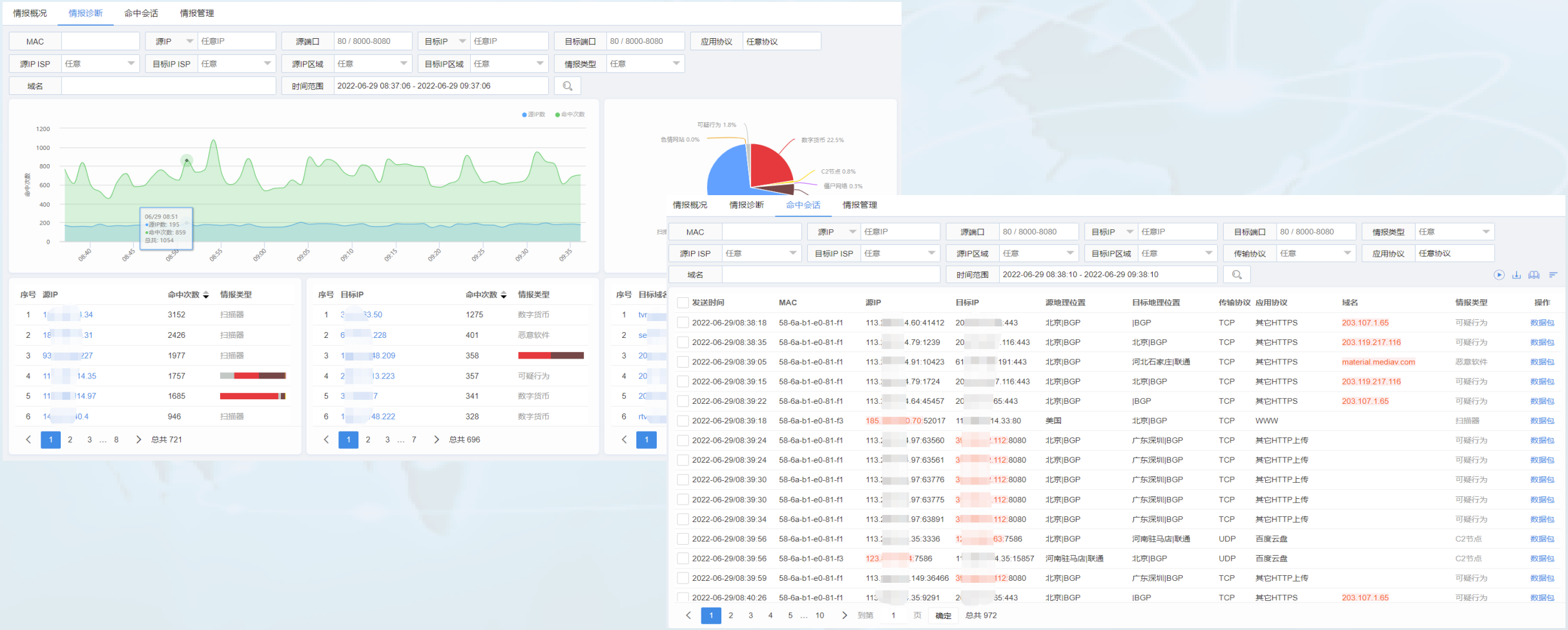
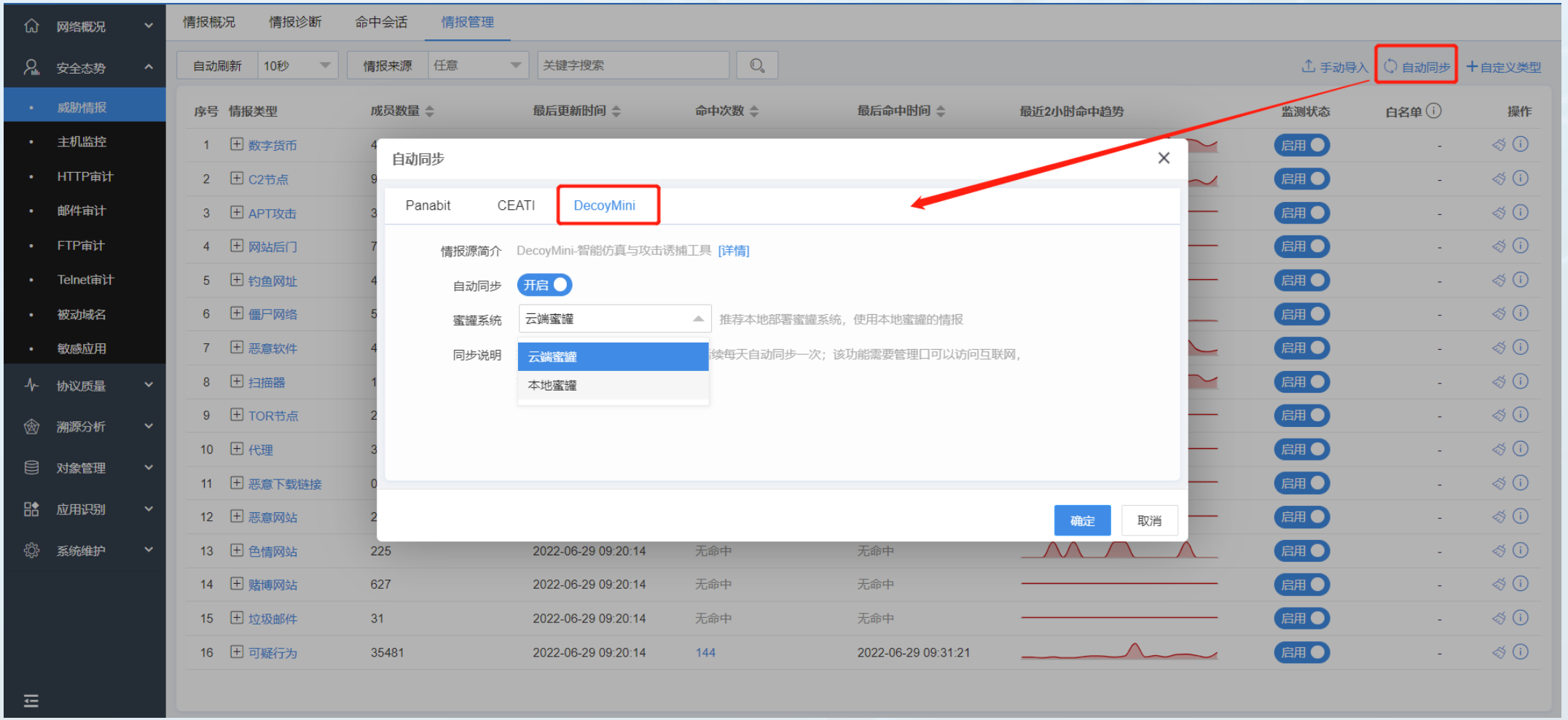
免费蜜罐软件——DecoyMini介绍

Panabit NTM与威胁情报



作为一个汇集多种威胁情报源的平台，Panabit NTM可以为情报的匹配提供免费载体，对匹配威胁情报的流量进行发现与溯源

NTM支持DecoyMini本地情报



Panabit NTM TANGr1p1版本中，支持与DecoyMini进行对接

真实案例-某高校日志服务器被入侵事件

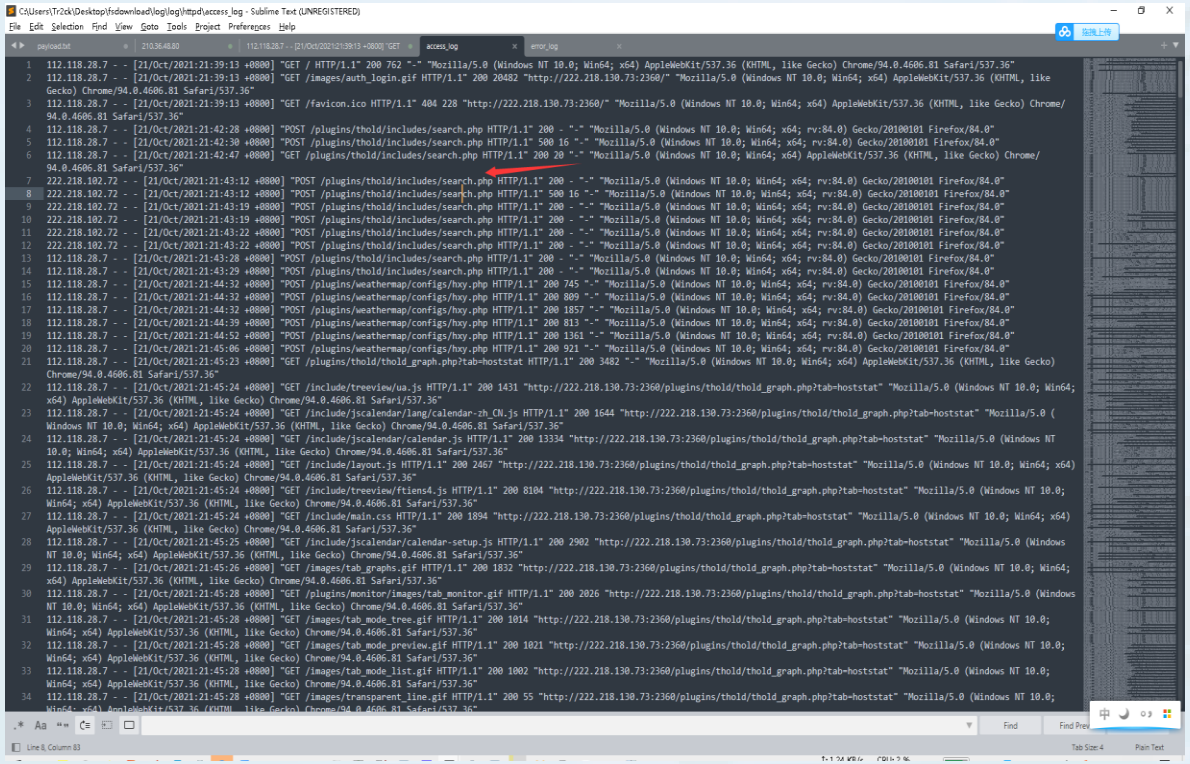
事件 / 风险事件 admin

查询 导出 提交情报...

