



用户手册 V1.9.1「SaaSV3.3.8」

(文档编号: MG-SY-2021-007)

北京知道创宇信息技术股份有限公司



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 V1.9.1「SaaSV3.3.8」

© 版权所有 北京知道创宇信息技术股份有限公司

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. 7	^上 品介绍	1
2. D	风险大盘	2
2.1.	数据时间筛选	2
2.2.	威胁总览	3

2.2		
3.3.	威胁致据	
4.	安全态势大屏	
5. 걜	蜜罐管理	
5.1.	蜜罐部署	5
5.1.1	1. 部署云蜜罐	5
5.1.2	2. 部署客户端蜜罐	10
5.2.	蜜罐列表	14
5.3.	蜜罐设置	14
5.4.	定制蜜罐	16
5.4.1	1. 克隆蜜罐	17
5.4.2	2. 自定义蜜罐	
5.4.3	3. 默认蜜罐	
6. 楶	客户端管理	
6.1.	客户端列表	
6.2.	客户端部署	20
6.3.	客户端操作	22
6.4.	客户端卸载	
7. 걜	蜜饵管理	
7.1.	邮件蜜饵	23
7.2.	文件蜜饵	
8. 质	成胁情报	
8.1.	攻击者画像	
© 202	21 北京知道创宇信息技术股份有限公司	IV



8.2. 文件下载	29
8.3. 攻击日志	29
8.3.1. 日志操作	30
8.4. 安全事件	32
9. 数据管理	33
9.1. 行为分析报告	33
9.2. 日志数据下载	34
10. 策略配置	36
10.1. SYSLOG 配置	36
10.2. 白名单配置	36
10.2.1. 计入攻击日志配置	36
10.2.2. 添加白名单 IP	37
10.2.3. 添加白名单 MAC	37
10.2.4. 白名单删除	38
10.3. 蜜罐模板配置	39
10.3.1. 默认蜜罐	39
10.3.2. 定制蜜罐	39
11. 监控管理	39
12. 通知管理	39
12.1. 威胁告警	39
12.2. 系统通知	39



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。



2019-08-29 17:49:51					~ 2019-09-29 17:49:51									
<< <		20	19年;	B月						20	19年	9月		> >
_	=	\equiv	四	五	六			_	=	\equiv	四	五	六	日
29		31	1	2	З	4			27	28	29		31	1
5	6	7	8	9	10	11		2	3	4	5	6	7	8
12	13	14	15	16	17	18		9	10	11	12	13	14	15
19	20	21	22	23	24	25		16	17	18	19	20	21	22
26	27	28	29	30	31	1		23	24	25	26	27	28	29
2		4	5	6	7			30	1	2	3	4	5	6
											3	先择时	t间	确定

图 2. 选择时间段



3.2. 威胁总览

- 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。

			2021-03-19 ~	2021-03-26 📋				
受攻击中 当前安全状态	22 当前蜜罐总数	8 _{ip} 5 _{指纹} 24小时黒客溯源		10 24小时威胁指数				
图 3. 威胁总览 3.3. 威胁数据								

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;

抓获安全事件 捕获安全事件;	件统计 ^{总数} 264条		捕获安全事件类型TOP 5 外网URL探测	124	捕获安全事件趋势 100 ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
			外网端口扫描	79	75 8
■ 高危	51条	19%	内网 Shell 命令执行	36	50
■ 中危	213条	80%	内网 SQL 注入	15	25
= 低危			外网POP3頻繁连接	5	
			-		2021-03-25 16:00:00 2021-03-25 22:00:00 2021-03-26 04:00:00 2021-03-26 10:00:00
捕获攻击日家	志统计		一 捕获攻击日志类型TOP 5		2021-03-25 16:00:00 2021-03-25 22:00:00 2021-03-26 04:00:00 2021-03-26 10:00:00 (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (2021-03-26 10:00:00) (202
捕获攻击日 調 捕获攻击日志/	志统计 总数12321 _条		捕获攻击日志类型TOP 5 第口扫描	6545	2021-03-25 16:00:00 2021-03-25 22:00:00 2021-03-26 04:00:00 2021-03-26 10:00:00 捕获攻击日志趋势)00
捕获攻击日 幕 捕获攻击日志,	志统计 总数12321 _条		捕获攻击日志类型TOP 5 端口扫描 URL访问	6545 5595	2021-03-25 16:00:00 2021-03-25 22:00:00 2021-03-26 04:00:00 2021-03-26 10:00:00 捕获攻击日志趋势 100
捕获攻击日志 捕获攻击日志	志统计 ^{总数} 12321条 10条	0%	<mark>捕获攻击日志类型TOP 5</mark> 塔口扫描 URL协问 Shell命令执行	6545 5595 100	2021-03-25 16:00:00 2021-03-25 22:00:00 2021-03-26 04:00:00 2021-03-26 10:00:00 捕获攻击日志趋势 100 100
捕获攻击日 調 捕获攻击日志	志统计 总数12321条 10条 100条	0%	捕获攻击日志类型TOP 5 译口扫描 URL访问 Shell命令执行	6545 5595 100 40	2021-03-25 16:00:00 2021-03-25 22:00:00 2021-03-26 04:00:00 2021-03-26 10:00:00 捕获攻击日志趋势 100 100

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;
- 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;
- **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。



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。

 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);

◎ 风险大盘		旨页 / 蜜繡管理		
8 蜜罐管理		蜜罐管理	× 1	
よ 客户端管理				
国 威胁情报	~	当前已邮署257个蜜罐 蜜罐状态:正常 261 审核中 31 待解析 21 异常 2131 邮署失败 81 重置失败 5		部署蜜羅
➡ 数据管理	~	蜜罐类型: 全部 🗸	请输入蜜罐名称/蜜罐IP/域名	搜索
◎ 系统配置	~			

