创宇蜜罐

威胁诱捕与溯源系统

用户手册 V1.9.1「SaaSV3.3.8」

（文档编号：MG-SY-2021-007）

文档说明

威胁诱捕与溯源系统用户手册 V1.9.1「SaaSV3.3.8」

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

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. 风险大盘

2.1. 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。

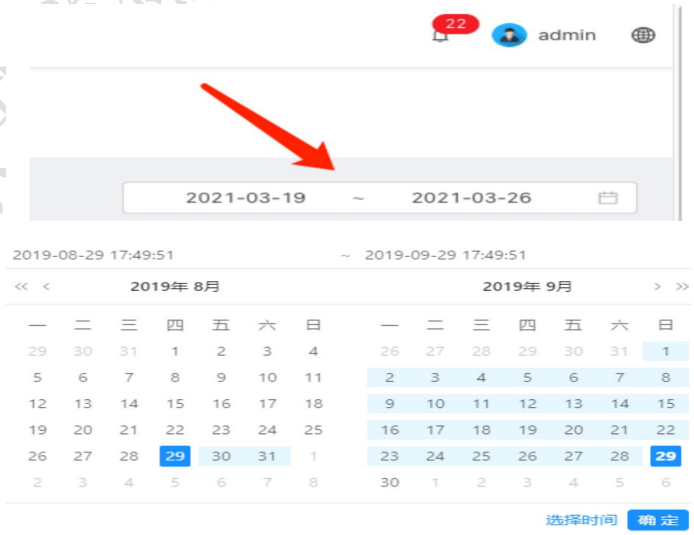

图 2. 选择时间段

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。

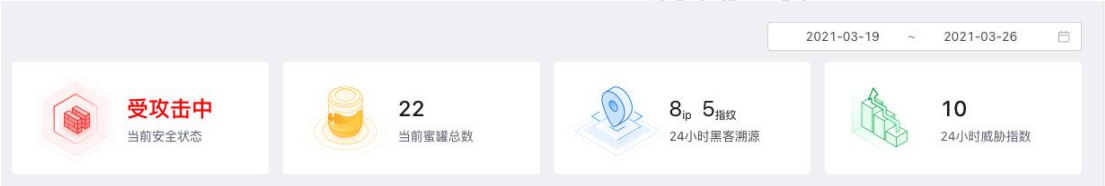

图 3. 威胁总览

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。

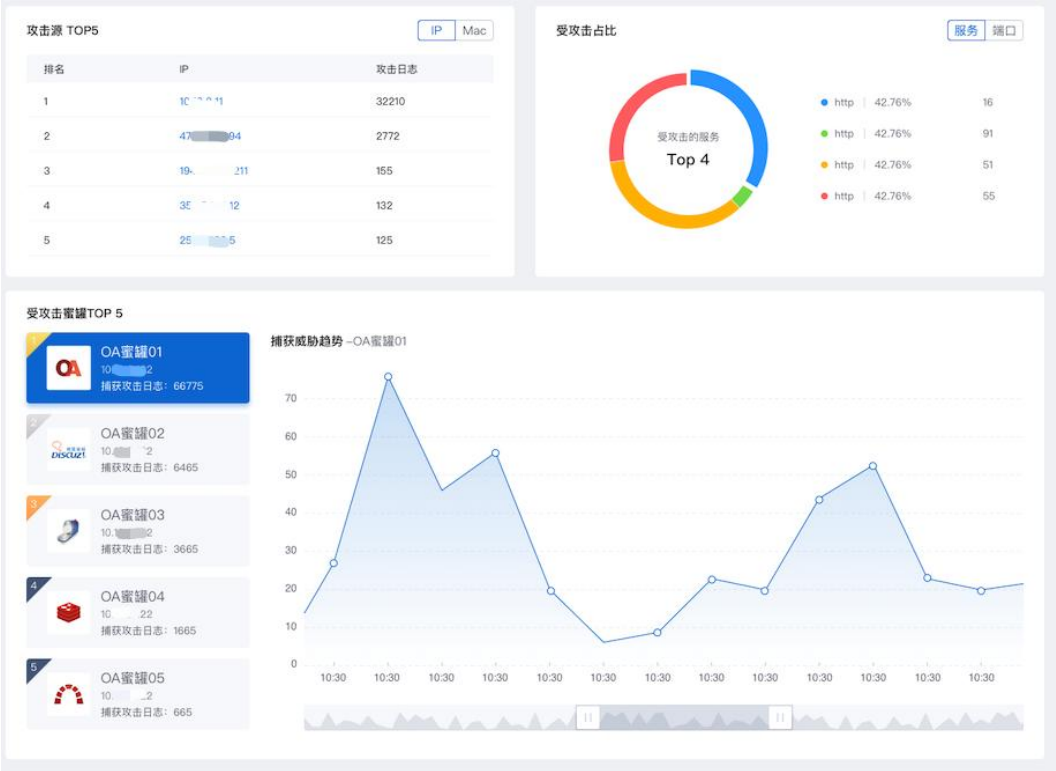

图 5. 攻击源和受攻击占比

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。

支持对攻击者、蜜罐、攻击日志进行下钻，查看对应详情。

图 6. 蜜罐安全态势

5. 蜜罐管理

5.1. 蜜罐部署

5.1.1. 部署云蜜罐

云蜜罐适用于外网蜜罐场景，有域名即可接入多个云蜜罐。蜜罐将伪装成常见的 Web 站点（如：Discuz、WordPress、OA、禅道、云盘等），引诱黑客访问域名、进入云蜜罐，并记录黑客在云蜜罐中的行为，可对黑客进行全网溯源、反制。

1) 点击“蜜罐管理”菜单，点击页面右上角的“部署蜜罐”按钮，选择“云蜜罐”，进入部署云蜜罐页面。（首次部署时，可在风险大盘页面点击“立即部署”按钮后，选择“云蜜罐”进入部署页面）；

