CAICT 中国信通院　FreeBuf 咨询

国内网络安全信息与事件管理类产品研究与测试报告

（2021 年）

——先进网络安全能力验证评估系列报告

中国信息通信研究院安全研究所
上海斗象科技有限公司

2021 年 3 月

版权声明

前　言

安全运营是企业对于网络安全工作的有效管理和高效输出。随着企业规模变大、面临的威胁环境更为复杂，如何通过有限的人员对数量庞大的安全事件进行管理与快速响应，如何更精确的度量当前的关键安全指标，如何将安全工作与业务有效结合更好地赋能业务，这是安全运营不断发展、优化的意义所在。

随着业界对安全运营活动的认知逐渐改变，用户行为分析、安全编排自动化与响应、威胁情报等等，都被列入安全运营的核心需求。

总体来看，安全运营的发展过程是一个技术不断融合、内涵不断丰富的过程，当下以及未来一段时期内的安全运营将会是以SIEM[1]/SOC[2]为核心，结合大数据分析、机器学习、人工智能技术，融合更多运营功能，形成新一代安全运营服务。

如果将安全产品与技术作为企业安全工作的输入，那么良好的安全事件运营则是企业安全能力的稳定输出。而现在，日益复杂的安全事件与落后的安全运营能力成为了现阶段安全建设中的主要矛盾。安全建设的输入和输出处于非常不对等的情况。

对企业而言，安全管理及运营涉及方方面面，不仅仅从单点去考虑，还需要从企业整体安全运维的角度，根据不同的安全侧重点，体系化分类管理安全事件，做到事件管理标准化、关联信息详实化、人员/工具定位精准化，这样才可以做到高效安全响应。

[1] SIEM：Security Information And Event Management，指安全信息和事件管理。
[2] SOC：Security Operations Center，指安全运营中心。

为了更好地满足基础电信和互联网、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，中国信息通信研究院（以下简称“中国信通院”）安全研究所联合 FreeBuf 咨询共同完成了此次 SIEM/SOC 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。本次测试是对各企业的 SIEM/SOC 类产品的“能力拔高测试”，以体现该产品在某一个技术能力领域的硬核实力。测试方案内容不仅基于现有相关标准，并且依据 Gartner 对 SIEM/SOC 的能力定义以及综合国内各安全企业最佳实践。到报名截止日期 2020 年 10 月 23 日为止，共有 20 款产品报名，符合测试要求的 14 款产品参与此次验证评估。

本报告由中国信通院安全研究所对国内主流SIEM/SOC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，并深入总结国内 SIEM/SOC 类产品的基本现状，并尝试对其发展趋势进行评估和预测，为企业安全建设提供有效参考，提升安全运营与响应能力。

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）：

北京神州绿盟科技有限公司、杭州安恒信息技术股份有限公司、

北京安达亚科技有限公司、新华三信息安全技术有限公司、中电福富信息科技有限公司、任子行网络技术股份有限公司、北京神州泰岳信息安全技术有限公司、网神信息技术（北京）股份有限公司、厦门服云信息科技有限公司、北京盛华安信息技术有限公司、亚信科技（成都）有限公司、上海观安信息技术股份有限公司、腾讯云计算（北京）有限责任公司、深信服科技股份有限公司。

目 录

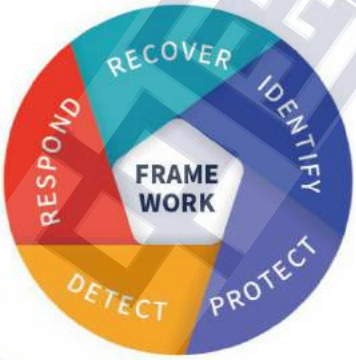
图 目 录

表 目 录

一、安全运营的演变与发展

（一）安全运营的定义

根据 2014 年美国 NIST[3] 发布的 Cybersecurity Framework，安全运营可以拆解为 5 个版块：风险识别（Identify）、安全防御（Protect）、安全检测（Detect）、安全响应（Response）和安全恢复（Recovery）。而安全运营的核心即解决问题，通过提出安全解决构想、验证效果、分析问题、诊断问题、协调资源解决问题并持续迭代优化，推动整体安全目标的实现。



资料来源：NIST

图 1 Cybersecurity Framework

随着企业规模变大、面临的威胁环境更为复杂，如何通过有限的人员对数量庞大的安全事件进行管理与响应，如何将安全工作与业务有效结合更好地赋能业务，是安全运营不断发展、优化的目的所在。

[3] NIST：National Institute of Standards and Technology，指美国国家标准与技术研究院。

（二）安全运营的发展

经过近 30 年的发展，国内的安全运营从粗放型逐渐转向业务与技术双驱动的精细化运营。

（1）基础架构阶段

八九十年代末，计算机应用迅速拓展，第一批计算机安全相关政策、举措开始实施，重点行业、大型企业的安全需求开始显现。这一时期，头部行业的企事业单位正视网络安全，将其作为系统建设中的重要内容之一，并且建立专门的安全部门以开展信息安全工作。网络安全厂商迎来初步发展期，将其主要研发精力投入于防火墙、IDS、杀毒软件三大件上，奠定了传统的安全运营基础架构。

（2）快速发展阶段

九十年代末至 2010 年，国内网络安全行业基本结束野蛮生长阶段。等级保护相关标准规范体系相继密集出台，中小型企业、传统企业将补全安全能力作为主要安全建设工作，而安全运营的主要手段依然以防火墙、IDS、防病毒为主，呈现快速发展、被动防御的特点。

（3）体系化阶段

2010 年后，随着国内大部分企业完成信息安全建设进程，国家和企业对于合规需求进一步升级，安全运营迎来体系化发展阶段。

安全管理中心、态势感知等安全运营理念在信息系统建设中同步运用。企业将安全运营作为体系化工作开展，以基础安全设备为

边界防护，内部建立完整的安全运营中心/体系，进行整体安全规划、逐步开展自研并引入国内外多种安全运营理念。

（4）技术驱动阶段

2018 年后，AI、大数据、云计算飞速发展，新技术催生了新的业务场景，也让企业面临传统安全边界消失、攻击面无处不在、业务增长带来的数据量暴增等问题。为了实现快速、持续的响应，安全人员不得不与复杂的操作流程以及匮乏的资源、技能和预算做斗争。然而此起彼伏的安全事件让安全运营人员即便依托安全运营平台，仍然疲于应付。企业开始寻求更高效、自动化的安全运营方式，安全运营从被动式转变为主动式，注重从防御、检测、响应和预测四个维度构建纵深的网络安全运营体系。

（三）安全运营的技术实践

本质上，安全运营是一个安全理念和运营体系，而在国内外落地过程中，安全运营逐渐衍生出多种形态，如常见的 SIEM、SOC、态势感知平台等。一般来说，不同国家、不同厂商对于某一安全运营产品/解决方案的名称可能存在差异，通过目前市面上已有的安全运营产品/服务/架构的了解，能够帮助企业更好地理解安全运营是如何把技术、流程和人结合起来服务于安全的。

表 1 安全运营各类形态要点整理

序号	落地形态	类别	适用企业	重要组件/技术	重要功能
1	SIEM 安全信息和事件管理	技术、产品	中小型企业；大型组织	日志管理系统、多个检测和分析组件	聚集系统日志和事件，使用关联和统计模型识别潜

					在的安全事件，向安全人员发出警报，并提供上下文信息以协助调查
2	SOC 安全运营中心	技术、流程、组织	安全体系建设完善的企业；大型组织	漏洞扫描程序、渗透测试工具、入侵检测系统、端点检测和响应（EDR）、日志管理系统	协助管理人员进行事件分析、风险分析、预警管理和应急响应处理
3	NGSOC 态势感知与安全运营平台	技术、流程、组织	安全体系建设完善的企业；大型组织	大数据平台、基于威胁情报的监测、数据采集、基于机器学习的安全分析	海量数据、关联分析、对安全趋势的预测
4	SRC 安全应急响应中心	组织	安全体系建设完善的企业	漏洞报告平台/xSRC	情报搜集和汇总、事件处理，建立内部和外界的沟通
5	SOAPA 安全运营和分析平台架构	架构、组织	大型组织	端点检测/响应（EDR）、事故响应平台（IRP）、反恶意软件沙箱、漏洞扫描器和安全资产管理	基于架构的分析管理，安全分析人员能采用不同工具，进行实时的数据挖掘和威胁处置

资料来源：Freebuf.com

在以上多个安全运营形态中，技术、流程和人都必不可缺，且安全运营能力重点体现在数据收集、事件分析及响应等方面。

近几年，安全运营的各种形态在不断集成、融合其他安全技术、工具和策略，在优化发展过程中，不同的安全运营平台/产品相互之间存在一定的功能交叉甚至重合。比如，SIEM 作为重要的检测响应技术，被 SOC、SOAPA 等多个安全运营形态采用与融合，并且在安全运营中扮演重要角色。因此，尽管 SIEM、SOC 等在能力侧重点、技术等细节上存在差异，但在安全运营能力的整体提升方面的目标仍然是一致的。