#	名称	级别	类型	标签	描述	IP	时间	操作
1	SSH服务诱捕到Login事件(4)	高	服务访问	SSH服务 Login	用户 root 登录成功	172.16.0.236	2021-10-21 22:13:31	
2	新华网诱捕到GET事件(11)	中	WEB访问	新华网 GET	访问首页: /	172.16.0.236	2021-10-21 22:06:56	
3	WEB业务系统诱捕到GET事件(22)	中	WEB访问	WEB业务系统 GET	访问首页: /	172.16.0.236	2021-10-21 22:06:53	
4	WebLogic诱捕到GET事件(11)	中	中间件访问	WebLogic GET	访问首页: /	172.16.0.236	2021-10-21 22:06:51	
5	FTP服务诱捕到Auth事件(2)	高	服务访问	FTP服务 Auth	用户登录(User: admin; Pwd: 123456)	172.16.0.236	2021-10-21 22:06:49	
6	FTP服务诱捕到Auth事件(132)	中	服务访问	FTP服务 Auth	用户登录(User: ftp; Pwd: 123456)	172.16.0.236	2021-10-21 22:06:49	
7	log.TCP诱捕到TryConn事件(9)	中	网络操作	log.TCP TryConn	172.16.0.236:35856 尝试连接 172.16.0.137:445	172.16.0.236	2021-10-21 22:06:42	
8	log.ICMP诱捕到ICMP事件(2)	中	网络操作	log.ICMP ICMP	172.16.0.236 Ping 172.16.0.33	172.16.0.236	2021-10-21 22:06:21	

10	服务访问	SSH服务	Exec	执行命令: exit		成功	信息	172.16.0.236
11	服务访问	SSH服务	Exec	执行命令: ls -l /usr/sbin		成功	信息	172.16.0.236
12	服务访问	SSH服务	Exec	执行命令: ls -l /usr		成功	信息	172.16.0.236
13	服务访问	SSH服务	Exec	执行未知命令: /usr/sbin/ifconfig		失败	信息	172.16.0.236
14	服务访问	SSH服务	登录	用户 root 登录成功		成功	严重	172.16.0.236
15	服务访问	SSH服务	Exec	执行命令: ls -l /bash		成功	信息	172.16.0.236
16	服务访问	SSH服务	Exec	执行命令: ls -l /bin		成功	信息	172.16.0.236
17	服务访问	SSH服务	Exec	执行命令: ls -l		成功	信息	172.16.0.236
18	服务访问	SSH服务	Exec	执行命令: cd		成功	信息	172.16.0.236
19	服务访问	SSH服务	Exec	执行命令: cd ~		成功	信息	172.16.0.236
20	服务访问	SSH服务	Exec	执行命令: pwd		成功	信息	172.16.0.236

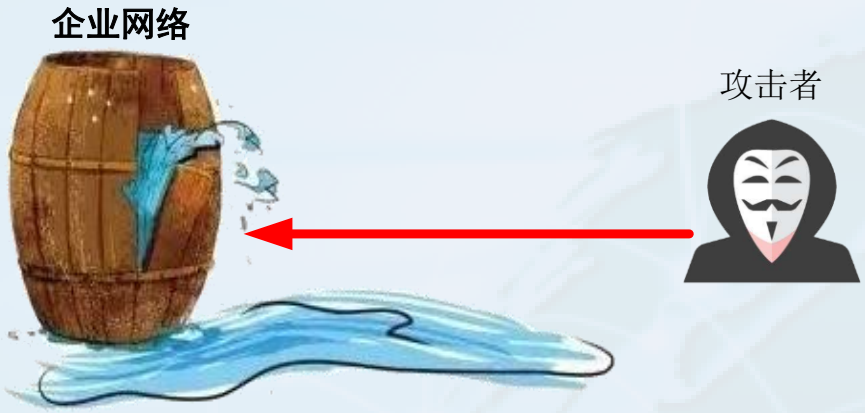
真实案例-某高校日志服务器被入侵事件



本次事件攻击者通过日志服务器80端口WEB服务的漏洞进入内网

由于该高校内网部署了DecoyMini，在攻击者刚进入内网进行环境探测阶段就及时被蜜罐监测发现，并及时进行了预警。在运维人员的快速处置下，第一时间阻断了攻击的进一步扩散，避免了更大的损失。

欺骗防御技术



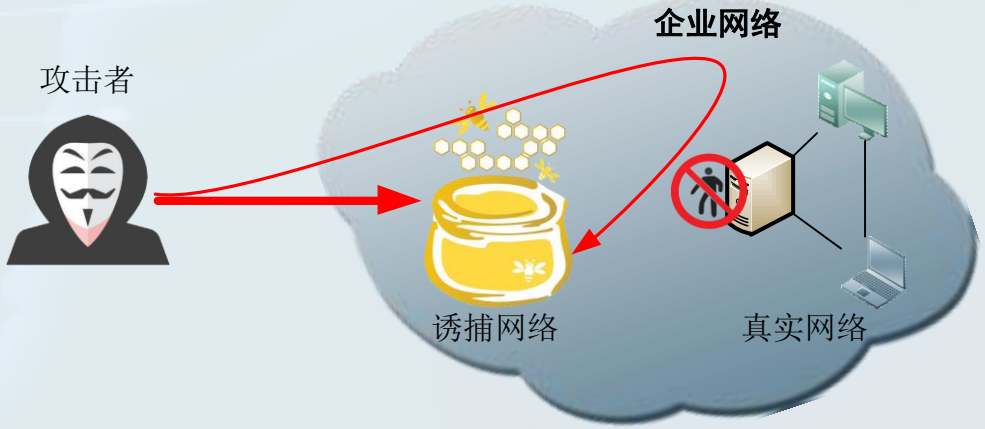
“木桶理论”：整体的安全性取决于最薄弱的一个环节

传统网络防御中，防守者需要充分、全面、完整的对网络和系统的安全漏洞和风险进行分析、评估和整改来确保整个网络的安全。

但企业攻击面众多，很难完全及时发现所有问题或风险，攻击者只需要抓住一次机会就可以攻破网络、达成目标。

- 攻击者是否已入侵？
- 攻击者是谁？
- 攻击者的目的是什么？

网络欺骗防御属于网络**主动防御**范畴，以攻防对抗思路为基础，以攻击者视角去发现威胁。通过构造大量虚假的网络环境、主机、服务和诱饵，引诱攻击者去访问虚假环境来及时发现攻击并对攻击者进行溯源反制，以保护客户真实资产。



欺骗防御技术可有效扭转攻防不对称的态势，化被动为主动！

免费蜜罐DecoyMini特点

DecoyMini•智能仿真与攻击诱捕工具是北京吉沃科技推出的一款完全免费的蜜罐工具，可用于**互联网攻击感知**、**内网横向攻击监测**和**网络攻防演习监测**等场景。

DECOYMINI

智能仿真：插件化的仿真模板，一键导入云端仿真模板库就可以在本地网络快速部署多样化的安全可控的仿真服务和应用，支持对WEB站点进行自动学习和仿真

攻击诱捕：支持快速部署蜜罐群，使用虚拟IP，将网络内空闲的IP资源绑定到一到多个仿真环境上，支持动态绑定端口来增加蜜罐诱惑性，大大提高攻击诱捕的能力

灵活扩展：采用可视化仿真编排引擎，用户通过界面配置即可实现对自定义的网络协议、服务或应用的仿真，模板支持系统间快速迁移和通过DecoyMini论坛进行分享

部署简便：支持主流操作系统（Windows 32/64位,CentOS/Ubuntu/Debian/Kali 32/64位,树莓派等），支持单节点、多节点集中管理，部署灵活、一键安装、使用简单；

安全有效：基于商业化蜜罐产品（DecoyPro）能力积累，以企业级技术做免费蜜罐工具（DecoyMini），产品安全性好，成熟度高、稳定性有保障

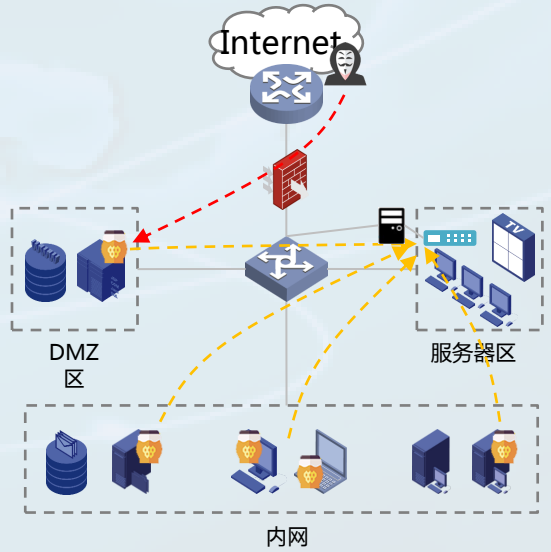
应用场景1：互联网攻击诱捕分析

场景痛点

- ✓ 互联网攻击频繁，风险事件频发；
- ✓ 网络攻击技术复杂多样，传统安全设备无法有效识别高级，隐蔽攻击行为；
- ✓ 安全人员，技术力量有限，缺少自动化安全威胁分析应急处置能力；
- ✓ 掌握潜在的攻击来源；

技术能力

- ✓ 资源环境智能仿真；
- ✓ 网络攻击诱捕分析；
- ✓ 安全威胁监测预警；
- ✓ 风险事件响应处置；
- ✓ 威胁情报共享分析；
- ✓ 安全态势可视化展示；



价值

- 智能仿真攻击诱捕
- 内生威胁情报生产
- 网络攻击应急处置能力
- 常态化的外网攻击感知

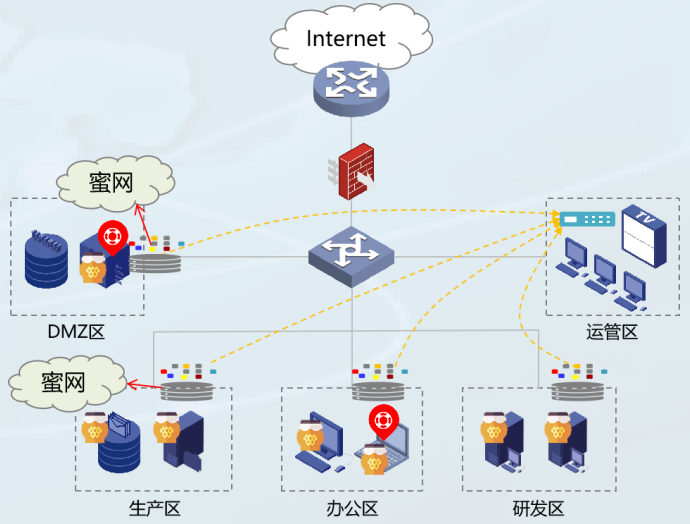
应用场景2：内网横向攻击监测预警

场景痛点

- ✓ 内部网络访问控制不严格，横向渗透严重
- ✓ 内网系统安全漏洞、弱口令威胁严峻，极易遭受恶意攻击；
- ✓ 内部人员安全意识淡薄，易感恶意软件，导致内网感染；
- ✓ 缺少常态化内网威胁检测手段，内部威胁无从发现；

技术能力

- ✓ 丰富的服务应用模板；
- ✓ 灵活的攻击诱捕策略；
- ✓ 灵敏的网络行为监测；
- ✓ 威胁情报共享分析；
- ✓ 可视化网络威胁感知；



价值

- 内网失陷主机监测
- 内网异常攻击监测
- 内生威胁情报生产
- 常态化的内网威胁感知

应用场景3：网络攻防对抗演习监测分析

场景痛点

- ✓ 攻防演习常态化，攻击对抗监测预警能力；
- ✓ 攻击手段复杂，攻击行为精准捕获能力；
- ✓ 攻击行为隐蔽，攻击事件溯源分析能力；
- ✓ 攻击行为快速，攻击行为快速感知处置能力；