图 7. 部署蜜罐入口

5 知道创宇 KNOWINSEC.COM	创宇蜜罐-威胁诱捕与溯源系统 SaaS 版用户手册
^{普页 / 數湯管理} 选择部署方式	
	立即部署蜜罐,开启威胁诱捕溯源服务 ^{当前套管为:} 创建蜜罐圆试套锤 (过期时间2021-02-02 00:00:00)
	 一共可節署 2 个電識(後入 2个子域名),当前已部署 2 个客戶端蜜編,0个云蜜編,还可部署0 个蜜 編(後入 2 个子域名)
	客户總電罐 适用于內阿當組场景需要准备服务器或虚拟机部署客户端 取 消 工 如即都署

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;

■ 域名 选择蜜罐 ^{最场限,有域名即可接入多个云蜜罐。蜜罐 齿点 (如): Discuz, WordPress, OA, 禅}
■ 域名 选择蜜罐 ^{最场限,有域名即可接入多个云蜜罐。蜜罐 齿点 (如): Discuz, WordPress, OA, 禅}
■ 域名 选择蜜罐 膨脹,有域名即可接入多个云蜜罐。蜜罐 齿点(如:Discuz, WordPress, OA, 禅
■ 域名 选择蜜罐
城名 选择蜜罐 融质,有域名即可接入多个云蜜罐。蜜罐 店店(如: Discuz, WordPress, OA, 禅
● 选择蜜罐 减名 选择蜜罐 ^{最场质,有域名即可接入多个云蜜罐。蜜罐 站点(如: Discuz, WordPress, OA, 禅}
域名 选择蜜罐 ^{最场景,有域名即可接入多个云蜜罐。蜜罐 6.5 (如): Discuz, WordPress, OA, 禅}
電场景,有域名即可接入多个云蜜罐。蜜罐 访声(如: Discuz, WordPress, OA, 禅
最场景,有域名即可接入多个云蜜罐。蜜罐 访声(如:Discuz, WordPress, OA, 禅
最场景,有域名即可接入多个云蜜罐。蜜罐 访声(如:Discuz、WordPress、OA、禅
晶场景,有域名即可接入多个云蜜罐。蜜罐 访声(如:Discuz,WordPress、OA、禅
晶场景,有域名即可接入多个云蜜罐。蜜罐 访声(如:Discuz,WordPress, OA、禅
電场景,有域名即可接入多个云蜜罐。蜜罐 访点(如:Discuz,WordPress、OA、弹
店点(如:Discuz、WordPress、OA、禅
AND AND A CONTRACT OF A CONTRACT.
馬各访问项名、进入云蜜羅,开记录馬客在 19里案进行全网湖酒 后制
」而曾近1]主网加标、汉即。
.com
部署 下一步
部署

÷

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;



[/云蜜罐/部署云蜜罐 署云蜜罐				
		•		
	输入根	域名 选择蜜罐		
前可接入云蜜罐数量:2,请根据实际情况进行	部署,请勿输入与真实业务相	同的子域名。		 ● 添加蜜罐 全部消
统为您智能推荐以下蜜罐-域名映射关系:				
蜜罐类型		子域名		操作
▲ 然之OA OA类 ∨		oa	.abc.com	删除
		山上 前照 梁 续 长期		
				-

 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。

/ 云蜜罐						
寳 罐						
前已部署1个蜜罐 蜜罐状	态: 正常 0 异常 <mark>0</mark> 审核中 1 部	3署中 <mark>0</mark>				⊕ 部署蜜舗
罐类型: 全部	\sim			请输入蜜罐名称/蜜罐	P/域名/客户端名利	搜索 搜索
쭡罐类型	蜜罐名称	部署模式	Ŧ	蜜罐状态	Ŧ	操作
OA 然之OA	然之OA区	云蜜罐	軍権	亥中 ⑦		设置
				#1条		10 冬/雨
						10 3432
			- T). T			
	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	11. 云蜜罐印	í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;



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。

^{首页 / 云蜜罐 / 蜜罐设置} 域名解析说明	
 阿里云配置步骤 DNSpod 配置步骤 	
 进入 阿里云 域名解析商域名配置平台; 、进入域名解析栏目,在对应根域名下对子域名(当前为: bg.abc.com)进行A记录解析, 3、返回蜜罐管理页,查看子域名解析状态。 	解析到对应的 <mark>蜜罐IP地址(当前为:: 7)</mark> ;
图 13. 域名解析说明	

 \sim

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。

云蜜罐						
当前已部署1个蜜罐 蜜罐状	ː杰: 正常 0 异常 <mark>0</mark> 审核中 <mark>0</mark>	那署中 0				④ 部署蜜
蜜罐类型: 全部	v			请输入蜜罐名称/蜜罐IP	/域名/客户端名称搜	素搜
蜜罐类型	蜜罐名称	部署模式	Ŧ	蜜罐状态	Ψ	操作
OA 然之OA	然之OA 🗹	云蜜罐	待解	近 ⑦ 去解析域名 已完成		设置
				共1条	< 1 >	10 条/页
	图 14.	云蜜罐待解树	斤-已完成		15	
首页 / 云蜜罐 云蜜罐						
当前已部署1个蜜罐 蜜罐状	态: 正常 0 异常 <mark>0 </mark> 审核中 0 音	『署中 0				 ① 部署蜜
蜜罐类型: 全部	×			请输入蜜罐名称/蜜罐IF	/域名/客户端名称搜	索 搜
蜜罐类型	蜜罐名称	部署模式	Ŧ	蜜罐状态	Ŧ	操作
OA 然之OA	然之OA区	云蜜罐	(II#	③ 已服务几秒	威胁	日志 设置
				共1条	< 1 >	10 条/页

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。

图 15.

