作：蜜网管理-->诱饵管理--> 办公网诱饵-->编辑

诱饵名称自定义，选择关联沙箱（将该沙箱的信息添加到诱饵文件中）， 如下图添加办公网诱饵。

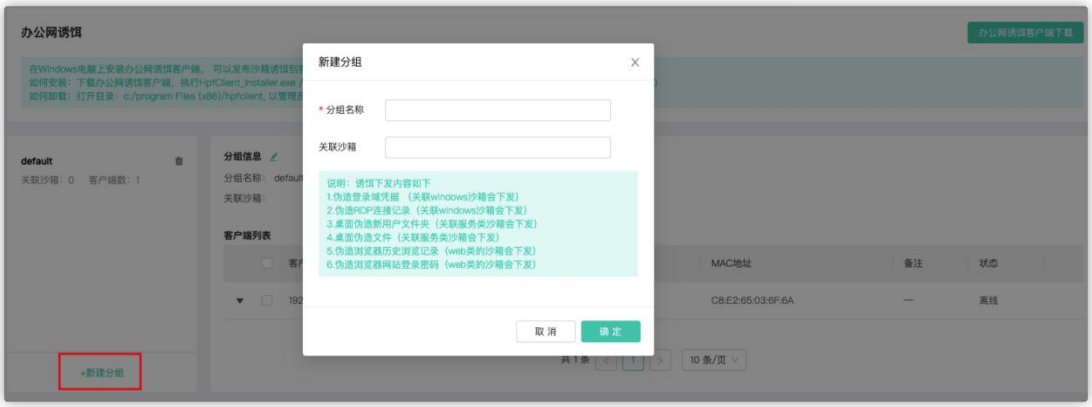


图 3-5-6-5 添加办公网诱饵

输入完成，点击‘确定’按钮即可。

3) 文件诱饵

文件诱饵功能，用户可将敏感文件上传到幻阵页面上，幻阵将文件进行打标后，提供下载功能，客户将打标后的文件下载到本地，当攻击者使用 office 打开文件时，幻阵可感知到并且进行告警。

图 3-5-6-6 文件诱饵页面

打开诱饵文件后，幻阵产生告警事件:

4) 互联网诱饵

互联网诱饵主要是针对攻击者在攻击前期信息收集阶段，在互联网发布沙箱信息，诱骗攻击者进入到相关沙箱中。

添加互联网诱饵操作：蜜网管理-->诱饵管理--> 互联网诱饵-->添加办公网诱饵

诱饵名称自定义，诱饵类型（目前支持 github， github 是一个互联网平台，部分研发人员会将研发项目的代码配置文件等放到该平台进行管理，所以该平台成为黑客喜欢搜集情报的场景），选择关联沙箱，输入 github 账号以及 token;

如果希望将敏感信息暴露为公网可达的 IP 地址，请将关联的沙箱 IP 地址映射为公网 IP 地址，并在“设置沙箱发布地址处”填写允许被攻击者访问的公网 IP。

如下图添加互联网诱饵。

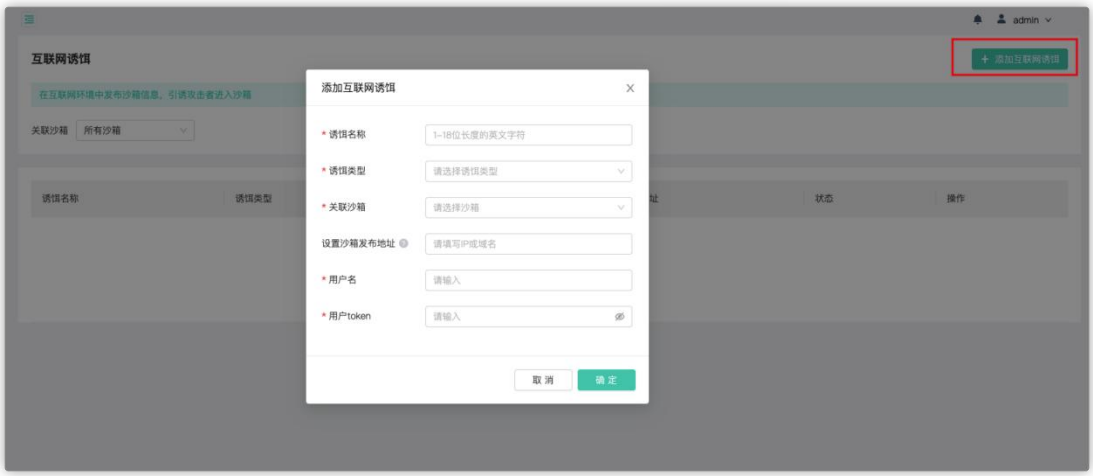


图 3-5-6-6 添加互联网诱饵

输入完成，确保 github 内容输入正确，点击‘确认’按钮，在诱饵列表会生成相应的诱饵记录，但还处于‘未发布’状态。勾选需要发布的互联网诱饵，点击‘发布’按钮，，状态变为‘发布中’，大约 5 分钟之后，状态变为‘已发布’，表示该条诱饵已经发布成功，可以对单条记录

进行‘编辑’和‘删除’操作，如下图互联网诱饵管理。

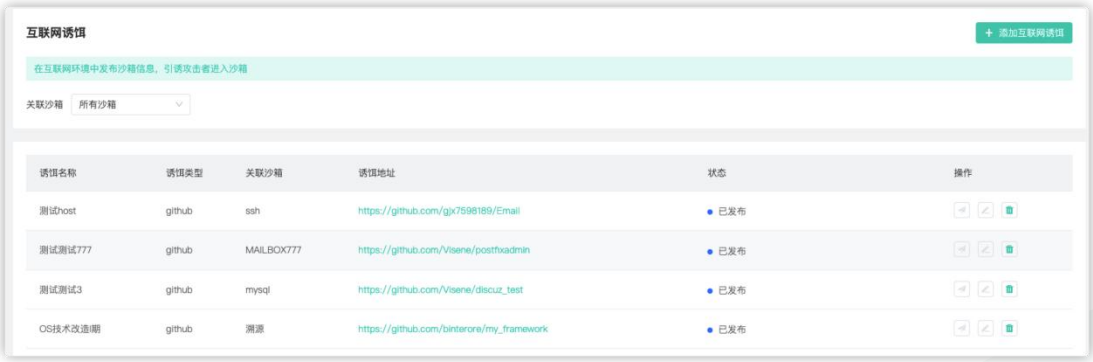


图 3-5-6-7 互联网诱饵管理

状态变为‘已发布’之后，访问诱饵列表中的诱饵地址，看到该页面下有该沙箱的相关信息，表示该条互联网诱饵发布成功，如下图互联网诱饵页面：

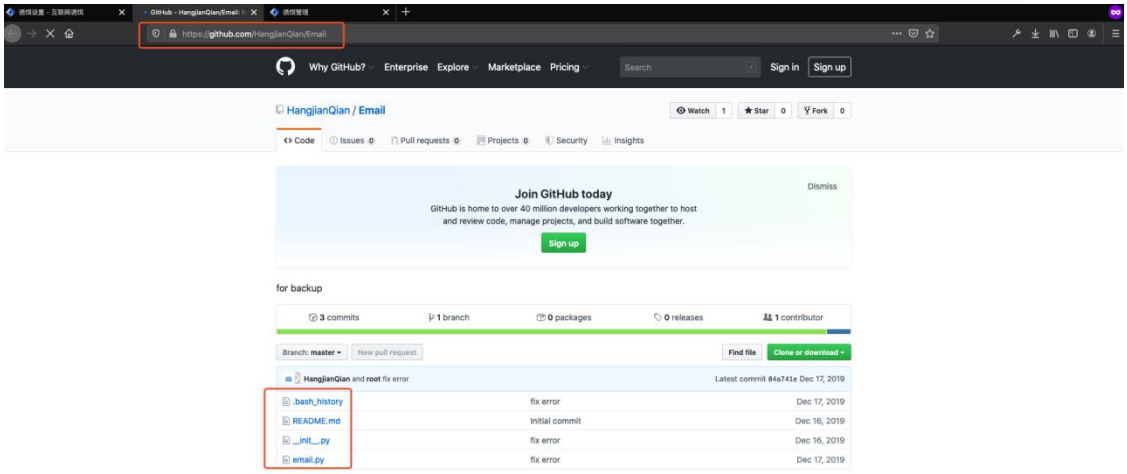


图 3-5-6-8 互联网诱饵页面

5) 主机诱饵

主机诱饵通过将用户编辑的虚假信息，散布到各个 Linux 主机上，迷惑攻击者。 关联伪装代理，将直接把主机诱饵下发至伪装代理主机上。点击【蜜网管理】—【诱饵管理】—【主机诱饵】—【添加主机诱饵】。

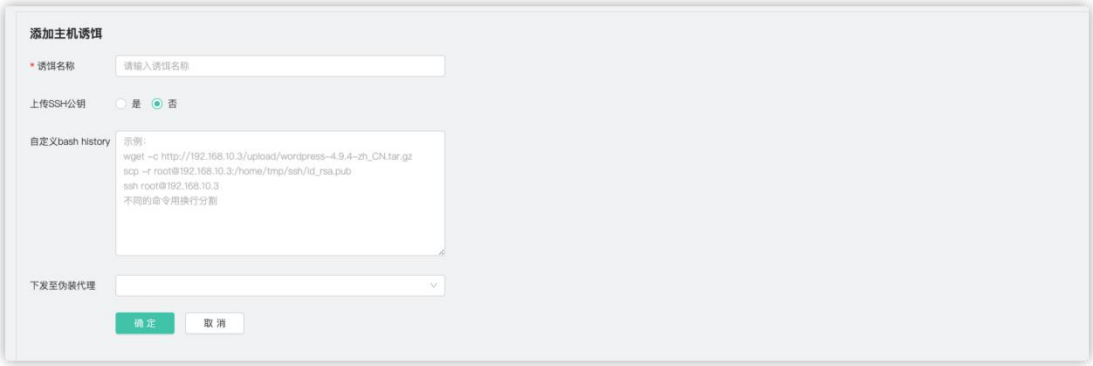


图 3-5-6-9 添加主机诱饵页面

诱饵名称自定义，选择是否上传 ssh 公钥，选择是会将伪装代理的公钥上传至 ssh 沙箱中（使用该功能需要为 ssh 沙箱关联 IP），自定义 bash history，选择下发的伪装代理。

