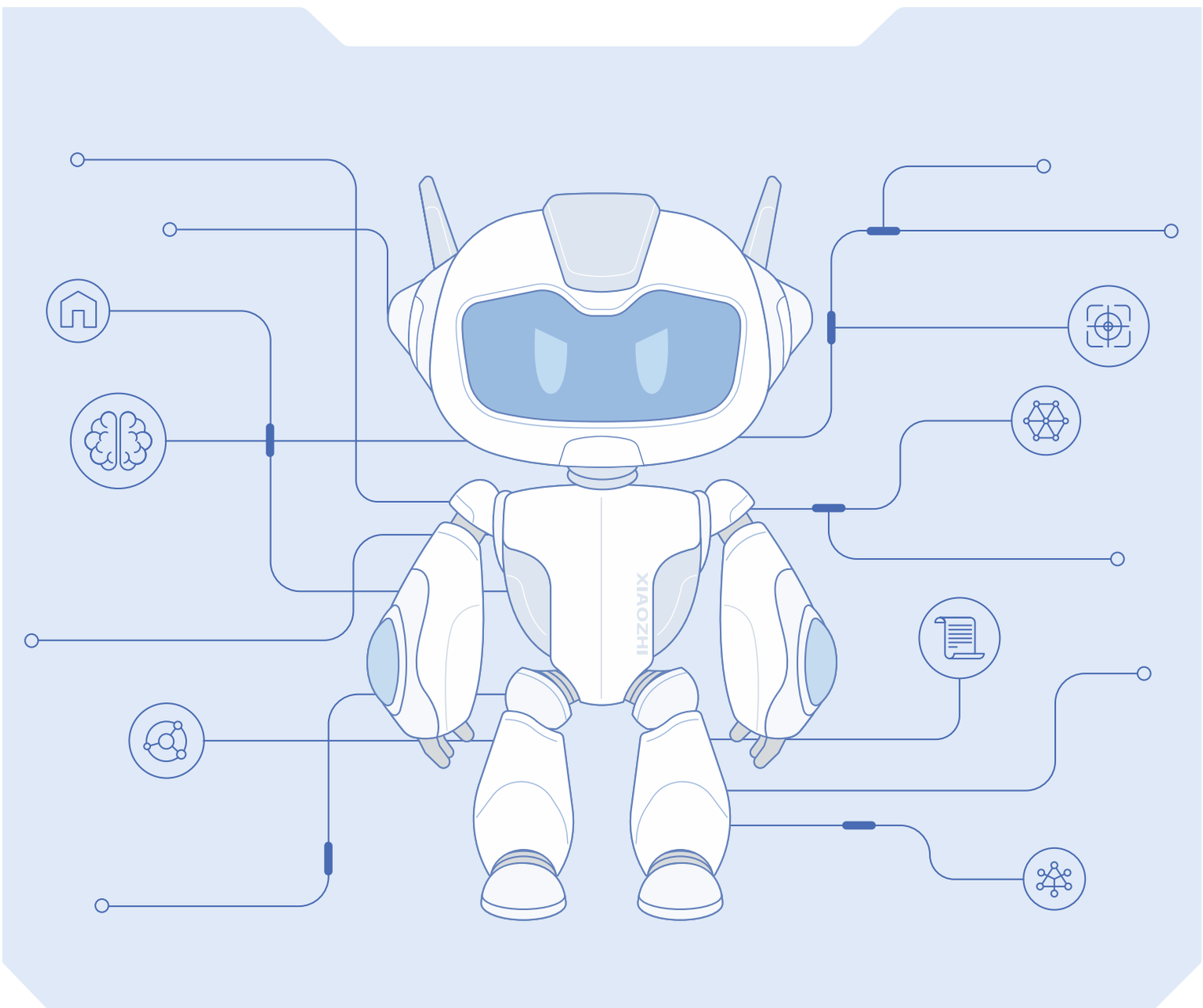
产品白皮书

小智--新一代自动化渗透测试平台



四维创智（北京）科技发展有限公司

目录

一.概述

1.1 渗透测试当下的“短板”

当前，全球网络安全形势依然严峻，针对关键行业和新技术、新场景的网络安全威胁事件频发。“十四五”时期，为应对安全新形势、新挑战，网络安全理念内涵、技术产品、产业格局等都将迎来关键变革。

以攻代防的渗透测试，在过去代表先进的网络安全理念，主动出击的渗透方式让无数潜在漏洞无所遁形。但随着云计算、人工智能、大数据等新一代信息技术的发展与迭代，传统的渗透测试方案在现今多元的实际场景中，易出现误报、漏报、效率低下等一系列问题。这使得业务的正常运转受到影响，甚至可能动摇企业安全基本盘。

归根结底，在网络安全场景趋向多元化复杂化的今天，传统渗透测试本身存在难以弥补的短板，长远来看安全能力的缺口仍将持续放大。

当前渗透测试短板		
个人依赖度强	时效性差	误报率高
涉及知识面宽、专业性要求高、依赖经验专业人员短缺 人工服务过程管理缺失，结果不可控 结果受人员能力影响大	人工耗时长，自动化只能提供辅助，解决不了替代问题 需求范围广，应用场景复杂，渗透结果不全面	传统漏洞扫描工具对多数漏洞的检测急于版本匹配机制，导致误报率高，用户信任度低

1.2 “小智”的突围之道：智能认知与决策执行

“小智”在传统渗透测试的基础上进行了全方位的革新。以算法重构渗透测试产品能力，模拟“大脑”的认知与决策能力，与时俱进。根据实际应用场景和前沿技术智能更新，及时发现网络和系统中的风险与薄弱点，为客户提供高效全面的业务风险识别与管理能力，降低业务安全风险。

