创宇蜜罐

威胁诱捕与溯源系统

用户手册 V1.6.0「私有版 V2.1.4」

（文档编号：MG-SY-2021-007）

文档说明

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属北京知道创宇信息技术股份有限公司（以下简称“知道创宇”）所有，受到有关产权及版权法保护。任何个人、机构未经知道创宇的书面授权许可，不得以任何方式复制或引用本文件的任何片断。

威胁诱捕与溯源系统用户手册 V1.6.0「私有版 V2.1.4」

北京市朝阳区望京 SOHO T3-A 座-15 层

SOHO T3-A Block-15, Wangjing, Chaoyang District, Beijing

客户热线（Customer Hotline）： 400-060-9587 / 010-57076191

传真（Fax）： 010-57076117

邮编（Post Code）： 100102

邮箱（Email）： sec@knownsec.com

文档更新记录

更新时间	文档版本	系统版本	更新内容
2021/03/24	V1.4	私有版 V2.1.3	新增：可视化模块、定制蜜罐、安全事件、中继模式、蜜饵管理、蜜罐监控 变更：蜜罐管理优化、攻击日志优化、白名单优化、安全策略配置
2021/04/07	V1.5	私有版 V2.1.3	变更：附录 1 优化
2021/05/31	V1.6.0	私有版 V2.1.4	新增：蜜罐场景模板、单 IP 多端口部署、IPV6 支持(5.1 节)、攻击者画像(处置、白名单、数据导出)(8.1 节) 变更：客户端管理(暂停、停止)(6 节)

目录

1. 产品介绍

近年来，随着攻防手段的不断演变，不论是交锋日益激烈的网络安全日常防护，还是常态化的网络攻防演练，高对抗性俨然成为了网络安全攻防的本质。市场在明确对抗重要性这一前提下，越发注重能够摆脱“原地等待被动挨打”现象的主动防御，而可以实现网络威胁诱捕与溯源的蜜罐技术就这样逐渐得到广泛关注。

每年的网络安全专项行动涉及关键信息基础设施的网络安全攻防演练参与者和攻击手段都在不断演变。随着各个行业信息化脚步的迈进，安全大考范围也逐步扩大，防守方选择的防护手段也在逐步升级，比如设置蜜罐就成为了企业改变网络攻防模式中的不对称性、实现从被动防御转变为主动防御的重要手段之一。

创宇蜜罐作为一款运用网络欺骗技术、通过故意混淆和误导来实现对高级威胁的检测和防御的产品，在保障蜜罐自身安全性的前提下，通过在攻击者必经之路上构造陷阱，混淆其攻击目标，诱导攻击者进入与真实网络隔离的蜜场，让攻击者在蜜场中消耗大量精力，留下攻击痕迹。它能够对入侵行为进行实时告警，将其诱骗隔离以延缓攻击，并帮助用户追踪溯源、延缓攻击和安全加固，从而保护企业核心资产安全。

与此同时，创宇蜜罐通过无侵入、轻量级的软件客户端安装来实现网络自动覆盖，可快速在企业内网形成蜜网入口，目前已为教育、电力、金融等多行业单位提供安全保障，并收获了来自用户的高度评价。

2. 登录

浏览器中输入蜜罐管理平台地址，输入账号、密码进行登录，**建议使用 Chrome 谷歌浏览器（版本≥65）**访问 Web 管理端。

图 1. 登录页面

3. 风险大盘

3.1. 数据时间筛选

风险大盘页面会对捕获到的攻击进行汇总显示，默认展示最近 7 天的数据，可点击右上角的「时间筛选框」自定义查看的时间周期。

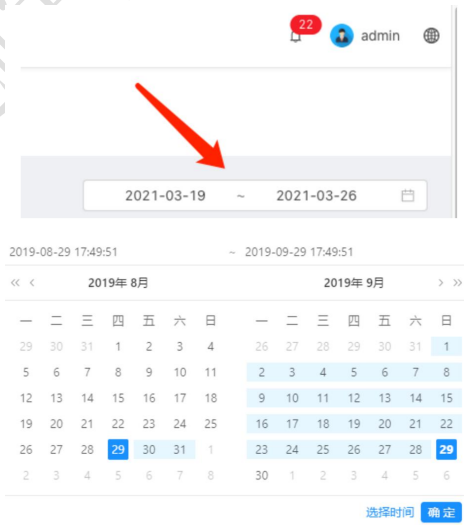

图 2. 选择时间段

3.2. 威胁总览

1) **当前安全状态**：根据蜜罐系统受攻击情况进行变化，若当前没有攻击则显示“正常”，若最近 5 分钟有过攻击，则显示为“受攻击中”；

2) **当前蜜罐总数**：数据统计了当前已部署的蜜罐总数；

3) **24 小时黑客溯源**：数据统计了 24 小时内捕获到的攻击源 IP 或拥有指纹信息的攻击源 IP 的数量；

4) **24 小时威胁指数**：根据 24 小时内系统威胁情况，从攻击日志威胁类型、攻击者溯源结果、攻击日志频率及攻击行为等智能分析出当前系统的威胁指数。20 分以下为低危，20-50 分为中危，50-80 分为高危，80-100 分为严重。

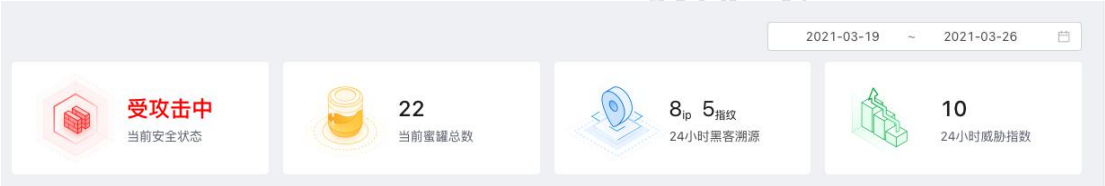

图 3. 威胁总览

3.3. 威胁数据

1) **数据统计**：展示捕获到的安全事件/攻击日志的危险等级、威胁类型以及攻击趋势；

图 4. 威胁数据

2) **攻击源 TOP 5**：统计了攻击源 IP 和攻击源 MAC 地址 的攻击日志数量由多到少的前五名，点击可进入该攻击源的画像详情页；

3) **受攻击占比**：统计了系统中所部署蜜罐的服务和端口受到攻击日志数量由多到少的前五名；

4) **受攻击蜜罐 TOP5**：统计了系统中捕获攻击日志数量最多的前 5 个蜜罐，点击可查看捕获攻击趋势。

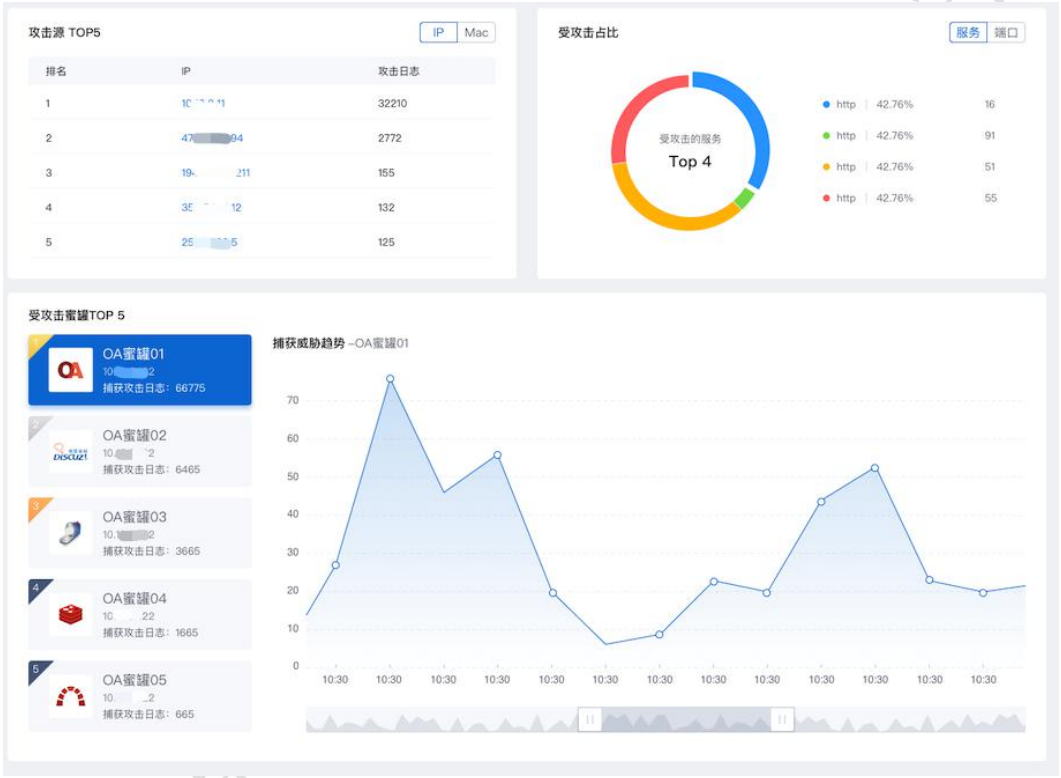

图 5. 攻击源和受攻击占比

4. 安全态势大屏

实时展示蜜罐系统的安全态势，根据蜜罐部署情况与网络环境展示当前网络拓扑图与受到攻击的状态，可选择查看实时攻击状态，也可对近 1 小时或近 24 小时的攻击进行回放。

图 6. 蜜罐安全态势

5. 蜜罐管理

5.1. 蜜罐部署

蜜罐部署在内网蜜罐场景，可接收来自内网的威胁攻击以及自主探测的行为，对黑客进行攻击交互与溯源追踪，并及时发出告警。

蜜罐以客户端作为入口，用户可直接使用系统内置客户端，也可单独在所防护的网段中准备一台客户端设备来部署客户端软件，客户端用于代理转发内网威胁流量至蜜场中（具体部署方法请参照第 6 节-客户端管理），客户端为在线状态时，就可以部署该客户端对应的蜜罐了。

1) 点击“蜜罐管理”菜单，点击页面右上角的“部署蜜罐”按钮，进入部署蜜罐页面；

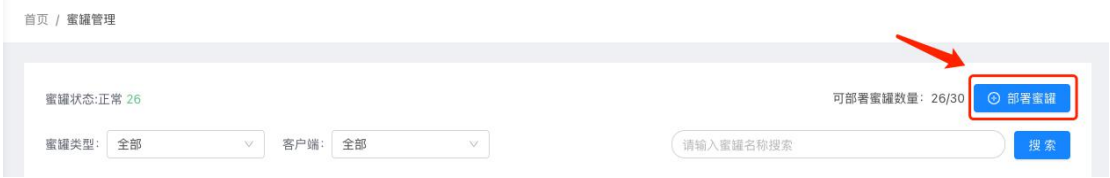

图 7. 部署蜜罐入口

也可在“客户端管理”菜单中，选择已部署好并在线的客户端上的“部署蜜罐”按钮，进入部署蜜罐页面；

图 8. 客户端列表点击部署蜜罐

2) 进入“部署蜜罐”页面后，首先选择蜜罐类型：

用户可根据业务场景或服务类型，选择对应的蜜罐，常用的蜜罐类型有：OA、OpenSSH、ZABBIX、禅道等。若无匹配蜜罐，用户也可以通过定制蜜罐来克隆或自定义业务系统（具体定制方法请参照第 5.4 节-定制蜜罐）；

