
免费蜜罐软件——DecoyMini 介绍



Panabit NTM与威胁情报

情报概况 情报诊断 命中会话 情报管理

MAC: [] 源IP: 任意IP 源端口: 80 / 8000-8080 目标IP: 任意IP 目标端口: 80 / 8000-8080 应用协议: 任意协议

源IP ISP: 任意 目标IP ISP: 任意 源IP区域: 任意 目标IP区域: 任意 情报类型: 任意

域名: [] 时间范围: 2022-06-29 08:37:06 - 2022-06-29 09:37:06

情报概况 情报诊断 命中会话 情报管理

MAC: [] 源IP: 任意IP 源端口: 80 / 8000-8080 目标IP: 任意IP 目标端口: 80 / 8000-8080 情报类型: 任意

源IP ISP: 任意 目标IP ISP: 任意 源IP区域: 任意 目标IP区域: 任意 传输协议: 任意 应用协议: 任意协议

域名: [] 时间范围: 2022-06-29 08:38:10 - 2022-06-29 09:38:10

序号	源IP	命中次数	情报类型	序号	目标IP	命中次数	情报类型
1	1.34	3152	扫描器	1	33.50	1275	数字货币
2	16.31	2426	扫描器	2	6.228	401	恶意软件
3	93.227	1977	扫描器	3	18.209	358	可疑行为
4	11.14.35	1757		4	13.223	357	可疑行为
5	11.114.97	1685		5	3.7	341	数字货币
6	14.10.4	946	扫描器	6	1.48.222	328	数字货币

序号	目标域	发送时间	MAC	源IP	目标IP	源地理位置	目标地理位置	传输协议	应用协议	域名	情报类型	操作
1	ivr	2022-06-29/08:38:18	58-6a-b1-e0-81-f1	113.4.60.41412	20.116.443	北京[BGP]	[BGP]	TCP	其它HTTPS	203.107.1.65	可疑行为	数据包
2	se	2022-06-29/08:38:35	58-6a-b1-e0-81-f1	113.4.79.1239	20.116.443	北京[BGP]	北京[BGP]	TCP	其它HTTPS	203.119.217.116	可疑行为	数据包
3	20	2022-06-29/08:39:05	58-6a-b1-e0-81-f1	113.4.9.10423	61.191.443	北京[BGP]	河北石家庄[联通]	TCP	其它HTTPS	material.mediac.com	恶意软件	数据包
4	20	2022-06-29/08:39:15	58-6a-b1-e0-81-f1	113.4.1.79.1724	20.7.116.443	北京[BGP]	北京[BGP]	TCP	其它HTTPS	203.119.217.116	可疑行为	数据包
5	20	2022-06-29/08:39:22	58-6a-b1-e0-81-f1	113.4.1.64.45457	20.65.443	北京[BGP]	[BGP]	TCP	其它HTTPS	203.107.1.65	可疑行为	数据包
6	rtv	2022-06-29/08:39:18	58-6a-b1-e0-81-f3	185.0.70.52017	11.14.33.80	美国	北京[BGP]	TCP	WWW		扫描器	数据包
		2022-06-29/08:39:24	58-6a-b1-e0-81-f1	113.4.1.97.63560	3.112.8080	北京[BGP]	广东深圳[BGP]	TCP	其它HTTP上传		可疑行为	数据包
		2022-06-29/08:39:24	58-6a-b1-e0-81-f1	113.4.1.97.63561	3.112.8080	北京[BGP]	广东深圳[BGP]	TCP	其它HTTP上传		可疑行为	数据包
		2022-06-29/08:39:30	58-6a-b1-e0-81-f1	113.4.1.97.63776	3.112.8080	北京[BGP]	广东深圳[BGP]	TCP	其它HTTP上传		可疑行为	数据包
		2022-06-29/08:39:30	58-6a-b1-e0-81-f1	113.4.1.97.63775	3.112.8080	北京[BGP]	广东深圳[BGP]	TCP	其它HTTP上传		可疑行为	数据包
		2022-06-29/08:39:34	58-6a-b1-e0-81-f1	113.4.1.97.63891	3.112.8080	北京[BGP]	广东深圳[BGP]	TCP	其它HTTP上传		可疑行为	数据包
		2022-06-29/08:39:56	58-6a-b1-e0-81-f1	113.4.1.35.3336	1.63.7586	北京[BGP]	河南驻马店[联通]	UDP	百度云盘		C2节点	数据包
		2022-06-29/08:39:56	58-6a-b1-e0-81-f3	123.4.1.7586	1.4.35.15857	河南驻马店[联通]	北京[BGP]	UDP	百度云盘		C2节点	数据包
		2022-06-29/08:39:59	58-6a-b1-e0-81-f1	113.4.1.149.36466	3.112.8080	北京[BGP]	广东深圳[BGP]	TCP	其它HTTP上传		可疑行为	数据包
		2022-06-29/08:40:26	58-6a-b1-e0-81-f1	113.4.1.35.9291	2.35.443	北京[BGP]	IBGP	TCP	其它HTTPS	203.107.1.65	可疑行为	数据包

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

The screenshot shows the Panabit NTM interface with a modal window for configuring '自动同步' (Auto Sync) for the 'DecoyMini' intelligence source. The modal window includes the following settings:

- 情报源: DecoyMini
- 情报源简介: DecoyMini-智能仿真与攻击诱捕工具 [详情]
- 自动同步: 开启 (checked)
- 蜜罐系统: 云端蜜罐 (selected)
- 同步说明: 云端蜜罐 (selected)

The background interface shows a table of intelligence sources with columns for '序号', '情报类型', '成员数量', '最后更新时间', '命中次数', '最后命中时间', '最近2小时命中趋势', '监测状态', '白名单', and '操作'. The 'DecoyMini' source is highlighted in the table.

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

群聊
聊天记录

蜜罐报警机器人 10-21 下午 10:06

[内网蜜罐通知][...]
[中]log.TCP诱捕到TryConn事件

事件名称: log.TCP诱捕到TryConn事件
目的IP: [...]
源IP: 172.16.0.236
类型: log.network
级别: 中
描述: 172.16.0.236:35856 尝试连接 [...]:445
事件ID: jQDihe8PgF8wUFpCCg6V4U
时间: 2021-10-21 22:06:25+08:00

查看详情: <http://...?secevt=jQDihe8PgF8wUFpCCg6V4U>

蜜罐报警机器人 10-21 下午 10:06

[内网蜜罐通知][...][高]SSH服务诱捕到Login事件

事件名称: SSH服务诱捕到Login事件
目的IP: [...]
源IP: 172.16.0.236
类型: svc
级别: 高
描述: 用户 root 登录成功
事件ID: djXchBkXjs6t5UDsCr7z39
时间: 2021-10-21 22:06:42+08:00

事件 / 风险事件

admin

提交情报...

