CAICT 中国信通院

国内威胁诱捕（蜜罐）类产品研究与测试报告

——先进网络安全能力验证评估系列报告

（2021 年）

中国信息通信研究院安全研究所

2021 年 12 月

版权声明

编制说明

本报告由中国信息通信研究院安全研究所（以下简称“信通院安全所”）撰写，限于撰写时间、知识局限等因素，内容恐有疏漏，烦请各位读者不吝指正。报告中的威胁诱捕（蜜罐）类产品的测试报名时间为2021年01月05日至2021年02月04日，共有38家企业报名，其中34家企业顺利完成测试。感谢以下参与测试的企业（排名不分先后）：

北京神州绿盟科技有限公司、广州非凡信息安全技术有限公司、烽台科技（北京）有限公司、杭州安恒信息技术股份有限公司、杭州默安科技有限公司、杭州智航云安全技术有限公司、北京长亭科技有限公司、上海观安信息技术股份有限公司、北京吉沃科技有限公司、北京智仁智信安全技术有限公司、广州锦行网络科技有限公司、北京四海图宇科技有限公司、北京天融信网络安全技术有限公司、北京元支点信息安全技术有限公司、北京安天网络安全技术有限公司、山东云天安全技术有限公司、北京鸿腾智能科技有限公司、北京安域领创科技有限公司、北京永信至诚科技股份有限公司、江苏天翼安全技术有限公司、腾讯云计算（北京）有限公司、北京经纬信安科技有限公司、杭州天谷信息科技有限公司、上海沪景信息科技有限公司、北京知道创宇信息技术股份有限公司、紫金山实验室、北京网御星云信息技术有限公司、网神信息技术（北京）股份有限公司、北京启明星辰信息安全技术有限公司、恒安嘉新（北京）科技有限公司、中国科学院信息工程研究所、江苏君立华域信息安

全技术股份有限公司、北京微步在线科技有限公司、上海斗象信息科技有限公司。

同时特别致谢 FreeBuf 咨询对本报告提供的相关支持工作。

前　言

威胁诱捕技术是一种基于应用蜜罐、虚拟系统、虚拟网络等多种方式且具有主动、积极、欺骗性质的网络安全检测技术。随着网络安全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。在这一背景下，威胁诱捕类产品（蜜罐）的应用得到广泛关注。

为了落实工信部关于网络安全产业高质量发展政策要求，培育公平竞争的市场环境，开展网络安全产品服务能力评价、网络安全工程建设与系统运行维护质量评价和面向新技术新业务的安全评估，同时更好地满足电信和互联网、金融、能源和医疗等行业用户在 5G 网络、云计算、物联网等新型业务场景下的实际需要，为其在网络安全产品能力选型中提供技术参考，信通院安全所策划撰写此次《国内威胁诱捕（蜜罐）类产品研究与测试报告（2021）》。

报告中产业市场应用现状内容通过现场走访、资料整合及问卷调查的形式，对国内外近百家企业的使用情况进行对比分析，深入总结国内威胁诱捕（蜜罐）类产品的基本现状，并尝试对其发展趋势进行评估和预测。报告同时对国内主流威胁诱捕（蜜罐）类产品进行基本面测试评估，并输出测试、分析结果与整体报告。

报告中的测试部分主要针对当前行业内主流企业的产品，内容和角度覆盖全面且广泛，包括产品功能、性能以及自身安全，包含十余种技术能力指标测试项。本次测试是作为蜜罐类产品类的“能

力拔高测试”，以体现相关产品在某一个功能领域的真实技术实力，并非是符合性或合规性测试，也不是作为某项采购入围的强制要求。

目 录

图 目 录

表 目 录

一、威胁诱捕（蜜罐）技术演变及发展历程

随着网络攻击对抗升级，传统的单向边界防御技术愈发不能满足企业应对高级未知威胁的需求，蜜罐技术的出现及成熟改变了这一被动防御的局面。

蜜罐（Honeypot Technology）是一种通过工具诱骗攻击者，令安全人员得以观察攻击者行为的主动网络防御技术，其应对的不是攻击或漏洞，而是关注攻击者本身。该项技术通过欺骗诱捕打乱攻击节奏，增加攻击复杂度，给企业增加更多响应时间，并有可能对攻击者进行分析溯源从而预防攻击。

从 2015 年起，Gartner 连续四年将攻击欺骗列为最具有潜力的安全技术。主要原因包括：**一是**该技术是通过欺骗或者诱骗的手段来挫败或者阻止攻击者的认知过程；**二是**可自动化部署在企业防火墙后，利用攻击欺骗检测出已经入侵到内网的攻击者；**三是**在端点、网络、应用、数据等不同的层面用不同的方法实现对应的攻击欺骗，从而对攻击者进行诱捕。

目前，蜜罐技术作为常见的威胁检测及欺骗防御手段，已经在国内外得到较为广泛的应用。

（一）蜜罐技术发展历程

蜜罐从概念到落地从 1998 年开始。该技术发展初期主要是通过虚拟的操作系统和网络服务，对入侵者实施欺骗。初期蜜罐技术根据针对攻击的回应方式可以分为回应式和黑洞式，前者对攻击者的所有探测和攻击行为都予以满足和应答，后者则是完全不予应答，

如同“黑洞”一样吞食所有的攻击行为。

现阶段，由于企业网络逐渐呈现架构高复杂化、安全报警信息海量化的特点，给欺骗防御技术即蜜罐技术在模拟对象类型、仿真精细度、自动化程度等方面提出了更高的要求。厂商和安全研究人员不断对蜜罐技术进行优化，从而逐渐形成新型蜜罐、蜜网、分布式蜜罐、分布式蜜网乃至蜜场等多种落地形态。

蜜罐的发展期可大致划分为 5 个阶段：

表 1 蜜罐技术发展期

概念期	发展初期	完善期	市场应用期	创新发展期
新型防御思路	蜜罐产品 DTK 发布	Spitzner 提出蜜网技术；分布式概念被引入蜜罐技术的发展	扩展并应用至工业控制系统等多个领域	基于新型攻击方式和威胁形势，结合新兴技术创新蜜罐技术
1989-1997 年	1998 年	1999-2003 年	2004-2020 年	2020 年-今

来源：FreeBuf 咨询

从蜜罐技术部署层面看，蜜罐的模拟能力已经从终端系统模拟发展到应用层模拟，具备了更高的交付能力；产品部署形态则从实体机部署变成了实体加虚拟部署两种形态，部署形式则以探针导向和流量牵引为主。

（二）蜜罐关键技术演变

完整的蜜罐涵盖 3 个核心技术点，即网络欺骗（诱捕环境构建）、监控记录（监控入侵行为）、处置措施（将监控获取的数据进行提取、分析从而实现追踪溯源等目的）。

其中，网络欺骗是蜜罐技术体系中的核心技术，将原本假的、

非真实的、没有价值的信息伪装成看似真实、有价值的信息，从而达到欺骗攻击者的核心目的。

在《A Note on the Role of Deception in Information Protection》[1]中，Cohen 对欺骗的特点做了如下总结：**一是**欺骗增加了攻击者工作量，因为他们无法轻易预测哪些攻击行为会成功，哪些会失败；**二是**欺骗允许防御者追踪攻击者的种种入侵尝试并在攻击者找到防御者的真实漏洞之前进行响应；**三是**欺骗消耗攻击者资源；**四是**欺骗对攻击者的技能水平提出了更高要求；**五是**欺骗增加了攻击者的不确定性。

由于蜜罐是通过欺骗将攻击者引入诱捕环境从而实现主动防御，因此我们可以根据欺骗的实施时间，将网络欺骗技术分为攻击前欺骗和攻击时欺骗。

攻击前欺骗主要通过仿真环境的构建来实现。传统的蜜罐一般提供单维的仿真，仿真对象包括特定的主机、服务、应用环境，其中环境仿真技术主要包括软件仿真技术、容器仿真技术、虚拟机仿真技术等：

1. 软件仿真：可仿真应用软件，但交互能力相对较低；

2. 容器仿真：可仿真应用软件、系统软件，具备高交互能力；

3. 虚拟机仿真：可仿真应用软件、系统软件及设备，具备高交互能力。

蜜罐本身基于仿真技术，但为了实现欺骗诱捕需要结合更多对

1 Cohen F . A note on the role of deception in information protection[J]. Computers & Security, 1998, 17(98):483-506. IN K M, et al. An experimental evaluation to determine if port scans are precursors to an attack[C]//2005 International Conference on Dependable Systems and Networks (DSN'05). 2005:

于业务的理解和威胁的认知，所以现阶段的蜜罐更多是提供多维仿真，即在仿真技术的基础下，通过结合真实网络环境和企业业务环境，定制环境仿真配置及相关数据，如通过端口重定向在蜜罐中模拟出一个非工作服务，在与提供真实服务主机相同类型和配置的主机上绑定虚拟服务，从而增强“真实性”，实现更高欺骗性。

当诱捕环境构建完成，攻击者进入仿真环境，为了确认系统的真实性往往会对网络流量进行查探，因此在攻击时欺骗阶段，需要配合流量仿真技术、网络动态配置技术、重定向技术依次实现构造仿真流量、模拟正常的网络行为、使得网络状态随时间改变以及检测到恶意数据流时进行重定向（避免影响正常业务）。综合多种欺骗技术手段的蜜罐可以达到欺骗效果增强，最终诱敌深入的目的。

随着攻防对抗升级，蜜罐技术也在不断发展，将为主动防御体系带来更多的应用价值，比如：

1. 通过更细粒度的业务环境模拟，将模拟从终端发展到应用层、文件层；

2. 结合 Al 等新技术进行攻击者行为分析；

3. 出现拟态特征构建和动态演化技术，提升新型蜜罐的自适应能力。

二、威胁诱捕（蜜罐）产品发展现状

（一）蜜罐技术分类

蜜罐技术发展到现在，已出现多种成熟的蜜罐工具。一套成熟的蜜罐系统通常由核心模块和辅助模块两部分组成：核心功能模块

是诱骗与监测攻击方的必需组件，具备构建仿真环境、捕获攻击数据以及威胁分析等功能；辅助模块是蜜罐系统扩展需求，包含系统安全风险控制、配置与管理、反蜜罐侦查等功能。

通常，蜜罐可以按照部署方式、设计标准两种方式分类。

1.按照部署方式分类

按照部署方式，蜜罐可分为产品型和研究型两类。

产品型蜜罐的目的在于为一个企业的网络提供安全保护，包括检测攻击、防止攻击造成破坏及帮助管理员对攻击做出及时正确的响应等功能。一般产品型蜜罐较容易部署，且不需要管理员投入大量的工作。较具代表性的产品型蜜罐包括 DTK、honeyd 等开源工具和 KFSensor、ManTraq 等一系列的商业产品。

研究型蜜罐则是专门用于对黑客攻击的捕获和分析，通过部署研究型蜜罐，对黑客攻击进行追踪和分析，能够捕获黑客的攻击记录，了解到黑客所使用的攻击工具及攻击方法，甚至能够监听到黑客之间的交谈，从而掌握他们的心理状态等信息。研究型蜜罐需要研究人员投入大量的时间和精力进行攻击监视和分析工作。

表 2 产品型蜜罐和研究型蜜罐的优缺点对比

	产品型蜜罐	研究型蜜罐
优点	易部署、易于使用	收集更多有价值信息
缺点	收集信息能力有限	维护及使用较复杂
目的	为企业或组织提供安全防护	收集黑客攻击信息并进行分析

来源：FreeBuf 咨询

2.按照设计标准分类

蜜罐还可按照交互度的等级划分为低交互蜜罐、中交互度蜜罐和高交互蜜罐。交互度反映了黑客在蜜罐上进行攻击活动的自由度。

低交互蜜罐一般仅仅模拟操作系统和网络服务，较容易部署且风险较小，但黑客在低交互蜜罐中能够进行的攻击行为有限，因此通过低交互蜜罐能够收集的信息也比较有限。同时由于低交互蜜罐是虚拟蜜罐，或多或少存在着一些容易被黑客所识别的指纹信息。因此，产品型蜜罐一般属于低交互蜜罐。

中交互蜜罐提供了更多的交互信息，但还是没有提供一个真实的操作系统。通过这种较高程度的交互，更复杂一些的攻击手段就可以被记录和分析。中交互蜜罐是对真正的操作系统各种行为的模拟，在这个模拟行为的系统中，用户可以进行各种随心所欲的配置，让蜜罐看起来和一个真正的操作系统没有区别。

高交互蜜罐则完全提供真实的操作系统和网络服务，没有任何的模拟。从黑客角度上看，高交互蜜罐与真实环境完全无差别，因此在高交互蜜罐中，能够获得许多黑客攻击的信息。但高交互蜜罐在提升黑客活动自由度的同时，又加大了部署和维护的复杂度并扩大了风险。所以高交互蜜罐一般都属于研究型蜜罐，近些年厂商提供的蜜罐产品或方案都倾向于此，最大程度地扭转攻防不对等的局面。

表 3 不同交互度蜜罐对比

	低交互蜜罐	中交互蜜罐	高交互蜜罐
功能	仅模拟简单的操作系统和服务	模拟较为复杂的系统服务	模拟真实的系统环境，为攻击者提供不受限的访问权限
捕获信息量	少	一般	丰富
部署难易度	简单	中等	复杂
攻击者识别度	易	一般	困难
安全风险	低	较低	较高

来源：FreeBuf 咨询

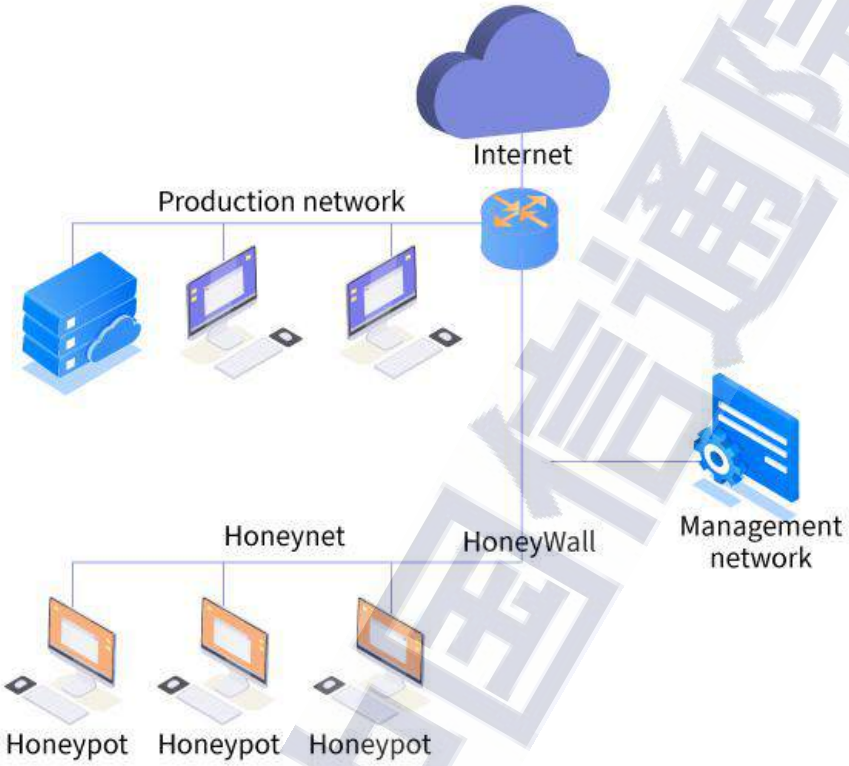
（二）蜜罐技术部署形态

在蜜罐工具软件与关键机制随着安全威胁变化而不断得到发展的同时，如何有效地将不同类型蜜罐技术在公共互联网或大规模业务网络中进行部署，以扩大安全威胁的监测范围并提升监测能力，成为了蜜罐技术研究的一个重要关注点。世界蜜网项目组织（The Honeynet Project）是信息安全领域一个著名的全球性非盈利研究联盟机构，1999 年由著名信息安全专家 Lance Spitzner 发起创建，并在蜜罐基础上提出蜜网（Honeynet）、蜜场（Honeyfarm）和蜜标（Honeytoken）的概念，用以描述不同目标环境下的蜜罐部署形态。

1. 蜜网

蜜网是在蜜罐技术上逐步发展起来的一个新的概念，有时也称作“诱捕网络”。当多个蜜罐被网络连接在一起，组成一个大型虚假业务系统，利用其中一部分主机吸引攻击者入侵，通过监测入侵过

程，一方面收集攻击者的攻击行为，另一方面可以更新相应的安全防护策略时，这种由多个蜜罐组成的模拟网络就称为蜜网。



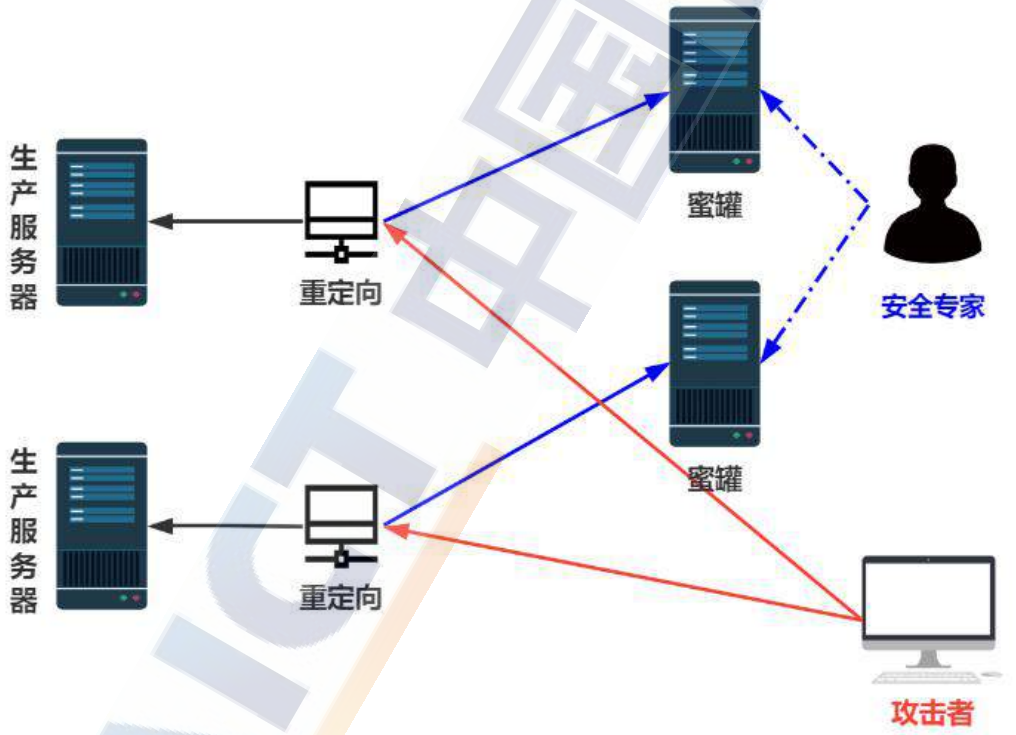
来源：FreeBuf 咨询

图 1 蜜网基本体系结构图

蜜网主要是一种研究型的高交互蜜罐技术。由于蜜网涉及到多个蜜罐之间的网络体系架构设计，同时为了提高高交互性，又会存在一些真实的业务逻辑，因此，蜜网的设计相对蜜罐来说要复杂得多。蜜网设计有着三大核心需求：**即网络控制、行为捕获和行为分析。**通过网络控制能够确保攻击者不能利用蜜网危害正常业务系统的安全；行为捕获技术能够检测并审计攻击者的所有行为数据；而行为分析技术则帮助安全研究人员从捕获的数据中分析出攻击方的具体活动。

2. 蜜场

蜜场是通过代理方式扩展诱饵节点部署范围的蜜罐系统形态。在蜜场中，便于实现对实物设备的管理维护和数据集中分析，诱饵环境和监控模块往往被集中在一个固定的节点或网络中，而轻量级的代理部署在任意网络节点中，将网络攻击重定向至诱饵环境，从而减少真实诱饵节点部署数量，降低系统实现成本和运维难度。蜜场需要对代理节点处的网络流量进行判别和转发，同时兼顾通信的时效性，排除多个代理间的数据干扰。



来源：中国信息通信研究院

图 2 蜜场技术概念图示

如图 2 所示，在蜜场体系架构中，蜜罐系统都被集中部署于一个受控的欺骗网络环境中，由安全专家来负责维护、管理与威胁数

据分析。而在业务网络中仅仅部署一些轻量级的重定向器，将不明身份访问者的网络流量或者通过入侵防御系统等设备检测出的已知网络攻击会话，重定向迁移至蜜场环境中，由蜜罐系统与攻击源进行交互，在具有伪装性的欺骗环境中更加深入地分析这些安全威胁。

3. 蜜标

蜜标是一种特殊的蜜罐诱饵，它不是任何的主机节点，而是一种带标记的数字实体。它被定义为不用于常规生产目的的任何存储资源，例如文本文件，电子邮件消息或数据库记录。蜜标必须是特有的，能够很容易与其他资源进行区分，以避免误报。

来源：中国信息通信研究院

图 3 蜜标部署原理

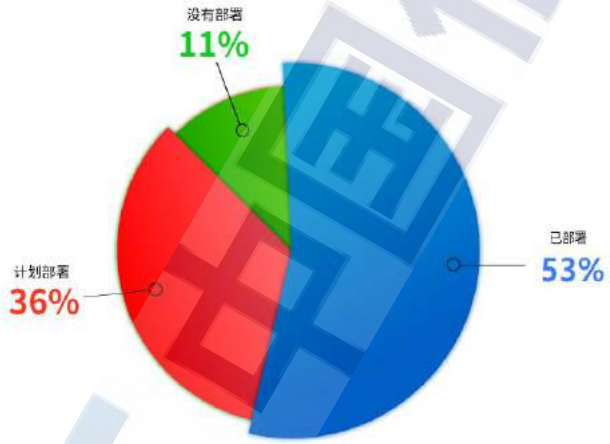
蜜标具有极高的灵活性，可以在攻击过程的任意环节中作为诱饵或探针，利用虚假的账户或内容进行逐步诱导，并识别细粒度的攻击操作（如文件读取、传递和扩散等）。蜜标与蜜罐的主要区别在

于可以轻量级地独立使用，也可以以探针的形式与蜜罐搭配部署。目前由于对蜜标缺乏有效的监视和控制手段，搭配部署形式更为常见，即作为其他蜜罐形态中诱饵内容的补充，辅助捕获特定的攻击行为。

三、国内威胁诱捕（蜜罐）产品市场应用现状

（一）威胁诱捕（蜜罐）产品国内部署现状

1. 企业选择部署威胁诱捕（蜜罐）产品情况



来源：FreeBuf 咨询根据调研数据整理

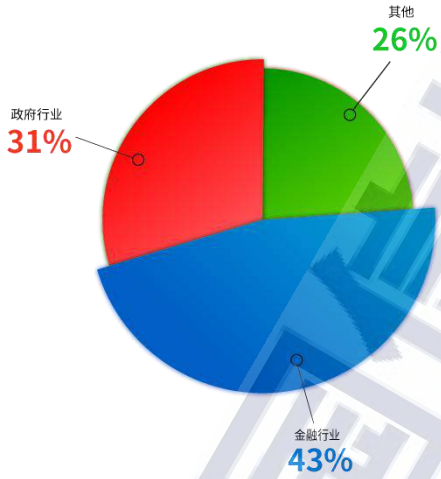
图 4 企业是否选择部署威胁诱捕（蜜罐）产品

从调研结果来看，针对威胁诱捕（蜜罐）产品的选择，有 53%的企业已经部署，还有 36%的企业计划部署。

2. 已部署蜜罐产品的行业分布

根据调研数据，已部署威胁诱捕（蜜罐）产品的企业中，74%为金融和政府行业。事实上，近年来为保障国家重大活动网络安全、

促进和推动国家关键信息基础设施安全防护工作，欺骗防御技术已成为蓝军对抗的利器之一，企业对于威胁诱捕（蜜罐）产品的应用需求也在不断提升。

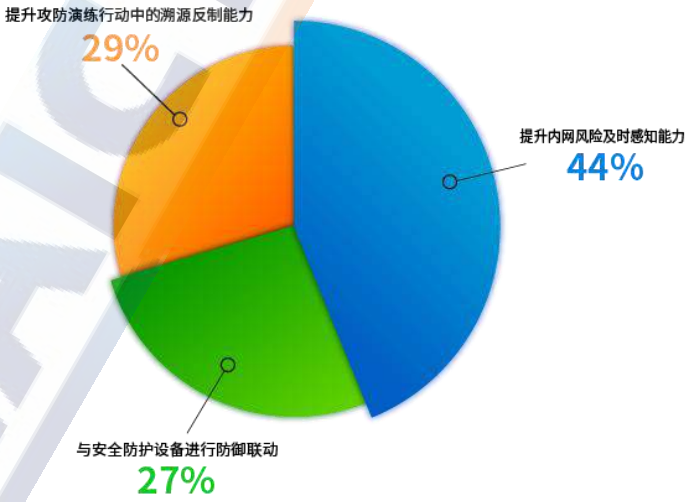


来源：FreeBuf 咨询根据调研数据整理

图 5 已部署威胁诱捕（蜜罐）产品的行业分布

（二）威胁诱捕（蜜罐）产品能力应用现状

1. 企业部署威胁诱捕（蜜罐）产品的主要目的

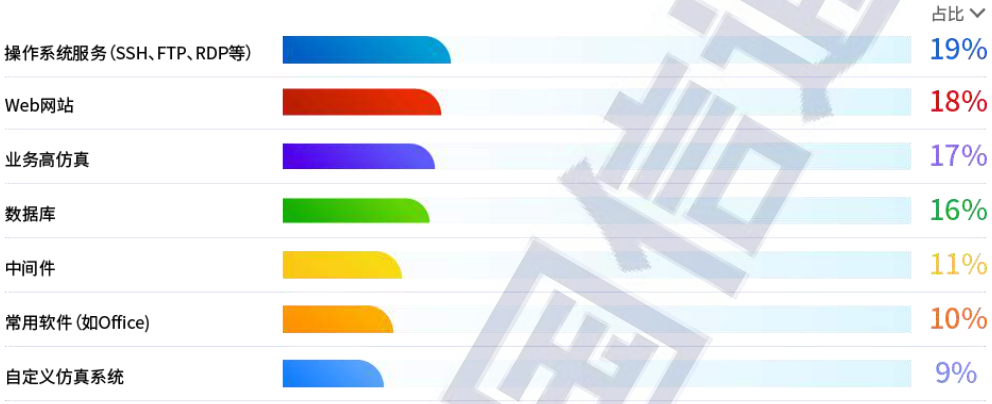


来源：FreeBuf 咨询根据调研数据整理

图 6 企业部署蜜罐产品的主要目的

根据调研结果，44%的企业需要蜜罐产品“提升内网风险及时感知能力”，此外，“提升攻防演练行动中的溯源反制能力”和“与安全防护设备进行防御联动”也是大部分企业部署产品的主要诉求。

