CAICT 中国信通院　FreeBuf 咨询

网络安全产品技术能力验证评估系列报告

中国网络流量监测与分析产品研究报告

（2020 年）

中国信息通信研究院安全研究所

2020 年 09 月

版权声明

前　言

随着 NTA/NDR[1]技术的发展，该技术已经逐渐应用于网络威胁和异常行为的检测，经过实际网络环境的验证和不断的迭代，检测的有效性和准确性都有了大幅度的提高，为网络威胁和异常行为处置奠定了基础，为产品的推广和应用提供了广阔的前景。

为更好地满足行业用户在 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选型过程中提供技术能力参考，中国信息通信研究院安全研究所（以下简称“信通院安全所”）联合 FreeBuf 咨询共同完成了此次 NTA/NDR 类产品调研和测试工作。

本次测试主要是针对当前行业内主流企业的产品进行技术能力测试，测试内容和角度覆盖全面且广泛，测试内容包括产品功能、性能以及自身安全测试，覆盖数十种技术能力指标测试项。本次测试并非是符合性或合规性测试，也并非是作为某项采购入围的强制要求，而是作为 NTA/NDR 类产品的“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。测试方案内容不仅基于现有相关标准，并且依据 Gartner 对 NTA/NDR 的能力定义以及综合国内各安全企业的最佳实践。

到报名截止日期 2020 年 7 月 13 日为止，共有 28 个企业，28 个 NTA/NDR 类产品报名参与此次测试，实际到场测试企业和产品数量与报名情况一致。其中，有一款产品由两个企业共同开发完成。另外，有一个企业受测产品为两款。

[1] NTA：Network Traffic Analysis，指网络流量分析。
NDR：Network Detection & Response 指网络检测与响应。

本报告由信通院安全所对国内主流NTA/NDR类产品进行基本面测试评估，并输出整体测试、分析结果与整体报告。由FreeBuf咨询通过现场走访、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，总结国内NTA/NDR类产品的基本现状，并尝试对其发展趋势进行评估和预测。

在这里要特别感谢以下企业参与测试并为测试工作提供相关支持（排名不分先后）：

北京安博通科技股份有限公司、北京安态科技有限公司、北京安天网络安全技术有限公司、北京浩瀚深度信息技术股份有限公司、北京华安普特网络科技有限公司、北京兰云科技有限公司、北京神州绿盟信息技术有限公司、北京派网软件有限公司、北京微智信业科技有限公司、北京知道创宇信息技术股份有限公司、成都科来软件有限公司、成都深思科技有限公司、东巽科技（北京）有限公司、杭州安恒信息技术股份有限公司、恒安嘉新（北京）科技股份公司、湖南友道信息技术有限公司、江苏省未来网络创新研究院、奇安信科技集团股份有限公司、上海斗象信息科技有限公司、深信服科技股份有限公司、神州灵云（北京）科技有限公司、是德科技（中国）有限公司、腾讯科技（北京）有限公司、天津市国瑞数码安全系统股份有限公司、亚信科技（成都）有限公司、中电福富信息科技有限公司、中新网络信息安全股份有限公司、中移（杭州）信息技术有限公司、珠海市一知安全科技有限公司。

目 录

图 目 录

表 目 录

一、国内网络流量监测与分析技术现状

（一）国内网络流量发展现状

伴随着 IT 与互联网应用的快速发展，如物联网设备规模性增长、5G 商业落地等，网络流量迎来爆炸性增长。根据 CNNIC[2]发布的第 45 次《中国互联网络发展状况统计报告》，截至 2020 年 3 月，我国网民规模达 9.04 亿，互联网普及率达 64.5%。其中，移动互联网流量大幅增长，2019 年 1 至 12 月，移动互联网接入流量消费达 1220.0 亿 GB。互联网流量日益增长的背后不仅仅是个人用户的移动互联网使用持续深化，同时反映出大量企业的业务向线上转移、来源复杂和所承载的信息多样化。网络流量中承载的庞大业务信息（支付信息、账号信息等）所反映出来的数据是最为直观、真实和有效的。安全方面，网络边界模糊对流量监测带来了一定的挑战，同时网络流量的发展特性对企业安全也提出了一定的挑战，如恶意流量和加密流量的发展。

数据来源：工业和信息化部

图 1 移动互联网接入流量

[2] CNNIC：China Internet Network Information Center，中国互联网络信息中心。是经国家主管部门批准，于 1997 年 6 月 3 日组建的管理和服务机构，行使国家互联网络信息中心的职责。

（二）新兴流量监测与分析技术

网络流量分析技术 NTA 于 2013 年首次被提出，并且在 2016 年逐渐兴起。2017 年，NTA 被 Gartner 评选为 2017 年十一大信息安全新兴技术之一，同时也被认为是五种检测高级威胁[3]的手段之一，开始进入到更多企业视线里。在 Gartner 的定义里，NTA 是以网络流量为基础，应用人工智能、大数据处理等先进技术，基于流量行为进行实时分析并展示异常事件的客观事实。

在 NTA 提出伊始，重点在于网络流量与分析的能力，但随着 NTA 的不断发展，企业开始突破其技术的局限性，增加检测和响应的功能，尤其是针对高级威胁的行为分析与快速响应。因此，“NTA”这个术语已经不能够完全涵盖这些新的特征，由此，网络检测与响应技术 NDR 应运而生。2020 年，Gartner 用全新发布的《NDR 全球市场指南》替代了原有的《NTA 全球市场指南》，也标志着 NDR 正式进入大众视野。在使用 NTA 的基础上，NDR 通过与防火墙、EDR[4]、NAC[5]或 SOAR[6]平台的智能集成，添加了历史元数据用于调查、威胁搜寻和自动威胁响应。

IDS[7]/IPS[8]和防火墙等其他系统，通常仅监视网络外围，如果攻击者的行为成功地突破了网络范围而没有被发现，则攻击者的行为

[3] 高级威胁：通常指高级可持续威胁攻击（APT：Advanced Persistent Threat），也称为定向威胁攻击，指某组织对特定对象展开的持续有效的攻击活动。

[4] Gartner 的 AntonChuvakin 于 2013 年 7 月首次创造了端点威胁检测和响应 (Endpoint Threat Detection and Response，ETDR) 这一术语，用来定义一种“检测和调查主机/端点上可疑活动（及其痕迹）”的工具。后来通常称为端点检测和响应 (EDR)。

[5] NAC：Network access control，网络访问控制。

[6] SOAR：Security Orchestration, Automation and Response，安全编排自动化与响应。

[7] IDS：intrusion detection system，入侵检测系统。

[8] IPS：Intrusion Prevention System 入侵防御系统。

将不会被注意到。

NTA/NDR 主要分析南北向和东西向的流量[9]，通过使用工具组合来检测攻击，包括机器学习、行为分析、危害指标和回顾性分析。使用这些工具，可以防止在网络范围内以及在攻击者已经获得对网络基础结构的访问权限的情况下进行攻击。同时，NTA/NDR 可以记录原始流量数据，这些数据对于检测和隔离攻击以及验证威胁搜寻假设可能是宝贵的资源。

（二）行业应用现状

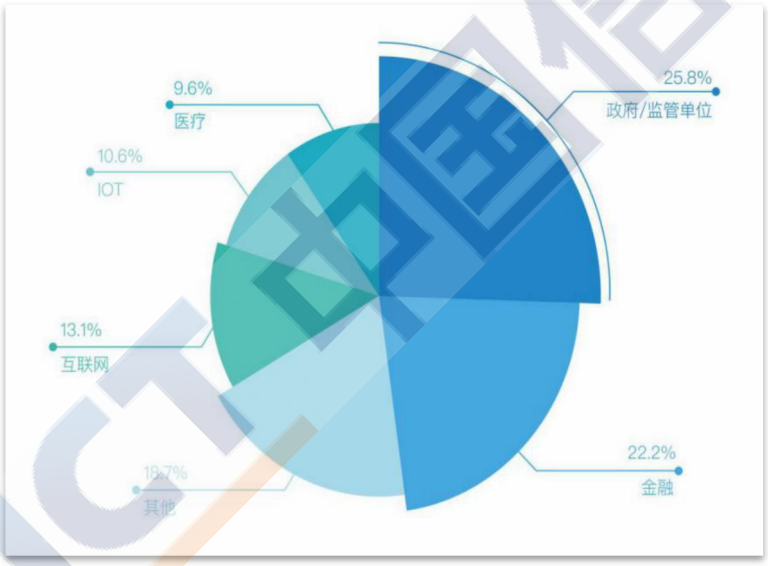


图 5 NTA/NDR 类产品的行业应用比例

调研发现，政府和监管部门、金融、互联网、医疗、物联网行业的安全需求推动了 NTA/NDR 类产品国内市场发展，这五个细分行业共占据了 81.3%的市场应用份额。

分析原因，不难发现，这是目前对新兴技术、高级威胁以及攻

[9]南北向流量/东西向流量：一般南北（上下）是客户端与数据中心的流量。东西（左右）是各个数据中心中的服务器之间的流量。

防对抗最重视及关注的五个行业。未来随着新基建等政策持续落地，网络流量监测与分析产品还将进一步增加市场应用占比。

（三）应用场景

在市面上已经存在 IDS/IPS、WAF[10]、防火墙等多种解决南北向流量问题产品的情况下,NTA/NDR 等纯网络流量监测与分析产品依然被企业关注并需要的原因在于其可以帮助企事业单位发现多个场景下基于流量的威胁行为。**一是日常异常流量监测应用场景。**大多的安全产品强调威胁可视化，网络流量正是黑客入侵及其它威胁行为发生时会随之产生的重要特征。NTA/NDR 类产品主要应用于网络流量的行为分析，强调对于异常流量行为的实时监测，更快发现威胁及溯源，弥补其它安全工具的不足之处，例如高频攻击、恶意软件入侵、内网横移[11]、数据外泄、僵尸网络[12]、恶意挖矿[13]、网络蠕虫和高级威胁所产生的恶意流量。**二是攻防演练中的应用。**攻防演练中，不论攻击成功与否，攻击行为的载体只可能是网络流量。因此，网络流量监测与分析技术也可以说是蓝军的一张王牌，通过对正常业务与威胁行为模式进行建模，能够在第一时间发现入侵事件，甚至还原整个攻击流程。

[10]WAF：Web Application Firewall Web 应用防护系统，也称为：网站应用级入侵防御系统。
[11]内网横移：攻击者获取到某台内网机器的控制权限之后，进一步在内网进行横向移动，以及攻击域控服务器。
[12]僵尸网络：是指采用一种或多种传播手段，将大量主机感染僵尸病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。
[13]恶意挖矿：在用户不知情或未经允许的情况下，占用用户终端设备的系统资源和网络资源进行挖矿，从而获取虚拟币牟利。