- **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。

✓ 云蜜罐成功部署

- ▶ 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
 © 2021 北京知道创宇信息技术股份有限公司

 \$\$ 9 页 共 40 页



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);

		首页 / 蜜繡管理	
ダ 蜜罐管理		蜜罐管理	
太 客户端管理			
I 威胁情报	*	当前已部署257个宝罐 蜜罐状态:正常 26 审核中 3 待解析 2 异常 213 部署失败 8 重置失败 5	② 御客蜜謡
▷ 数据管理	~	蜜罐类型: 全部 🗸	(请输入蜜罐名称/蜜罐IP/域名 搜索
③ 系統配置	~	图 16 部署蜜罐入口	

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;

◎ 风险大盘		首页 / 客户端管理				
8 蜜罐管理		客户端管理				
ム 客户端管理						
🗉 威胁情报	.*	客户端状态: 在线: 0 离线: 2 关闭: 0			如何卸载客	戶蜡? ⊙ 部署客户线
▶ 数据管理	*	客户端状态: 全部 ∨		× .	(请输入客户编名称/于网护搜索	援索
◎ 系统配置	~					
♀ 通知管理		カ公区 ② 相序版本: 1.5.31 発音 P 首: 1↑ 用P: miguan3	蜜貓部著情况: 建议每个客户端不多于200个蜜罐	今 (2) (2) (2) (2) (2) (2) (2) (2)	各戶編状态: 在送 	生新志者 ① 重启 关闭

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);

部署審	お報								
选择蜜	建 景分类 按类型分类								
办 4		数据中心区 适用于数据中心网络环	100 A	DMZ	Ole -	生产服务区		应用服务区	* 9
	Redis ElasticS MongoDB	MySQL Memcac	Page 2.		ee Red 部看 蜜謡	lis蜜鼬 is蜜鼬是一种开源免费 计情况 暂未邮署。	、遵守BSD协议、高性能的K4	ay-Value数据库。 默认端曰:	6379
			图 18.	根据	场景选	择蜜罐	Ż		
部署蜜罐							/ . /		
选择蜜罐 按场景分类	按类型分类	访问控制系统	客户管理系统	财务等理	國家統	开发应用类	教經库	TiQ	中面件
						/ inclaring a	AN INC.	10074	
ATE SSH Rsync San	足物重線 PP Vic SMTP ・ かわる アクワコ TELNET	DNS MongoDB Z13 建築文件	MySQL Memcac	OpenSSH	SS SSL □4 部	H 蜜鍵 蜜罐是一种为远程登 注: ubuntu/ubuntu 雪情況 5个 客户端: 51	澡会话提供安全性的协议。 、 用户: 5个	用以收集攻击者使用的凭握	, 默以端曰: 22: 登录
	Ţ	, FI	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。

* 请选择客户端:	办公区 🗸		部署新的客户端
*请选择网卡IP:	10.8.246.136/24		
	该网段(10.8.246.136/24)以下IP(端口)已绑定蜜 罐: 10.8.246.231(80)		
*蜜罐IP:	10 . 8 . 246		如: 22,89,100-103
*服务端口设置:	HTTP 80		
	注意: 1、蜜罐IP必须与网卡IP在同一个网段内; 2、蜜罐IP必须是该网段的空闲IP;		
开启甜度设置:			
×	图 20. 部署客户端蜜舖	 歯 佳	
● 甜度设	/置 (可洗)		

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。



开启甜度设置:		
公司名称:	请输入公司名称	
公司logo:	土 上传文件 文件大小不能超过50M	
管理员密码:	请输入管理员密码	
	图 21. 甜度设置.	21.6

4) 部署蜜罐成功后,蜜罐列表会显示相应的蜜罐信息。

	_							
◎ 风险大盘		首页 / 蜜罐管理						
8 蜜繡管理		蜜罐管理						
よ 客户端管理								
回 威胁情报	~	当前已部署1个蜜罐 蜜罐状态:正常 1						⊙ 部署蜜罐
▷ 数据管理	*	蜜罐类型: 全部 ✓			(请输入》	(雄名称/蜜罐印/域名		提索
◎ 系統配置	÷							
O		蜜罐类型	蜜罐名称	部署模式	T	蜜罐状态	Ŧ	操作
₩ 2/16/4		OA 然之OA	然之OA 🗹	864	EX	③ 已服务几秒	3	或胁日志 设置
						共1条	< 1	> 10 奈/页 >
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。

前已部	著. 个蜜罐 蜜罐状态:正	常 軍核中 异常 部署失敗 重算	重失则					③ 部業蜜謡 日
[羅类型:	全部	◇ 客户端: 全部 ◇						
	蜜罐类型	蜜罐名称	部署模式	Ψ	蜜罐状态	Ψ	用户	备注 操作
	OA 然之OA	然之OA(2) 区	云蜜罐	軍核	• 0		mg @sc	设置
	OA 然之OA	然之OA(1) 区	云蜜罐	部署失	0		mç @sc	攻击日志 设置
	OA 然之OA	然之OA 🗹	客戶議	F R	🕐 ⑦ 已停止服务7 个月		mı 1@sc	攻击日志 设置
	OA 然之OA	然之OA 🗹	云蜜罐	F#	⑦ 已停止服务7 个月		mgi 1@sc	攻击日志 设置
								共4条 < 1 > 10条/
			XX					
			反 92	应	(塘石)主			

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。

然之OA 正常 已服务3 小时 子城名如何解析到蜜罐?		(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
蜜驢序号: 000770 部署模式: 云雪端	蜜骝类型: 然之OA OA英	蜜驢部署时间: 2021-12-09 11:41:46





● 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)。

蜜罐信息	取消 更新
子域名:webabc.com	

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。

蜜罐信息		编辑
客户端:办公区 蜜罐IP(共1个): • 10.8.246.180	子网IP:10.8.246.134	
	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。)