图 7. 部署蜜罐入口

图 8. 选择云蜜罐

2) 进入部署云蜜罐页面，首先需要输入用户自己的根域名；

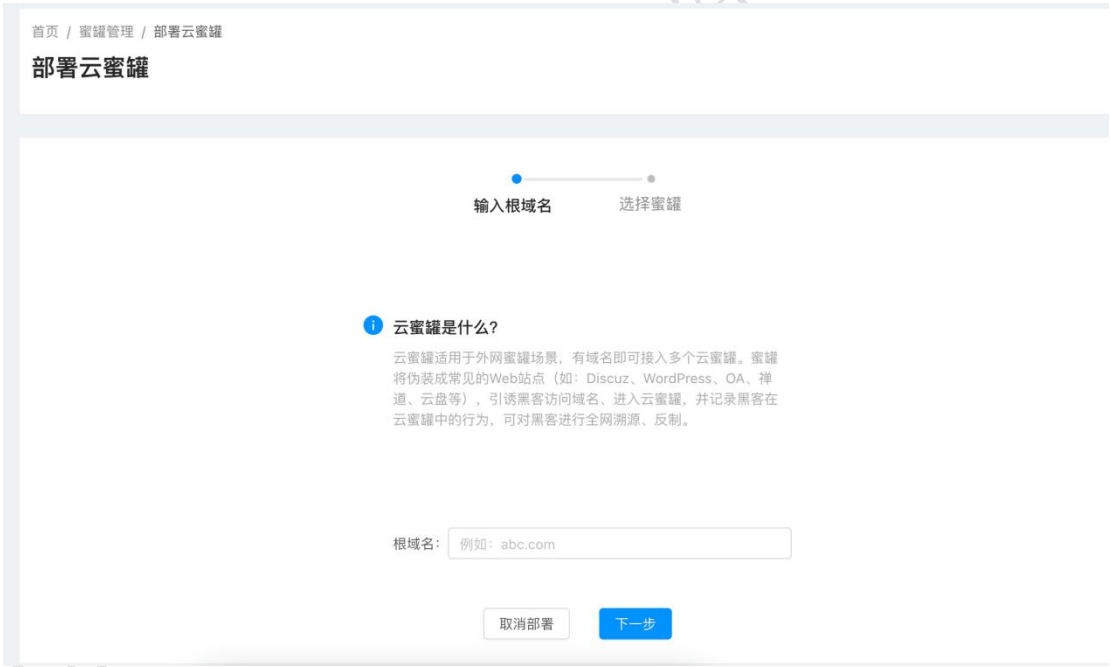

图 9. 输入根域名

3) 点击下一步，根据第一步输入的根域名，选择云蜜罐类型并输入子域名；（首次部署或选择了蜜罐类型后，蜜罐系统会智能推荐对应的子域名，请根据实际情况进行子域名部署，请勿输入与真实业务相同或是已部署过蜜罐的子域名。）列表左上方展示了当前可接入的云蜜罐数量，右上方可添加和清空当前正在部署的云蜜罐数据，也可直接删除单条数据；

图 10. 添加云蜜罐

4) 点击“部署蜜罐”按钮，回到蜜罐列表页，此时蜜罐状态为“审核中”，请主动联系商务经理推动审核；若审核失败，可联系厂商处理。

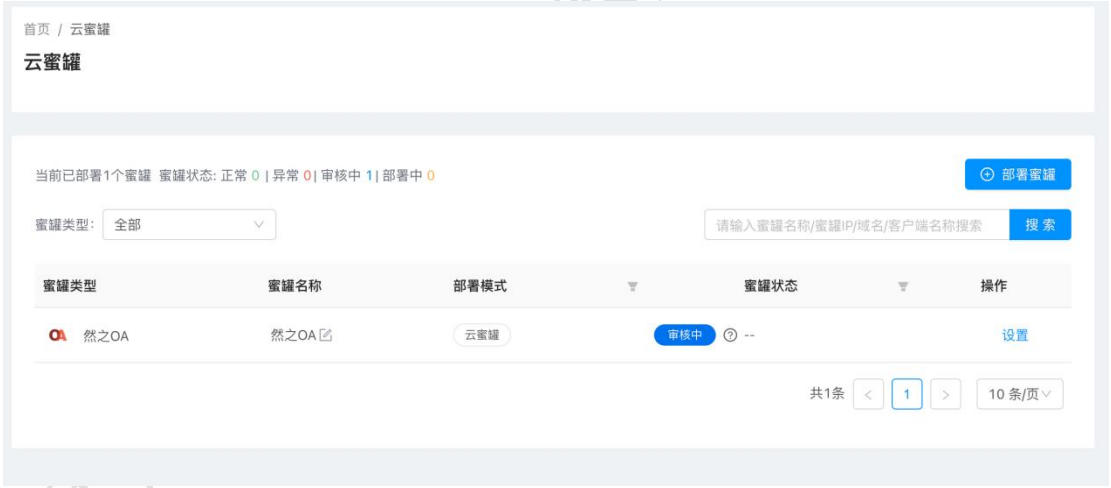

图 11. 云蜜罐审核中

5) 审核通过后，蜜罐状态会变为“待解析”，此时需要根据根域名的具体情况，到对应的域名提供商平台进行域名解析，点击“去解析域名”可在域名解析说明页查看具体配置步骤；