二、安全信息实践管理技术发展现状

（一）技术早期发展

在 SIEM 萌芽阶段，收集 IT 网络资源产生的各种日志，进行存储和查询的日志管理是行业主流。而建立在日志管理之上的 SIM[4]和 SEM[5]就在这一时期出现。初代 SIEM 的定义也由此开启，2005 年，Gartner 首次将 SIM 和 SEM 整合到一起，并提出了 SIEM 的概念，为安全运营和管理揭开了新的篇章。

此后，随着安全合规政策的出现，又衍生出了新一代日志管理技术 LM[6]。LM 与前者的区别在于，更加强调日志的广泛收集、海量存储、原始日志保留及安全合规，并借鉴搜索引擎技术实现快速检索分析能力。

现代 SIEM 的定义实质上融合了 SIM、SEM、LM 三者，尽管各个厂商产品间的重点技术能力略有区分，但以此为基础的大方向是一致的：即基于大数据基础架构的集成式 SIEM，为来自企业和组织中所有 IT 资源产生的安全信息（日志、告警等）进行统一实时监控、历史分析，对来自外部的入侵和内部的违规、误操作行为进行监控、审计分析、调查取证、出具报表报告，实现 IT 资源合规性管理的目标。

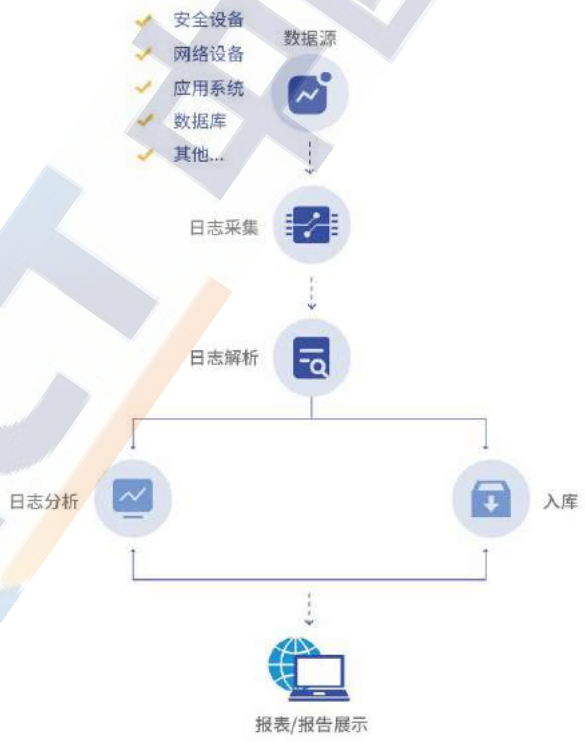
2010 年后，伴随着安全运营的热度 SIEM 同样迎来蓬勃发展期，

[4] SIM：Security Information Management，指安全信息管理。
[5] SEM：Security Event Management，指安全事件管理。
[6] LM：Log Management，日志管理

在市场占领和技术成熟度上都有了突破。2013 年，SIEM 全球市场规模达到 15 亿美元，相比 2012 年度增长 16%，预示着 SIEM 市场完全成熟且竞争激烈。同时，在合规要求下，SIEM 的目标群体转向中小型企业，为了解决小型企业无力购买整体 SIEM 解决方案/服务、缺乏管理 SIEM 的专业员工等问题，SIEM 开始在产品形态、功能，还有商业模式上进行创新，推出 SaaS 软件即服务，进一步推动 SIEM 的广泛部署。

（二）基础核心能力

SIEM/SOC 的核心功能包括了日志收集、跨源关联和分析事件能力等，常见 SIEM 工作流程可参考下图：



资料来源：FreeBuf.com

图 2　常见 SIEM 工作流

SIEM 在数据流水线的每个阶段都需要进行精细的管理、数据提取、策略、查看警报和分析异常。其中，SIEM 的核心技术点包括：

日志采集及处理

SIEM 需要从企业相关组织系统中广泛收集日志和事件，每个设备每次发生某事时都会生成一个事件，并将事件收集到平面日志文件或数据库中。SIEM 的任务是从设备收集数据，对其进行标准化并将其保存为能够进行分析的格式。一般来讲，SIEM 通过四种方式收集数据：

表 2 SIEM/SOC 日志汇总的四种方式

系统日志	标准的记录协议。网络管理员可以设置一台 Syslog 服务器，以接收来自多个系统的日志，并将其以高效，简洁的格式存储，该格式易于查询。
事件流	SNMP/Netflow/IPFIX 等协议允许网络设备提供有关其操作的标准信息，这些信息可以被日志聚合器拦截，解析并添加到中央日志存储中。
日志收集器	在网络设备上运行的软件代理，捕获日志信息，对其进行解析，然后将其发送到集中的聚合器组件以进行存储和分析。
直接访问	日志聚合器可以使用 API 或网络协议直接访问网络设备或计算系统，以直接接收日志。这种方法需要对每个数据源进行自定义集成。

数据来源：FreeBuf.com

在日志采集后，SIEM 还需要进行日志处理，即从多个来源获取原始系统日志后，识别其结构或架构并将其转变为一致的标准化数据源的技术。

日志关联分析

SIEM 需要汇总所有历史日志数据并进行实时分析警报，通常通过分析数据建立关系，以帮助识别异常、漏洞和事件，这也是 SIEM 最关键的一项能力。传统 SIEM 产品使用关联规则和脆弱性和风险评估技术从日志数据生成警报，但是这两种技术存在误报及新型威胁难以抵御地风险，因此部分头部 SIEM 厂商积极应用实时关联分析引擎，分析数据包括对安全事件、漏洞信息、监控列表、资产信息、网络信息等信息，同时应用机器学习、用户行为分析等高级分析技术，着力提高 SIEM 的智能分析能力。

安全产出

SIEM 处于安全运营的关键环节，其应用目的之一便是帮助安全运营人员高效处理安全事件。因此清晰完善的安全产出尤为重要。例如根据安全事件产出相关报告，如人员异常登录报告、恶意软件活动报等，同时根据事件分析产生安全警报。SIEM 安全产出主要提供警报和通知、仪表盘、数据探索及 API 和 WEB 服务等能力。

尽管 SIEM 在事件分析和响应上已有成熟的体系，但近几年趋向复杂化、高级化的网络攻击依然对于以 SIEM 为主要解决方案的安全运营提出了挑战。**一是** SIEM 采用关系数据库技术构建，但随着日志数据源的数量增加，数据库的负载不断加重，限制了实时响应能力；**二是** SIEM 在运行中会产生大量告警事件，“告警过载”等于无告警；**三是** SIEM 采用模式匹配引擎技术（签名技术）进行上下文的匹配，

容易产生大量误报；**四是** SIEM 简单地将事件的严重程度划分为高、中、低，缺乏细致的决策参考，对企业网络安全专业人才的技能提出更高的要求。

根据 CMS Distribution 公司对企业安全运营的技术调研发现，传统的SIEM解决方案产生大量告警事件使得安全运营人员分身乏术，同时专业安全技能人才的缺失，使得传统 SIEM 解决方案的平均寿命已经缩短到 18-24 个月，无法有效应对云计算、大数据、物联网、人工智能新时代的网络安全挑战。当 SIEM 的不足开始凸显，企业的安全水位线难以被满足，也亟须 SIEM 有新的突破以应对更高级的威胁。

三、国内 SIEM/SOC 类产品应用现状

（一）国内企业安全运营态势画像

1. 安全检测类产品部署现状

大多数企业都依靠部署安全产品和解决方案管理安全和合规建设。根据调研结果，有 33.5%的受访企业部署了 11 个以上的网络安全检测类产品，部署数量在 6-10 之间的企业占比为 16.7%。