蜜罐甜度		取消	更新
公司名称:	请输入公司名称		
公司logo:	上 上传文件 文件大小不能超过 50M		
管理员密码	请输入管理员密码		

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

溯源插件		
☑ 系统内置 ②	高级溯源 ③	
✓ 网络信息✓ PC信息✓ 虚拟身份信息	☐ 获取身份信息	
	X/XX	

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。



部署蜜罐

OA类 访问控制系统 客户管理系统 开发应用类 数据库 中间件 其他 定制重量	l							
1000000000000000000000000000000000000	OA类	访问控制系统	客户管理系统	开发应用类	数据库	中间件	其他	定制蜜罐
(上上) 智无蜜硼数据,可立即定制				Ø				
智力部績政括。可立即定制					<u>-</u>			
				智无蜜龌数	晤,可立即定制			

图 29. 部署蜜罐-定制蜜罐

首页 / 策略配置 / 蜜罐模板配置		
 请在专业技术人员指导下谨慎修改或添加模板 		
		◎ 浅加速板 删除
	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";



★ 模板类型	- 李確樂語 白宝公樂語 野汁能語	
in mart		
蜜罐LOGO:	上传	
	文件大小不能超过50M,支持文件扩展名:png、svg	
* 夕秒		
10110	Ľ	
* 描述:	:	
* 古際101		
「兄咩URL」	AL: https://www.baidu.com 注音:古路IIpI 需要提服务器网络司法	
2012 1.12	江高小りに座りれた間重幅加大力品で知ら	
7012-1-1-		
	取消添加 添加楔板	

 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。

OA类	访问控制系统	客户管理系统	开发应用类	数据库	中间件	其他	定制蜜罐
日日 1117 111 日定义変展 万境密	2 定制新電線			■■■ 自定义 部署情 IP: 17 甜皮ジ	火電器 電磁 記況 予 客戸端:1↑ 2010		
	fr.	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;



 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、 人口文件名必须为 index.html),信息填写无误后,点击"添加模板";

首页	页 / 策略配置	/ 蜜罐模板配置									
		* 模板类型:	克隆蜜罐	自定义蜜罐	默认蜜罐						
		蜜罐LOGO:	-上 上传								
			文件大小不能起	迢过50M,支持3	文件扩展名:png、	svg					
		*名称:						à			
		* 描述:						li			
		* 代码包:	上 上传文件 注意: 1.支持扩展名。 2.文件大小不能 3.入口文件名成	zip ,请打包资源 指超过500M; 必须为index.htm	原后上传; I。						
							取消添加	添加模板			
							1				
			冬	33. 眢	管罐模板面	置-自定)	义蜜罐				
4)	进入	"蜜罐	管理>	部署蜜	罐"页面	ī,选择	"定制蜜	瓘" 丿	场景中	对应的	蜜

 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。

部署蜜罐

OA类	访问控制系统	客户管理系统	开发应用类	数据库	中间件	其他	定制蜜罐
日定义蜜鼬 克隆蜜	■ 定制新蜜羅			自定义 11.11 自定义 前来特	蜜甜 蜜罐		
				P雪田 IP: 1介	> 客户端: 1个		
				甜度语			

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。

	首页 / 客户端管理		
8 重建管理	客戶端管理		
人 客户端管理			
□ 威胁情报	答户端状态:在线:1 离线:1 关闭:0		如何卸载客户端? 💿 部署客户端
➡ 数据管理	客戶端状态: 全部 ∨		(请输入客户端名称/子网印搜索 搜索
	*		
	● か公区 区 利用版本: 15.31 同士 P 数: 1个	蜜媛部書情况: 1个 建议每个客户端不多于200个蜜媛 ※著蜜媛	審戶編就志: ● 在线
	DMZ区 □ 电升版本: 1.5.28 同性中夏: 1个	#編纂書儀況: 建议場个客户編不多子200个書編 形司言編	客户編状态: ・ 頁述 単新部署 重度 关闭
	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:

 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。

◎ 风险大盘	首页 / 客户端管理		
♂ 蜜貓管理	客户端管理		
A 客户端管理			
I 威胁情报 ~	客户端状态: 在线: 1 离线: 1 关闭: 0		如何卸载客户端?
D 数据管理 >	客户端状态: 全部 V		(请输入客户端名称/子网IP现客)
③ 系統配置 ~	1998		
Q 通知管理	か公区 2 和伊版本: 1.5.31 岡卡 IP 数: 1 个	蜜鍵部署情况: 1个 建议每个客户端不多于200个蜜罐 。 部署蜜罐	 客户膳状态: 在該 重加部署 ・ 更応
	DMZ区 区 相序版本: 1.5.28 所作 P 数: 1个	蜜貓那看情况: 1个 建议每个客户端不多于200个蜜罐 影响素端	春戶編状态: • 高线 重新部署 重启 关闭
		ズノ	
	图 36. 点日	占部署客户端	
	1. C		
	客户端部署流程		×
	-		
	m 1 准备一台独立设备		
	在需要防护的 VLAN 中准备一台符合	配置要求的客户端设备:	
	8 ・ 部署环境支持 CentOS 6. Ubuntu	16.04、Ubuntu 18.04 64位系统。	
		500	
		500.	清泉
	• 网络可以访问服务中心。		
	• 独立设备,请不要在业务系统上部	部署客尸端。	
	2 获取安装客户端的命令行		未
	curl http://		
—————————————————————————————————————	And the second sec	1	尽击 复制
N' Y	①该命令只能安装一个客户端,用户使用品	后命令失效。	
	3 执行命令行		
	复制部署命令,在第一步准备好的客户端设	备中打开命令行终端,以 root 身份登录,	将部署命令粘贴至
	终端内执行后返回此页面。		