当攻击者进入伪装代理之后，可以查看到用户提前伪装好的 linux 命令，将攻击者引入 ssh 沙箱中。

图 3-5-6-10 主机诱饵页面

6) 感知节点

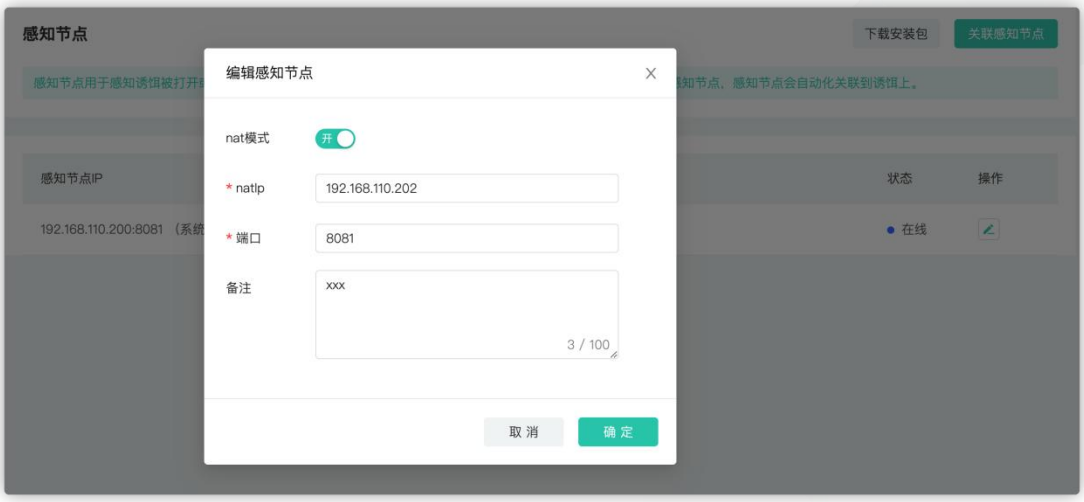
感知节点用于感知诱饵被打开或者攻击者触碰到的行为，用户可下载感知节点包，在存在诱饵的网络里安装对应的感知节点，感知节点会自动化关联到诱饵上。如下图所示。

图 3-5-6-17 感知节点

用户可以进行感知节点的添加和管理，点击右上角下载安装包，安装完成后即可安装，待安装完成后点击关联感知节点进行感知节点的关联，如下图所示。

图 3-5-6-18 关联感知节点

点击编辑，可开启 nat 模式，对于内网部署的感知节点映射到外网，填写 natIP 和端口



3.6 报表管理

3.6.1 威胁分析报告

威胁分析报告，用户可根据实际需求，选择特定时间段生成相关报表，报表内容主要包括：报表基本信息、综述、事件趋势分析图、沙箱攻击统计、黑客情报统计、攻击事件统计、资产受攻击统计等，生成报表时间 2 分钟左右，报表生成之后支持下载和在线查看。

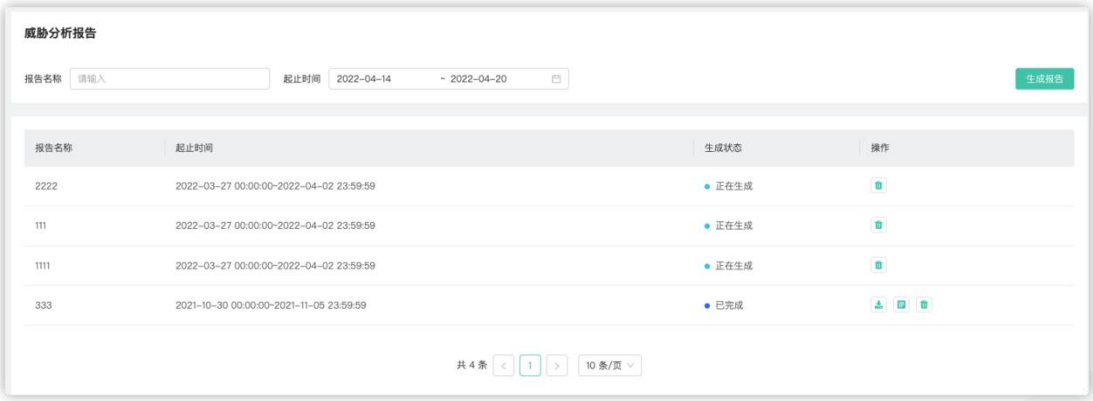


图 3-6-1 生成报表页面

3.6.2 攻击源分析报告

用户可按攻击源进行报告生成，报告包括攻击源的所有攻击事件。

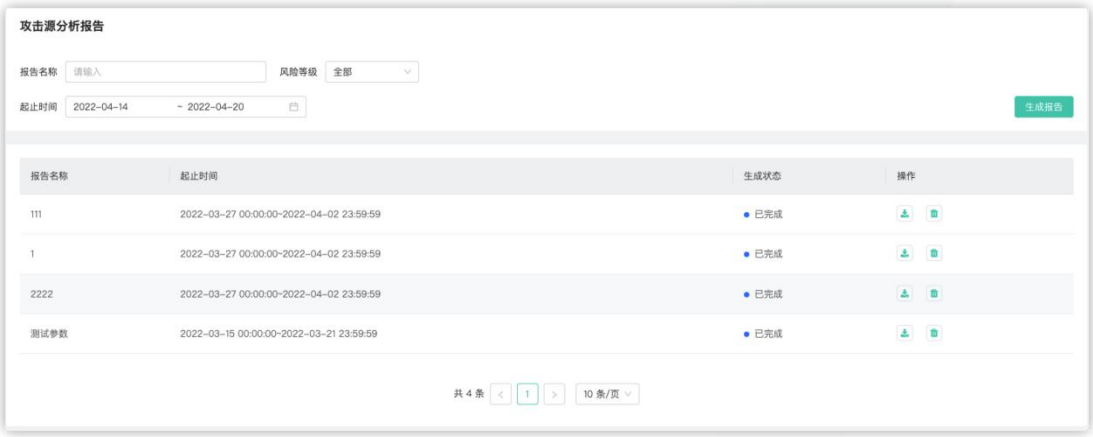


图 3-6-2 按攻击源生成报表页面

3.6.3 黑客画像报告

用户可按黑客画像进行报告生成，报告包括黑客设备指纹，IP，攻击链路等。

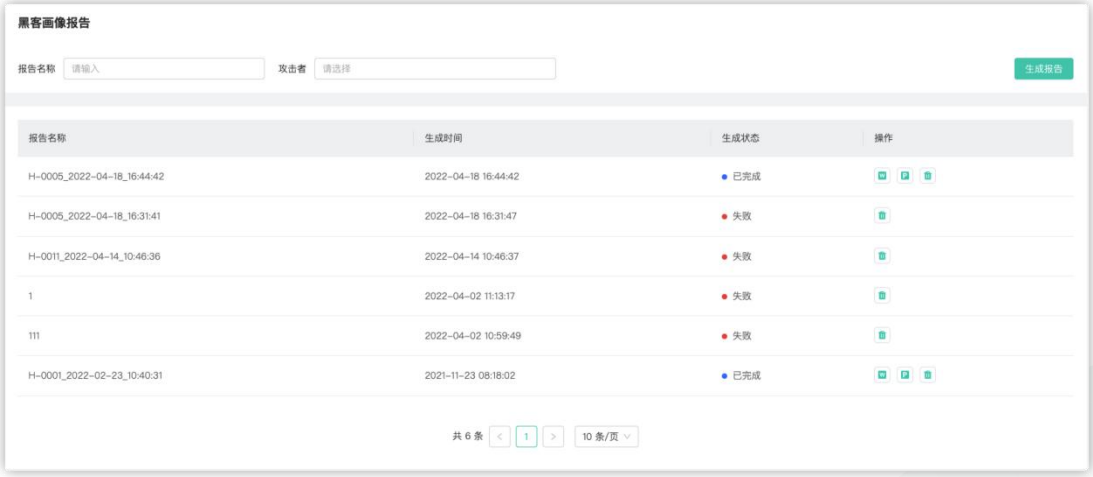


图 3-6-3 按黑客画像生成报表页面

3.6.4 行为分析报告

用户可按攻击者行为进行报告生成，报告包括沙箱名称、攻击者 IP、行为类型、起止时间、生成状态以及操作。

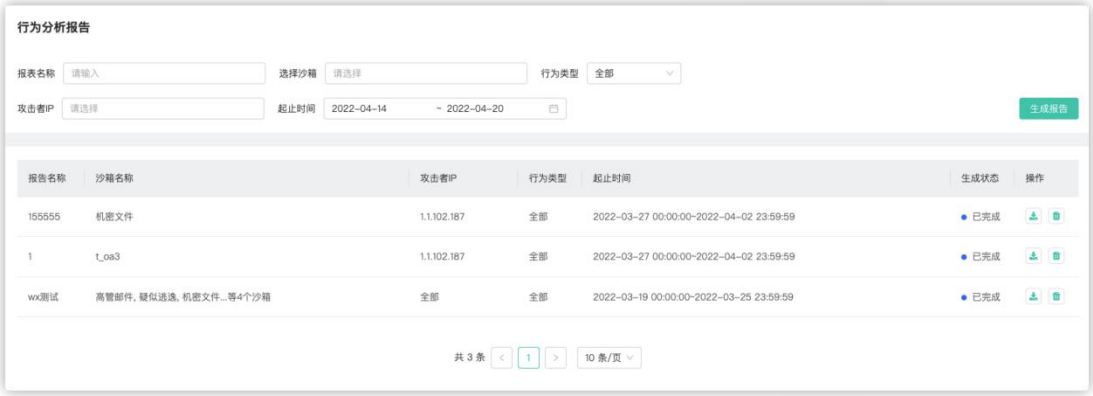


图 3-6-4 按攻击行为生成报表页面

3.7 联动配置

3.7.1 威胁情报中心联动

支持同本地威胁情报中心及云端威胁情报中心进行联动。获取的数据会基于相同的设备指纹从威胁情报中心同步信息，在【黑客画像页面】->【情报联动数据】，展示某设备指纹关联到情报中心的黑客 ID，ID 来自威胁情报，点击 ID 可跳转到情报中心对应的 ID 详情页。

对于本地的威胁情报的数据，用户可以自定义设置推送时间、地址。定时发送给本地的情报中心。

如果想要获取更多的威胁情报，用户需要打开云端威胁情报同步及获取更多威胁情报的开关，填写公司名称、公司官网、所属行业，点击保存之后即可获取更多情报。公司名称、公司官网、所属行业会同步订正【账号管理】处信息。