2. 企业希望涵盖哪些业务类型的威胁诱捕（蜜罐）产品

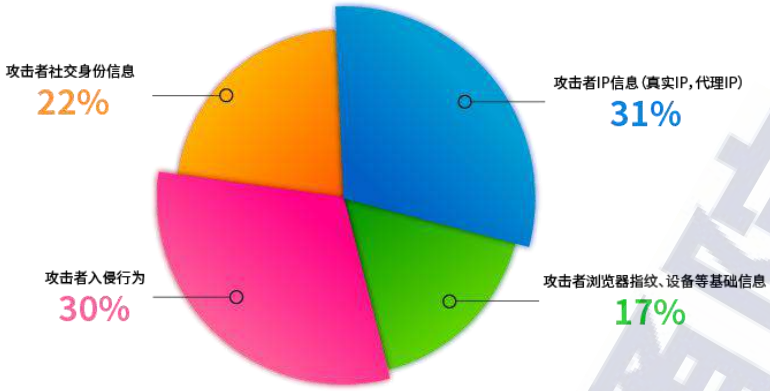


来源：FreeBuf 咨询根据调研数据整理

图 7 企业希望蜜罐产品覆盖的业务类型

根据调研结果，大部分企业希望威胁诱捕（蜜罐）产品覆盖更多业务类型，70%的受访者希望包括操作系统服务、Web 网站、业务高仿真、数据库等业务类型。

3. 企业最关心威胁诱捕（蜜罐）产品溯源获取的哪些信息



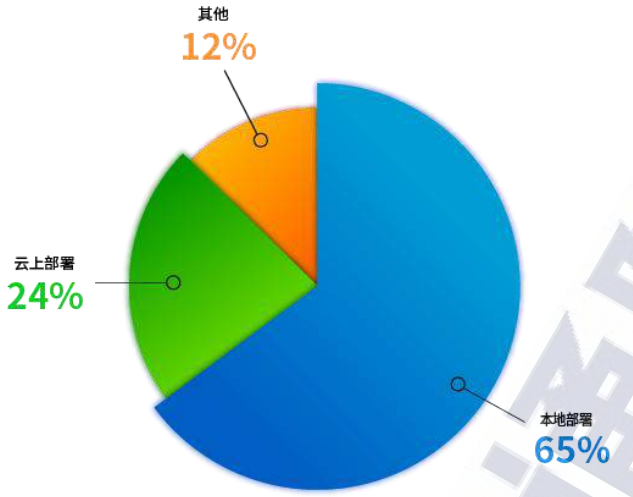
来源：FreeBuf 咨询根据调研数据整理

图 8 企业关注的蜜罐产品溯源信息

网络攻防本质上是攻守双方从技术、战术和心理多方位的角逐，当防守方占据了先机，就要根据攻击方所表现出的行为特征采取反制措施，因此需要完整记录攻击方的操作行为，便于防守方安全人员进行分析，判断其攻击意图和下步计划。当防守方搜集到足够多攻击者信息时，能够借助基础信息库对攻击者进行追踪和溯源，这也是企业最关注的威胁诱捕（蜜罐）产品的核心能力。

调研结果显示，企业最关心的蜜罐溯源信息包括四方面，攻击者 IP 信息（真实 IP、代理 IP）、攻击者入侵行为、攻击者社交身份信息（QQ、微信、爱奇艺等）、攻击者浏览器指纹、设备等基础信息。

4. 企业希望蜜罐产品满足哪些部署方式



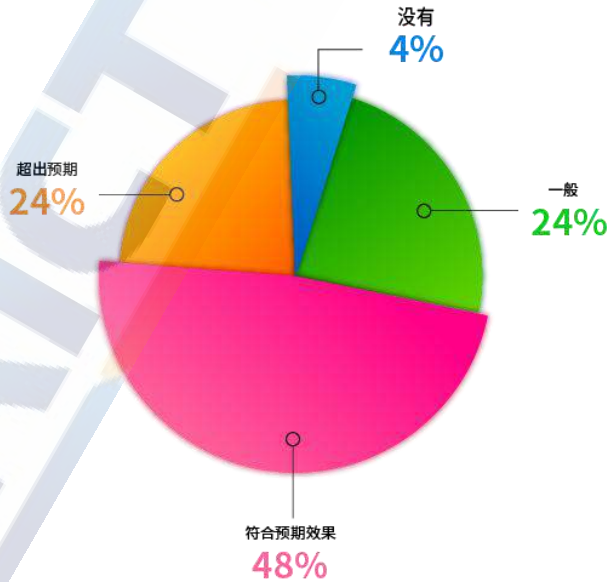
来源：FreeBuf 咨询根据调研数据整理

图 9 企业希望蜜罐产品满足的部署方式

随着企业业务环境变化，上云趋势加强，企业对蜜罐产品的部署需求也在变化。调研结果显示，65%的企业仍选择本地部署模式，还有 24%的企业希望产品满足云上部署模式。

（三）威胁诱捕（蜜罐）产品应用评价

1. 已部署的蜜罐产品效果是否已达到预期

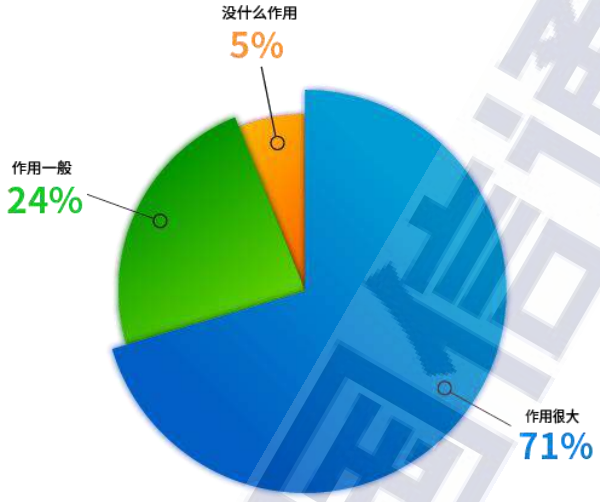


来源：FreeBuf 咨询根据调研数据整理

图 10 蜜罐产品效果是否达到预期

调研结果显示，48%的受访对象认为蜜罐产品效果符合预期效果，还有 24%的企业认为其超出预期，另有 4%的企业认为产品没有达到预期效果，主要体现为溯源反制能力与预期效果有一定差距。

2. 已部署的蜜罐产品在攻防演练中作用如何

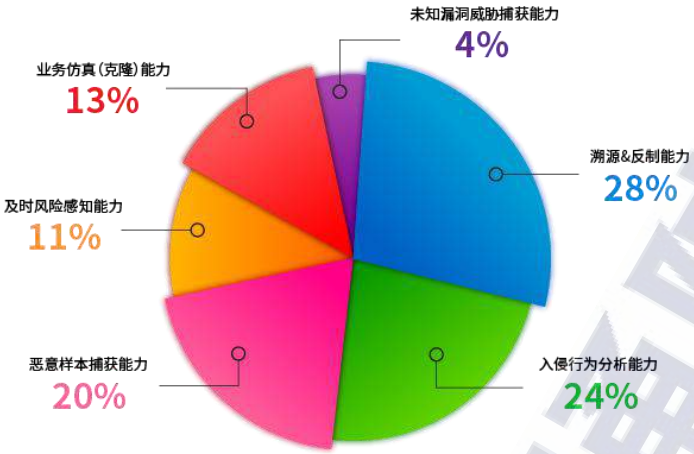


来源：FreeBuf 咨询根据调研数据整理

图 11 蜜罐产品在攻防演练中的效果

越来越多的企业应用蜜罐产品作为蓝军利器，在攻防演练中采用欺骗伪装来提升整体防护能力，改善攻防双方力量不对等的现状。对于蜜罐产品在攻防演练中的效果，调研结果显示，71%的企业认为其作用很大，另有 5%的企业由于安全团队规模小，缺乏人力物力部署和运维复杂蜜罐产品等原因，认为产品没什么作用。

3. 蜜罐产品在后续开发中应该增强哪些能力

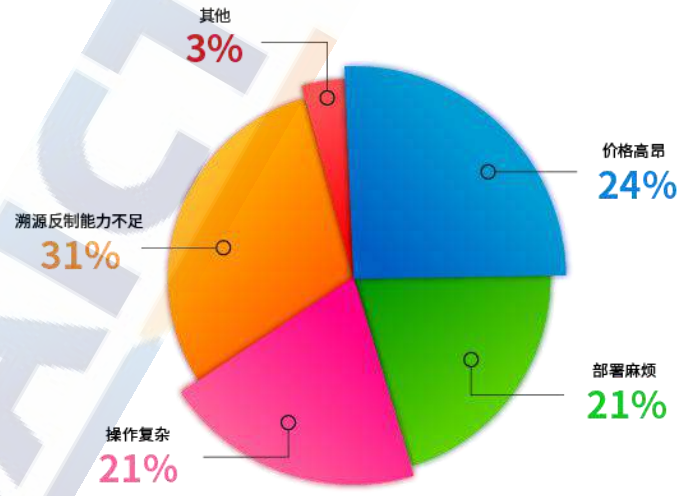


来源：FreeBuf 咨询根据调研数据整理

图 12 蜜罐产品需增强的能力

随着网络安全日常防护意识的增强和网络攻防演练的常态化展开，知己知彼成为了网络安全攻防的最大核心需求。在明确对抗重要性这一前提下，企业越发注重由被动防御转变为主动防御。调研结果显示，72%的企业认为蜜罐产品需增强“溯源和反制能力”、“入侵行为分析能力”及“恶意样本捕获能力”。

4. 企业对于现阶段蜜罐产品使用不满意度



来源：FreeBuf 咨询根据调研数据整理

图 13 企业对蜜罐产品不满意调查

根据调研，97%的企业用户对现阶段蜜罐产品不满意的问题主要集中在以下四个方面：“溯源反制能力不足”、“价格高昂”、“部署麻烦”、“操作复杂”。

四、蜜罐类产品测试情况综述

（一）测试基本情况

本次蜜罐类先进网络安全能力验证评估工作在信通院安全所网络安全实验室进行，开始于 2021 年 03 月 09 日，结束于 2021 年 05 月 21 日。

各参测企业提供的受测产品数量不同，如表 4 所示，普遍为一台至两台。两台设备参与测试的通常其中一台设备作为探针，另外一台设备作为安全分析和展示系统。参与测试的产品大部分采用标准 1U 或 2U 服务器，其中也有部分企业采用定制的专用主机。

因报名参加本期蜜罐类产品测试的企业较多且测试时间有限，本次测试采用多个企业产品并行测试，且每个企业测试总时长不超过五个工作日。

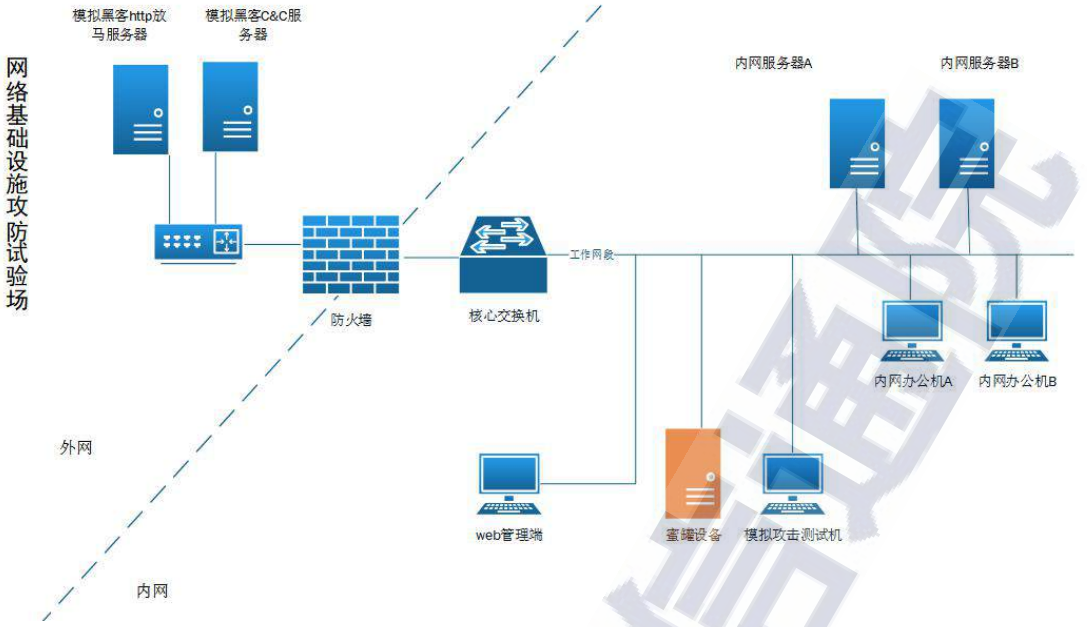
表 4 各企业到场测试产品情况

企业名称	简称	台数
北京永信至诚科技股份有限公司	永信至诚	2
北京长亭科技有限公司	长亭科技	1
烽台科技（北京）有限公司	烽台科技	1
杭州默安科技有限公司	默安科技	1
北京经纬信安科技有限公司	经纬信安	1
北京知道创宇信息技术股份有限公司	知道创宇	1
北京元支点信息安全技术有限公司	元支点	1
中国科学院信息工程研究所	信工所	1
江苏君立华域信息安全技术股份有限公司	君立华域	1

北京天融信网络安全技术有限公司	天融信	1
北京安天网络安全技术有限公司	北京安天	2
广州锦行网络科技有限公司	广州锦行	2
上海观安信息技术股份有限公司	上海观安	1
杭州安恒信息技术股份有限公司	杭州安恒	1
广州非凡信息安全技术有限公司	广州非凡	2
北京网御星云信息技术有限公司	网御星云	1
北京启明星辰信息安全技术有限公司	启明星辰	1
上海沪景信息科技有限公司	上海沪景	1
杭州天谷信息科技有限公司	杭州天谷	1
紫金山实验室	紫金山	1
北京鸿腾智能科技有限公司	北京鸿腾	1
网神信息技术（北京）股份有限公司	网神信息	1
北京吉沃科技有限公司	北京吉沃	1
山东云天安全技术有限公司	山东云天	1
北京智仁智信安全技术有限公司	智信安全	1
江苏天翼安全技术有限公司	江苏天翼	1
北京安域领创科技有限公司	安域领创	1
北京神州绿盟科技有限公司	神州绿盟	1
腾讯云计算（北京）有限公司	腾讯云	1
杭州智航云安全技术有限公司	智航云安全	1
北京四海图宇科技有限公司	四海图宇	1
恒安嘉新（北京）科技有限公司	恒安嘉新	1
北京微步在线科技有限公司	微步在线	1
上海斗象信息科技有限公司	斗象科技	2

来源：中国信息通信研究院

（二）测试环境介绍



来源：中国信息通信研究院

图 14 测试网络拓扑图

蜜罐类产品以普通电子终端设备的形态部署在需要感知的网段内，用于感知内部网络攻击，告警内部受害主机；对内网威胁监控预警；提供威胁事件、攻击链、攻击样本；精准告警内部网络威胁。蜜罐类产品应能够捕获攻击方的攻击行为、攻击工具，深入分析攻击方的攻击方法，判断攻击意图和动机，全面地展现安全威胁。

本次的测试环境准备了相关的恶意代码样本包，用于支持此功能的受测产品对恶意代码样本的分析。此外，通过部署 IXIA PerfectStormONE 流量发生器模拟部分网络攻击，但因为蜜罐类产品属于交互性较高的行为分析类产品，所以流量发生器只作为辅助测试手段。

如图 14 所示测试环境拓扑情况，受测产品的与交换机连接，所有产品管理口进行统一管理。受测产品需要配置 192.168.2.0 网段 IP

接入到受测网络中。为了保证测试结果截图的真实性，管理口 IP 以及其他相关采集分析设备被分配的 IP 不可以私自改变，在测试结果截图中应包含页面全屏，显示出管理 IP，以明确该测试截图内容为现场测试结果截图。

来源：中国信息通信研究院

图 15 测试现场

（三）测试方法说明

本次测试包括产品功能测试、性能测试和产品自身安全测试。**在功能测试方面**，对蜜罐欺骗防御系统应具备的功能提出具体要求，包括主机行为监测、网络行为监测、失陷主机监测、威胁情报产出、威胁行为的攻击链标记、日志审计等等。对满足测试内容的部分进行截图和说明，证明该产品对该测试项的满足程度。**在性能测试方面**，对蜜罐欺骗防御系统应该达到的性能指标作出推定，例如产品

的负荷量、识别威胁的检测速率、可识别的样本库等。**在自身安全测试方面**，是对蜜罐欺骗防御系统自身安全和防护能力提出的各种要求，比如产品配置管理要求、交付与运行要求、开发规范要求等。

本次测试对于结果的评价，包括不支持、基本支持、支持较好和完全支持。

本次测试对于结果的评价，只针对到场测试的产品的型号、版本号。

（四）测试内容简介

蜜罐类产品技术测试方案中共涉及二十个大项、五十一个功能小项，覆盖产品的功能、性能和安全性三大方向。

表 5 蜜罐类产品测试项目表

测试大项		测试小项
功能测试	服务伪装功能	总体要求
		网络服务仿真
		操作系统仿真
		数据库仿真
		Web 应用仿真
	欺骗防御功能	伪装欺骗功能
		捕获监测功能
		威胁情报产出功能
		威胁行为攻击链标记
	风险分析功能	入侵实时分析
		攻击关联分析
		关联威胁情报
		样本信息展示
		攻击维度分析
		攻击事件分析
		攻击分析模型
	风险展示功能	蜜网监控分析
		攻击事件分析
		诱捕态势感知

	蜜罐管理功能	节点信息
		节点操作
		镜像管理
		场景模板管理
		蜜饵管理
		流量重定向
		漏洞管理
		自定义拓扑图
		节点拓补自动生成
		联动功能
		时间校准
		机构管理
安全性测试	安全管理	安全角色管理
		远程保密传输
		可信管理主机
		系统可用性监测
	用户标识与鉴别	用户标识
		身份鉴别
	响应处理	告警
		事件记录
性能测试	设备预警安全事件与安全事件发生的时间间隔	
	安全事件的识别速度	
	单台设备至少支持同时开启的高交互蜜罐数量	
	蜜罐场景启动及切换	
	设备可识别的木马家族数量	
	攻击事件留存时间及导出	
	捕获行为数量	
	页面响应速度	
	内置检测规则	
	内置威胁情报	
	内置 IP 库	
	内置漏洞模板	

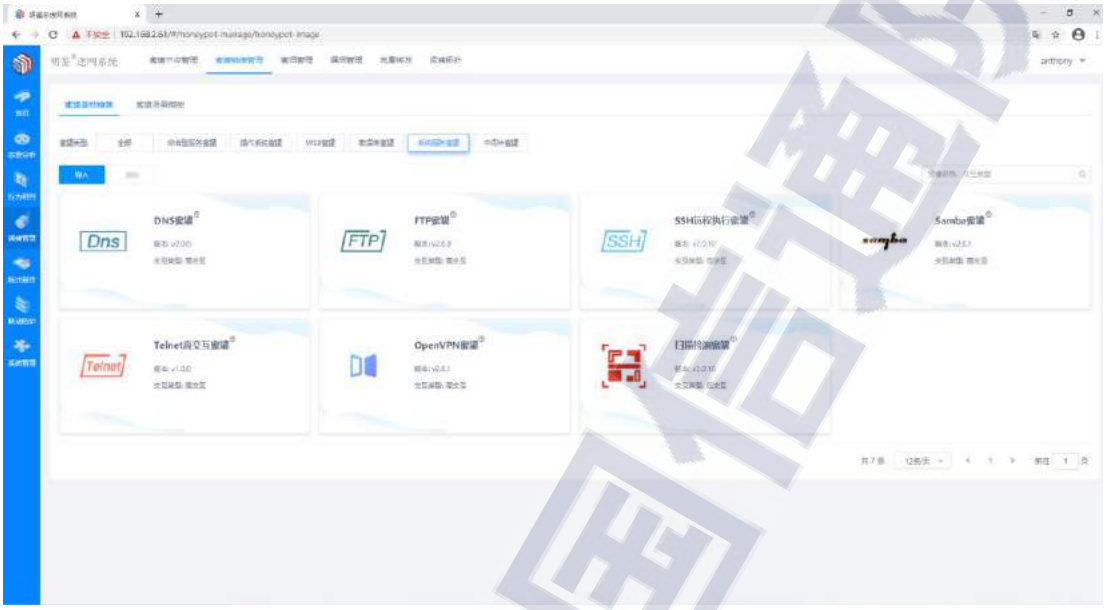
来源：中国信息通信研究院

五、蜜罐类产品测试结果总体分析

（一）交互模式支持度较为全面

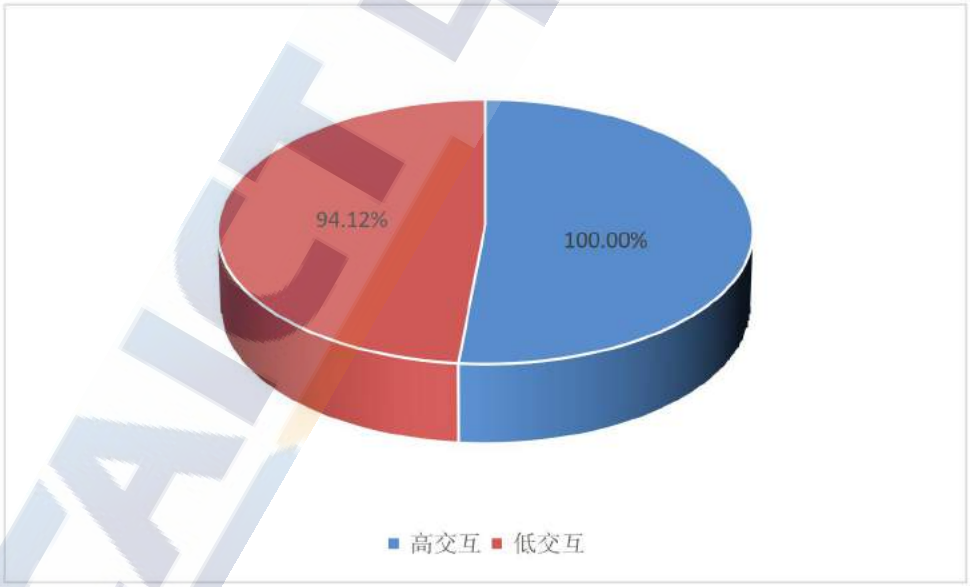
通过测试结果发现，几乎全部受测产品都能很好地支持不同的

交互类型。本次测试方案对受测产品进行了交互类型支持能力的总体要求进行了测试，测试包含的受测产品应能支持高交互、低交互两种类型的蜜罐。



来源：中国信息通信研究院

图 16 某蜜罐产品功能界面图



来源：中国信息通信研究院

图 17 受测产品交互种类支持情况

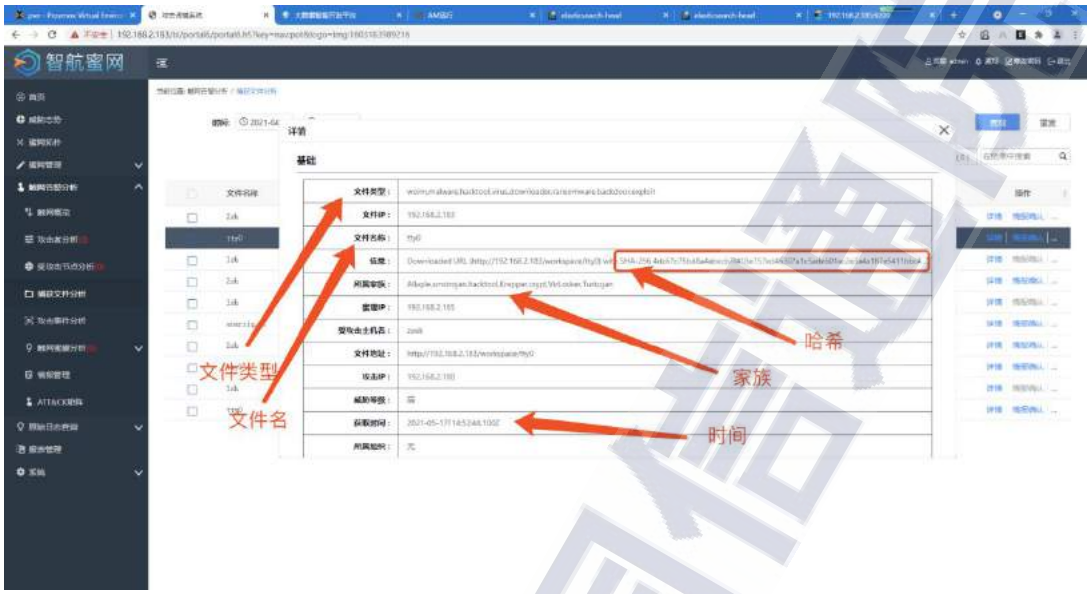
如图 17 所示，受测产品中，只有两款产品不支持低交互的蜜罐

类型，而高交互的蜜罐类型则 34 款产品全部支持。一般情况下，低交互蜜罐仅仅模拟操作系统和网络服务，较容易部署且风险较小，但黑客在低交互蜜罐中能够进行的攻击活动为有限，因此通过低交互蜜罐能够收集的信息也比较有限。而高交互蜜罐能够提供完全真实的操作系统和网络服务，从攻击者角度上看没有任何的模拟痕迹。因此在高交互蜜罐中，我们能够获得许多黑客攻击的信息，往往偏向于攻击手段研究型蜜瓜更倾向于高交互的蜜罐部署方式。此外，受测产品中还有部分支持“中交互”，中交互蜜罐相低交互蜜罐虽然能够提供更多的交互信息，但仍然不是提供一个真实的操作系统。而且中交互与低交互的功能边界不易区分，本次测试不对中交互型蜜罐作要求。虽然，高交互、低交互的蜜罐形式都有各自的优缺点，但从本次测试结果总体来看，国内蜜罐类产品在不同交互种类的支持上较为全面，为蜜罐在不同的部署需求和场景中提供了较为灵活地选择。