图 37. 复制部署客户端命令

 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。



zi [s	ni@yanshi- sudo] zhi	ubuntu-16-04 的密码:	:~\$ sudo	su			· · · · · ·		
ro	ot@yanshi	-UDUNTU-16-04	4:/nome/1	zni# cur	L nttp:/	/		12200	F/B3ch/44
00	15e9f-f2cd % Total	% Received	% Xferd	Averag Dload	e Speed	Time Total	Time Spent	Time Left	Current Speed
10	00 3272	0 3272	0 0	102k	0 -	- : - :	!!	::-	- 106k
Tr	stalling	Beehive!		20211					
>	Downloadi	ng tarball.							
	% Total	% Received	% Xferd	Ауегаа	e Speed	Time	Time	Time	Current
				Dload	Upload	Total	Spent	Left	Speed
10	00 4856k	0 4856k	0 0	3047k	. 0 -	-::	0:00:01	::-	- 3046k
>	Extractin	g to /opt/be	ehive						
Th	nis script	will instal	l in /op	t/beehiv	e				
>	Starting	service							
>	Successfu	lly installe	d! Beehiv	ve is ru	nning no				
го	oot	5439 1	4 14:13	?	00:00:	00 /opt/	beehive/b	eehive	
ГС	oot	5449 5439	2 14:13	?	00:00:	00 /opt/	beehive/b	eehive	
ГС	oot	5490 5362	0 14:13	pts/1	00:00:	00 grep	beehive		
го	oot@yanshi	-ubuntu-16-04	4:/home/:	zhi#					
							x.	Σ^{1}	
			图 38.	部署历	戊功后的	提示			
							- Ya	YY.	
							\sim		
3)	部軍市	伪后 定户	澧州太 -	为"在维	"	1			
5)	아지 타 네니				0		えし		
						X. N	\sim		

○ 风险大盘 ♂ 蜜貓管理		^{首页 / 客户端管理} 客户端管理				
 本 各户時管理 1 成砂(併投 > 数据管理 ◎ 系統記置 Q 通知管理 	• •	 第户編状念: 在法:11萬法:11关邦:0 第户編状念: 主部 > カ公区 ご 単分区 ご 単分区 ご 	星城石泉住在 名: 建成百十五中國名亦于200个東國	1个 部署集編	30何加収客 (清始入客户法名称)子例中提索 (有始 入 客户法名称)子例中提索 (在社)	PM7 O 645PM R5 2557 O 25 xm
		DMZ区 [2] 田序版本: 1.5.28 同学中世: 1个	重要が考核法 : 諸以後今後の他不多于200个復編	1个 印册密辑	客户端状态: • 高线	RREA RE XA
		图 39.	部署成功后客户端状态			

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。 \succ

▶ 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 © 2021 北京知道创宇信息技术股份有限公司 第 22 页 共 40 页



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。)



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 © 2021 北京知道创宇信息技术股份有限公司 第 23 页 共 40 页



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":

首页 / 蜜饵管理							
邮件蜜饵	文件蜜饵						
① 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	罐时将触发警告。				
							+ 添加邮件蜜饵
诱饵邮件名	开始日期	发送日期	发送频率	状态	关联蜜罐ip	创建时间	操作
			图 42.		邮件蜜饵	. All	

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);

ø
ø
ø
ø
Ø
1.

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);

邮件信息	
* 发送频率:	v
* 开始日期:	请选择开始日期
* 发送时间:	请选择时间 ①
* 关联蜜罐IP:	请选择关联篮键IP V
邮件标题:	
*邮件模板:	v
	字间距 · 行高 · 三 常规 · 三 三 K A A, - 三 三 三
	注意: 上述邮件模板内容内 "MGIP" 标识不能删除,系统后台将自动以关联蜜毽IP督换该标识!
	测试发送 提交
	Ell. 7
-	图 44. 邮件蜜饵-邮件信息

- 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"。



) 生成包含诱导进入蜜	灌内容的蜜饵邮件,攻击	者从邮件跳转到蜜笋	輩时将触发警告。				
秀饵邮件名	开始日期	发送日期	发送频率	状态	关联蜜罐ip	创建时间	+ 添加邮件蜜 操作
内网密码过期通知	2021-03-29	18:00	单次		然之OA(1C .55)	2021-03-29 18:22:04	编辑删除
vanght-test	2021-03-26	10:28	单次		然之OA(10 55)	2021-03-26 10:23:09	编辑删除

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";

自贝 / 重時昌桂			
邮件蜜饵 文件蜜饵			
① 生成包含诱导进入蜜罐内容的蜜饵文件,攻击	者从文档跳转到蜜罐时将触发告警。		
			+ 添加文件蜜馆
诱饵文件名	关联蜜罐ip	创建时间	操作
KI	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;



关联蜜罐IP:	请选择关联蜜罐IP	~	
文件模板:	请选择文件模板	~	

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"。

R6日 <i>六 01- タ</i>	光 取樂語(m	命任志奉告十六百	+ 添加文件
- 台管理员登录说明书	杰文 (10 .55)	دی معدد اور می معدد معدد معدد معدد معدد معدد معدد م	11mtF 親儀
2台管理员登录说明书	然之OA(10 55)	2021-03-23 19:46:40	下载 删除
2台管理员登录说明书	然之OA(10 55)	2021-03-23 19:42:34	下载 删除
			< 1 > 10条/
-	图 48.	文件蜜饵列表	

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。



						1 2021/04,	/12 16:00:00 - 2	021/04/19 16:00:00 茴
今日増量 ② 『P IP	79 次	◎ 指纹	32	画像	总量 IP	141654 次	🦲 指纹	13488734 次
3 IP 属性 内网 IP ×	国内 IP ×	~	处置状态 全	部	4	请输入IP/唯一核	识符搜索	Q (5) 노 数据导出
攻击者 🔽		攻击时间	攻击次数	攻击手段 🔽	指纹数据	是否白名单	♡ 操作	
2	已处置	2021/04/12 16:00:00 / 2021/04/19 16:00:00	3000	扫描	PC 数据	是	宣看详情	移出白名单 设为未处置
中国 山东・潍坊 	未处置	2021/04/12 16:00:00 / 2021/04/19 16:00:00	3000	扫描	PC 数据	否	查看详惯	6)加入白名单⑦投为已处置
2 中国 湖南·娄底 fc2c069359	未处置	2021/04/12 16:00:00 / 2021/04/19 16:00:00	3000	扫描	PC 数据	否	 是否确认将 10.0.0 取消 	0.1 移出白名单?
1 未处置 中国 山东·潍坊		2021/04/12 16:00:00 / 2021/04/19 16:00:00	3000	扫描	PC 数据	否	查看详情	加入自希单 设为已处置