对于没有成功传输到云端的威胁情报，支持用户对威胁情报数据下载，手动导入。

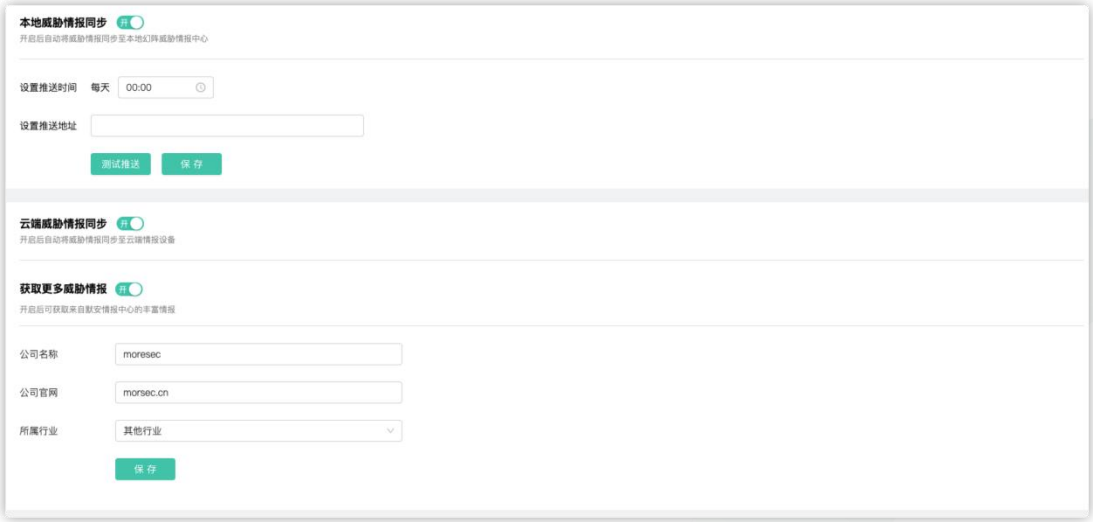


图 3-7-1 威胁情报中心联动界面

3.7.2 安全运营平台联动

支持与 MSS 安全运营平台进行联动。通过私有协议主动上报行为数据至 MSS 安全运营平台，对原始行为进行筛选，精准发现安全威胁，提高安全事件的检出率和监测准确率；MSS 平台通过升级监测机制对幻阵版本进行策略判断，并运用 AI 计算最短升级路径，通过访问密钥对安全设备进行在线升级

幻阵联动安全运营平台的配置界面如下，用户先在 MSS 平台-联动配置处添加幻阵产品的 ak/sk 等基本信息，然后在幻阵-平台联动处通过填写正确的安全运营平台的地址点击确定后，即可完成注册。

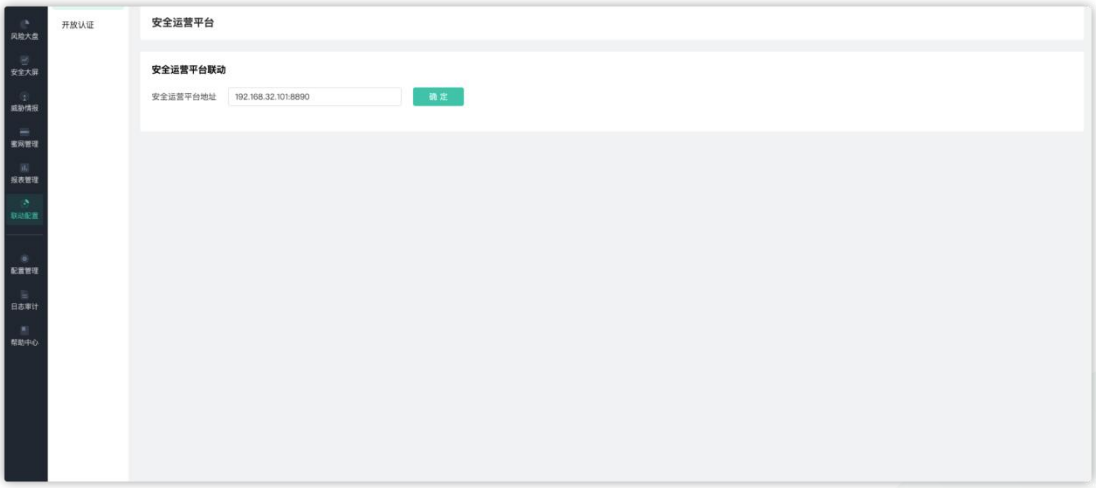


图 3-7-3 安全运营平台界面

3.7.3 日志同步

通过配置 SYSLOG 服务器地址（默认端口为 514），默安幻阵会对每一次攻击行为的详细信息以日志的形式发送到该服务器。配置界面如下图 日志同步界面所示，填写 SYSLOG 服务器 IP 地址后点击'发送测试'，大概 10 秒后，页面会提示'是否成功'；点击【保存】即可生效；普通用户只能看到相关信息，不能对日志同步界面进行操作。

图 3-7-4 日志同步界面

3.7.4 情报联动

情报联动包括了攻击 IP 的联动和恶意文件的联动，当有新的 IP 地址对沙箱发起攻击时，攻击 IP 联动会同步发送恶意的 IP 地址信息到对应接口，当有攻击者上传病毒木马等恶意文

件时，恶意文件联动会同步发送恶意文件路径信息等到相应的接口，二者都以 HTTP POST 方式发送 JSON 格式的数据到 HTTP 服务器。如果需要启用该功能，用户需要先搭建相应的 HTTP 服务器来接受同步数据。配置界面如下图所示，在相应栏中填入配置好的 HTTP 服务器的地址后点击'发送测试'，大概 10 秒后，页面会提示'是否成功'；点击【保存】即可生效。

图 3-7-5 情报联动界面

3.7.5 开放认证

开放认证可以支持幻阵与其他平台进行联动。通过点击添加平台，输入平台地址、AccessKey 和 SecretKey，可获取相应平台的对应 AK 的 API 权限，以此与其他平台进行联动。如果需要使用该功能，用户需要购买刃甲或其它平台设备。

添加完成后，可在界面上对 AccessKey 进行复制，点击验证按钮，输入验证码和管理员密码可查看完整 SecretKey，还可以进行删除操作。

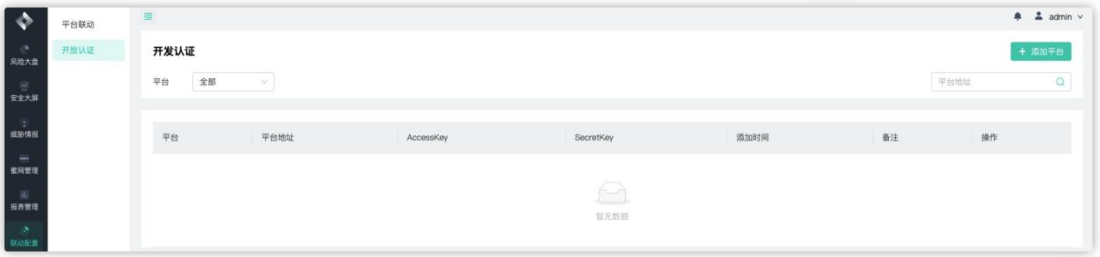


图 3-7-5 开放认证界面

图 3-7-6 添加平台界面

3.8 配置管理

3.8.1 账号管理-基本信息

界面展示了当前账户的个人信息、公司信息;个人信息包括用户名、类型、邮箱、电话、创建时间、密码强度; 公司信息包括公司名称、公司官网、所属行业;