数据来源：FreeBuf.com

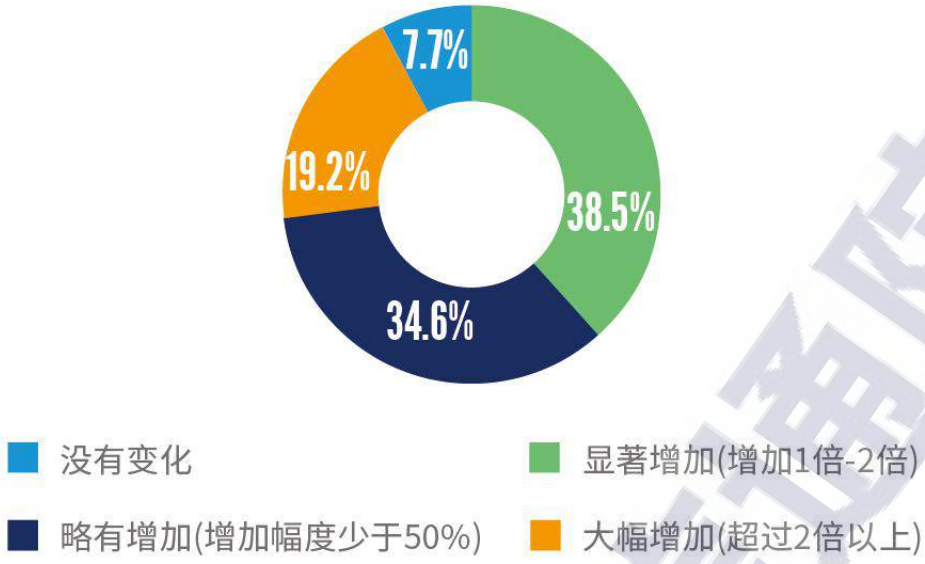
图 3　企业部署网络安全检测类产品的数量比例

直观地看，通过众多安全检测类产品的部署，企业具备相对成熟的单点安全防护能力，安全团队能够解决大部分基础安全问题。此外，企业对安全建设的投入和重视程度也可见一斑。

2. 安全警报数量现状

随着安全检测产品部署数量的增加，势必会产生更多的安全警报。对此，报告分别针对企业安全警报数量、安全警报变化状态和产生原因进行了调研，详细调研结果如下：

■ **过去 1 年中，企业安全事件警报的数量如何变化？**

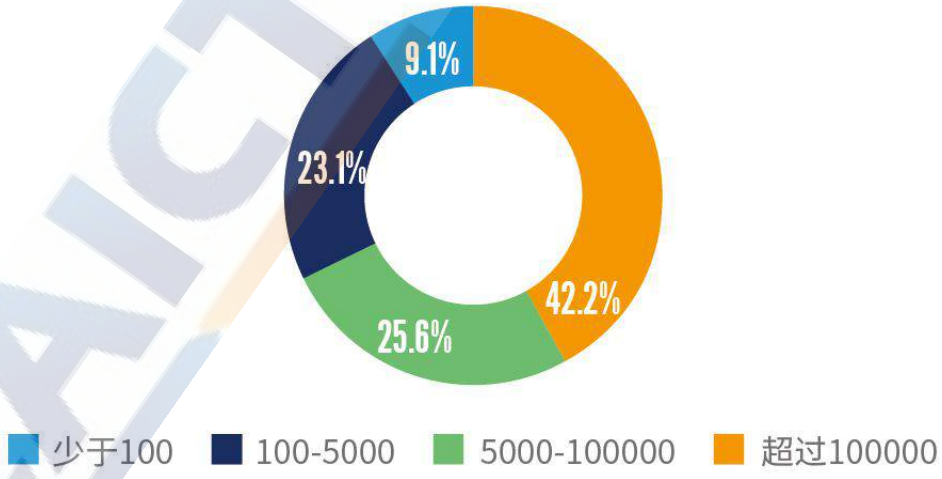


数据来源：FreeBuf.com

图 4　企业安全事件警报数量

调研结果显示，38.5%的受访企业在过去一年间的安全事件警报数量显著增加（增加 1 倍-2 倍），19.2%的企业在过去一年间的安全警报数量呈现大幅增加（超过 2 倍 以上），仅有 7.7%的企业表示过去一年的安全警报数量几乎没有变化。