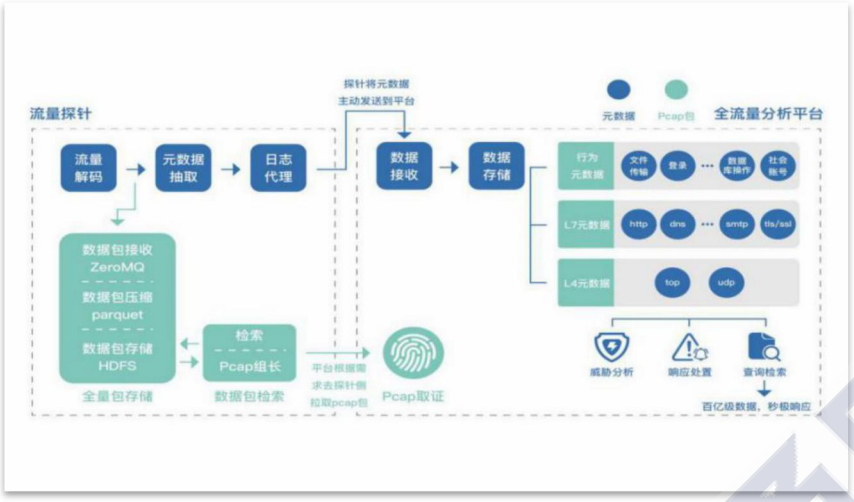


图 2 NTA 逻辑示意图

二、国内 NTA/NDR 类产品应用现状

（一）市场应用现状

近年来，随着攻击技术的发展，以高级持续性威胁（APT）为代表的新型攻击手段渐渐兴起，网络威胁形势变得更为严峻。从调研结果来看，针对网络流量监测与分析类产品的部署选择，有 32.6%的企业已经部署 NTA/NDR 类产品，还有 14.8%的受访企业表示计划部署此类产品。

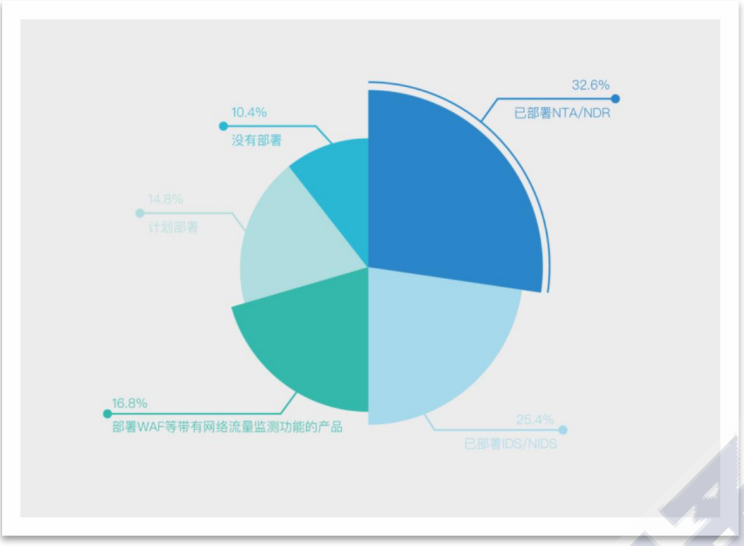


图 3 企业对于网络流量监测与分析产品的选择比例图

此外，通过对企业部署 NTA/NDR 类产品的流量采集区域调研显示，22.95%的企业选择部署在 DMZ 区[14]，20.59%的企业选择部署在 Web 服务，20.39%的企业选择部署在生产区域。

图 4 企业对于网络流量监测与分析产品的选择比例图

[14] DMZ：demilitarized zone 的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。

（三）攻防对抗场景下的应用现状

近年来，为促进和推动国家重大活动网络安全和国家关键信息基础设施安全防护工作，利用网络流量展开的攻防对抗逐渐成为趋势，企业对于 NTA/NDR 类产品的应用需求也在不断聚焦于此。调研发现，目前企业对 NTA/NDR 类产品特性的关注主要聚焦于以下两个方面，其中提升威胁分析和溯源能力的关注比例为 35.0%，实时分析原始网络数据包流量（NetFlow 记录等）的关注比例为 27.0%。

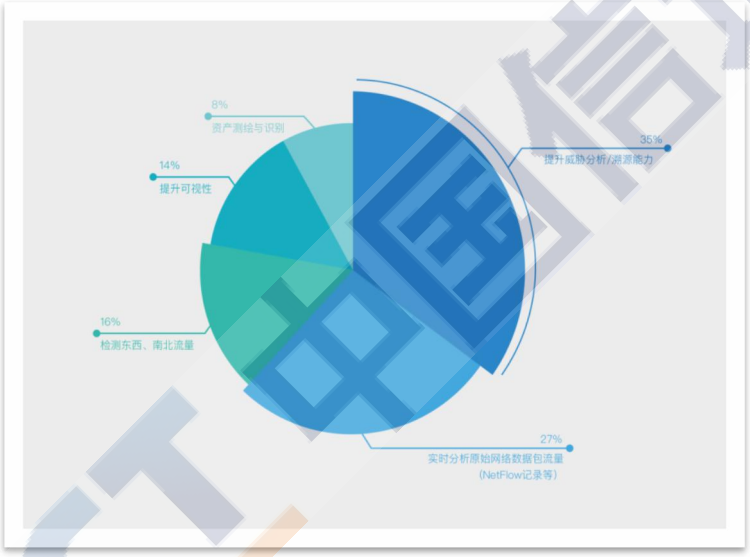


图 6 企业对 NTA/NDR 类产品特性的关注比例

而这两项能力恰好是攻防对抗场景中极为重要的环节，NTA/NDR 类产品正是将机器学习、高级分析和基于规则的检测结合起来，根据上下文收集的数据来确定后期的攻击行为，从而帮助企业最大化扭转攻防不对等的不利局面。

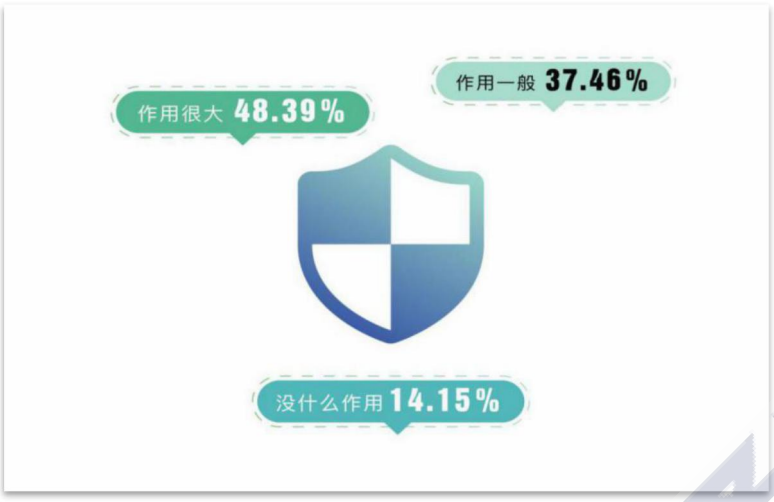


图 7 NTA/NDR 类产品在攻防演练中的作用

针对产品部署在攻防演练场景的使用效果，调研数据显示：48.39%的企业认为作用很大，37.46%的企业认为作用一般，14.15%的企业认为没什么作用。

（四）企业对 NTA/NDR 类产品的预期

针对已部署 NTA/NDR 类产品的调研对象，23.7%的企业认为产品符合预期效果，21.3%的企业对所部署的产品表示不满，仅有 7.1%的企业认为产品防护效果超过预期。

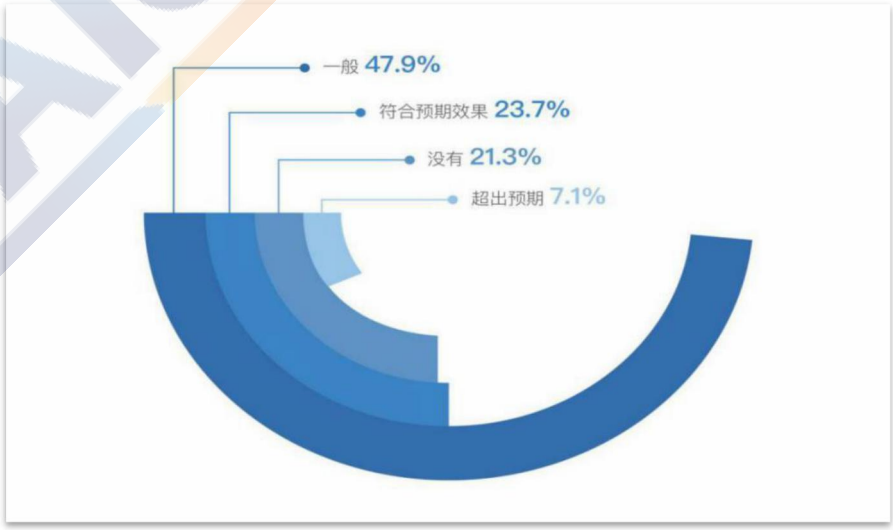


图 8 NTA/NDR 类产品的用户综合评价比例

根据调研，企业用户对现阶段 NTA/NDR 类产品不满意的问题主要包括以下两个方面：23.48%的企业认为价格高昂，22.61%的企业认为产品的事件误报率过高。

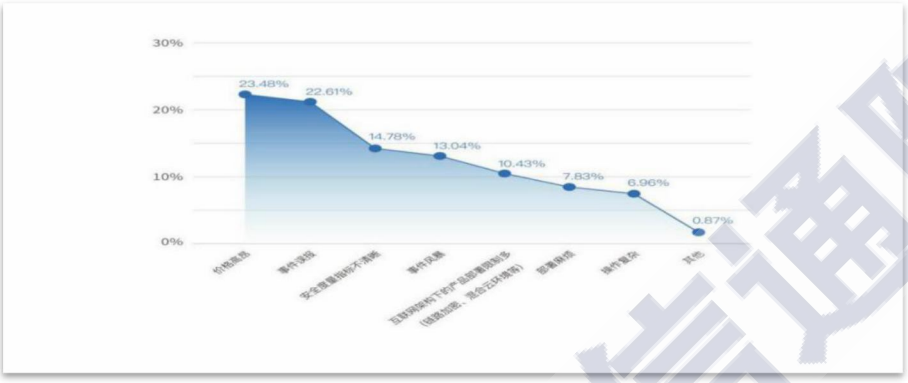


图 9 企业对 NTA/NDR 类产品不满意的原因

（五）企业期待 NTA/NDR 类产品的能力

针对 NTA/NDR 类产品的属性及应用场景，除了核心的威胁溯源及全流量存储与监测能力外，还需提升网络可视化功能。在此基础上，加密流量的分析、基于行为的数据分析能力也需着力增强。