（二）威胁情报的赋能有待加强和完善

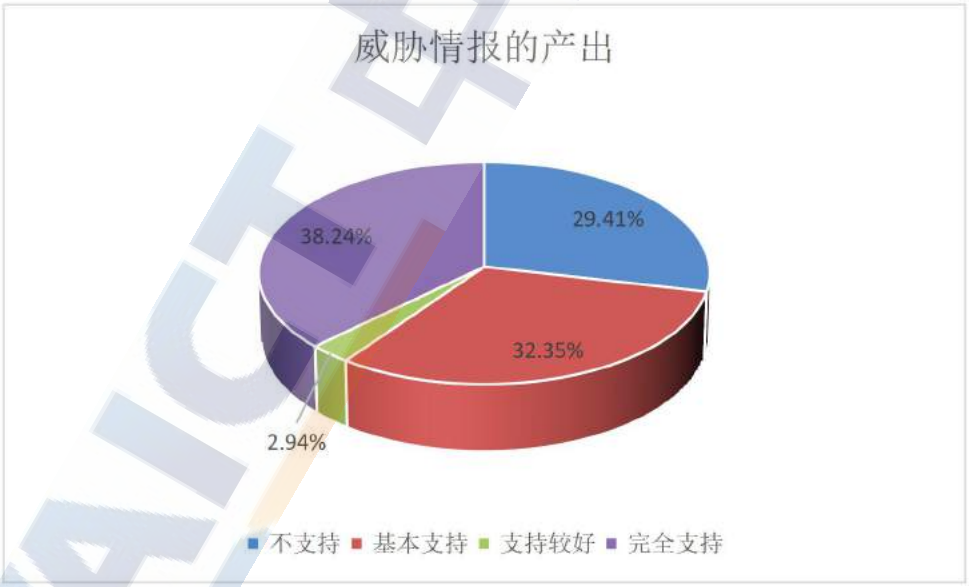
通过测试结果发现，**仅有少数受测的蜜罐产品能够实现与威胁情报进行联动，多数产品不具备此功能或实现程度不高**。本次测试方案中，针对威胁情报在蜜罐中的应用主要包含两个方面，一方面是受测产品对于捕获收集的相关数据产出形成威胁情报的能力，包括但不限于样本 MD5、IP 或域名形式的 C&C 信息等。另一方面，验证受测产品是否支持内置的威胁情报，并能够对捕获样本展示详细的威胁情报关联信息，包括关联文件名、关联文件哈希、关联文

件类型、关联文件家族信息、关联文件最后上传时间、关联类型信息等。



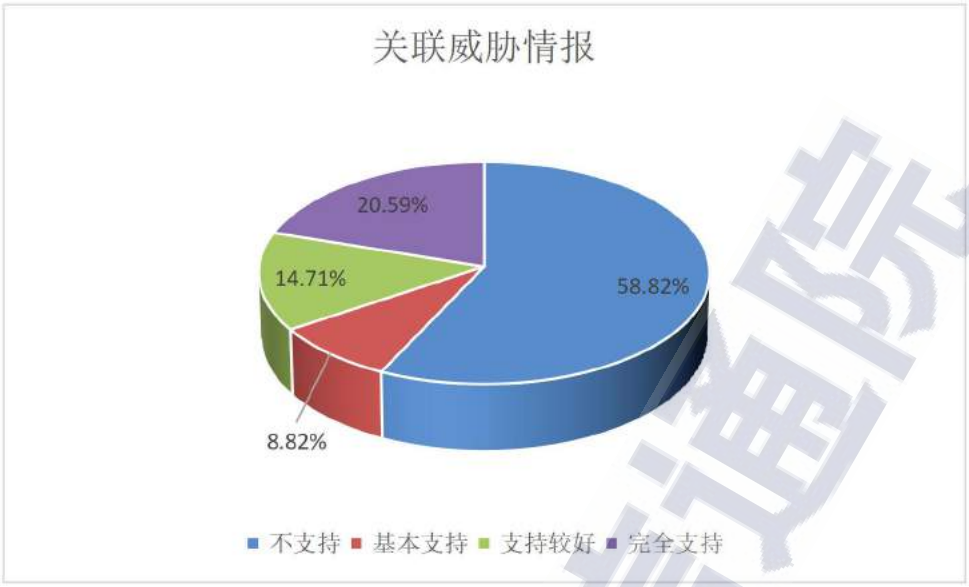
来源：中国信息通信研究院

图 18 某蜜罐产品功能界面图



来源：中国信息通信研究院

图 19 受测产品威胁情报产出功能支持情况



来源：中国信息通信研究院

图 20 受测产品关联威胁情况功能支持情况

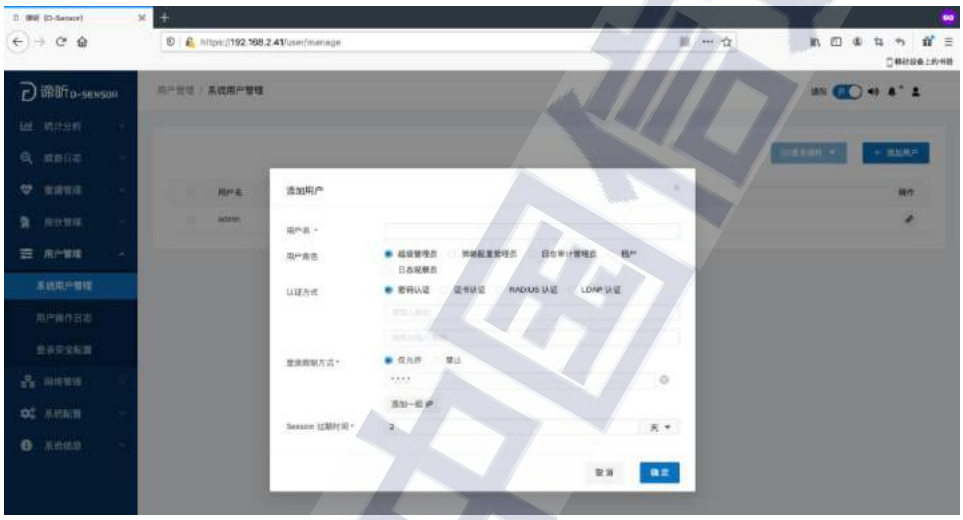
如图 19 和图 20 所示，34 款受测产品在威胁情报产出中，支持率相对较高，只有 29.41%的产品不支持。但关联威胁情报的功能支持率比较低，不支持此功能的产品达到 20 款，占比 58.82%；能够完全支持关联威胁情报功能的产品 7 款，仅占全部受测产品的 20.59%。

威胁情报是关于IT或信息资产所面临的现有或潜在威胁的循证知识，包括情境、机制、指标、推论与可行建议，这些知识可为威胁响应提供决策依据[2]。蜜罐产品是各个部署环节收集情报的重要手段之一，如何对收集的威胁情报进行挖掘和分析，进一步了解攻击数据中不同信息间的联系，从而搞清攻击者的攻击方式和意图，是蜜罐类产品发展不可或缺的一环。因此，**威胁情报在蜜罐中的应用仍然需要网络安全企业不断深入研究和实践。**

2 Gartner 在 2014 年发表的《安全威胁情报服务市场指南》（Market Guide for Security Threat Intelligence Service）

（三）产品自身管理能力总体较好

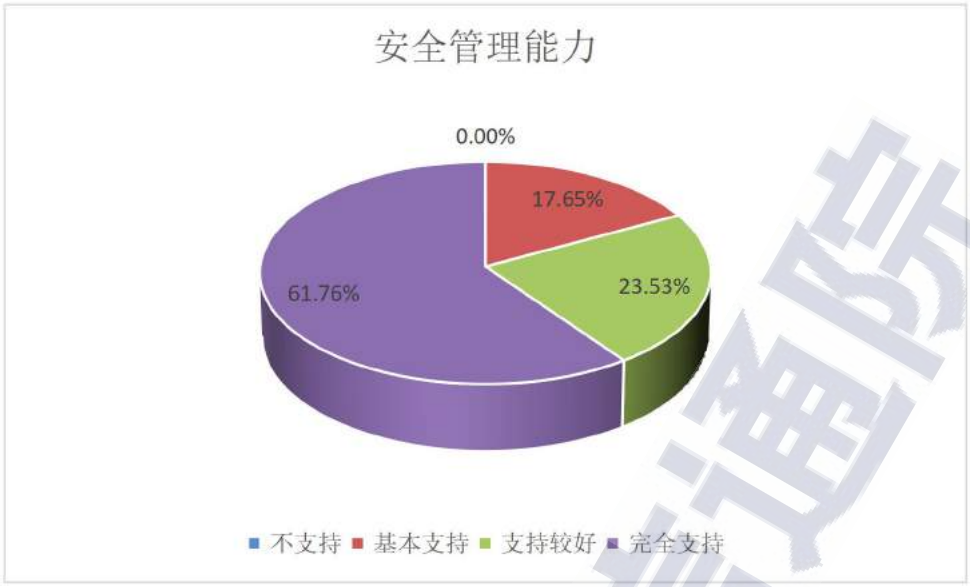
通过测试结果发现，绝大部分受测产品在产品自身安全方面支持较好。**在安全管理方面**，具备安全角色管理、远程保密传输、可信管理主机、系统可用性监测等功能。**在用户标识与鉴别方面**，具备权限划分、功能划分与角色划分等功能。**在响应处理方面**，具备告警和事件记录等功能。



来源：中国信息通信研究院

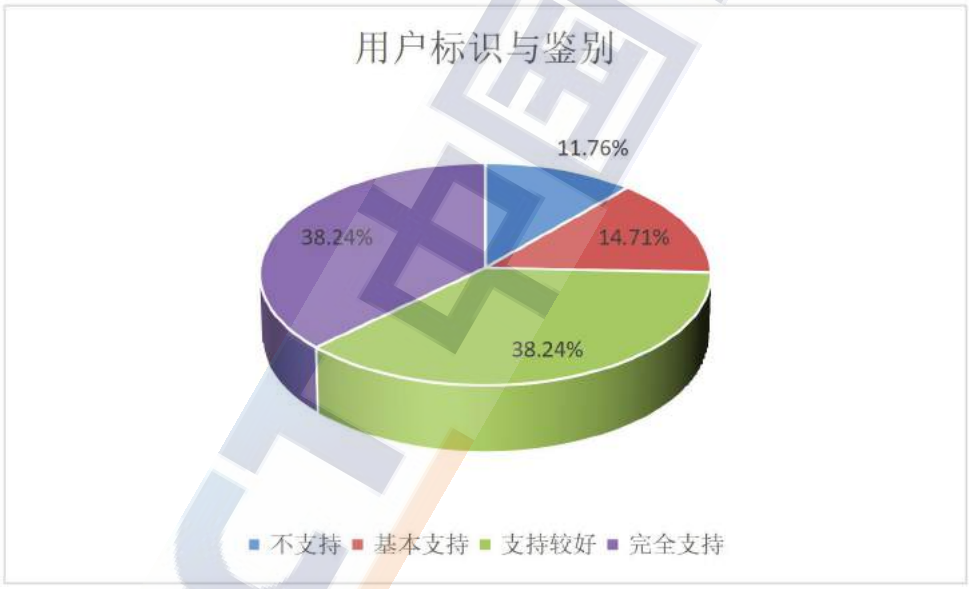
图 21 某蜜罐产品功能界面图

通过测试结果发现，**绝大部分产品具有完善的自身管理能力。**如图 22 至图 24 所示，其中大部分产品在安全管理、用户标识与鉴别、响应处理等三个方面支持较好。



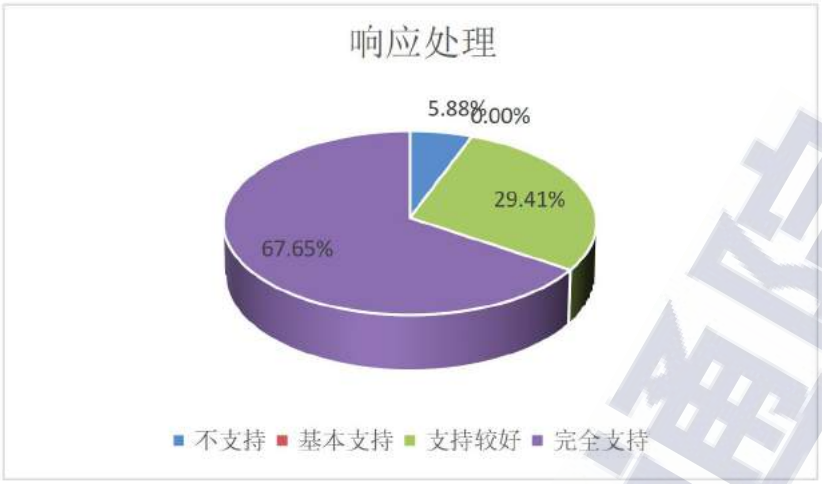
来源：中国信息通信研究院

图 22 产品自身管理功能结果比例图



来源：中国信息通信研究院

图 23 产品用户标识与鉴别功能结果比例图



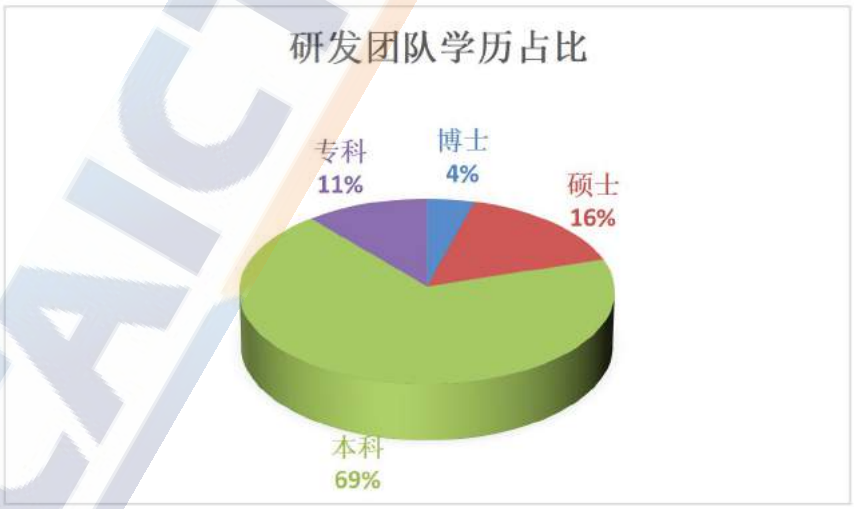
来源：中国信息通信研究院

图 24 产品响应处理功能结果比例图

（四）蜜罐研发团队需加强人才投入

在本次测试过程中，为了评估蜜罐产品在国内的开发投入情况，我们对受测企业在不泄露个人基本隐私信息的前提下，进行了产品研发团队成员的简历汇总和统计，包括但不限于产品架构师、产品经理、系统架构师、后端研发和前端研发等。

本次所调研数据并未经过核实验真，以下数据只作为参考。



来源：中国信息通信研究院

图 25 企业研发团队情况分析

通过汇总 34 家蜜罐企业的研发团队信息发现，当前受测企业对于蜜罐类产品的开发团队的人员投入最多为 20 人，最低为 1 人，绝大部分企业的人员投入不到 10 人，平均为 6.27 人。在研发团队学历构成中。本科学历占绝大部分，有 5 家企业投入了博士人才，占比 4%。

尽管一个产品的研发能力取决于研发团队的综合素质和水平，不能以学历做定论，但研发团队的学历在一定程度上代表着一款产品的研发厚度和深度。因此，如何科学有效的组建和管理一支产品研发团队、运用科学有效的手段提高团队积极性和创新性，从而提升蜜罐产品的整体技术水平和竞争力，是需要各企业不断摸索的一个过程。

六、蜜罐类产品测试结果功能维度分析

（一）服务伪装功能测试结果分析

1. 本节概述

蜜罐类产品最核心的功能，就是模拟通常实际生产环境中的主要资产、端口、服务，甚至构建一个模拟网络运行环境，伪装成真实的信息系统，这样就可以引诱黑客进行攻击，从而可以对攻击行为进行捕获和分析。当前网络空间安全对抗中，攻击方的方法和手段不断迭代更新，蜜罐的伪装能力和交互能力也应不断丰富和拓展，才能不断应对攻击者的行为、混淆攻击目标、滞后攻击威胁，进一步分析攻击过程、提前研判攻击目的以及溯源攻击者的信息。

本次测试中，从总体要求、网络服务仿真、操作系统仿真、数

据库仿真、Web 应用仿真和高级服务仿真等几个方面对参与测试的产品进行了逐一地验证。其中，**总体要求**是对蜜罐类产品是否能够支持高、低交互进行验证。另外从**网络服务仿真、操作系统仿真、数据库仿真、Web 应用仿真**等几个常见角度对产品进行服务伪装功能的验证。在**高级服务仿真**的测试要求中，验证了测试产品支持各类高级服务仿真功能的情况，如溯源蜜罐、TCP 协议仿真、自定义 Web（Python、PHP 等）服务、自定义 TCP 响应服务等。

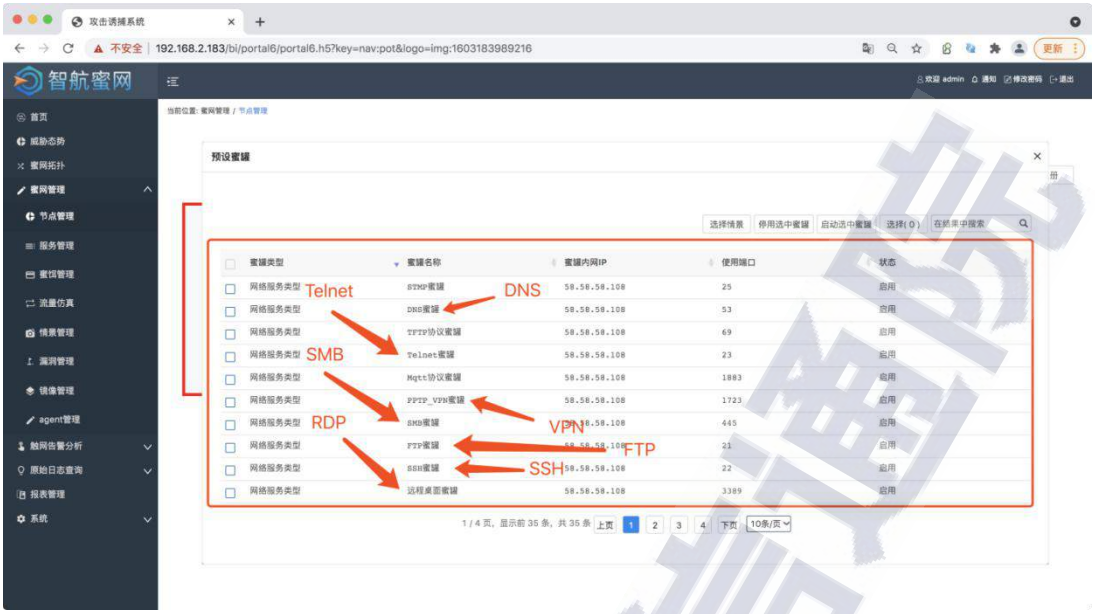
本项测试内容旨在从不同的服务伪装类别和能力上，对受测产品进行分析和汇总，研究当前国内蜜罐类产品在服务伪装能力上的技术发展趋势和不足。

2. 测试结果情况

（1）网络服务仿真

本次测试除对于不同交互类型支持的“总体要求”外，要求受测产品需支持各类网络服务仿真，包含但不限于 IPSEC、DNS、SMB、SSH、FTP、TELNET、RDP 等至少十种应用协议。

从测试结果来看，该测试项在 34 款产品中测试的平均支持率为 76.47%，其中 SSH 和 TELNET 基本都能够支持。该项支持较好或完全支持的为 25 款产品，占比 73.53%，仍有 9 款产品在各类网络服务仿真中支持种类较少。



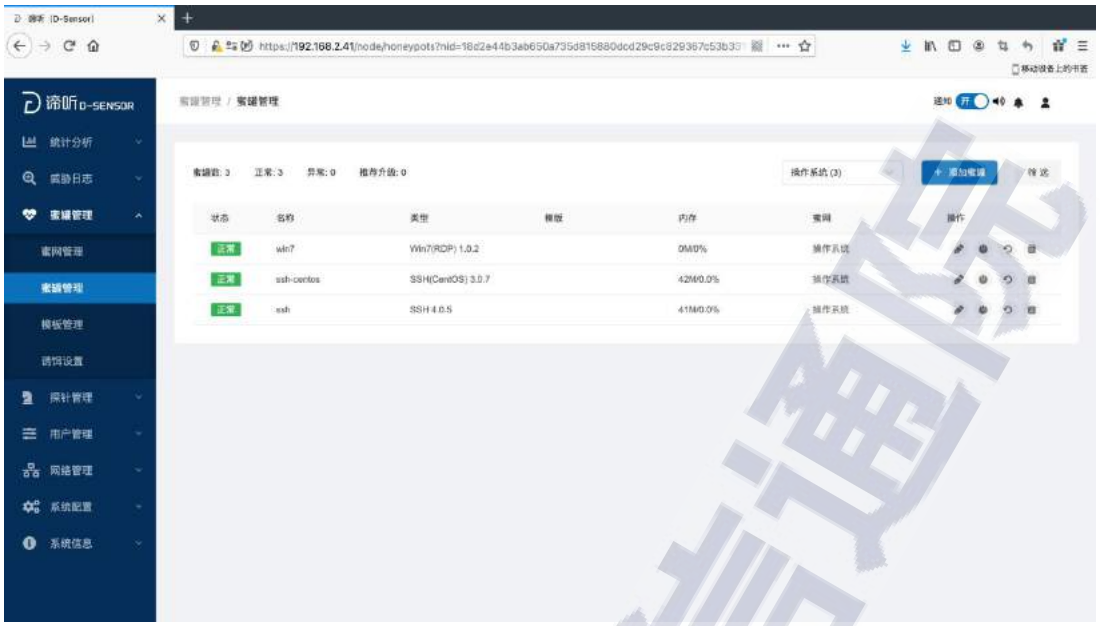
来源：中国信息通信研究院

图 26 某蜜罐产品功能界面图

（2）操作系统仿真

该项测试要求受测产品需支持操作系统仿真，包含但不限于 Windows、CentOS 等。

从测试结果来看，该测试项有 26 款产品完全支持，占 34 款产品的 76.47%。此外 7 款产品仅支持其中一类操作系统。仅有 1 款产品完全不支持操作系统仿真。从做操系统支持程度来看，在部分支持的产品中，绝大部分不支持的类型为 Windows 操作系统，而 CentOS 类的操作系统基本都可以支持。