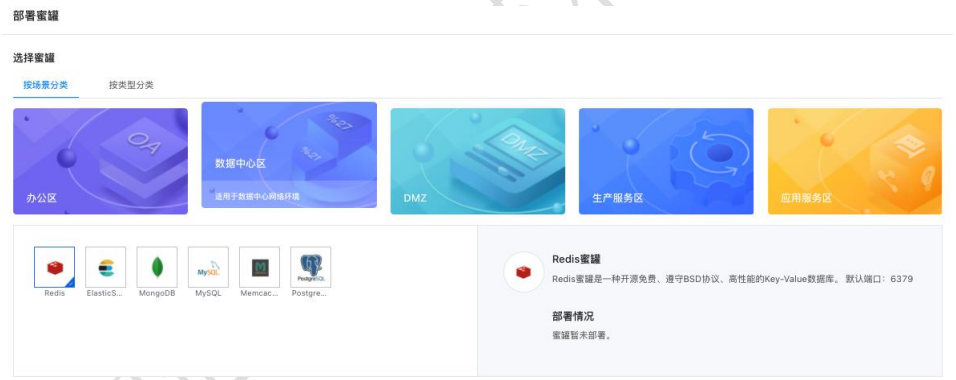

图 9. 根据场景选择蜜罐

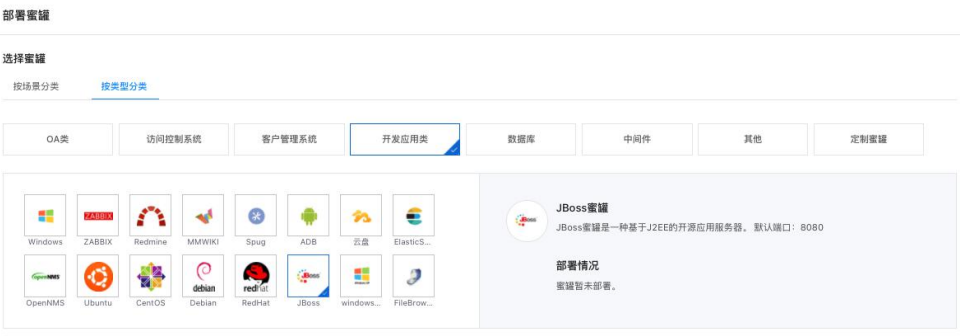

图 10. 根据类型选择蜜罐

3) 选择好蜜罐类型后，继续配置蜜罐。蜜罐的配置方法分为“直连模式”与“中继模式”；

- **直连模式**

“直连模式”是指用户在需要防护的网段中部署了一台客户端后(或直接使用内置客户端），通过 IP 覆盖能在当前网段内虚拟出多个网卡进行蜜罐部署。如果有多个网段的业务场景时，用户需要在不同网段分别部署客户端设备，或是拥有一台多网口的客户端设备，也可以直接使用「中继模式」。

具体步骤如下：

① 选择客户端：用户可选择已部署并且当前在线的客户端，系统会自动识别该客户端的子网掩码（CIDR 表示法）并带出该客户端上的网卡 IP 信息；

② 客户端网卡 IP：此项针对当客户端设备存在多个网卡时，可选择其中的某一个网卡 IP（若您的网络环境是 IPV6，请选择对应的 IPV6 地址），系统会自动带出该网段已绑定蜜罐的情况，防止 IP(端口)冲突；

③ 蜜罐 IP：输入访问蜜罐对应的 IP；

此阶段实现 IP 覆盖(在客户端设备上生成多个虚拟网卡指向蜜罐，有多个 IP 入口可进入蜜罐)的方法如下:

【使用 IPV4】：在蜜罐 IP 最右侧框中输入多组数字，如：22,89,100-103；

【使用 IPV6】：在蜜罐 IP 输入框内输入多个蜜罐 IP 地址，以‘回车’分割；

④ 蜜罐端口设置：展示所选蜜罐类型的默认端口，用户可自行设置 1-65535 范围内的端口，且支持同一个 IP 的不同端口绑定不同的蜜罐。

图 11. 直连模式

- **中继模式**

使用中继模式的前提是将蜜罐系统或独立客户端设备接入汇聚交换机 Trunk 端口（一般由厂商进行配置，配置方法见附录 1）。在页面中配置需要防护网段的 vlanID、vlan 子网掩码/IPV6 前缀以及网关，网段可以是交换机 Trunk 端口配置允许的任意一个网段，这样就实现跨网段部署蜜罐，再结合 IP 覆盖，则可在不同网段中虚拟出多个 IP。

具体步骤如下：

① 选择客户端：用户需要选择接入交换机 Trunk 端口的客户端，系统会自动识别客户端的子网掩码，对可输入的蜜罐 IP 范围进行限制；

② 客户端网卡 IP：此项针对当客户端设备存在多个网卡时，可选择其中的某一个网卡 IP（若您的网络环境是 IPV6，请选择对应的 IPV6 地址），系统会自动带出该网段已绑定蜜罐的情况，防止 IP(端口)冲突；

③ vlanID、vlan 子网掩码/IPV6 前缀、网关：根据交换机的配置，输入交换机允许通信且需要部署蜜罐的网段 vlanID、vlan 子网掩码/IPV6 前缀、网关(此阶段用于识别所部署的网段）。

④ 蜜罐 IP：输入访问蜜罐对应的 IP；

此阶段实现 IP 覆盖(在客户端设备上生成多个虚拟网卡指向蜜罐，有多个 IP

入口可进入蜜罐)的方法如下:

【使用 IPV4】：在蜜罐 IP 最右侧框中输入多组数字，如：22,89,100-103；

【使用 IPV6】：在蜜罐 IP 输入框内输入多个蜜罐 IP 地址，以‘回车’分割；

⑤ 蜜罐端口设置：展示所选蜜罐类型的默认端口，用户可自行设置 1-65535 范围内的端口，且支持同一个 IP 的不同端口绑定不同的蜜罐。

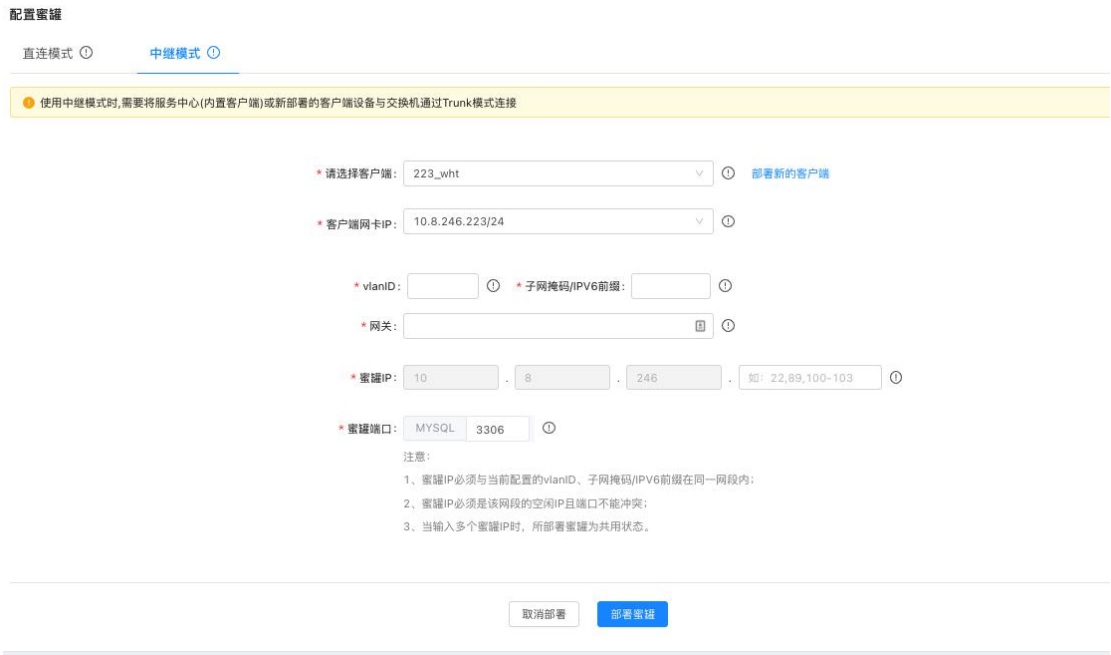

图 12. 中继模式

- **甜度设置（可选）**

蜜罐详情中，可开启甜度设置，此操作可选，每一个蜜罐都可以自定义端口，部分蜜罐支持内部字段的自定义；比如 OA 蜜罐中，如果填写了公司名称与公司 logo，蜜罐系统中的标题与 logo 会变成用户自定义的内容；如果填写了管理员密码，蜜罐系统默认账号的密码也会随之改变成用户设定的密码。

若不开启甜度设置，则为以系统默认配置为准。

图 13. 甜度设置

4) 部署蜜罐成功后，蜜罐列表会显示相应的蜜罐信息。

图 14. 蜜罐部署成功

蜜罐状态说明

- 正常：蜜罐正常运行。
- 部分异常：部分蜜罐 IP 异常，可进入蜜罐设置页中对异常蜜罐 IP 进行排查处理。
- 异常：蜜罐状态异常，可进行如下操作：① 进入蜜罐设置页检查客户端是否离线或端口冲突；② 若客户端正常，请重置蜜罐。
- 部署中/重置中：蜜罐正处于部署中或重置中。
- 部署失败/重置失败：蜜罐部署失败或重置失败，可进入蜜罐设置页删除蜜罐后进行重新部署。

5.2. 蜜罐列表

蜜罐列表是对蜜罐进行管理的页面，可以部署、查看和管理蜜罐，列表上方展示了当前蜜罐的状态统计，右侧可以对相关信息进行搜索。

在列表中可直接修改蜜罐名称，鼠标悬浮查看当前蜜罐对应的客户端名称；列表展示了蜜罐的部署模式是直连模式还是中继模式，鼠标悬浮查看对应客户端的网卡 IP；点击“威胁日志”可跳转到攻击日志页面，会展示该蜜罐对应的日志数据；点击设置可进入该蜜罐的设置页。