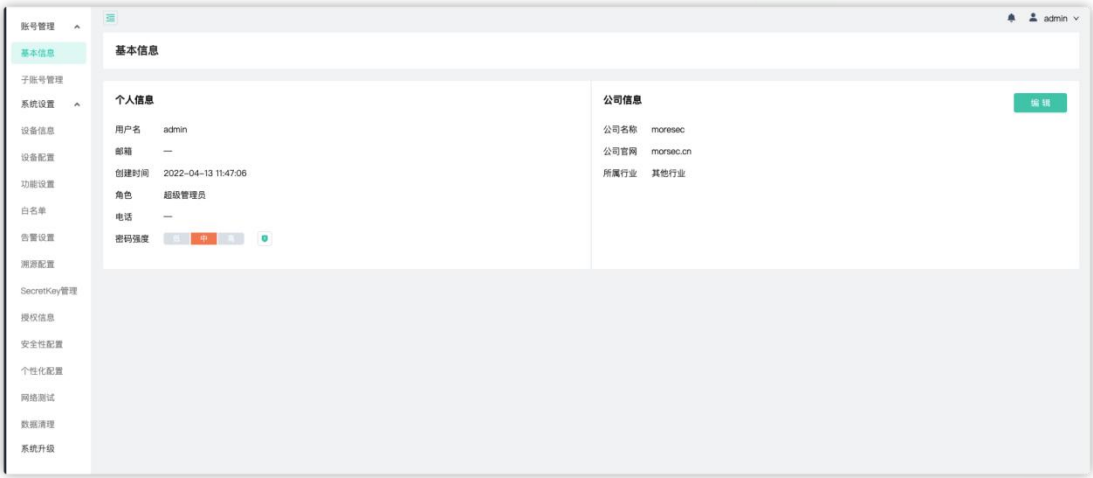


图 3-8-1 账号管理

页面可以修改个人信息和公司信息，点击编辑，修改个人信息。

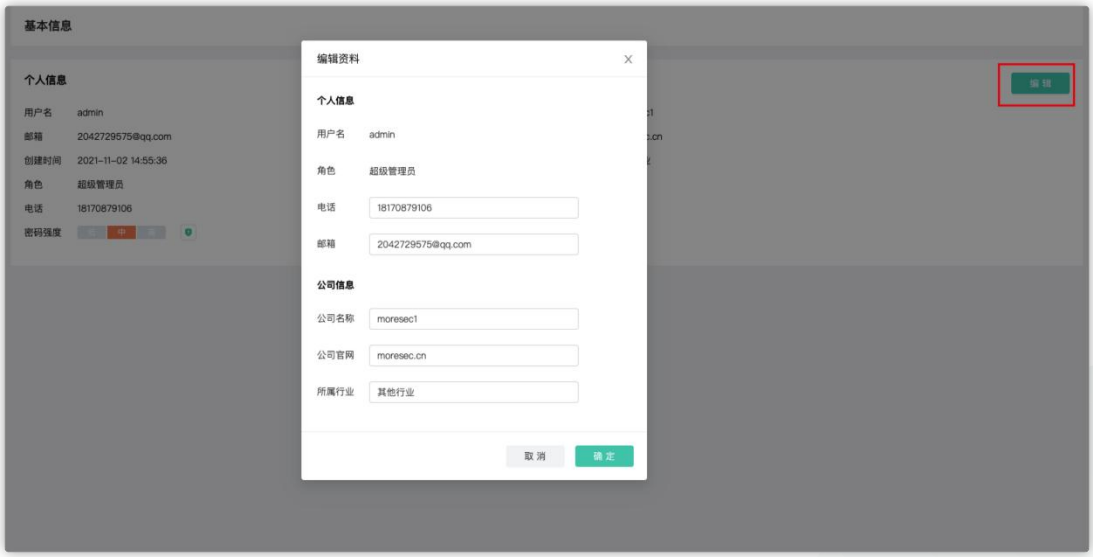


图 3-8-2 编辑个人信息

页面可以修改，点击 修改密码按钮，修改密码。

图 3-8-3 修改密码

3.8.2 账号管理-子账户管理

子账号管理包括子账户用户名、创建时间、认证方式、允许登陆地址、邮箱、电话、角色以及操作。

超级管理员可根据实际安全管理需求，添加管理员权限用户、普通用户和审计员并可指定认证方式和其允许登陆地址，如图 3-8-4 添加用户界面。

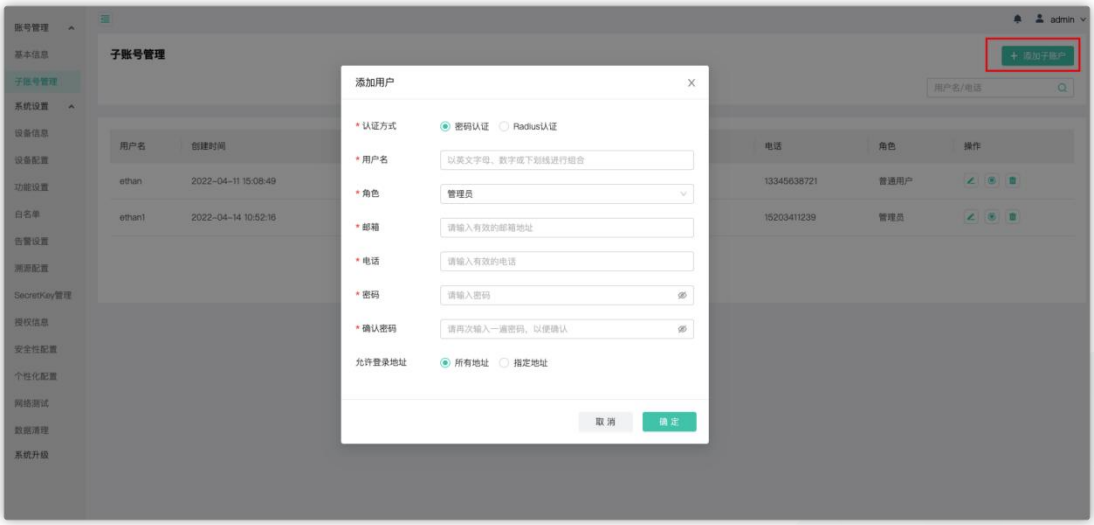


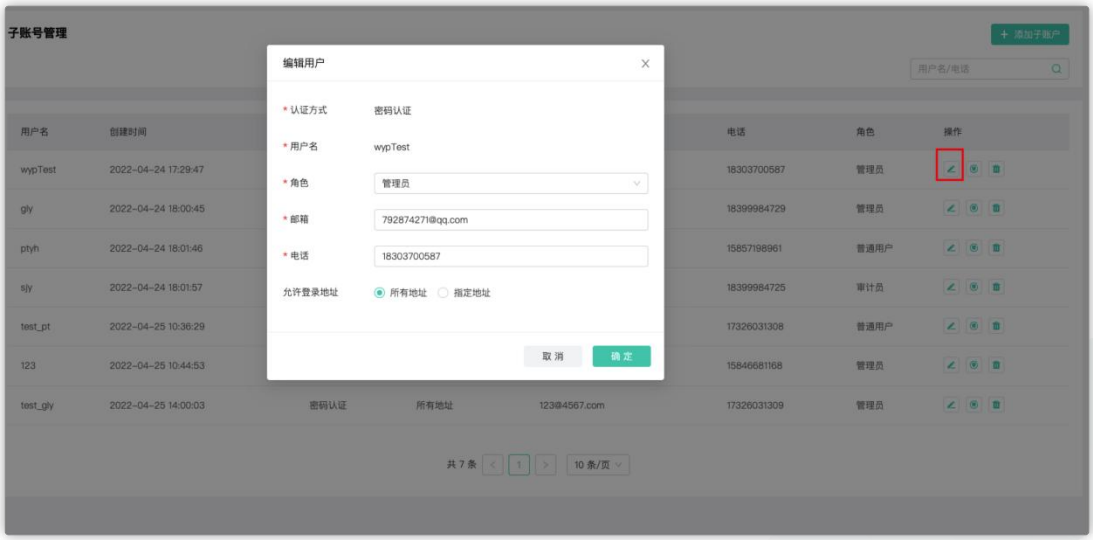
图 3-8-4 添加用户（所有用户）

界面下方的子账号管理列表，会将添加的用户展示到列表中，并可对子账号进行管理。在子账户管理列表的右上方，具有模糊搜索功能，可以对用户名/电话模糊搜索。子账户管理列表下方，具有翻页功能，默认每页展示 10 条。如下图所示：

图 3-8-7 子账号管理

权限分配为：超级管理员可进行一切操作，管理员不可以对任何功能和数据进行删除操，普通用户只可以查看数据，审计员仅可查看个人信息，查看下载日志。

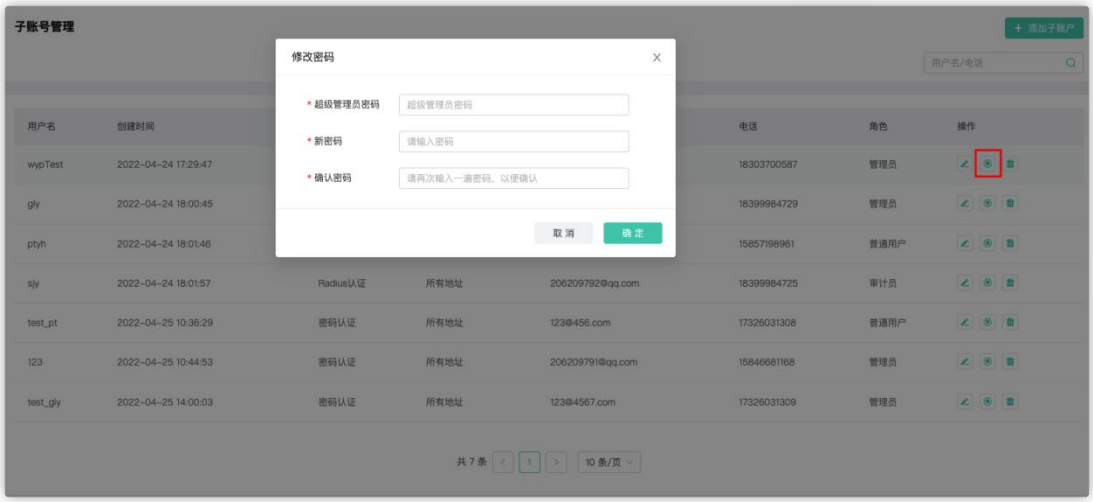
超级管理员可以编辑子账户信息，包括修改子账户角色、邮箱、电话、允许登录地址等，如下图所示。



超级管理员可根据实际安全管理需求，‘’删除用户；如下图删除用户界面。

图 3-8-8 删除用户

超级管理员可重置子账户密码，点击“重置”按钮，输入超级管理员的密码和重置后的新密码；如下图所示。



3.8.3 账号管理-授权信息

授权信息包括设备指纹、产品到期时间、license 版本、伪装代理上限、沙箱上限、产品序列号。

3.8.4 系统设置

1) 设备信息

设备信息页面展示默安幻阵所有设备的基本情况，其中支持沙箱数量表示该设备最多可创建的沙箱数，当前沙箱数量表示当前已创建的沙箱数，正在运行沙箱数，正在初始化沙箱，以及该设备下所有沙箱信息。如下图设备配置；普通用户只能看到相关信息，不能对设备进行重启操作。如果需要重启某台设备，可选择需要重启的设备，点击重启按钮，设备重启需要五分钟左右，重启设备之前建议停用所有与该设备相关的沙箱。