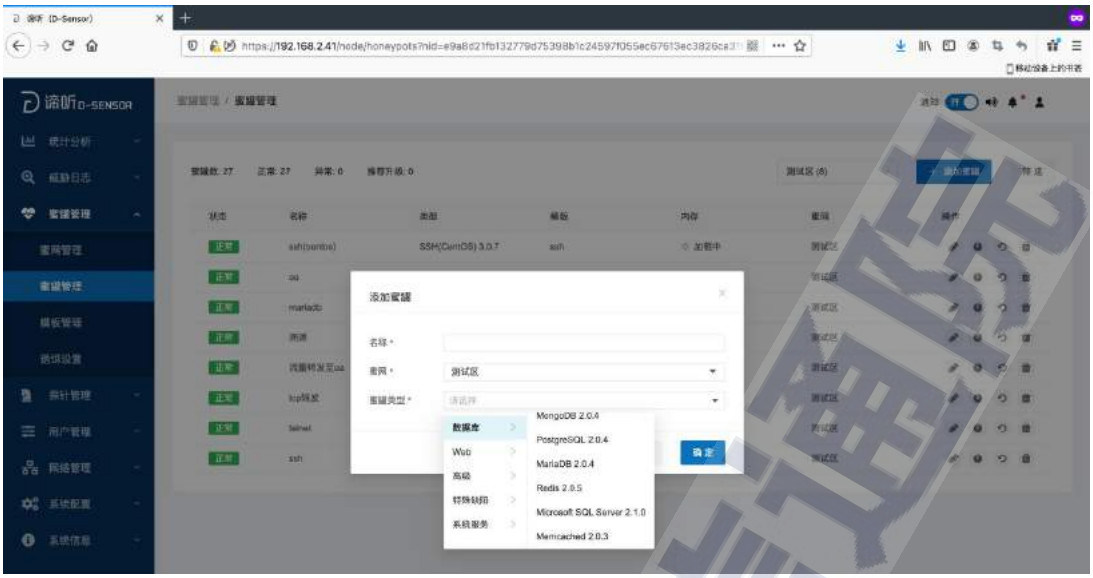
来源：中国信息通信研究院

图 27 某蜜罐产品功能界面图

（3）数据库仿真

该项测试要求受测产品需支持对常见数据库系统的仿真，包括但不限于 Redis、MySQL、MSSQL、Oracle、MongoDB、Memcached、MariaDB、PostgreSQL 等。

从测试结果来看，有 24 款产品完全支持至少四种数据库的仿真功能，占 34 款产品的 70.59%。此外支持三种数据库类别的为 4 款产品，支持两种数据库类别的为两款产品，仅支持 1 种数据库类别的为 4 款产品。



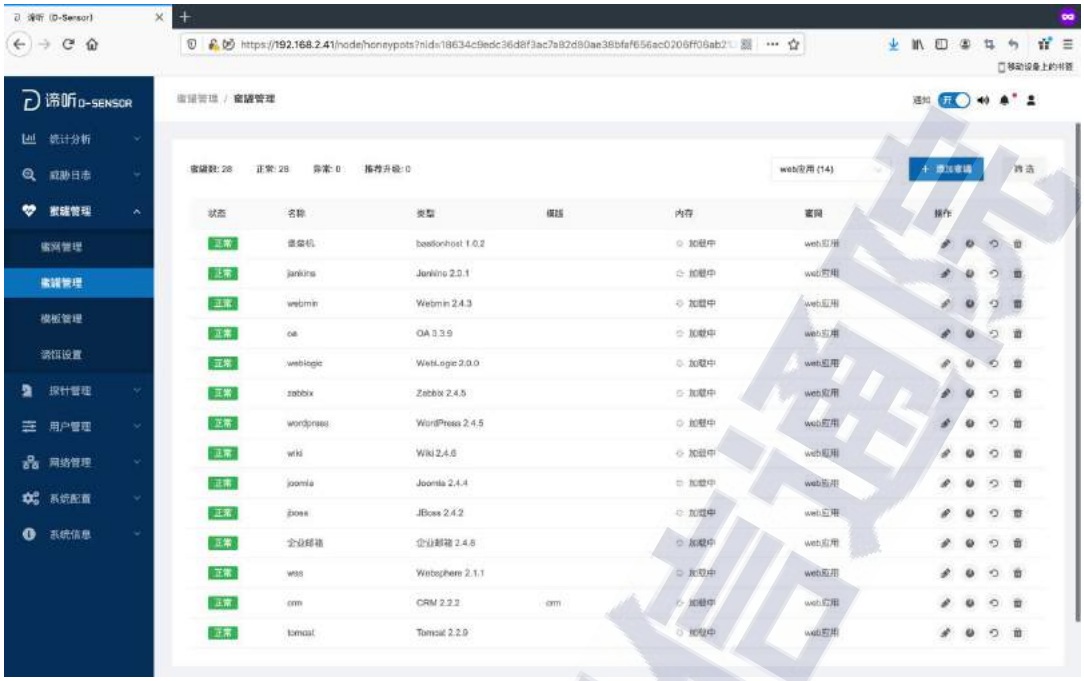
来源：中国信息通信研究院

图 28 某蜜罐产品功能界面图

（4）Web 应用仿真

该项测试要求受测产品需支持常见Web 应用的仿真，包括 CRM、Zabbix、OA、Wordpress、JBoss、Tomcat、Joomla、Weblogic、Docker 仓库、WAS 服务、企业邮箱、运维审计堡垒机、沙箱等。

从测试结果来看，有 15 款产品完全支持二十种不同类别的 Web 应用仿真功能，占 34 款产品的 44.11%。仅能支持十种以下 Web 应用仿真的产品为 10 款，占比 29.41%。



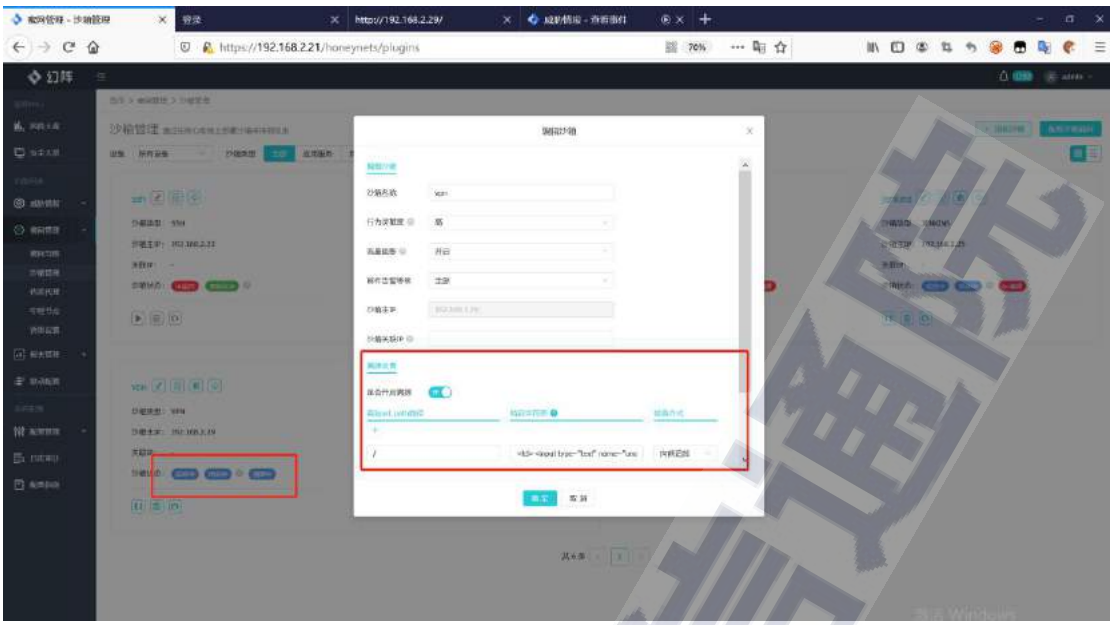
来源：中国信息通信研究院

图 29 某蜜罐产品功能界面图

（5）高级服务仿真

该项测试要求受测产品需支持各类高级服务的仿真，包括但不限于溯源、TCP 协议仿真、自定义 Web（Python、PHP 等）服务、自定义 TCP 响应服务等。高级服务仿真的意义在于通过对基础伪装服务的“升级”，打造一个更贴合实战场景的高级伪装功能，使蜜罐产品面对攻击者时能够产生更好的迷惑性和攻击黏性。

从测试结果来看，该测试项有 12 款产品完全支持各类高级仿真功能，占 34 款产品的 35.29%。部分支持的为 13 款产品，占比 38.24%，不支持的为 9 款产品，占比 26.47%。

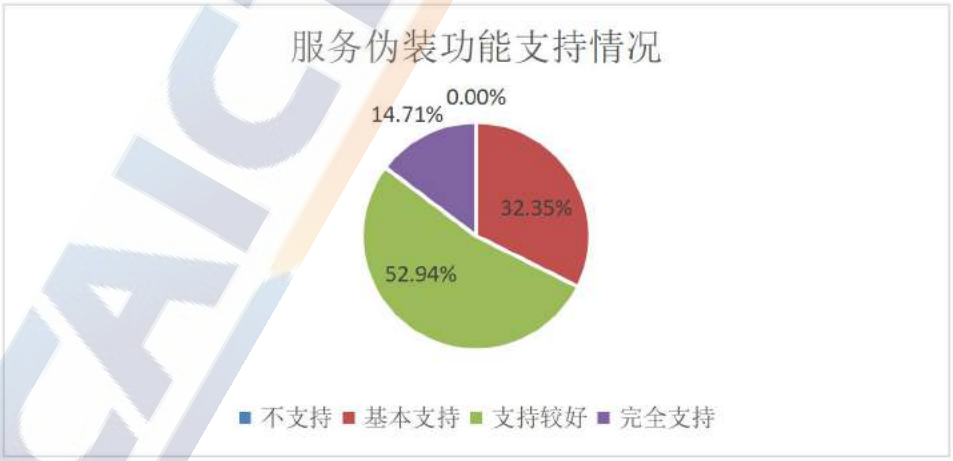


来源：中国信息通信研究院

图 30 某蜜罐产品功能界面图

3. 服务伪装能力维度排名（前十）

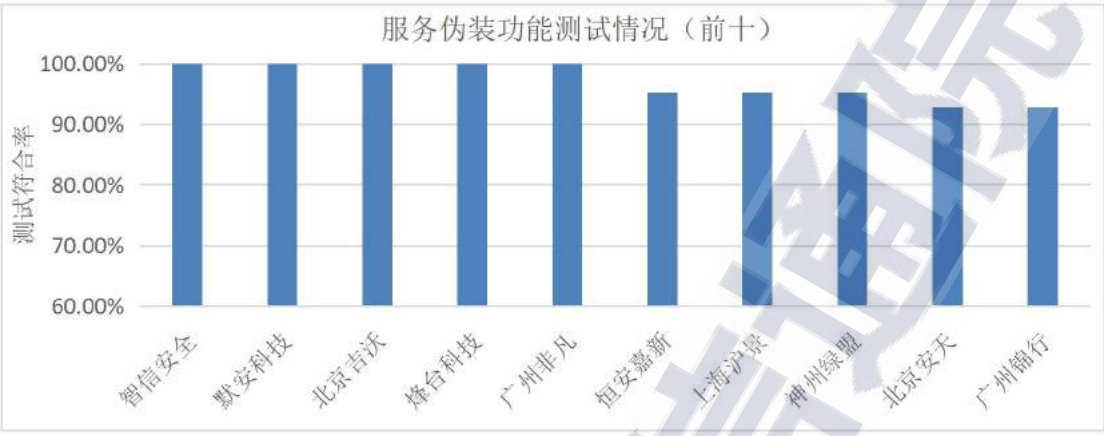
从服务伪装功能总体支持情况来看，完全支持和支持较好的产品为 23 款，约占全部测试产品的 68%。各测试项中，基础服务仿真的总体支持率相对较好，但“高级服务仿真”的测试结果支持率相对较低，拉低了整体比率。



来源：中国信息通信研究院

图 31 服务伪装功能支持情况

根据对 34 款产品的测试结果进行审核、分析和汇总，统计出针对蜜罐类产品服务伪装功能支持率相对较好的十款产品，如下图。



来源：中国信息通信研究院

图 32 服务伪装功能测试结果图

表 6 服务伪装能力组

厂家	产品	型号	版本
北京智仁智信安全技术有限公司	魔境网络安全预警系统	I7000	NSA-V1.0
杭州默安科技有限公司	幻阵高级威胁检测系统	MoreSec-H	V2.8.3
北京吉沃科技有限公司	智能仿真与诱捕防御系统	DecoyPro	V2.0
烽台科技（北京）有限公司	灯塔安全威胁诱捕审计系统	ICS-TSS	V1.0
广州非凡信息安全技术有限公司	幻影-攻击诱捕与威胁检测系统	okpot	V1.0
恒安嘉新（北京）科技有限公司	金甲-全息诱捕威胁分析平台	Deception Shell-S5	V2.0
上海沪景信息科技有限公司	网络威胁诱捕系统	ANT8220	V1.0
北京神州绿盟科技有限公司	绿盟科技高级威胁狩猎	EDR-ATHNX 3-HD1000	V5.0
北京安天网络安全技术有限公司	捕风蜜罐系统 V3.0	ACS-POT-10 00	V3.3.3.0
广州锦行网络科技有限公司	幻云-欺骗防御与本地威胁情报平台	JES-HYS-05 18	V2.5

来源：中国信息通信研究院

（二）欺骗防御功能测试结果分析

1.本节概述

大量研究表明，网络攻击之前通常伴有侦查阶段。有研究指出70%的攻击活动之前都存在侦查行为[3]。网络攻击博弈中，攻击方一般都是通过对网络侦查获取一定的可用信息，进而决定下一步的攻击动作。欺骗防御正是在这个环节中，通过干扰攻击方的认知以促使其采取有利于防御方的行动。与传统安全技术相比，网络欺骗不是着眼于攻击特征而是攻击者本身，这个功能可以扭转攻击者与防御者之间攻防不对称的局面。

本次测试中，对各参测的蜜罐类产品在欺骗防御的相关功能上进行测试和验证。测试的方向包括伪装欺骗、捕获监测、情报产出和攻击链标记等功能。

2.测试结果情况

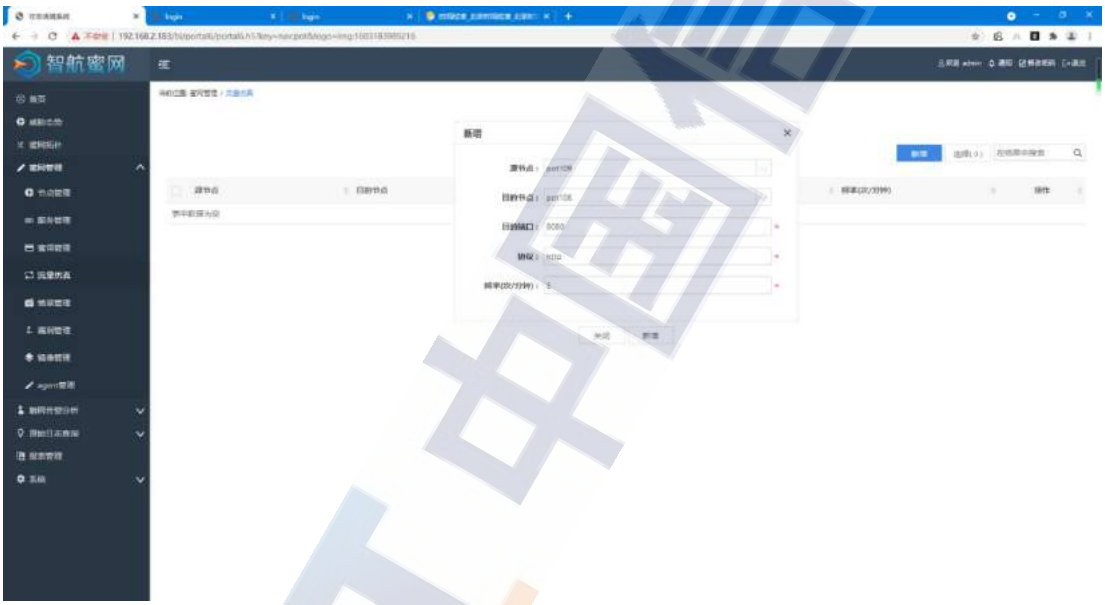
（1）伪装欺骗

伪装欺骗功能主要验证发现与登录、动态变更端口服务、攻击转移、IPV6 支持情况、系统诱饵定制、诱导登录、流量仿真、蜜饵预设类型、漏洞预设类型等几个方面在受测蜜罐类产品上的支持情况。

基于该测试项有较高的用例数量和测试宽度，因此从测试结果来看，该测试项仅有两款产品完全支持，占 34 款产品的 5.88%。大部分产品都是支持部分测试项，其中支持较好的和基本支持的均为

3 PANJWANI S, TAN S, JARRIN K M, et al. An experimental evaluation to determine if port scans are precursors to an attack[C]//2005 International Conference on Dependable Systems and Networks (DSN'05). 2005: 602-611.

16 款产品，合计占比 94.12%。未发现完全不支持该测试项的产品。值得一提的在本次测试欺骗防御功能中，一个测试项为“流量仿真”功能，验证受测产品是否支持设定定期自动产生对蜜罐的访问流量，刷新访问日志。该测试项希望能够验证蜜罐类产品能够在完善的服务伪装功能下，最大化模拟真实环境，包括模拟真实环境下的业务流量和访问日志，旨在避免使敏感的攻击者因蜜罐的过于“清白”，而放弃进一步的攻击尝试，从而影响伪装欺骗功能的效果。



来源：中国信息通信研究院

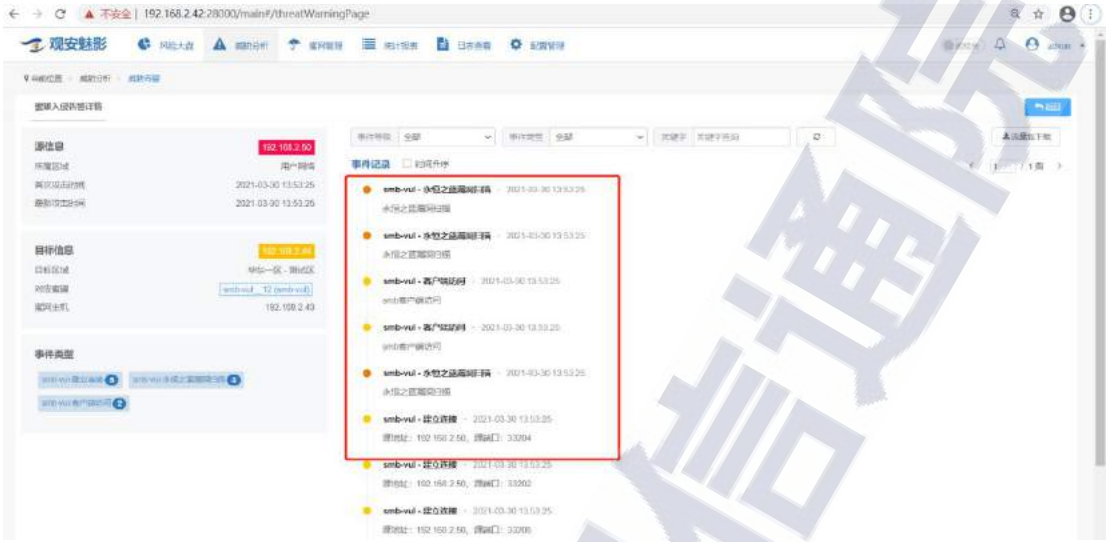
图 33 某蜜罐产品功能界面图

（2）捕获监测

捕获监测功能主要验证蜜罐在主机行为监测、网络行为监测、失陷主机监测等几个方面的支持情况。

总体来说该测试的测试结果的支持情况较好，虽然仅有 5 款产品完全支持，占 34 款产品的 14.7%。但是大部分产品都属于能够较

好支持测试要求，共计 20 款，占比 58.82%。此外，基本支持测试要求的为 9 款，占比 26.47%。未发现完全不支持该测试项的产品。



来源：中国信息通信研究院

图 34 某蜜罐产品功能界面图

（3）情报产出

该测试项主要验证受测蜜罐是否支持针对产品收集到的数据产出威胁情报的能力，包括但不限于样本 MD5、IP 或域名形式的 C&C 信息等。

受测产品中，完全支持此测试项的为 12 款，占受测产品的 35.29%，不支持的产品为 11 款，基本支持的产品为 10 款，占比共为 61.76%。而测试成绩居中的支持较好的产品仅为 1 款。从总体测试结果看，该测试结果相对“两极分化”。国内部分企业的威胁情报库的建设和相关功能都比较完善，而参与测试的部分产品或企业属于新兴企业，在威胁情报等增加产品“厚度”的能力方面相对较弱。

来源：中国信息通信研究院

图 35 某蜜罐产品功能界面图

（4）攻击链标记

该测试项主要验证受测蜜罐是否支持按照攻击者攻击的时间展示攻击链，攻击链中应包含但不限于攻击者 IP、受攻击者 IP、威胁行为、攻击时间、PCAP 信息等；以及网络入侵、横向渗透、恶意目的等攻击阶段的恶意行为。

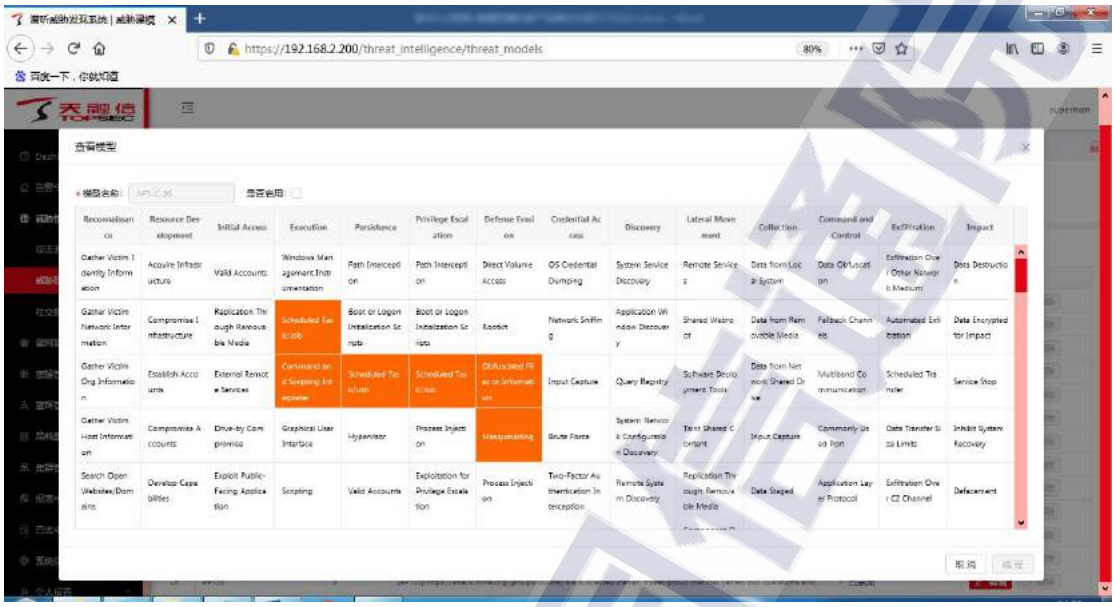
受测产品中，完全支持此测试项的为 12 款，占受测产品的 35.29%，不支持的为 9 款产品，占比 26.47%。此外，支持较好地为 6 款，基本支持的 7 款。

从测试结果分析，当前各产品参考的攻击模型主要是 KillChain[4] 和 ATT&CK[5]。各企业在 APT 网络攻击对抗不断深入的大背景下，

[4] KillChain：指洛克希德-马丁公司的网络杀伤链，也称网络攻击生命周期。它是一个描述攻击环节的六阶段模型，该理论也可以用来反制此类攻击（即反杀伤链）。杀伤链共有“发现-定位-跟踪-瞄准-打击-达成目标”六个环节。

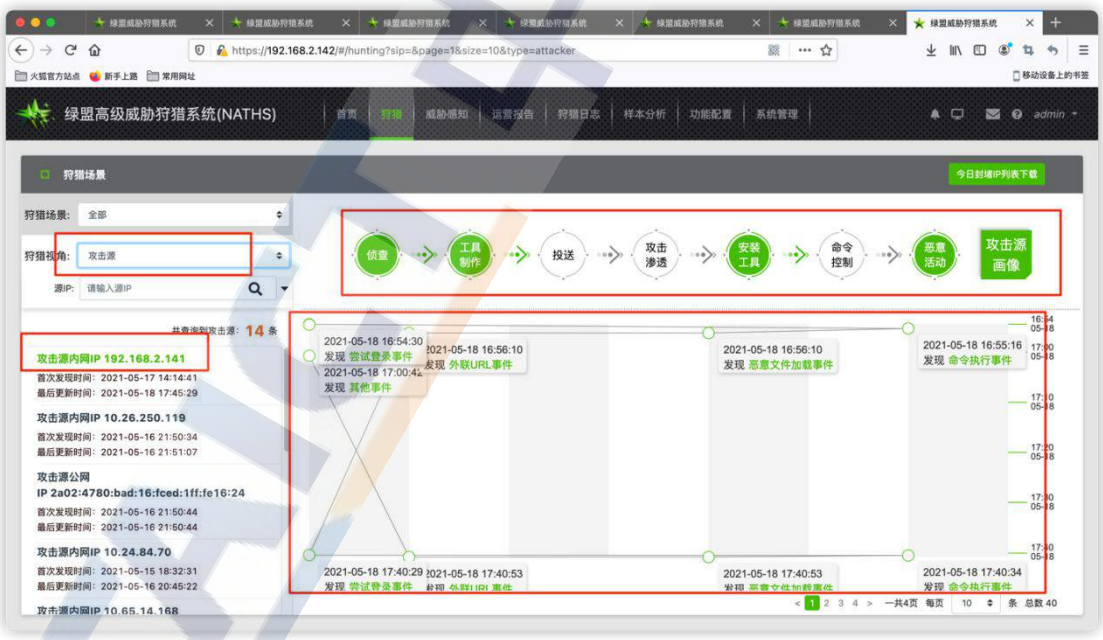
[5]ATTRCK&CK：Adversarial Tactics, Techniques, and Common Knowledge 缩写。它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型。该模型由 MITRE 公司提出，这个公司一直以来都在为美国军方做威胁建模，之前著名的 STIX 模型也是由该公司提出的。