查询 导出

#	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(2)	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/ffconfig	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

```

1 112.118.28.7 - - [21/Oct/2021:21:39:13 +0800] "GET / HTTP/1.1" 200 762 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
2 112.118.28.7 - - [21/Oct/2021:21:39:13 +0800] "GET /images/auth_login.gif HTTP/1.1" 200 20482 "http://222.218.130.73:2360/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
3 112.118.28.7 - - [21/Oct/2021:21:39:13 +0800] "GET /favicon.ico HTTP/1.1" 404 228 "http://222.218.130.73:2360/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
4 112.118.28.7 - - [21/Oct/2021:21:42:28 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
5 112.118.28.7 - - [21/Oct/2021:21:42:30 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 500 16 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
6 112.118.28.7 - - [21/Oct/2021:21:42:47 +0800] "GET /plugins/thold/includes/search.php HTTP/1.1" 200 20 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
7 222.218.102.72 - - [21/Oct/2021:21:43:12 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
8 222.218.102.72 - - [21/Oct/2021:21:43:12 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 500 16 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
9 222.218.102.72 - - [21/Oct/2021:21:43:19 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
10 222.218.102.72 - - [21/Oct/2021:21:43:19 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
11 222.218.102.72 - - [21/Oct/2021:21:43:22 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
12 222.218.102.72 - - [21/Oct/2021:21:43:22 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
13 112.118.28.7 - - [21/Oct/2021:21:43:28 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
14 112.118.28.7 - - [21/Oct/2021:21:43:29 +0800] "POST /plugins/thold/includes/search.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
15 112.118.28.7 - - [21/Oct/2021:21:44:32 +0800] "POST /plugins/wealthmap/configs/hxy.php HTTP/1.1" 200 745 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
16 112.118.28.7 - - [21/Oct/2021:21:44:32 +0800] "POST /plugins/wealthmap/configs/hxy.php HTTP/1.1" 200 809 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
17 112.118.28.7 - - [21/Oct/2021:21:44:32 +0800] "POST /plugins/wealthmap/configs/hxy.php HTTP/1.1" 200 1857 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
18 112.118.28.7 - - [21/Oct/2021:21:44:39 +0800] "POST /plugins/wealthmap/configs/hxy.php HTTP/1.1" 200 813 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
19 112.118.28.7 - - [21/Oct/2021:21:44:52 +0800] "POST /plugins/wealthmap/configs/hxy.php HTTP/1.1" 200 1361 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
20 112.118.28.7 - - [21/Oct/2021:21:45:06 +0800] "POST /plugins/wealthmap/configs/hxy.php HTTP/1.1" 200 921 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
21 112.118.28.7 - - [21/Oct/2021:21:45:23 +0800] "GET /plugins/thold/thold_graph.php?tab=hoststat HTTP/1.1" 200 3482 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
22 112.118.28.7 - - [21/Oct/2021:21:45:24 +0800] "GET /include/treeview/ua.js HTTP/1.1" 200 1431 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
23 112.118.28.7 - - [21/Oct/2021:21:45:24 +0800] "GET /include/jscalendar/lang/calendar-zh_CN.js HTTP/1.1" 200 1644 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
24 112.118.28.7 - - [21/Oct/2021:21:45:24 +0800] "GET /include/jscalendar/calendar.js HTTP/1.1" 200 13334 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
25 112.118.28.7 - - [21/Oct/2021:21:45:24 +0800] "GET /include/layout-js HTTP/1.1" 200 2467 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
26 112.118.28.7 - - [21/Oct/2021:21:45:24 +0800] "GET /include/treeview/feinsm.js HTTP/1.1" 200 8104 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
27 112.118.28.7 - - [21/Oct/2021:21:45:24 +0800] "GET /include/main.css HTTP/1.1" 200 1894 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
28 112.118.28.7 - - [21/Oct/2021:21:45:25 +0800] "GET /include/jscalendar/calendar-setup.js HTTP/1.1" 200 2902 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
29 112.118.28.7 - - [21/Oct/2021:21:45:28 +0800] "GET /images/tab_mode_tree.gif HTTP/1.1" 200 1014 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
30 112.118.28.7 - - [21/Oct/2021:21:45:28 +0800] "GET /plugins/monitor/images/tab_monitor.gif HTTP/1.1" 200 2026 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
31 112.118.28.7 - - [21/Oct/2021:21:45:28 +0800] "GET /images/tab_mode_preview.gif HTTP/1.1" 200 1021 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
32 112.118.28.7 - - [21/Oct/2021:21:45:28 +0800] "GET /images/tab_mode_list.gif HTTP/1.1" 200 1002 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"
33 112.118.28.7 - - [21/Oct/2021:21:45:28 +0800] "GET /images/transparent_line.gif HTTP/1.1" 200 55 "http://222.218.130.73:2360/plugins/thold/thold_graph.php?tab=hoststat" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36"

```

IP 相关数据信息

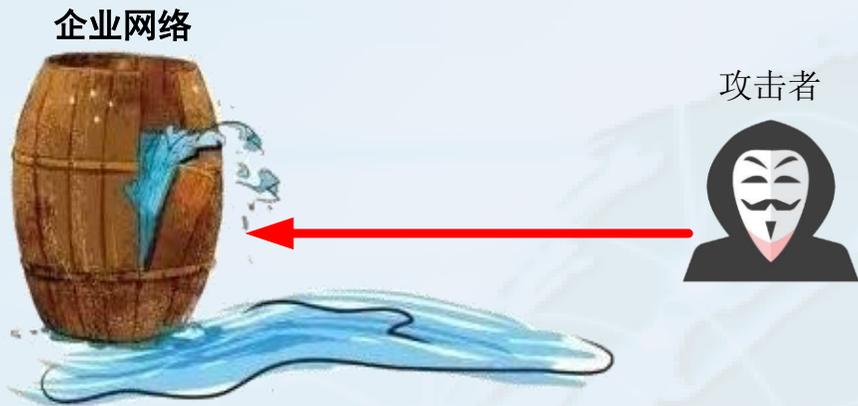
数据	城市级信息(数据来源于企业库)
当前IP	222.218.102.72 Ping Trace 域名
地理位置	中国广西南宁 产品详情
运营商	chinatelecom.com.cn
线路	电信
应用场景	请登录后查看 产品详情
地区中心经纬度	22.817002,108.366543
数据	国内区县级
地理位置	中国广西南宁青秀区 产品详情
数据	国内高精度
地理位置	中国广西南宁青秀区丽原天城
数据	网络安全风控基础数据
ASN数据	CIDR
A5134	222.218.0.0/16
	CHINANET-BACKBONE - No.31,Jin-rong Street, CN

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

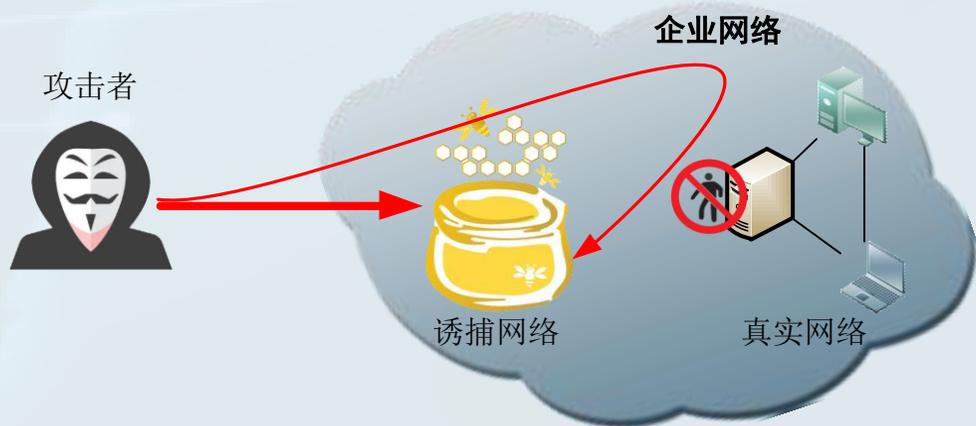
传统网络防御中，防守者需要充分、全面、完整的对网络和系统的安全漏洞和风险进行分析、评估和整改来确保整个网络的安全。