虚拟 IP 为幻阵高级模式配置的 natIP。

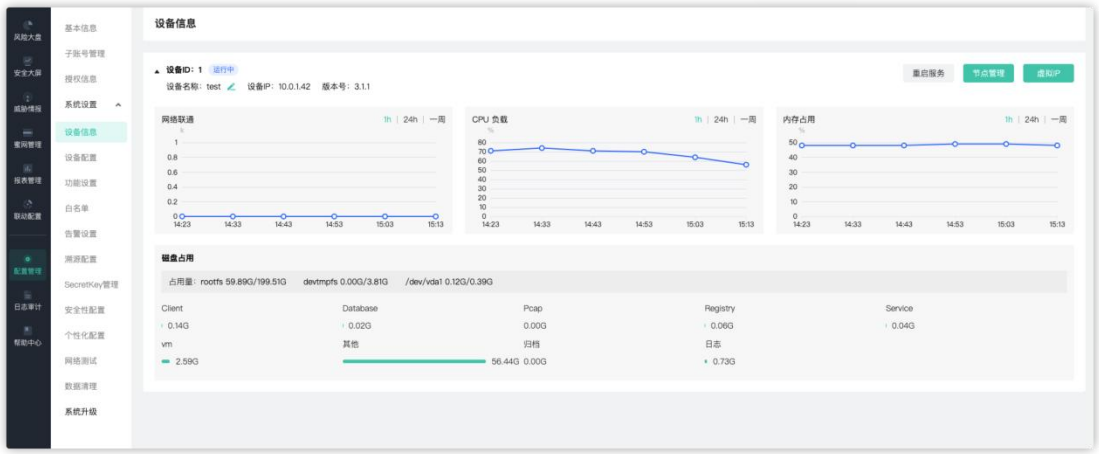


图 3-8-9 设备信息

节点管理页面（仅云化版支持）展示客户端设备下节点卡片信息，包括节点 IP、节点版本、节点状态、节点标签、Docker 网络、节点资源占用和硬盘占用；

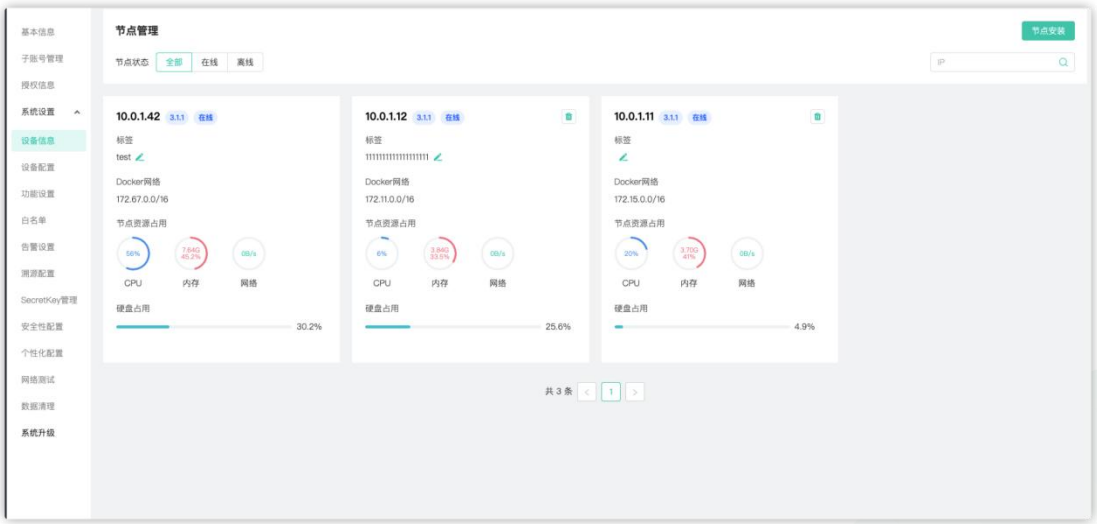


图 3-8-9-1

点击【节点安装】按钮可下载节点，节点安装仅支持 linux 操作系统，支持离线下载安装或复制执行命令进行安装，安装成功后，对应节点将在节点管理页面上线。

图 3-8-9-2

2) 设备配置

设备配置包括修改系统时间、下载系统运行日志、一键诊断和 pcap 包下载功能，如下图所示。

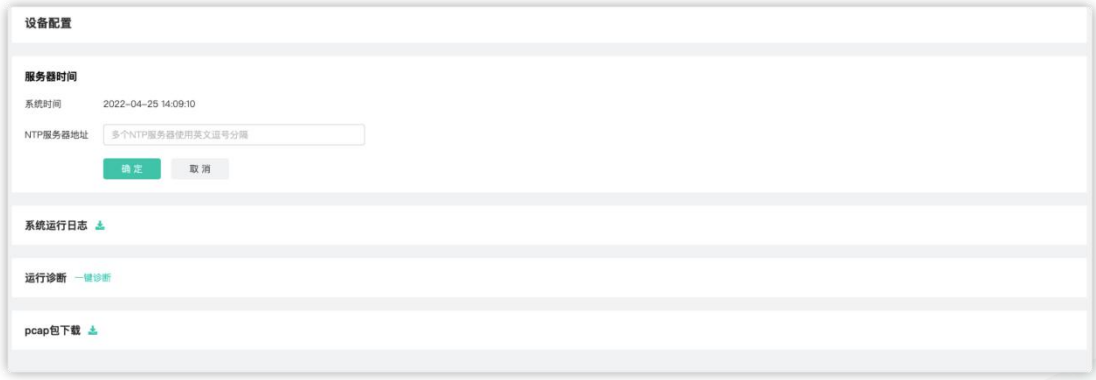


图 3-8-10 设备配置

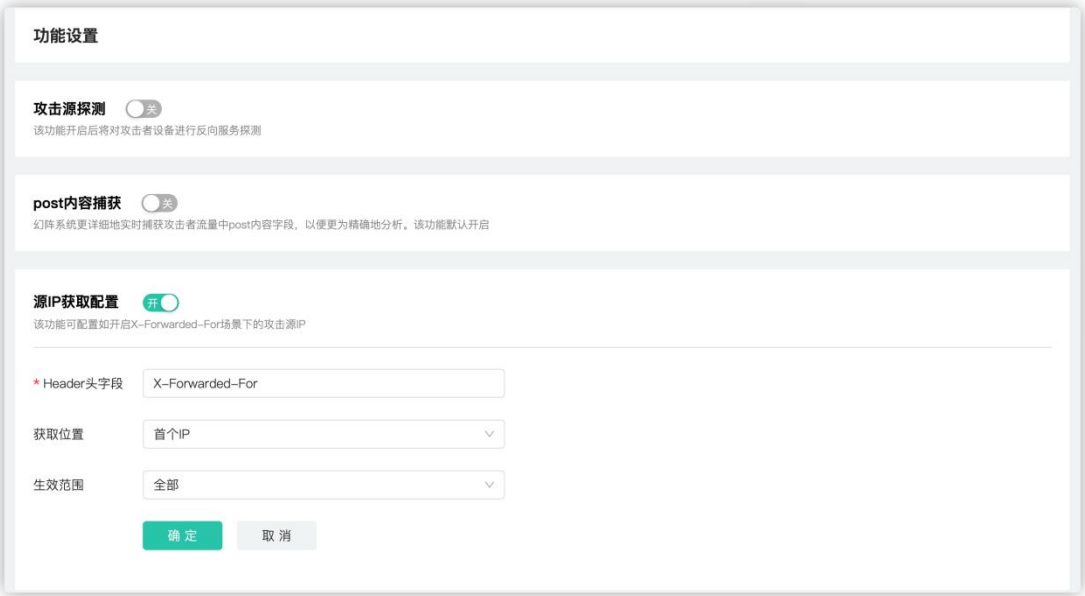
3) 功能设置

功能设置包含【攻击源探测开关】、【POST 内容捕获】、【源 IP 获取配置】、【认证配置】；

【POST 内容捕获】：当开启该开关时，会捕获攻击的 post 数据，反之关闭该开关，将不捕获 post 数据；

【攻击源探测】：可根据用户需求选择开关，此开关开启之后幻阵会反向探测攻击者的信息；

【源 IP 获取配置】：用户可自定义获取攻击源，若关闭获取 header 头，则直接获取沙箱上一条 IP，当沙箱通过负载均衡映射的情况下，需要开启获取 header 头，幻阵会获取指定 header 头字段作为攻击者源 IP。用户也可使用生效范围，对特定源 IP 的流量获取 header 头作为攻击源。



【Radius 认证配置】:用户可以配置 Raduis 认证服务器，配置认证端口，输入 Raduis 服务器的地址，填写共享密钥后，点击【保存】，配置生效。

【Ldap 认证配置】:用户输入服务器地址、认证账号、认证密码、用户搜索基准、用户规律规则、用户属性等配置后，点击【保存】，配置生效。

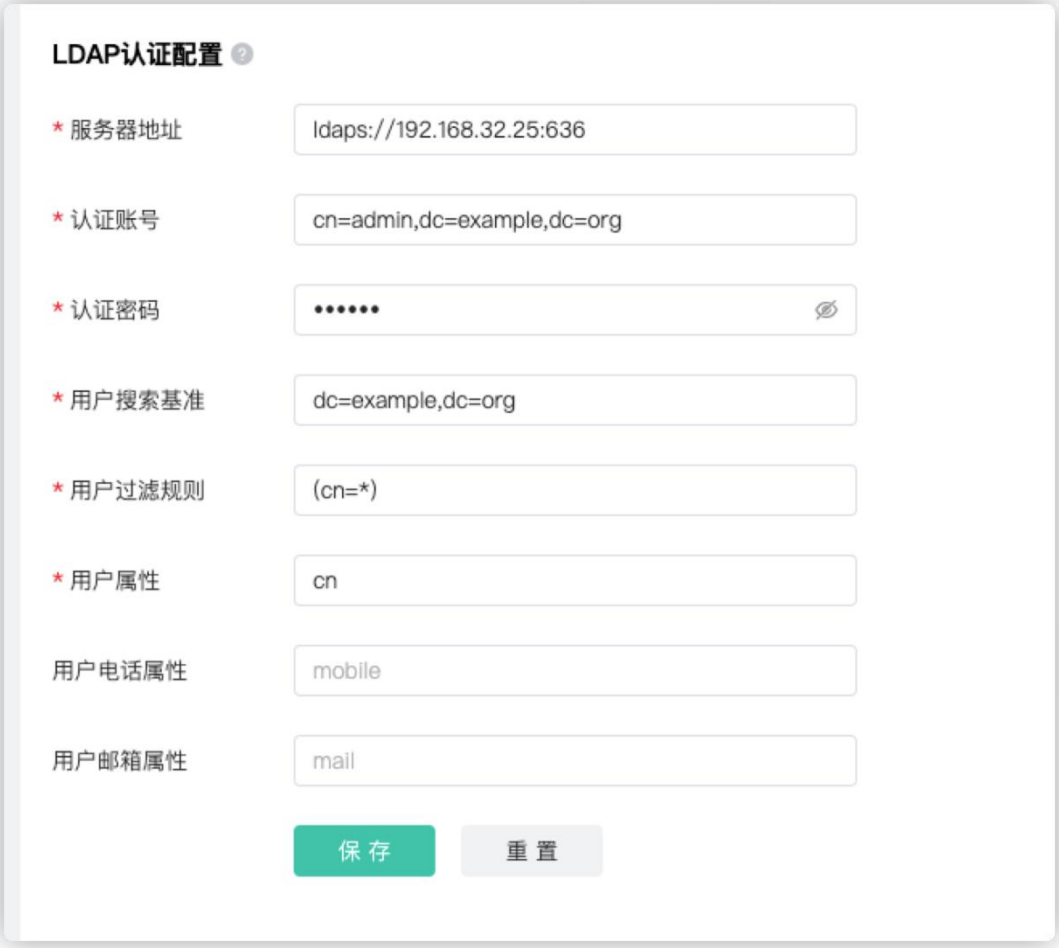


图 3-8-14 功能设置界面

4) 白名单

超级管理员可设置扫描白名单和系统白名单，加入扫描白名单的 IP 如果对默安幻阵的沙箱、伪装代理等进行了扫描或者手工渗透等，默安幻阵将不记录事件和产生告警；加入系统白名单的 IP 才能访问默安幻阵管理页面。页面可对白名单进行添加、修改、删除操作。逃逸检测白名单中的 IP 出现攻击逃逸，系统不会捕获其行为。加入流量阻断白名单中的 IP 将会放开白名单地址中的流量阻断限制。