1.2.1 网络场景信息的智能认知

“小智-智能渗透测试平台”基于漏洞情报知识图谱，对网络场景中的各种信息元素如组件信息、攻击面元素等数据进行系统性的统一管理，以实现在渗透测试过程当中对目标网络场景进行自动化构建，并运用知识推理技术对场景元素进行扩展和悖论校正，完成对网络场景的智能认知。

1.2.2 任务流程的复杂逻辑决策执行

“小智”依托于知识图谱的知识推理技术，联合其他智能体，实现高阶谓词逻辑的智能化决策技术。在具体渗透测试过程当中，“小智”以 **“ATT&CK”** 为框架，为实现各类攻击动作进行统一管理和调度，以信息驱动原理作为知识推理的核心，基于多阶谓词逻辑推理，将知识图谱中包含的抽象攻击事件释放为具体攻击事件，以保证在流程调度上的结果正确性，并能够显示所有具备逻辑可能性的攻击路径。

二.小智——新一代自动化渗透测试平台

“小智-智能渗透测试平台”（以下简称“小智”）是国内率先实现 **“AI+网络安全检测”** 的智能渗透测试平台，能够实现自动化完成从信息收集、漏洞验证、漏洞利用、输出报告的渗透测试全过程。

7*24小时，解放人工

渗透测试安全人才的缺口一直存在，且人无法不间断的进行工作。“小智”可以将安全专家从高强度的工作中解放，通过机器持续提供服务。真正做到“机器为主，人工为辅”。有效提升渗透测试效率。

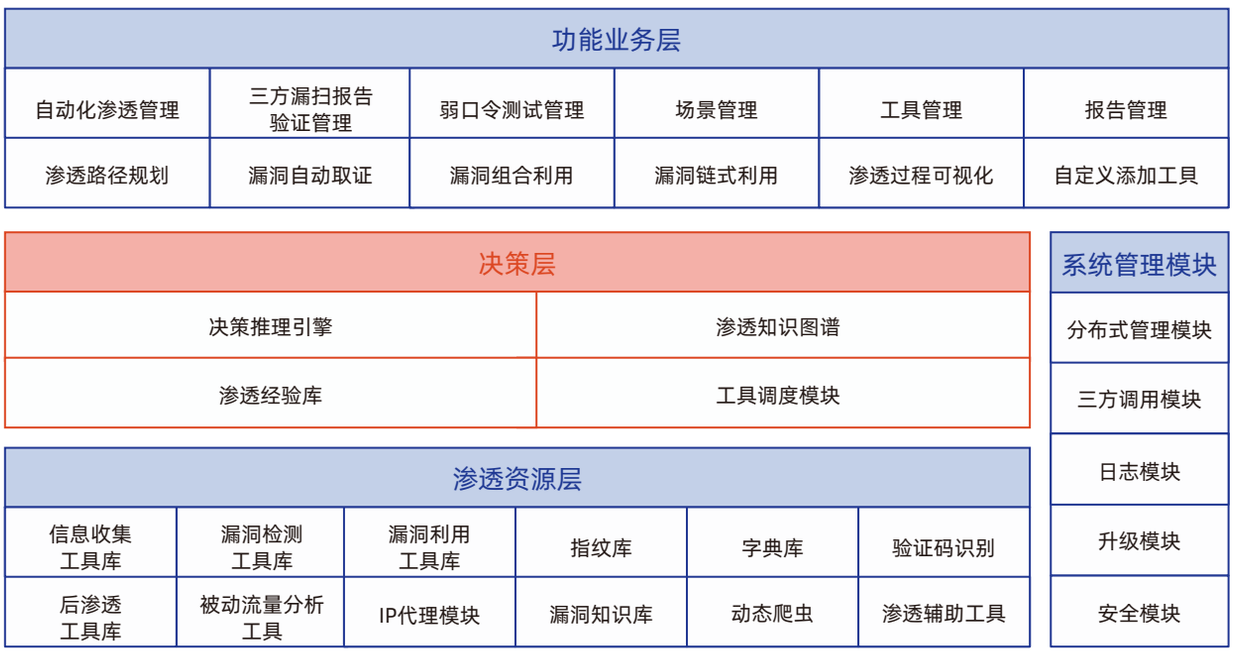
经验可存储，持续成长

“小智”能将渗透过程中积累的实战经验转化为机器可存储、识别、处理的结构化数据，实现对测试目标的自主探测、关联分析、合理决策，以贴近人工渗透测试的行为和方式，减少对业务系统的影响；并且可以在自动化测试过程中借助人工智能算法不断进行“智力”的升级优化，循环往复，实现自我驱动成长。

打破信息差，自动执行

“小智”能够自动化检测主机、web、视频监控、办公自动化设备的安全薄弱点，并且能够对相关漏洞进行自动验证、利用、取证。“小智”能主动发现信息化系统的风险点，并且在测试过程中注重多个风险点之间的关联利用，打破了传统网络安全检测平台针对威胁利用的单一性和不连贯性。

2.1 产品架构



(图1:产品架构图)

小智由渗透资源层、决策层、功能业务层、系统管理模块组成

- 资源层为渗透测试提供渗透原子能力，能够直接使用渗透工具对目标执行攻击测试。
- 决策层的推理决策引擎在渗透过程中通过知识图谱和渗透经验库对收集的渗透数据和渗透状态进行推理分析，确定下一步最佳渗透路径，实现渗透路径规划，并通过调度模块调用资源层的渗透工具进行渗透攻击，同时将数据同步给业务功能层。
- 业务功能层接收和分析决策引层数据，并将数据向用户展示，同时进行渗透任务管理和渗透工具管理等。
- 系统管理模块主要支撑系统相关基础功能。