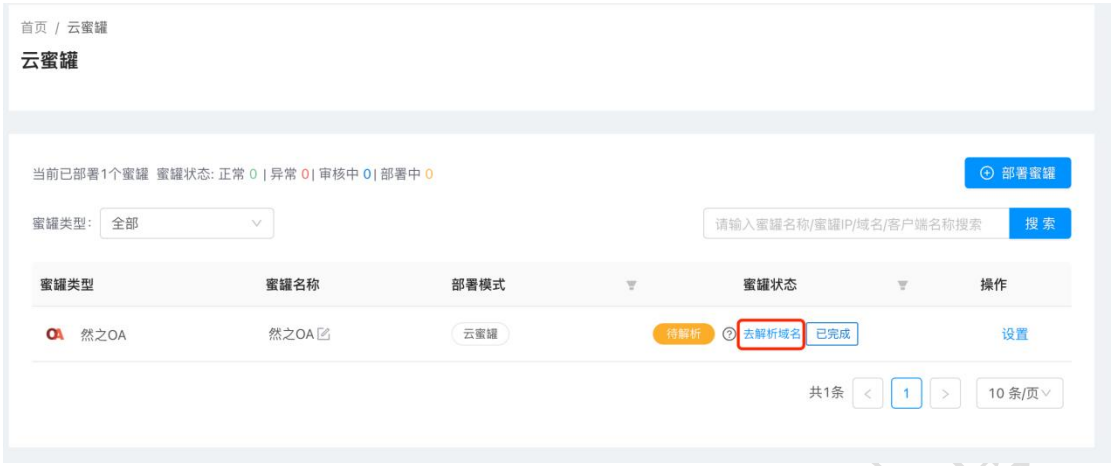

图 12. 云蜜罐待解析

6) 根据域名解析说明页的配置步骤，到对应域名提供商平台将当前记录的子域名进行 A 记录解析，解析到当前的蜜罐 IP 地址上。

图 13. 域名解析说明

7) 返回蜜罐列表页，在蜜罐状态处点击“已完成”按钮，蜜罐状态变为正常时，则部署成功，此时通过该子域名可访问到蜜罐。

图 14. 云蜜罐待解析-已完成

图 15. 云蜜罐成功部署

云蜜罐状态说明

- 正常：蜜罐正常运行。
- 审核中：系统审核中，可联系厂商进行审核。
- 审核失败：系统审核失败，若有疑问，请联系厂商。
- 待解析：请根据解析指南到域名厂商处进行域名解析，若已配置解析请点击蜜罐列表中的“已完成”按钮。
- 异常：蜜罐状态异常，可尝试重置蜜罐或重新部署蜜罐。
- 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，可删除蜜罐后进行重新

部署。

5.1.2. 部署客户端蜜罐

客户端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，进入部署客户端蜜罐页面，（首次部署时，可在风险大盘页面点击“立即部署”按钮后，选择“客户端蜜罐”进入部署页面）；

图 16. 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，进入部署客户端蜜罐页面；

图 17. 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）；

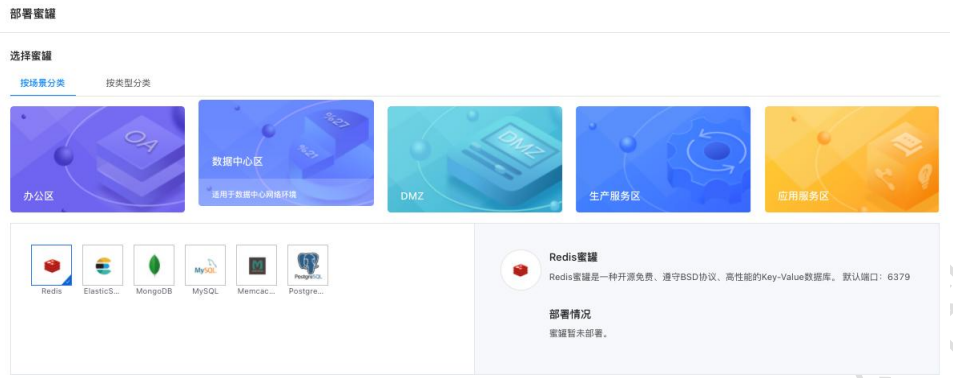

图 18. 根据场景选择蜜罐

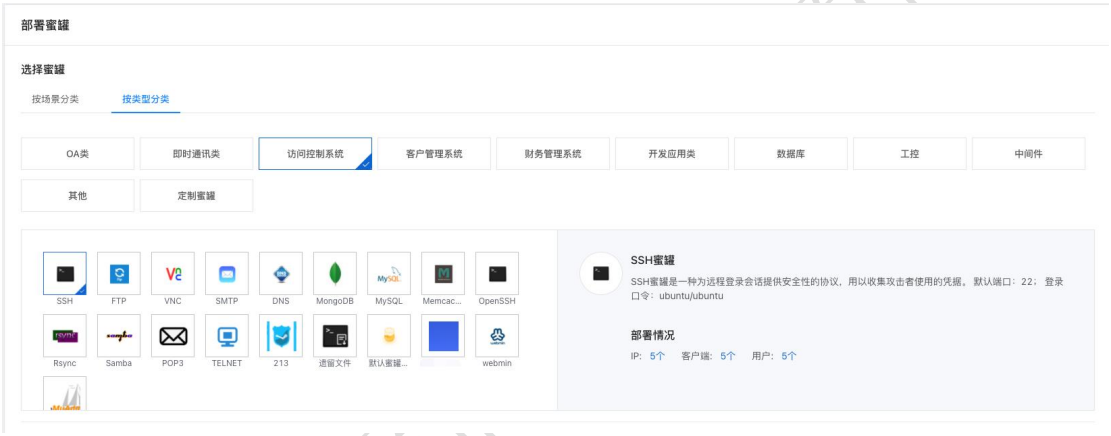

图 19. 根据类型选择蜜罐

3) 选择好蜜罐类型后，继续配置蜜罐：

用户在需要防护的网段中部署了一台客户端后，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，用户需要部署多台客户端设备，或是拥有一台多网口的客户端设备。

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，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；此阶段可在蜜罐 IP 最右侧框中输入多组数字，如：22,89,100-103，就能够在客户端设备上生成多个虚拟网卡指向蜜罐，此时就有多个 IP 入口可进入蜜罐，实现 IP 覆盖；

④ 服务端口设置：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 20. 部署客户端蜜罐

- **甜度设置（可选）**

蜜罐详情中，可开启甜度设置，此操作可选，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 21. 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 22. 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云蜜罐还是客户端蜜罐，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。