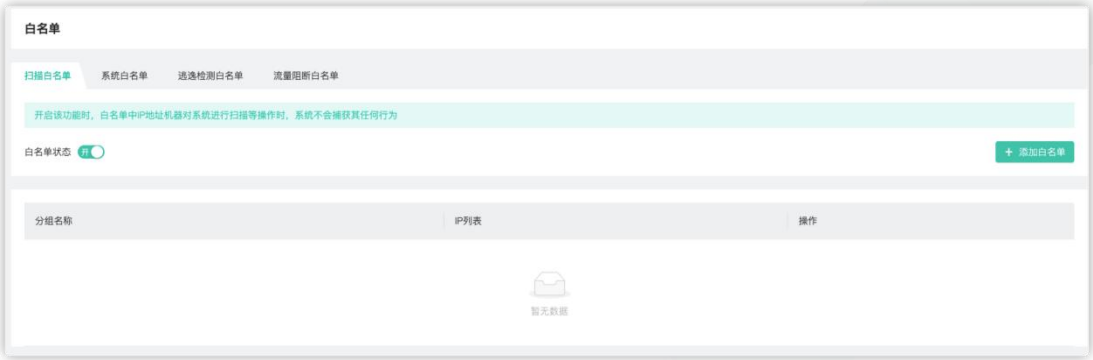


图 3-8-12 白名单界面

添加白名单，输入相关信息之后，点击确认进入白名单管理界面，状态变为‘开’时，表示白名单开启。

图 3-8-13 添加扫描白名单界面

5) 告警设置

告警包括系统异常状态告警和入侵事件告警，当默安幻阵系统出现异常状态时会通过配置的邮箱信息实时发送告警邮件，入侵事件告警根据配置的告警频率，以该时间间隔为单位

监测是否有入侵事件发生，如果有则会发送最近的 10 条入侵事件至设置的接收者邮箱告警。配置界面如下图告警界面所示，填写发送邮件的用户、邮箱服务器信息和接收邮箱等信息，点击【确定】即可生效；普通用户只能看到相关信息，不能对告警页面进行操作，告警设置同时还会同步到消息中心。

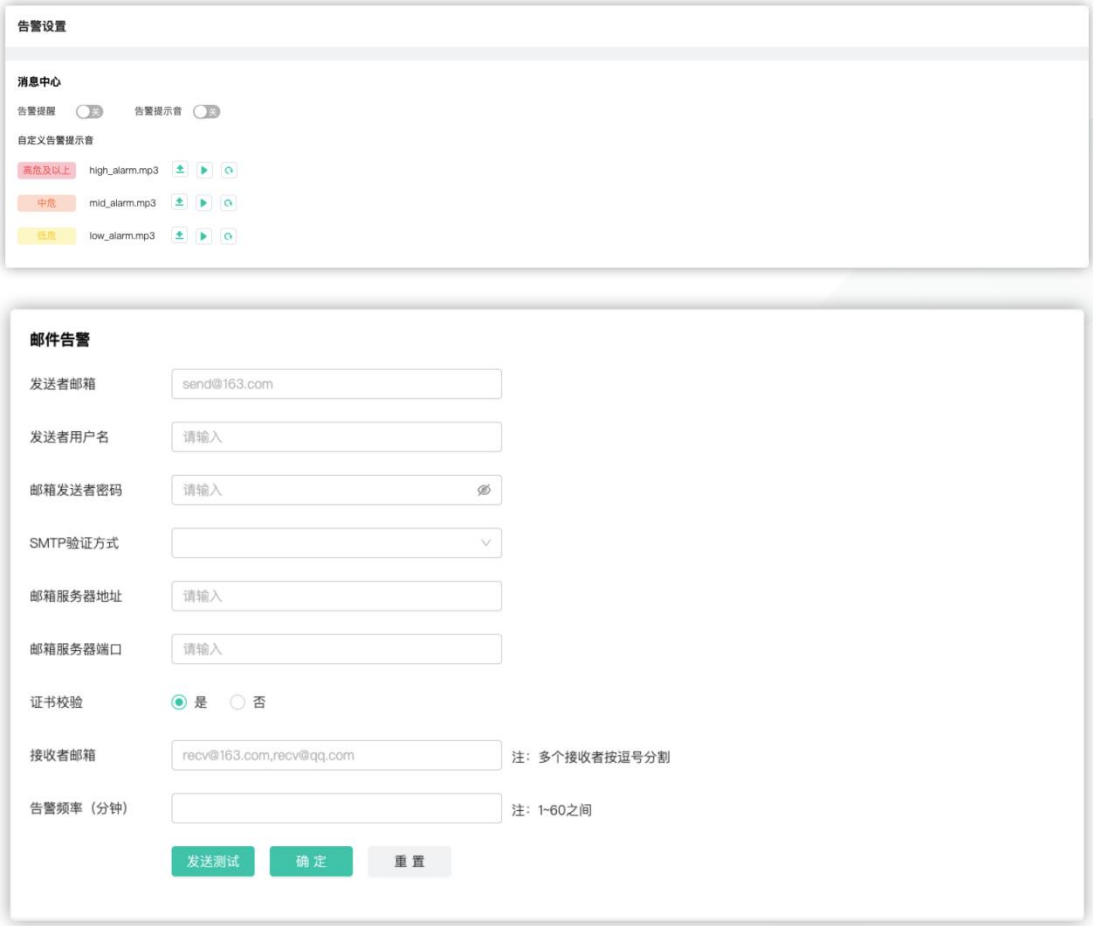


图 3-8-11 告警界面

6) 溯源配置

用户可自定义配置溯源函数，参照左边溯源函数示例模式，每个网络 id 获取后进行 return 即可，当前可直接使用溯源示例函数。同时用户可自定义溯源模块生效时间，可全部生效，也可选择某天的某个时间段和每周的某个时间段生效。

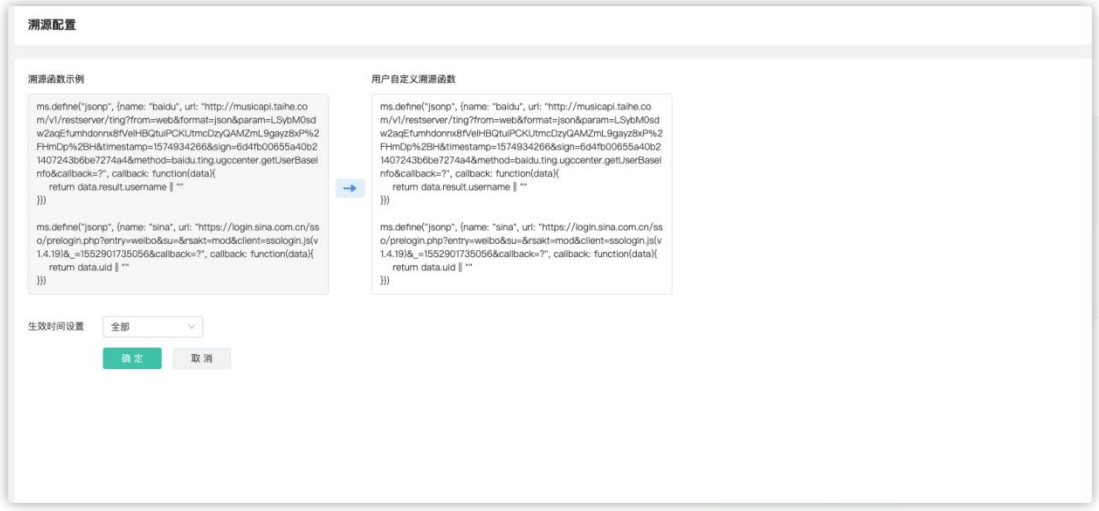


图 3-8-18 溯源配置

7) SecretKey 管理

幻阵与刃甲进行联动时需要填写 SecretKey，一个 SecretKey 可以对应一个刃甲，也可以多个刃甲使用同一个 SecretKey。用户可以进行 SecretKey 的添加，复制以及删除操作。

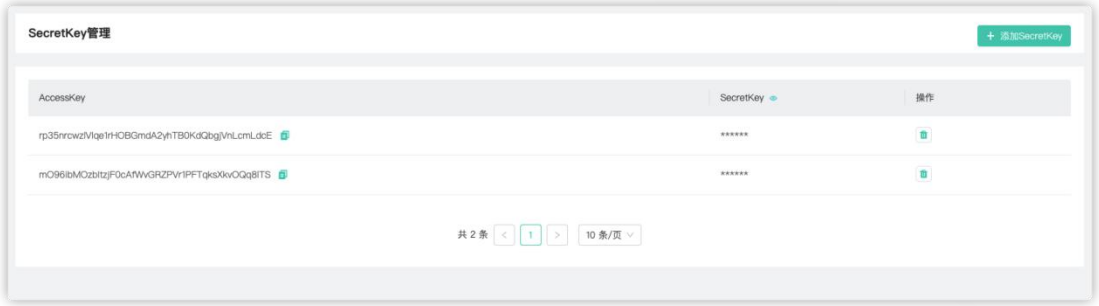
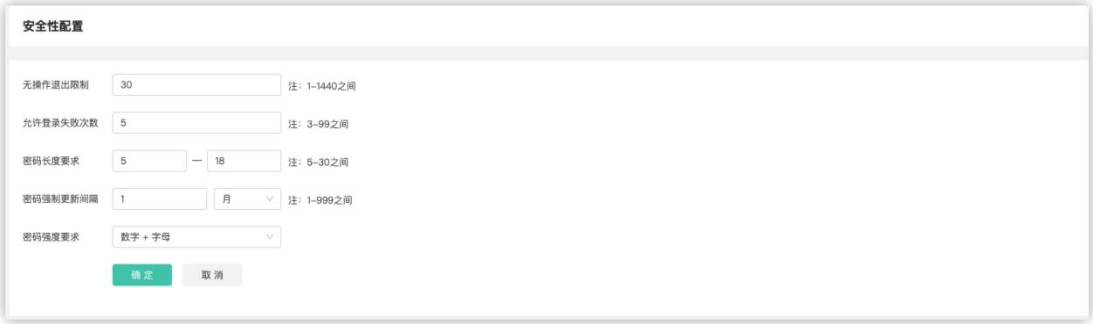


图 3-8-21 SecretKey 管理

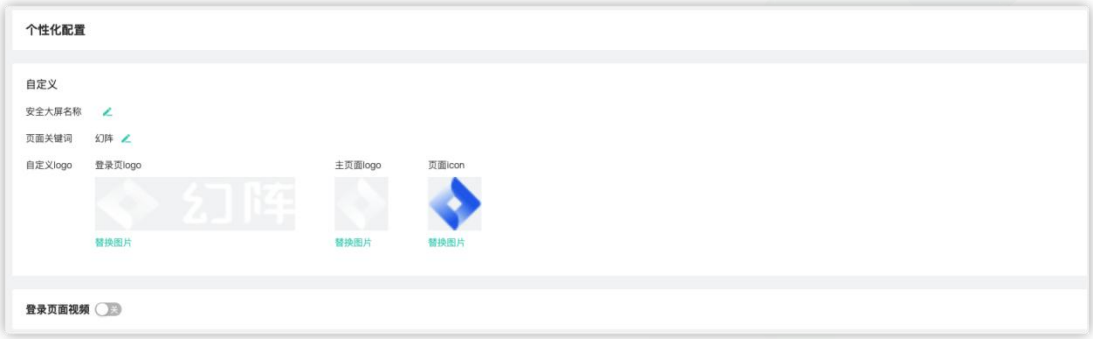
8) 安全性配置

安全性配置可以设置允许登陆失败次数、密码长度要求、密码强制更新间隔以及密码强度，修改安全性配置后，若现用密码不符合安全性配置的要求，在下一次登录时需修改密码；



9) 个性化配置

包含【安全大屏名称】，【自定义 logo】，【页面关键词】
【安全大屏幕名称】可自定义名字
【自定义 logo】可上传登录页面，主页面 logo，以及页面图标;
【页面关键字】也可用户自定义，