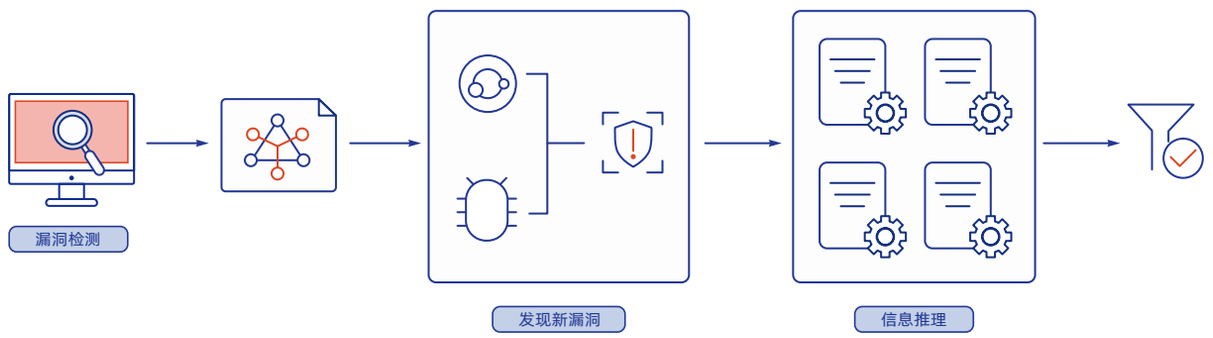
2.2 功能特色

2.2.1 漏洞利用

漏洞组合利用

“小智”的漏洞组合利用是在进行自动化渗透测试过程中基于知识图谱的关联性，通过多个已发现的漏洞进行关联组合分析来发现新漏洞。传统漏洞扫描基于规则匹配，不具备组合分析能力，只能够发现单点漏洞。“小智”在进行漏洞组合利用时，如检测到SQL注入漏洞获取到账号与密码，同时通过web路径爆破发现后台登录点时，知识图谱的特性会自动将两个漏洞获取的信息进行关联组合，从而自动登录系统后台。

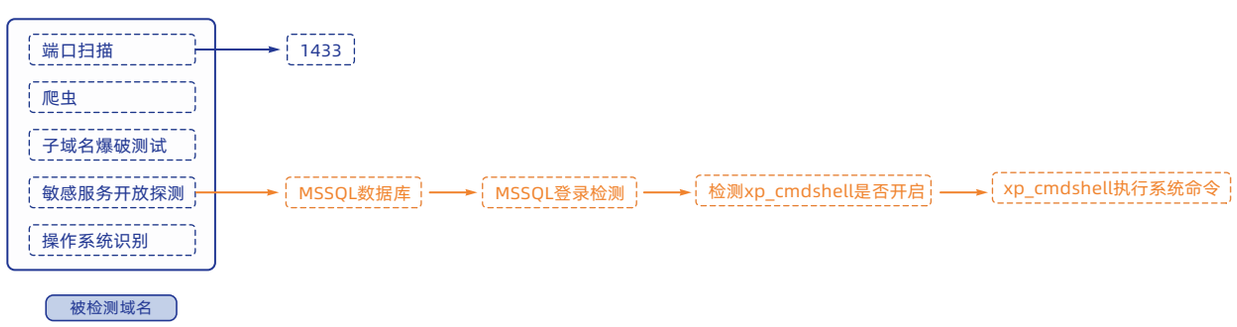
通过漏洞组合利用，小智能够发现更全面的漏洞、发现需要人工分析推理的潜在安全隐患，具备更强的检测能力，从而提高系统安全检测全面性。



(图2:漏洞组合利用)

漏洞链式利用

“小智”的漏洞链式利用是系统在检测到某个漏洞时，会根据此漏洞的知识图谱连接特性，来发现此漏洞是否具备深入利用特性。传统漏洞扫描无法探测单点漏洞能否深入连接利用，只能将获取的漏洞信息进行反馈。小智在单漏洞上能进一步再发现漏洞，从而实现对漏洞更深入全面的检测。



(图3:漏洞链式利用)

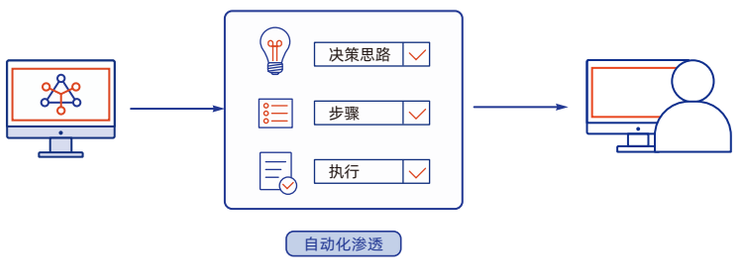
2.2.2 路径功能

渗透路径规划

系统在渗透测试过程中，能够基于知识图谱和专家系统对收集回来的信息和当前渗透状态进行综合推理决策，分析出当前存在的渗透测试路径，并选择最优路径进行渗透。相较传统漏扫和其他基于机器学习的渗透测试平台，“小智“能够模拟黑客思维，如“经验丰富的安全人员”般进行推理决策，从而实现最高效自动化检测。

实时绘制渗透测试路径图

系统可通过思维导图的方式实时展示对目标站点的完整渗透过程，展现自动化渗透过程中的决策思路、步骤和执行的操作，实现渗透测试全过程重现。”小智“可为安全人员提供渗透思路，便于安全人员发现安全隐患，及时阻断外部攻击，保障系统安全稳定性。