技术能力

- ✓ 多元化环境智能仿真；
- ✓ 攻击反制场景构建；
- ✓ 网络攻击诱捕分析；
- ✓ 威胁情报共享分析；
- ✓ 攻击溯源画像分析；
- ✓ 攻击联动处置阻断；

价值

- ● 智能仿真、攻击监控预警
- ● 网络攻击诱饵投放反制
- ● 攻击者信息画像取证分析
- ● 完整攻击链溯源分析得分

技术架构

吉沃科技

DecoyMini欺骗防御社区（技术论坛）

仿真模板、威胁情报

管理中心

节点管理 | 风险事件 | 诱捕日志 | 诱捕策略 | 仿真模板 | 事件预警

数据存储（Sqlite） | 规则匹配 | 关联分析 | 威胁情报

WEB管理

诱捕探针

仿真模板引擎

仿真模板1 | 仿真模板2 | 仿真模板3 | 仿真模板4 | 仿真模板5 …

蜜罐1 | 蜜罐2 | 蜜罐3 | 蜜罐4 | 蜜罐5 | 蜜罐6 | 蜜罐7 …

攻击流量分析 | 攻击行为监控 | 攻击特征提取

Windows | Linux | 国产OS

网络攻击

DecoyMini下载

下载地址：

https://github.com/decoymini

http://decoymini.decoyit.com

用户手册：

https://bbs.decoyit.com/doc/智能仿真与攻击诱捕工具(DecoyMini)用户手册_v1.1.pdf

DecoyMini安装

部署模式

- 单节点模式：管理中心与诱捕探针一体式运行在一台主机上，为 DecoyMini 默认模式。
- 集中管理模式：在网络中选择一台主机部署 DecoyMini 软件作为管理中心，在多个主机上以诱捕探针模式部署诱捕节点，将诱捕节点集中到此管理中心统一管理。

环境需求

配置\类别	单节点	管理中心	诱捕探针
最低配置	CPU ≥ 2核; 内存 ≥ 2G; 硬盘 ≥ 50G	CPU ≥ 4核; 内存 ≥ 4G; 硬盘 ≥ 100G	CPU ≥ 2核; 内存 ≥ 1G; 硬盘 ≥ 10G
推荐配置	CPU 4 核; 内存 4G; 硬盘 100G	CPU 6 核; 内存 8G; 硬盘 200G	CPU 2 核; 内存 2G; 硬盘 20G

单节点/管理中心安装

➢DecoyMini_xxx [-install]

诱捕探针安装

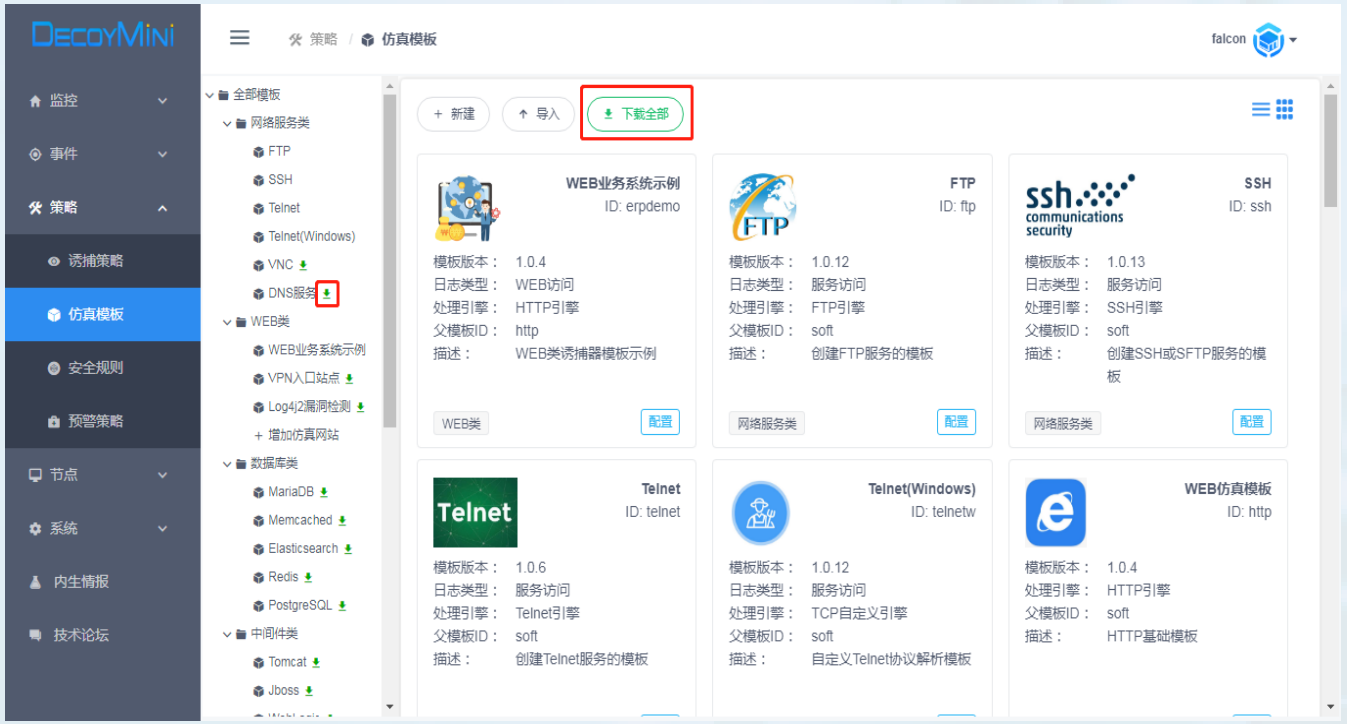
➢DecoyMini_xxx -install -addr http://192.168.8.100:8080

账户注册/系统登录

浏览器访问 http://监听IP:监听端口 打开管理端

可访问互联网的环境，注册论坛账号登录，支持一个账号管理多个DecoyMini系统
DecoyMini与欺骗防御技术论坛无缝衔接、支持论坛自动登录、一键导入仿真模板

一键导入仿真模板



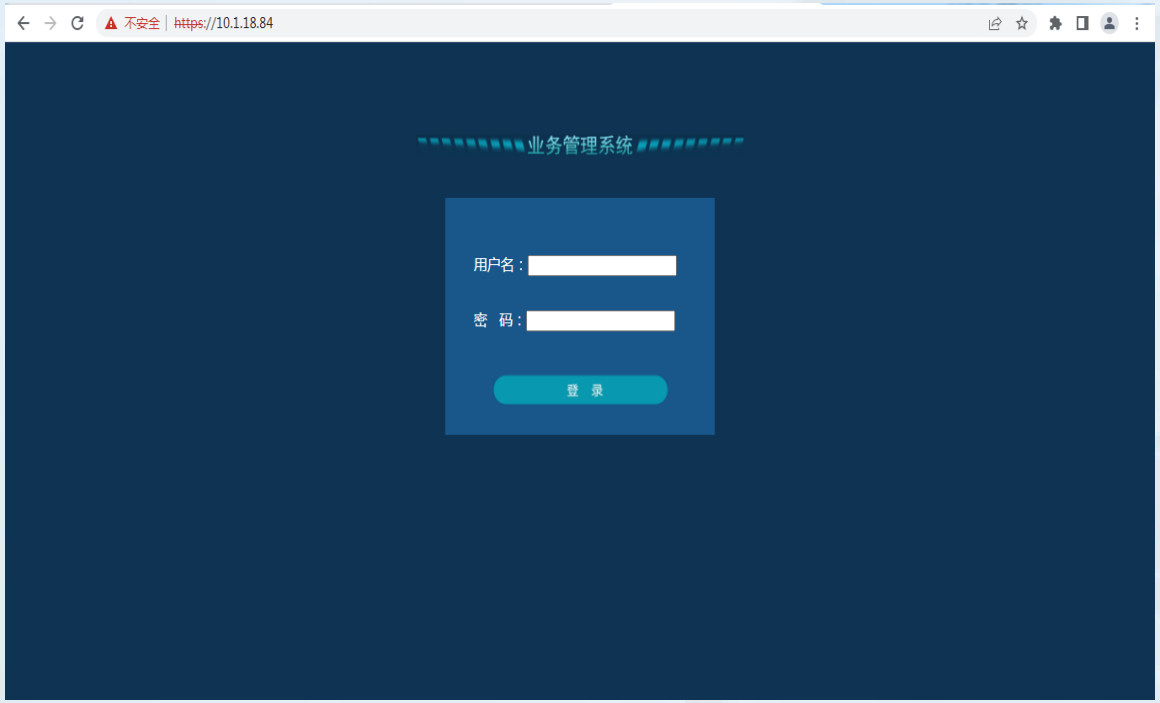
- 自动下载：在仿真模板里点击“下载全部”，一键下载技术论坛里常用仿真模板集合；
- 手动下载：访问技术论坛（https://bbs.decoyit.com），手动下载需要使用的仿真模板进行导入；

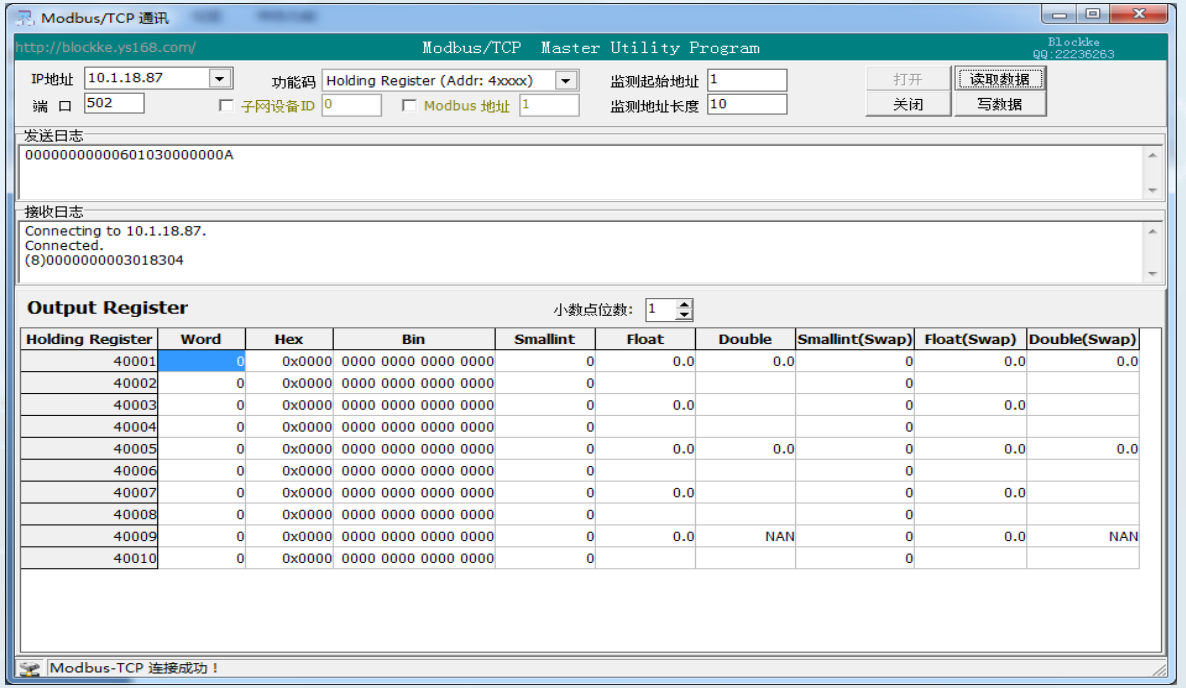
新建仿真模板

通过界面自定义对请求数据的解析规则，提取出关键属性，基于对关键属性的匹配，来响应对应的个性化数据，实现对协议、服务和应用的自定义仿真。

对于自定义的仿真模板支持导出分享，可以分享到其它DecoyMini环境，实现仿真能力的快速迁移；也可以分享到DecoyMini技术论坛，将有机会获得论坛礼品或现金奖励。