蜜罐支持批量删除，勾选需要删除的蜜罐，点击右上角删除按钮即可进行批量删除。

图 23. 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。

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。

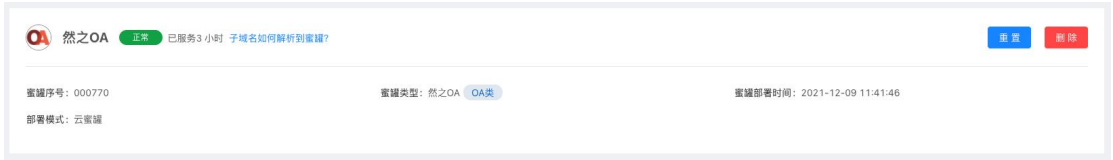

图 24. 蜜罐设置页

- **云蜜罐信息**

在“蜜罐信息”模块可查看当前云蜜罐对应的子域名与需要解析到的蜜罐 IP，也可对云蜜罐的子域名进行修改（修改后需要到域名提供商平台重新解析）。

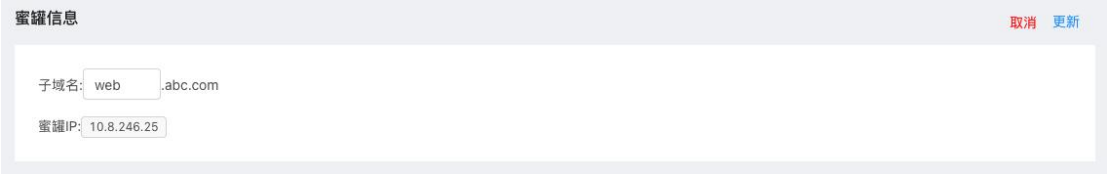

图 25. 蜜罐设置页-云蜜罐信息

- **客户端蜜罐信息**

在“蜜罐信息”模块可查看当前客户端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。

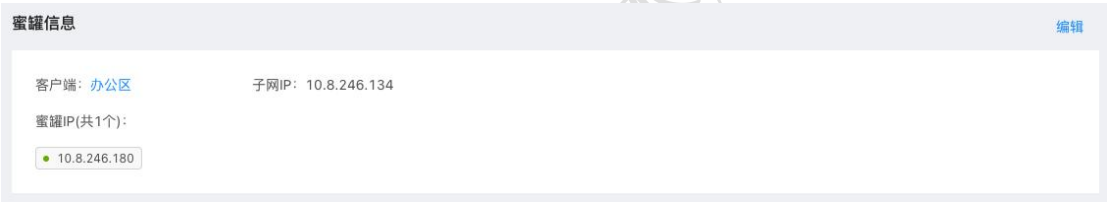

图 26. 蜜罐设置页-客户端蜜罐信息

- **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。）

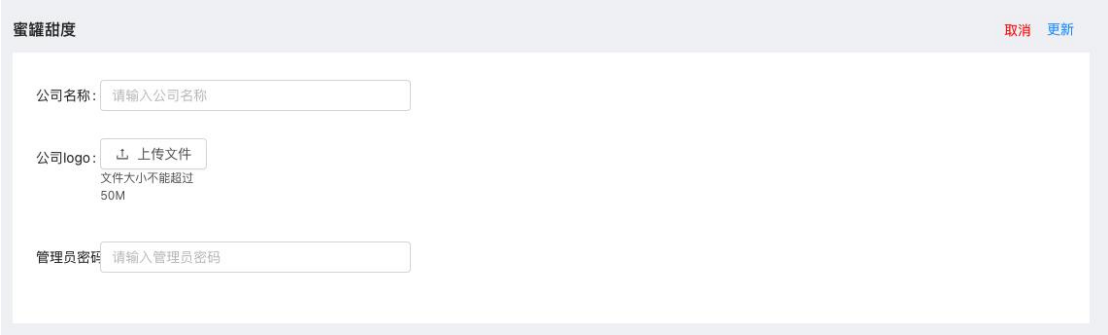

图 27. 蜜罐设置页-甜度设置

- **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 28. 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“蜜罐管理-->部署蜜罐-->添加定制蜜罐”或“策略配置-->蜜罐模板配置-->» 添加模板”进入定制蜜罐页面。

图 29. 部署蜜罐-定制蜜罐

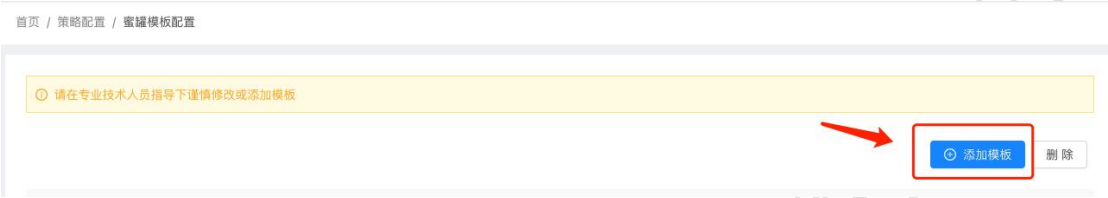

图 30. 蜜罐模板配置-添加模板

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 31. 蜜罐模板配置-克隆蜜罐

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 32. 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 33. 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 34. 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。