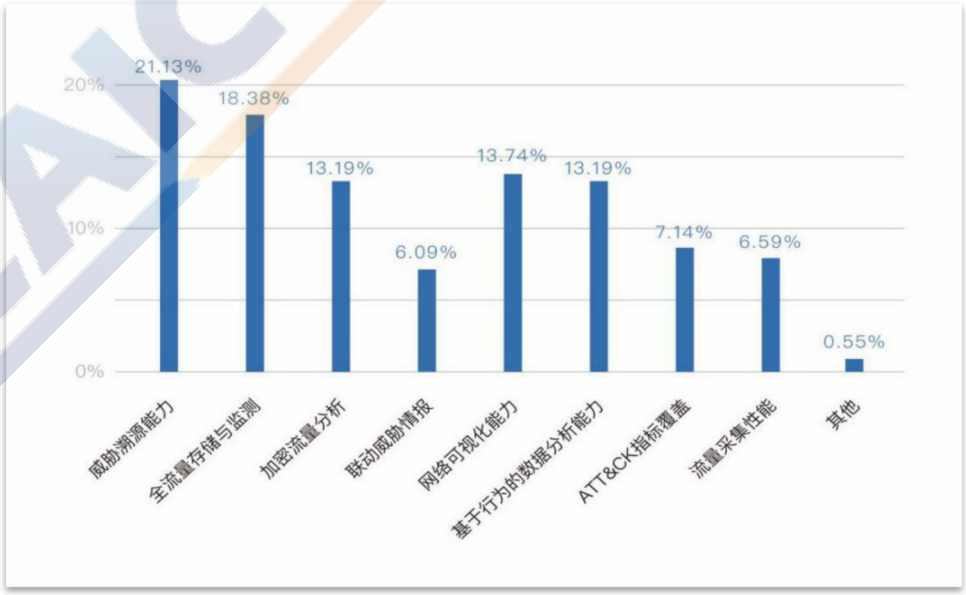


图 10 企业期望 NTA/NDR 类产品改进的能力

超过 50%的企业认为目前的 NTA/NDR 类产品需要提升威胁溯源、全流量监测及网络可视化这三项核心能力。

从调研情况来看，大多数企业非常关注 NTA/NDR 类产品的应用能力，国内企业对此的技术投入比例也在不断增强。随着越来越多的企业开始重视突发安全事件的应对能力和高级威胁的防护能力，国内 NTA/NDR 类产品的市场应用将进一步扩大。

三、NTA/NDR 类产品测试情况综述

（一）测试基本情况

本次 NTA/NDR 类网络安全技术能力测试在信通院安全所网络安全实验室进行，开始于 2020 年 6 月 22 日，结束于 2020 年 7 月 31 日。各参测企业根据测试方案分别组合了自身的产品模块和技术能力。

各参测企业参与受测的产品数量不同，如表 1 所示，每个参测企业产品数量从一台至五台数量不等，但普遍为一台至两台，通常一台设备作为流量采集探针，另外一台设备作为安全分析和展示系统，对于采用两台以上设备的企业通常是将安全分析模块进行了能力拆分，例如安全攻击分析模块、恶意文件沙箱分析模块以及总体分析和展示模块几个部分。所有参与测试的产品均采用了标准 1U 或 2U 标准服务器，少部分企业采用了专用定制设备。

表 1 各企业到场测试产品台数

企业简称	台数	企业简称	台数
斗象科技	5	湖南友道	1
绿盟科技	4	安态科技	1
深信服	3	中移杭研院	1
奇安信	3	一知安全	1
安天科技	2	安博通	1
安恒信息	2	深思科技	1
恒安嘉新	2	国瑞数码	1
中新网安	2	华安普特	1
微智信业	2	中电福富	1
派网软件	2	知道创宇	1
科来	2	东巽科技	1
兰云科技	2	神州灵云	1
浩瀚深度	2	江苏未来网络创新研究院	1
腾讯科技	2	亚信 TDA	1
亚信 SpiderFlow	1	/	/

（二）测试环境介绍

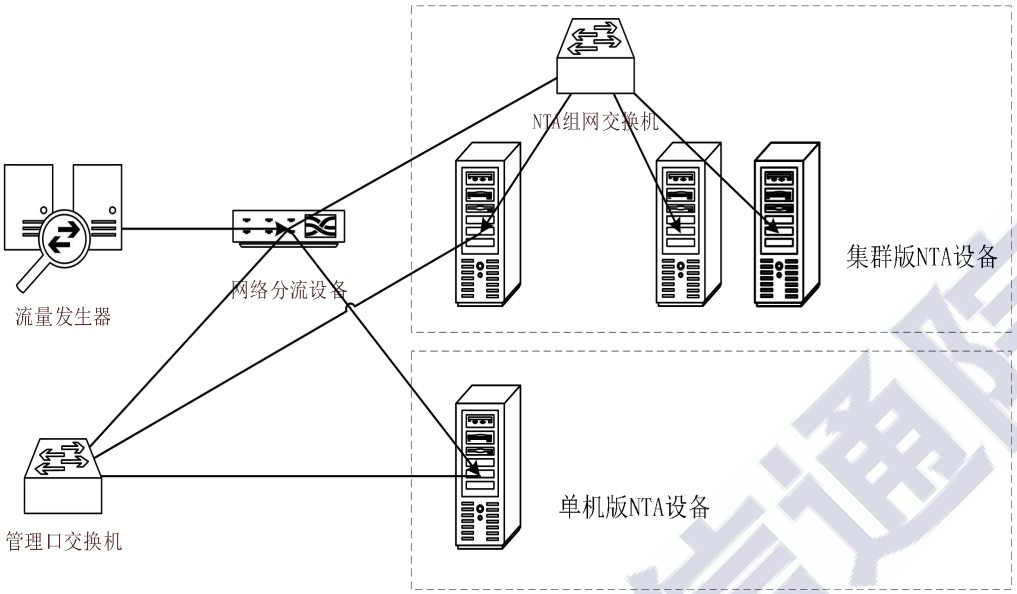


图 11 测试网络拓扑图

本次测试主要采用 IXIA PerfectStormONE 流量发生器模拟网络流量、攻击以及恶意程序等，采用 IXIA Vision E40 分流设备进行多路模拟流量生成。如图 11 所示测试环境拓扑情况，流量发生器与分流设备相连接，并配置流量策略，分流设备将模拟的测试流量同时下发多份，受测产品的采集口（或通过交换机转发）与分流设备相连。管理口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 172.16.5.0 网段 IP 作为管理 IP，并接入到受测网络中。为了保障在对测试结果进行截图并说明过程中的真实性，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。

图 12 测试现场

（三）测试方法说明

本次测试包括产品功能测试、性能测试和系统自身安全测试。**在功能测试方面**，由 IXIA PerfectStormONE 流量发生器生成相关流量，随后在产品找到采集或分析结果相应界面，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。对于不需要专门利用流量发生器的测试项，直接在产品界面截图中进行描述说明。**在性能测试方面**，根据产品型号（千兆或万兆），由 IXIA PerfectStormONE 流量发生器进行最大量生成混合流量,受测产品记录流量采集峰值以及峰值期间 CPU 或内存资源的消耗情况。**在自身安全测试方面**，由专业白帽子渗透测试工程师利用各类 Web 检测工具，结合手工测试对设备系统和应用层面进行全面渗透测试。

图 13 IXIA PerfectStorm ONE 流量发生器 Web 界面

（四）测试对象范围

常用的网络流量监测技术主要包括主机内嵌软件监测、基于 SNMP 协议的流量监测、基于 NetFlow 的流量监测、基于硬件探针的检测等。而网络流量分析则从带宽、网络协议、基于网段的业务、网络异常流量、应用服务异常等方面着手。近年来，业界则主要使用 DPI[15]和 DFI[16]来进行流量分析，尤其是 DPI 技术可以大幅增强流量识别的精度。总体来说，DFI 注重量的统计、DPI 注重内容的分析。

目前，网络流量监测和分析既指特定用途的硬件设备（比如各家安全企业提供的 NTA/NDR 类产品），也指基于网络层的安全分析技术。不同于主机层、应用层是以日志、请求等为分析对象，流量分析面对的是更底层的网络数据包，信息元素更多，分析更为复杂。

[15] DPI：Deep Packet Inspection，是一种基于数据包的深度检测技术，针对不同的网络应用层载荷（例如 HTTP、DNS 等）进行深度检测，通过对报文的有效载荷检测决定其合法性。

[16] DFI：Deep Flow Inspection，是一种基于流量行为的应用识别技术，以流为基本研究对象，从庞大的网络流数据中提取流的特征，比如流大小、流速度等。也就是不同的应用类型体现在会话连接或者数据流上的状态不同。

本次测试对象范围要求以 DPI/DFI 流量采集技术为主的 NTA/NDR 类产品，不限于网络全流量监测与安全分析系统、网络异常行为监测系统、流量威胁探针系统、高级可持续性安全威胁监测系统、大数据智能安全分析系统、态势感知威胁预警系统等。

（五）测试内容简介

本次测试内容范围覆盖从原始网络流量采集、还原，并进行网络攻击、恶意程序、APT 等安全分析并告警，生成结果报告，并对风险进行处置和溯源等网络流量全生命周期分析能力测试。如表 2 所示，测试内容包括产品功能测试、产品性能测试和产品自身安全测试三个方向。其中产品功能测试包括网络流量识别能力、安全分析能力、安全事件处置能力、安全事件溯源能力、自身管理能力、自身日志审计能力六大产品能力，其中网络流量识别能力和安全分析能力是本次测试的重点方向。产品性能测试包括网络流量吞吐能力和系统资源使用情况测试。自身安全测试包括针对系统的 Web 应用安全和业务逻辑安全测试。

表 2 NTA/NDR 类产品测试项目表

测试大项	测试小项
网络流量识别能力	流量采集方式
	识别网络协议类型
	识别网络协议内容
	识别网络文件类型

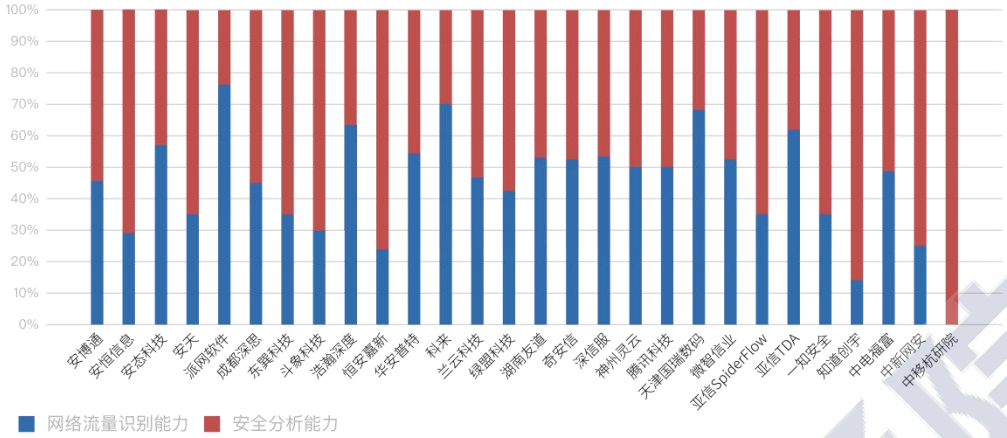
	识别网络文件内容
	网络资产识别
	网络资产批量导入
	网络资产主动识别
	识别网络资产内容
	流量数据统计能力
安全分析能力	安全分析能力
	安全事件分析
	安全关联分析能力
	自定义网络行为分析
	恶意文件分析方式
	恶意文件分析能力
	结果数据可视化能力
安全事件处置能力	告警能力
	联动能力
	应急处置流程和工单处理能力
安全事件溯源能力	风险描述
	调查溯源
管理能力	监测配置能力
	存储配置

	报告导出
	数据报表与统计
	用户角色权限管理
	升级管理
日志审计	审计日志生成
	日志可理解性
	审计日志可查阅
自身安全	网络访问控制
	Web 应用&逻辑业务
平台性能	最大实时吞吐
	CPU、内存使用率监测