仿真模板配置示例





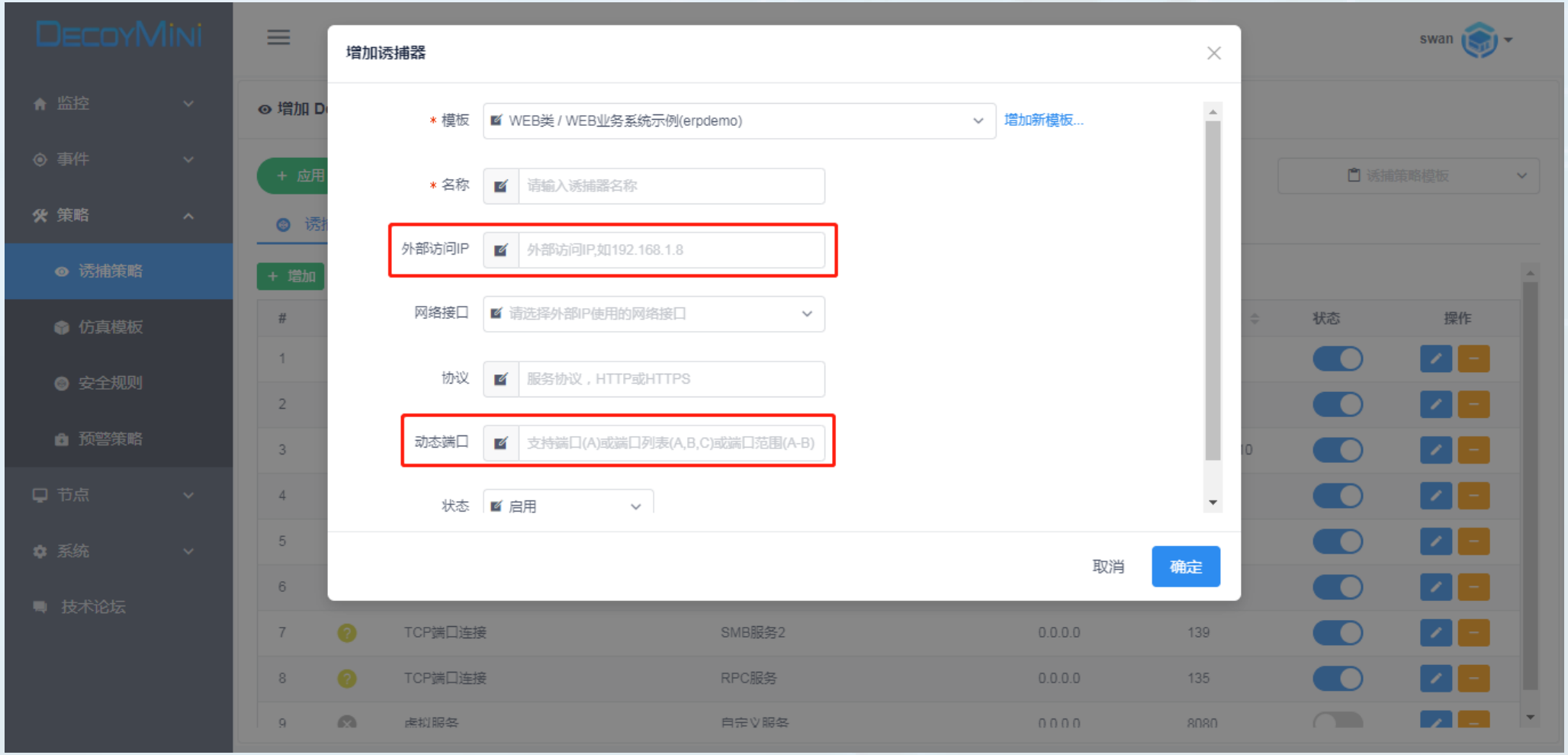
用免费蜜罐软件快速部署业务系统蜜罐
https://www.freebuf.com/articles/es/328397.html

用免费蜜罐工具配置Modbus工控蜜罐：
https://www.4hou.com/posts/lXB7

部署蜜罐/诱捕器

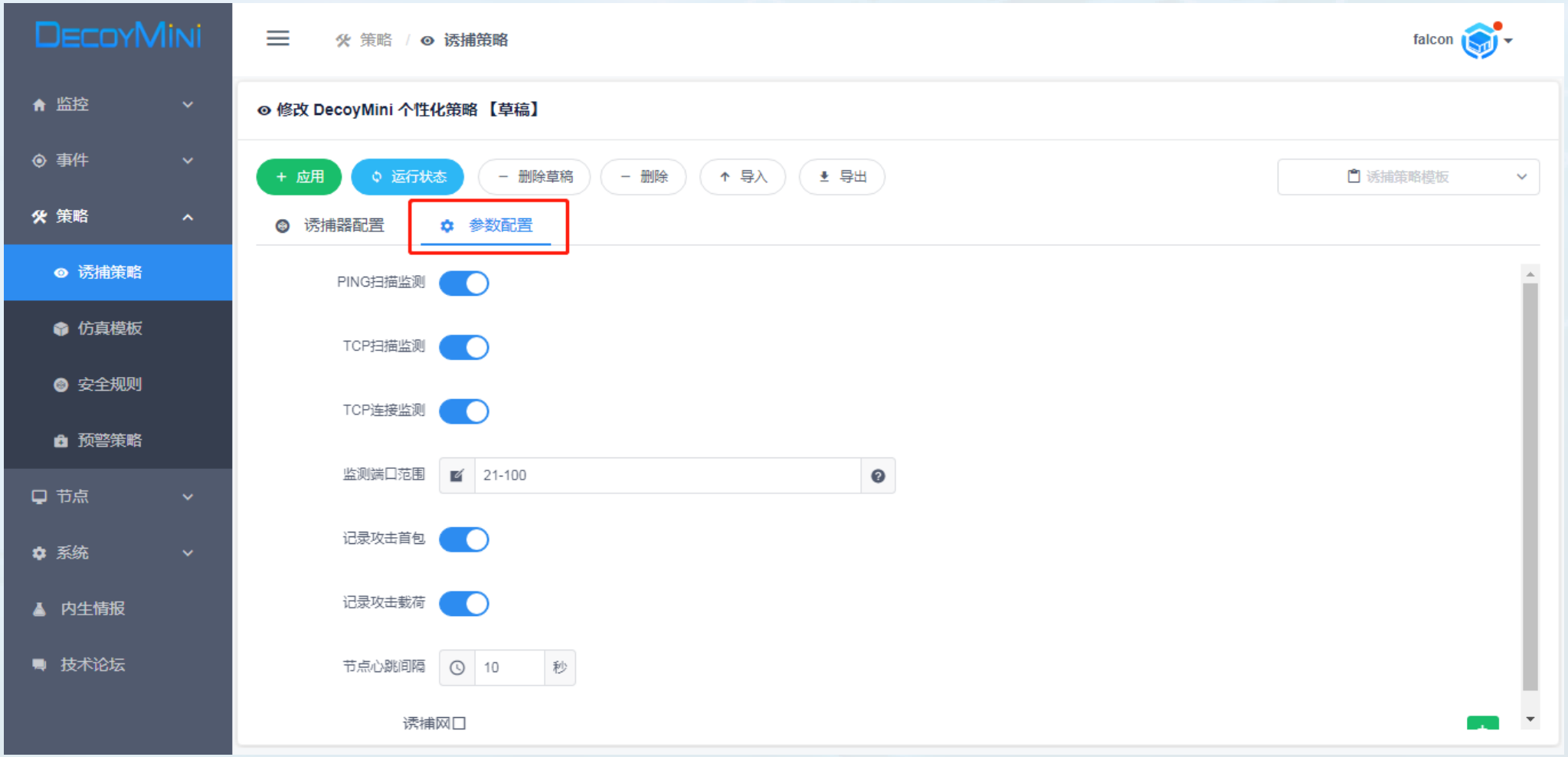
使用策略模板预置蜜罐策略，或手动增加需要部署的蜜罐，点击“应用”下发诱捕策略。

增加新蜜罐



支持虚拟IP和动态端口技术，支持将诱捕器直接部署在网络内空闲的IP上，实现一个DecoyMini节点虚拟多IP来模拟多台主机，快速组建蜜罐群，有效提高蜜罐的覆盖率，用较小的部署资源实现最大化的攻击诱捕效果。