(图4:实时绘制渗透路径图)

2.2.3 修复验证

“小智”可通过修复验证任务来对已完成渗透检测的目标的漏洞再次进行自动化检测确认。过去为确认漏扫结果，通常需人工验证，费时、费力、费钱。小智可一键自动检测出被测目标中漏洞的实时新状态，并以“已修复”、“未修复”、“新出现”的标签加以区分。结果清晰可见，全面提升效率。

(图5:修复验证)

2.2.4 报告验证

“小智“通过验证第三方漏洞扫描器导出的测试报告中的漏洞，从漏扫报告中抽取被测目标的信息，并通过POC/EXP验证漏扫报告中的漏洞是否存在。以减少常规漏扫的误报率，节省人工手动验证的繁杂工序。

(图6:报告验证)

2.2.5 漏洞取证

系统自动对弱口令、信息泄漏、远程命令执行、SQL注入等漏洞进行风险数据取证，且能实时绘制出检测到漏洞的攻击路径。通过登录凭证、数据库数据、远程控制、信息泄漏、文件泄漏等漏洞数据，“小智”集成了专业水准的安全人员能力，可以短时间内精准漏洞取证。

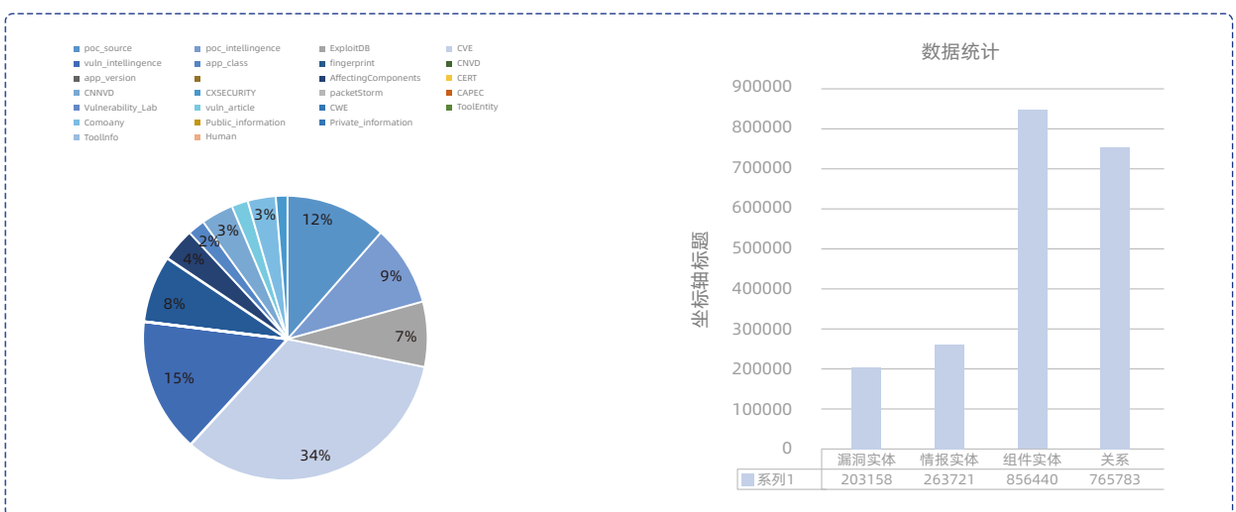
(图7:漏洞取证)

三.核心技术

3.1 立体化漏洞情报知识图谱构建技术

现在各单位、厂商所维护的漏洞管理标准不同，所反映出的信息不同，导致许多漏洞情报在具体场景应用中无法有效提供信息。为了在渗透测试任务中实现复杂网络场景、多目标联动测试的能力，小智对全网已知漏洞及其情报进行统筹性的整合分析，构建了覆盖漏洞作用目标、分析情报、时空热度等多维立体描述的漏洞情报知识图谱。知识图谱的构建，为小智提供了一个涵盖**“ATT&CK”**框架所描述的全部战术阶段需要的完整的系统性漏洞情报框架，对于复杂网络、多目标联动等大型渗透测试任务的能力提供“基建”支持。