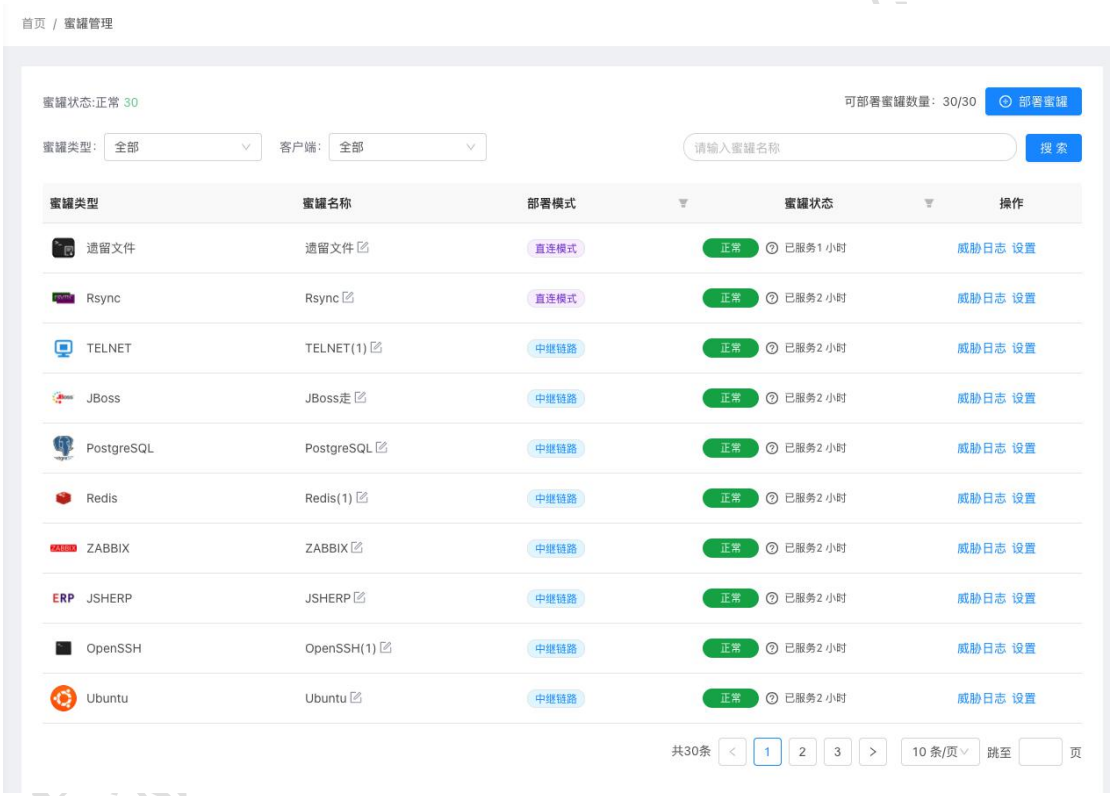

图 15. 蜜罐列表

5.3. 蜜罐设置

在蜜罐列表页面，点击蜜罐“操作-设置”链接会跳转到蜜罐设置页面。蜜罐设置页面会显示蜜罐类型、蜜罐状态、蜜罐部署时间、部署模式、服务端口等信息，左上角可切换蜜罐查看不同蜜罐的设置页。

在蜜罐设置页可以点击右上角的按钮对蜜罐进行重置或删除。

图 16. 蜜罐设置页

- **蜜罐信息**

在“蜜罐信息”模块可查看当前蜜罐属于哪一个客户端以及对应的子网 IP，会显示所有的蜜罐 IP 与对应状态，同时可删除蜜罐 IP，或新增覆盖出大量的蜜罐 IP。

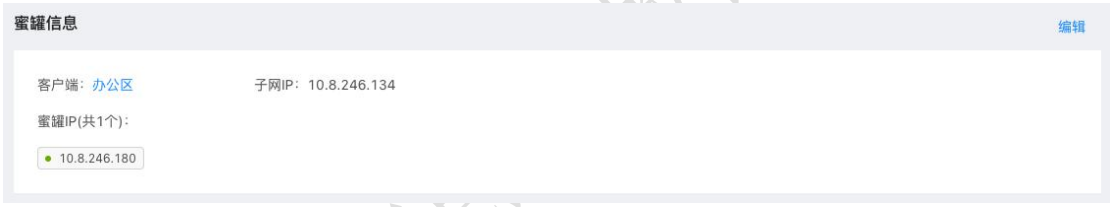

图 17. 蜜罐设置页-蜜罐信息

- **甜度设置**

部分蜜罐支持修改甜度设置，比如 OA 蜜罐中，如果填写了公司名称与公司 logo，蜜罐系统中的标题与 logo 会变成用户自定义的内容；如果填写了管理员密码，蜜罐系统默认账号的密码也会随之改变成用户设定的密码。

（修改蜜罐甜度或重置蜜罐时，会使蜜罐恢复原始设置，蜜罐中若额外预置了内容，则会丢失。）

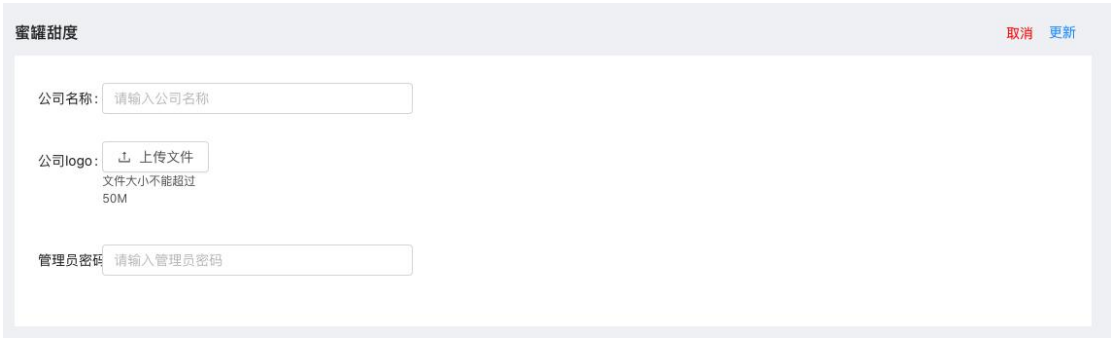

图 18. 蜜罐设置页-甜度设置

- **溯源插件**

溯源插件模块展示了当前蜜罐是否绑定了溯源插件。

图 19. 蜜罐设置页-溯源插件

5.4. 定制蜜罐

定制蜜罐提供给用户能够根据业务需求定制仿真业务系统蜜罐的能力，能够模仿用户网络环境内真实业务站点，提高蜜罐的迷惑性。以下给出了克隆蜜罐与自定义蜜罐两种定制蜜罐的方法。

点击菜单“蜜罐管理-->部署蜜罐-->按类型分类-->选择「定制蜜罐」-->添加定制蜜罐”或点击菜单“策略配置-->蜜罐模板配置-->添加模板”进入定制蜜罐页面。

图 20. 部署蜜罐-定制蜜罐

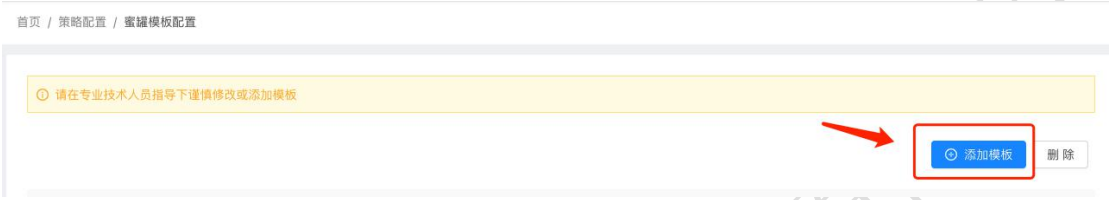

图 21. 蜜罐模板配置-添加模板

5.4.1. 克隆蜜罐

定制克隆蜜罐的具体步骤：

1) “模板类型”选择“克隆蜜罐”；

2) 填写蜜罐 LOGO（可选）、蜜罐名称、蜜罐描述；

3) 填写需要克隆系统的 URL，需要蜜罐系统服务器网络可达，信息填写无误后，点击“添加模板”；

图 22. 蜜罐模板配置-克隆蜜罐

4) 进入“蜜罐管理-->部署蜜罐-->按类型分类”页面，选择“定制蜜罐”场景中对应的蜜罐进行部署。

图 23. 部署定制蜜罐

5.4.2. 自定义蜜罐

定制自定义蜜罐的具体步骤:

1) “模板类型”选择“自定义蜜罐”；

2) 填写蜜罐 LOGO（可选）、蜜罐名称、蜜罐描述;