四、NTA/NDR 类产品测试结果总体分析

（一）不同技术方向“划分”企业能力阵营

通过测试结果发现，在不考虑受测企业的供测产品数量和产品功能组合不同情况的影响下，**多数受测产品具有技术能力倾向性，**其中，部分产品能力倾向于网络流量识别，主要包括各类网络协议的识别、各类文件的识别与还原等，部分产品则倾向于安全分析能力，主要包括网络攻击行为分析、恶意程序分析、APT 关联分析以及综合态势展示能力等。



数据来源：测试结果

图 14 受测产品主要能力占比

如图 14 所示，各产品网络流量识别能力和安全分析能力对比，其中蓝色部分是网络流量识别能力测试项结果总和，红色部分为安全分析测试项结果总和，蓝色占比多意味着产品网络流量识别能力较强，红色占比多表示安全分析能力强。从整体上看，网络流量识别和安全分析能力相对平衡,即两种能力各占比例 50%左右的受测产品不足 10 家。

（二）自动化处置能力有待落地和完善

通过测试结果发现，**大多数产品具备基本的告警功能，但自动化编排响应能力有待提高**。根据测试用例要求，受测产品**在告警能力方面**，可进行实时有效告警，告警方式包括界面、邮件、短信、站内信等，并且告警信息在系统中有详细记录。**在联动能力方面**，具备与其他设备 API/Syslog/SNMP 等接口的配置，并且可以与企业其他产品和其他企业或开源组件实现数据联动，以满足风险通知等

其他扩展功能。

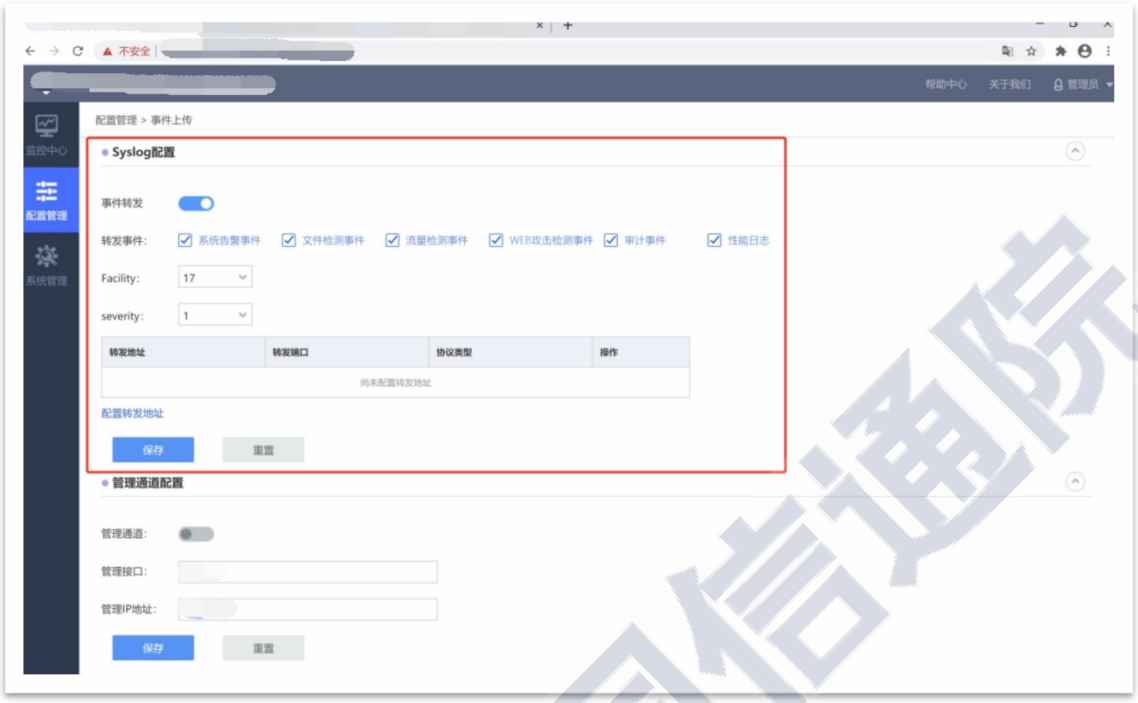


图 15 某产品告警能力测试结果截图

KillChain[17]/ATT&CK[18]技术落地仍需完善。通过测试结果发现，仅有不足 8 款产品实现了基于各类攻击链的告警分析，以 ATT&CK 为例，包括初始访问、执行、持久化、授权、防御规避、凭证访问等全过程告警功能。但是在风险告警与攻击链构成防御策略方面仍需不断完善。随着各企业在国家 APT 网络攻击对抗领域的不断深入研究与实践，应持续完善产品能力，以在网络安全防御与应急响应工作中起到实际效果。

[17] 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。

[18] 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。

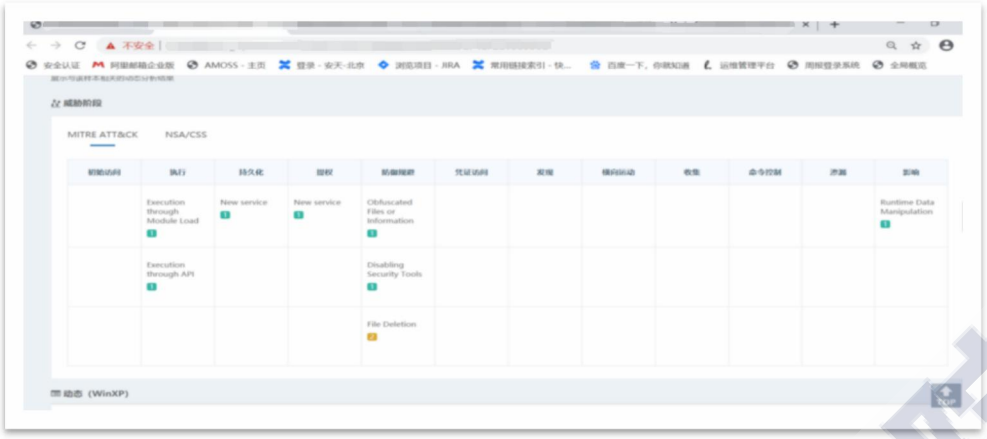


图 16 某产品攻击链功能测试结果截图

SOAR 能力缺乏在 NTA/NDR 类产品中落地。通过测试结果发现，在工单管理能力方面，仅有 10 款产品实现了最基本的事件状态管理，其中 6 款产品具备工单流转与处置全过程管理能力，不足 4 款产品具备完善的基于不同角色的处置流程全过程管理，但是在自动化判断方面仍需不断研究改进。另外 18 款产品不具备工单管理功能。

图 17 某产品攻击链功能测试结果截图

在安全编排自动化与响应能力方面，绝大多数受测产品未体现出相关优势，需要在实践中不断完善和改进。

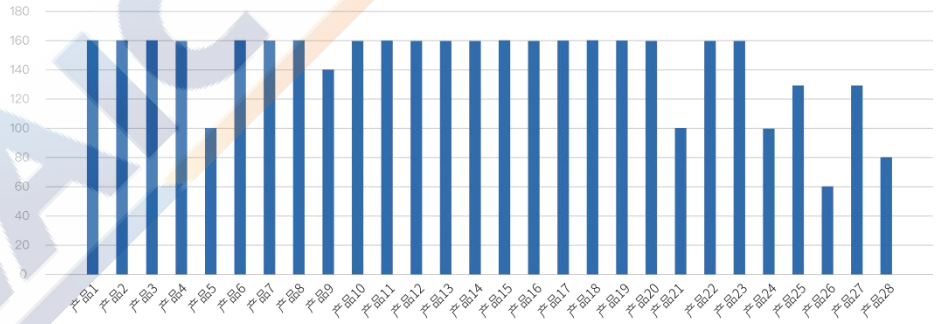
（三）基于 IP 和主机的溯源功能不分轩轾

通过测试结果发现，**虽距实现精准溯源仍有一定距离，但多数**

产品基本满足此次测试项。受测产品基本支持风险事件关联协议日志进行联合检索、风险事件 PCAP[19]流量包下载、恶意文件下载。支持网络协议全文高级检索，对不同类型协议支持动态字段查询和展示。可以留存全量网络文件数据，并提供文件解析及文件下载功能。可以留存全量网络数据包，提供查询及 PCAP 包下载功能。

图 18 某产品溯源能力测试结果截图

如图 19 所示，具有较好测试结果的受测产品有 20 款，约占受测产品数量的 70%左右，仅有 1 款产品需在此方面重点完善。多数受测企业具备在自身流量采集范围内，基于 IP 的攻击路径还原能力。



数据来源：测试结果

图 19 基本溯源能力测试分数统计结果

[19] PCAP：一种网络抓包的文件格式。给抓包系统提供了一个高层次的接口。所有网络上的数据包，甚至是那些发送给其他主机的，通过这种机制，都是可以捕获的。它也支持把捕获的数据包保存为本地文件和从本地文件读取信息。

追踪溯源是网络安全技术能力难点，要想准确溯源攻击组织和手段、攻击路径等，需要采集更多的数据，提高分析发现能力，结合威胁情报平台等其他系统，同时，需要安全技术人员通过数据分析逐步实现。**因此，网络攻击追踪溯源仍然是需要网络安全企业不断深入研究和实践的关键技术领域。**

（四）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**在监测配置方面**，具备包括不限于协议流量类型、文件类型、网络区域配置、风险监测配置等功能。**在存储配置方面**，配置内容具备包括存储时间、存储范围、存储数据类型等功能。**在报告导出方面**，具备基于攻击事件、网络协议、资产内容等多维度灵活导出功能。**在数据报表统计分析方面**，统计维度包括风险趋势、资产动态、实时动态等信息的展示功能。**在角色权限管理方面**，具备权限划分、功能划分与角色划分等功能。**在升级管理方面**，具备在线升级功能和离线升级功能，且支持对系统和策略的分别升级。

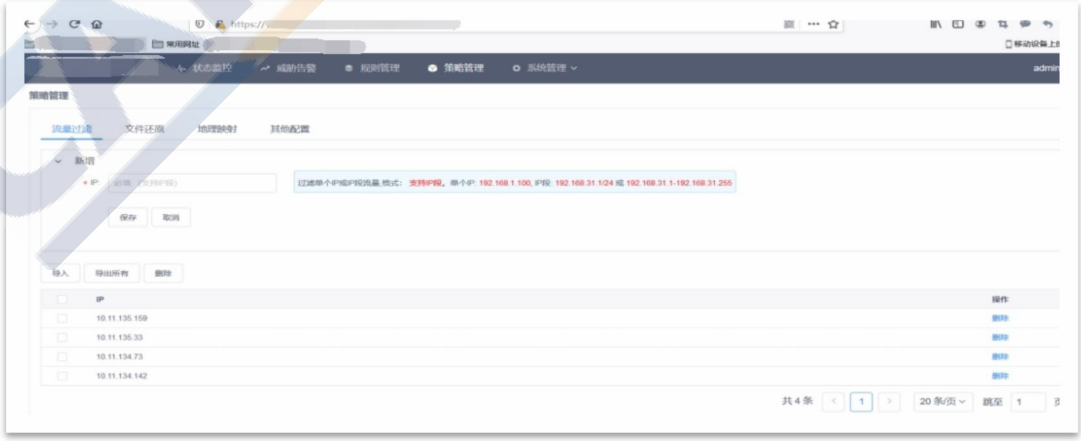
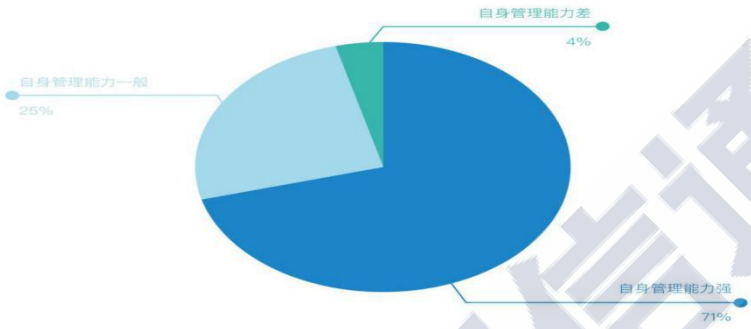