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。



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





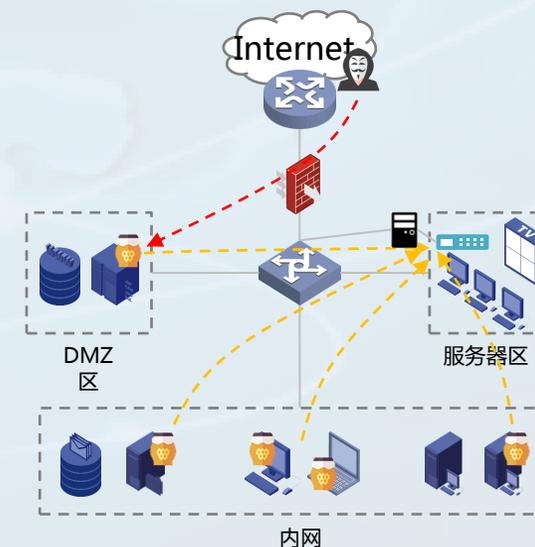
应用场景1：互联网攻击诱捕分析

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



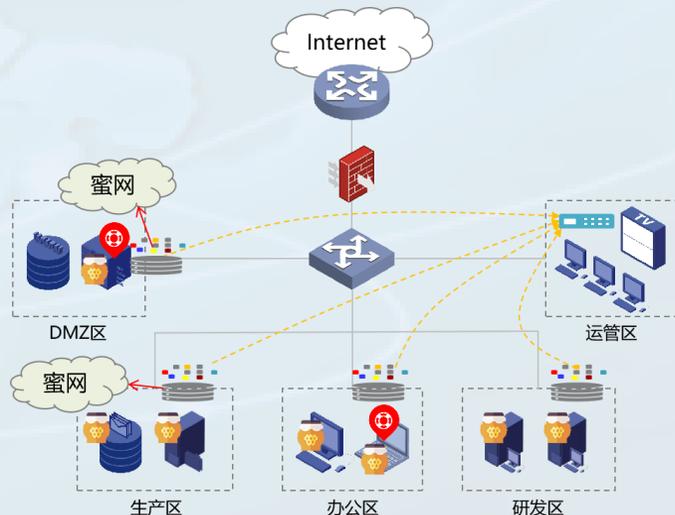
应用场景2：内网横向攻击监测预警

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
- 内生威胁情报生产
- 内网异常攻击监测
- 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
- 攻击者信息画像取证分析
- 网络攻击诱饵投放反制
- 完整攻击链溯源分析得分



技术架构

DecoyMini欺骗防御社区（技术论坛）

仿真模板、威胁情报

WEB管理

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

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

部署虚假的服务和应用, 吸引攻击者进行攻击, 在虚拟环境中对攻击者行为进行抓取和存储, 基于对攻击者的行为分析来实现攻击预警、威胁分析和溯源取证; 工具加入了云情报分享激励计划, 通过情报和仿真模板的分享用户还可以获得丰厚的奖励。

bbs.decoyit.com

ssh security web simulation ftp
telnet attacker hacker hw ti
honeytrap deception honeypots
honeynet decoy

Readme

Releases 10

v1.0.2472 Latest
9 days ago

+ 9 releases

欺骗防御是近些年出现的新技术, 以攻防对抗思路为基础, 让防守者得以观察攻击者行为的新兴网络安全防御战术。传统的安全防御思路, 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, 但是网络的攻击面众多, 很难完全及时发现所有问题或风险; 而攻击者只需要抓住一次机会就可以达到其攻击目标。欺骗防御技术跟传统安全模型完全相反, 攻击者除非 100% 正确, 否则就会触碰到诱捕环境进而暴露攻击行为。

首页 关于吉沃 产品与服务 技术支持 咨询购买 联系我们 下载&交流

DecoyMini·智能仿真与攻击诱捕工具

下载DecoyMini :

Windows 32/64位 | CentOS/Ubuntu/Debian/Kali 64位 | CentOS/Ubuntu/Debian/Kali 32位 树莓派

历史版本下载 → 技术论坛 →

智能仿真与攻击诱捕工具(DecoyMini)用户手册_v1.1.pdf

1 / 60 100%

智能仿真与攻击诱捕工具 (DecoyMini)

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](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]

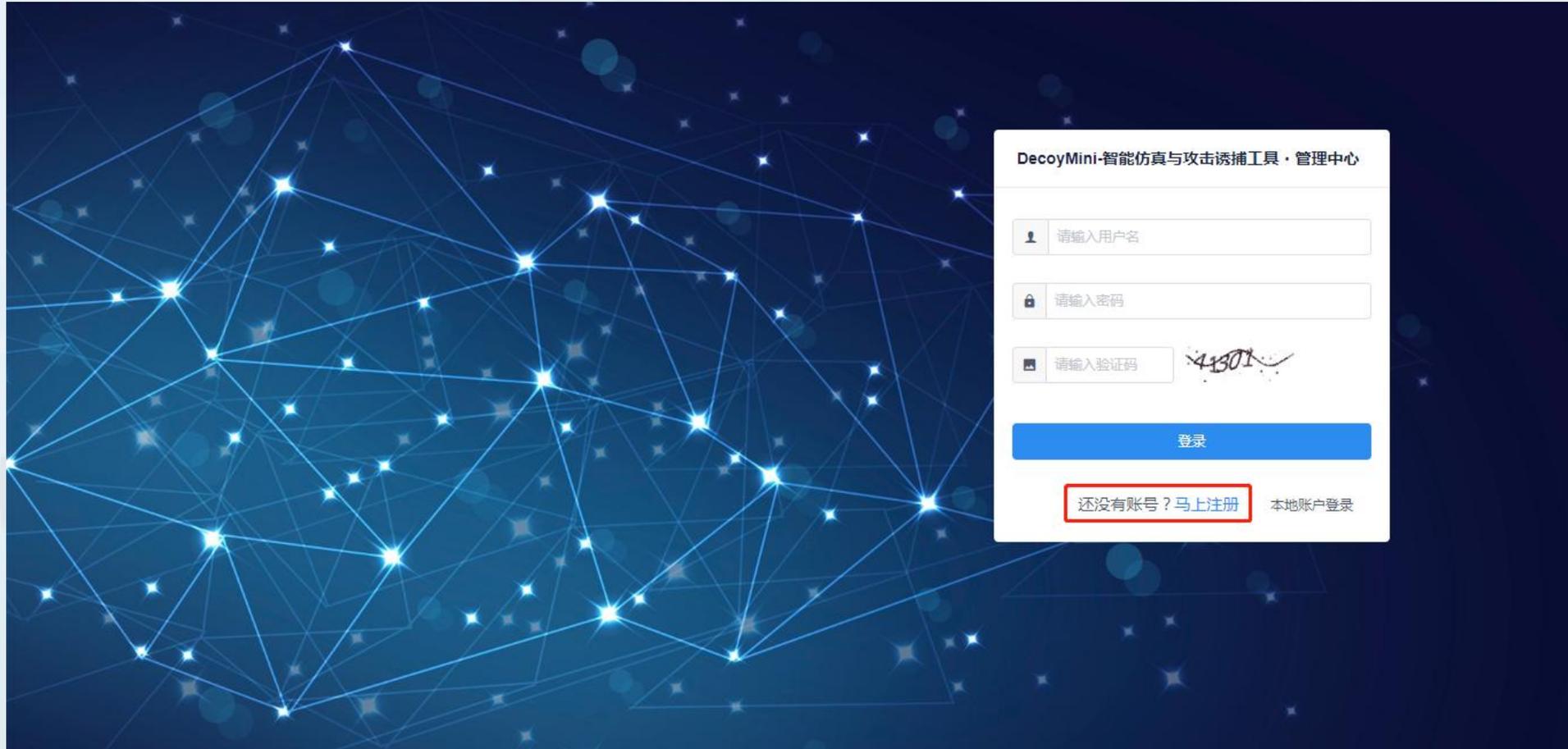
诱捕探针安装

➤ 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

The screenshot shows the DecoyMini web interface. On the left is a navigation sidebar with categories like '监控', '事件', '策略', '诱捕策略', '仿真模板', '安全规则', '预警策略', '节点', '系统', '内生情报', and '技术论坛'. The main area is titled '仿真模板' and contains a grid of template cards. A red box highlights the '下载全部' (Download All) button at the top. The template cards include:

- WEB业务系统示例** (ID: erpdemo): 模板版本: 1.0.4, 日志类型: WEB访问, 处理引擎: HTTP引擎, 父模板ID: http, 描述: WEB类诱捕器模板示例.
- FTP** (ID: ftp): 模板版本: 1.0.12, 日志类型: 服务访问, 处理引擎: FTP引擎, 父模板ID: soft, 描述: 创建FTP服务的模板.
- ssh communications security** (ID: ssh): 模板版本: 1.0.13, 日志类型: 服务访问, 处理引擎: SSH引擎, 父模板ID: soft, 描述: 创建SSH或SFTP服务的模板.
- Telnet** (ID: telnet): 模板版本: 1.0.6, 日志类型: 服务访问, 处理引擎: Telnet引擎, 父模板ID: soft, 描述: 创建Telnet服务的模板.
- Telnet(Windows)** (ID: telnetw): 模板版本: 1.0.12, 日志类型: 服务访问, 处理引擎: TCP自定义引擎, 父模板ID: soft, 描述: 自定义Telnet协议解析模板.
- WEB仿真模板** (ID: http): 模板版本: 1.0.4, 处理引擎: HTTP引擎, 父模板ID: soft, 描述: HTTP基础模板.

The screenshot shows the DecoyMini forum page. The browser address bar shows 'bbs.decoyit.com/forum-57-1.html'. The forum header includes 'DECOYMINI 技术交流社区' and navigation links for '帖子', '请输入搜索内容', '应用', '设置', '安全资讯', '安全工具', '综合资料', '技术资料', and '环境'. The forum title is '仿真模板'. Below the title, there is a message: 'Mini 用户可在此处分享模板使用心得及自己创建的模板!' and statistics: '本版主题 19 | 今日发帖 0 | 排名 6.1 | 收藏本版 0'. A '板规' (Board Rules) section follows, stating '分享模板使用心得及自己创建的模板!'. At the bottom, there are category filters: '全部', '使用秘籍 2', '网络服务类 2', 'WEB类 2', '数据库类 4', '中间件类 6', '应用类 2', '设备类 1', and '其他类'.

- 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

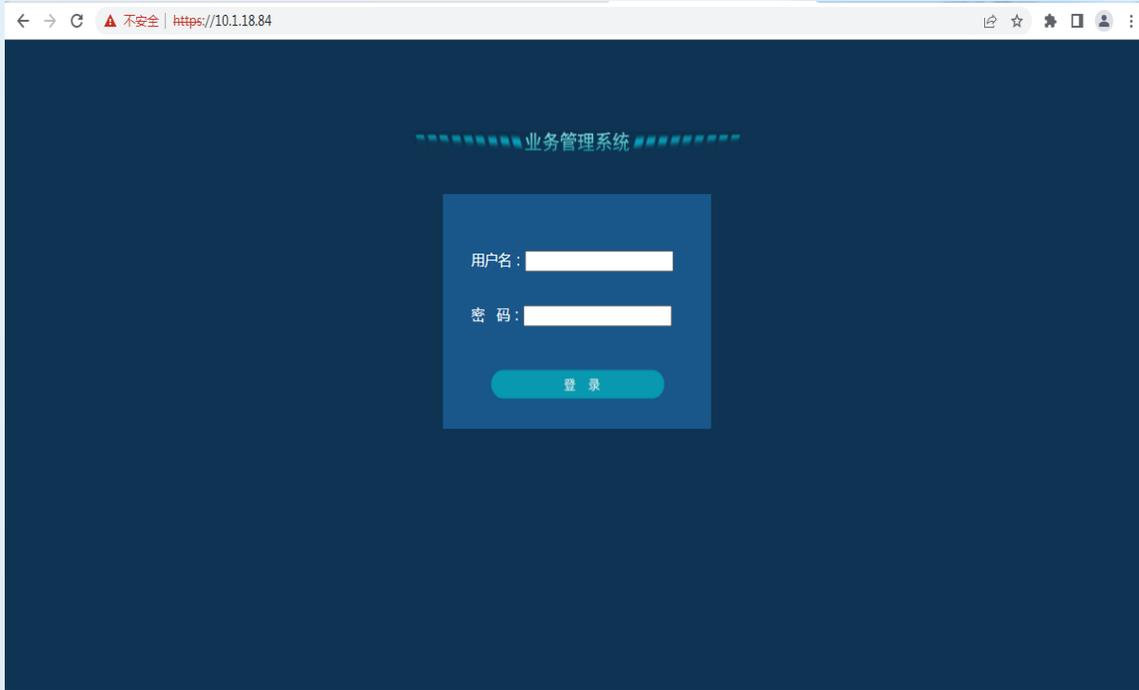
The screenshot displays the DecoyMini web interface for editing a simulation template. The sidebar on the left contains navigation menus for various system components. The main panel shows the '编辑 test 模板' (Edit test template) form, which includes a list of actions (发布, 创建子模板, 导出, 删除) and a '分享模板...' button. The form is divided into tabs: '基础信息' (Basic Information), '参数设置' (Parameter Settings), '响应数据' (Response Data), '资源文件' (Resource Files), and '作者信息' (Author Information). The '基础信息' tab is active, showing fields for '模板ID' (test), '模板名称' (test), '事件日志类型' (请选择), '类别' (其它类), '支持软件版本' (≥), '处理引擎' (TCP自定义引擎), and '父模板名称' (soft).

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

The screenshot displays the DecoyMini web interface for configuring a strategy. The left sidebar contains navigation items: 监控, 事件, 策略, 诱捕策略 (selected), 仿真模板, 安全规则, 预警策略, 节点, 系统, 内生情报, and 技术论坛. The main content area is titled '修改 DecoyMini 个性化策略【草稿】' and includes a toolbar with buttons: '+ 应用' (highlighted in red), '运行状态', '- 删除草稿', '- 删除', '↑ 导入', and '↓ 导出'. Below the toolbar are tabs for '诱捕器配置' and '参数配置'. A dropdown menu (highlighted in red) is open, showing options: '诱捕策略模板', '内网横向渗透监测', and '互联网攻击诱捕'. The main area displays six service templates: SSH服务, FTP服务, VNC服务, MySQL数据库, Redis数据库, and DNS服务. Each template card shows its icon, name, status (运行), category (网络服务类 or 数据库类), IP address, and a '启用' toggle switch.