3) 上传相关业务系统的资源代码包（扩展名为.zip 且大小不能超过 500M、入口文件名必须为 index.html），信息填写无误后，点击“添加模板”；

图 24. 蜜罐模板配置-自定义蜜罐

4) 进入“蜜罐管理-->部署蜜罐”页面，选择“定制蜜罐”场景中对应的蜜罐进行部署。

图 25. 部署定制蜜罐

5.4.3. 默认蜜罐

默认蜜罐主要提供给厂商对蜜场中的系统内置蜜罐进行配置。

6. 客户端管理

6.1. 客户端列表

点击“客户端管理”菜单，进入客户端列表。

客户端列表是对客户端进行管理的页面，可以部署、查看和管理客户端。

图 26. 客户端列表

蜜罐系统默认有一个内置客户端，用户可直接在内置客户端上部署蜜罐，使用中继模式时，也可选择系统内置客户端。内置客户端可以进行重启和启动/暂停操作。

6.2. 客户端部署

若不选择系统内置客户端，用户也可以自行准备一台设备作为客户端，客户端设备的配置要求如下：

- 部署环境支持 CentOS 6, CentOS 7, Ubuntu 16.04，Ubuntu 18.04 64 位系统。

- 配置不低于单核 amd64、内存 1G、硬盘 50G。
- 网络可以访问蜜罐系统服务中心。
- 独立设备，请不要在业务系统上部署客户端。

具体的部署方式：

1) 进入客户端列表页面，点击“部署客户端”按钮，将弹窗的部署设备命令，粘贴至已提前准备的好设备中运行。

图 27. 点击部署客户端

图 28. 复制部署客户端命令

2) 以 root 权限登陆到准备好的部署设备上执行该命令，该命令只能安装一个客户端，用户使用后命令失效，客户端安装启动成功后，会给出相应

的提示。

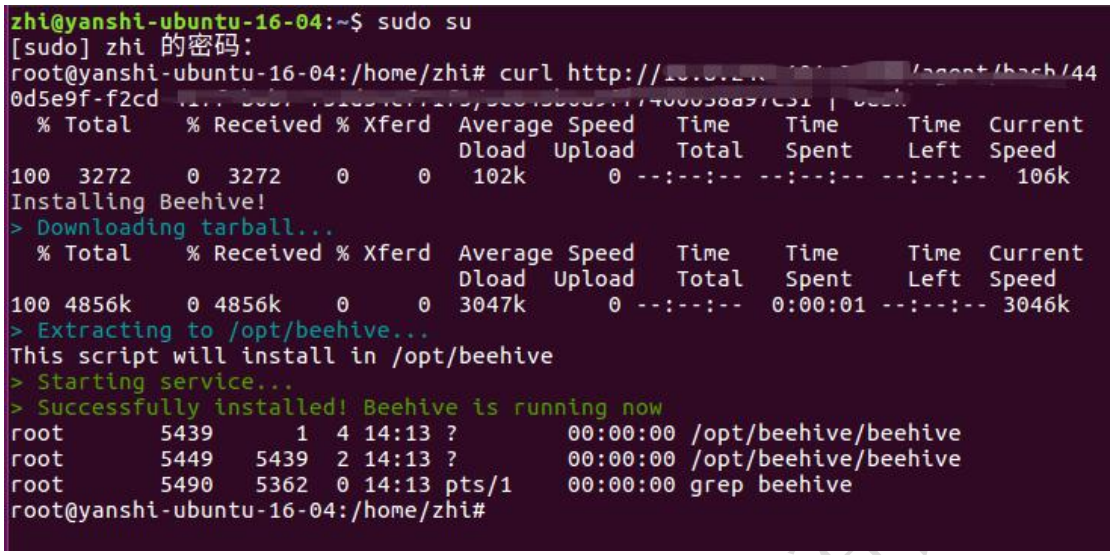

图 29. 部署成功后的提示

3) 部署成功后，客户端状态为“在线”。

图 30. 部署成功后客户端状态

客户端状态说明

- 在线：客户端设备与管理中心设备已正常连接，可进行蜜罐的部署。
- 离线：未能连接客户端设备，可检查设备联网状态或尝试重启客户端。
- 暂停：已暂停客户端设备与管理中心的连接，如有需要，请启动客户端。
- 停止：已停止客户端设备与管理中心的连接，可卸载客户端程序并删除客户端。

6.3. 客户端操作

1) 重新部署：客户端状态变为“在线”后，若用户想更换客户端设备，需要先将原有的客户端上的软件进程关闭或卸载原设备上的客户端软件，使客户端状态变为“**离线**”后，将“重新部署”弹框中的命令粘贴至新的客户端设备中执行即可。

2) 重启：当客户端出现离线或需要更新网卡等情况，可点击“重启”尝试；

3) 暂停：若想暂时断开客户端连接，可对在线的客户端进行“暂停”操作；

4) 启动：若想开启客户端连接，可对暂停的客户端进行“启动”操作；

5) 停止：若想永久断开客户端连接并保留当前客户端信息，可对客户端进行“停止”操作，停止后只能删除当前客户端数据，不能再重新开启。

6) 删除：若想在界面上删除此条客户端信息，可直接点击删除客户端。（删除客户端只是删除在蜜罐系统上的数据，设备上的删除请参考 6.4 客户端卸载。）

图 31. 对客户端进行操作

6.4. 客户端卸载

卸载客户端软件，只需要在客户端设备上执行以下命令：

sudo sh -c 'beehive -s stop && beehive -s uninstall && rm -rf /opt/beehive && rm -f /usr/bin/beehive'

再次在命令中输入“beehive”，出现以下内容时，表示卸载成功；

图 32. 客户端卸载

7. 蜜饵管理

7.1. 邮件蜜饵

邮件蜜饵用于生成包含诱导进入蜜罐内容的蜜饵邮件，攻击者从邮件跳转到蜜罐时将触发告警。通过向一些敏感邮箱定期发送蜜饵邮件，可与 Web 蜜罐关联生成带有蜜罐 IP 入口的邮件内容。

添加邮件蜜饵具体步骤：

1) 进入“蜜饵管理”-->“邮件蜜饵”页面，点击“添加邮件蜜饵”：

图 33. 邮件蜜饵

2) 填写邮箱信息：发送者邮箱、发送者邮箱密码、发件人（可选择输入发件人名称）、邮箱服务器的地址（格式为 smtp.xxx.com）以及邮件服务端口、接收蜜饵邮箱（可以输入多个邮箱接收邮件，每个邮箱以‘回车’分割）；

图 34. 邮件蜜饵-邮箱信息

3) 填写邮件信息：发送频率（可以选择单次、每周、每两周或每月，系统会根据配置的发送频率发送蜜饵邮件到接收蜜饵邮箱）、开始日期（开始发送邮件的日期）、发送时间（邮件发送的具体时间）、关联蜜罐 IP（在邮件内容中诱导进入的蜜罐 IP）、邮件标题（可选择输入，默认为邮件模板名称）、邮件模板（可选择系统提供的邮件模板，并支持在下方的富文本编辑器中修改，模板中的__MGIP__" 标识不能删除）；

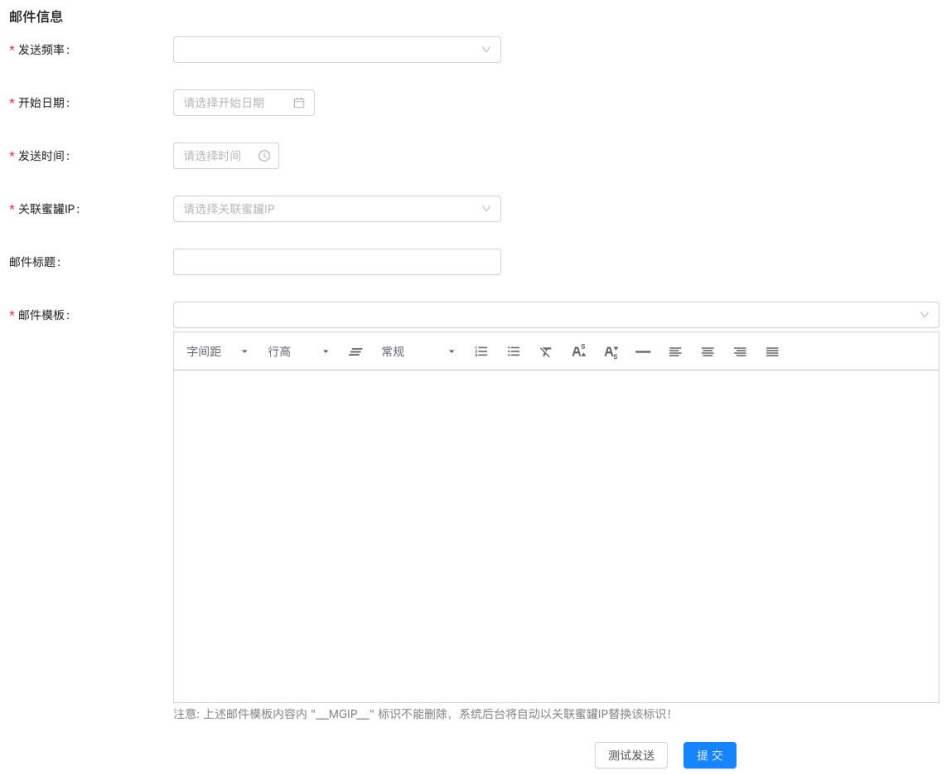

图 35. 邮件蜜饵-邮件信息

4) 点击“测试发送”会根据配置的邮件信息发送邮件到测试接收邮箱。测试接收邮箱中查看到邮件，说明设置正确，点击“提交”即可保存当前配置内容。

5) 在邮件蜜饵列表会生成相应的蜜饵记录，可通过状态开关控制是否启用邮件蜜饵，支持对单条数据进行“编辑”和“删除”。

图 36. 邮件蜜饵列表

7.2. 文件蜜饵

文件蜜饵用于生成包含诱导进入蜜罐内容的蜜饵文件，攻击者从文件跳转到蜜罐时将触发告警。通过关联当前已部署的蜜罐，生成包含蜜罐入口 IP 的蜜饵文件，用户可下载文件并散布在办公网区域，诱导攻击者进入蜜罐。

添加文件蜜饵具体步骤：

1) 进入“蜜饵管理”-->“文件蜜饵”页面，点击“添加文件蜜饵”；

图 37. 添加文件蜜饵

2) 选择需要关联的蜜罐 IP 与将要使用的文件模板，点击确定；

图 38. 添加文件蜜饵-选择

3) 在文件蜜饵列表会生成相应的蜜饵记录，支持对单条数据进行“下载”和“删除”。

图 39. 文件蜜饵列表

8. 威胁情报

8.1. 攻击者画像

蜜罐捕获到攻击威胁后，会将攻击者 IP 以画像形式进行记录，列表中会以是否获取到指纹信息进行区分，展示攻击源 IP、攻击时间、攻击次数、攻击手段、指纹数据信息。

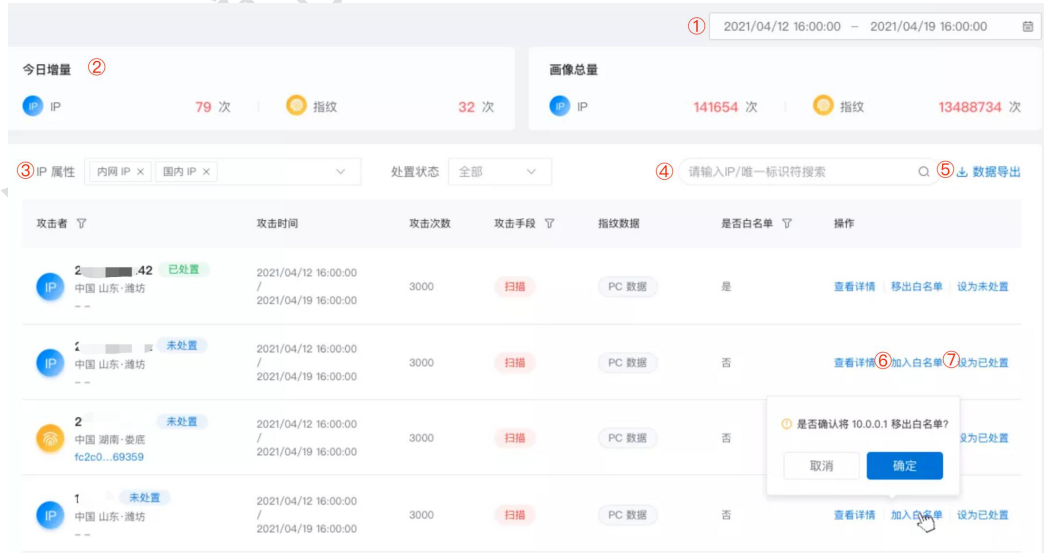

图 40. 攻击者画像列表

界面功能点说明：

① 时间筛选：根据时间筛选器，界面会展示「最新攻击时间」符合时间范围的攻击者画像；

② 数据统计：展示今日和历史捕获到的攻击源 IP 以及拥有指纹的攻击源 IP 数量；

③ IP 属性：支持对国外 IP、国内 IP、内网 IP 进行筛选；

④ 搜索：支持对攻击者 IP/唯一标识符搜索；

⑤ 数据导出：根据当前筛选情况，导出 excel 攻击者画像数据报告；

⑥ 白名单操作：可一键添加/移出白名单；

⑦ 处置标识：支持对攻击源 IP 打上「已处置/未处置」标识。

点击「查看详情」，可以查看单个攻击源 IP 的攻击数据信息、威胁趋势以及攻击手段，获取到的攻击者指纹信息也会在页面上展示，并且以时间线的方式显示攻击者路径，相同指纹的攻击者还会进行关联，整个攻击者画像详情页在右上角提供图片格式的下载功能。