图 20 某产品管理功能测试结果截图

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 21 所示，其中 71%受测产品具有较为完善的自身管理能力，满足测试功能要求，25%受测产品在自身管理功能方面有待提高，4%受测产品不具备自身管理相关能力。



数据来源：测试结果

图 21 产品自身管理功能结果比例图

五、NTA/NDR 类产品流量识别能力分析

（一）网络协议识别展示能力各有所长

在本测试用例中，利用流量发生器构造了 100 余种协议和应用，包括 SAP、SMTP、SNMPv2c、DNS、SMBv2、POP3、Twitter、SSH、Radius、SOCKs5、Zoom meeting chat、TikTok、Baidu、IQiyi、HTTP、HTTPS、FTP、TFTP 、MSSQL、MySQL、Whois、DCE RPC、IPP、NNTP、X11、Mongodb、WebDav、RPC、MQTT、Amazon、Db2、NetBios、WhatsApp、aim6、tacacs+、QQLive、classic stun、Gadu Gadu、Microsoft lync sipe、QQ 等，运行 5 分钟，通过受测产品查看是否完全识别并解析

各类协议内容。

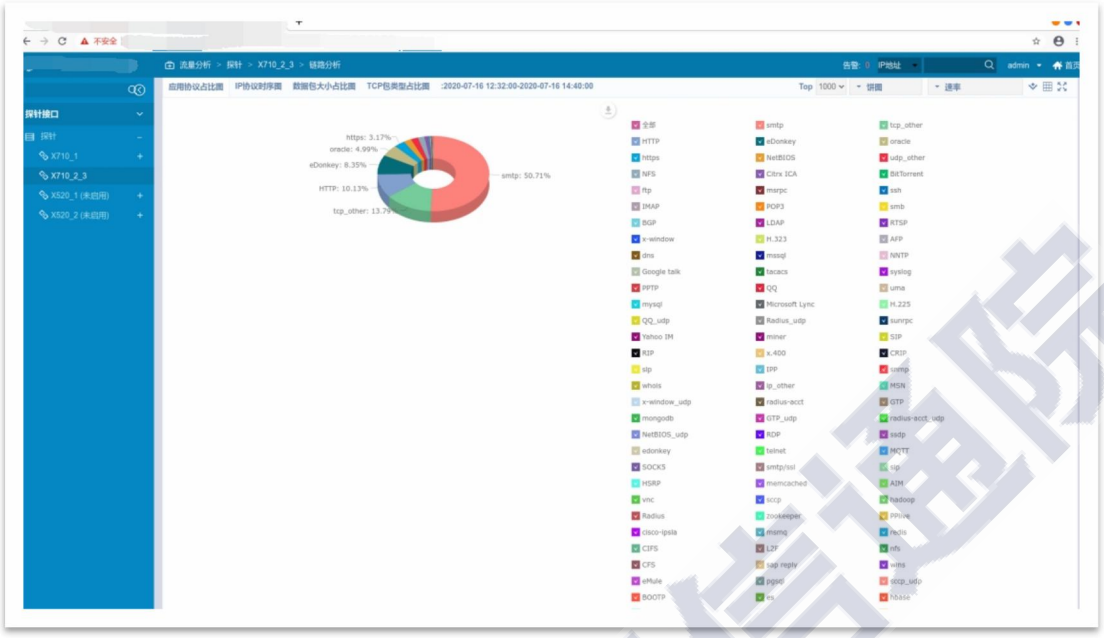


图 22 某产品协议识别能力测试结果截图 1

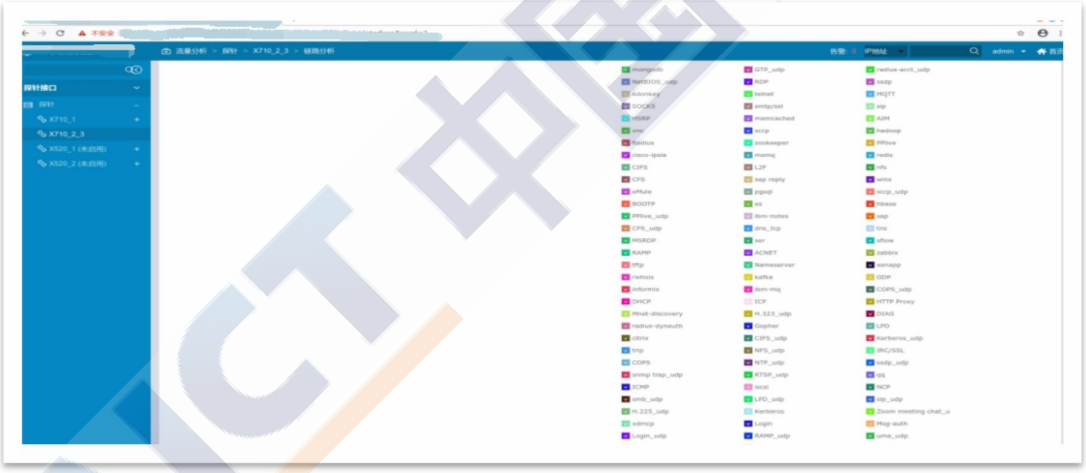
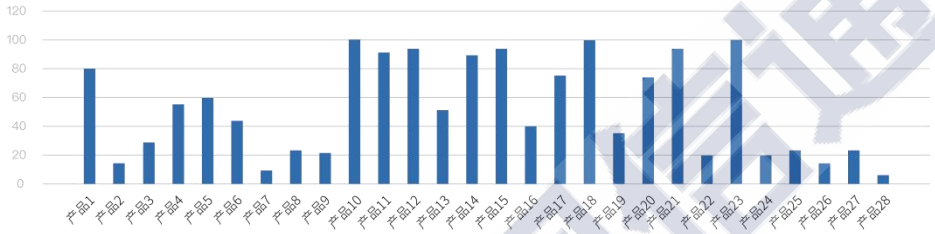


图 23 某产品协议识别能力测试结果截图 2

通过测试结果发现，**各产品对协议和应用的识别数量差异较大**，如图 24 所示，识别出约 0-20 余种协议的产品有 8 个，识别出 20-40 余种协议的产品有 6 个，识别出 40-60 余种协议的产品有 4 个，识别出 60-80 余种协议的产品有 3 个，识别出 80 以上种协议的产品有

7 个。总体拉看，产品的流量识别能力分别趋向于“协议识别类别多”和“精准识别还原部分协议内容”，猜测这是由于不同企业针对 NTA/NDR 类产品的能力侧重点不同，有的优势在全流量数据还原识别，有的优势在于网络、Web 应用安全分析，仅识别了 HTTP、SMTP、POP3、FTP 等协议。个别参与此次测试的产品方向侧重于各类互联网应用和互联网游戏的流量识别和数据分析。



数据来源：测试结果

图 24 产品协议识别情况

（二）网络流量识别还原内容因需而定

1.绝大多数产品可全字段还原 HTTP 协议

在本测试用例中，利用流量发生器构造了 HTTP 应用，每个 TCP 连接中包含一个 GET 和一个 POST 请求。通过受测产品查看 HTTP 协议内容，筛选 HTTP 流量协议，查看协议中解析的字段信息，HTTP 协议应包含但不限于 HTTP 请求头（User-Agent、Referer、Host、Content-Type、X-Forwarded-For 及其他自定义字段）、HTTP URL、HTTP GET/POST 参数、HTTP 返回码、返回头、返回内容、HTTP 源/目的地址、HTTP 源/目的端口等信息。