应持续完善产品能力，在网络安全防御与应急响应工作中起到实际效果。



来源：中国信息通信研究院

图 36 某蜜罐产品功能界面图

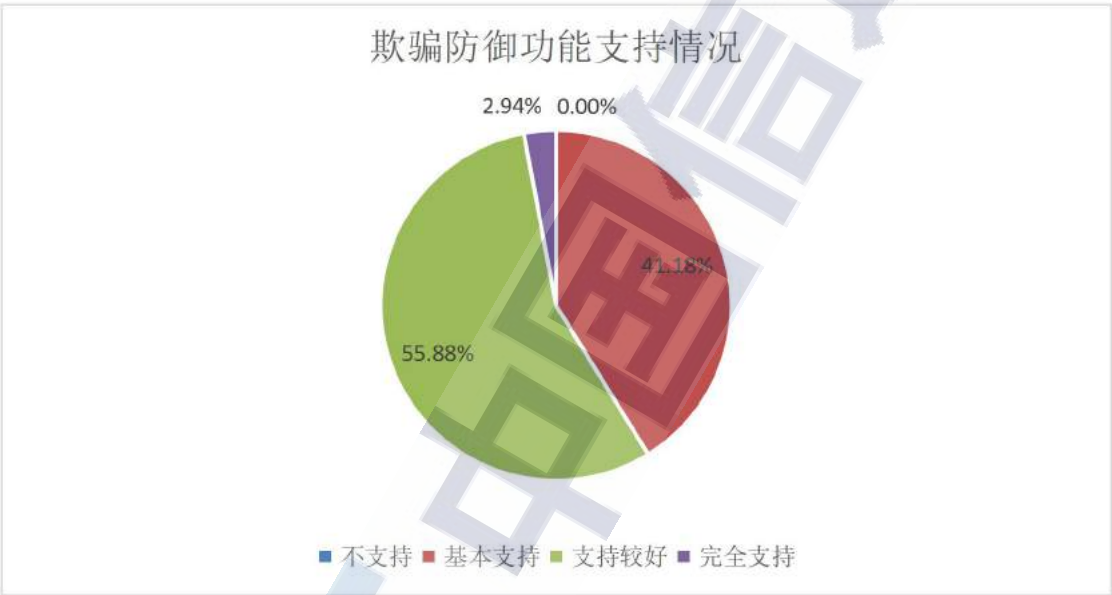


来源：中国信息通信研究院

图 37 某蜜罐产品功能界面图

3.欺骗防御能力维度排名（前十）

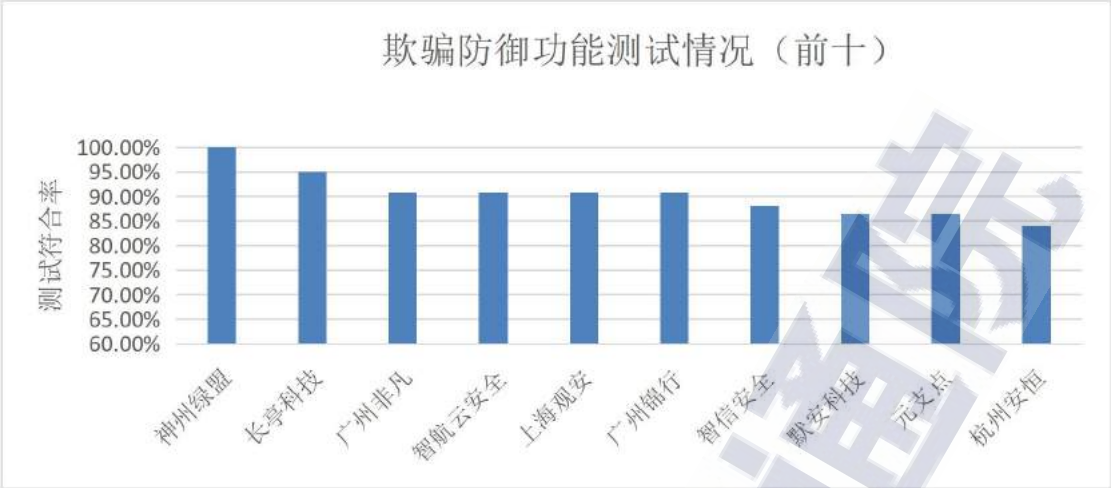
从欺骗防御功能总体支持情况来看，完全支持的仅为 1 款产品，支持较好的产品为 19 款，基本支持的产品为 14 款。各测试项中，伪装欺骗和捕获监测为欺骗防御的基本能力，各个测试产品表现良好；而情报产出和攻击链标记的辅助功能，测试结果相对偏低，平均支持率均为 50%至 60%。



来源：中国信息通信研究院

图 38 欺骗防御功能支持情况

根据对 34 款产品的测试结果进行审核、分析和汇总，统计出针对蜜罐类产品欺骗防御功能支持率相对较好的十款产品，如下图。



来源：中国信息通信研究院

图 39 欺骗防御功能测试结果图

表 7 欺骗防御能力组

厂家	产品	型号	版本
北京神州绿盟科技有限公司	绿盟科技高级威胁狩猎	EDR-ATHNX3-HD1000	V5.0
北京长亭科技有限公司	长亭谛听（D-Sensor）内网威胁感应系统	DS-H40-M50	DS-H40-21.01.001
广州非凡信息安全技术有限公司	幻影-攻击诱捕与威胁检测系统	Okpot	V1.0
杭州智航云安全技术有限公司	智航蜜网	ZHHW-S-P	V3.1
上海观安信息技术股份有限公司	魅影威胁监测系统		V2
广州锦行网络科技有限公司	幻云-欺骗防御与本地威胁情报平台	JES-HYS-0518	V2.5
北京智仁智信安全技术有限公司	魔境网络安全预警系统	I7000	NSA-V1.0
杭州默安科技有限公司	幻阵高级威胁检测系统	MoreSec-H	V2.8.3
北京元支点信息安全技术有限公司	有影攻击诱捕系统	YZD-DP-001	V3
杭州安恒信息技术股份有限公司	明鉴迷网系统	DAS-HPOT-3000	V2.0.9

来源：中国信息通信研究院

（三）风险分析功能测试结果分析

1. 本节概述

蜜罐类产品的主要作用是针对攻击的检测、捕获、分析、取证以及预警等。其中，分析取证在研究攻击的特征和发展趋势上起到关键性作用，只有当被捕获的攻击对象从攻击手段、攻击目的、攻击样本、攻击源等多方面进行风险的关联分析，才能够配合安全部门研究和抵御系统面临的或即将面临的威胁。

本次测试中，对各参测的蜜罐类产品在风险分析的相关功能上进行测试和验证。测试的方向包括入侵实时分析、攻击关联分析、关联威胁情报、样本信息展示、攻击维度分析和攻击事件分析等功能。

2. 测试结果情况

（1）入侵实时分析

入侵实时分析功能主要验证蜜罐是否支持威胁或入侵的实时分析判断，并可以持续跟踪攻击后续行为，发现入侵主机的黑客的攻击手法和采用的工具。

从测试结果来看，该测试项绝大部分产品测试结果较好，完全支持测试要求的产品高达 29 款，占全部收测产品的 85.29%。其余 5 款产品不支持此功能。

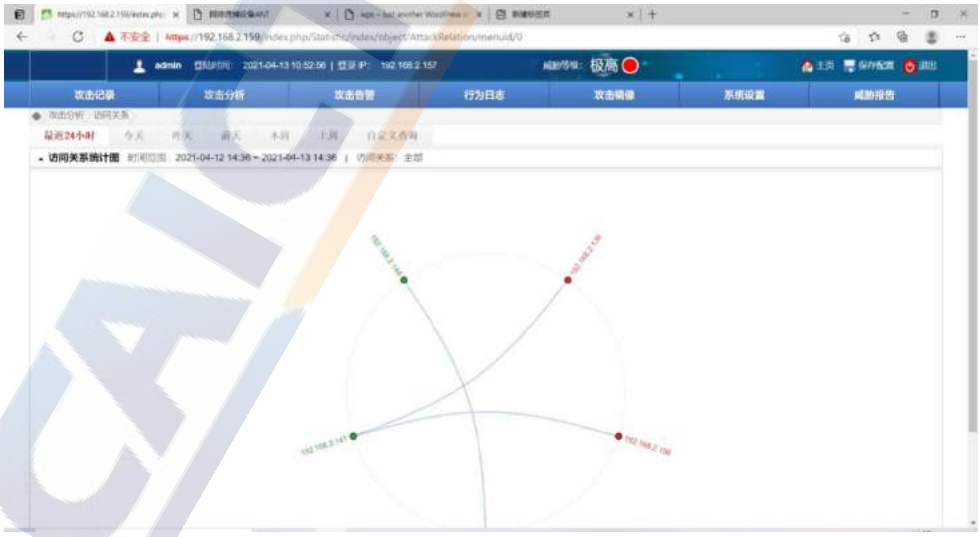
来源：中国信息通信研究院

图 40 某蜜罐产品功能界面图

（2）攻击关联分析

攻击关联分析功能主要验证蜜罐产品是否支持对攻击者进行关联分析，并以图表形式展示攻击者的攻击关系。

从测试结果来看，受测产品对于该项测试的结果支持率相对较好，其中 27 款完全满足测试要求，占全部测试产品的 79.41%。其余 7 款产品均为不支持或基本支持。



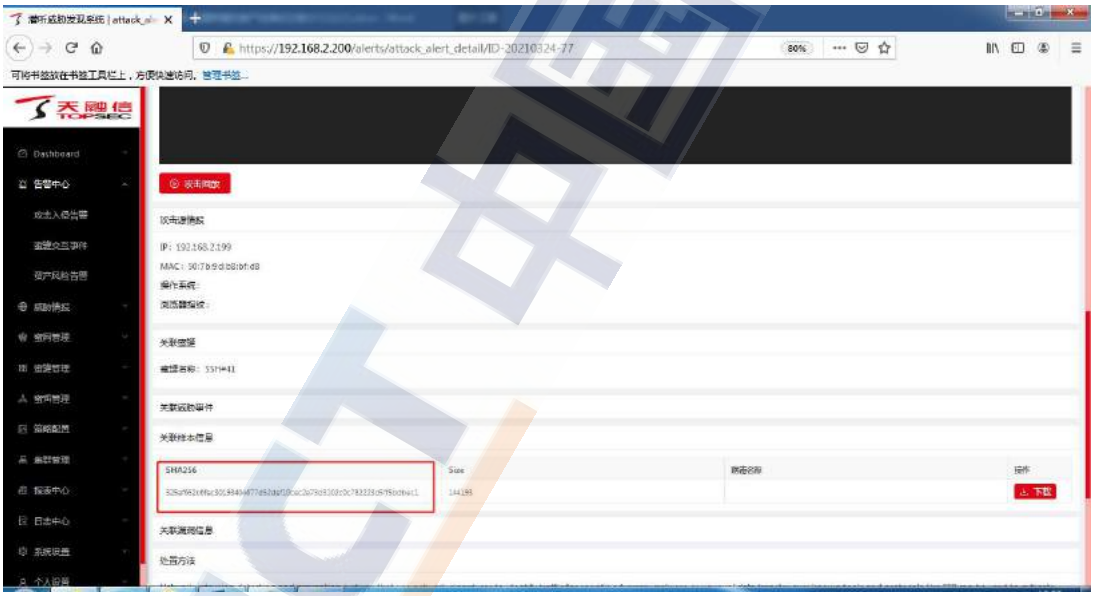
来源：中国信息通信研究院

图 41 某蜜罐产品功能界面图

（3）关联威胁情报

关联威胁情报功能主要验证蜜罐是否内置了威胁情报库，是否能够分析展示样本的详细关联文件情报，包括关联文件名、关联文件哈希、关联文件类型、关联文件家族信息、关联文件最后上传时间、关联类型信息等。

从测试结果来看，该测试项与上一节“情报产出”功能的测试结果一致，支持率普遍不高。其中完全支持的受测产品仅有 7 款，占全部受测产品的 20.59%，不支持测试要求的产品为 20 款，占比 58.82，其余 7 款产品为基本支持和支持较好。



来源：中国信息通信研究院

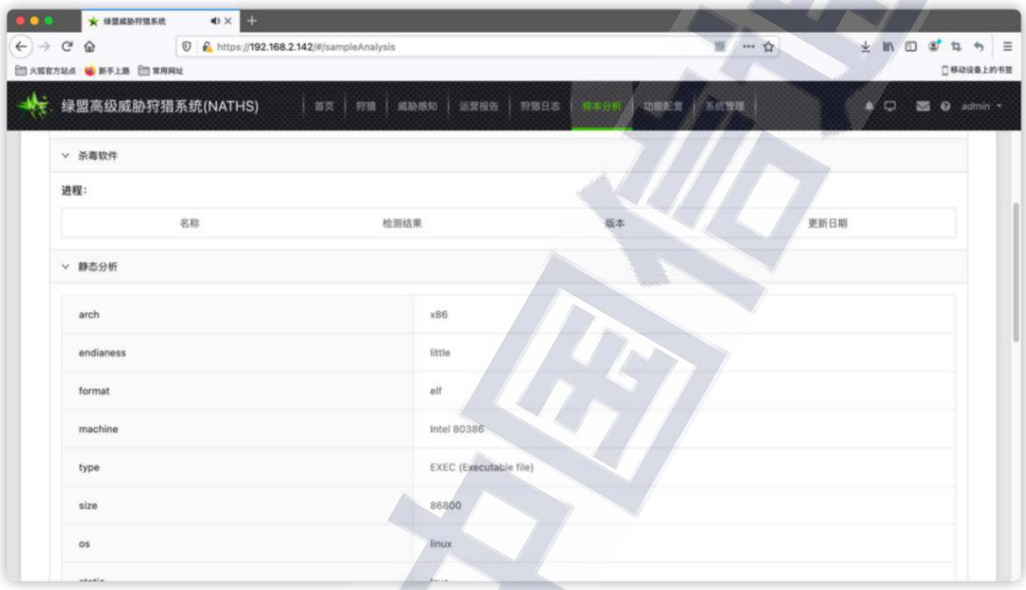
图 42 某蜜罐产品功能界面图

（4）样本信息展示

样本信息展示功能主要验证蜜罐是否能够分析展示样本的基本信息，包括威胁等级、样本类型、文件类型、MD5、编译时间、加

壳信息等；是否能够支持对样本的动态分析，分析结果包括但不限于动态行为描述、行为图、进程树、网络行为、截屏信息等。

从测试结果来看，该测试项仅有两款产品完全支持，占 34 款产品的 5.88%。19 款产品不具备此功能，占比 55.88%。基本支持的产品为 9 款，支持较好的为 4 款。



来源：中国信息通信研究院

图 43 某蜜罐产品功能界面图

（5）攻击维度分析

攻击维度分析功能主要验证蜜罐是否支持展示攻击者指纹信息、攻击动作、关联事件等不同维度信息。

从测试结果来看，该测试项的支持率总体较高，其中完全支持测试要求的产品为 30 款，占全部受测产品的 88.24%。其余产品均为部分支持。

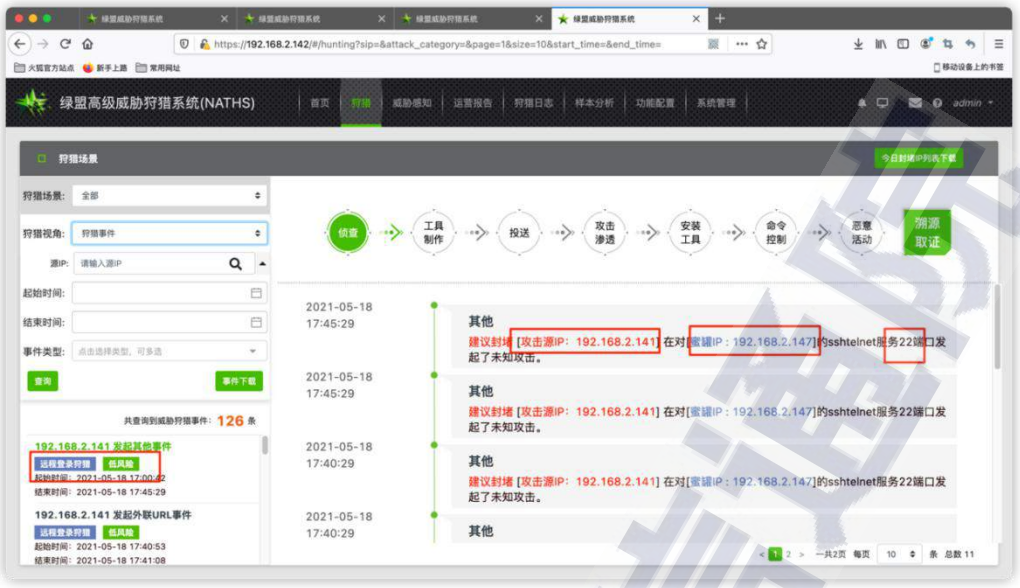
来源：中国信息通信研究院

图 44 某蜜罐产品功能界面图

（6）攻击事件分析

攻击事件分析功能主要验证蜜罐产品是否支持从事件角度，以列表形式对攻击事件进行展示，包括但不限于攻击时间、攻击源 IP、攻击目标、目标类型、攻击次数、风险等级、事件类型等。

此从测试结果来看，该测试项全部受测产品均可支持。其中，有 24 款产品完全支持测试要求，占受测产品的 71.59%，9 款产品为支持较好，1 款产品为基本支持。

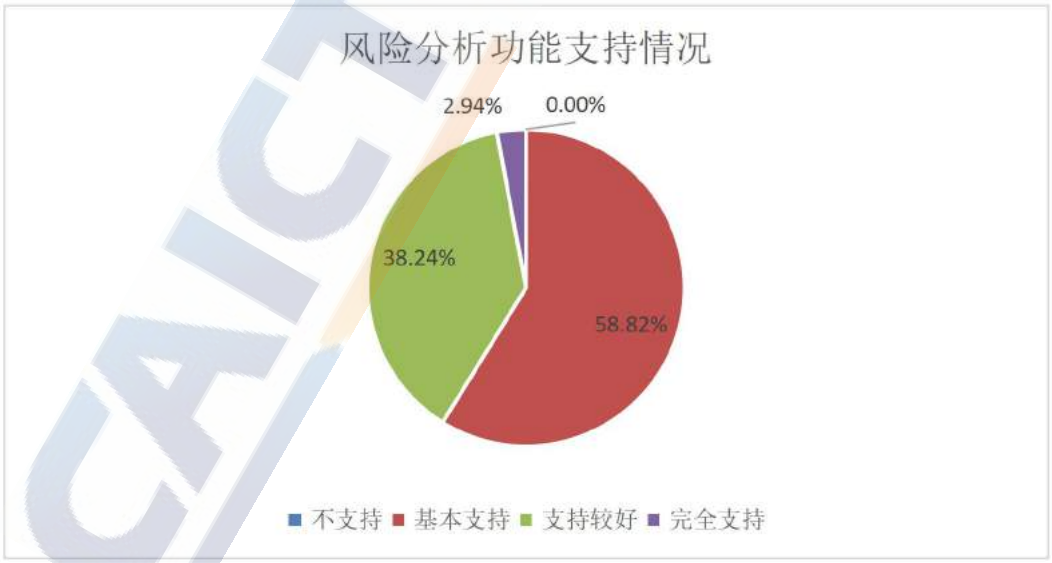


来源：中国信息通信研究院

图 45 某蜜罐产品功能界面图

3. 风险分析能力维度排名（前十）

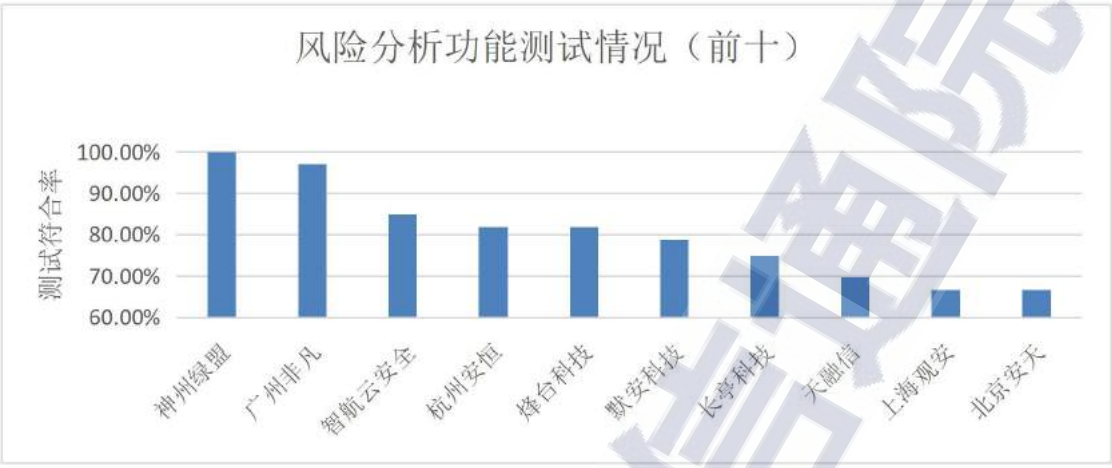
从风险分析功能总体支持情况来看，完全支持的产品虽然只有 1 款，但绝大部分产品都是支持较好和基本支持。未发现不支持测试要求的产品。



来源：中国信息通信研究院

图 46 风险分析功能支持情况

根据对 34 款产品的测试结果进行审核、分析和汇总，统计出针对蜜罐类产品风险分析功能支持率相对较好的十款产品，如下图。



来源：中国信息通信研究院

图 47 风险分析功能测试结果图

表 8 风险分析能力组

厂家	产品	型号	版本
北京神州绿盟科技有限公司	绿盟科技高级威胁狩猎	EDR-ATHNX3-HD1000	V5.0
广州非凡信息安全技术有限公司	幻影-攻击诱捕与威胁检测系统	okpot	V1.0
杭州智航云安全技术有限公司	智航蜜网	ZHHW-S-P	V3.1
杭州安恒信息技术股份有限公司	明鉴迷网系统	DAS-HPOT-3000	V2.0.9
烽台科技（北京）有限公司	灯塔安全威胁诱捕审计系统	ICS-TSS	V1.0
杭州默安科技有限公司	幻阵高级威胁检测系统	MoreSec-H	V2.8.3
北京长亭科技有限公司	长亭谛听（D-Sensor）内网威胁感应系统	DS-H40-M50	DS-H40-21.01.001
北京天融信网络安全技术有限公司	天融信潜听威胁发现系统	TopHPP	V3
上海观安信息技术股份有限公司	魅影威胁监测系统		V2
北京安天网络安全技术有限公司	捕风蜜罐系统 V3.0	ACS-POT-1000	V3.3.3.0

来源：中国信息通信研究院

（四）风险展示功能测试结果分析

1. 本节概述

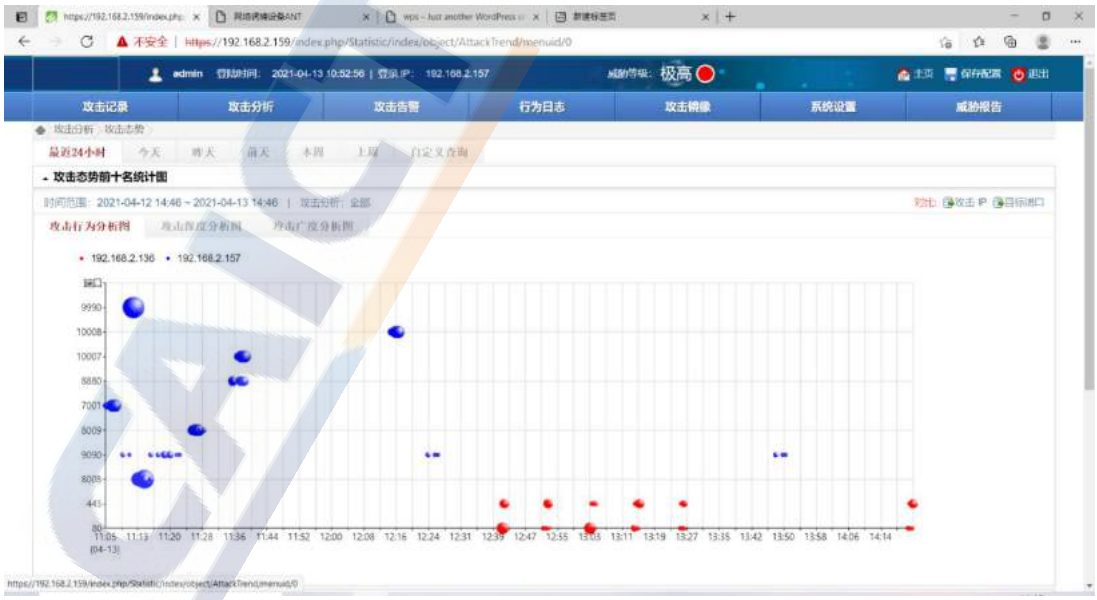
本次测试中，对各参测蜜罐类产品的风险展示功能进行测试和验证。测试的方向包括蜜罐监控分析、攻击事件分析和诱捕态势感知等功能。

2. 测试结果情况

（1）蜜罐监控分析

蜜罐监控分析功能主要验证蜜罐产品是否支持监控数据展示功能，以图形化和结构化方式展示蜜罐监控数据，并以时间、入侵事件、入侵源 IP、目标 IP、定期统计等多种角度呈现。

从测试结果来看，受测产品在该项的测试结果整体较好。其中 28 款产品完全支持测试要求，占受测产品的 82.35%。仅有 1 款产品不具备此功能，其余产品都对测试要求支持较好。