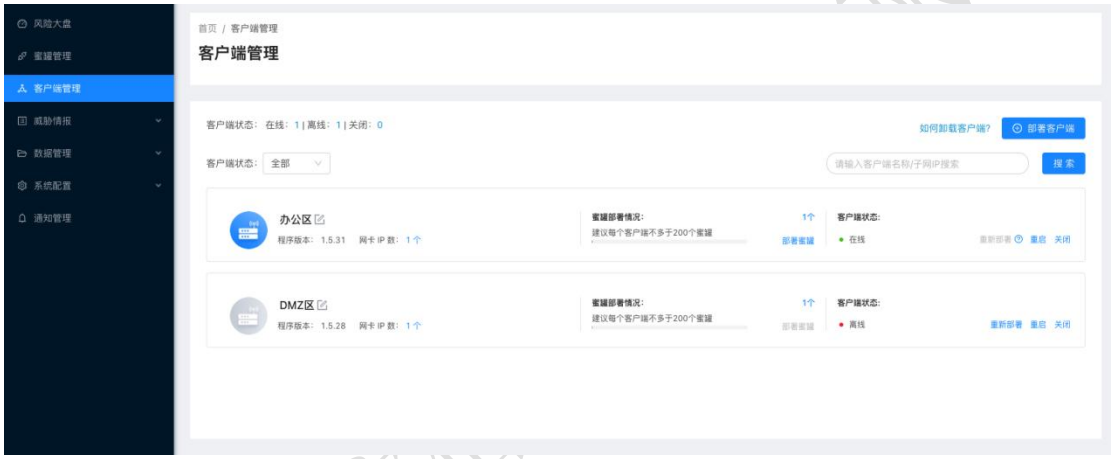

图 35. 客户端列表

6.2. 客户端部署

用户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。

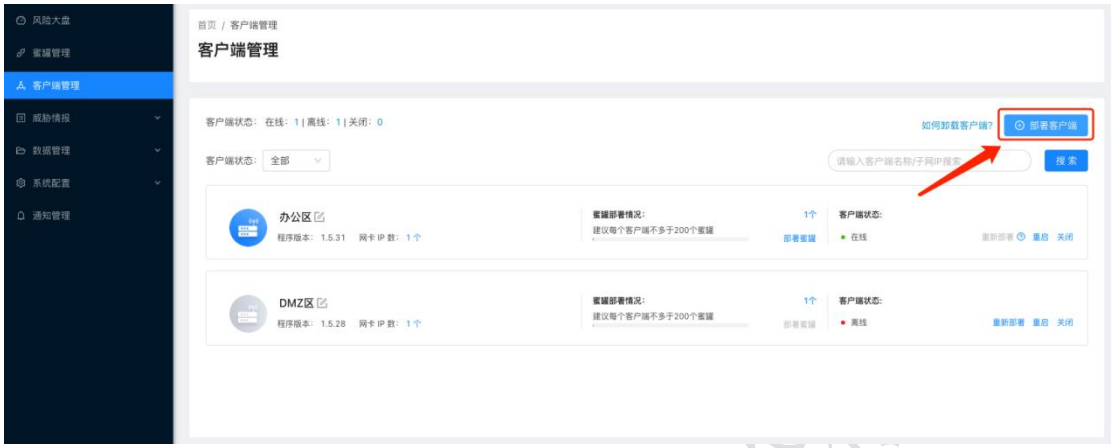

图 36. 点击部署客户端

图 37. 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。

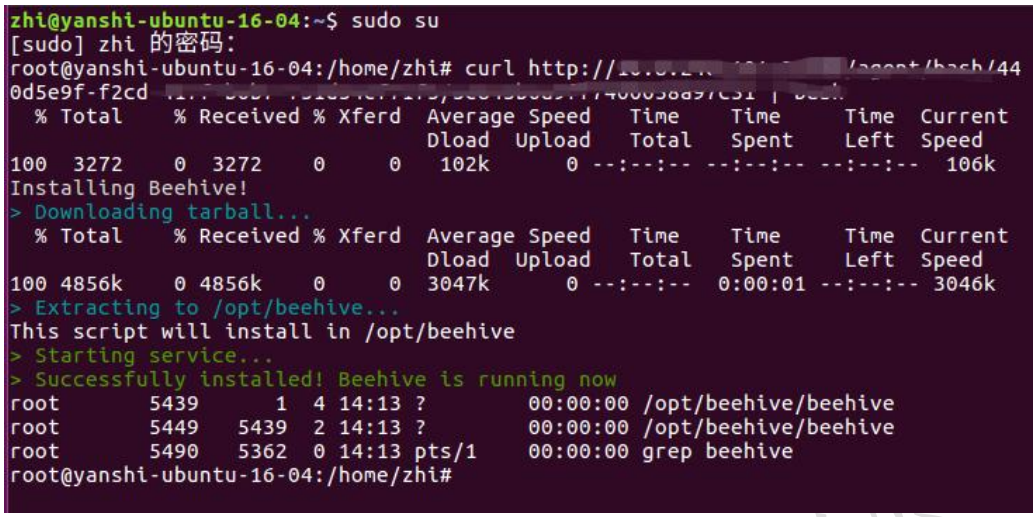

图 38. 部署成功后的提示

3) 部署成功后，客户端状态为“在线”。

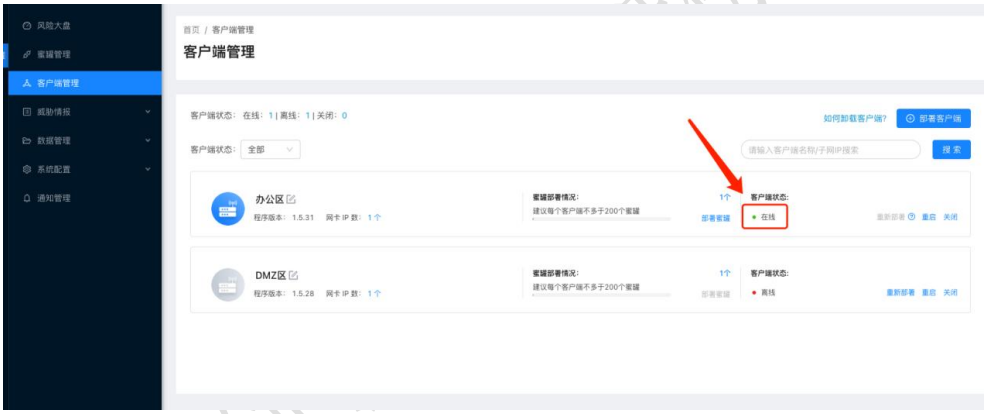

图 39. 部署成功后客户端状态

客户端状态说明

- --：当前暂未部署客户端，可粘贴部署命令至设备中进行客户端部署。
- 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。
- 关闭：已关闭客户端设备与管理中心的连接，如有需要，请重新开启。

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) 关闭：若想断开客户端连接，可对在线的客户端进行“关闭”操作；

4) 开启：若想开启客户端连接，可对关闭的客户端进行“开启”操作；

5) 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 40. 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 41. 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 42. 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 43. 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）；