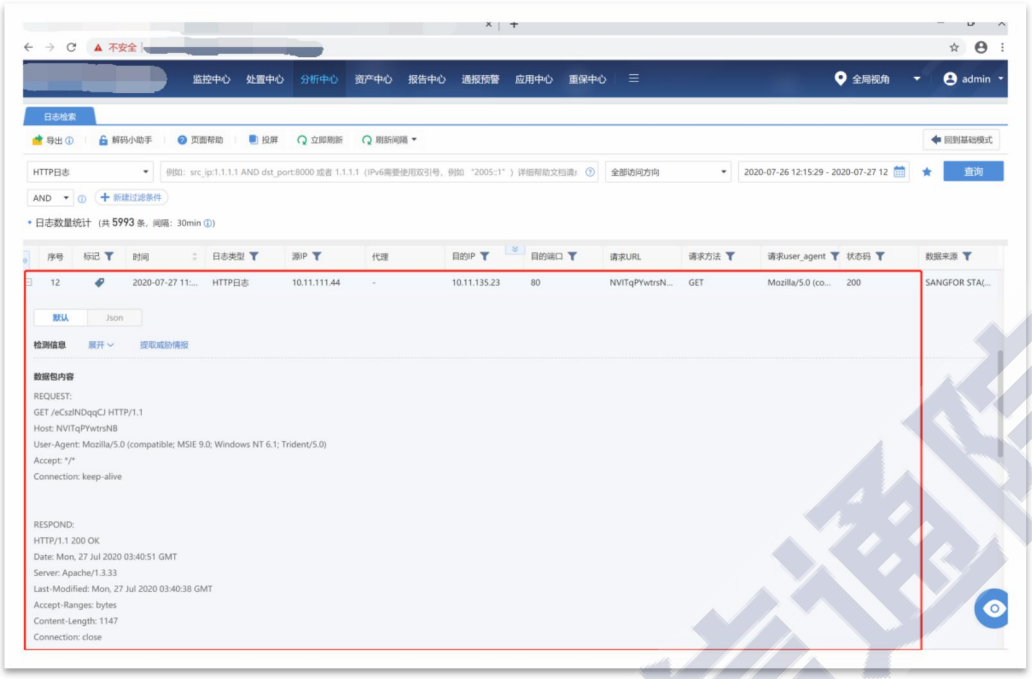


图 25 某产品 HTTP 协议还原测试结果截图 1

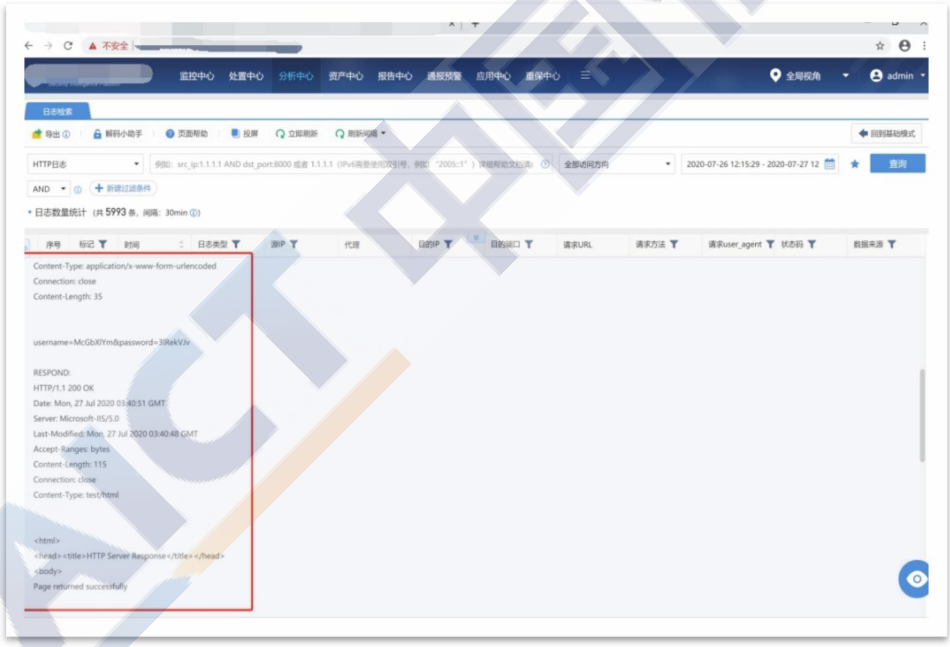
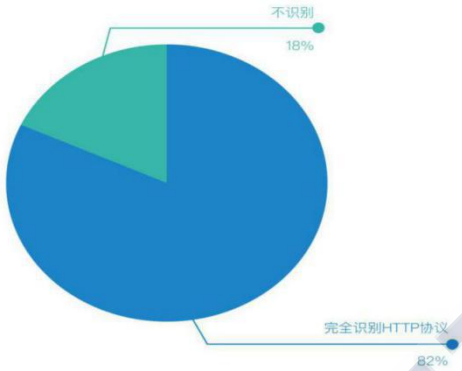


图 26 某产品 HTTP 协议还原测试结果截图 2

通过测试结果发现，**80%以上受测产品对 HTTP 协议全字段还原完整**。如图 27 所示，仅有 18%受测产品对 HTTP 协议解析不完整，仅

包含五元组等少量字段信息。



数据来源：测试结果

图 27 HTTP 协议支持比例

HTTP 协议解析是用来分析各类 Web 应用攻击的必要原始数据，如果受测产品功能侧重于攻击分析，则该协议的解析分析能力就为必要条件。对于侧重于 WEB 安全分析、WEB 业务分析的企业均对 HTTP 协议分析字段内容还原全面且完整，对于部分侧重于全网流量态势分析的企业，在 HTTP 协议解析细节方面并未做到完善。

2. 网络文件是否识别多由文件风险决定

在本测试用例中，利用流量发生器构造 HTTP 应用，每个 GET 动作请求一个文件，一共 50 余种文件类型，包括 mp3、pdf、jpg/jpeg、zip、exe、htm/html/xhtml、css、flv、avi、js、wav、docx、rtf、vxd、bmp、gif、png、xslx、vbe、vbs、ini、txt、dat、pem 等文件格式。通过受测产品查看可以支持识别文件类型的种类、系统信息、是否展示网络文件信息等。

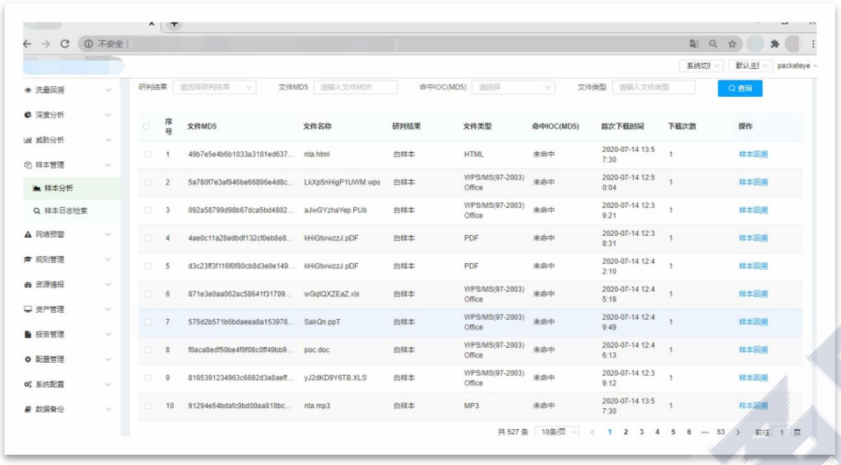
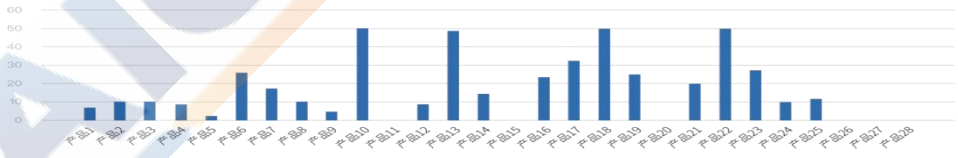


图 28 某产品文件识别功能测试结果截图

通过测试结果发现，**60%以上受测产品还原文件类型不超过 30 种**。由于现网的业务环境复杂，传输中的文件类型较多且存在自身占用空间较大，产品要对各类文件进行判断识别需要占用大量系统资源，而对于以网络攻击能力为主的产品通过识别文件类型并不能对分析网络攻击有更多的帮助，因此，未将有限的系统资源应用在此功能上，如果受测产品主要功能为信息内容或数据安全方面，则在此功能测试中应当会有较好表现。



数据来源：测试结果

图 29 产品还原文件类型数量

3. 网络正常文件内容还原仍需更加精准

在本测试用例中，利用流量发生器构造了 HTTP 应用，每个 GET

动作请求一个PDF文件，文件内容随机生成，包含关键词“CAICTNTA”。同时解析内容包括文件名、文件大小、文件格式、来源 IP、目的 IP、MD5 值、HASH 等信息。

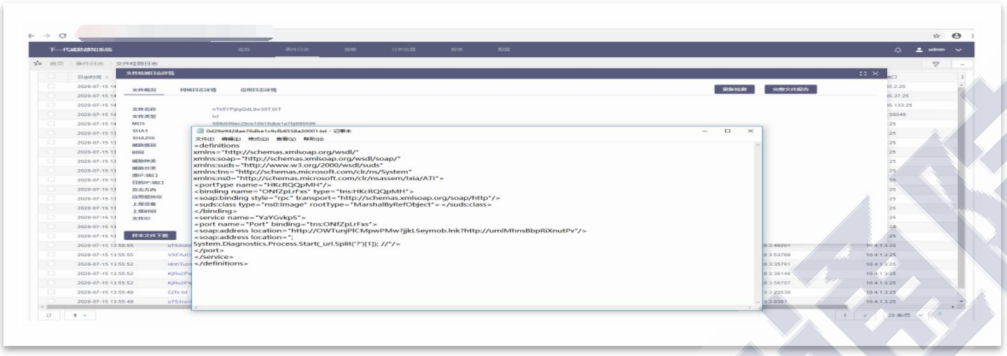
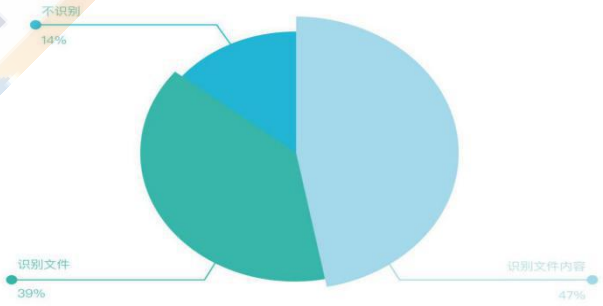


图 30 某产品 HTTP 协议还原测试结果截图

通过测试结果发现，**仅有部分受测产品完整还原出文件，并识别出文件中的关键词**。47%的受测产品能够满足该测试用例，其中部分产品需要提前配置好关键词策略，由流量发生器重新发起测试流量进行功能复测，可实现该功能。39%受测产品能识别出基本文件信息，包括文件名、文件大小、文件格式、来源和目的 IP、MD5 值、HASH 值等。14%的受测企业识别不到文件。



数据来源：测试结果

图 31 产品文件内容识别比例

通过和企业技术人员沟通得知，多数受测产品仅对有攻击特征的流量进行文件还原，以进一步利用沙箱分析，而作为普通的正常文件则不进行还原。

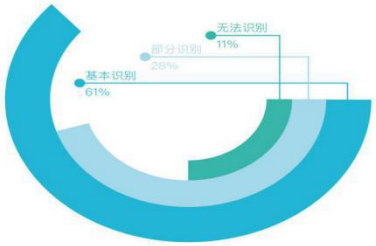
（三）NTA/NDR 产品中资产发现能力一般

在本测试用例中，利用流量发生器构造了四种应用协议，分别为 HTTP、SMB、FTP 和 SMTP 协议，并在流量中包含了服务器操作系统、软件组件、软件框架、数据库等资产信息，受测产品需要实现如下功能，一是查看受测产品是否能够准确对资产指纹识别。二是具有资产识别的独立功能且能从流量中获取资产信息的能力，三是能通过导入模板，对进行资产数据编写。四是通过 API 接口或导入功能进行资产数据上传。五是具备网络资产自动化补全等相关功能。

图 32 某产品资产识别功能测试结果截图

通过测试结果发现，**多数 NTA/NDR 类产品在资产识别方面能力表现平平**。61%受测产品识别出部分服务器、操作系统、软件组件、软件框架、数据库等资产信息。28%受测产品仅识别出了流量中资产五元组基本信息。11%受测产品不支持资产发现功能。多数 NTA/NDR

类产品并未将资产探测与管理作为主要能力。据了解，部分企业具有独立的网络空间资产测绘和管理产品，用于资产识别探测和管理。



数据来源：测试结果

图 33 产品资产识别功能比例

六、NTA/NDR 类产品安全分析能力分析

（一）具备各类网络攻击发现和分析能力

在本测试用例中，利用流量发生器构造了 8000 余种类型网络攻击，其中包括 Web 应用攻击、数据库攻击、内网渗透、通用应用漏洞攻击、后门识别、异常协议等，验证受测系统的网络攻击识别和分析能力。

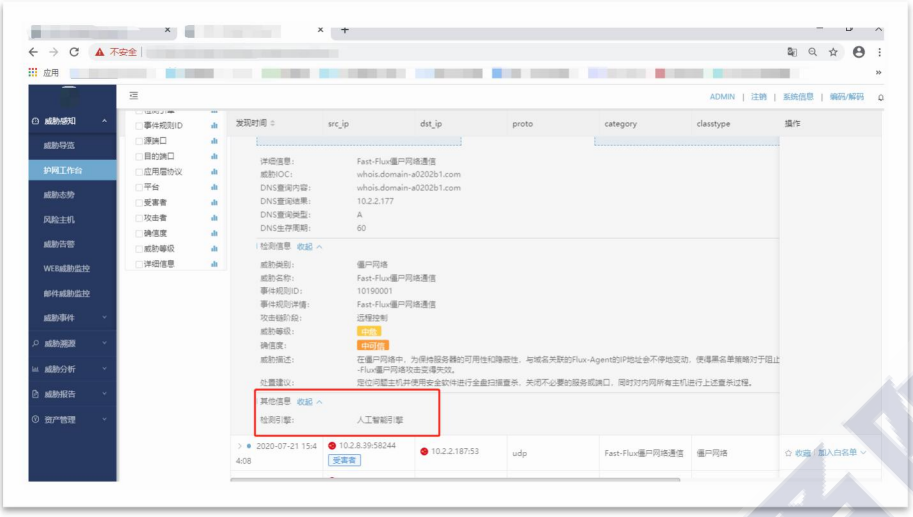


图 34 某产品网络攻击识别能力测试结果截图 1

通过测试结果发现，**多数企业可对网络攻击特征基本识别，需加强机器学习、数据图谱等高级关联分析和溯源展示能力。在网络攻击识别方面，**多数受测产品能识别出 Web 应用攻击、弱口令、暴力破解、扫描与爬虫、数据库攻击、敏感信息泄露、恶意通信流量、内网渗透、通用应用漏洞攻击、恶意软件、后门识别、异常协议等攻击行为。