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。

ID. ■ 5	非白名单 记 未处置 记	文件下载 (名) 画像下载
攻击总次数: 132 次	开始攻击时间: 2021-09-17 15:03:01 最新攻击时间: 2021-09-17 15:32:54	
攻击蜜罐 然之OA(2) 132次		
X/V	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。

#获攻击日志统;;	t		捕获攻击日志类型TOP 5		捕获攻击日志趋势				
#获攻击日志总数	2587 😤		URL访问	1907	1200		~		
			端口扫描	362	900		0		
高危	6条	1%	IP探测	214	600				
中危	68条	2%	Shell命令执行	56	300	0			自定义列
低危	2513景	97%	-	30	0 — 0		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	6	
					2021-09-11 08:00:0	0 2021	-09-14 08:00:00 2021-09-17 0	::00::00	
日志列表								导出,	
		[0.00] -							
标登: 王部	✓ 范隘等级:	王即 / 月	双击阶段: 按双击者四子	·域名/目标IP/蜜罐名称/客/	『端名称提案				投業 高級
Ŗ	文击时间	攻击者	宮 >>> 受攻击IP/域名 (蜜罐)	威胁标签	危险等级	攻击阶段	攻击详情	处置建议	操作
202	21-09-17 5:28:03	10.8.15.14 >	>> 10.8.246.57 (80)(然之OA(2))	URL访问	低意	侦查跟踪	访问 URL(GET):http://10.8.246.5 7/sys/index.php?m=mi	根据URL访问攻	下载PCAP (2.1 KB)
展开 202 1!	21-09-17 5:28:01	10.8.15.115	>>> 10.8.246.57 (80) (然之OA(2))	URL访问	低意	侦查跟踪	访问 URL(GET):http://10.8.246.5 7/doc/index.php?m=do	根据URL访问攻	下载PCAP (213.0 KB) 下载文件
1 - 2 2 3 4 5 6 7 - 8 9 10 11 12 13 14 14	<pre>{ "connId": "Ifdfe97eb "connId": "Ifdfe97eb "ctackerPort": 550 "ctackerPort": 550 "ctackerPort": 550 "ctackerPort": ["conned": "10.8.4 "conned": "10.8.4 "ctacgetPort": ["ctacgetPort": ["ctacgetPort": ["ctacgetPort": ["ctacgetPort": "LtargetPort": ["ctacgetPort": "LtargetPort": ["ctacgetPort: "LtargetPort": "LtargetPort": "LtargetPort": ["ctacgetPort: "LtargetPort: "LtargetPort": ["ctacgetPort: "LtargetPort: "LtargetPort": ["ctacgetPort: "LtargetPort: "LtargetPort:</pre>	3000bf", 15.115", 7, 2:03.72:41:82", 5.57", 56:a3:aa:b9", 5681898, /index.php?m=doct /index.php?m=doct /index.php?m=doct	M-view6docID-11*, 5-view6docID-11 HTTP/.1.1\manufact: 10	.8.246.57 \r\n Accept: t pt-Longuage: zh-CN,zh;	ext/html,application q=0.3\r\mconnection:	ı∕xhtml+xml,app keep-alive\r)lication∕xml;q=0.9,imoge/avif,i n£cokie: rid⇔6igtängtepfdaaprm	mage/webp,image/apng, hbbouZ&1; long∞zh-cn;	*/*;q=0.8,applicati themme=default; io

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。



捕获攻击日	18歳() 5月28日 (1997) 1997 (1997		捕获攻击日志类型TOP 5 端□扫描 	36380	捕获攻击日志趋势 20000 15000			p	~
高危	253条	1%	SQL注入	214	10000			/	
■ 中危	139条	1%	, MySQL攻击	70	5000			5	
■ 低危	42648祭	99%	旧理論制	56	0 2021-12-02 08:0	00:00 20	21-12-04 08:00:00 2021-12-0	6 08:00:00 2021-	12-08 08:00:00
攻击日志列	表 共1000条数据							1 过滤扫描攻击	日志 ③ 上数据导出 ◎
(按攻击者)	P/子域名/目标IP/蜜罐名称/客户蜡	名称搜索							搜索 高级搜索
选择字段									
	攻击时间	攻击者	>>>> 受攻击iP/域名 (蜜罐)	威胁标签	危险等级	攻击阶段	攻击详情	处置建议	操作 🛛 😨
+	2021-12-09 11:08:12	10., 13 >	>>> we' '0) (Struts2)	URL访问	112 A	侦查跟踪	访问 URL(GET):httr p/f	根据URL访问攻	下载PCAP (144.45 KB)
+	2021-12-09 11:08:12	10. 13 >	>>> web. (80) (Struts2)	URL访问	12.12	侦查跟踪	访问 URL(GET):http://////////////////////////////////	根据URL访问攻	<mark>下戱PCAP</mark> (144.45 KB)
+	2021-12-09 11:08:11	1C 113 >	>> wet op (80) (Struts2)	URL访问	(#1/8	侦查跟踪	访问 URL(GET):h p/in	根据URL访问攻	下载PCAP (100.54 KB)
	2021-12-09		11	s over debuts	(at as	JA vision ov	访问	an an an an an an	下载PCAP (62.39
			图 52. 攻击	日志-一	键过滤打	日描攻	击日志	KL.	