来源：中国信息通信研究院

图 48 某蜜罐产品功能界面图

（2）攻击事件分析

攻击事件分析功能主要验证蜜罐产品是否支持攻击事件分析以及数据统计展示。包含但不限于攻击方法收集、网络预警防御、入侵攻击取证展示等功能。能够包含但不限于对指定的攻击事件数据进行汇总统计，生成攻击事件报告，报告内容包含进程树、控制台监控、网络数据量统计等数据项以及攻击过程中关键节点行为描述。

从测试结果来看，该测试项有 13 款产品完全支持测试要求，占 34 款产品的 38.24%。4 款产品为支持较好、16 款产品为基本支持，仅有 1 款产品不具备此功能。

来源：中国信息通信研究院

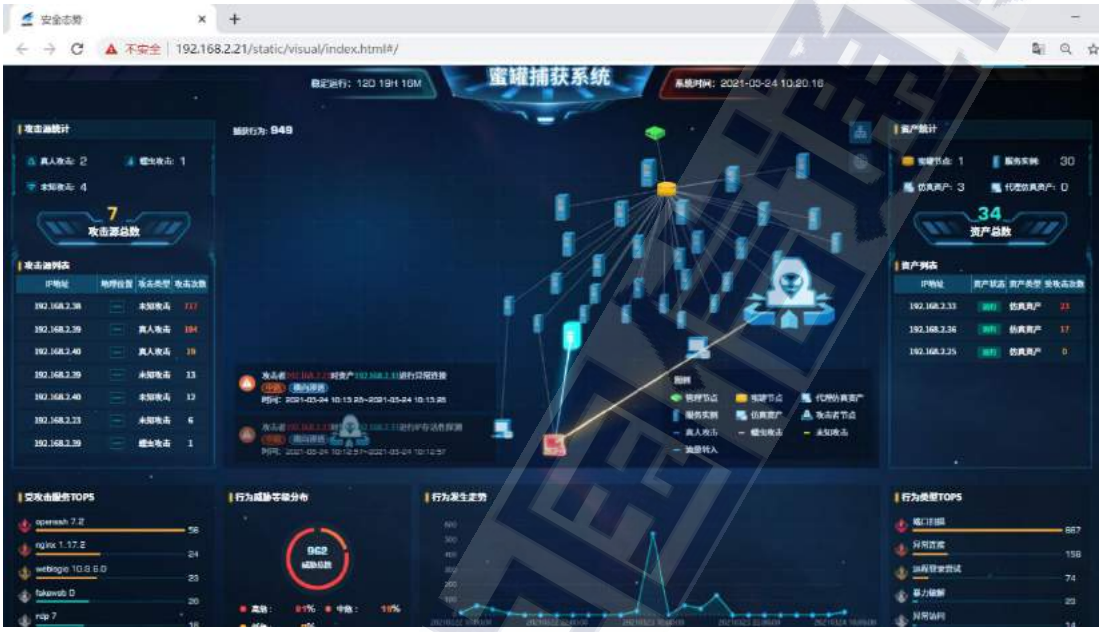
图 49 某蜜罐产品功能界面图

（3）诱捕态势感知

诱捕态势感知功能主要验证蜜罐产品是否支持诱捕态势大屏展示，包含但不限于体现各类蜜罐在业务拓扑中部署的位置、最新攻击告警、蜜罐类型分布、攻击源热力图、攻击事件分布、蜜罐进出

流量情况、攻击者分析及杀伤链等。

从测试结果来看，该测试项 7 款产品完全支持，占 34 款产品的 20.59%。10 款产品为支持较好、6 款产品为基本支持，其余 11 款产品不具备此功能。不具备此功能的产品占比 32.35%。

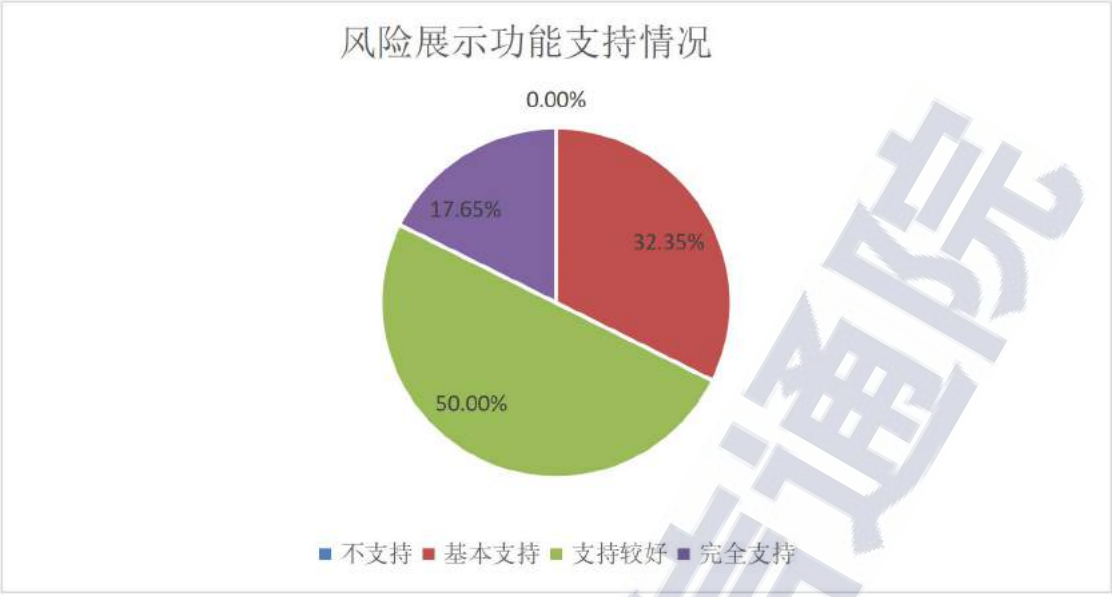


来源：中国信息通信研究院

图 50 某蜜罐产品功能界面图

3. 风险展示能力维度排名（前十）

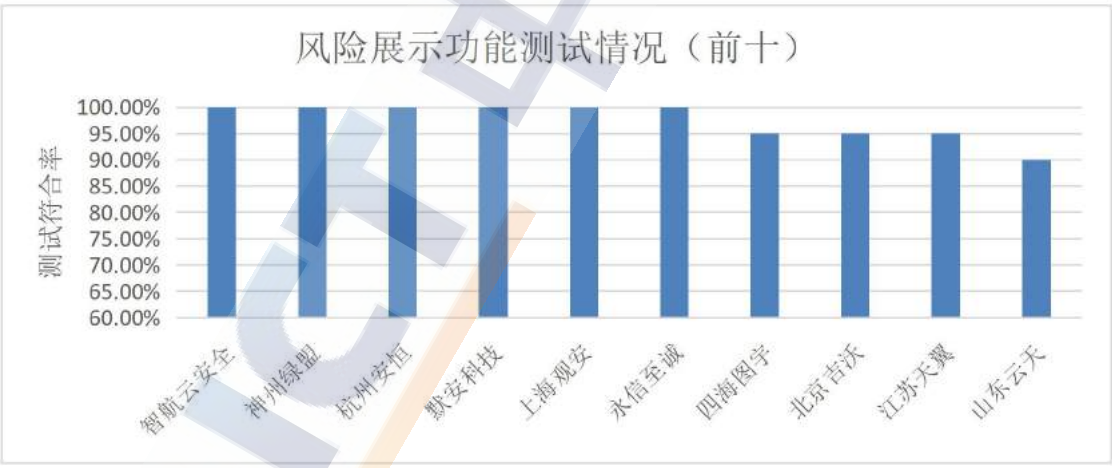
从风险展示功能总体支持情况来看，完全支持和支持较好的产品为 23 款，约占全部测试产品的 68%。基本支持的产品为 11 款，未发现不支持的产品。



来源：中国信息通信研究院

图 51 风险展示功能支持情况

根据对 34 款产品的测试结果进行审核、分析和汇总，统计出针对蜜罐类产品风险展示功能支持率相对较好的十款产品，如下图。



来源：中国信息通信研究院

图 52 风险展示功能测试情况

表 9 风险展示能力组

厂家	产品	型号	版本
杭州智航云安全技术有限公司	智航蜜网	ZHHW-S-P	V3.1
北京神州绿盟科技有限公司	绿盟科技高级威胁狩猎	EDR-ATHNX3-HD1000	V5.0
杭州安恒信息技术股份有限公司	明鉴迷网系统	DAS-HPOT-3000	V2.0.9
杭州默安科技有限公司	幻阵高级威胁检测系统	MoreSec-H	V2.8.3
上海观安信息技术股份有限公司	魅影威胁监测系统		V2
北京永信至诚科技股份有限公司	春秋云阵蜜罐系统	ECQYZ-HA	V2.0
北京四海图宇科技有限公司	天池蜜罐	FTS-TTA 680	FTS-TTA-680-V1.0
北京吉沃科技有限公司	智能仿真与诱捕防御系统	DecoyPro	V2.0
江苏天翼安全技术有限公司	幻视入侵感知与威胁溯源系统	h-sensor-8010	V2.9.3
山东云天安全技术有限公司	昊天工控蜜罐系统（工业仿真影子蜜网形态）	HT-HIS-HN 系列	2.0

来源：中国信息通信研究院

（五）蜜罐管理功能测试结果分析

1. 本节概述

本次测试中，对各参测的蜜罐类产品在管理功能上进行测试和验证。测试的方向包括蜜罐节点信息和节点操作、镜像管理和场景模板管理、蜜饵管理和漏洞管理、拓扑和其他相关管理等功能。

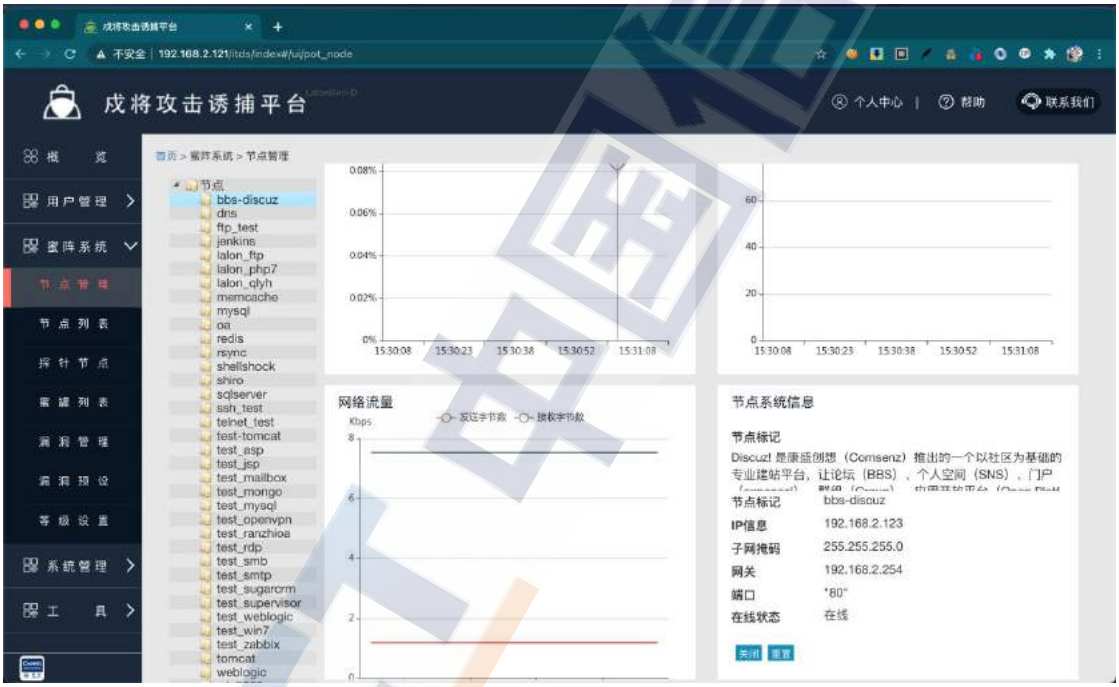
2. 测试结果情况

（1）节点信息和节点操作

节点信息和节点操作功能主要验证蜜罐产品是否支持展示已部

署的蜜罐节点的相关信息，包括但不限于蜜罐名称、蜜罐 IP、蜜罐镜像、部署区域、受攻击次数、状态、CPU、内存和磁盘利用情况等；验证是否支持对已部署的运行状态下的蜜罐节点进行操作，包括但不限于删除、暂停、停止、运行等。

从测试结果来看，该测试项总体支持率较高。其中有 18 款产品完全支持测试要求，占 34 款产品的 52.94%。15 款产品为支持较好，1 款产品为基本支持，未发现不支持此测试要求的产品。



来源：中国信息通信研究院

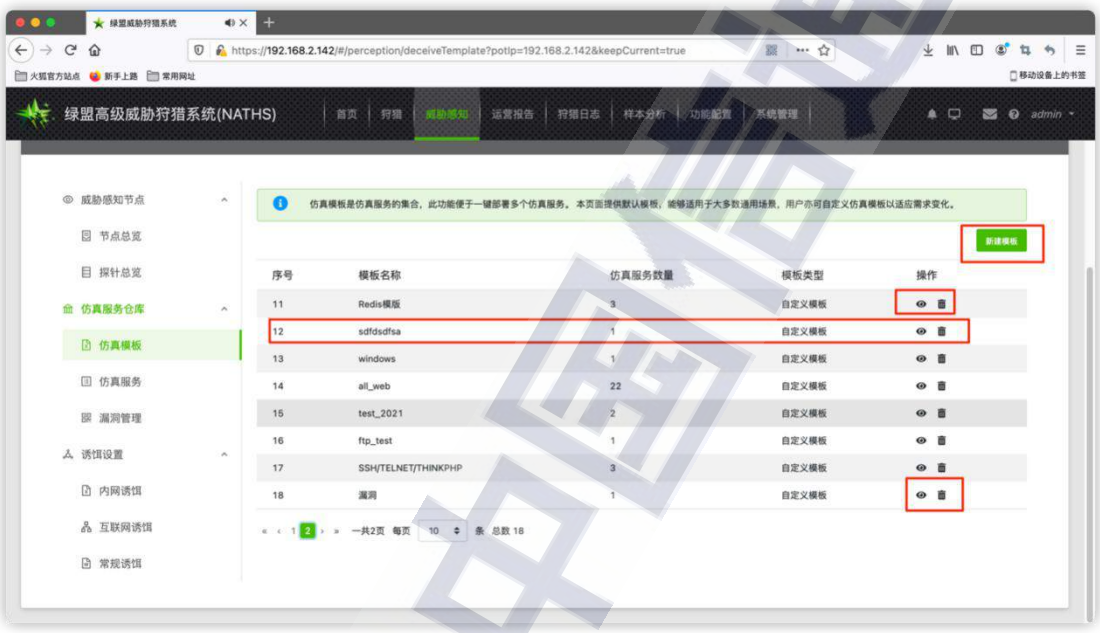
图 53 某蜜罐产品功能界面图

（2）镜像管理和场景模板管理

镜像管理和场景模板管理功能主要验证蜜罐产品是否支持蜜罐镜像的管理，包含但不限于支持导入、删除、查看镜像详情、部署蜜罐节点等功能；验证是否支持场景模板的管理，包含但不限于支

持自定义场景模板、按照场景模板批量部署蜜罐、删除场景模板等功能。

从测试结果来看，该测试项有 11 款产品完全支持测试要求，占 34 款产品的 32.35%，支持较好的产品为 7 款，基本支持的产品为 10 款，其余 6 款产品不具备此功能。



来源：中国信息通信研究院

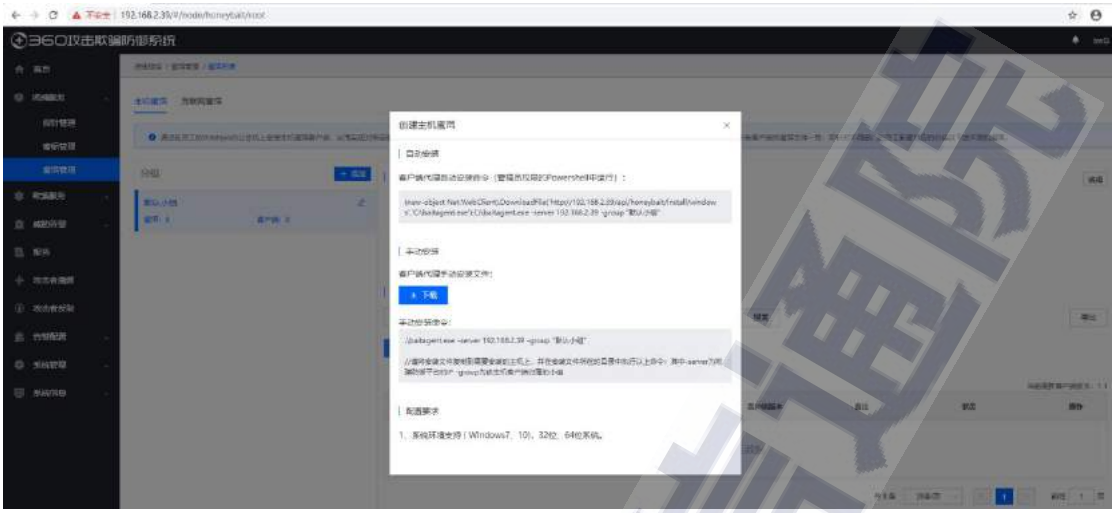
图 54 某蜜罐产品功能界面图

（3）蜜饵管理和漏洞管理

蜜饵管理和漏洞管理功能主要验证蜜罐产品是否支持对文件蜜饵、GitHub 蜜饵进行操作，包括但不限于新增、删除、下载、编辑等功能；验证是否支持漏洞管理，包含但不限于导入、删除、查看 POC、查看漏洞详情等操作。

从测试结果来看，该测试项有 6 款产品完全支持测试要求，占 34 款产品的 17.65%，支持较好的产品为 5 款，基本支持的产品为

15 款，其余 8 款产品不具备此功能。



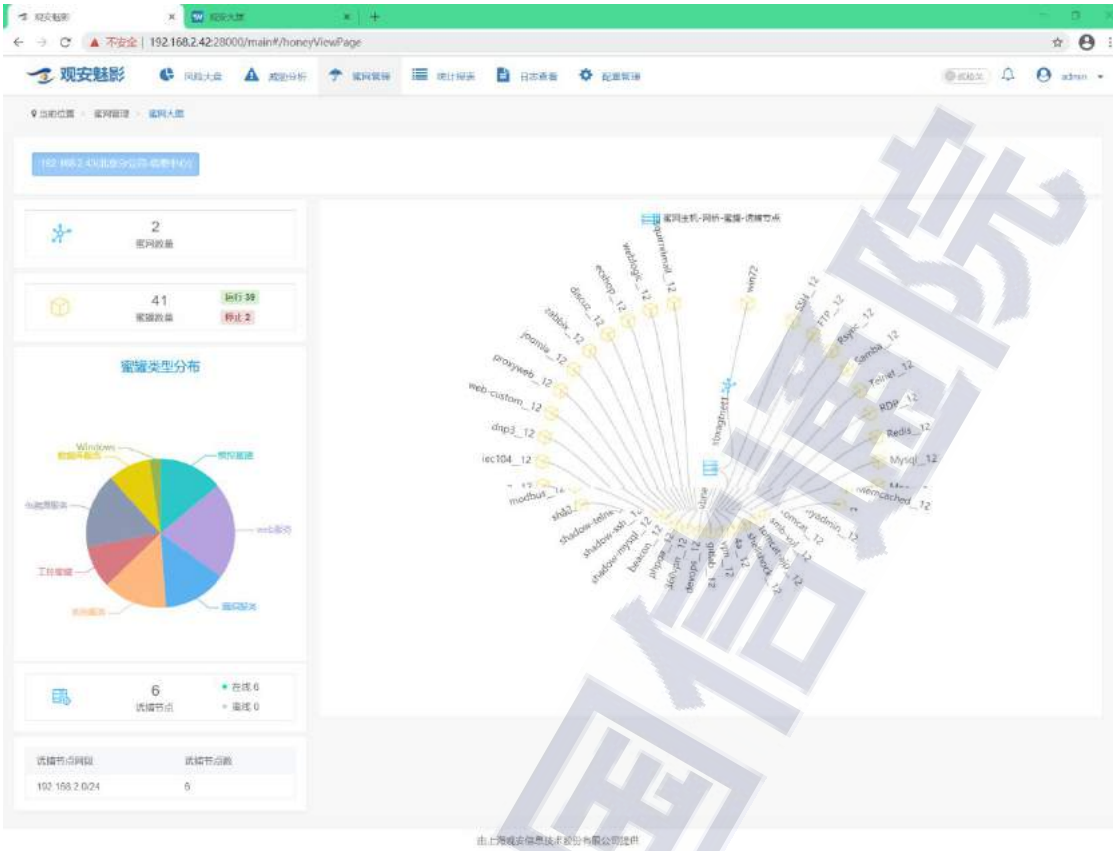
来源：中国信息通信研究院

图 55 某蜜罐产品功能界面图

（4）拓扑功能

拓扑功能主要验证蜜罐是否支持自定义诱捕拓扑绘制，并支持在大屏展示；另一方面验证是否支持自动生成蜜罐节点拓扑，直观展示蜜罐节点、蜜饵、流量转发 Agent 等关联信息。

从测试结果来看，该测试项有 11 款产品完全支持测试要求，占 34 款产品的 32.35%，支持较好的产品为两款，基本支持的产品为 7 款，其余 14 款产品不具备此功能。



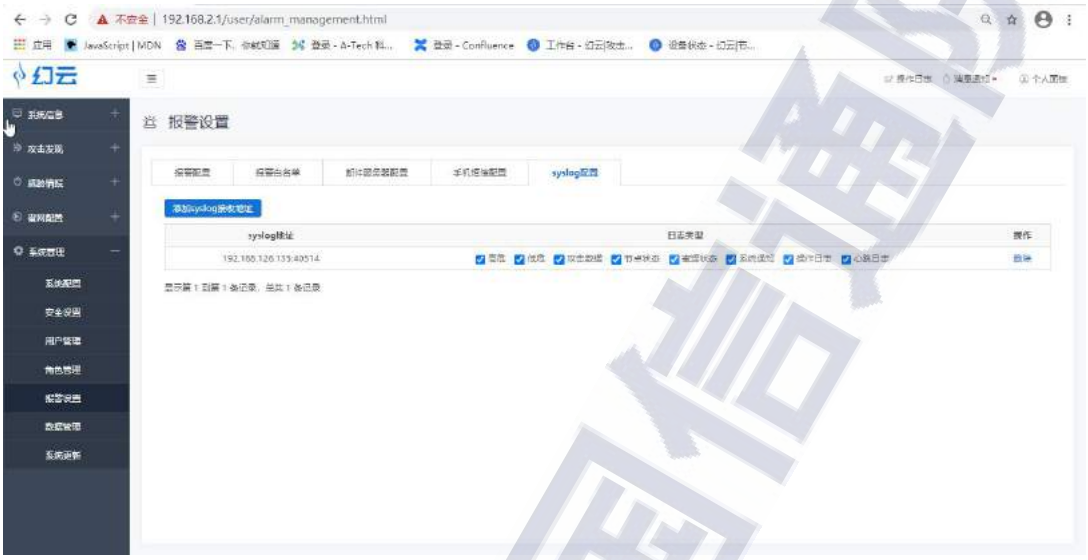
来源：中国信息通信研究院

图 56 某蜜罐产品功能界面图

（5）其他管理功能

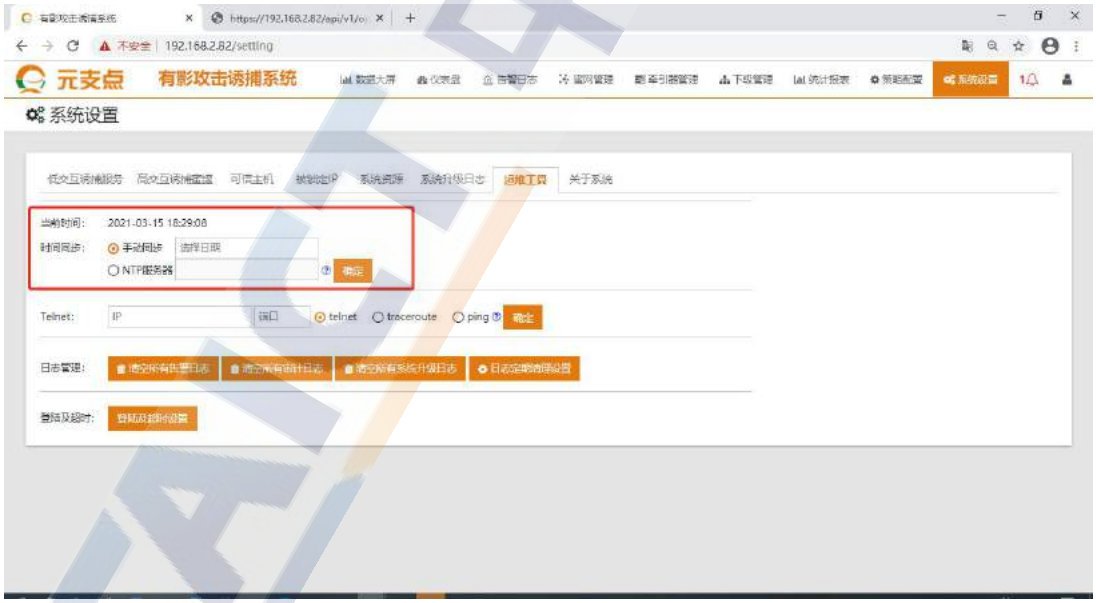
本次测试中，对于蜜罐的管理功能进行了测试验证，包括但不限于联动功能、时间校准、机构管理等。其中，联动功能是指第三方平台联动功能，比如通过 SYSLOG 推送威胁情报数据，并且支持与防火墙联动，完成网络阻断；时间校准功能要求受测产品支持系统时间管理，可通过 NTP 服务器、同步本机时间、自定义时间等方式校正时间；机构管理要求受测产品应支持使用单位的组织机构管理，可访问机构管理界面、通过机构下划诱捕节点、蜜罐主机及区域。