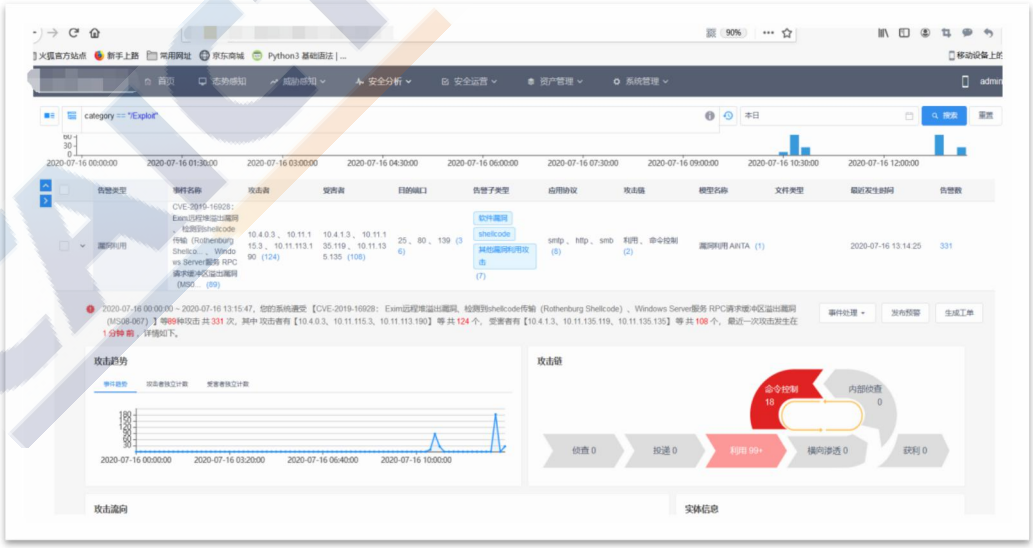


图 35 某产品网络攻击识别能力测试结果截图 2

在攻击分析手段方面，少部分企业具备安全分析模型配置、机器学习引擎配置等。**在攻击路径展示方面**，少部分企业支持多形式数据图谱关联分析。**在威胁溯源方面**，多数产品可基本实现基于 IP 的行为路径追踪。

（二）基本具备多步骤攻击关联分析能力

在本测试用例中，利用流量发生器构造具有完整攻击链的 APT 攻击，其中包括利用 Maze Ransomware、AZORult、Neutrino 等勒索病毒等恶意程序进行攻击，攻击方 IP 为 1.0.0.0 网段，查看受测产品是否具备针对网络勒索行为的自定义攻击场景、风险关联分析功能、是否具备自定义关联事件模板，按照既定事件以“与”关系进行组合，构建的攻击流量是否能触发自定义事件模板且能按预期输出安全场景告警。

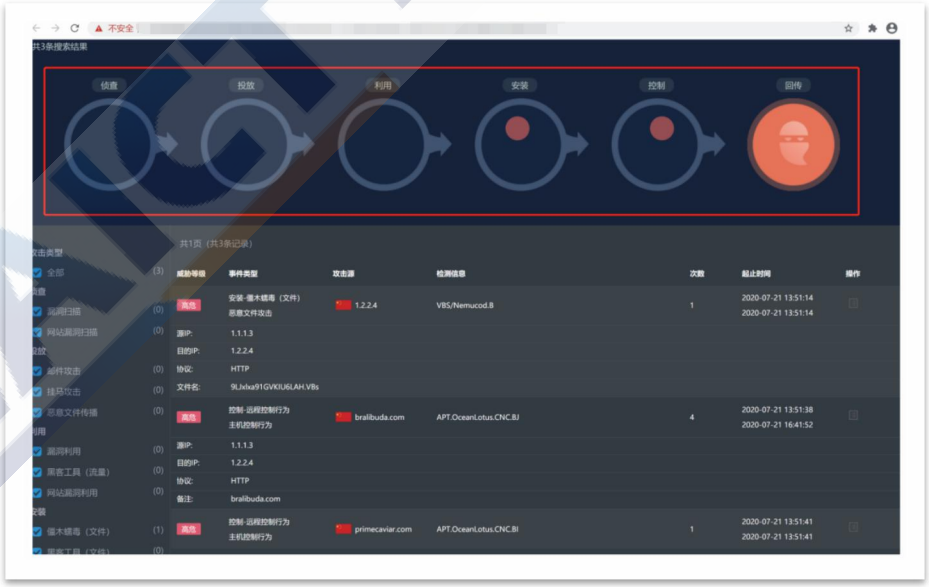


图 36 某产品 APT 攻击识别能力测试结果截图 1

[20] Maze Ransomware、AZORult31F、Neutrino：一些窃取信息的恶意程序、勒索病毒。

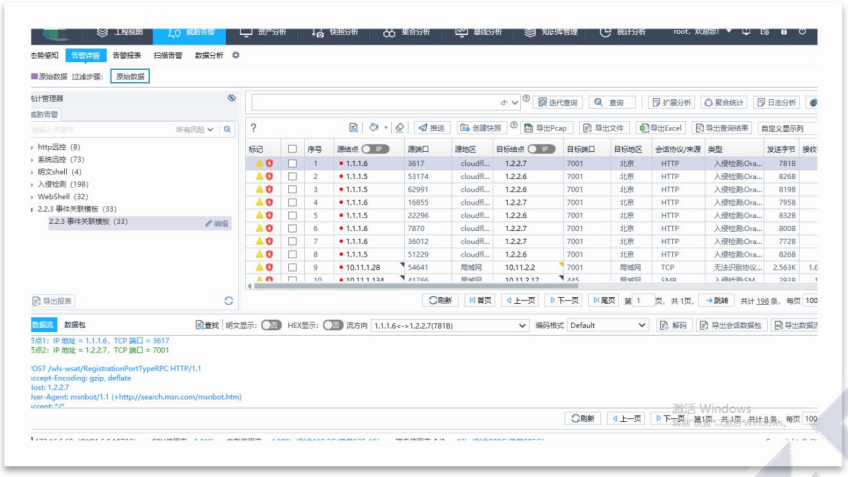
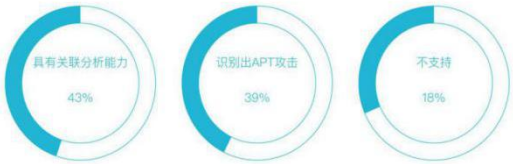


图 37 某产品 APT 攻击识别能力测试结果截图 2

通过测试结果发现，**多数受测产品虽具备基本关联分析能力，但能够准确分析测试用例中的网络勒索行为过程的较少。**如图 38 所示，18%受测企业发现测试流量中的攻击并绘制出勒索行为的多步骤攻击过程，43%受测企业虽然具备多步骤攻击的关联分析功能，但未识别测试流量中的网络勒索行为，39%受测企业不具备相关功能。对于无法自动识别出的网络勒索行为攻击链条的受测产品，多数可以通过各攻击特征的自定义查询功能和人工关联分析实现对网络勒索行为记录的关联查询。



数据来源：测试结果

图 38 产品 APT 识别能力比例

（三）网络恶意程序分析能力总体可用

在本测试用例中，利用流量发生器生成并发送了近七年（2014-2020 年）恶意程序攻击 6000 余种，其中包括多种文件类型、多种操作行为，以及多态病毒等各类变种攻击。受测产品查看系统是否能识别恶意文件能力，通过检出报告并和原厂人员进行访谈，确认恶意文件的检测方式，验证恶意文件的分析方式，不限于静态规则、动态沙箱、机器学习、威胁情报等。

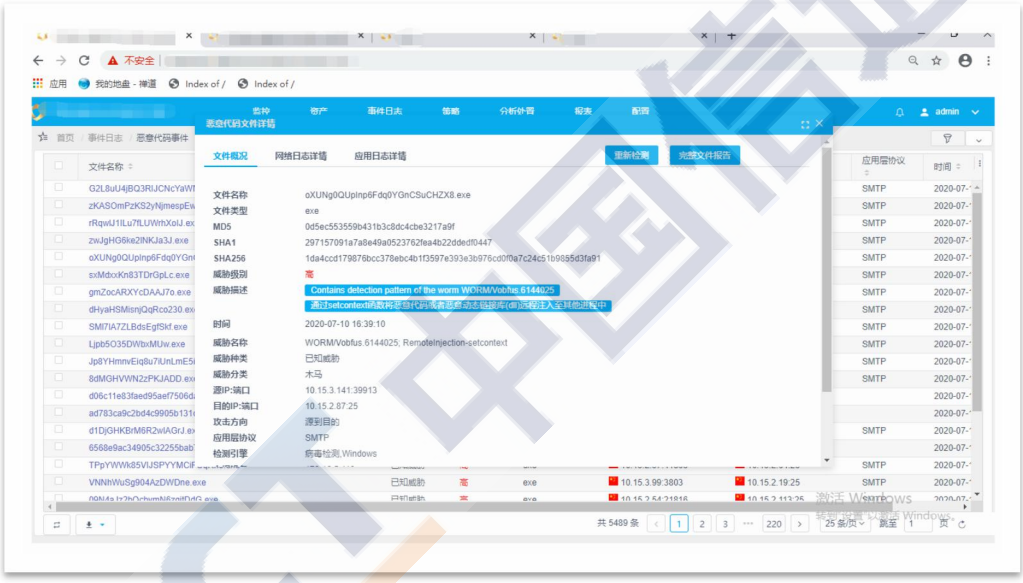
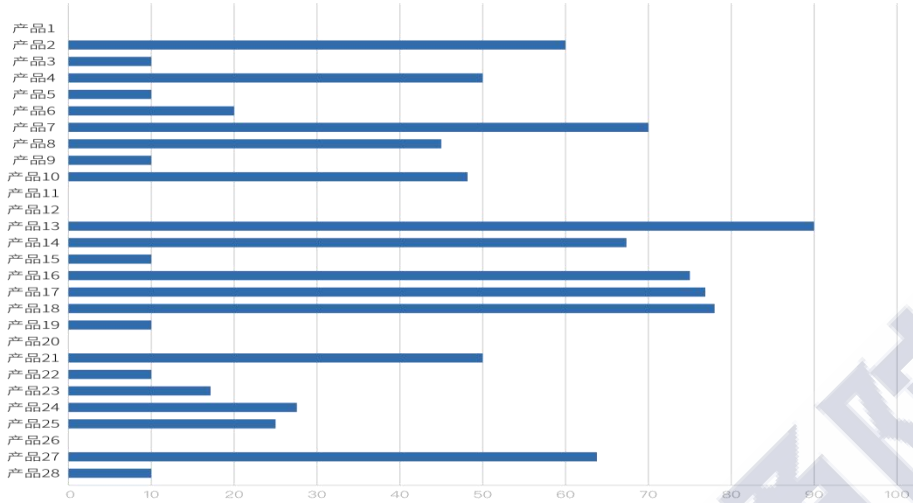