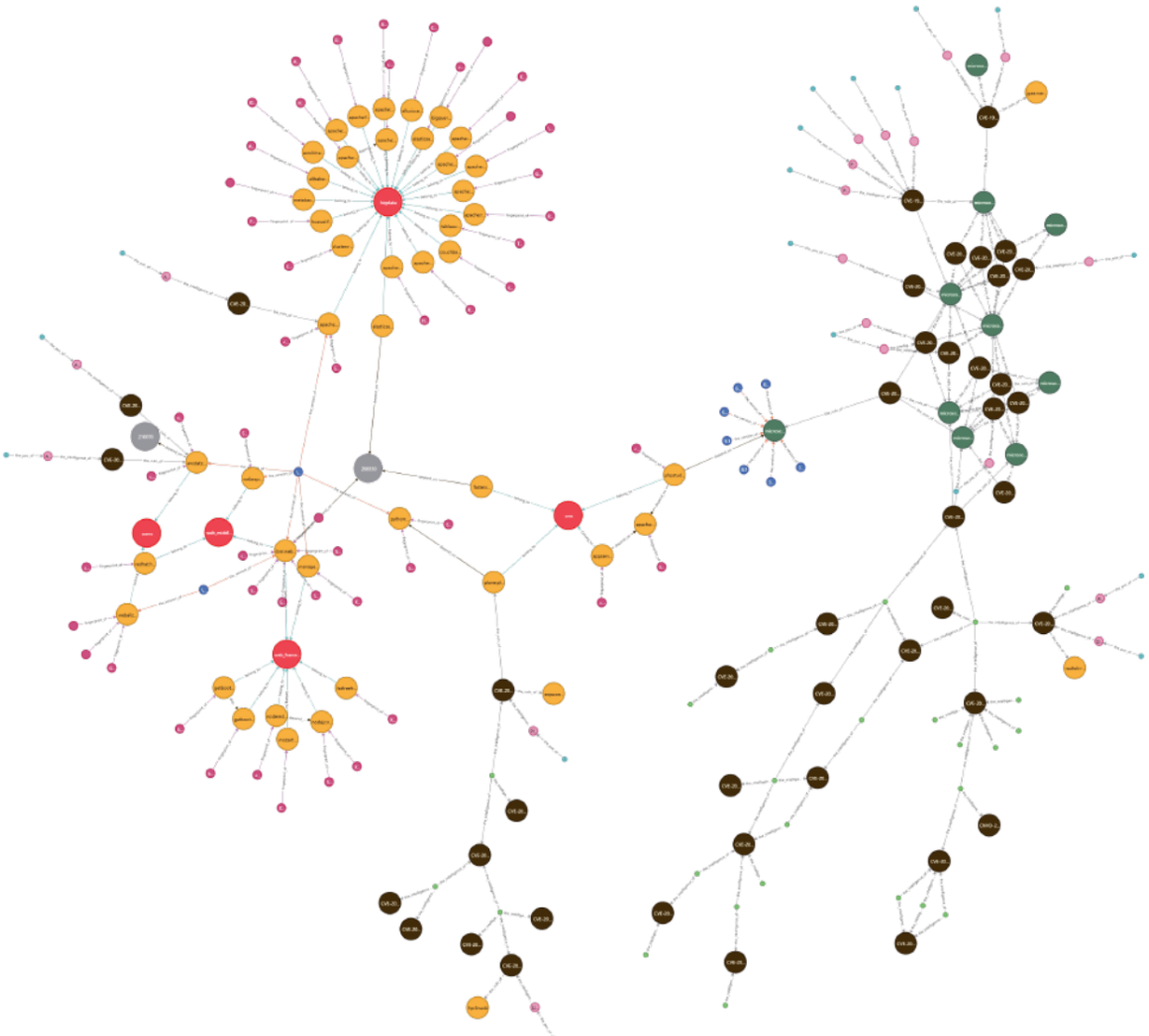
图谱目前覆盖全网开源漏洞情报，收录有效漏洞信息**214499**条，相关情报**50w+**，涵盖包括**CVE/CWE/CAPEC/CNVD/CNNVD/ATT&CK/STIX2.0**等国内外权威情报描述标准，具备推理效益的关系类型43种，关系总数超**100w**级。



(图8:数据统计)

3.2 基于事件知识图谱的智能任务决策

渗透测试过程中，一般通过已知的信息来进行测试工具的选择与执行，并在工具的执行过程中获取新的信息，层层递进，最终获取系统权限。整体过程，符合“认知决策”过程模型，于是便可以通过知识图谱构建基础事件单元，以数据驱动为核心原理，基于**POMDP**和**多阶谓词逻辑推理技术**实现渗透路径规划、动作调度、事件演绎的全流程智能决策与执行。故使“小智”具备未知场景自适应、攻击收益自校正、复杂逻辑的动作决策与执行等实战化能力。



(图9:知识图谱)

3.3 安全能力融合的垂直领域开发语言-YAK

YAK作为“一站式”安全能力基座，通过自身融合的丰富的底层安全能力和函数级插件扩展能力，为小智提供了全面的渗透测试能力，并能够支持用户快捷实现渗透测试能力自定义扩展。

(图10:Yaklang能力图谱)