■ **企业过去一年间大约处置了多少有效安全警报事件？**

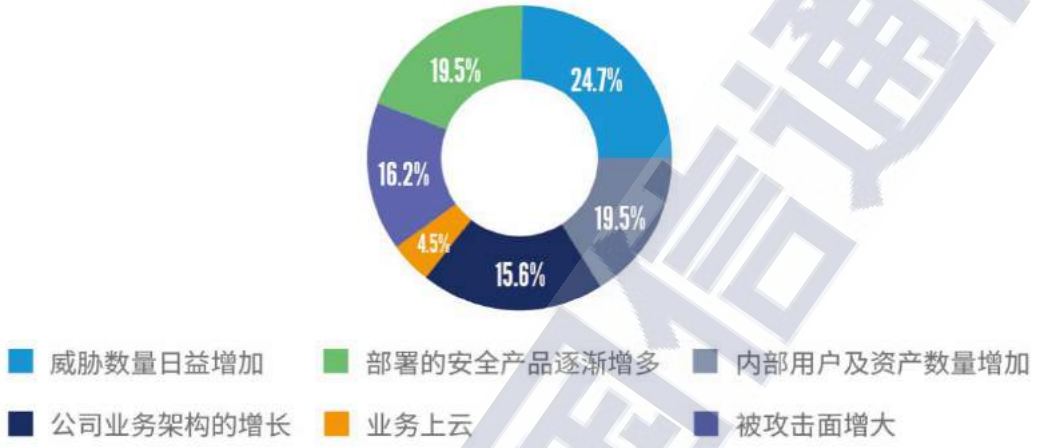


数据来源：FreeBuf.com

图 5　企业安全警报有效事件处理

调研结果显示，23.1%的受访企业在过去一年间处置了 100000+的安全警报，仅有 9.1%的企业在过去一年间处置了少于 100 的安全警报。

■ **是什么问题导致安全警报事件增加？**



数据来源：FreeBuf.com

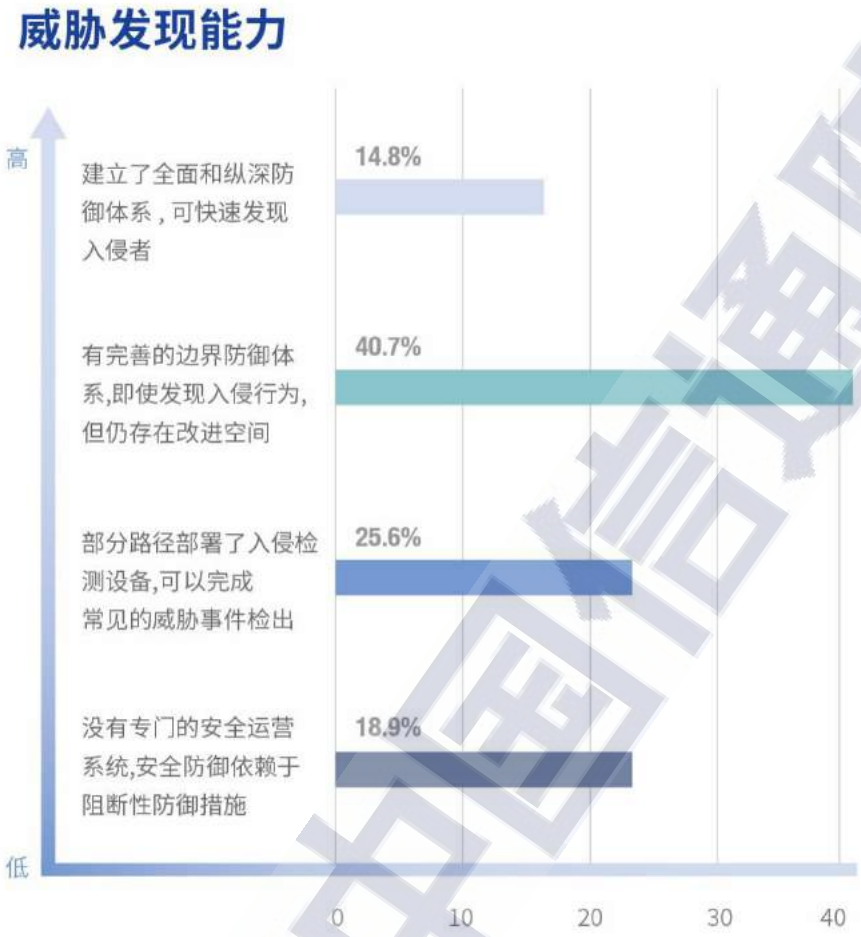
图 6　企业安全警报数量增加原因

根据调研结果，共有 63.7%的受访企业认为【威胁数量日益增加】、【部署的安全产品逐渐增多】、【内部用户及资产数量增加】是企业安全警报数量激增的核心原因。

3. 企业安全运营&威胁发现能力现状

针对企业安全运营&威胁发现能力现状，报告分别从企业威胁发现能力自评、企业安全运营能力自评、企业安全运营问题三个方面进行了调研。详细调研结果如下：

■ **企业目前威胁发现能力的评价为：**

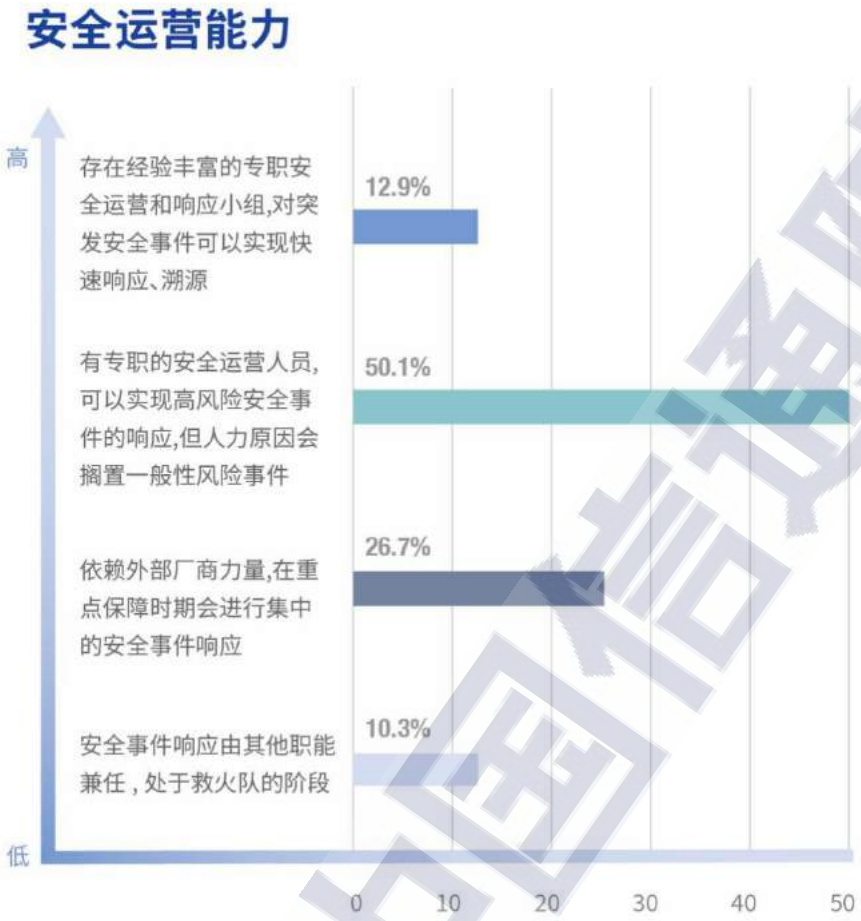


数据来源：FreeBuf.com

图 7　企业威胁发现能力评价

根据调研结果，四成的受访企业认为自己【有完善的边界防御体系，可及时发现入侵行为，但仍存在改进空间】，仅有 14.8%的受访用户具备自信并表示自己【建立了全面和纵深防御体系，可快速发现入侵者】。

■ **企业目前的安全运营能力评价为：**

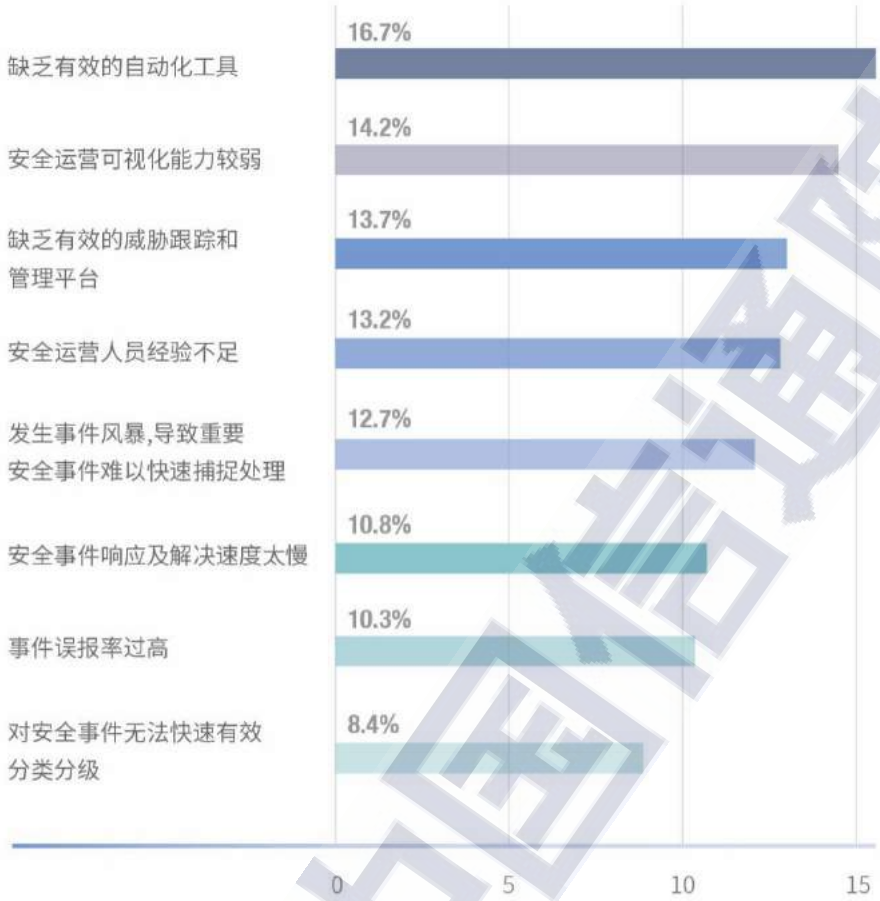


数据来源：FreeBuf.com

图 8　企业安全运营能力评价

根据调研结果，半数受访企业认为安全运营能力处于【有专职的安全运营人员，可以实现高风险安全事件的响应，但人力资源会搁置一般性风险事件】的阶段。值得关注的是，安全运营能力成熟度最高级和最低级的企业比例相当，这也意味着目前国内企业安全运营能力仍处于两极分化阶段，不乏已经在安全建设及运营阶段走在前列的国内企业，但同时仍旧有部分企业处于初级救火队的阶段。

■ 企业面临着哪些安全运营问题？



数据来源：FreeBuf.com

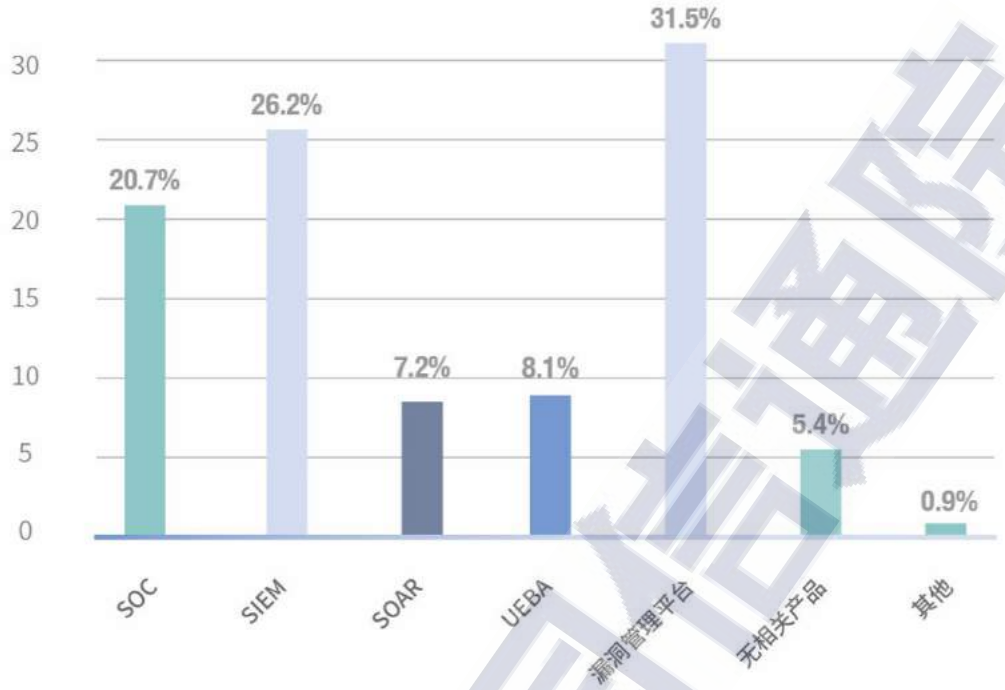
图 9　企业安全运营能力缺陷问题分析

根据调研结果，【缺乏有效的自动化工具】、【安全运营可视化能力弱】、【缺乏有效的威胁跟踪和管理平台】、【安全运营人员经验不足】是大多数企业面临的运营问题。

（二）国内安全信息和事件管理类产品应用现状

1. 安全信息和事件管理类产品国内部署现状

■ **企业是否选择部署安全信息和事件管理类产品？**



数据来源：FreeBuf.com

图 10 企业是否选择部署安全信息和事件管理类产品

从调研结果来看，针对安全信息和事件管理类产品的部署选择，有 46.9%的企业已经部署 SIEM/SOC 产品。同时报告也观察到，近九成企业不会选择单独部署 SIEM/SOC 产品，同时还会配合 UEBA、SOAR、漏洞管理等产品进行综合应用。

■ **企业部署商用安全信息和事件管理类产品的品牌选择：**

商用安全信息和事件管理类产品的厂商品牌较多，竞争也非常激烈。根据调研结果，国内企业对安全信息和事件管理类产品的品牌选择上，国外厂商并不占据压倒性优势地位，有 51.1%的企业选择部署国内厂商的产品。