图 39 某产品恶意程序识别能力测试结果截图

通过测试结果发现，如图 40 所示，纵轴的分值为产品识别出的恶意程序占全部测试流量中恶意程序比例，其中有 15 个受测产品不具备或仅检测出少量恶意程序，其余产品检测出的恶意程序较多。测试效果表现较好的企业主要采用了流量识别分析和沙箱一体机，或者单独配备了专门的沙箱产品参与本次测试。



数据来源：测试结果

图 40 各产品恶意程序识别能力分值

七、NTA/NDR 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 NTA/NDR 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，需要在市场上完成产品的落地和被广泛采用，NTA/NDR 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）大规模攻防演练进一步催化 NTA/NDR 市场需求

随着攻防演练的规模化、常态化发展，未来将有越来越多的高级攻击以及基于零日漏洞的攻击，对企业防御能力提出更高的要求。NTA/NDR 基于流量的天然威胁检测优势，使其具备优秀的威胁感知和响应能力，能够在攻防演练乃至攻防实战中发挥足够作用，符合企

业的关键需求。因此，预计 NTA/NDR 的市场需求将快速增加。

（二）NTA/NDR 或着力产品差异化，打造核心卖点

简单地监测来自 SPAN[21]端口的流量不能成为网络流量监测与分析产品的核心竞争力和卖点，在这一功能上，已经有多种成熟的产品都可以实现，而 NTA/NDR 等主打网络流量监测与分析的产品需要进一步强调差异化和产品突出优势。溯源能力的提升、分析数据的广度（获取网络分析以外的更多数据，实现更大范围的威胁检测）、整多重逻辑的报警判断、事件响应能力将成为其突破重点。

（三）网络加密流量解析与分析成为新挑战

加密流量发展对于流量监测与分析提出了更大的挑战。目前市面上的 NTA/NDR 类产品大多不支持直接的加密流量解析，但加密流量趋势背景下，市场对此的需求是切实存在的。因此，企业或有三个方向。一是面对业务侧加密流量，选择 NTA+外部流量解密产品/技术的辅助来应对。二是面对恶意加密流量，进行有监督的 AI 行为学习，并结合人工介入分析。一方面，加密的出站流量标记为可疑流量，可以通过 NTA 报警，人工介入分析。另一方面加密流量的三次握手行为对 NTA 而言是可见的，通过与感知分析集成并结合威胁情况，可在一定程度评估、分析是否为恶意加密流量。

[21] SPAN，Switched Port Analyzer，直译为交换端口分析器。是一种交换机的端口镜像技术。作用主要是为了给某种网络分析器提供网络数据流，SPAN 并不会影响源端口的数据交换，它只是将源端口发送或接收的数据包副本发送到监控端口。

（四）联动攻击链的流量场景化分析需进一步落地

从攻防对抗中提炼典型，通过追踪关联多点攻击事件，建立与之对应的分析模型并最终输出具有场景化的对抗能力，是 NTA/NDR 在未来一段时间内仍需进一步落地实现的。

（五）流量分析转移到云上以实现可伸缩性成趋势

在收集和分析海量的流量数据过程中，中小型企业面临流量处理或储存能力受限的问题，而将分析转移到云上给出了更好的解决方案。基于云的流量分析有利于企业的数据处理和存储，并且在分析引擎添加和更换上有更好的灵活性。

八、NTA/NDR 类产品发展建议

（一）深耕自身技术优势，实现技术能力互补

在新冠肺炎疫情的影响与推动下，2020 年全球网络安全相关硬件、软件、服务市场的总投资将达到 1252.1 亿美元，较 2019 年同比增长 6.0%，与上期预测保持了较高的一致性 [22]。未来，我国将培育形成一批年营收超过 20 亿的网络安全企业，形成若干具有国际竞争力的网络安全骨干企业，网络安全产业规模超过 2000 亿 [23]。高市场份额的产业意味着会吸引更多的企业进入 NTA/NDR 类产品领域，建议各企业发挥自身产品优势，“深挖”自身技术能力，打造具有核心竞争力产品，避免产品同质化。推进产品核心技术能力创新，

[22] 来源于 IDC《全球网络安全支出指南》（Worldwide Security Spending Guide, 2020V2）
[23] 来源于工信部 2019 年《关于促进网络安全产业发展的指导意见（征求意见稿）》。

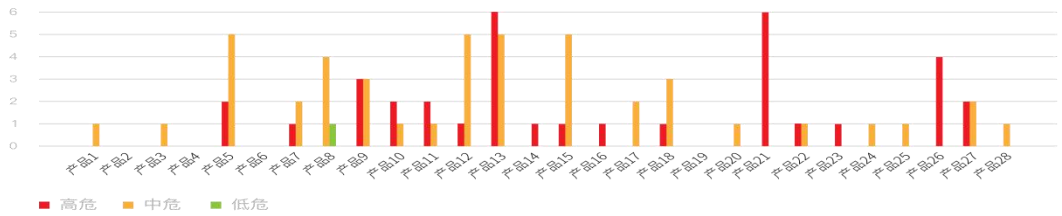
加强 NTA/NDR 技术领域产品优势互补，共同做大做强 NTA/NDR 类产品市场份额，引领行业市场良性发展。

（二）围绕新型网络场景，满足业务安全需求

随着 5G、工业物联网、物联网、云计算、大数据和人工智能等技术推动着信息化的发展，不同行业的核心业务也已经高度依赖信息化，但是信息化环境的复杂性也带来了不可预知的安全风险，网络安全的内涵和外延也在不断扩大。网络安全的目标逐渐由防止数据被破坏、被泄漏和网络瘫痪，进一步升级为保护网络空间安全，确保关键基础设施的安全，提升网络安全防护与对抗能力，保障数字化业务发展，从而确保生产安全、社会安全、和国家安全。因此，NTA/NDR 类网络安全产品也将经历从外到内的进化。“从流量采集与识别到开始运用大数据做到看见、看清威胁，再到开始逐渐从外部向内部进化，触及网络安全的本质。必须将 NTA/NDR 类网络安全产品能力建设于内部的业务系统之上，使信息化系统天生具备“免疫力”，进一步从根源解决网络安全问题，从而形成与信息化紧密融合的“内生安全”能力。

（三）夯实产品自身安全，保障可信可控可靠

通过对本次 NTA/NDR 类产品的渗透测试，发现多数受测产品均或多或少存在 WEB 安全漏洞。如图 41 所示，受测产品仅有 3 款产品暂未发现安全漏洞，接近 90%受测产品具有高危和中危漏洞的 WEB 应用漏洞，其中包括 XSS 跨站脚本漏洞、CSRF 跨站请求伪造、重要信息泄露、越权访问等问题。



数据来源：测试结果

图 41 各受测产品安全漏洞情况

在自身产品安全管理方面，建议加强针对自身产品的全生命周期安全管理，重点应当加强出货设备安全管理，对于出货的设备，无论是正式供货产品还是试用或测试产品，均应进行安全加固，将自身安全作为出货标准的一道“红线”。**在自身产品安全漏洞方面**，建议重点关注第三方开源组件或接口的安全性，使用第三方组件或接口前，产品应当通过全面渗透测试和安全加固。

九、NTA/NDR 类产品能力分组

（一）专业能力领域

综合技术能力组（排名不分先后）	
厂家	产品
知道创宇	创宇云图威胁检测系统
兰云科技	兰眼下一代威胁感知系统
恒安嘉新	金睛企业安全威胁感知系统
斗象科技	PRS-NTA 全流量存储与分析系统
绿盟科技	绿盟全流量威胁分析系统
深信服	深信服安全感知平台
腾讯安全	腾讯 T-Sec 高级威胁检测系统

流量识别能力组（排名不分先后）	
厂家	产品
恒安嘉新	金睛企业安全威胁感知系统
科来	科来全流量安全分析系统

兰云科技	兰眼下一代威胁感知系统
派网软件	Panabit 一体化智能应用网关
深信服	深信服安全感知平台
神州灵云	神州灵云网络全流量分析系统

安全分析能力组（排名不分先后）	
厂家	**产品**
安恒信息	AiLPHA 大数据智能安全平台
安天	安天探海威胁检测系统
东巽科技	铁穹高级持续性威胁预警系统
斗象科技	PRS-NTA 全流量存储与分析系统
恒安嘉新	金睛企业安全威胁感知系统
兰云科技	兰眼下一代威胁感知系统
绿盟科技	绿盟全流量威胁分析系统
奇安信	奇安信网神新一代安全感知系统
深信服	深信服安全感知平台

（二）行业应用能力领域

运营商行业应用组（排名不分先后）	
厂家	**产品**
安博通	安博通网络流量分析系统
浩瀚深度	HDS2000 系列产品流量分析系统
微智信业	微智互联网威胁感知系统
亚信安全	亚信网络流量分析系统 SpiderFlow 亚信安全深度威胁发现设备 TDA
中电福富	福富全流量分析监控系统
中移杭研	中移网络入侵检测分析系统

政府行业应用组（排名不分先后）	
厂家	**产品**
深思科技	深思全流量威胁极速检测系统
安态科技	安态网络安全威胁感知系统
一知安全	大圣网络威胁预警平台
友道信息	钛石网络安全流量监测分析系统
中新网安	中新金盾高级持续性威胁防御平台

关于

中国信息通信研究院简介

中国信息通信研究院始建于 1957 年，是工业和信息化部直属科研事业单位。多年来，中国信通院始终秉持“国家高端专业智库产业创新发展平台”的发展定位和“厚德实学兴业致远”的核心文化价值理念，在行业发展的重大战略、规划、政策、标准和测试认证等方面发挥了有力支撑作用，为我国通信业跨越式发展和信息技术产业创新壮大起到了重要推动作用。

中国信息通信研究院安全研究所简介

中国信息通信研究院安全研究所，是专门从事 ICT 领域安全技术研究的科研机构，主要职责包括开展信息通信领域安全的战略性和、前瞻性、技术性问题研究，为国家主管部门有关网络安全发展战略、决策、规范的制定提供强有力的技术支撑。安全所拥有雄厚的网络安全技术评估评测能力以及高端的专业网络安全支撑团队，承担大量重大网络安全专项科研课题，牵头制定大量国际国内网络信息安全标准规范，对前沿新兴网络安全技术的研究有深厚积累。

FreeBuf 咨询简介

FreeBuf.COM 网络安全行业门户，每日发布专业的安全资讯、技术剖析，分享国内外安全资源与行业洞见，是网络安全从业者与爱好者广泛关注的行业社区平台。FreeBuf 咨询集结安全行业经验丰富的安全专家和分析师，常年对信息安全技术、行业动态保持追踪，洞悉安全行业现状和趋势，呈现最专业的研究与咨询服务。

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

邮政编码：100191

联系电话：010-62308680

传真：010-62300264

网址：www.caict.ac.cn