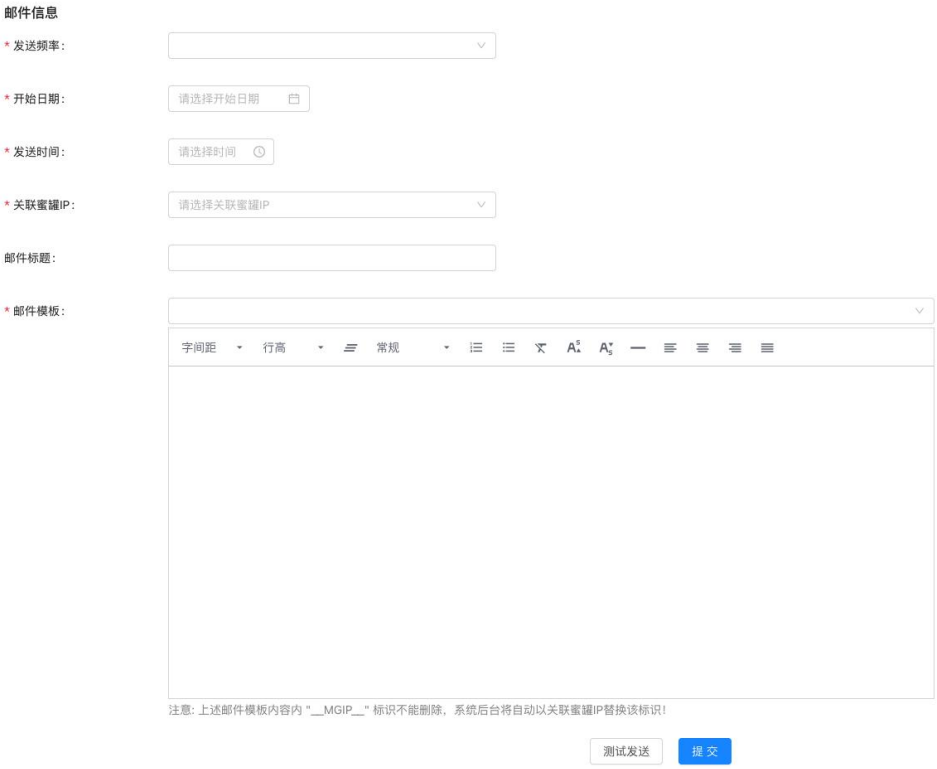

图 44. 邮件蜜饵-邮件信息

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 45. 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 46. 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 47. 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 48. 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。

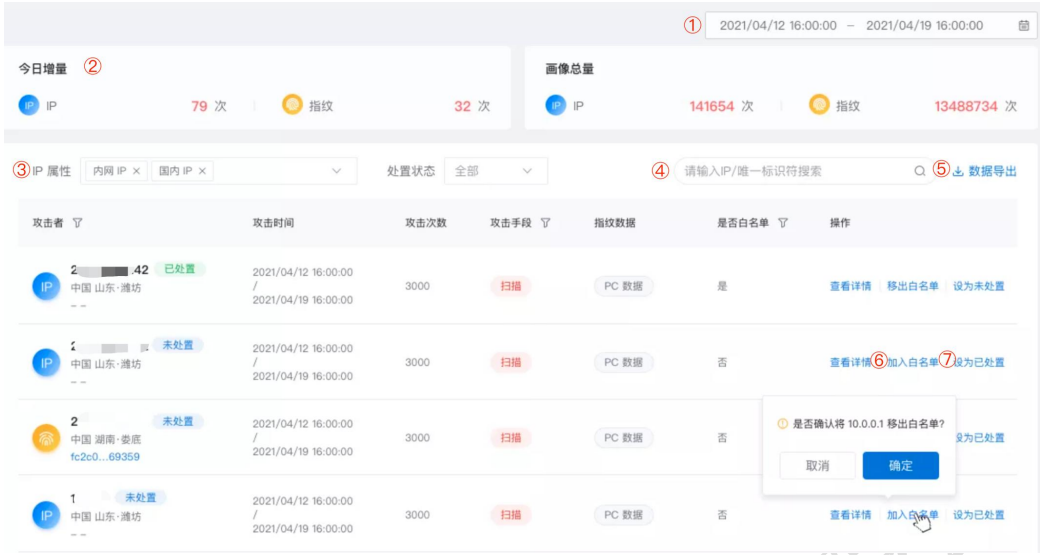

图 49. 攻击者画像列表

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 的攻击数据信息以及其他攻击者相关信息，包括:

- 攻击者 IP
- 攻击数据统计：攻击总次数、开始攻击时间、最新攻击时间、攻击蜜罐及对应次数

- 攻击趋势：攻击频率时间轴
- 攻击手段：攻击手段 TOP5 统计
- 攻击记录：攻击历史记录时间轴
- 指纹数据：包括攻击者的网络数据、PC 信息、指纹关联攻击者
- 虚拟身份信息
- 高精地理位置
- 全网攻击数据
- 外部威胁情报

点击「画像下载」即可以图片形式保存当前攻击者画像信息。

8.2. 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，另 web 类蜜罐会捕获 web 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），也可在对应的【文件上传】日志进行文件下载。

图 50. 攻击者画像详情-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；
- 上传文件的攻击日志支持文件下载；
- 点击单条日志左侧的“+”号可以查看具体的日志内容。