8.2. 遗留文件下载

部署“遗留文件蜜罐”可捕获到黑客在此蜜罐中上传的文件，识别到上传行为的攻击源会被打上“文件上传”的攻击手段标签，可以攻击源为维度在详情页进行遗留文件下载分析（文件包含风险，请谨慎下载）。

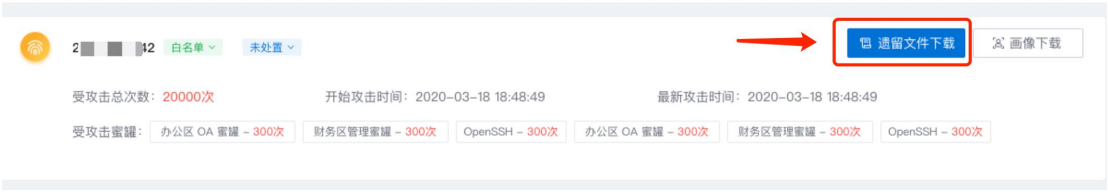

图 41. 攻击者画像详情-遗留文件下载

8.3. 攻击日志

攻击日志页面可以查看蜜罐被攻击的日志，点击“蜜罐名称”会链接到蜜罐设

置页面。

页面可通过简单搜索和高级搜索在全日志中进行查询，“列显示”按钮可设置当前显示的字段列，“自定义下载”按钮可对当前日志数据进行下载。

OpenSSH 蜜罐与 Windows 蜜罐支持在攻击详情中查看攻击回放，除扫描外的攻击日志支持 PCAP 包下载；点击单条日志左侧的“+”号可以查看具体的日志内容。

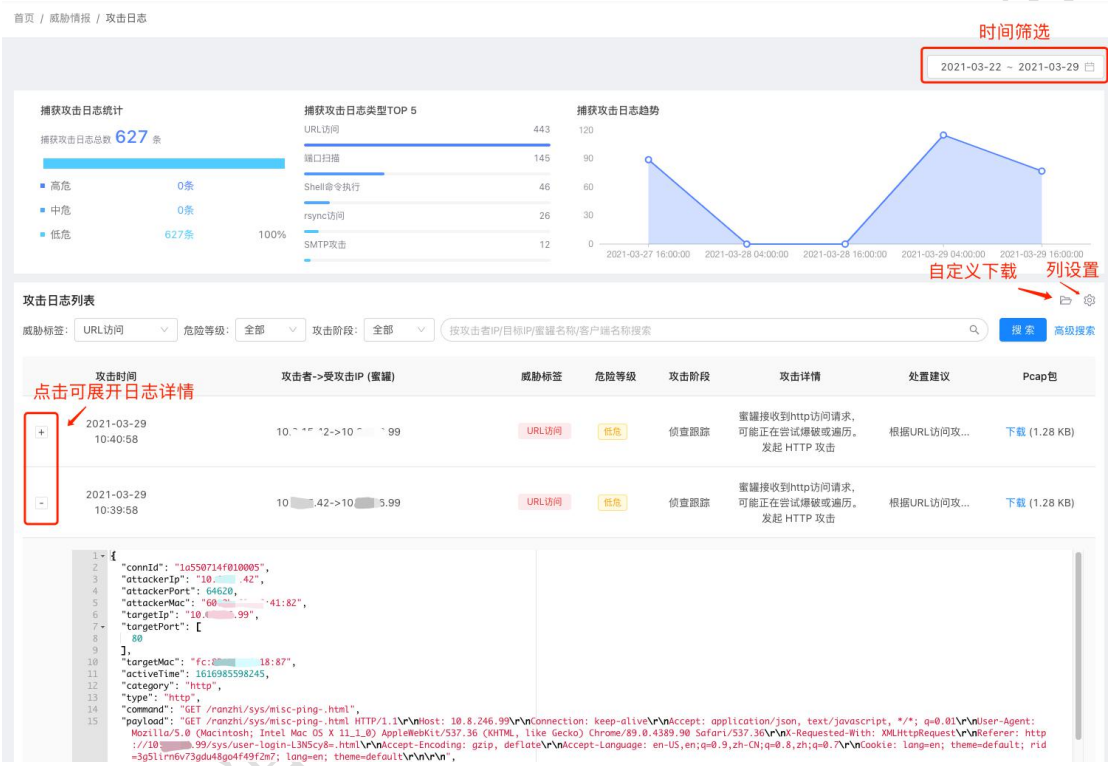

图 42. 攻击日志

8.3.1. 日志操作

蜜罐系统的威胁日志使用了强大的搜索引擎，可以在极短的时间内搜索和分析大量的数据。

- **列设置**

可以通过页面右上角的“列设置”按钮对所展示的字段进行定义。

图 43. 攻击日志-列设置

- **高级搜索**

日志系统提供一套查询语法用于高级搜索设置查询条件，帮助用户更有效地查询日志。

图 44. 攻击日志-高级搜索

查询语句	查询示例
任意字段的值可能是 a	威胁分类可能为 http 的日志：

a	http
a 字段的值可能是 b a:b	威胁分类可能为 http 的日志： category:"http"
同时包含 a 和 b 的日志 a AND b 或者 ab	威胁分类为 smtp 且攻击源为 10.8.15.100 的日志： category:"smtp" AND attackerIp:"10.8.15.100"
包含 a 或者包含 b 的日志 a OR b	威胁分类为 smtp 或 ssh 的日志： category:"smtp" "ssh" 或者 category:"smtp" OR "ssh"
包含 a 但是不包含 b 的日志 a NOT b	威胁分类为 smtp 且攻击源不为 10.8.15.100 的日志： category:"smtp" NOT attackerIp:"10.8.15.100"
所有日志中不包含 a 的日志 NOT a	威胁分类不为 http 的日志： NOT category:"http"
查询包含 a 而且包含 b,但是不包含 c 的日志 a AND b NOT c	攻击源 Ip 为 10.8.15.104 且蜜罐名称为然之 OA 但是受攻击 ip 不为 10.8.246.99 的日志： attackerIp:"10.8.15.104" AND beehiveName:"然之 OA" NOT targetIp:"10.8.246.99"
包含 a 或者包含 b，而且一定包含 c 的日志 (a OR b) AND c	攻击源 Ip 为 10.8.15.104 或蜜罐名称为然之 OA 但是受攻击 ip 一定为 10.8.246.99 的日志： (attackerIp:"10.8.15.104" AND beehiveName:"然之 OA") AND targetIp:"10.8.246.99"
包含 a 或者包含 b，单不包括 c 的日志	攻击源 Ip 为 10.8.15.104 或蜜罐名称为然之 OA 但是受攻

(a OR b) NOT c	击 ip 一定为 10.8.246.99 的日志： (attackerIp:"10.8.15.104" AND beehiveName:"然之 OA") NOT targetIp:"10.8.246.99"
包含 a 而且包含 b，可能包含 c 的日志 a AND b OR c	攻击源 Ip 为 10.8.15.104 且蜜罐名称为然之 OA，受攻击 ip 可能为 10.8.246.99 的日志： attackerIp:"10.8.15.104" AND beehiveName:"然之 OA" OR targetIp:"10.8.246.99"
查询存在某个字段的日志 字段名:*	包含 payload 字段的日志： payload:*
查询以 a 开头的日志 a*	包含以 GET 开头的日志： GET*