从测试结果来看，该测试项有 5 款产品完全支持测试要求，占 34 款产品的 14.7%，支持较好的产品为 9 款，基本支持的产品为 19 款，其余 1 款产品不具备此功能。



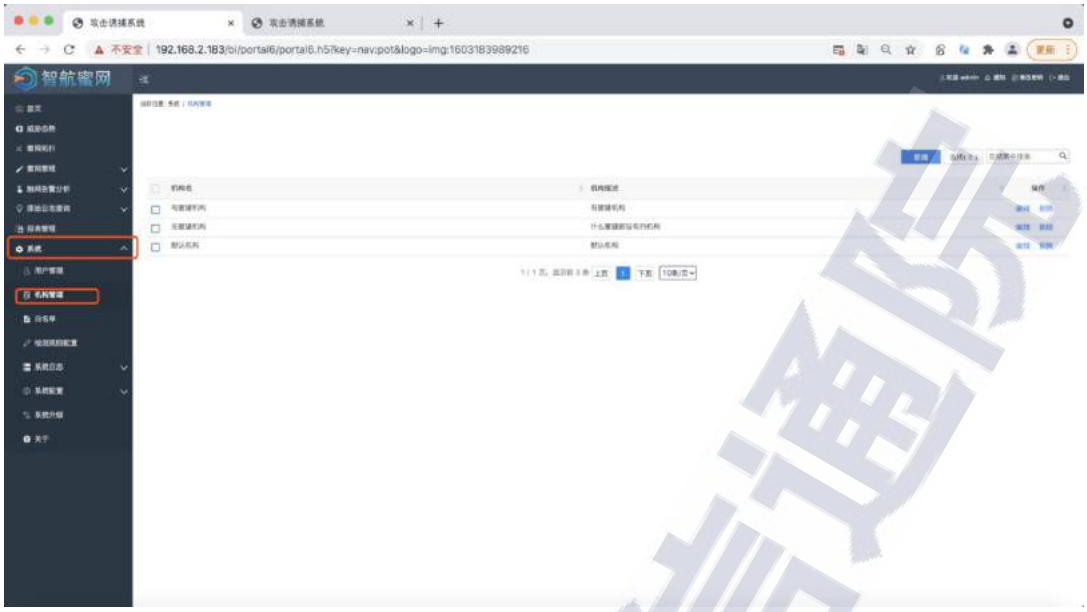
来源：中国信息通信研究院

图 57 某蜜罐产品功能界面图



来源：中国信息通信研究院

图 58 某蜜罐产品功能界面图

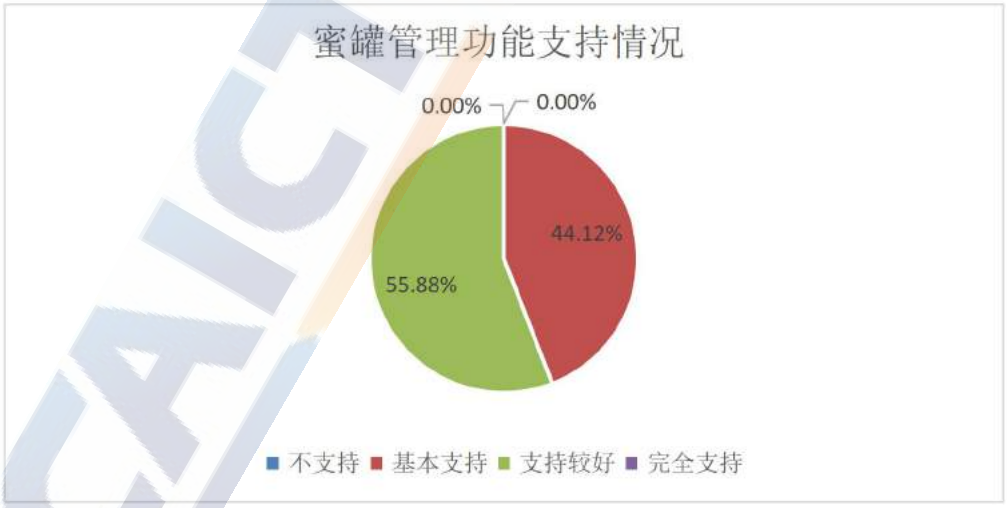


来源：中国信息通信研究院

图 59 某蜜罐产品功能界面图

3. 蜜罐管理能力维度排名（前十）

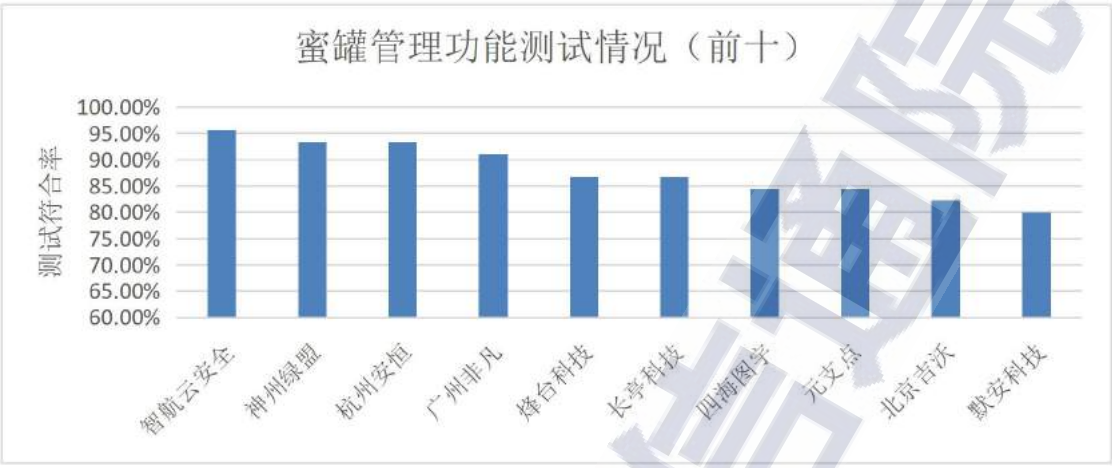
从蜜罐管理功能总体支持情况来看，虽然没有完全支持测试要求的受测产品，但也未发现不支持的产品。支持较好的产品为 19 款，基本支持的产品为 15 款。



来源：中国信息通信研究院

图 60 蜜罐管理功能支持情况

根据对 34 款产品的测试结果进行审核、分析和汇总，统计出针对蜜罐类产品服务伪装功能支持率相对较好的十款产品，如下图。



来源：中国信息通信研究院

图 61 蜜罐管理功能测试情况

表 10 蜜罐管理能力组

厂家	产品	型号	版本
杭州智航云安全技术有限公司	智航蜜网	ZHHW-S-P	V3.1
北京神州绿盟科技有限公司	绿盟科技高级威胁狩猎	EDR-ATHNX3-HD1000	V5.0
杭州安恒信息技术股份有限公司	明鉴迷网系统	DAS-HPOT-3000	V2.0.9
广州非凡信息安全技术有限公司	幻影-攻击诱捕与威胁检测系统	Okpot	V1.0
烽台科技（北京）有限公司	灯塔安全威胁诱捕审计系统	ICS-TSS	V1.0
北京长亭科技有限公司	长亭谛听（D-Sensor）内网威胁感应系统	DS-H40-M50	DS-H40-21.01.001
北京四海图宇科技有限公司	天池蜜罐	FTS-TTA 680	FTS-TTA-680-V1.0
北京元支点信息安全技术有限公司	有影攻击诱捕系统	YZD-DP-001	V3
北京吉沃科技有限公司	智能仿真与诱捕防御系统	DecoyPro	V2.0

杭州默安科技有限公司	幻阵高级威胁检测系统	MoreSec-H	V2.8.3

来源：中国信息通信研究院

（六）安全性功能测试结果分析

1. 本节概述

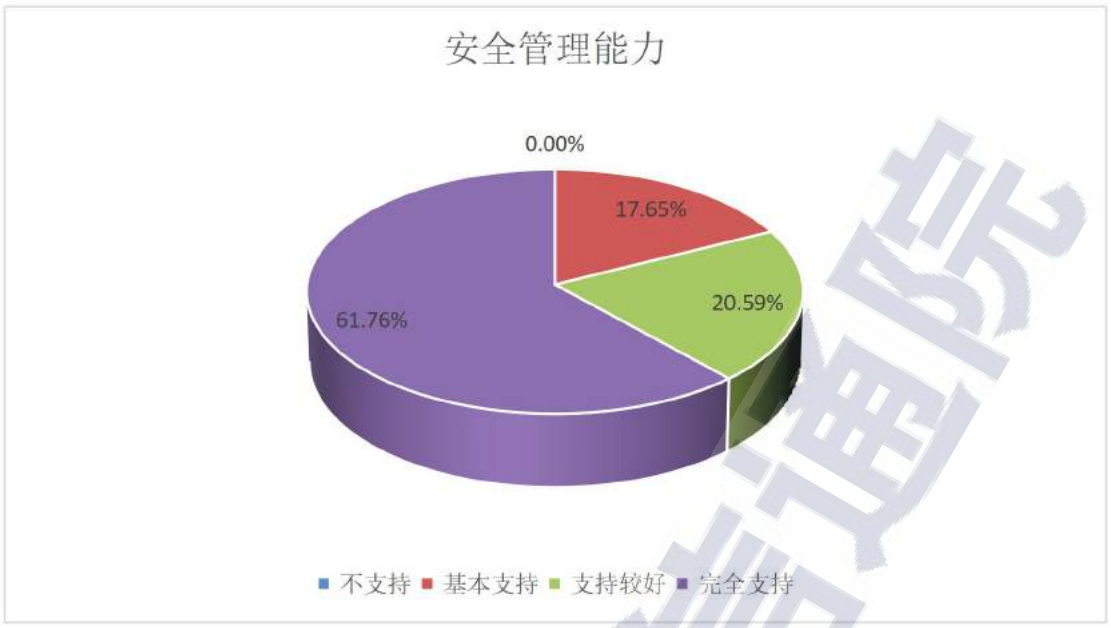
本次测试中，对各参测的蜜罐类产品在安全性的相关功能上进行测试和验证。测试主要包括安全管理能力、用户标识与鉴别和响应处理等功能。

2. 测试结果情况

（1）安全管理

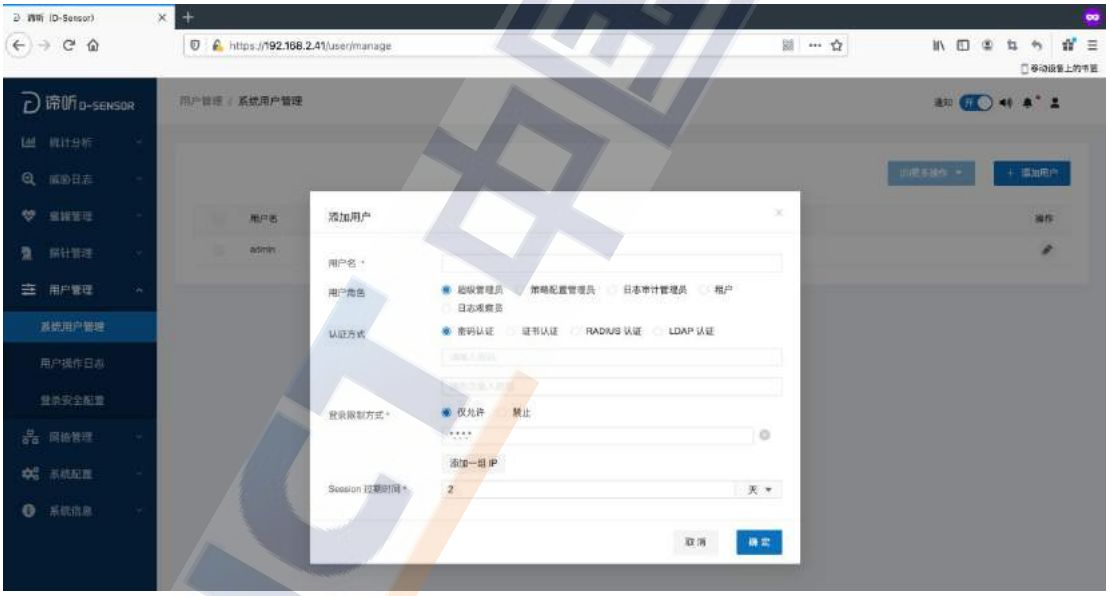
安全管理功能主要验证蜜罐产品是否具备与安全管理相关的功能，包括安全角色管理、远程保密传输、可信管理主机、系统可用性监测等功能。

从测试结果来看，该测试项总体支持率较高。其中有 21 款产品完全支持测试要求，占 34 款产品的 61.76%。7 款产品为支持较好，其余 6 款产品为基本支持，未发现不支持此测试要求的产品。从总体上看，国内的安全企业在安全管理的基础能力上已经具备一定的意识并体现在各自的安全产品的相关功能中。



来源：中国信息通信研究院

图 62 安全管理能力支持情况



来源：中国信息通信研究院

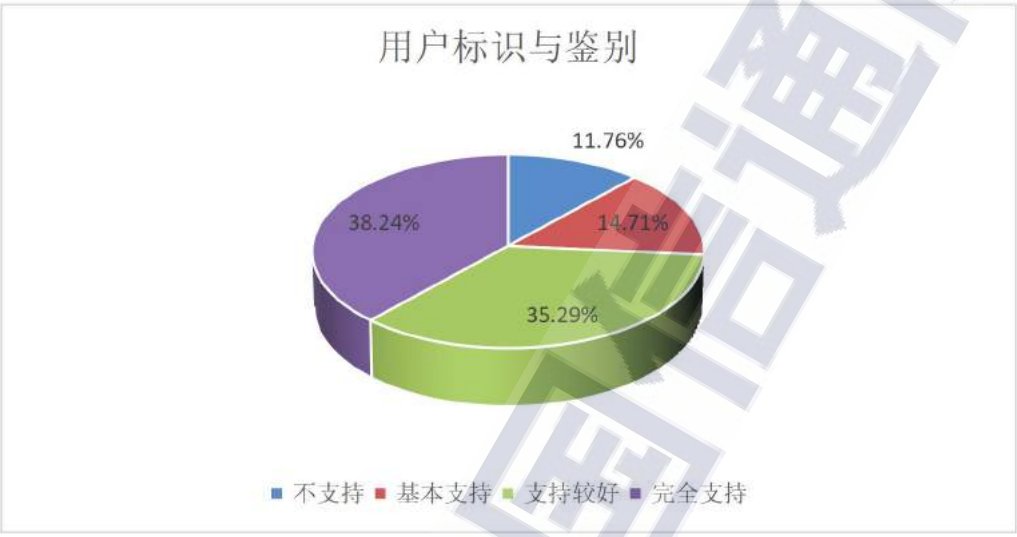
图 63 某蜜罐产品功能界面图

（2）用户标识与鉴别

用户标识与鉴别功能主要验证蜜罐产品的管理员属性、权限、唯一标识等功能设置是否完备；用户身份鉴别能力、数据查阅修改

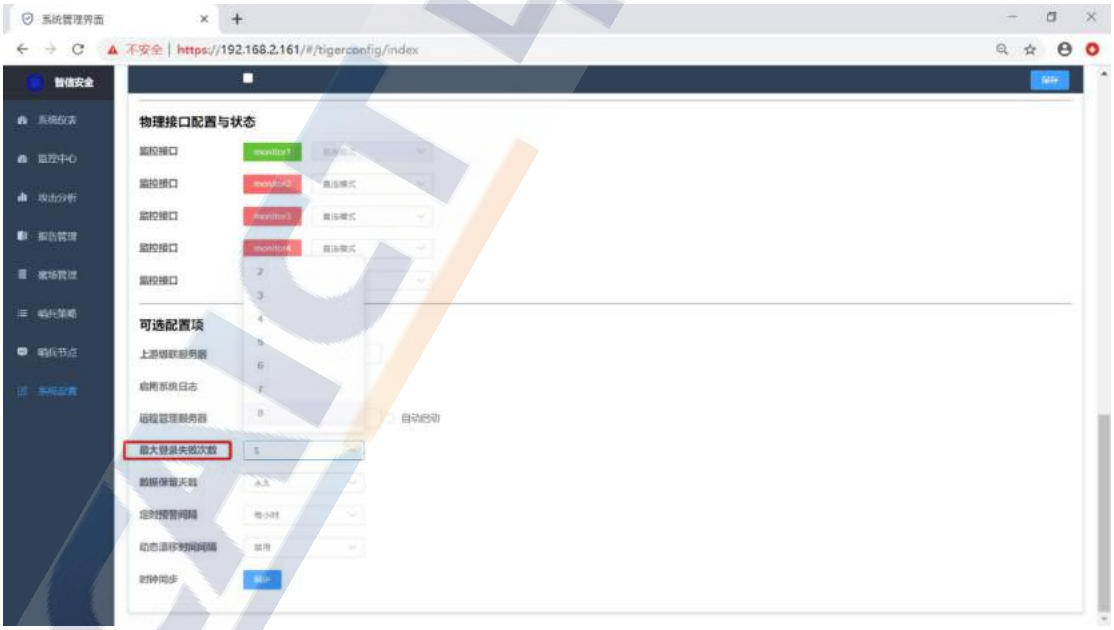
权限鉴别能力、鉴别失败处理机制是否合理等。

从测试结果来看，有 13 款产品完全支持测试要求，占 34 款产品的 38.24%。12 款产品为支持较好，5 款产品为基本支持。仍存在 4 款产品完全不支持该功能，占比 11.76%。



来源：中国信息通信研究院

图 64 用户标识与鉴别支持情况



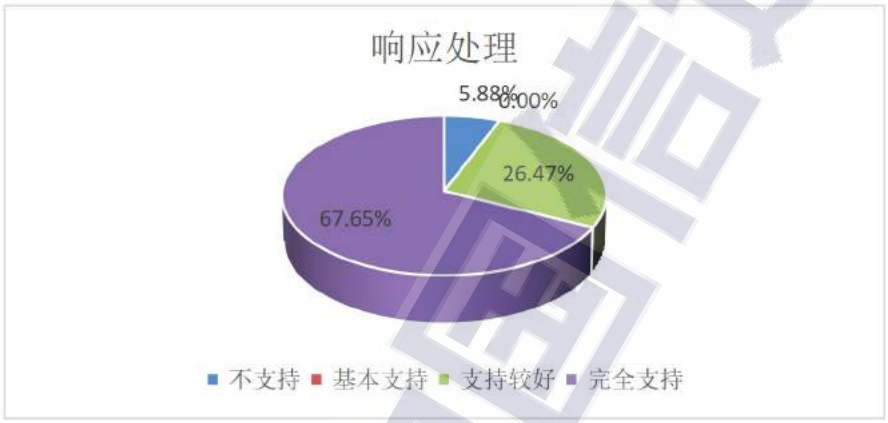
来源：中国信息通信研究院

图 65 某蜜罐产品功能界面图

（3）响应处理

响应处理功能主要验证蜜罐产品告警信息的丰富性和告警配置的灵活性以及针对安全威胁事件记录的安全性和完善度等。

从测试结果来看，有 23 款产品完全支持测试要求，占 34 款产品的 67.65%。9 款产品为支持较好，其余 2 款产品完全不支持该功能，占比 5.88%。



来源：中国信息通信研究院

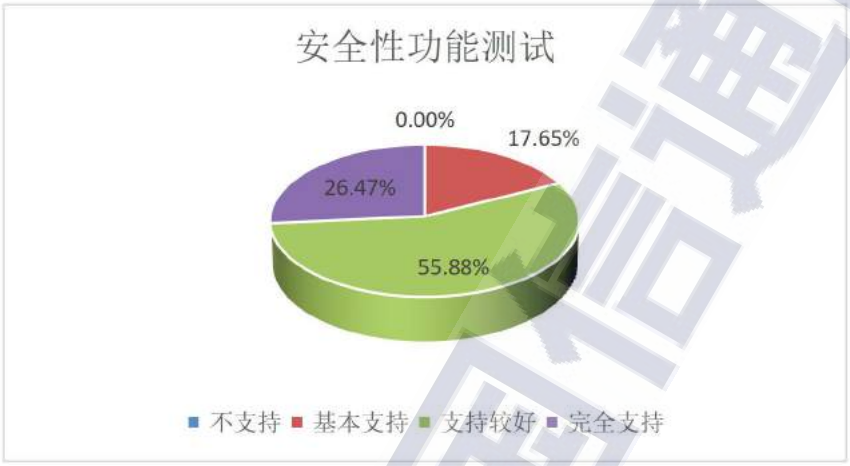
图 66 响应处理能力支持情况

来源：中国信息通信研究院

图 67 某蜜罐产品功能界面图

3. 蜜罐安全性维度排名（前十）

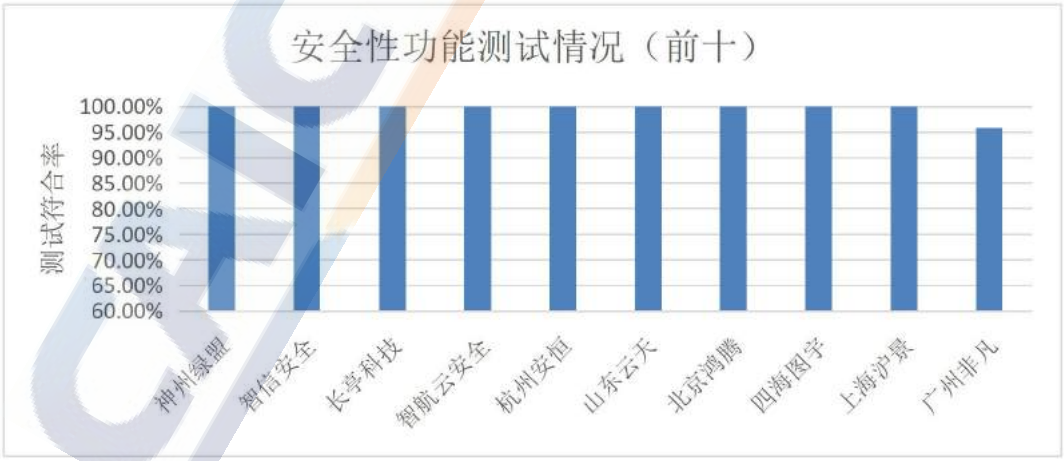
从蜜罐安全性相关功能的总体支持情况来看，完全支持的为 9 款产品和支持较好的产品为 23 款，约占全部测试产品的 68%。基本支持的产品为 11 款，未发现不支持的产品。



来源：中国信息通信研究院

图 68 安全性功能测试支持情况

根据对 34 款产品的测试结果进行审核、分析和汇总，统计出针对蜜罐类产品风险展示功能支持率相对较好的十款产品，如图 69 所示。



来源：中国信息通信研究院

图 69 安全性功能测试情况

表 11 蜜罐安全性能力组

厂家	产品	型号	版本
北京神州绿盟科技有限公司	绿盟科技高级威胁狩猎	EDR-ATHNX3-HD1000	V5.0
北京智仁智信安全技术有限公司	魔境网络安全预警系统	I7000	NSA-V1.0
北京长亭科技有限公司	长亭谛听（D-Sensor）内网威胁感应系统	DS-H40-M50	DS-H40-21.01.001
杭州智航云安全技术有限公司	智航蜜网	ZHHW-S-P	V3.1
杭州安恒信息技术股份有限公司	明鉴迷网系统	DAS-HPOT-3000	V2.0.9
山东云天安全技术有限公司	昊天工控蜜罐系统（工业仿真影子蜜网形态）	HT-HIS-HN 系列	2.0
北京鸿腾智能科技有限公司	360 攻击欺骗防御系统	NT-HP1010-C-HS	V2.0.1
北京四海图宇科技有限公司	天池蜜罐	FTS-TTA 680	FTS-TTA-680-V1.0
上海沪景信息科技有限公司	网络威胁诱捕系统	ANT8220	V1.0
广州非凡信息安全技术有限公司	幻影-攻击诱捕与威胁检测系统	okpot	V1.0

来源：中国信息通信研究院

（七）性能测试结果分析

本次测试中，除对蜜罐类产品在功能和安全性上进行测试和验证外，还对蜜罐类产品的性能进行了测试。主要包含如表 12 所示的相关测试项。

表 12 性能测试项

序号	性能测试项
1	设备预警安全事件与安全事件发生的时间间隔（秒）
2	安全事件的识别速度（个/秒）
3	单台设备至少支持同时开启的高交互蜜罐数量（个）
4	蜜罐场景启动及切换（秒）

5	页面响应速度（秒）
6	捕获行为数量（种）
7	设备可识别的木马家族数量（个）
8	内置检测规则（万条）
9	内置威胁情报（万条）
10	内置 IP 库（万条）
11	内置漏洞模板（条）

来源：中国信息通信研究院

从蜜罐的部署目的和方式来看，蜜罐类产品的性能要求并非是该类产品的关键性指标。蜜罐产品并非流量节点型设备，也不承载过多的访问负载。因此在本次测试中，一方面从安全事件的识别速度、预警速度、蜜罐场景切换速度和页面响应速度进行测试验证；另一方面，验证蜜罐类产品自身威胁情报的赋能，比如：捕获行为数量、可识别的木马家族数量、内置检测规则、内置威胁情报、内置 IP 库和内置漏洞模板等。