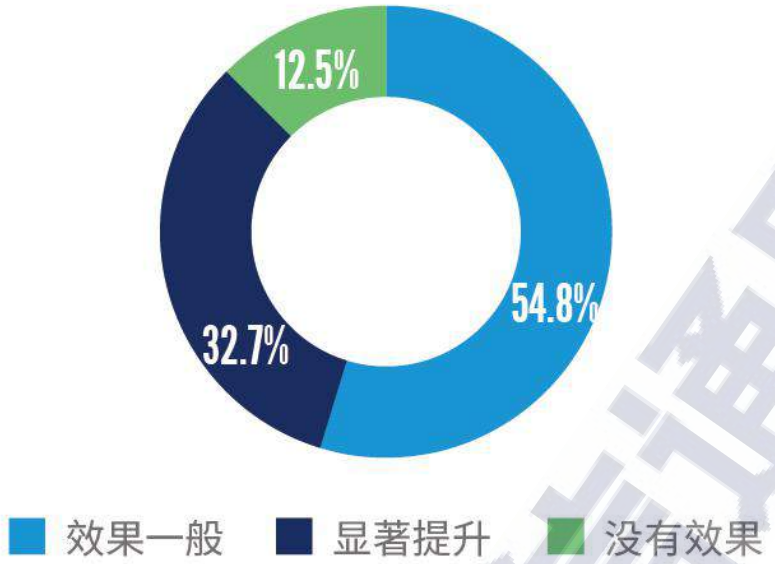
数据来源：FreeBuf.com

图 11 国内企业品牌选择

国内厂商布局安全信息和事件管理类产品也是近几年开始的动作，在 Gartner 历年发布的 SIEM 产品魔力象限中，无论在市场还是技术领域，无一例外都是国外厂商占据领导者地位。但随着近几年国内安全信息和事件管理类产品市场的猛烈需求和发展，国内厂商也在纷纷投入精力切入该市场，根据该调研结果也能看到国产厂商在国内安全信息和事件管理类产品市场发展中所做的努力与成果。

2.安全信息和事件管理类产品使用效果评价

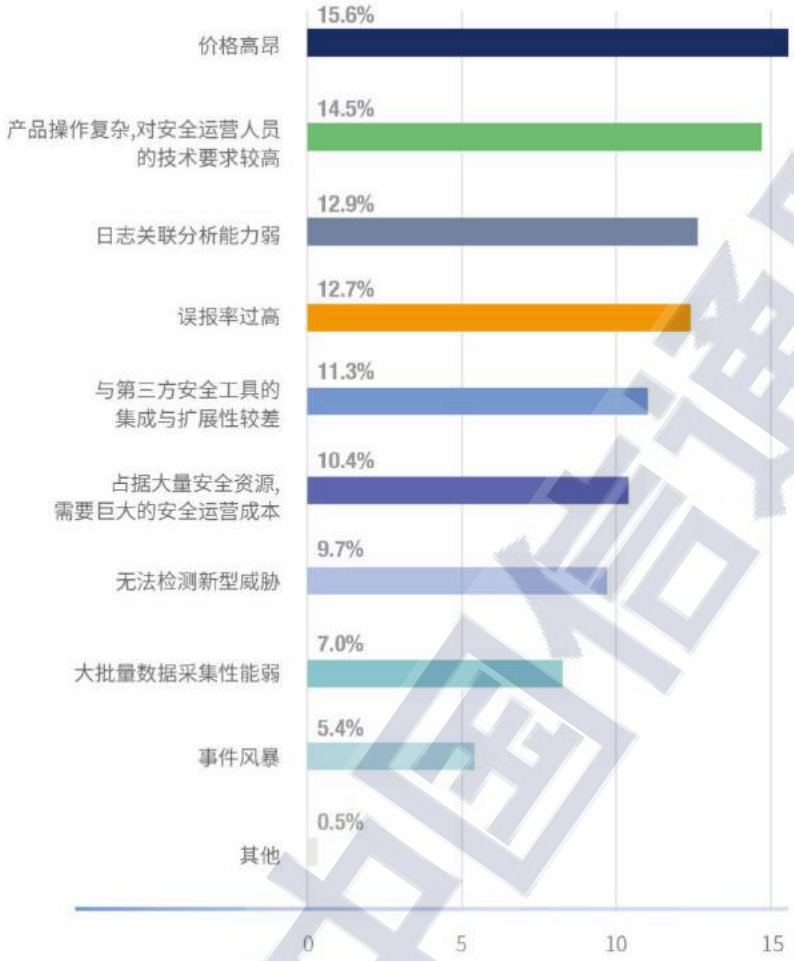
针对已部署 SIEM 地调研对象，54.8%的企业认为部署 SIEM 对企业安全运营效率提升的效果一般，32.7%的企业认为部署 SIEM 可以显著提升企业安全运营效率。



数据来源：FreeBuf.com

图 12 产品使用效果评价

根据调研，企业用户对现阶段 SIEM 产品不满意的问题主要集中在以下六个方面：【价格高昂】、【产品操作复杂，对安全运营人员的技术要求较高】、【日志关联分析能力弱】、【误报率过高】、【占据大量安全资源，需要巨大的安全运营投入】、【与第三方安全工具的集成性较差】。



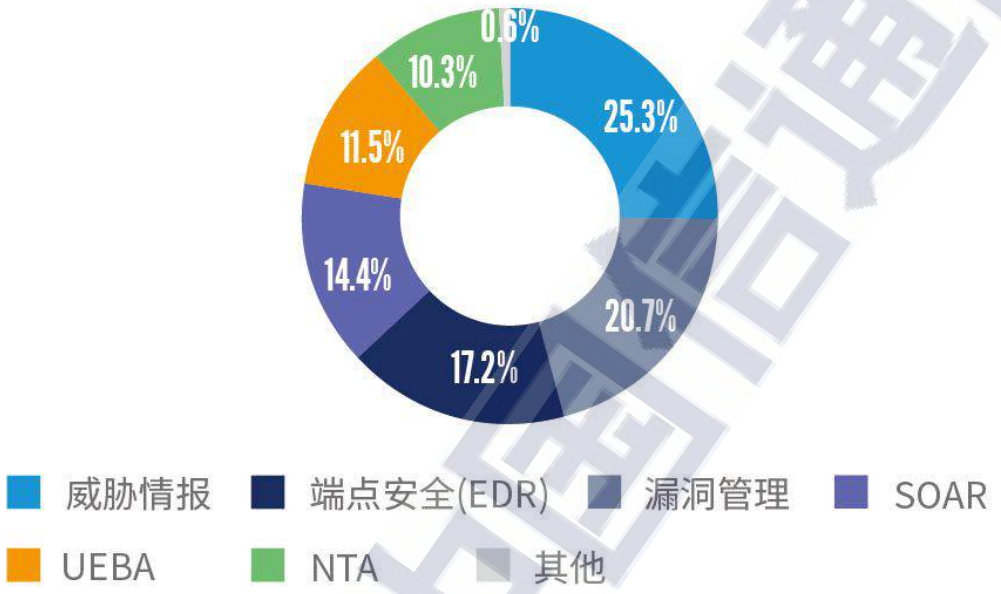
数据来源：FreeBuf.com

图 13 企业对 SIEM 类产品不满意调查

3. 企业对 SIEM 集成安全能力的期望

随着“Smart SIEM”理念的发展，企业对 SIEM 的期望不仅仅局限于传统 SIEM 提供的安全事信息和事件管理能力。新一代 SIEM 解决方案更加趋向于融合多项安全能力，将安全需求打通，并基于用户的选择进行按需扩展，从而帮助企业更加高效统一地完成安全运营工作。

针对企业对 SIEM 集成安全能力的期望，报告进行了定向调研，调研结果显示：威胁情报、端点安全（EDR）、漏洞管理、SOAR、UEBA、NTA 是大部分企业期望集成至 SIEM 平台的安全能力。