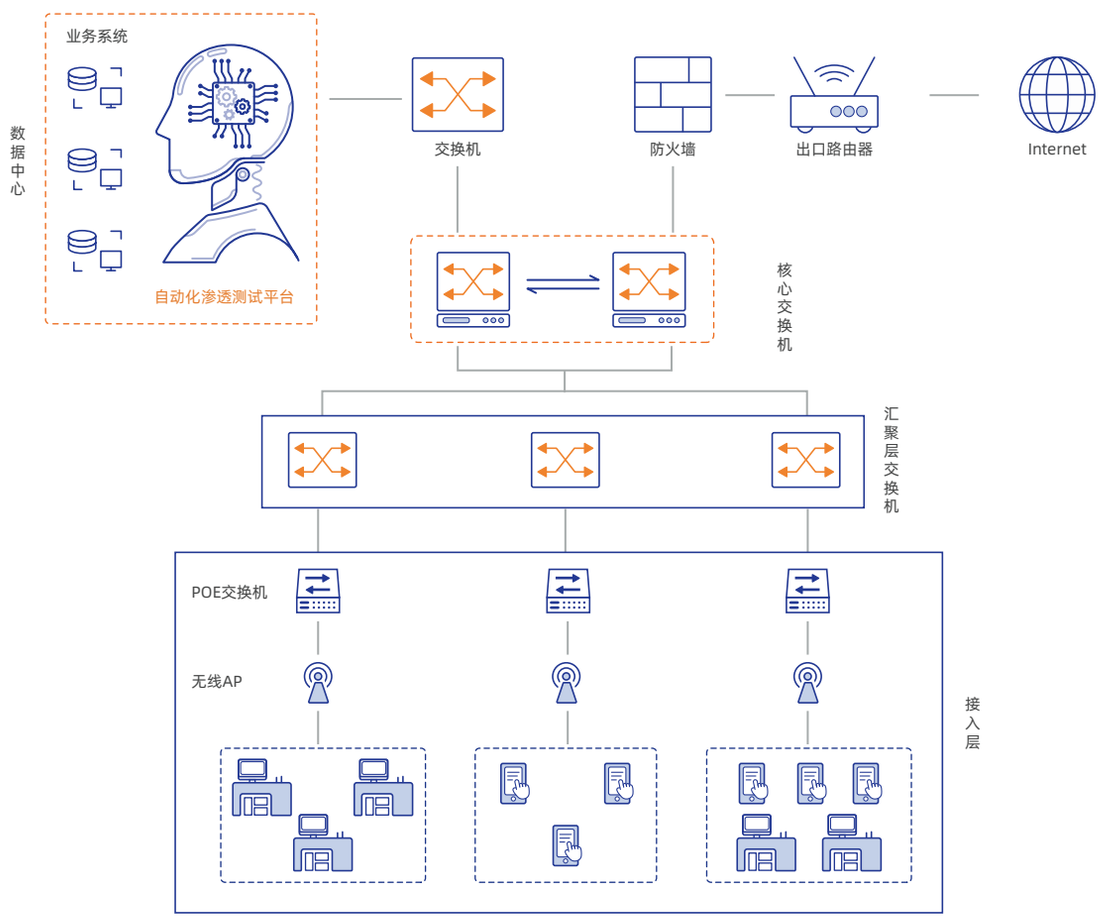
四.部署方式

产品能够固定部署在机房的传统服务器上，也可部署在云平台上

4.1 固定部署

固定部署方式是将产品部署在机房，主要用于测试检测单位内部网络的部署，且对并发渗透测试数量不大的情况。

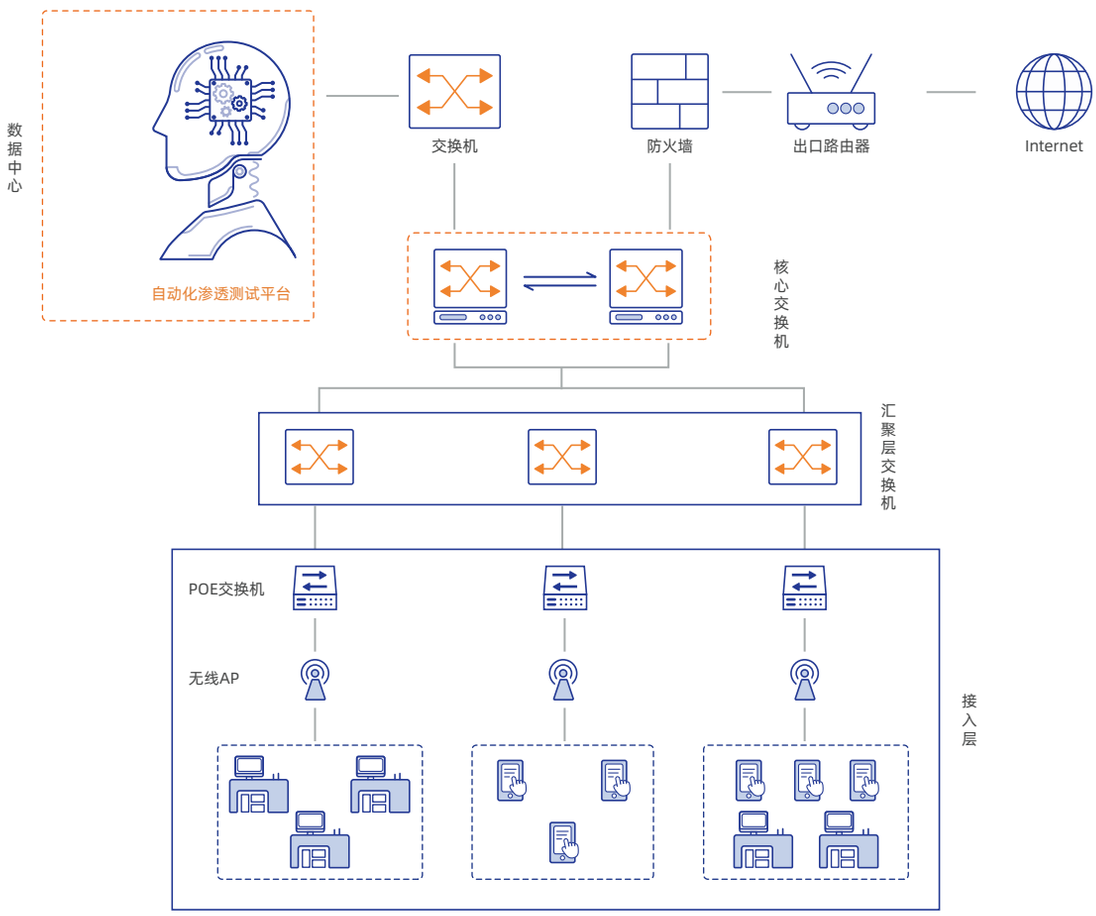
部署时将设备固定在服务器机架上，同时将设备的网络接口连接到交换机端口上，只要被测目标和系统网络可达，即可实现对被测目标进行检测。



(图7:小智-智能渗透测试平台-固定部署图)

4.2 云部署

云部署是将系统部署在云服务器上，主要用于客户对于并发量需求较大，且对并发需求有扩展的情况。


数据中心
自动化渗透测试平台
交换机
防火墙
出口路由器
Internet
核心交换机
汇聚层交换机
POE交换机
无线AP
接入层

5.2 日常安全检测

通常企业需定期对内部业务系统进行渗透检测，但安全人员少、专业水平不均衡，导致实际人工渗透测试工作量大、检测效果不理想、检测不到位。“小智”自动化执行周期性渗透测试，7*24小时坚守阵地，对资源漏洞的周期性监控与检测，提高渗透测试效率和全面性。