图 51. 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。

- **一键过滤扫描攻击日志**

用户可一键过滤扫描攻击类日志，聚焦高价值日志。

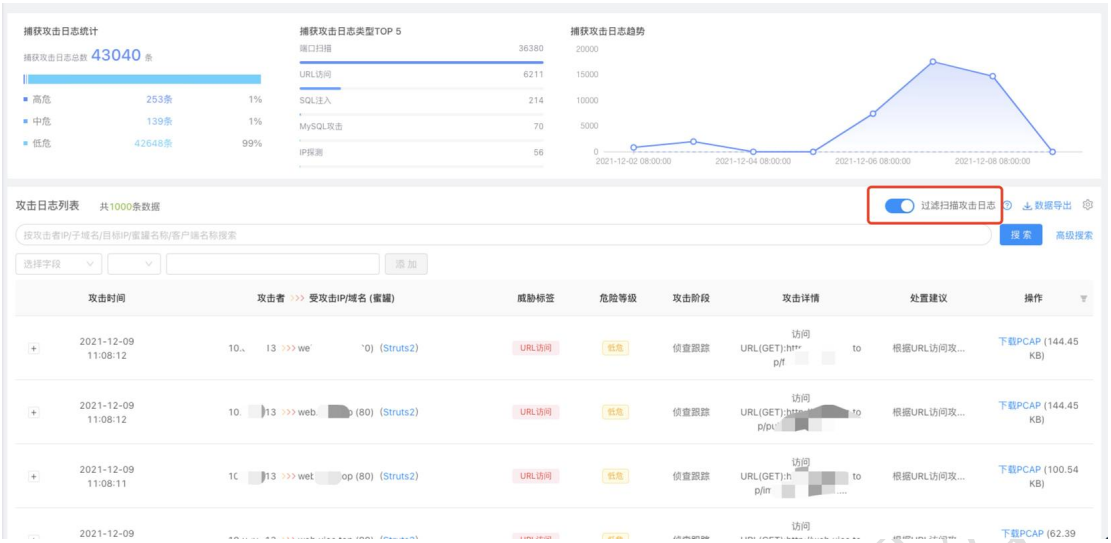

图 52. 攻击日志-一键过滤扫描攻击日志

- **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。

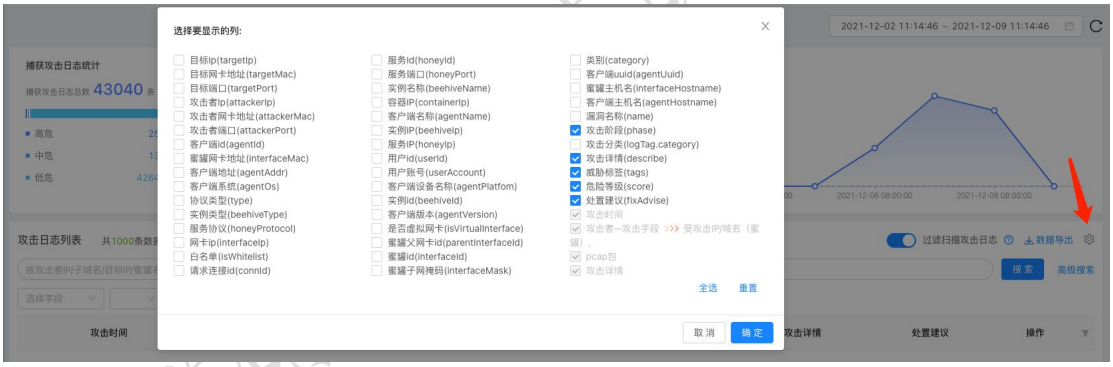

图 53. 攻击日志-列设置

- **简单搜索**

日志系统提供简洁易用的条件过滤搜索器，用户可根据关键字进行快速搜索，也可根据指定字段添加条件搜索，各个条件可以快速启用/禁用/删除。

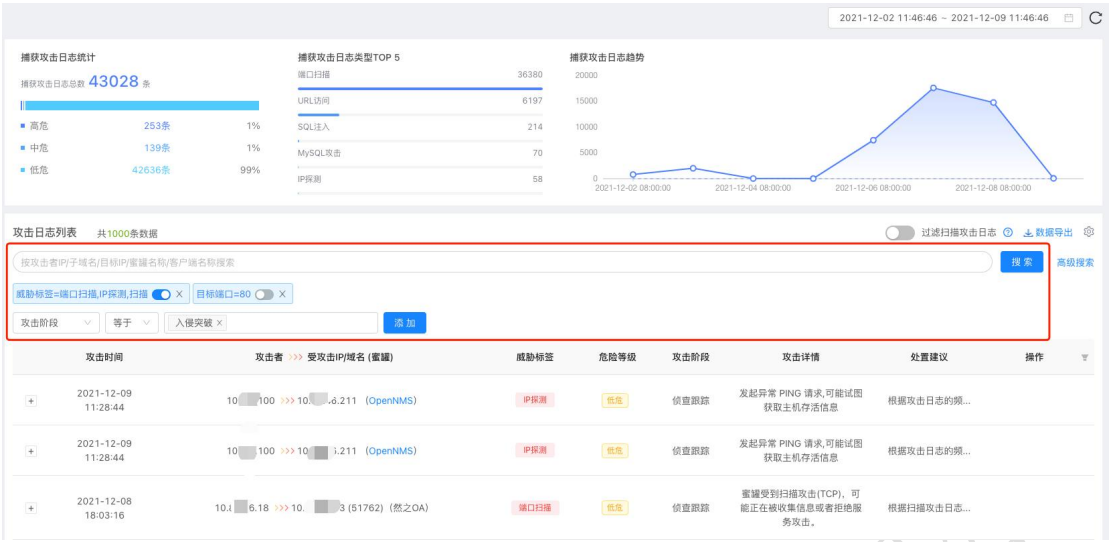

图 54.　攻击日志-简单搜索

- **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。

点击【语法帮助】，查看查询语句与示例，帮助用户快速学习使用高级搜索语法。

图 55.　攻击日志-高级搜索

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。

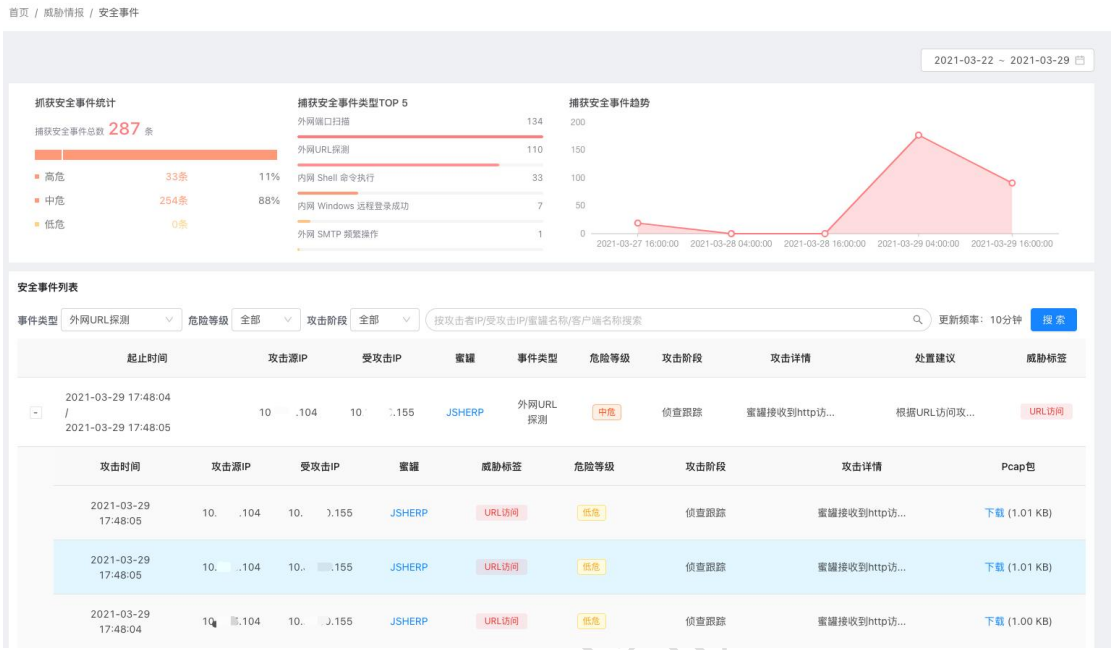

图 56. 安全事件

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；

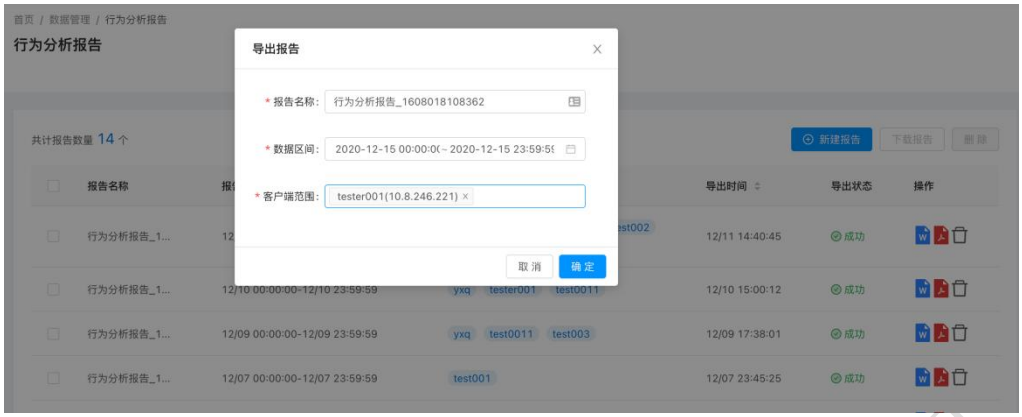

图 57. 新建报告

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 58. 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 59. 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 60. 日志下载按钮