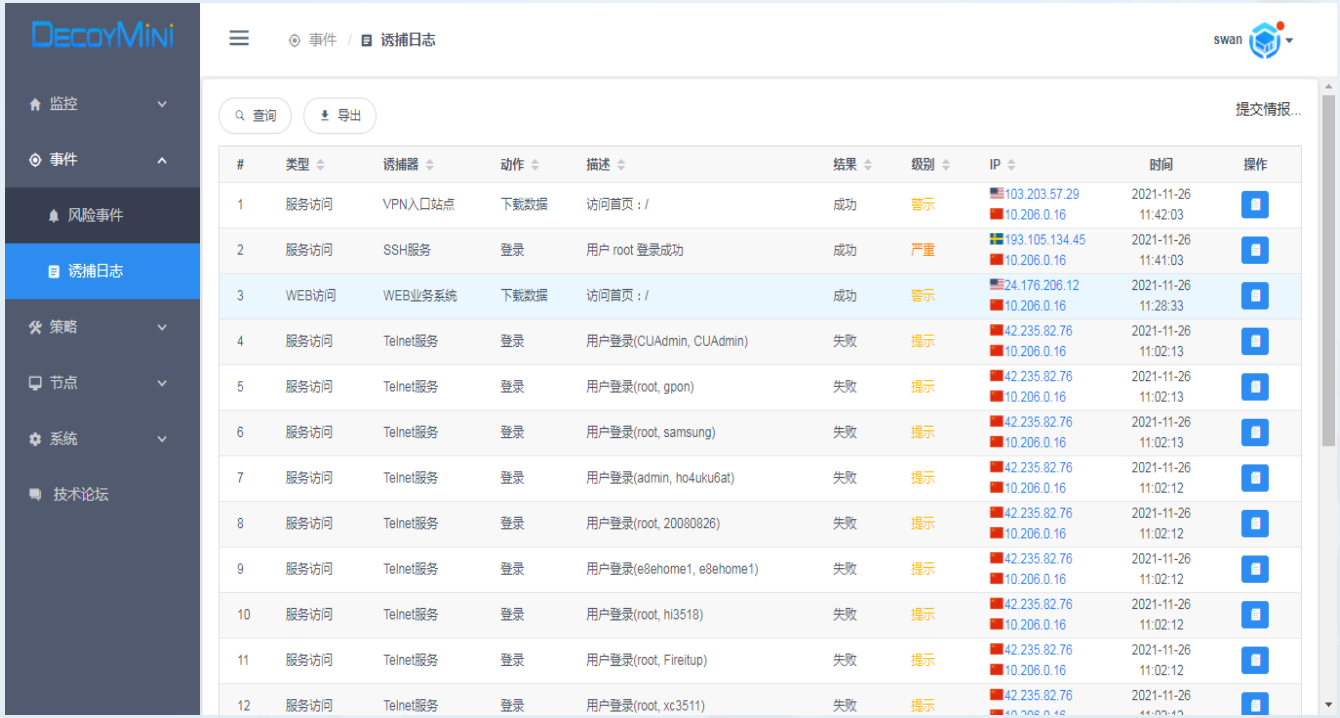
配置诱捕参数



提供对PING扫描、TCP扫描等行为进行监测

提供对指定端口范围的TCP连接进行监测，支持记录连接行为、攻击首包和攻击载荷

诱捕日志



DecoyMini完整记录攻击者发起的各种攻击行为，生成诱捕日志

包括攻击者源IP、攻击的蜜罐、操作类型、操作账户、攻击描述、攻击结果、影响程度、攻击时间等信息

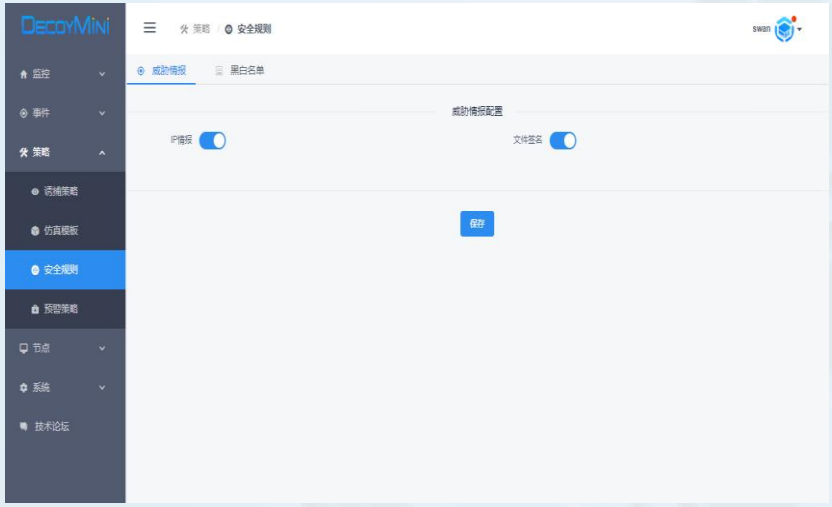
同时支持对攻击者发起攻击对应的攻击首包以及攻击载荷进行记录

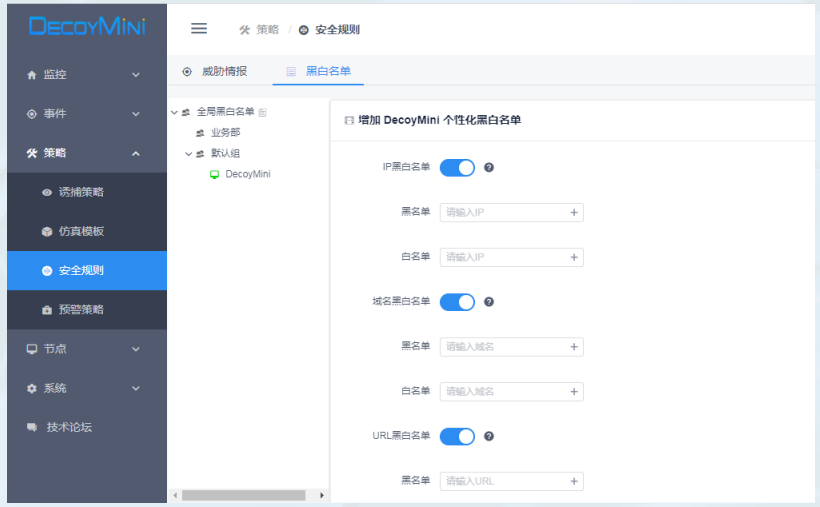
诱捕日志

对攻击者通过FTP，SFTP等方式上传的可疑文件，支持通过界面直接下载

支持以“时间线”方式来展示攻击者攻击的详细过程。

威胁情报、黑白名单



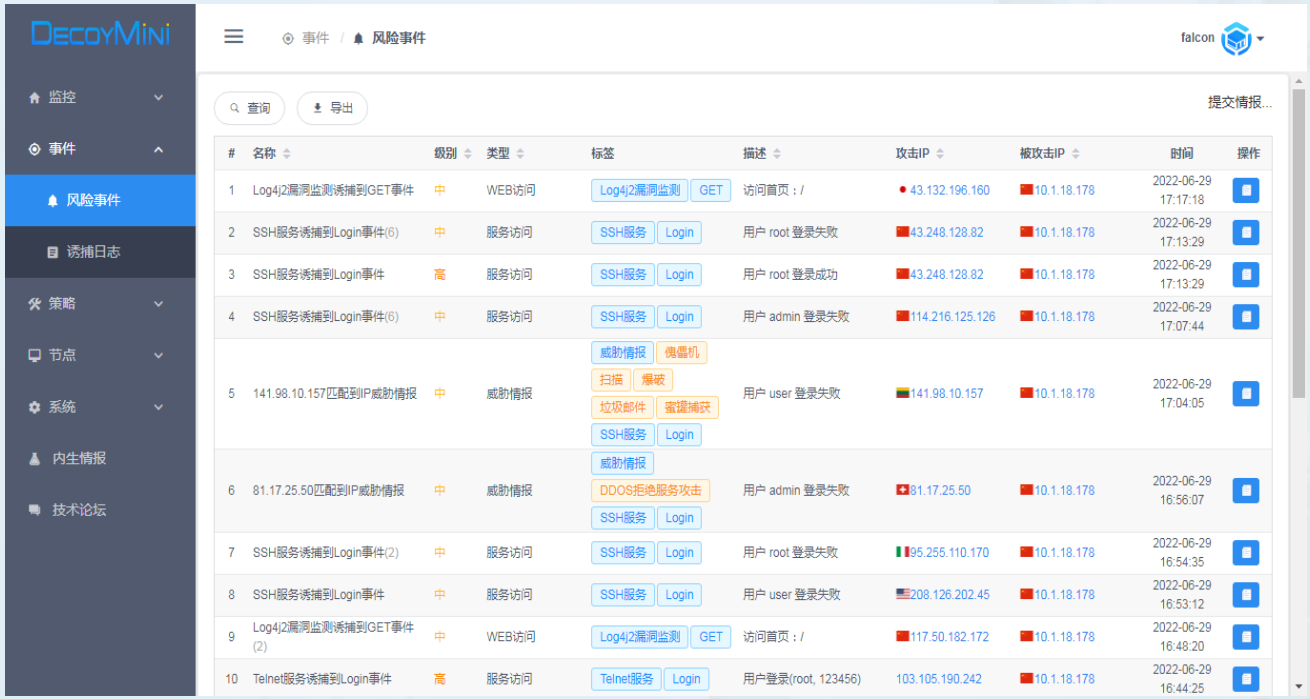


支持威胁情报检测，通过定期和云端威胁情报平台同步，及时更新最新的情报数据到本地，利用威胁情报能够快速识别各类攻击行为

支持用户自定义IP黑白名单、网络端口黑白名单、文件黑白名单等

对于授权的扫描行为，支持一键增加白名单

关联分析 -> 风险事件



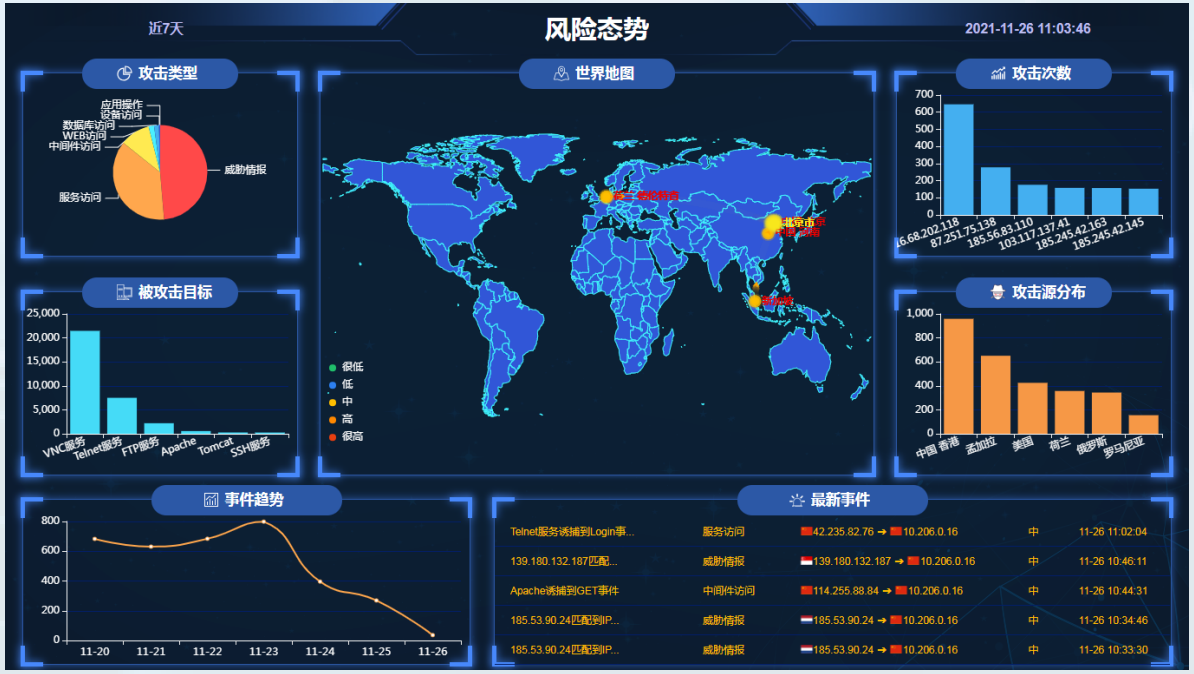
基于内置关联分析规则提供对各诱捕器产生的诱捕日志进行多维度关联分析、去重合并DecoyMini产生的风险事件准确性高，告警数量少