5.3 重大活动保障

政府、金融、大型央企一般在重大活动前会进行安全检测，保障所有业务系统不被外界入侵。重大保障时间紧、系统多、安全人员少，导致安全外包成本水涨船高。部署“小智”，能快速确认现场安全风险，包括资产、网络等，减少外包依赖，保障活动效果。

5.4 执法检测

公安/网信办需要对所辖区域内的网络进行安全性检测，执法效果既要求人员渗透专业性和有效的安全监测手段，又要体现安全执法检测的权威性。“小智”可实现辖区内网络大规模的自动化渗透检测，且不需要繁琐的步骤，便携式设备可直接带入被测单位，有效检测网络安全漏洞，现场安全执法检测，让漏洞无所遁形。

5.5 突发漏洞检测

市面上爆发风险高、影响大的漏洞时，一般需要安全人员手动排查当前系统是否存在此漏洞。通过手工排查漏洞工作量大，且对安全人员的水平要求较高。小智的自动化漏洞检测功能和持续更新的漏洞库，能够快速检测出系统中哪些资产存在新爆发的高风险漏洞，达到高效排查资产漏洞的目的。

六.客户案例

“小智-智能渗透测试平台”已服务于通信、电力、金融、能源等多个行业。根据客户反馈信息，小智能够显著降低渗透测试人员工作量，提高渗透测试效率，降低漏洞检测的误报率。

6.1 小智在电力行业的智能化应用

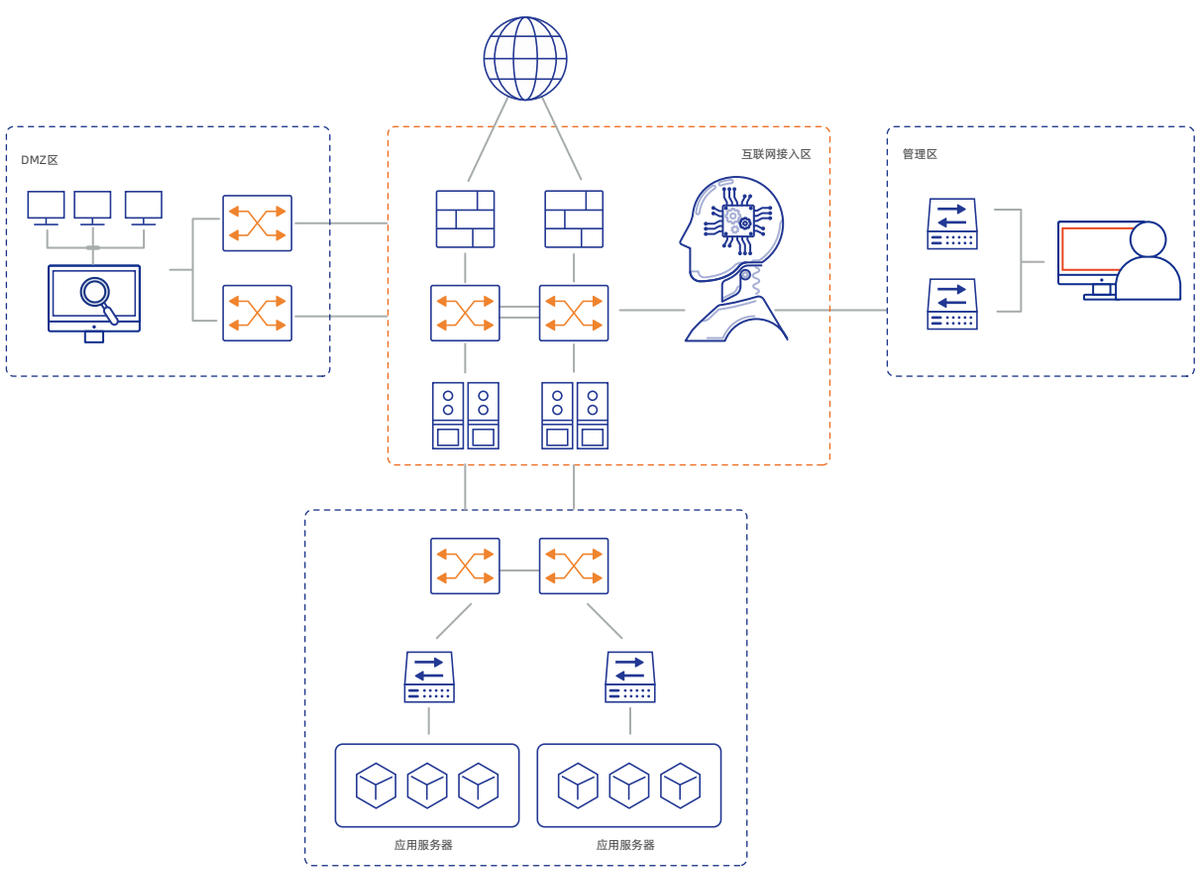
电力行业业务系统普遍繁多，无论内网还是外网都存在广泛的网络接入点，这都是潜在的攻击风险点。与此同时，系统内部具备渗透测试能力的安全人员数量较少。客户为完成系统的渗透安全检测，以往通常找安全公司外包，极大的增加了安全检测的成本，且过程中使用的工具极多。