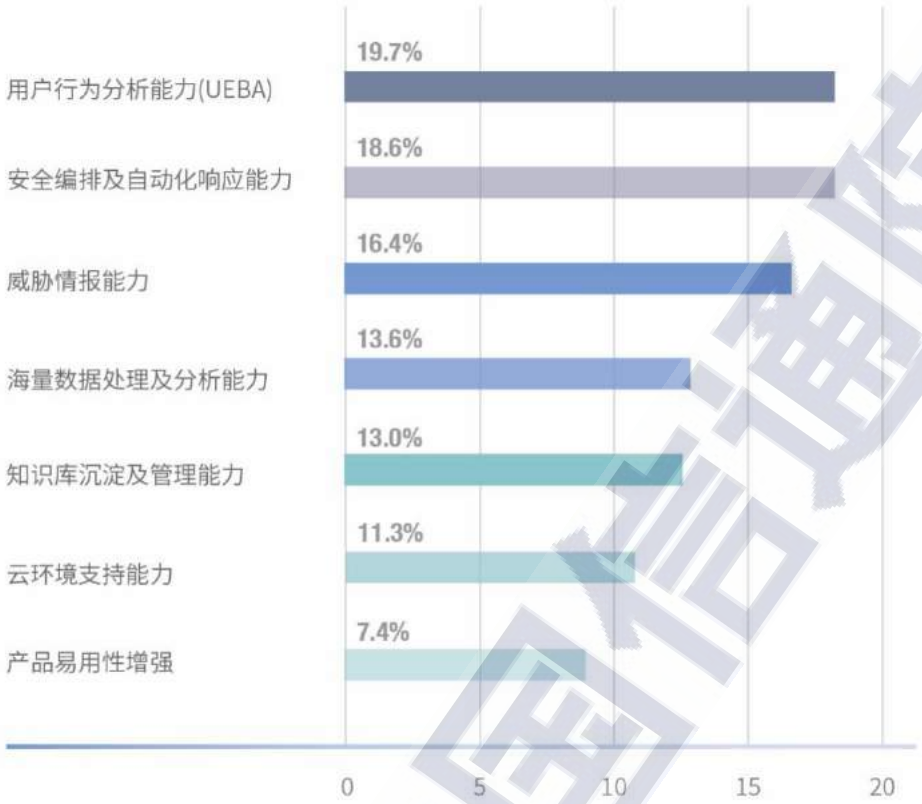


数据来源：FreeBuf.com

图 14 企业对 SIEM 集成安全能力的期望

4. 企业对 SIEM 产品期望改进的能力

根据调研结果，54.7%的企业认为 SIEM 产品需要提升【威胁情报能力】、【用户行为分析能力（UEBA）】、【安全编排及自动化响应能力】这三项能力。



数据来源：FreeBuf.com

图 15 企业期盼改进的能力

四、SIEM/SOC 类产品测试情况综述

（一）测试基本情况

本次SIEM/SOC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 2020 年 11 月 2 日，结束于 2020 年 12 月 8 日。各参测企业根据测试方案分别组合自身的产品模块和技术能力，完成了 SIEM/SOC 能力验证评估。

各参测企业受测的产品数量不同，如表 3 所示，每个参测企业产品数量从一台至五台数量不等，但普遍为两台至三台，通常一台设备作为采集探针，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，例如态势感知模块、威胁感知模块、运维审计类探针模块以及总体分析和展示模块几个部分。参与测试的产品均采用了标准 1U 或 2U 服务器。

表 3 各企业到场测试产品台数

企业名称	台数
任子行网络技术股份有限公司	5
北京盛华安信息技术有限公司	3
网神信息技术（北京）股份有限公司	3
北京安达亚科技有限公司	3
杭州安恒信息技术股份有限公司	2
上海观安信息技术股份有限公司	2
新华三信息安全技术有限公司	2
深信服科技股份有限公司	2

腾讯云计算（北京）有限责任公司	2
厦门服云信息科技有限公司	2
中电福富信息科技有限公司	2
北京神州绿盟科技有限公司	2
亚信科技（成都）有限公司	2
北京神州泰岳软件股份有限公司	1

数据来源：中国信息通信研究院

（二）测试环境介绍

资料来源：中国信息通信研究院

图 16 测试网络拓扑图

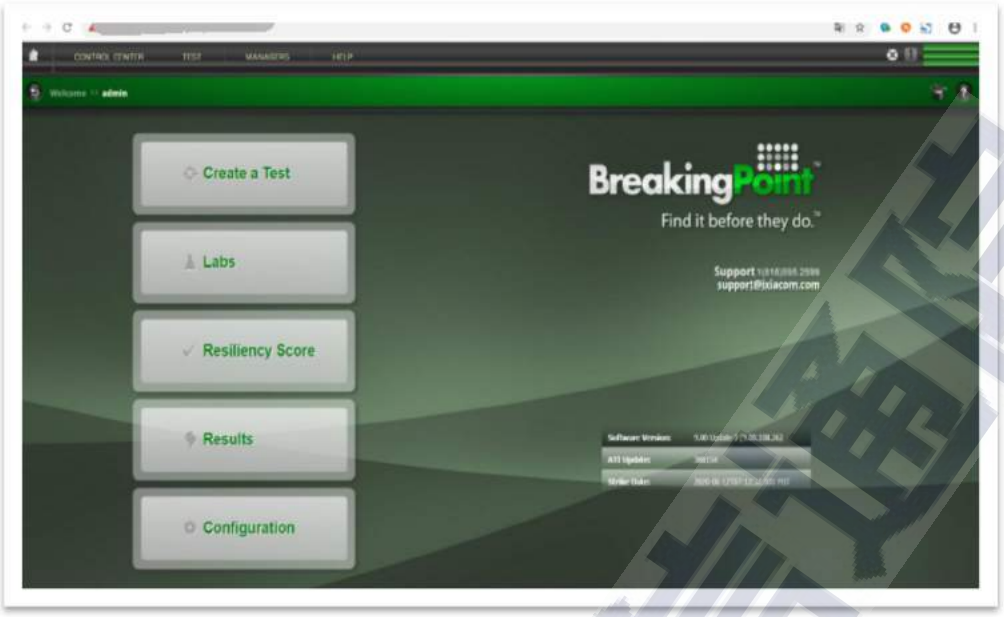
本次测试主要采用 IXIA PerfectStormONE 流量发生器（IP 地址：172.16.5.111）模拟网络流量、攻击以及恶意程序等，采用 IXIA Vision E40 分流设备（IP 地址：172.16.5.112）进行多路模拟流量生成。如图 16 所示测试环境网络拓扑情况，流量发生器与分流设备相连接，并配置流量策略，分流设备将模拟的测试流量同时下发多

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。为了保障整个测试过程的真实性与客观性，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是通过现场测试得到的结果截图。

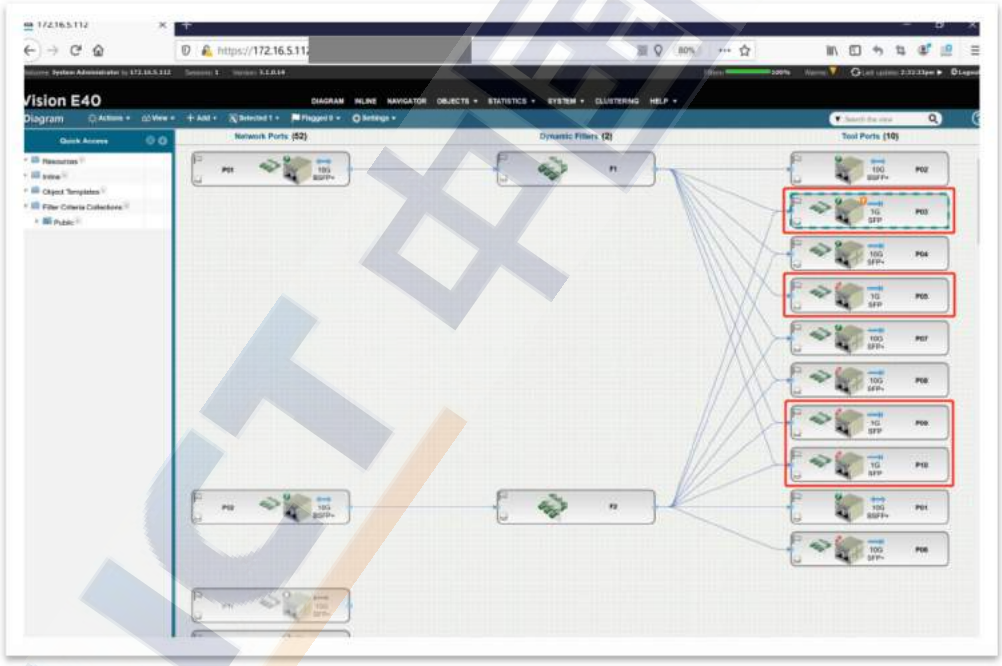
（三）测试方法说明

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 流量发生器生成最大混合流量，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，结合手工验证对设备系统和应用层面进行全面渗透测试。



资料来源：中国信息通信研究院

图 17 IXIA PerfectStorm ONE 流量发生器 Web 界面



资料来源：中国信息通信研究院

图 18 IXIA Vision E40 分流设备

（四）测试对象范围

一般情况下，SIEM/SOC 类产品从基础架构上主要分为采集层、

分析层、展现层。采集层通过对网络内的流量、日志进行基础性收集并进行标准化处理；分析层是一个 SIEM/SOC 类产品的核心技术体现，它通过多系统之间的关联、多数据/情报标准化之后的分析，进而形成威胁预警信息、态势感知信息、数据治理手段等。

本次测试对象范围主要包含安全信息和事件管理系统（SIEM）、SOC 安全运营中心、NGSOC 态势感知与安全运营平台、SRC 安全应急响应中心等产品形态和类别。其中包含的功能模块包含但不限于日志管理、威胁情报、漏洞扫描、态势感知、威胁预警、安全治理等子系统。

（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 等威胁识别，到安全分析和态势感知，到安全运营和安全治理，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 4 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 4 SIEM/SOC 类产品测试项目表