攻击预警

产生风险事件后，支持按事件类型、威胁级别、事件确信度、IP地址、时间等条件进行过滤

支持通过邮件、弹窗、企业微信、钉钉、飞书、Syslog等方式发生预警通知

风险监控



支持关键数据指标可视化展示，数据支持钻取分析

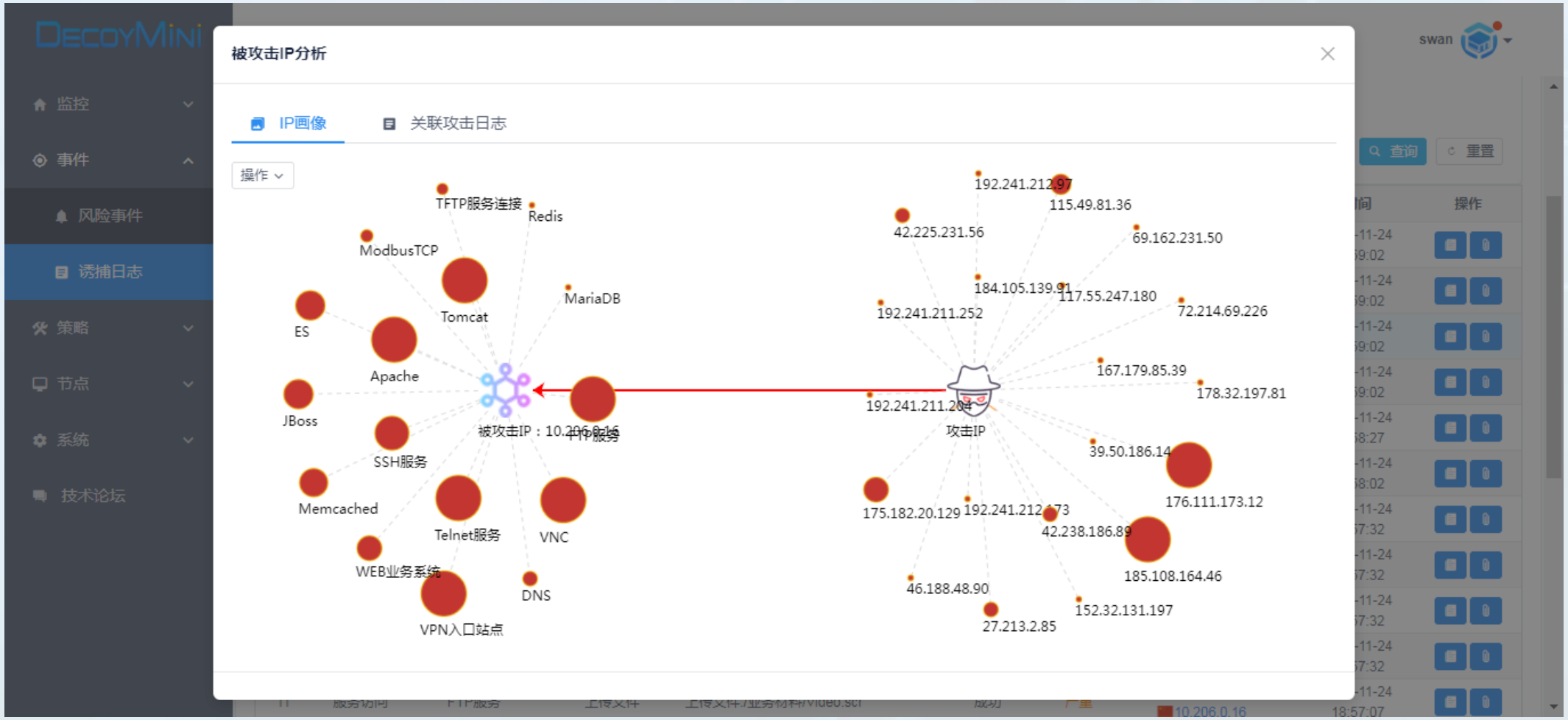
支持风险态势大屏展示，直观掌握全网安全态势

攻击IP画像

基于对攻击IP数据的分析，生成攻击IP画像，包括攻击者基本信息、攻击者主机特征、攻击者浏览器特征、攻击者主机曾开启的服务，攻击者攻击的范围等等

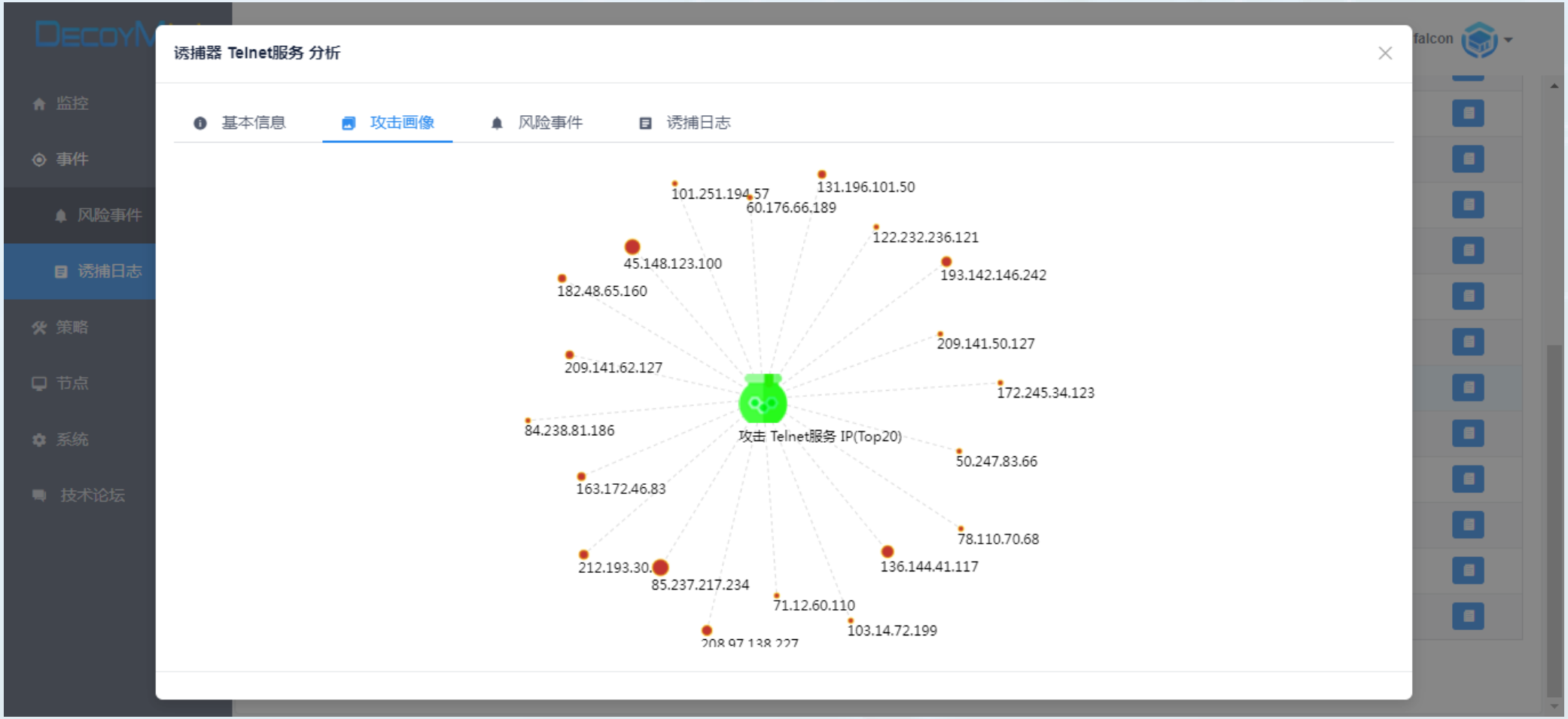
支持攻击IP外部威胁情报平台一键查询

被攻击IP画像



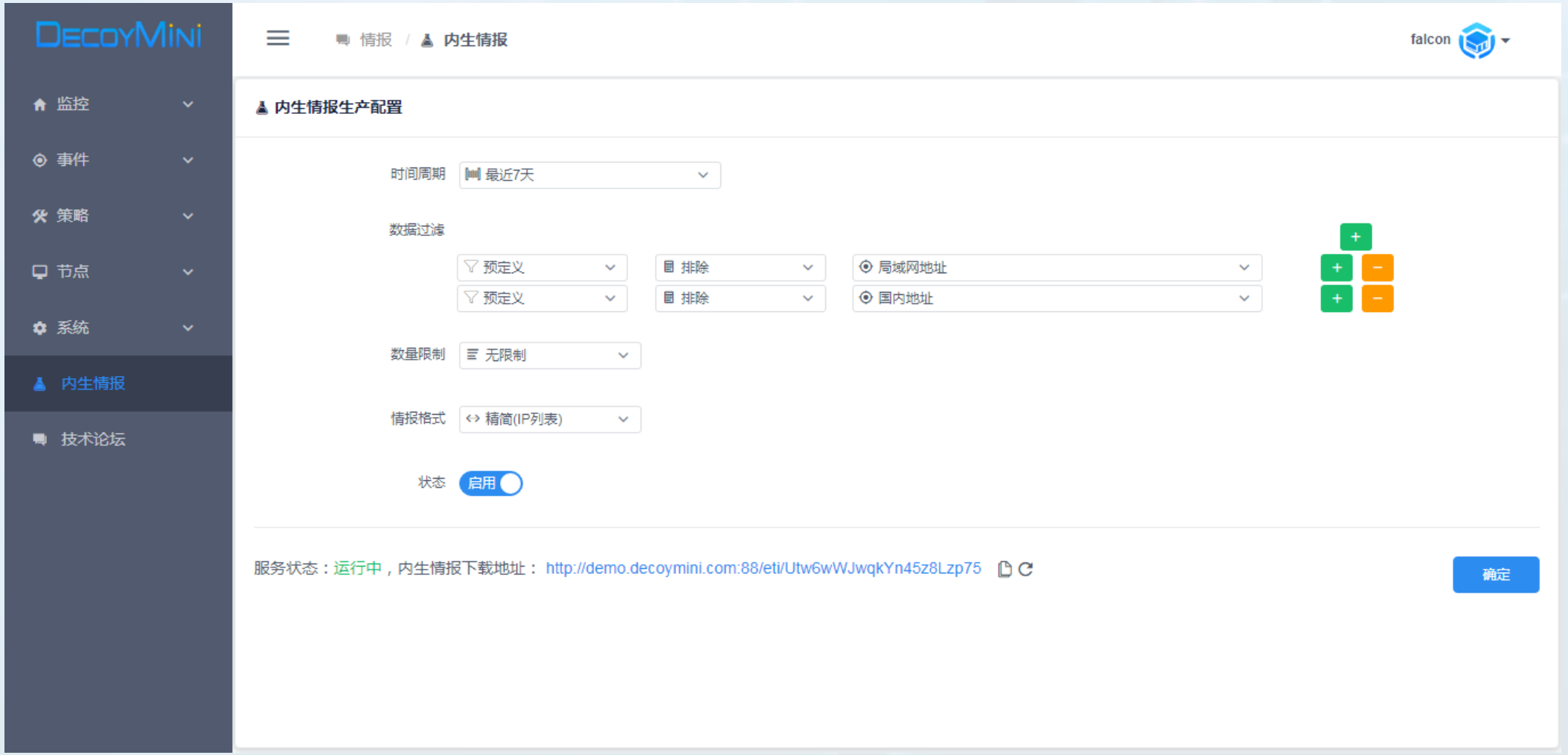
基于对被攻击IP事件、日志等数据的分析，生成被攻击IP画像，包括该IP上诱捕器被攻击情况、攻击来源统计等