8.4. 安全事件

安全事件页面可以查看当前系统中产生的安全事件，点击“蜜罐名称”会链接到蜜罐设置页面。

蜜罐系统可感知到来自外网或内网的端口扫描、URL 探测、暴力破解、远程登录、命令执行等安全事件；可点击事件左侧的“+”号，展开该安全事件对应聚合的攻击日志。

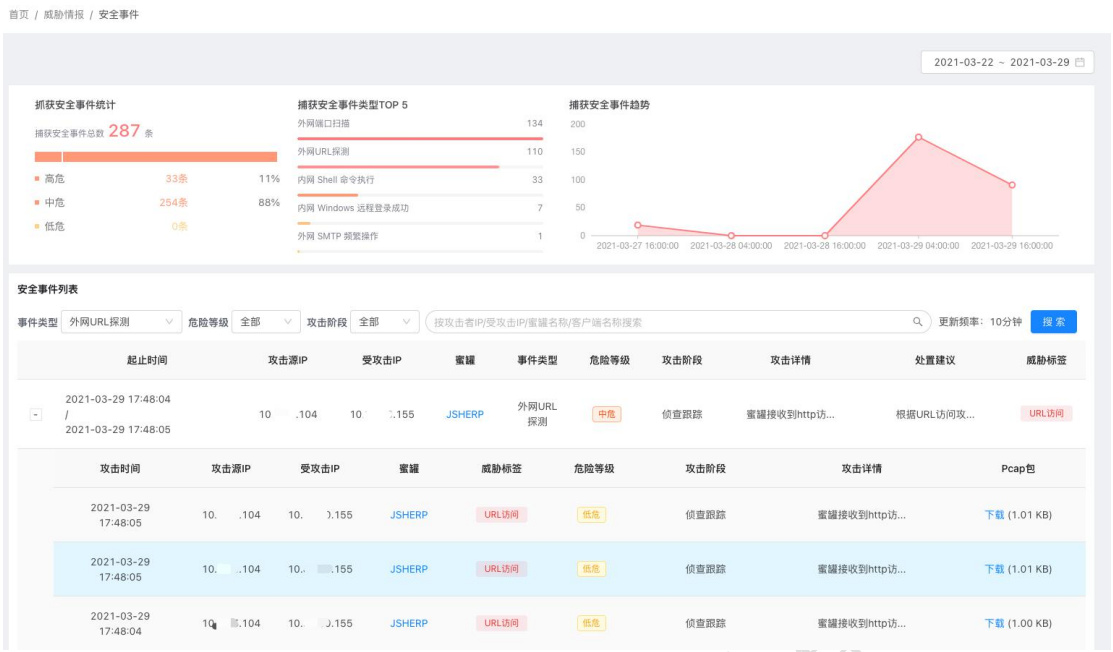

图 45.　安全事件

9. 数据管理

9.1. 行为分析报告

行为分析报告可以导出系统在某个时间段下以客户端为维度 word 版或 PDF 版的系统威胁数据以及相关状态的报告。

1) 点击“新建报告”输入报告的名称或使用系统自动命令，选择产生数据的时间段以及客户端范围；

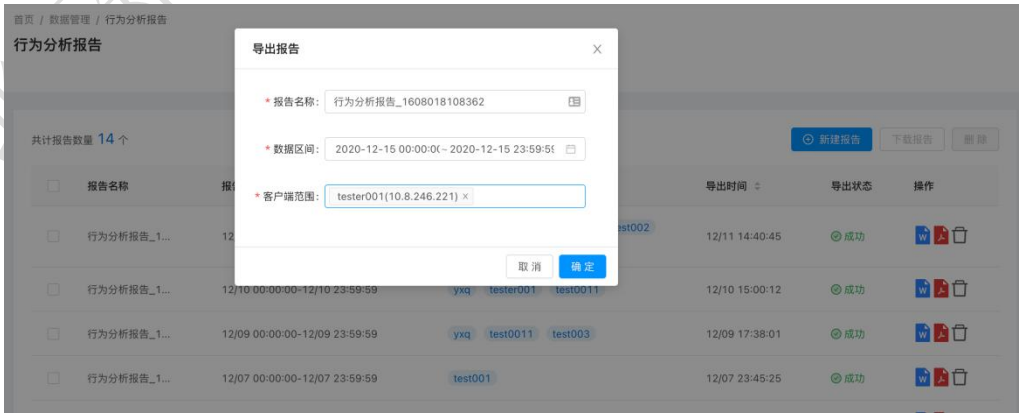

图 46.　新建报告

2) 点击确定后可在报告列表看到相关报告信息，列表中的报告信息支持批量下载与删除。

图 47. 报告管理

9.2. 日志数据下载

日志数据下载页面支持通过攻击日志页面筛选后的数据聚合下载。

1) 点击“前往日志页面生成数据报告”按钮跳转至攻击日志页面；

图 48. 日志数据下载入口

2) 在攻击日志页面通过搜索框进行筛选后，点击下载按钮，在弹出的对话中可定义报告的名称与需要下载的数据类型；

图 49.　日志下载按钮

图 50.　下载类型设置

3) 点击确定后会跳转至日志数据下载页看到相关报告信息，列表中的报告信息支持批量下载与删除。

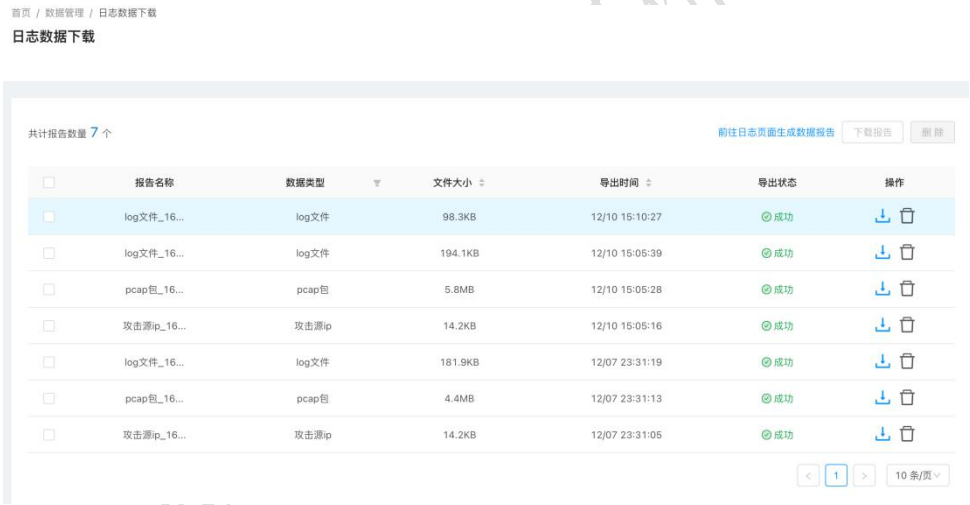

图 51.　日志数据列表

10. 策略配置

10.1. SYSLOG 配置

配置好 SYSLOG 服务后，将 SYSLOG 服务器地址添加进系统内，系统会实时将蜜罐捕获到的威胁日志通过 json 字符串的格式发送到 SYSLOG 服务器。

图 52. SYSLOG 配置

10.2. 白名单配置

用户可以将系统内已知的安全扫描 IP 或 MAC 加入白名单，避免产生报警记录。启用的白名单 IP/MAC 产生的攻击日志将不计入威胁态势统计。

10.2.1. 计入攻击日志配置

启用状态下的白名单 IP/MAC 产生的攻击流量默认会计入攻击日志，在“攻击日志”页面会展示打上绿色标签的攻击 IP/MAC；若用户不想将白名单 IP/MAC 计入攻击日志，将“计入攻击日志”配置成“否”即可。

图 53. 计入攻击日志配置

10.2.2. 添加白名单 IP

点击页面的“添加 IP”，在弹窗中编辑白名单 IP 信息进行保存（可批量添加白名单 IP）。白名单创建后，默认启用状态。

图 54. 添加白名单 IP

10.2.3. 添加白名单 MAC

点击页面的“添加 MAC”，在弹窗中编辑白名单 MAC 信息进行保存（可批量添加白名单 MAC）。白名单创建后，默认启用状态。

图 55. 添加白名单 MAC

10.2.4. 白名单删除

白名单创建后，可进行删除操作，点击数据后的“删除”链接即可，白名单删除后，该 IP 或 MAC 产生日志时会进行告警。

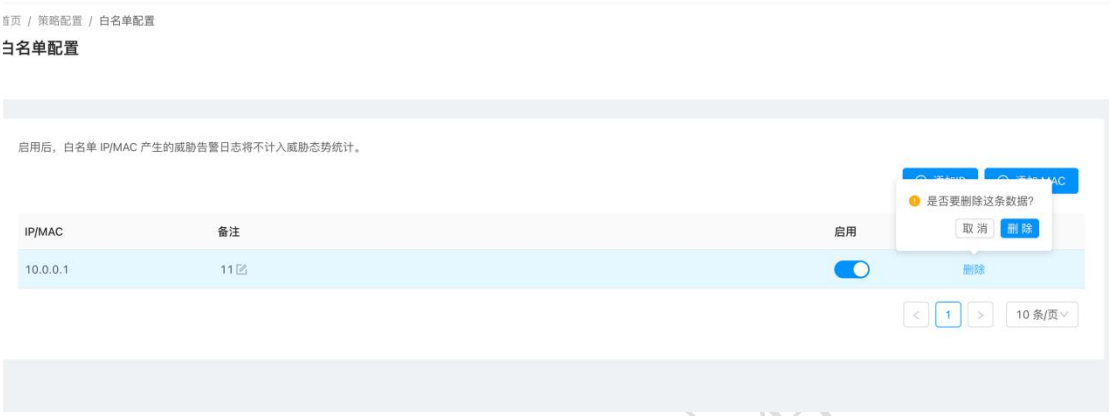

图 56. 删除白名单

10.3. 插件配置

插件配置页面用于添加获取指纹的 JS 插件，列表中可查看添加的插件信息，并且可以对插件进行删除。点击“添加插件”可以配置插件基本信息以及客户端和服务端的插件代码。

此功能建议用户在专业人员的指导下添加系统插件，否则可能会导致系统内置插件失效。

10.4. 蜜罐模板配置

10.4.1. 默认蜜罐

用于管理员配置系统中默认的蜜罐模板，点击“添加蜜罐模板”可以配置蜜罐基本信息、服务端口、甜度等信息，或在列表中对蜜罐信息进行编辑、删除操作。建议用户不要随意改动出厂时系统内置的蜜罐模板，否则可能会导致系统中的蜜罐无法正常部署。

10.4.2. 定制蜜罐

在蜜罐模板页面也可进行克隆蜜罐与自定义蜜罐的制作（具体定制方法请参照第 5.2 节-定制蜜罐）。

10.5. 虚拟 IP 配置

用于设置连接管理中心与客户端的系统网关 IP，可在路由器、防火墙等设备上将系统网关 IP 映射到需要安装客户端的服务器网络可达的 IP 地址后，在此页面中添加映射后的虚拟 IP。