测试大项	测试小项
日志采集识别与告警能力	日志的采集和标准化
威胁情报的采集与安全分析能力	威胁情报采集和管理能力
	攻击识别能力
	关联分析能力
	日志存储与检索能力
	实时监控能力
态势感知能力	攻击态势感知能力
	威胁态势感知能力
	资产态势感知能力
	运行态势感知能力
	风险态势感知能力
	ATT&CK 攻击链溯源能力
	用户实体画像分析能力
	UEBA 分析能力
	威胁追踪能力
	网站态势感知能力
	全网态势感知能力
安全运营与应急响应能力	安全预警能力

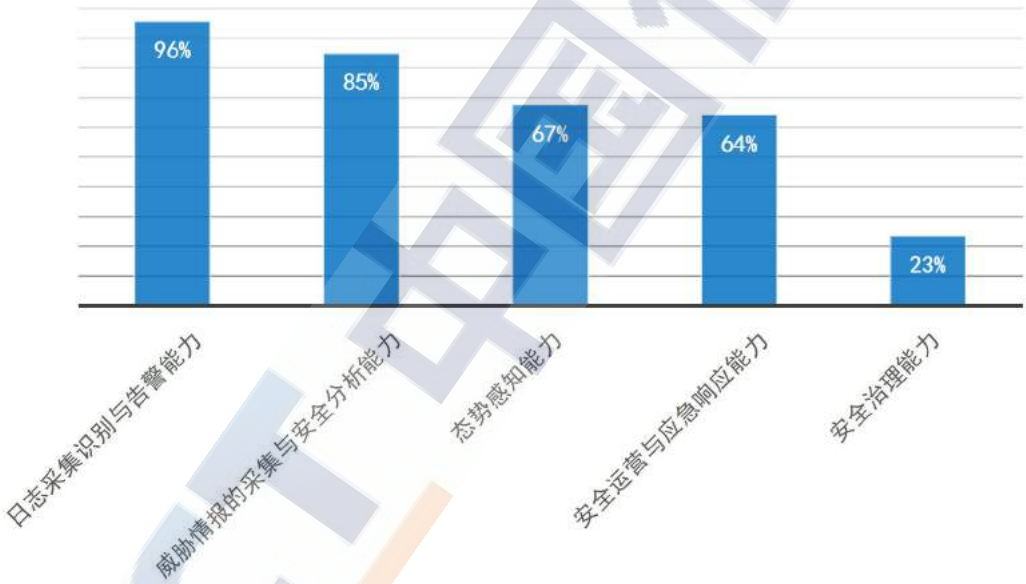
	安全告警能力
	联动处置能力
	工单管理功能
	安全编排和全过程自动化能力
	报表生成功能
安全治理能力	等级保护 2.0 合规验证能力
	安全治理分析能力
自身安全	网络访问控制
	Web 应用&逻辑业务
平台性能	最大实时吞吐
	CPU、内存使用率监测

数据来源：中国信息通信研究院

五、SIEM/SOC 类产品测试结果总体分析

（一）日志采集告警与基础分析支持较好

通过测试结果发现，**绝大部分受测产品的日志采集与告警、威胁情报采集与安全分析能力均表现良好。**如图 20 所示，全部受测产品的两个大项指标的符合率高达近 90%，侧面表明国内大部分 SIEM/SOC 类产品在日志与事件的收集、标准化和实时监控告警方面的技术能力已经相当成熟。

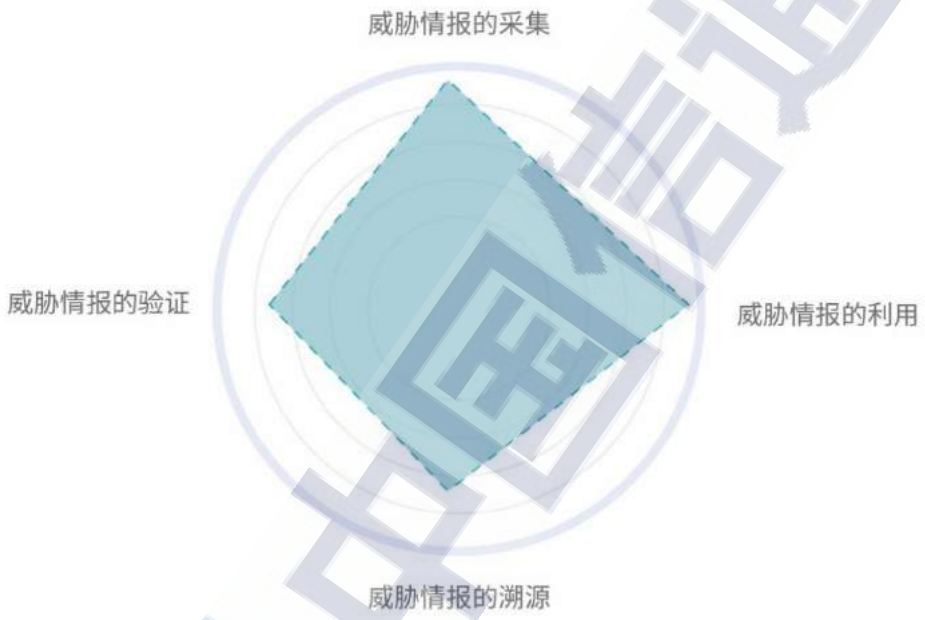


数据来源：中国信息通信研究院

图 19 受测产品主要功能满足率

一方面，本次测试中主要验证受测产品对于收集各信息系统及网络的流量、日志、运行状态、告警信息，包括 Syslog、SNMP、SNMP Trap、SSH、TELNET 和文件系统等方式接入日志类型数据；另一方面，本次测试对于威胁情报的采集、利用、溯源和验证方面进行了相关

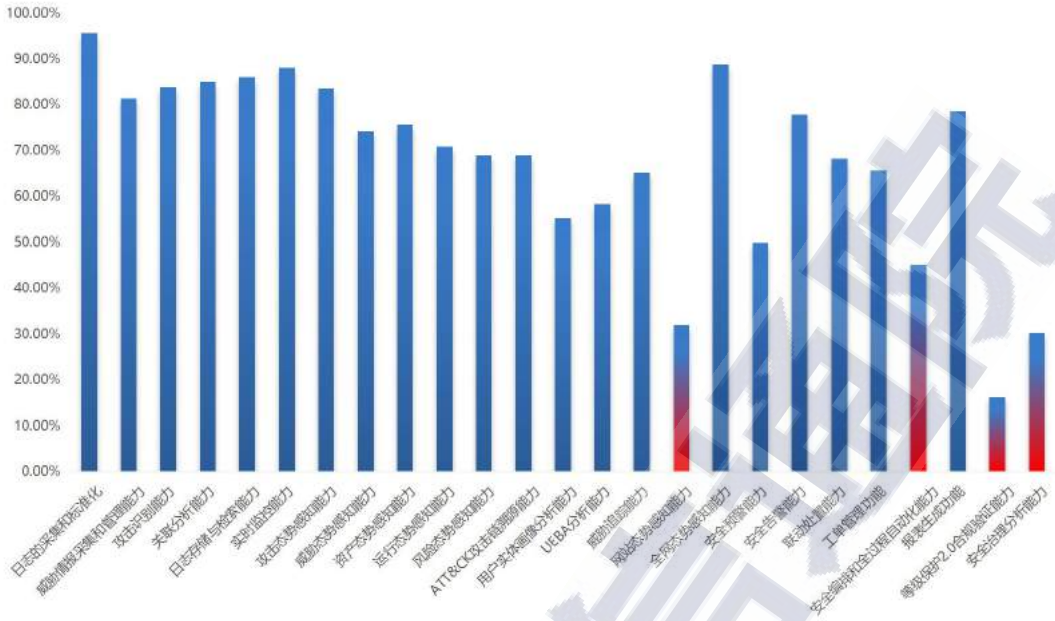
的测试，根据测试结果综合情况来看，受测产品普遍在威胁情报的采集和利用方面表现优异，但威胁情报的溯源和验证功能仍具有一定的优化空间。



数据来源：中国信息通信研究院

图 20 威胁情报能力

如图 22 所示，相对于受测产品的基础能力外，多数产品也普遍存在一定的功能短板，主要在自动编排能力和安全治理能力等方面。



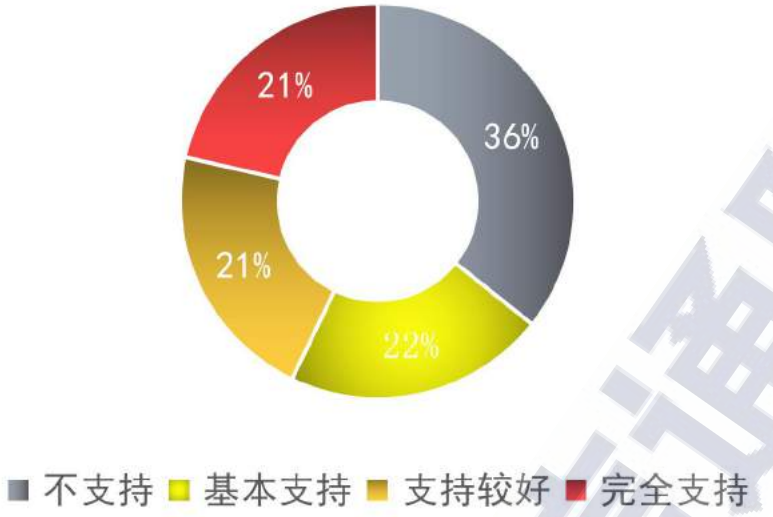
数据来源：中国信息通信研究院

图 21 受测产品主要能力占比

（二）自动化编排能力有待深化

现在的安全运营场景中，往往需要整合大量的系统信息和事件，运维工作的复杂度大大增加，因此必然需要产品提供丰富的事件响应与处理编排能力，能够基于一系列预定义的预处理策略、关联分析策略和合并策略自动化对告警严重性和处置优先级进行划分、自动化地执行匹配的剧本和应用动作，同时应能够对外提供 API 调用接口，供外部第三方应用系统调用，为它们提供编排、自动化与响应服务。