10) 网络测试

网络测试功能提供 ping、traceroute、route、curl、arp、telnet 命令，方便安装测试人员进行现场网络排查。

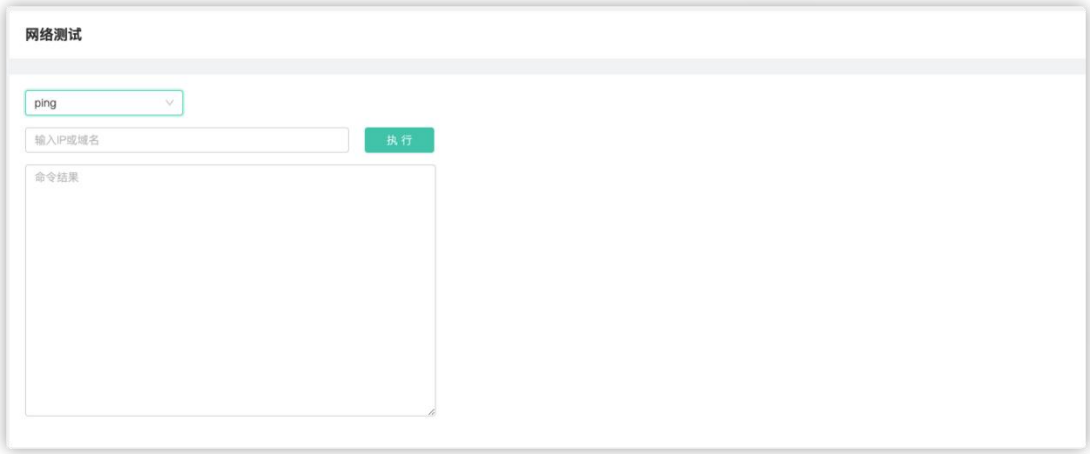


图 3-8-20 网络测试

11) 数据清理

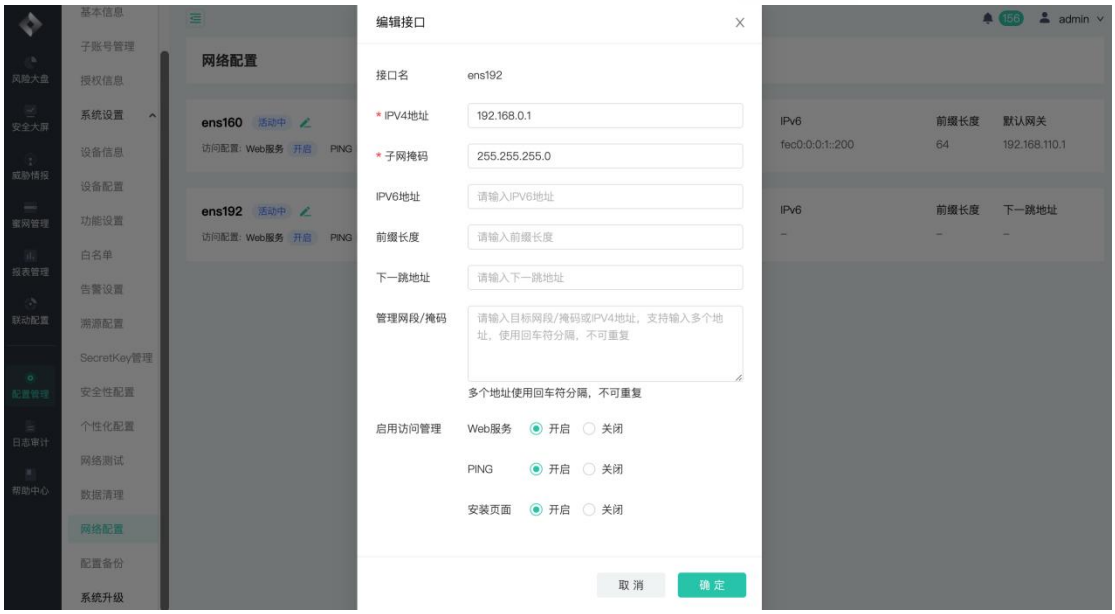
用户可以对幻阵数据进行清理。支持按照事件等级、攻击者类型、攻击时间（默认近七天数据不可删除）进行筛选后进行数据清理。

图 3-8-22 数据清理

12) 网络配置（仅标准版支持）

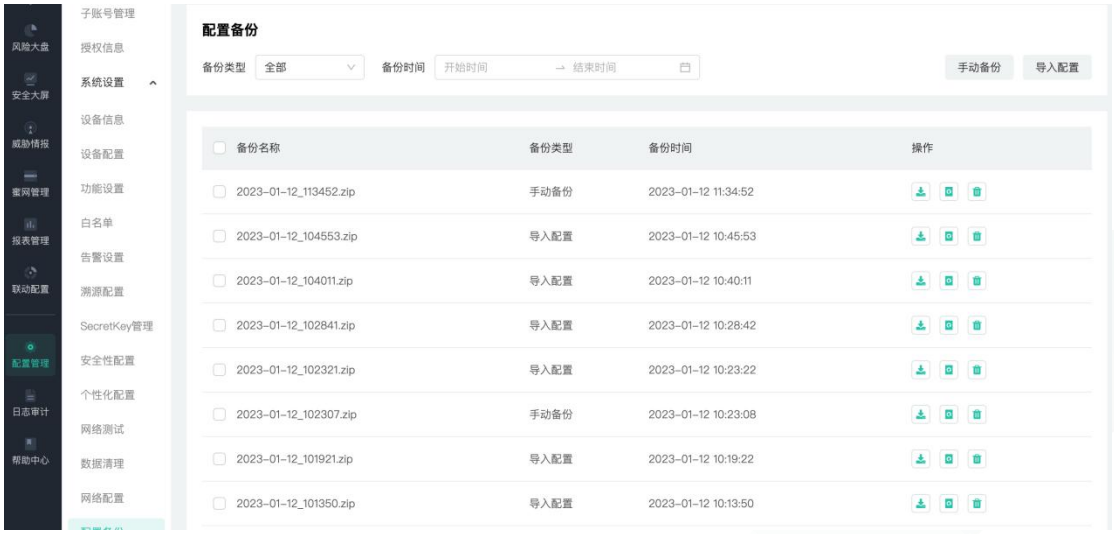
网络管理页面可查看业务口的网络管理信息，包括网卡名称、IPv4 地址、子网掩码、IPv6 地址、前缀长度、默认网关等；

此外还可进行带外管理配置，对管理口配置 IPv4d 地址、子网掩码、下一条地址、开启 web 服务后，点击确定，即可配置成功；PING 服务关闭后，对当前网卡的 IP 地址进行禁 PING 处理；关闭安装页面后，将无法访问安装页面。



13) 配置备份

配置备份页面支持备份系统配置，点击手动备份后，生成一条备份记录，生成的备份记录支持下载、恢复与删除；下载的数据支持导入配置。



3.8.5 系统升级

该页面可显示当前版本，版本更新概要以及历史版本

用户可点击【选择文件】按钮选择更新的文件压缩包，等待上传完成后进行升级，此过程耗时较长，且此过程是自动进行，出现“上传 100%”字样后会有较长时间停留，请耐心等待，升级成功后，在历史版本中可见新的升级记录；

图 3-8-23 系统升级界面

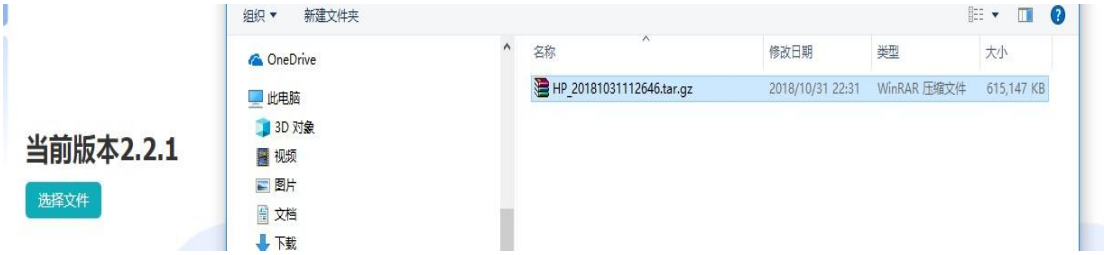


图 3-8-24 选择上传文件页面

图 3-8-25 上传文件界面

图 3-8-26 初始化界面

图 3-8-27 管理端更新完成界面

图 3-8-28 升级完成界面

点击  图标可查看升级详情，如下图所示：

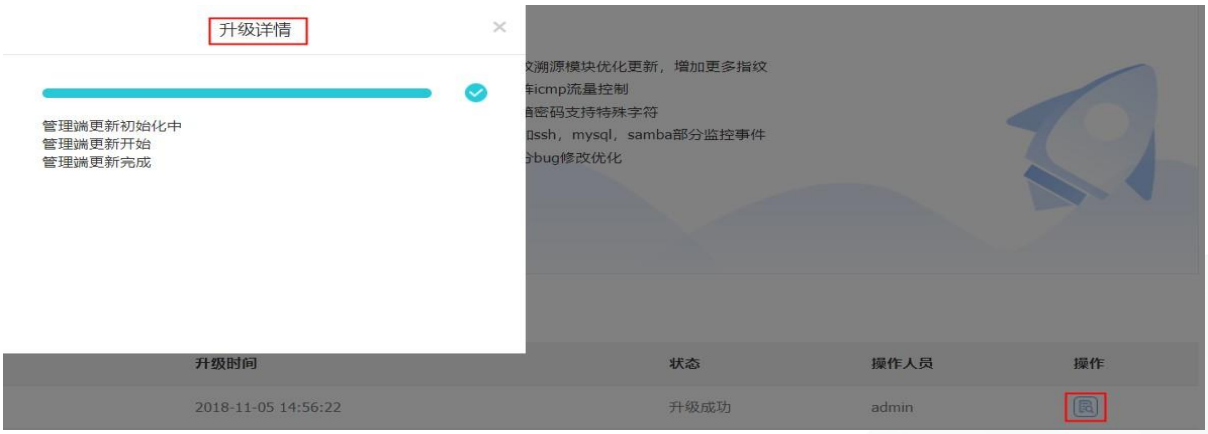


图 3-8-29 升级详情界面

3.9 日志审计

日志审计页面只有超级管理员可以清空日志，审计员有权限查看相应审计信息，日志审计页面会详细记录如下图日志审计页面包括登录用户、登录 IP、所有账户操作事件（包括添加用户、用户登录、用户注销、删除用户），以及审计时间；日志审计页面提供清空日志、下载 xls 日志报表、以及查询功能，超级管理员可以看到所有用户的操作记录。