诱捕器攻击画像



基于对被攻击诱捕器攻击数据的分析，生成诱捕器攻击画像，包括攻击诱捕器的IP列表、攻击次数等信息

输出内生情报



基于对攻击源的分析和过滤，生成内生情报，支持精简、STIX2等格式输出

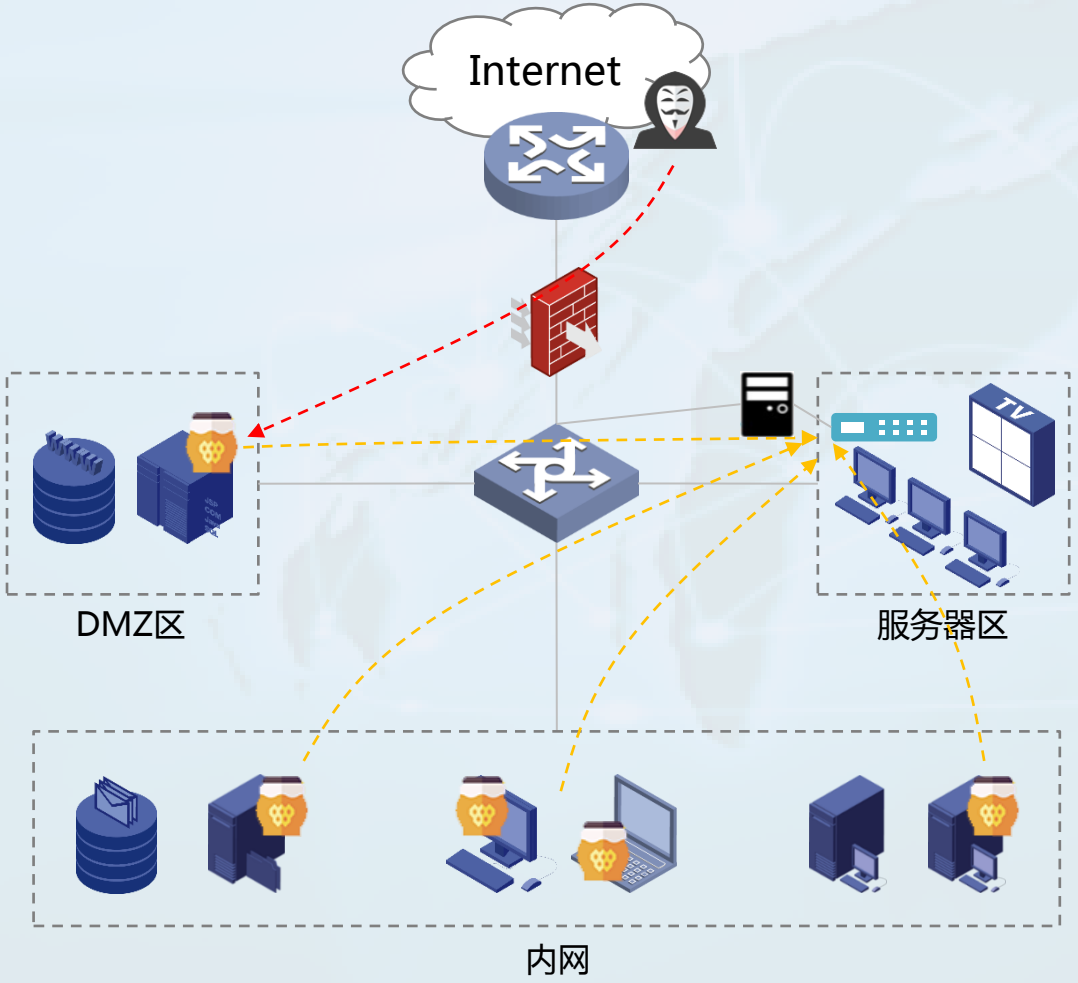
内生情报是威胁情报体系重要组成部分，是外部情报重要的情报能力补充

应用价值

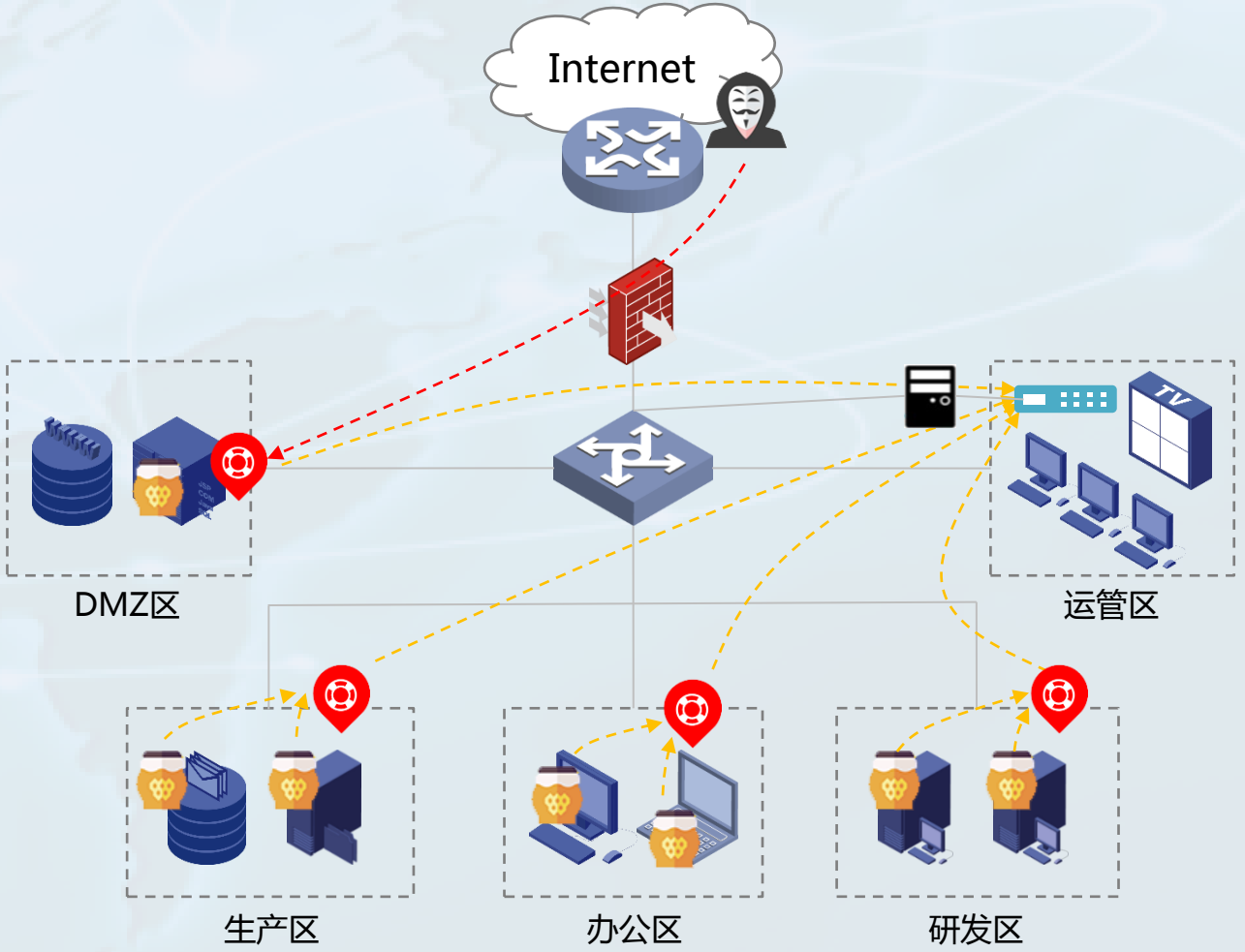
仿真灵活度高	• 插件化的仿真模板，简单配置就可实现对各种服务和系统的仿真，支持一键分享，一键部署
攻击诱捕效果好	• 支持分布式部署，支持在一台蜜罐上虚拟出多IP，快速组建蜜罐群，第一时间发现各种攻击行为
运维成本低	• 免费蜜罐软件，误报低，结合关联合并，告警数量少、准确度高，支持内生情报输出，大大降低安全运维投入，降低成本
24小时不间断值守	• 对接钉钉、企业微信、飞书或自有业务系统，极少的资源和人力投入，就可以实现7x24小时不间断远程值守