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

#	名称	IP	端口	状态	操作
1					
2					
3					
4					
5					
6					
7	TCP端口连接	0.0.0.0	139	启用	编辑 删除
8	TCP端口连接	0.0.0.0	135	启用	编辑 删除
9	虚拟服务	0.0.0.0	8080	禁用	编辑 删除

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

The screenshot displays the DecoyMini interface. On the left is a navigation sidebar with options like '监控', '事件', '风险事件', '诱捕日志', '策略', '节点', '系统', and '技术论坛'. The main area shows a table of luring logs with columns for #, 类型, 诱捕器, 动作, 描述, 结果, 级别, IP, 时间, and 操作. A detailed view on the right shows the '诱捕日志详情' for a specific event, including the source IP (86.149.213.135), target IP (10.1.18.178), and a hex dump of the attack packet.

#	类型	诱捕器	动作	描述	结果	级别	IP	时间	操作
1	服务访问	VPN入口站点	下载数据	访问首页: /	成功	警告	103.203.57.29 10.206.0.16	2021-11-26 11:42:03	[操作]
2	服务访问	SSH服务	登录	用户 root 登录成功	成功	严重	193.105.134.45 10.206.0.16	2021-11-26 11:41:03	[操作]
3	WEB访问	WEB业务系统	下载数据	访问首页: /	成功	警告	24.176.206.12 10.206.0.16	2021-11-26 11:28:33	[操作]
4	服务访问	Telnet服务	登录	用户登录(CUAdmin, CUAdmin)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:13	[操作]
5	服务访问	Telnet服务	登录	用户登录(root, gpon)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:13	[操作]
6	服务访问	Telnet服务	登录	用户登录(root, samsung)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:13	[操作]
7	服务访问	Telnet服务	登录	用户登录(admin, ho4uku6at)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:12	[操作]
8	服务访问	Telnet服务	登录	用户登录(root, 20080826)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:12	[操作]
9	服务访问	Telnet服务	登录	用户登录(e8ehome1, e8ehome1)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:12	[操作]
10	服务访问	Telnet服务	登录	用户登录(root, hi3518)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:12	[操作]
11	服务访问	Telnet服务	登录	用户登录(root, Fireitup)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:12	[操作]
12	服务访问	Telnet服务	登录	用户登录(root, xc3511)	失败	提示	42.235.82.76 10.206.0.16	2021-11-26 11:02:12	[操作]

诱捕日志详情

攻击源IP: 86.149.213.135:33463 英国 攻击目的IP: 10.1.18.178:22 本地

描述: 86.149.213.135:33463 连接 10.1.18.178:22

PACKET: 74 bytes

- Layer 1 (14 bytes) = Ethernet {Contents=[..14..] Payload=[..60..] SrcMAC=d4:b1:10:35:c2:90 DstMAC=00:0c:29:0f:c8:43 EthernetType=IPv4 Length=0}
- Layer 2 (20 bytes) = IPv4 {Contents=[..20..] Payload=[..40..] Version=4 IHL=5 TOS=32 Length=60 Id=27358

攻击首包: Flags=DF FragOffset=0 TTL=47 Protocol=TCP Checksum=38894 SrcIP=86.149.213.135 DstIP=10.1.18.178 Options=[] Padding=[]

- Layer 3 (40 bytes) = TCP {Contents=[..40..] Payload=[] SrcPort=33463 DstPort=22(ssh) Seq=1791015245 Ack=0 DataOffset=10 FIN=false SYN=true RST=false PSH=false ACK=false URG=false ECE=false CWR=false NS=false Window=14600 Checksum=18502 Urgent=0 Options=[..5..] Padding=[]}

攻击载荷:

```
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
-----
0000h: 53 53 48 2D 32 2E 30 2D 48 45 4C 4C 4F 57 4F 52 SSH-2.0-HELLOWOR
0010h: 4C 44 0D 0A 00 00 01 34 0A 14 30 19 59 7D 71 C2 LD.....4..0.Y)q.
0020h: F9 70 A1 E7 81 58 B1 BD C4 E9 00 00 00 54 64 69 .p...[.....Tdi
0030h: 66 66 69 65 2D 68 65 6C 6D 61 6E 2D 67 72 6F ffile-hellman-gro
```

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

诱捕日志详情

日志信息 | 时间线

[下载操作文件](#)

类型：服务访问	诱捕器：FTP服务
用户：admin	动作：上传文件
级别：严重	结果：成功
攻击源IP：58.23.127.246:54605 中国 福建 漳州	攻击目的IP：10.1.18.178:21 本地
描述：上传文件/业务材料/AV/lnk	
fileMd5：3a9349af006440c7e0da677724551239	
fileName：/业务材料/AV/lnk	
发送者：10.1.18.178	数据源：诱捕探针(Linux)
记录时间：2022-06-23 00:07:05	保存时间：2022-06-23 00:07:09

诱捕日志详情

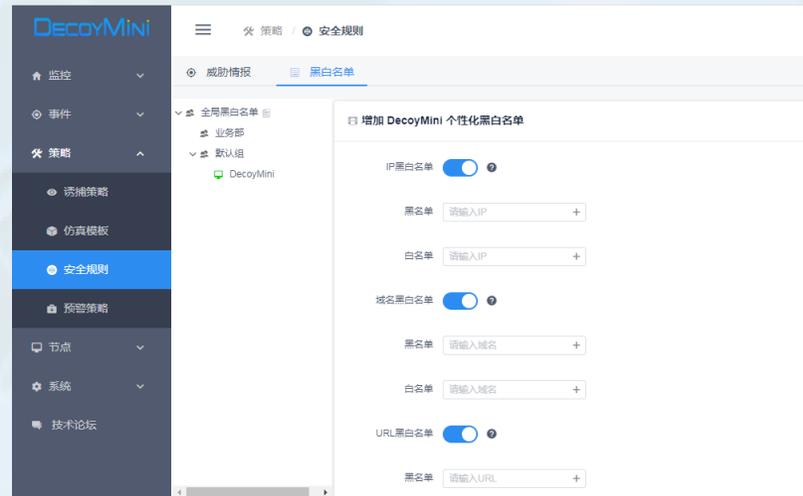
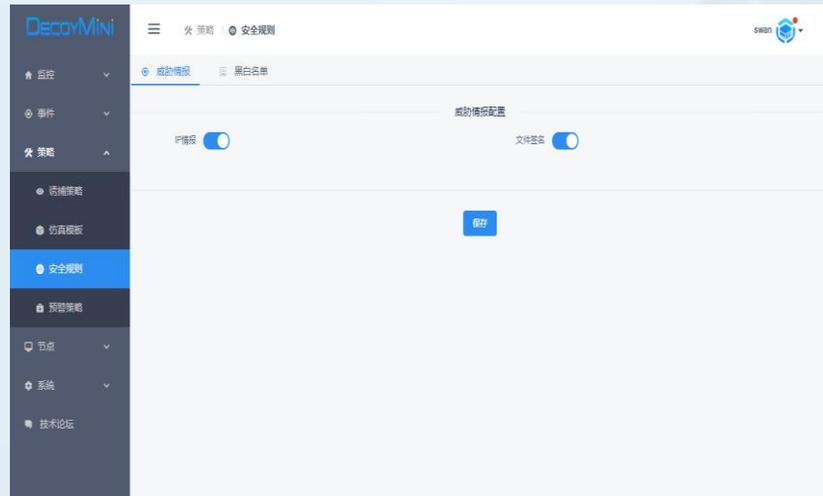
日志信息 | **时间线**

- [提示]** 2022-06-29 16:44:17 用户登录(root, klv1234)
类型：服务访问 日志源：Telnet服务 记录时间：2022-06-29 16:44:14
用户：无 操作：登录 结果：失败
攻击源：103.105.190.242:43757 印度尼西亚 攻击目标：10.1.18.178:23 本地
- [提示]** 2022-06-29 16:44:17 用户登录(root, oelinux123)
类型：服务访问 日志源：Telnet服务 记录时间：2022-06-29 16:44:14
用户：无 操作：登录 结果：失败
攻击源：103.105.190.242:43757 印度尼西亚 攻击目标：10.1.18.178:23 本地
- [提示]** 2022-06-29 16:44:17 用户登录(root, jvbzd)
类型：服务访问 日志源：Telnet服务 记录时间：2022-06-29 16:44:15
用户：无 操作：登录 结果：失败
攻击源：103.105.190.242:43757 印度尼西亚 攻击目标：10.1.18.178:23 本地

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

DecoyMini

- 监控
- 事件
 - 风险事件
 - 诱捕日志
- 策略
- 节点
- 系统
- 内生情报
- 技术论坛

事件 / 风险事件

falcon

查询 导出 提交情报...