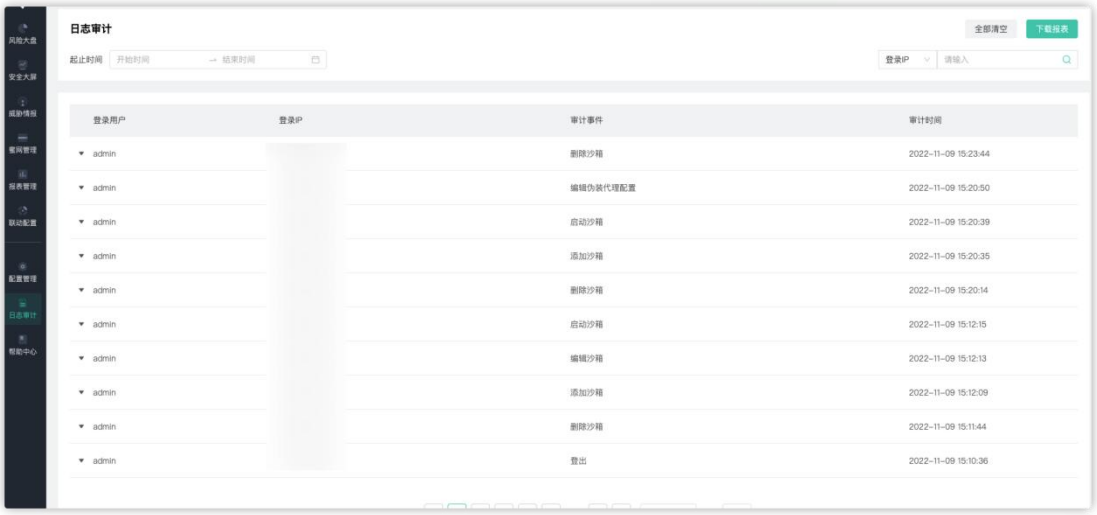


图 3-9-1 日志审计

3.10 帮助中心

帮助中心页面分为新手引导、产品文档以及免责声明页面。

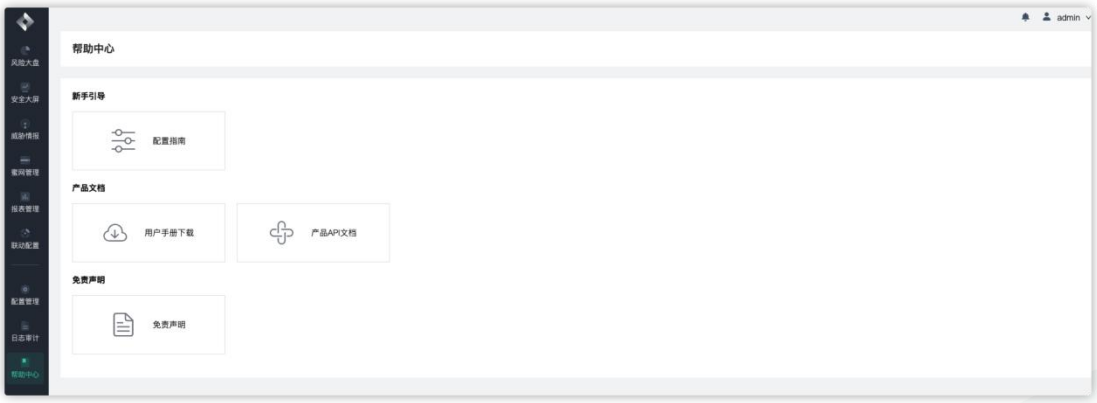


图 3-10-1 帮助中心页面

用户可以点击新手引导->配置指南查看幻阵基础配置及使用手法。

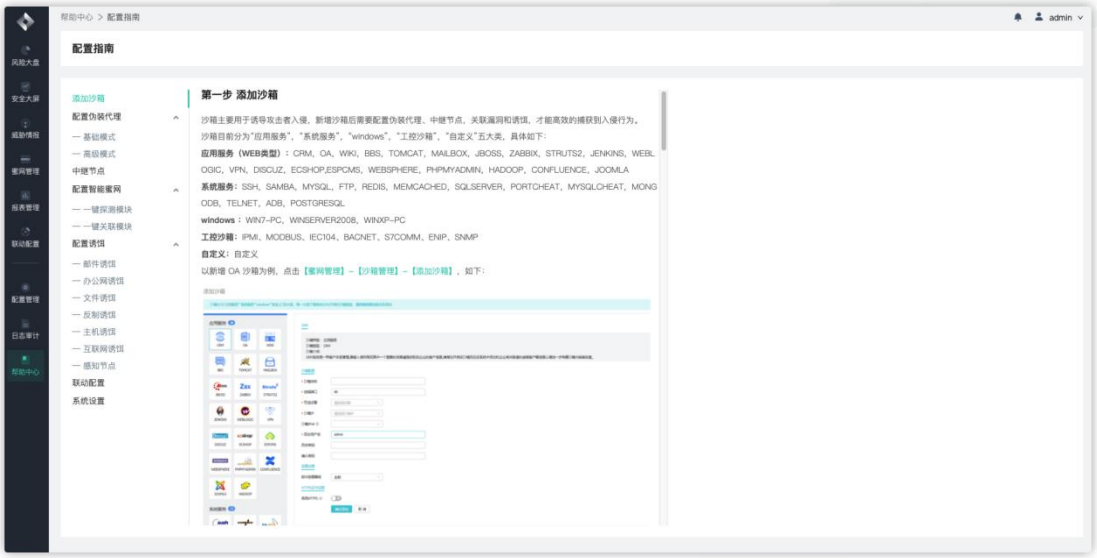


图 3-10-2 配置指南页面

不同权限的用户可以下载相对应权限的用户手册，超级管理员可以查看和下载产品 API 文档。

图 3-10-3 产品文档界面

用户可以点击免责声明查看杭州默安科技有限公司的免责声明文档。

图 3-10-4 免责声明界面

3.11 消息中心

消息中心用来展示相关攻击行为的告警，分为全部消息，处理消息以及已处理消息。使用者可以根据风险等级进行筛选，并且可以一键忽略全部消息或忽略中危低危消息。点击详情“”便会跳转到攻击事件回放页面，点击处理“”弹出消息处理弹窗，如下图所示，使用者可以加上处理意见，点击忽略“”即可忽略攻击消息。

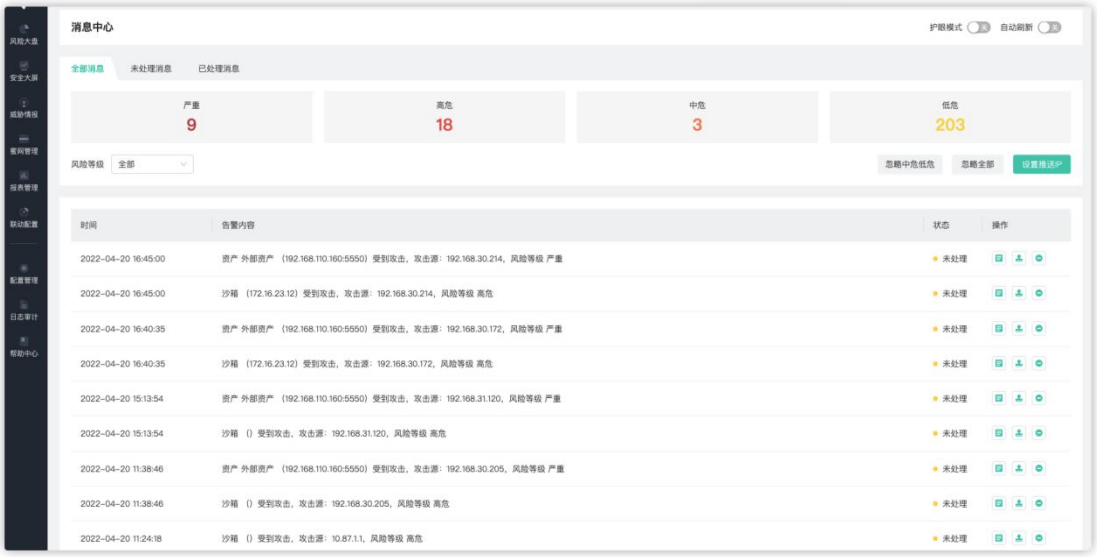


图 3-11-1 消息中心

图 3-11-2　消息处理

附录 A 自定义沙箱部署说明

i.　自定义沙箱说明

定义沙箱主要是为了用户根据自己的需求在自定义虚拟机里面部署仿真业务系统，仿真业务系统主要用于模仿用户真实业务站点，吸引攻击者入侵。

自定义沙箱为 linux 系统的虚拟机，自带 apache 和 ngnix 反向代理。

ii.　自定义沙箱部署

a）　新建自定义沙箱

在默安幻阵 web 管理云端新建一个自定义沙箱，记住自定义沙箱的 IP 地址、用户名和密码。

b）　查看修改配置

- 登录自定义沙箱

  利用 ssh 登录自定义沙箱 ssh 用户名/密码

- 查看 80 端口

  输入命令：netstat -tnlp　查看 80 端口是否已经打开；

  打开为正常；如果 80 端口没有打开，可销毁沙箱之后，重新新建自定义沙箱。

- 修改 apache 默认 webserver 的监听端口（默认 apache 监听端口为 80;设置成：127.0.0.1:8000）

  cd /etc/httpd/conf

vim httpd.conf

/Listen 回车,找到 Listen 80;

#注释此行（shift+#），添加新行：Listen 127.0.0.1:8000（:wq 保存退出）

- 将网站资源拷贝至自定义沙箱的指定目录

  将 html 页面拷贝到：/var/www/html 下面（将下面命令行中的 192.168.100.100 修改为沙箱 IP）；

  linux：scp -r ［资源包文件目录］ root@192.168.100.100:/var/www/html/

  windows：安装 putty.exe 和 pscp.exe

  cmd 命令：pscp -scp ［本地文件路劲］root@192.168.100.100:/var/www/html

- 启动 apache

  httpd -k restart;

验证：配置完成之后，通过浏览器访问 http://192.168.100.100/1.html(1.html 为上传的文件名)，正常返回页面即可。