典型部署方案

单节点部署

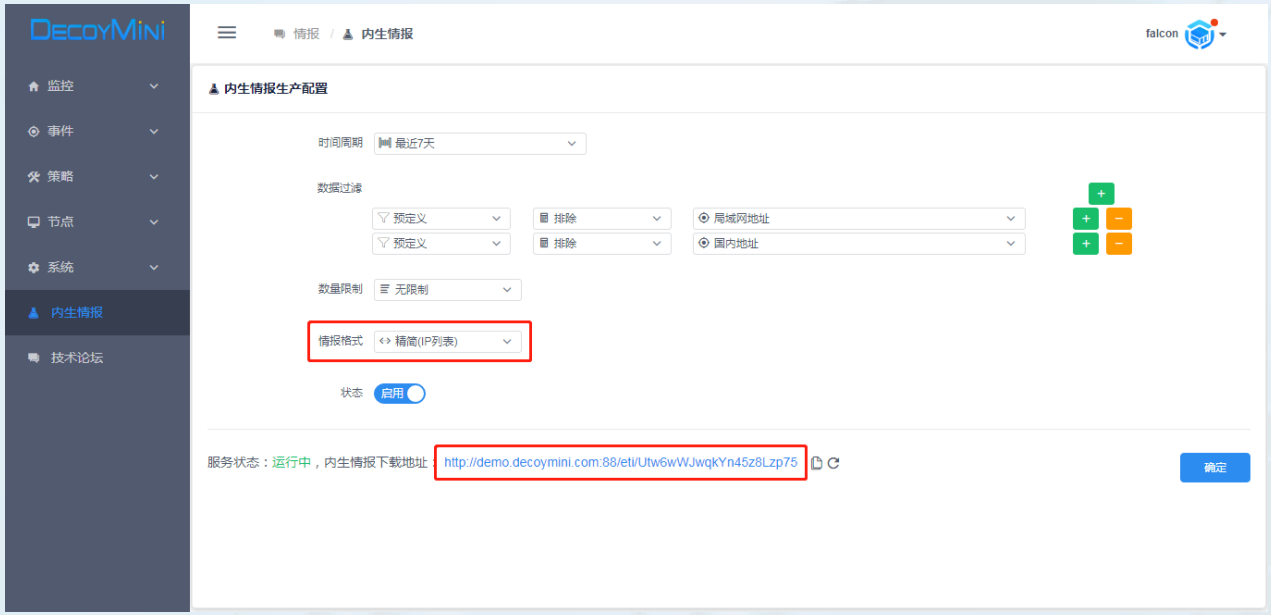


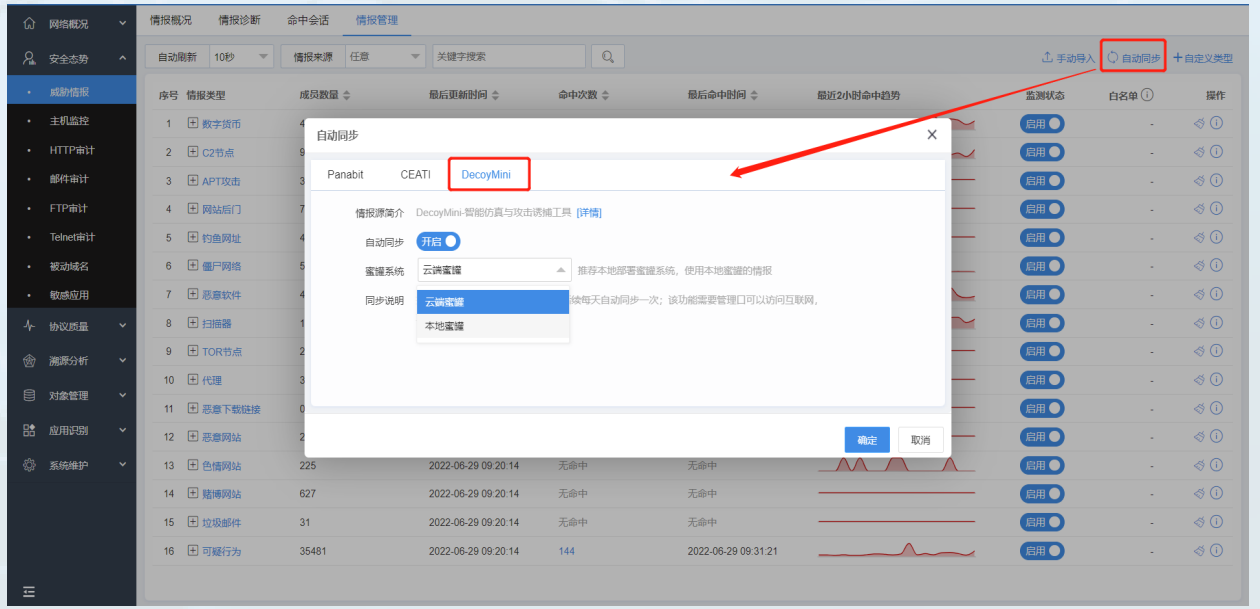
多节点部署



DecoyMini　诱捕探针　诱捕器/蜜罐　Panabit NTM

NTM与DecoyMini对接

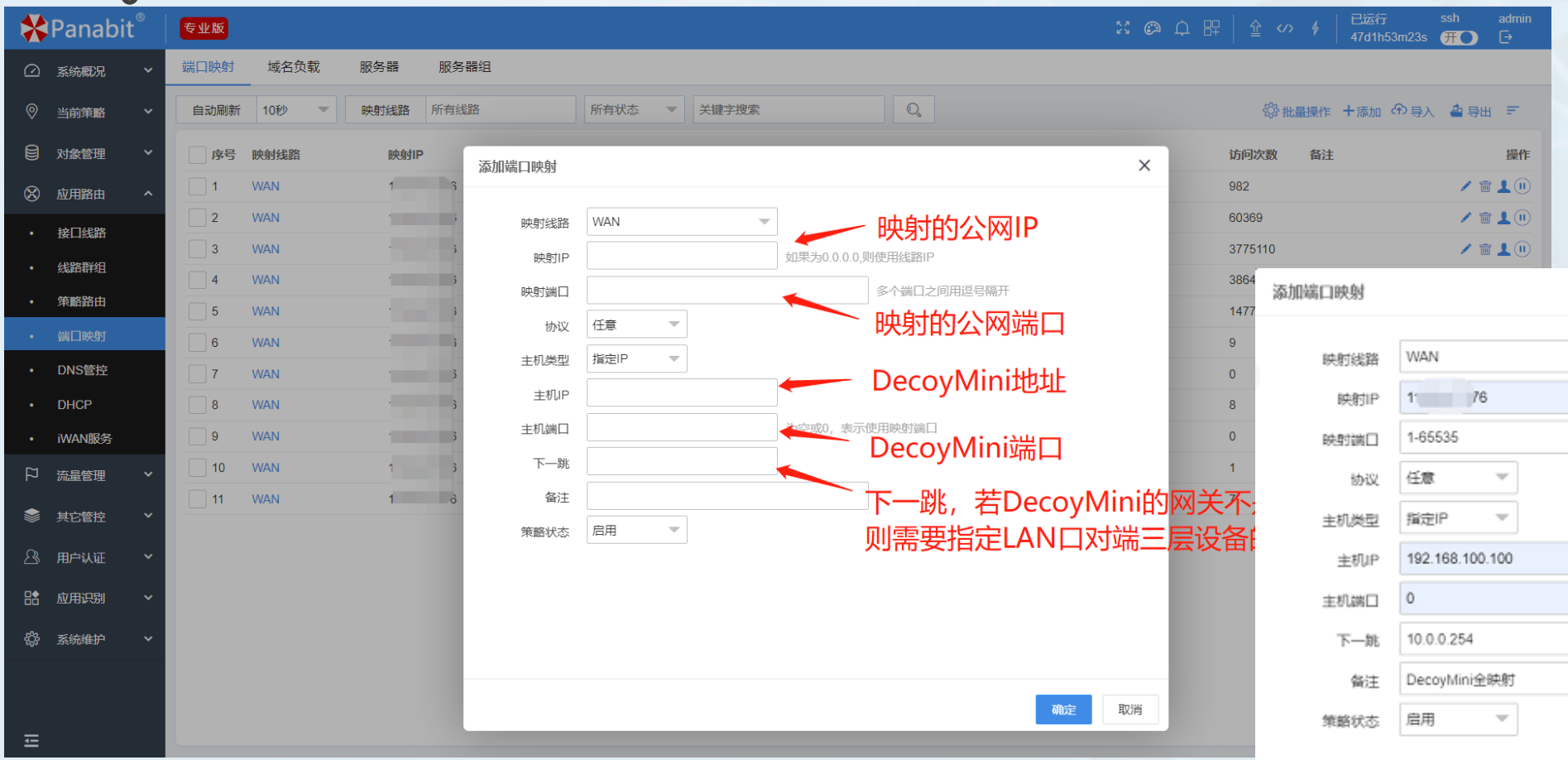


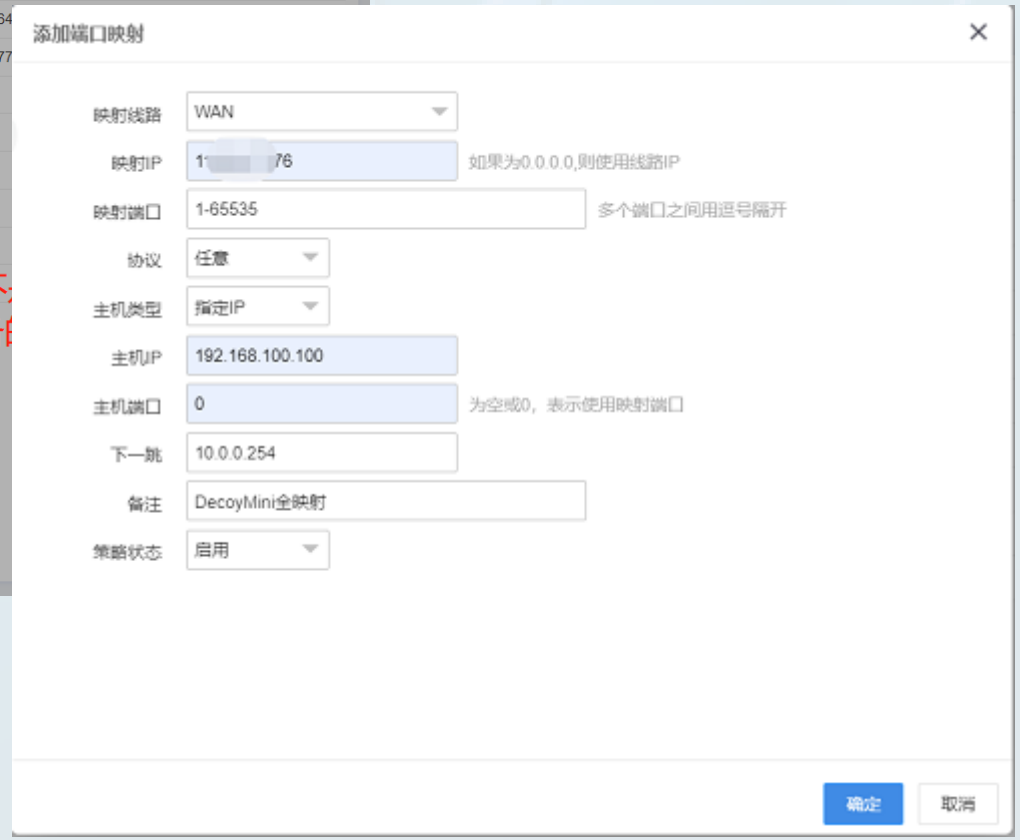


1、在DecoyMini系统配置内生情报输出规则，情报格式选择“精简”，开启情报服务，获得情报下载地址；

2、在NTM系统DecoyMini情报配置标签，选择“本地蜜罐”，填入DecoyMini生成的情报下载地址。

蜜罐端口映射

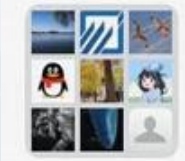




DecoyMini端口：

- 管理端口：安装时配置
- 业务端口：1226
- 蜜罐端口：诱捕策略配置

DecoyMini交流群



DecoyMini技术交流3群

该二维码7天内(7月8日前)有效，重新进入将更新

下载

DecoyMini免费下载链接：
https://github.com/decoymini
https://decoymini.decoyit.com

论坛

DecoyMini 技术交流社区：
http://bbs.decoyit.com

谢谢！