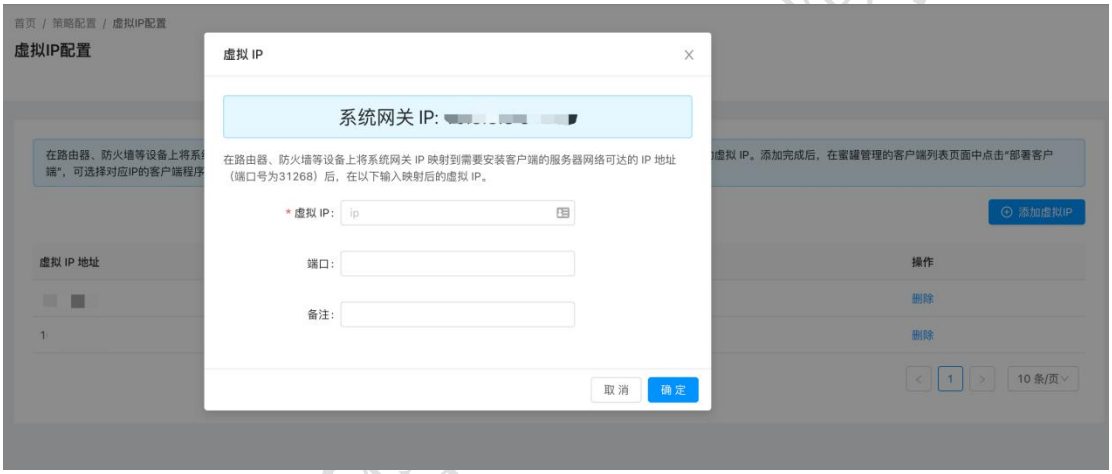

图 57. 虚拟 IP 配置

添加完成后，在客户端列表页面中点击“部署客户端”，可选择对应的系统网关 IP 进行部署。

此功能建议用户如果没有强需求的话不要随意改动，否则可能会导致客户端与管理中心连接失败。

10.6. 特征管理

特征管理页面展示了当前系统能够识别的特征规则的编号、漏洞名称、攻击分类、漏洞类型、威胁得分、处置建议及更新时间等。

用户可以点击右上角的“自定义”特征按钮，输入对应的特征信息，从而完成特征规则的添加。

被识别到的特征会在攻击日志页面，通过标签的形式在匹配日志数据的”威胁标签”字段中展示。

图 58. 特征管理

11. 权限管理

11.1. 用户管理

11.1.1. 用户列表

用户管理列表能够查看当前系统内的所有用户信息，可以对用户信息进行修改、设置有效期、重置密码、删除的操作。

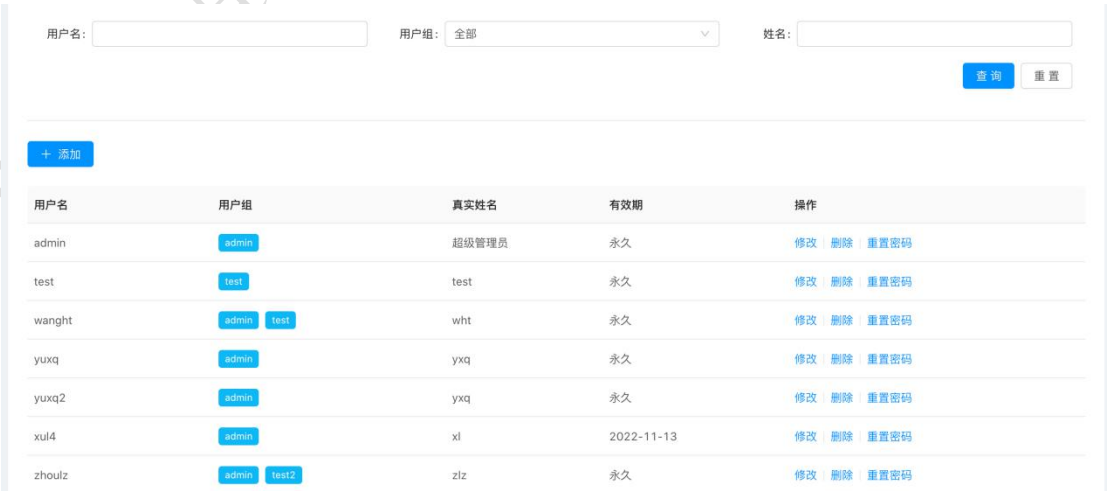

图 59. 用户管理

11.1.2. 添加用户

点击“添加”给系统新增用户，配置了账号、密码、姓名等信息的账号仅拥有登录系统的权限，更多的权限需要到用户组页面为该用户分配具有权限的用户组。

图 60. 添加用户

11.2. 用户组管理

用户组管理列表能够查看当前系统内的所有用户组信息，同时能够对用户组进行修改和删除。

图 61. 用户组管理

点击“权限管理”可以对当前用户组的用户权限进行分配。

其中，“查看所有数据权限”建议仅分给最高权限管理员，拥有该权限的用户可查看所有用户数据。

图 62.　权限管理

“成员管理”可以分配用户到所选用户组中，点击用户名后，通过“>”与“<”按钮移入或移出用户组。

图 63.　成员管理

点击“添加”按钮给系统新增用户组，配置用户组名称以及描述即可。

图 64. 添加用户组

11.3. 功能模块管理

功能模块列表能够查看当前系统内的所有功能模块信息，可以对功能模块信息进行修改、删除操作。点击“添加同级模块”给系统添加功能模块，需要配置模块的基本信息。

此功能建议用户不要随意改动，否则可能会导致系统中的功能异常。

12. 日志管理

12.1. 审计日志

审计日志页面会记录登录用户在系统内所做的操作，记录内容包括用户名、IP、时间、操作类型、操作内容、状态。页面可根据用户名、时间、操作类型、操作内容进行查询，根据月份导出数据报表（将日志导出到本地，以 .csv 存储，只能导出一个月的日志）。

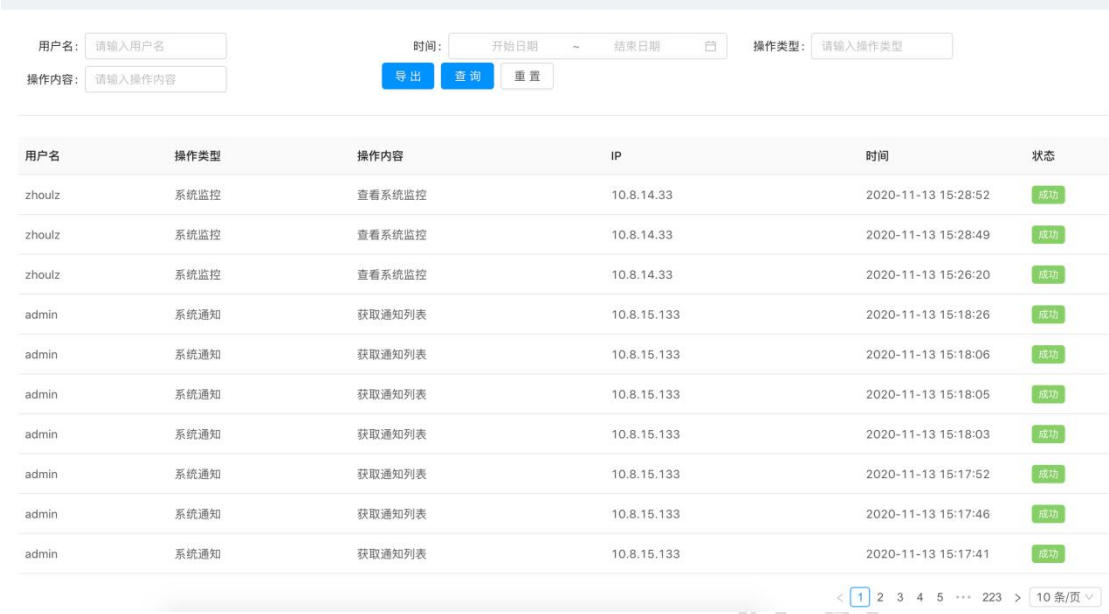

图 65. 审计日志

12.2. 日志清除

系统提供删除审计日志的功能，主要分自动删除和手动删除两种模式，清理后的日志将无法恢复。

自动删除，系统会根据这个时间去设置一个定时任务自动清除审计日志；

手动删除，会弹出框供您选择需要清除的日志时间段，点击确定后会立即执行删除操作。

图 66. 日志清除

13. 系统配置

13.1. 通知配置

13.1.1. 邮箱配置

邮箱配置中添加的邮箱，可以收取告警通知。根据页面必填字段要求正确填写 SMTP 邮箱服务器地址、SMTP 邮箱服务端口、发送者邮箱账号、发送者邮箱密码以及发件人，点击“提交”可成功保存邮箱配置信息。

图 67. 邮箱配置

点击页面中的“测试连接”按钮，在弹窗中输入收件人邮箱地址，点击“发送”，若能够接受到测试邮件，则表示邮箱配置正确。

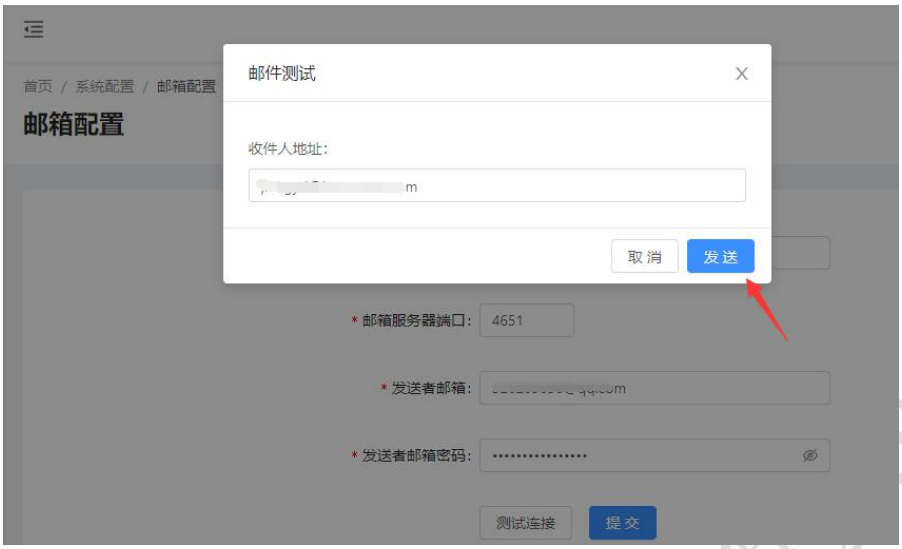

图 68. 邮件测试

13.2. 安全策略配置

此页面用于配置系统的安全策略，包括以下几个内容：

① 最大错误登录次数：限制了用户登录时输入密码错误的最大上限次数；

② 错误登录锁定时间范围：达到最大错误登录次数之后，用户账号被锁定无法登录的时间；

③ 会话超时时间：当前页面会话超时弹出的时间；

④ 多端登录：多端登录开启时，允许多个使用者多地同时登录一个账号，否则，同一时间只能有一个使用者登录在线，其他使用者会被下线（需要重新登录）；

⑤ 密码最短长度：设置用户密码的最短长度；

⑥ 密码复杂度：设置用户密码的复杂度；

⑦ 启用 JWT 认证：是否开启 JWT 认证模式。

图 69. 安全策略配置

13.2.1. JWT 认证方法

为了应对终端客户可能存在的对接已有系统的需求，在原有系统的 cookie/session 认证机制的基础上，同时支持 JWT 认证方法。

1) 获取 JWT Token;

POST /api/passport/jwt

Body:

{

"username":"用户名",

"password":"密码"

}

Response:

{

"code": 0,

"msg": "",

"data": {

"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWQiOiI1ZjA2ZTgzNTU3NTc0MzExNDVhMzFm

NmMiLCJpYXQiOjE1OTUyMjc3MzZ9.bdNWfjhi0r98CB54fPgeGoLgf9p2zX8kdqCT_92eoAE"

}

}

2) 使用 JWT Token 请求接口;

// 以请求网卡配置为例

GET /api/sys/setting/network

headers:

Authorization: Bearer ${token}

14. 监控管理

14.1. 系统监控

主机监控采集宿主机运行时的 CPU、内存、网络、磁盘使用 等信息，实时展示给用户。

服务监控实时展示前台服务、API 服务、数据库 以及其它业务方服务的运行监控情况

图 70. 系统监控

14.2. 系统告警配置

对系统空间的使用情况进行告警，可设置系统分区与业务分区使用率告警阈值、预警间隔；在“邮箱配置”页面配置了邮箱服务器后，在此处设置告警邮件收件邮箱，就能够通过邮件的方式收到告警通知。