考虑到蜜罐类产品的性能并非关键性指标，各企业参测产品在上述性能的测试项上也有着不同的规划，本次蜜罐类产品的性能测试采用“开放性测试”，即不限制测试方法和测试过程，各参测企业针对所列测试项，通过各自的测试方法得出结论并留存测试记录和截图。

从本次测试的结果来看，因未限定测试方法，各产品的性能测试结果上下限差别较大。

比如：对于蜜罐场景启动及切换时间的测试，部分产品自身在

“蜜罐内置场景”功能上做的十分成熟，内置了成熟的场景模板并包含了多个蜜罐节点，而另外一些产品只有简单的场景模板。这导致了蜜罐节点的场景启动和切换时间上的较大差别，因此测试结果不能做到有效评估。

此外，关于威胁情报的相关测试项中，本次测试要求相关情报库均为“内置”，如“内置 IP 库”、“内置威胁情报库”等。根据测试结果发现，半数以上的蜜罐产品不具备“内置”相关威胁情报库，而是采用“外部威胁情报”进行关联分析。目前，外部“威胁情报平台”类产品或“在线威胁情报中心”的模式发展较为成熟，蜜罐类产品作为诱导、捕获和分析攻击行为的产品，既需要关联现有威胁情报以便于做出更加精准的威胁判断，同时也是威胁情报产出的重要手段。因此，国内蜜罐类产品在未来的产品迭代演进中，在威胁情报的种类、数量、质量、即时性等方面，应加强从情报产出、到情报关联的相关功能。

七、蜜罐类产品部分特色功能验证

当前的网络安全威胁不断演进、迭代，攻击手段层出不穷、攻击目标多种多样，特别是高级持续性攻击隐蔽性很强。在攻防博弈过程中，蜜罐类产品为打破攻防平衡，也在逐渐开发新的技术、适应新的场景。

报告中通过对国内蜜罐类产品的市场调研，并进一步的测试验证，发现在当前国内主要的蜜罐类产品中，有一部分产品在具备传统的威胁诱捕基础能力外，开拓了具有一定特色的功能或模块，能

够通过不同维度的技术能力为最终应用场景带来更多元的安全赋能。

（一）基于自适应的智能化动态诱捕——智信安全

在进行宽范围部署的前提下，对大量蜜罐节点进行诱捕策略配置，是蜜罐类产品实施过程中遇到的一个大痛点，如果能够实现自动化配置、保证快速地实现大量蜜罐节点的诱捕策略配置，可以显著降低蜜罐部署过程中，以及后续蜜罐诱捕策略调整过程中的工作量。

北京智仁智信安全技术有限公司的魔境网络安全预警系统（I7000 NSA-V1.0）是面向企业内网的横向攻击预警需求开发的一款蜜罐诱捕产品。其中**自适应智能诱捕技术**是该产品的一个比较有特色的功能，该项技术已取得相关专利。

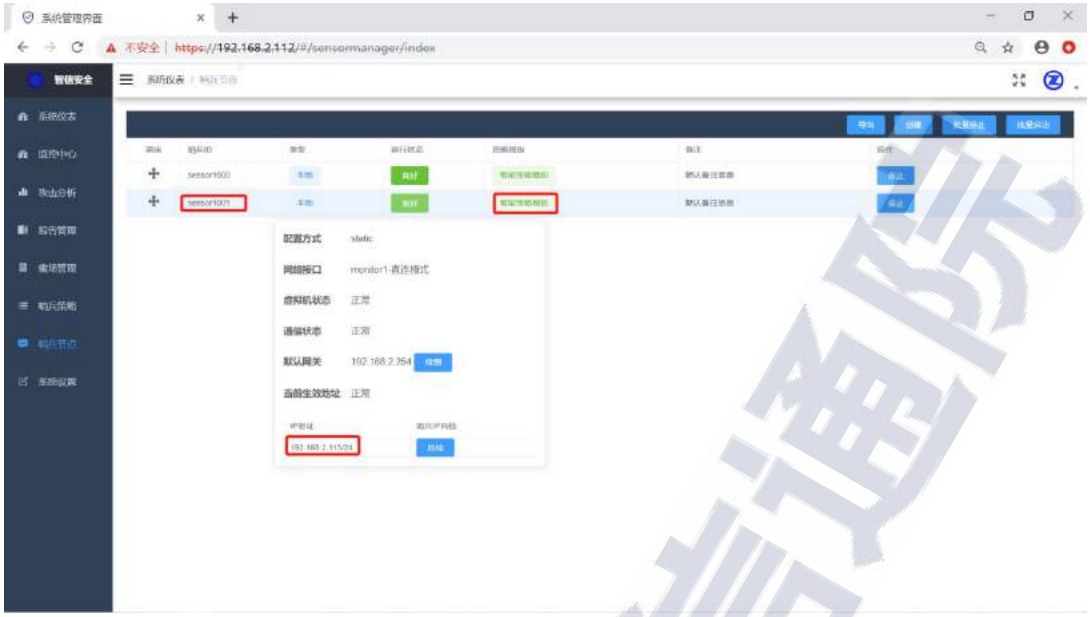
在蜜罐类产品的部署环境中，静态的蜜罐诱捕策略与攻击者意图不确定性之间存在巨大矛盾。简单地说就是蜜罐开放的端口和服务，很大程度上并不是攻击者想要的。因为这个矛盾的存在，蜜罐系统一直无法摆脱只能"守株待兔"的低效诱捕局面，以静态的蜜罐诱捕场景面对不确定的攻击意图，这个弊病会导致错失大量诱捕机会，导致诱捕率低下。自适应智能诱捕技术打破了传统诱捕技术以预设静态场景为基础的诱捕思路，**用不确定性对抗不确定性**。对全网的蜜罐节点不预设任何静态诱捕策略，而以攻击者行为为驱动，进行诱捕策略实时判决，实时生成具有高诱惑力的诱捕策略，提升诱捕成功率。

该产品的技术架构如下图所示：

来源：智信安全

图 70 智信蜜罐架构图

设备内部架构采用松耦合、分层结构搭建，从上到下依次为可扩展蜜罐服务资源池、智能策略编排引擎、虚拟蜜罐节点层、网络接入层。蜜罐服务资源池给智能策略编排引擎提供场景素材，支撑其进行诱捕策略编排；智能策略编排引擎给蜜罐节点层提供诱捕策略支撑，实现在蜜罐节点上输出动态、丰富、逼真的交互场景；网络接入层是虚拟蜜罐节点层与真实网络之间的媒介层，最终完成蜜罐节点在真实网络中的投放。



来源：智信安全

图 71 智信蜜罐测试界面图

产品在自适应智能诱捕技术上，主要有如下特点：

- 在批量部署的条件下，为每个蜜罐实时生成诱捕策略，同一个蜜罐面对不同攻击源体现出不同交互形态，实现了多态智能蜜罐；
- 动态智能策略可以保持每个蜜罐的诱捕策略处于动态的最佳状态，诱捕率明显提升；
- 全网诱捕策略免配置，在启用智能诱捕技术后无需再进行任何静态诱捕策略配置，该特性降低了系统的总持有成本。

智信安全的“新一代网络安全预警系统”，运用了自适应智能化动态诱捕功能，在低成本、大规模、自动化部署能力上，具有一定产品能力。为现有威胁诱捕类产品建设方案，提供了较好的发展方向。

（二）面向工控环境的蜜罐产品——山东云天

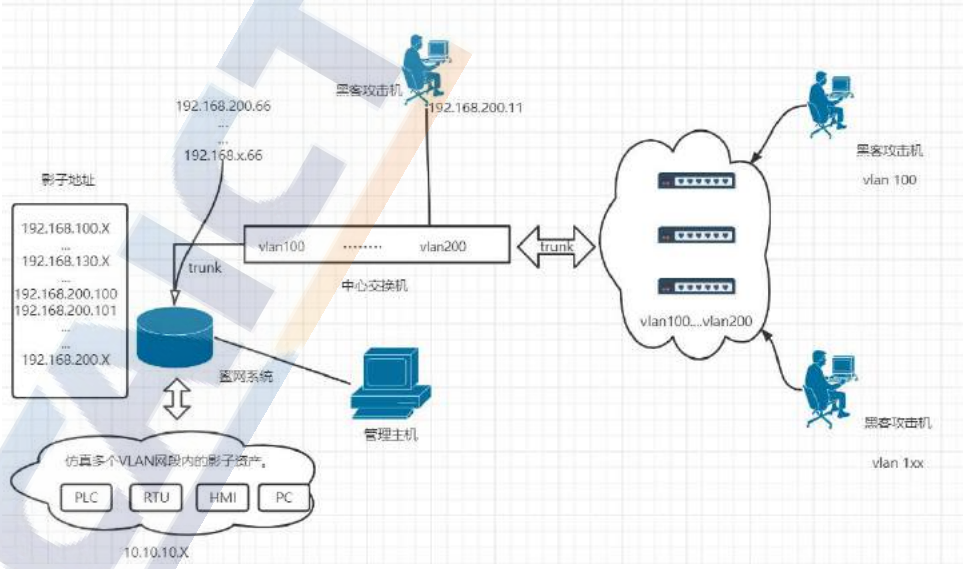
昊天工控蜜罐系统是云天安全自主研发的基于工控环境的欺骗防御和威胁情报产品。由于在工业网络场景下对 CIA 中的 A（可用性）要求极高，为适应工业网络安全并与传统网络安全相区别，该产品不主动产生和发送任何网络数据包。设计采用纯被动方式，通过定制化批量部署适用于各工业场景的多类型诱饵探针作为陷阱，诱使攻击方实施攻击并隔离攻击，及时发现威胁并告警。蜜罐对攻击行为进行捕获分析，清晰了解工业网内面对的安全威胁，便于通过技术和管理手段来增强实际工业系统的安全防护能力。产品可以伪装常用 IT 协议和工控协议，伪装工控设备、工控系统和工控场景，将收集的数据集中分析。可广泛适用于电厂、石油化工、供水、大型制造等工业环境，帮助企业控制规避安全风险。

除了对工业场景中常见的工业及 IT 协议进行软件基础仿真，满足低交互功能以外，还对部分实体工业资产进行硬件定制，如常见的西门子，施耐德 PLC，国产 RTU 等，并采用模块插拔方式进行实体蜜罐仿真，最大支持三个槽位的定制化工业控制资产，并可以通过外挂动态扩展，实现了工业协议层面真正意义上的高交互能力，极大地增加了对攻击者的迷惑性。

来源：山东云天

图 72 昊天工控蜜罐

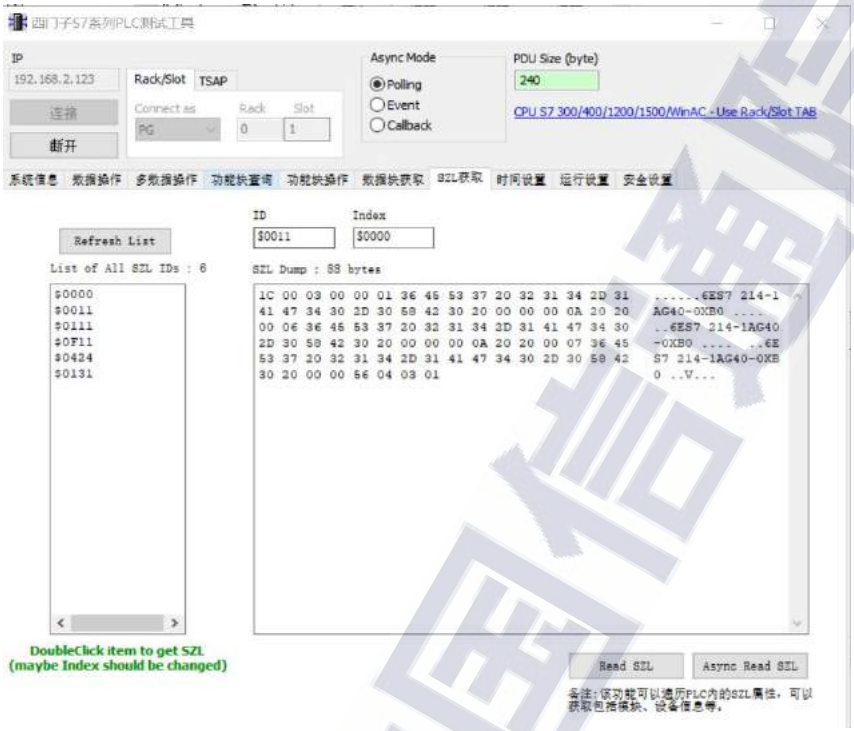
除影子系统功能外，设备还可以通过 trunk 方式接入工业现场网络交换机，将影子系统自身根据客户需求动态批量地跨网络部署，实现不同网段内按需动态播撒影子蜜饵的能力。具体示例如下：



来源：山东云天

图 73 工控蜜罐部署图

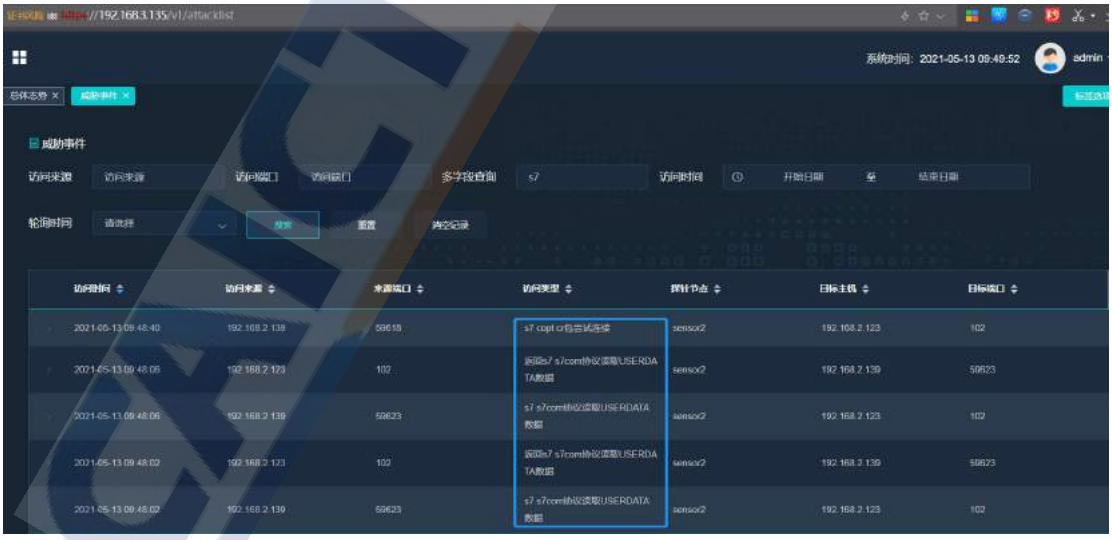
以西门子 PLC 为例，客户端发起连接到蜜罐，读取 SZL 信息，蜜罐侧检测攻击数据，解析具体工业指令内容。



来源：中国信息通信研究院

图 74 测试过程

蜜罐测检出西门子 S7 交互信息。



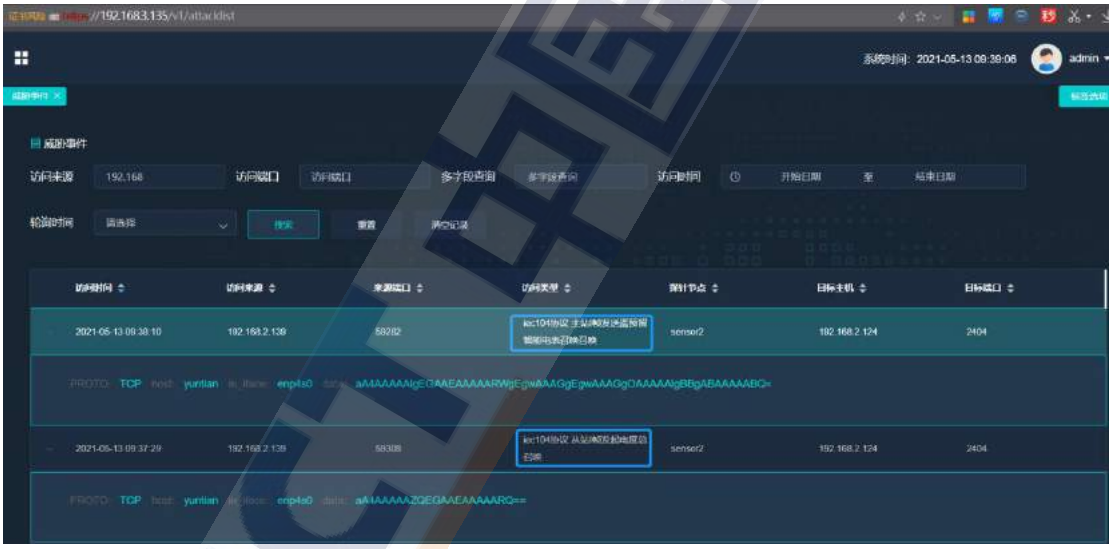
来源：中国信息通信研究院

图 75 测试过程界面

以国产 RTU（南大傲拓）为例，基于 IEC104 协议的具体工业控制执行指令的检出。

来源：中国信息通信研究院

图 76 测试过程



来源：中国信息通信研究院

图 77 测试结果展示

（三）拟态构造蜜罐——紫金山实验室

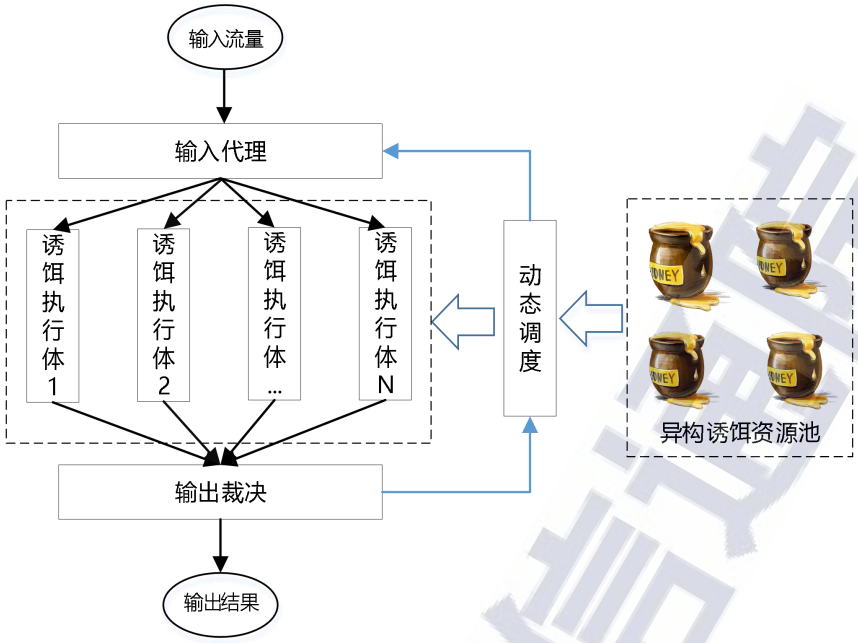
网络空间拟态防御（Cyberspace Mimic Defense，CMD）是一套“结构决定安全”的创新性网络空间内生安全防御原创技术。在网络空间防御领域，在目标对象给定服务功能和性能不变前提下，其

内部架构、冗余资源、运行机制、核心算法、异常表现等环境因素，以及可能附着其上的未知漏洞后门或木马病毒等都可以做策略性的时空变化。

为防御蜜罐系统中存在的虚拟机逃逸攻击，通过将拟态防御思想与蜜罐系统相结合，构造具有拟态防御能力的蜜罐系统，也是当前蜜罐类产品的一个特色功能发展方向。

蜜罐作为吸引攻击者攻击的目标，如果自身存在薄弱点，被攻击者利用相关逃逸漏洞对蜜罐系统展开攻击，导致攻击者获取蜜罐宿主机的控制权，那么部署在内网中的蜜罐系统将成为攻击者侵入内网的入口，并被当成跳板对其他真实业务系统展开攻击，将会产生巨大危害。

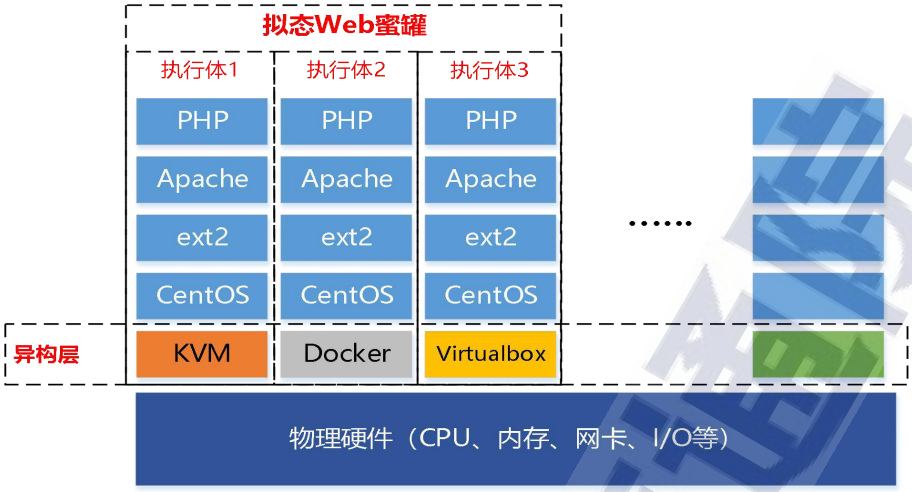
为了避免蜜罐系统被攻陷后作为攻击源的问题，将拟态防御思想融入到蜜罐系统中来构建具有内生安全的拟态构造蜜罐系统。其思路是在现有蜜罐系统的基础上进行拟态化改造，如下图所示，攻击流量首先通过输入代理分发到相同功能但不同实现方式的诱饵执行体中进行执行，执行结果进入输出裁决中进行一致性裁决，若裁决结果一致则输出，否则对异常诱饵执行体进行下线清洗，并从诱饵资源池中调用新的诱饵执行体替换被攻陷的执行体。



来源：紫金山实验室

图 78 拟态蜜罐架构图 1

蜜罐作为一种主动防御系统，是需要引诱攻击者对其进行攻击，这样才能记录攻击者的相关信息，如果对原有的蜜罐诱饵应用构建异构执行体，那么攻击者就能感知到同一种类型的蜜罐诱饵存在着不同的实现方式，攻击者难以进一步攻击，这样就阻碍了攻击者的攻击行为。因此其关键点是如何既能让攻击者顺利完成攻击过程又能保护蜜罐的安全性，这里的解决思路是蜜罐宿主操作系统上运行的虚拟机采用异构实现，如下图所示，在不同虚拟机上运行的是相同的蜜罐诱饵执行体，那么对于攻击者来说是很难觉察到自己同时是在三个蜜罐里。攻击者在不突破虚拟机的情况下，不会危害宿主机的安全，在突破虚拟机时，由于存在多个不同类型的虚拟机在同时运行，某一个漏洞一般针对具体的虚拟机类型，同一个漏洞能够攻击多个虚拟机平台概率极低，从而防御了蜜罐中的虚拟机逃逸。



来源：紫金山实验室

图 79 拟态蜜罐架构图 2

当前拟态防御思想已经应用到 Web 服务、防火墙、交换机、路由器等产品中，证明了其实用价值。紫金山实验室提出的“一种基于拟态构造的蜜罐系统”设计思路，将拟态防御思想与蜜罐主动防御系统相结合，构建具有内生安全的蜜罐系统，是针对蜜罐在实际部署存在被攻击者攻陷从而控制宿主机的情况的一种解决方案。

八、蜜罐类产品趋势展望

2016 年以来，国内外陆续有一些企业进入到网络流量分析产品市场，但从国内企业使用以蜜罐类产品为主的网络流量监测与分析产品的实际调研情况来看，市场仍然不够成熟。作为一个相对新兴的技术，要达到产品的落地和被广泛采用，蜜罐类产品仍需要一定的时间积累，但从技术和产品能力上看，其发展依然值得期待和持续关注。

（一）高仿真、高交互能力持续增强

诱捕环境能否有效迷惑攻击者，关键取决于诱捕环境是否能仿得足够真。简单的仿真环境较容易被攻击者识破，很难有效拖延攻击者的攻击行为。因此蜜罐技术持续趋向于高仿真、高交互的发展方向，例如当前业内模拟粒度通常是应用层面，而领先的攻击欺骗方案已经将模拟层次下降至文件层面，实现对文件泄漏渠道的溯源。

（二）应用场景更加广泛

威胁诱捕（蜜罐）技术除了实现攻击误导延缓以外，还可实现精准情报的溯源。基于精准的攻击情报，蜜罐可以作为业务模块集成于其他安全产品中，如激活日志和流量分析类产品，解决此类产品海量数据误报率高，威胁情报不易产出的痛点。此外，蜜罐可以产出高质量的本地威胁情报，这些情报数据可以和本地比如 WAF、防火墙进行联动来提高全网主动防御能力。正是由于蜜罐在多个领域均有着重要作用，因此未来应用场景势必会更加广泛。

（三）行业定制化需求进一步显现

随着 5G、工控、物联网等技术的发展，由于蜜罐在感知面上具有良好的环境适应性和协议无关性，可以在一定程度上弥补传统检测技术在新技术场景中应用受限的问题。因此，适配于特定行业和领域的定制化蜜罐方案需求进一步显现。例如结合工控安全技术特点，将蜜罐技术应用于工控安全态势感知，可有效获取针对工业控制系统及设备发起的网络攻击数据，分析攻击手段，剖析黑客活动趋势，目前工控蜜罐已在工控安全态势感知领域得到大量应用。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62308680

传真：010-62300264

网址：www.caict.ac.cn