图 61. 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。

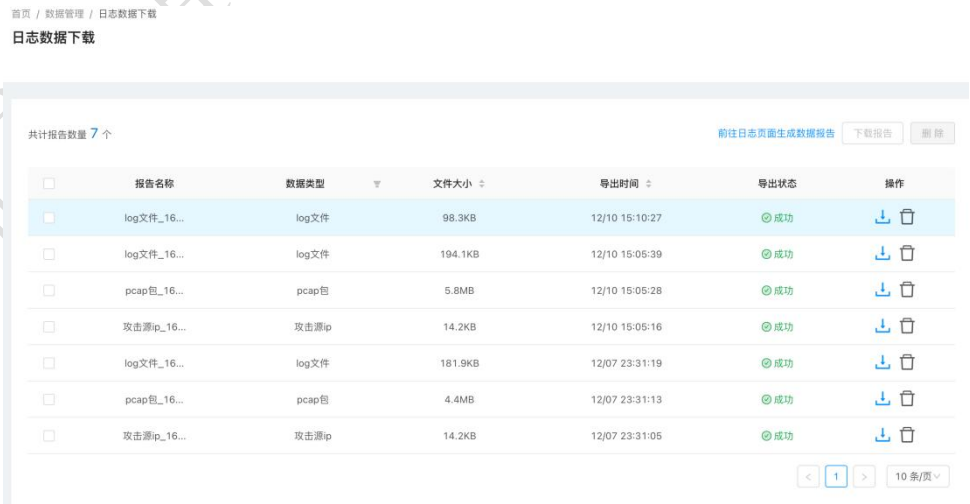

图 62. 日志数据列表

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 63. 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 64. 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 65. 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 66. 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。

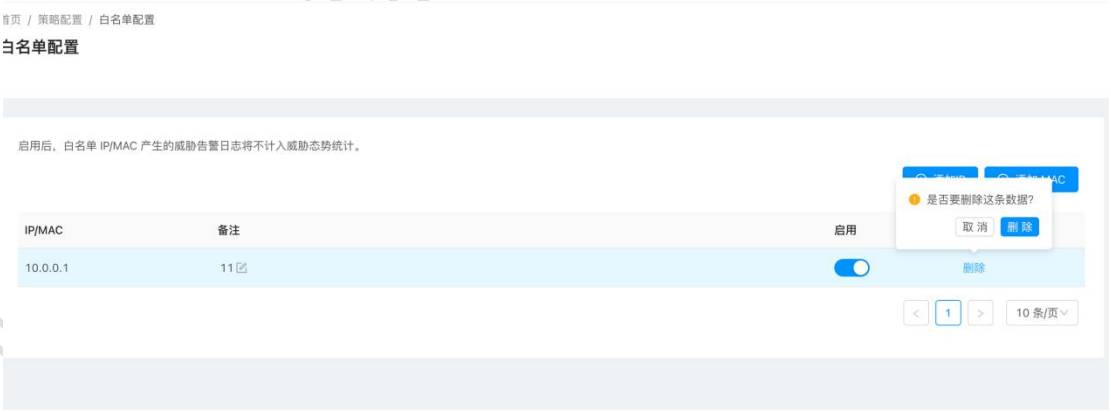

图 67. 删除白名单

10.3. 蜜罐模板配置

10.3.1. 默认蜜罐

用于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。

10.3.2. 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）。

11. 监控管理

展示客户端的状态、版本、CPU 占用、内存占用、硬盘情况。

12. 通知管理

12.1. 威胁告警

若部署了蜜罐后，蜜罐被攻击者攻击，则系统内会产生威胁告警。告警信息中会记录详细的攻击源 IP，点击“查看”会链接到威胁事件页面。

图 68. 威胁告警

可对未读消息标记为已读，也可对已读消息标记为未读。

12.2. 系统通知

部署的客户端离线或者恢复在线，都会在消息中心收到通知。蜜罐状态异常

或恢复正常，也会在消息中心收到通知。客户端相关的通知，点击“查看”会链接到客户端列表页面。蜜罐状态相关的通知，点击“查看”会链接到蜜罐详情页面。

图 69. 系统通知

可对未读消息标记为已读，也可对已读消息标记为未读。