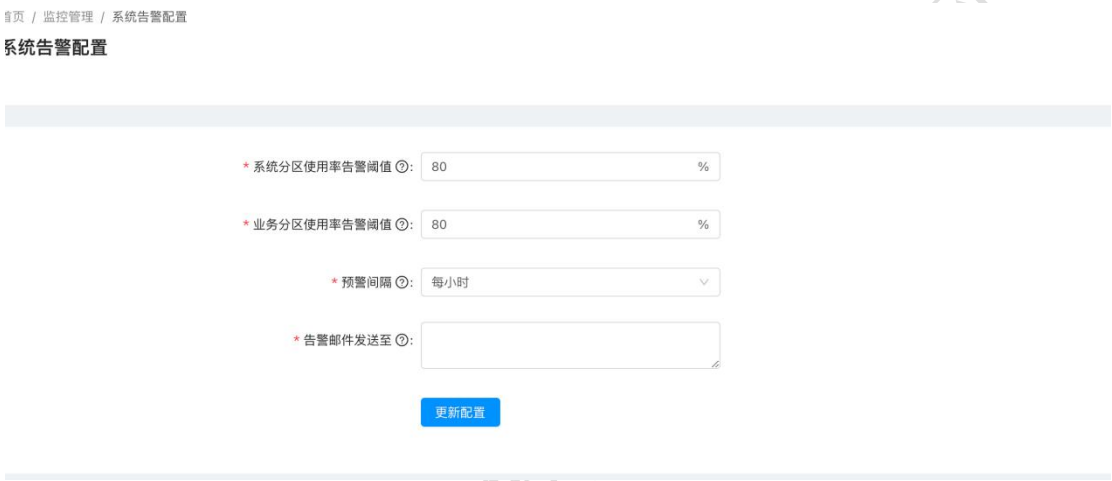

图 71. 系统告警配置

14.3. 蜜罐监控

展示客户端的状态、版本、CPU 占用、内存占用、硬盘情况以及蜜罐的服务状态、CPU 占用、内存占用、网络状态。

15. 硬件配置

15.1. 证书配置

证书是用来对系统内的功能和使用时长进行限制，证书包含允许使用的蜜罐数量、过期时间等内容，若用户想延长系统的使用期限等功能，需要购买证书，然后在证书管理页面进行更新证书。

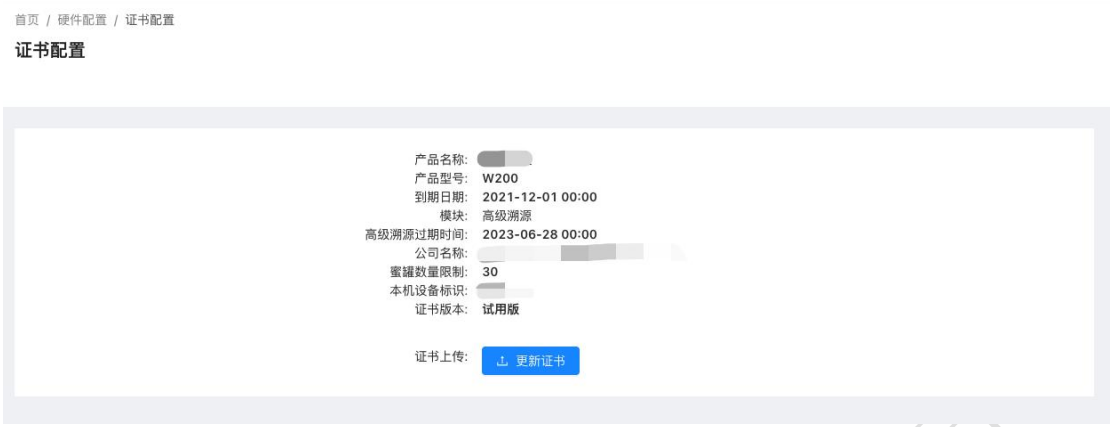

图 72. 证书配置

15.2. 网络配置

此页面可根据用户网络环境需要，对宿主机的网络进行配置。

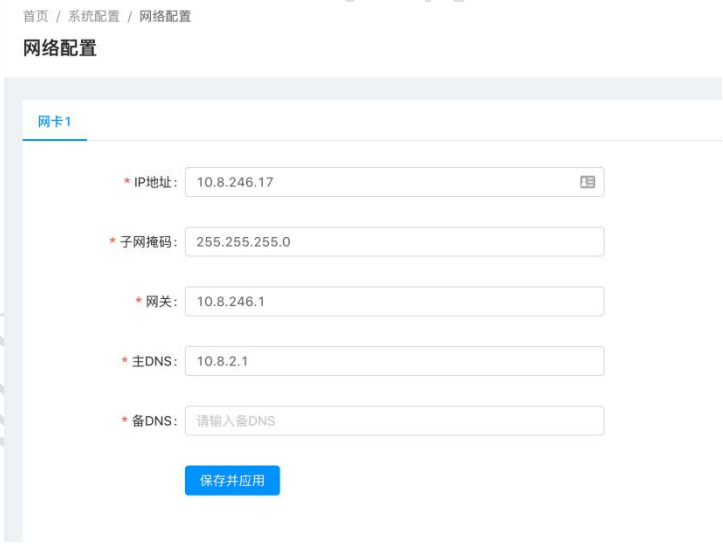

图 73. 网络配置

16. 升级更新

系统升级有两种模式。自动升级是系统检测到有新版本时，每天凌晨 3 点系统自动进行升级操作。手动升级是当系统检测到有新版本时，手动将新版本的文件包（pkg 格式）拖拽至指定区域进行上传。

系统升级后，会显示升级的版本号、日期、状态和详情信息。升级成功会显示更新的详情内容，升级失败会显示对应的错误信息。

图 74. 系统升级

17. 问题排查

17.1. 错误日志导出

当系统发送运行时错误时，用户可以点击“打包日志”导出最近产生的日志，供业务开发人员排查问题。

图 75. 错误日志导出

17.2. 远程协助

当遇到异常问题，用户需要先与厂商联系沟通，等待厂商确认后，方可进行远程协助操作。

设备连接到互联网情况下，开启远程协助功能可以让厂商支持人员在对应的远程协助频道进行远程支持和故障排查（操作完成后请关闭远程协助功能）。

如果远程协助启动失败，请检查 token 是否输入正确以及远程协助服务器连接是否正常。

图 76. 远程协助

18. 账号设置

点击系统右上角的用户名，可以选择“账号设置”进行用户信息的修改以及安全设置，修改账户密码或绑定邮箱、密保手机。

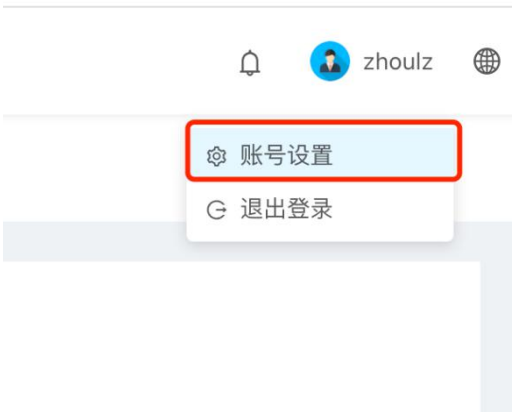

图 77. 账号设置

图 78. 安全设置

19. 通知管理

用户可通过右上角的铃铛进入通知管理页面。

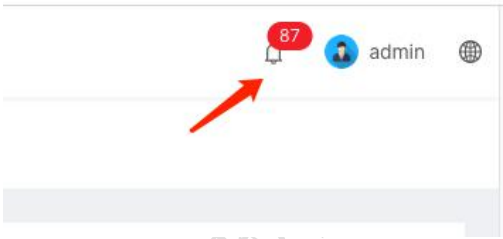

图 79. 告警通知入口

配置了系统告警配置的预警阈值后，当出现预设情况的空间占用，则会在站内进行告警通知。

当蜜罐捕捉到新的攻击源事件时，也会进行告警通知。

可删除告警消息，也可对未读消息标记为已读，对已读消息标记为未读。

图 80. 告警通知

附录 1. 中继模式配置方法

1. 假设前提

1) 蜜罐系统控制中心以 Access 端口接入 vlan 246 、IP 10.8.246.6/24;

2) 交换机 Trunk 端口允许 vlan 250，251;

需要对交换机，以及客户端网卡进行如下配置:

2. 交换机配置

除了 Trunk 端口本身 vlan 配置以外，还需要保证客户端设备可以访问蜜罐系统控制中心，所以交换机上配置如下（不同交换机的配置命令可能存在差异，需要根据具体的交换机型号进行配置）:

1) port link-type trunk

2) port trunk pvid vlan 246

3) port trunk permit vlan 246 250 251

```
<sw-ioffice-11f-ad>sys
System View: return to User View with Ctrl+Z.
[sw-ioffice-11f-ad]interface GigabitEthernet1/0/10
[sw-ioffice-11f-ad-GigabitEthernet1/0/10]port link-type trunk
[sw-ioffice-11f-ad-GigabitEthernet1/0/10]port trunk pvid vlan 246
[sw-ioffice-11f-ad-GigabitEthernet1/0/10]port trunk permit vlan 246 250 251
[sw-ioffice-11f-ad-GigabitEthernet1/0/10]dis this
#
interface GigabitEthernet1/0/10
 port link-type trunk
 port trunk permit vlan 1 246 250 to 251
 port trunk pvid vlan 246
#
return
```

图 81. 交换机配置

其中 pvid 与蜜罐系统控制中心的 vlan 一致，使客户端与蜜罐系统控制中心服务联通。

3. 客户端网卡配置

客户端可能存在两种部署方式：独立客户端设备，以及系统内置客户端。用户可自行配置独立客户端，系统内置客户端请联系厂商进行协助配置。

3.1 独立客户端网络配置

配置好客户端网卡 、子网掩 IP 码、网关，保证可以连通控制中心即可。

3.2 系统内置客户端配置（隔离网卡）

内置客户端需要隔离客户端网卡，将如下配置添加到/etc/rc.local 中(其中其中网卡名、IP、子网掩码以及网关，需要根据现场进行配置):

```
# 网卡名、IP、子网掩码以及网关，需要根据现场配置
# set real name and addr
isolateIfaceName="eno2"
isolateIfaceIp="192.168.2.100"
isolateIfaceMask="24"
isolateIfaceateway="192.168.2.1"

# create netns
netnsName="beehive_net_ns"

ip netns add ${netnsName}
ip link set $isolateIfaceName netns ${netnsName}
ip netns exec ${netnsName} ip addr add ${isolateIfaceIp}/${isolateIfaceMask} dev ${isolateIfaceName}
ip netns exec ${netnsName} ip link set ${isolateIfaceName} up
ip netns exec ${netnsName} ip route add default via ${isolateIfaceateway} dev ${isolateIfaceName} src ${isolateIfaceIp}
```