● 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。



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。



创宇蜜罐-威胁诱捕与溯源系统 SaaS 版用户手册

							2021-1	2-02 11:46:46 ~ 2021-12	-09 11:46:46	C
捕获攻击日	1志统计 ≈□=== 43028 ≈		捕获攻击日志类型TOP 5 端口扫描	36380	捕获攻击日志趋势 20000					
385.50 0 0	9682 - 10020 m		URL访问	6197	15000				٩	
■ 高危	253条	1%	SQL注入	214	10000					
 中危 低危 	139条 42636条	1%	MySQL攻击	70	5000					
110762			IP探測	58	0 2021-12-02 08:0	0:00 20	21-12-04 08:00:00 2021-12-0	6 08:00:00 2021-12-	8 08:00:00	b
攻击日志列 按攻击者IP	表 共1000条数据 //子域名/目标IP/蜜罐名称/答F	- 端名称搜索						过滤扫描攻击日;	5 ② 上数据 搜索	時出 Ø 高级搜索
威胁标签=单 攻击阶段	▲□扫描,P探測,扫描 ● ×	目标端□=80 ● ×	: 174 bû							
	攻击时间	攻击者	>>>> 受攻击IP/域名 (蜜罐)	威胁标签	危险等级	攻击阶段	攻击详情	处置建议	操作	Ψ
٠	2021-12-09 11:28:44	10 100 >	>> 106.211 (OpenNMS)	IP探测	低危	侦查跟踪	发起异常 PING 请求,可能试图 获取主机存活信息	根据攻击日志的频		
+	2021-12-09 11:28:44	10 100 >	>> 10 3.211 (OpenNMS)	IP探测	铣虎	侦查跟踪	发起异常 PING 请求,可能试图 获取主机存活信息	根据攻击日志的频		
*	2021-12-08 18:03:16	10.1 6.18 >>	>103 (51762)(然之OA)	端口扫描	低危	侦查跟踪	蜜罐受到扫描攻击(TCP),可 能正在被收集信息或者拒绝服 务攻击。	根据扫描攻击日志		

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。

					2021-12	2-02 11:14:46 ~ 2021-	12-09 11:14:46 🗎 C
宣询语句	说明				示例		×
а	任意字段的值可能是a	http 🖸					
a:b	a字段的值可能是b	catego	ry:"http" 🛛				
a AND b 或者 ab	同时包含a和b的日志	catego	ry:"smtp" AND	attackerIp:"	0.8.15.100" 🕽		
a OR b	包含a或者包含b的日志	catego	ry:"smtp" "ssh	n" 🚺 或者 categ	ory:"smtp" OR "ssh" 🕽		
a NOT b	包含a但是不包含b的日志	catego	ry:"smtp" NOT	attackerIp:"	0.8.15.100"		
攻击日志列表 共1000条数据 请输入查询的语句,例如: status:200 A	ND method: GET					过滤扫描攻击 搜索	日志 ③ 上数据导出 ◎ 语法帮助 简单搜索
攻击时间	攻击者 >>> 受攻击ⅠP/域名 (蜜繡)	威胁标签	危险等级	攻击阶段	攻击详情	处置建议	操作 亚
+ 2021-12-09 11:08:12	10 13 >>> we top (80) (Struts2)	URL访问	任危	侦查跟踪	访问 URL(GET):http p/fa	根据URL访问攻	下载PCAP (144.45 KB)

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
 © 2021 北京知道创宇信息技术股份有限公司
 第 32 页 共 40 页



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。

抓获安	全事件统计			捕获安全事件 外网端口扫描	类型TOP 5	134	捕获安全事件趋势 200			
捕获安排	全事件总数 287 条			小岡山田 探測		110	150		م	
高合		8	11%	rbill Shall dod:	207		100			
= 中危	254	*	88%	P Styl Street ap 63		-	100			م
• 低危	t 01			内例 Windows ;	5样登录成功	7	50 O-			
				外网 SMTP 頻繁	操作	1	0 2021-03-27 1	6:00:00 2021-03-28	04:00:00 2021-03-28 16:00:00 2021-03-25	9 04:00:00 2021-03-29 16:00:00
安全事件列	则表									
事件类型	外网URL探测 V	危险等级	全部	∨ 攻击阶段	全部 🗸	按攻击者IP/受攻击IP/蜜罐名	称/客户端名称搜索		م	、 更新頻率: 10分钟 / 搜
	起止时间		攻討	击源IP	受攻击IP	蜜罐 事件类型	危险等级	攻击阶段	攻击详情 女	上置建议 威胁标
-	2021-03-29 17:48:04 / 2021-03-29 17:48:05		10	.104 10	0.155	JSHERP 外网URL 採測	中危	侦查跟踪	蜜罐接收到http访 根据L	JRL访问攻 URL访
	攻击时间	攻击	源IP	受攻击IP	蜜罐	威胁标签	危险等级	攻击阶段	攻击详情	Pcap包
	2021-03-29 17:48:05	10.	.104	10.).155	JSHERP	URL访问	低危	侦查跟踪	蜜鑼接收到http访	下载 (1.01 KB)
	2021-03-29 17:48:05	10.	.104	10 155	JSHERP	URL访问	低危	侦查跟踪	蜜鑼接收到http访	下载 (1.01 KB)
	2021-03-29 17:48:04	1Q	1 5.104	10. J.155	JSHERP	URL访问	低危	侦查跟踪	蜜鑼接收到http访	下载 (1.00 KB)
							X	-//		
					KVI1	图 56. 安	全事件			

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。

 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;