#	名称	级别	类型	标签	描述	攻击IP	被攻击IP	时间	操作
1	Log4j2漏洞监测诱捕到GET事件	中	WEB访问	Log4j2漏洞监测 GET	访问首页: /	43.132.196.160	10.1.18.178	2022-06-29 17:17:18	
2	SSH服务诱捕到Login事件(6)	中	服务访问	SSH服务 Login	用户 root 登录失败	43.248.128.82	10.1.18.178	2022-06-29 17:13:29	
3	SSH服务诱捕到Login事件	高	服务访问	SSH服务 Login	用户 root 登录成功	43.248.128.82	10.1.18.178	2022-06-29 17:13:29	
4	SSH服务诱捕到Login事件(6)	中	服务访问	SSH服务 Login	用户 admin 登录失败	114.216.125.126	10.1.18.178	2022-06-29 17:07:44	
5	141.98.10.157匹配到IP威胁情报	中	威胁情报	威胁情报 僵尸机 扫描 爆破 垃圾邮件 蜜罐捕获 SSH服务 Login	用户 user 登录失败	141.98.10.157	10.1.18.178	2022-06-29 17:04:05	
6	81.17.25.50匹配到IP威胁情报	中	威胁情报	威胁情报 DDOS拒绝服务攻击 SSH服务 Login	用户 admin 登录失败	81.17.25.50	10.1.18.178	2022-06-29 16:56:07	
7	SSH服务诱捕到Login事件(2)	中	服务访问	SSH服务 Login	用户 root 登录失败	95.255.110.170	10.1.18.178	2022-06-29 16:54:35	
8	SSH服务诱捕到Login事件	中	服务访问	SSH服务 Login	用户 user 登录失败	208.126.202.45	10.1.18.178	2022-06-29 16:53:12	
9	Log4j2漏洞监测诱捕到GET事件(2)	中	WEB访问	Log4j2漏洞监测 GET	访问首页: /	117.50.182.172	10.1.18.178	2022-06-29 16:48:20	
10	Telnet服务诱捕到Login事件	高	服务访问	Telnet服务 Login	用户登录(root, 123456)	103.105.190.242	10.1.18.178	2022-06-29 16:44:25	

事件详情

事件名称: SSH服务诱捕到Login事件 级别: 中

事件类型: 服务访问 威胁分类: 无

攻击源IP: 114.216.125.126 中国 江苏 苏州 攻击目的IP: 10.1.18.178 本地

标签: SSH服务 Login 阶段: 单点突破

事件描述: 用户 admin 登录失败

影响: 攻击者的攻击行为可能会导致服务中断或者敏感数据泄露。

解决方案: 对发起攻击的主机进行安全排查。

规则名称: 威胁诱捕默认规则[级别:中] 合并数量: 6条

关联诱捕器: SSH服务 事件ID: xHcURZWzIX6acW4BgnCbAm

开始时间: 2022-06-29 17:07:44 结束时间: 2022-06-29 17:07:44

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

增加任务

数据过滤 +

处置方式 选择模板 手动配置

处置分类 预警通知

处置类型 请选择

- 邮件
- 弹窗
- 企业微信
- 钉钉
- 飞书
- Syslog输出

连接测试

优先级

状态

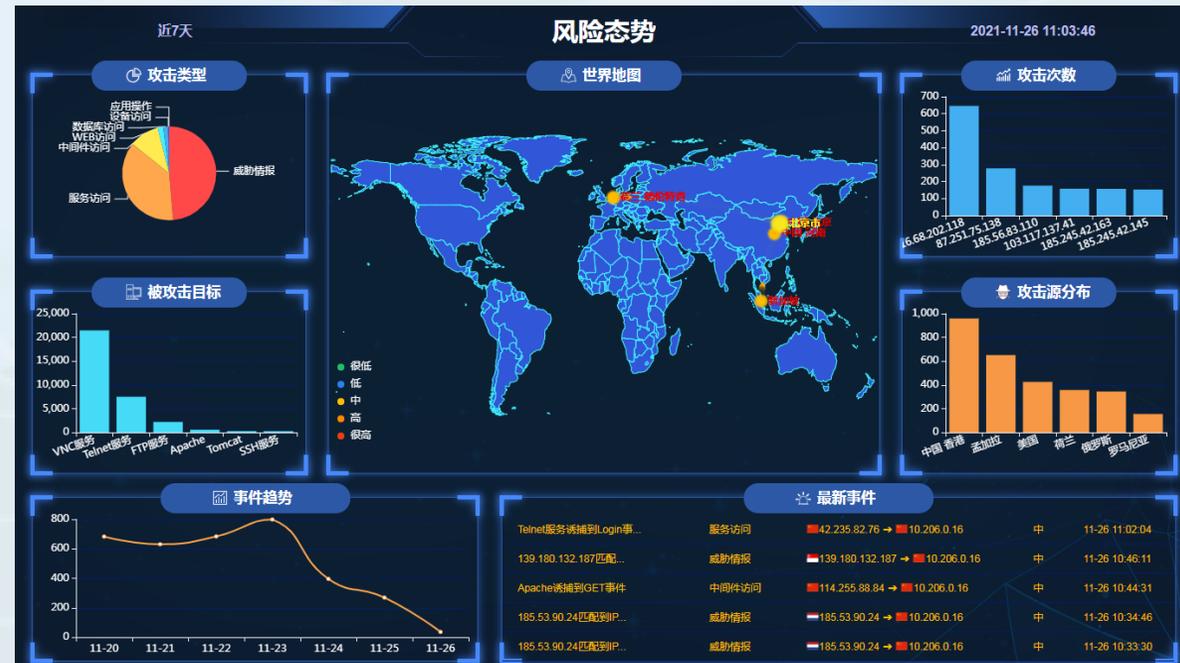
取消 确定

共 1 条 < 1 > 10 条/页

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

The screenshot displays the DecoyIT interface for analyzing an attack IP. The main window is titled "攻击IP [redacted] 分析" and contains several tabs: "攻击者画像" (Attacker Profile), "攻击者特征" (Attacker Characteristics), "风险事件" (Risk Events), and "诱捕日志" (Lure Log). The "攻击者画像" tab is active, showing a central "攻击IP" node with four main categories of information:

- 基本信息 (Basic Information):** Includes "最近攻击IP: 172.16.100.1041-11-30 13:44:26", "攻击者编号: 2111301344", "物理位置: 本地", and "最近攻击时间: 2021-11-30 13:44:26".
- 主机特征 (Host Characteristics):** Includes "系统时区: UTC+8:0", "显示器分辨率: 1366x768", "操作系统: Windows 7", and "系统平台: Windows".
- 浏览器特征 (Browser Characteristics):** Includes "浏览器引擎版本: 537.36", "浏览器版本: 96.0.4664.45", "浏览器名称: Chrome", "浏览器语言: zh-CN", "浏览器指纹: f95315231be32f82...", "浏览器插件: PDF Viewer; Chro...", and "浏览器引擎: AppleWebKit".
- 曾使用服务 (Previously Used Services):** Includes "80/http", "22/ssh", "6379/redis", and "8000/http".