从沟通过程中，确定客户最本质的需求是：

1. 建立自动化、规范化、且不依赖于个人因素的安全巡检工作机制；
2. 统一安全巡检过程中使用的工具，降低学习成本。

6.2 产品部署架构图

为降低渗透测试的成本，减轻渗透测试人员压力，通过**“小智-智能渗透测试平台”**实现了对新入网系统安全检测、对单位内的业务系统进行了周期性的渗透测试和提升人员能力，利用**“小智”**构建了安全巡检人工智能学习大脑，打造了适合自身业务的安全巡检统一工作平台。



(图9:产品部署架构图)

在使用小智智能化渗透平台对目标网络进行安全渗透检测的操作时，将渗透测试平台，与渗透目标网络中与互联网直接相连的防火墙之后的交换机进行连接，利用渗透测试平台对目标网络中的DMZ区、管理区和内网服务区的网络结构进行扫描，针对不同的网络环境针对性地给出具体的渗透方案并执行该方案，实现对目标网络中可能存在的漏洞进行最大程度的发现。

通过将“小智”应用于新上线的系统测试和日常业务系统测试，实现单一目标站点耗时从**13小时左右降至30-60分钟，替代60%以上的人工操作，漏洞覆盖率超过90%**，极大提升安全巡检效率、节省了人力成本，同步提升了安全巡检人员的工作能力、效率和质量。

同时帮助客户从三个方面解决客户需求：

01

建立专属知识图谱，贴身打造适合电网自身业务的渗透方案。

02

建立安全巡检统一工作平台，通过人工智能技术进行智能化的组合调用，最大限度的发挥各个工具的优势。

03

手工安全巡检走向自动化安全巡检，建立透明规范的巡检机制。

6.3 成效

01 提高安全巡检效率，降低人工成本:将安全巡检环节60%以上的重复人工部分进行替代，大大降低安全巡检人工成本。

02 进一步提升电网安全巡检的智能化水平，通过统一的平台进行集中式工作，降低技术学习的成本，缩短了整体业务安全应急响应周期。

03 通过“小智”将渗透过程中积累的实战经验转化为机器可存储、识别、处理的结构化数据，以工作经验反哺培养信任，方便快速上手，有助于安全人才梯队培养。

七. 服务客户

政 府

中华人民共和国公安部 The Ministry of Public Security of the People's Republic of China
中华人民共和国工业和信息化部 Ministry of Industry and Information Technology of the People's Republic of China
中华人民共和国交通运输部 Ministry of Transport of the People's Republic of China
中华人民共和国水利部 Ministry of Water Resources of the People's Republic of China
中国民用航空局 空中交通管理局 Air Traffic Management Bureau, CAAC
CSTC 中国软件评测中心（工业和信息化部软件与集成电路促进中心）
CCID赛迪 中国电子信息产业发展研究院 赛迪研究院
中国信息安全测评中心 China Information Technology Security Evaluation Center
中国工程物理研究院 China Academy of Engineering Physics

金 融

ICBC 中国工商银行
交通银行 Bank of Communications
招商银行 China Merchants Bank
中国光大银行 China Everbright Bank
中国平安 PING AN
中国建设银行 China Construction Bank
中国农业银行
兴业银行 Industrial Bank Co.,Ltd.
中国银行 Bank of China
中国民生银行 China Minsheng Bank
五矿国际信托有限公司 Minmetals International Trust Co.,Ltd
捷信 HOME CREDIT
中国人民银行 The People's Bank of China
中国银河证券 CGS
华夏银行 Huaxia Bank
泰康 Taikang
CFCA 中国金融认证中心

能 源

中国华能 China Huaneng
国家电网公司 State Grid Corporation of China
中煤集团
中化 sinochem
中国石油
中广核 CGN
鲁能集团 Luneng Group
中国五矿集团公司 China Minmetals Corporation
中国南方电网 China Southern Power Grid
Sinopec

运营商

China Unicom 中国联通
中国移动 China Mobile
中国电信 China Telecom

交 通

北京地铁 Beijing Subway

医 疗

北京清华长庚医院 Beijing Tsinghua Changgung Hospital

旅 游

去哪儿旅行

教 育

UESTC
Zhengzhou University

byit博易
亚信安全
PKUSE 北京北大软件工程股份有限公司 Beijing Beida Software Engineering Corp.,Ltd.
csic 中体彩科技发展有限公司 China Sports Lottery Technology Group

八. 关于我们

四维创智作为全球最早提出网络安全生态共建的高新企业，首次提出使用CDSL(CyberSecurity Domain Specific Language)模式向行业输出优秀的安全能力基座和技术解决方案。

公司多年来一直在AI+安全、移动安全、内网安全等领域精耕细作，先后推出多款自研安全产品，并针对行业的不同安全需求，提供不同的行业解决方案。同时也向全行业提供安全检测、渗透测试、风险评估、网络安全培训等服务。与能源(电力)、军工、金融等领域有广泛合作，客户及合作伙伴来自政府、军工、通信、电力等各领域。

立足于攻防一线，以“图灵完备”的Yaklang语言作为底层能力，为客户提供攻防一体的产品与服务。未来，四维创智将致力于为安全行业输出专业的基础设施，帮助客户解决安全融合问题，为客户带来全新的安全体系建设思路，打造网络安全生态产品共建体系。

坚持“做难而正确的事！”凭借先进的技术理念，帮助企业进行安全能力建设，帮助用户应对变化多端的互联网安全威胁。让世界更安全，让安全更简单。

| 小智--新一代自动化渗透测试平台 |

万径安全公众号

010-5945 6626（北京）
market@4dogs.cn
北京市海淀区 上地街道
金隅嘉华大厦 F座804
http://megavector.cn