行为分析报告	导出报告	×			
	*报告名称: 行为分析报告_1608018108362 归				
共计报告数量 14 个	* 数据区间: 2020-12-15 00:00:0(~2020-12-15 23:59:5ξ 📋			⊕ 新建报告	
报告名称	报: * 客户端范围: tester001(10.8.246.221) ×		导出时间 💠	导出状态	操作
行为分析报告_1	12	est002	12/11 14:40:45	③成功	
行为分析报告_1	取消 報 12/10 00:00:00-12/10 23:59:59 yxq tester001 testo0	11	12/10 15:00:12	⑧成功	
行为分析报告_1	12/09 00:00:00-12/09 23:59:59 yxq test0011 test00	0	12/09 17:38:01	④成功	
〇 行为分析报告_1	12/07 00:00:00-12/07 23:59:59 test001		12/07 23:45:25	③成功	
 行为分析报告_1 行为分析报告_1 行为分析报告_1 	12/10 00:00:00-12/10 23:59:59 yxq tester001 test00 12/09 00:00:00-12/09 23:59:59 yxq test0011 test00 12/07 00:00:00-12/07 23:59:59 test001	8	12/10 15:00:12 12/09 17:38:01 12/07 23:45:25	 ◎ 成功 ◎ 成功 	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。

报告名称	报告日期	客户端范围	导出时间 👙	导出状态	操作
行为分析报告_1	12/11 00:00:00-12/11 23:59:59	yxq tester001 test002 test002 test0011	12/11 14:40:45	②成功	🖬 🗾 🗍
行为分析报告_1	12/10 00:00:00-12/10 23:59:59	yxq tester001 test0011	12/10 15:00:12	⊗成功	🔂 🔁 🖸
行为分析报告_1	12/09 00:00:00-12/09 23:59:59	yxq test0011 test003	12/09 17:38:01	◎ 成功	🖬 🗖 🖸

9.2. 日志数据下载

首页/数据管理/行为分析报告 行为分析报告

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;

前往日志页面生成数据报告	下载报告 删 除
旦山山本大	+= <i>//</i> -



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;

俞入查询的语句,	例如: status:200 AND met	hod: GET Q	自定义下载
威胁标签	危险等级 ⑦ 🛛 👻	处置建议	攻击详情
	图 60.	日志下载按钮	A Br
日志数据下载			X
	报告名称:		
	* 数据类型: 💿 攻击源၊	p 🔵 pcap包 🔵 log文件	
			取消 确定
	图 61	下载类型设置	

 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。

共计报告数量	7个					前往日志页面生成数据报告	下载报告
	报告名称	数据类型	Ψ	文件大小 ≑	导出时间 ≑	导出状态	操作
	log文件_16	log文件		98.3KB	12/10 15:10:27	◎成功	1 Ū
	log文件_16	log文件		194.1KB	12/10 15:05:39	②成功	1 Ū
	pcap包_16	pcap包		5.8MB	12/10 15:05:28	②成功	1 Ū
	攻击源ip_16	攻击源ip		14.2KB	12/10 15:05:16	②成功	1
	log文件_16	log文件		181.9KB	12/07 23:31:19	②成功	1
	pcap包_16	pcap包		4.4MB	12/07 23:31:13	②成功	1 D
	攻击源ip_16	攻击源ip		14.2KB	12/07 23:31:05	②成功	10

图 62. 日志数据列表

XX



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。

该功能可以配置syslog用	务器地址,系统将实时威胁日志内容	l以json格式推送至syslog服务器,	5持多个syslog服务器推送。	
* syslog服务器地址:	tcp://~ ip + 培加syslog舰 测试发送 超交	: 514 务器		
	I	图 63. SYSL	OG 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。

首页 / 策略配置 /	白名单配置		
白名单配置			
启用后, 白名单	P/MAC 产生的威胁告警	日志将不计入威胁态势	的统计。
计入办主日本:			
计入攻击日志:		-	



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。

首页 / 策略配置 / 白名单配置				
白名单配置	添加白名单		×	
	÷ 10			
	AIP:			
后用后,日名单 IPJMAC 产生的威胁				
IP/MAC				启用
		り以棚八少 口石半 IP,一11項与一 。		
	批量备注:			
			取消 确定	

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。





- 五 / 华欧和帝 / 古夕英 和 帝				
名单配置	添加白名单		X	
	* MAC :			
启用后,白名单 IP/MAC 产生的威服				
IP/MAC				启用
		可以输入多个白名单 MAC 地址,一行填写一	8	
		个。		
	批量备注:			
			取消 确定	
		2	K	
	图 66	添加白夕单 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。

X

音页 白 :	王/策略配置/白名单配置 名单配置					
	启用后,白名单 IP/MAC 产生的威胁	协告警日志将不计入威胁态势统计	t.			
	IP/MAC	备注			启用	 是否要删除这条数据? 取消 服消
	10.0.0.1	11 🗷				删除
						< 1 > 10条/页>
			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。

威胁告警	未读1 全部	全部标记为已读
系统通知	(面) 捕获到1个攻击源事件,攻击源IP为: 10.0.1.4, 请尽快核实处理。	3天 查看 □ 更多 ∨
		< 1 > 10 条/页 >
	图 (0 异时件 游	

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。

0	"FlaredeMacBook-Air.local"CPU持续高负载超过80%,请及时对异常服务进行处理。	2 小时	查看 更多 ∨
0	"FlaredeMacBook-Airlocal"内存使用率超过80%。请非善是否有进程异常或优化服务配置。	4 /小망	查看 更多 >
0	"FlaredeMacBook-Airlocal"CPU持续高负载超过80%,请及时对异常服务进行处理。	20 小时	査者 更多 ∨
0	"FlaredeMacBook-Air.local"CPU持续高负载超过80%,请及时对异常服务进行处理。	1天	查看 ● 更多 ∨
0	"FlaredeMacBook-Air.local"CPU持续高负载超过80%,请及时对异常服务进行处理。	1天	查看 更多 >

可对未读消息标记为已读,也可对已读消息标记为未读。

© 2021 北京知道创宇信息技术股份有限公司