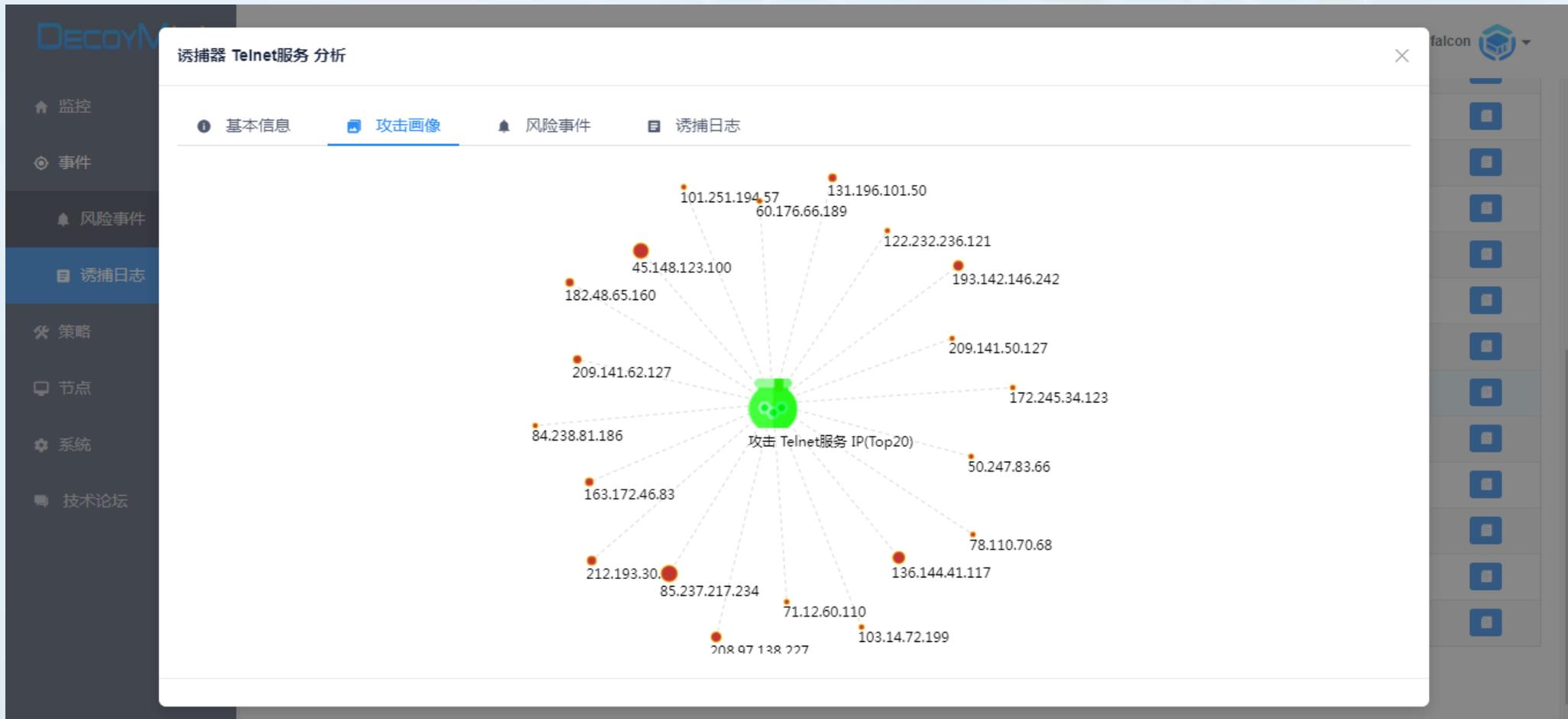
The "攻击目标" (Attack Target) is also visible, showing a red target icon and a red arrow pointing to a specific IP address. Below the main profile, a "诱捕日志详情" (Lure Log Details) window is open, showing a log entry for a successful connection. The log entry includes details such as "类型: 网络操作", "用户: 无", "级别: 警告", "攻击源IP: 194.31.98.252:41482", and "攻击目的IP: 10.1.18.178:23". A dropdown menu is visible over the log entry, with options like "加全局白名单", "加节点白名单", "查询'奇安信威胁情报中心'", and "查询'守望者威胁情报平台'".

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



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

DECOYMINI

情报 / 内生情报

falcon

内生情报生产配置

时间周期: 最近7天

数据过滤

排除: 局域网地址, 国内地址

数量限制: 无限制

情报格式: 精简(IP列表)

状态: 启用

服务状态: 运行中, 内生情报下载地址: <http://demo.decoymini.com:88/eti/Utw6wWJwqkYn45z8Lzp75>

确定

基于对攻击源的分析 and 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

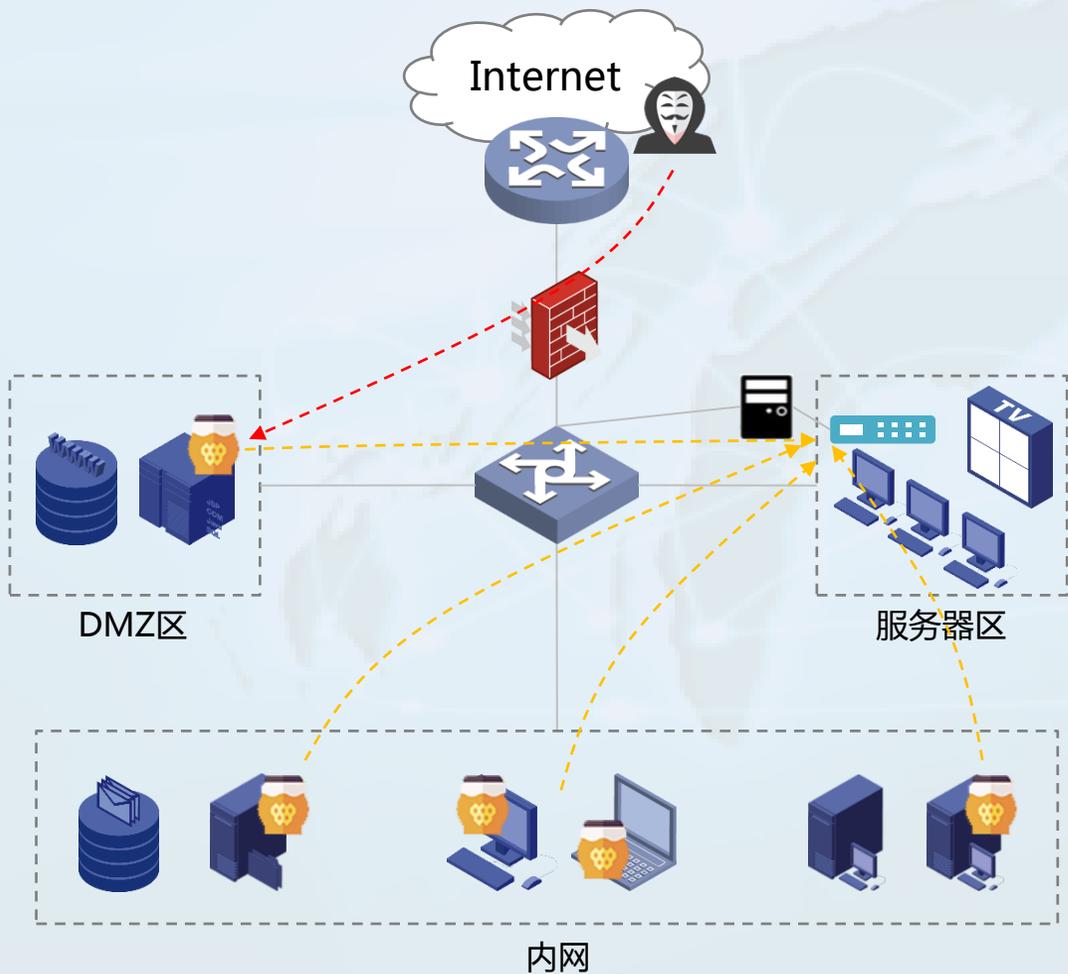
24小时不间断值守

- 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

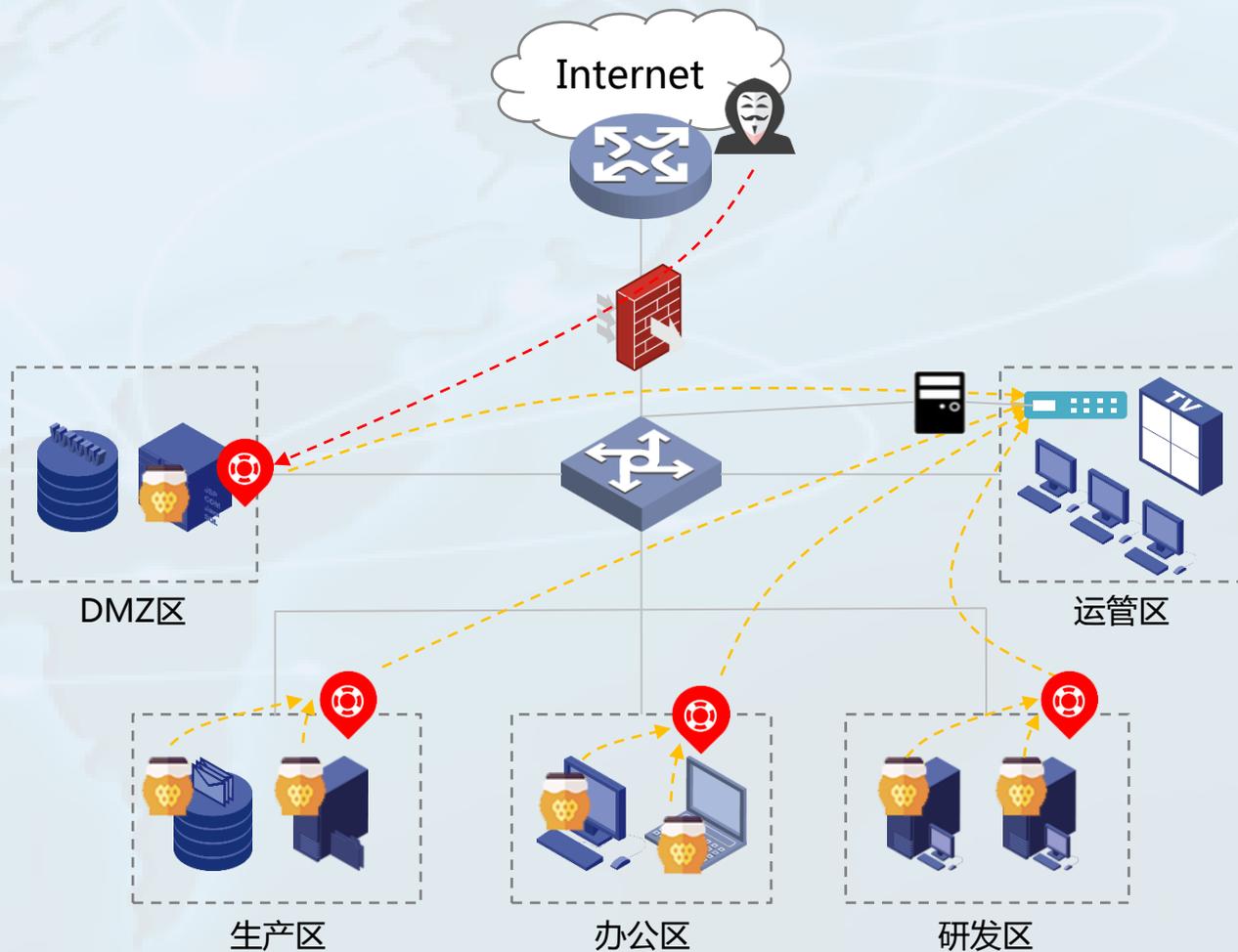


典型部署方案

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

The image shows two screenshots from a web interface. The left screenshot is from DecoyMini, showing the '内生情报生产配置' (Internal Intelligence Production Configuration) page. The '情报格式' (Intelligence Format) is set to '精简(IP列表)' (Concise (IP List)), and the '状态' (Status) is '启用' (Enabled). The '服务地址' (Service Address) is 'http://demo.decoymini.com:88/eti/Utw6wWJwqKYn45z8Lzp75'. The right screenshot is from NTM, showing the '情报管理' (Intelligence Management) page. A modal window '自动同步' (Automatic Sync) is open, with 'DecoyMini' selected as the '蜜罐系统' (Bait System) and '本地蜜罐' (Local Bait) selected as the '同步说明' (Sync Description). A red arrow points from the '自动同步' button in the top right of the NTM page to the modal window.

- 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

添加端口映射

映射线路: WAN (映射的公网IP)

映射IP: (如果为0.0.0.0,则使用线路IP)

映射端口: (多个端口之间用逗号隔开) (映射的公网端口)

协议: 任意

主机类型: 指定IP (DecoyMini地址)

主机IP: (DecoyMini端口)

主机端口: (为空或0, 表示使用映射端口)

下一跳: (下一跳, 若DecoyMini的网关不, 则需要指定LAN口对端三层设备的IP)

备注: (备注)

策略状态: 启用

确定 取消

添加端口映射

映射线路: WAN

映射IP: 192.168.100.100 (如果为0.0.0.0,则使用线路IP)

映射端口: 1-65535 (多个端口之间用逗号隔开)

协议: 任意

主机类型: 指定IP

主机IP: 192.168.100.100

主机端口: 0 (为空或0, 表示使用映射端口)

下一跳: 10.0.0.254

备注: DecoyMini全映射

策略状态: 启用

确定 取消

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



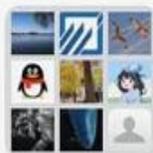
DecoyMini 交流群



DecoyMini 免费下载链接:

<https://github.com/decoymini>

<https://decoymini.decoyit.com>



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



DecoyMini 技术交流社区:

<http://bbs.decoyit.com>

The background features a light blue world map with white grid lines. A solid dark blue horizontal band is positioned across the middle of the slide. Two thin, dark blue horizontal lines are located at the top and bottom of the slide, with the top line being slightly longer than the bottom one.

谢谢！