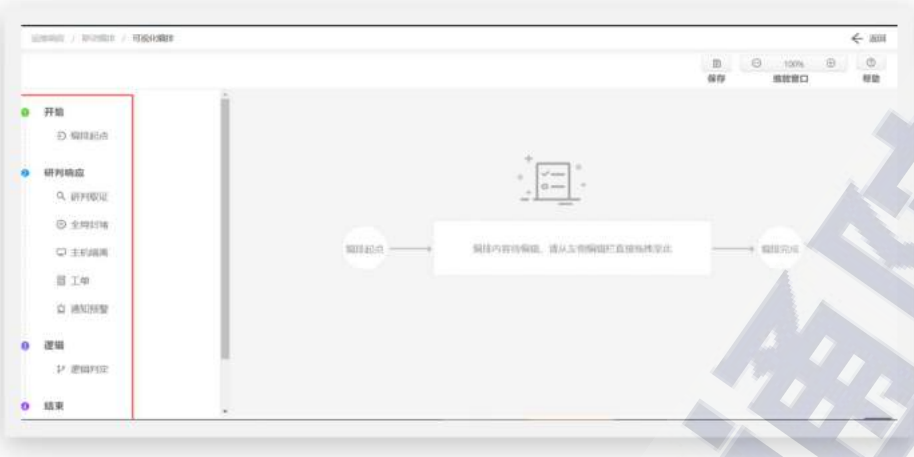
通过测试结果发现，**大多数产品具备基本的告警功能，但自动化编排响应能力有待完善。**在所有受测产品中，仅有三家完全支持自动化编排相应（SOAR），此项功能支持较好及以上的仅占全部受测产品的 42%，完全不支持此项功能的占全部受测产品的 36%。



数据来源：中国信息通信研究院

图 22 受测产品 SOAR 能力占比

根据测试用例要求，受测产品应具备自动化告警分诊、自动化安全响应、自动化剧本执行、自动化案件处置以及自动化服务调用等功能。不仅应实现实时有效告警，并且告警信息在系统中有详细记录。具备供第三方应用调用的接口的配置，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。就本次测试情况综合评估，**在安全编排自动化与响应能力方面，多数受测产品未体现出相关能力优势**，需要在实践中不断完善和改进。



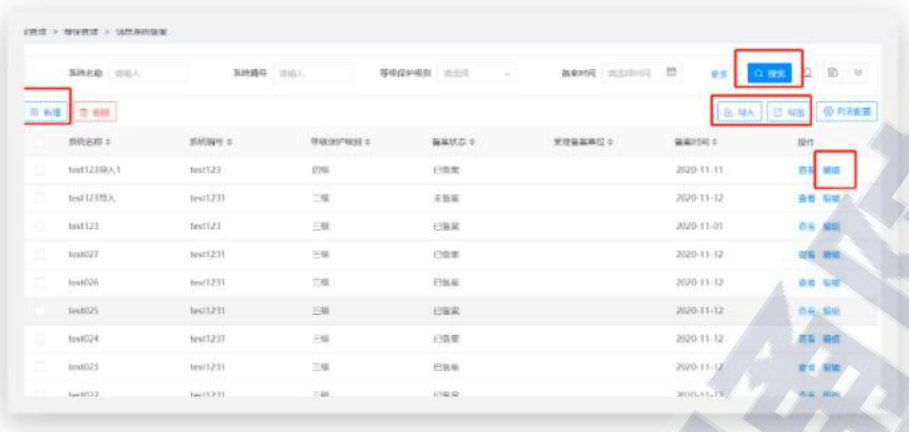
数据来源：中国信息通信研究院

图 23 SOAR 功能界面示意图

（三）安全合规审计能力亟需加强

本次测试在安全治理功能的测试方面，基于当前网络安全市场的运营趋势提出了两点测试项：等级保护 2.0 合规审计以及安全治理数据。

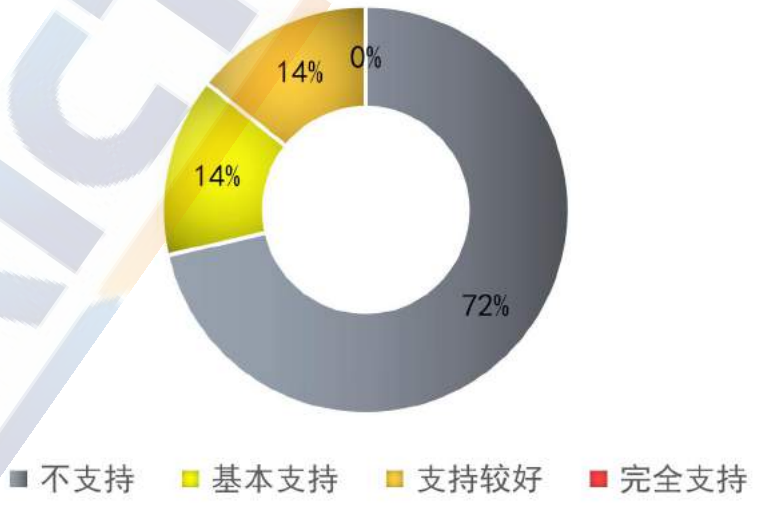
等级保护 2.0 合规审计。网络安全等级保护 2.0 制度，是我国网络空间安全领域的基本国策和基本制度。在等级保护 1.0 时代的基础上，更加注重主动防御，建立全流程的安全可信、动态感知和全面审计。SIEM/SOC 类产品作为企业安全运营的核心，承载着收集、分析和情报处理的关键功能，如果能通过等级保护 2.0 进行赋能与合规管理，将大大提高 SIEM/SOC 类产品应用的深度和广度。



数据来源：中国信息通信研究院

图 24 等级保护 2.0 审计功能示意图

根据测试结果，有 10 款产品完全不支持等级保护 2.0 的合规审计功能，占全部受测产品的 72%。没有一款受测产品能够完全支持本次的测试用例。但值得期待的是，其中 1 款产品在后续版本将加入等保审计功能，而另外部分产品可通过接入本次测试外的定制模块、探针等方式进行等保合规审计和安全信息事件地集中管理。从总体上看，**本次受测产品在等级保护 2.0 合规审计功能上亟需加强**。



数据来源：中国信息通信研究院

图 25 等级保护 2.0 审计功能占比

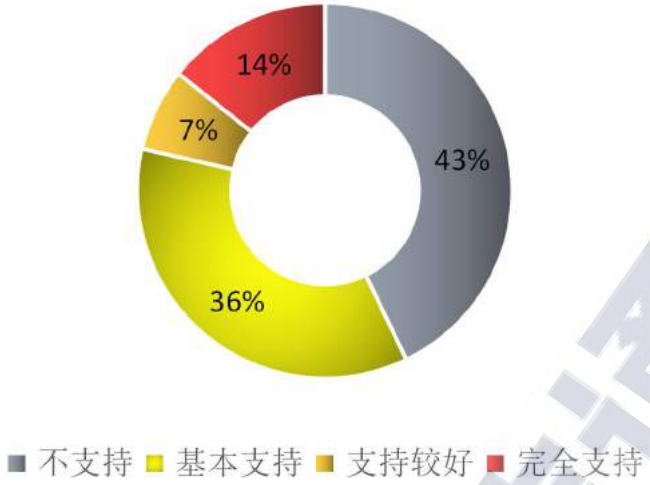
安全治理数据。本次测试中，增加了安全治理数据的功能检测，旨在展示安全治理整体数据、态势和成效。通过受测产品内置安全风险 KPI 指标，包括安全状况指标、运行能力指标、安全态势指标以及合规指标。查看总体安全治理情况。

通过测试结果发现，**虽距安全治理的要求还有一定距离，但多数产品已经基本具备功能**。大部分受测产品在功能上基本能够实现查看全网安全威胁指数、查看安全域 KPI 的态势、不同安全域的指标变化以及设置 KPI 的标准等。

数据来源：中国信息通信研究院

图 26 安全治理数据功能示意图

如图 28 所示，具有基本支持及以上测试结果的受测产品占比 64%，其中完全支持测试的受测产品有三款。

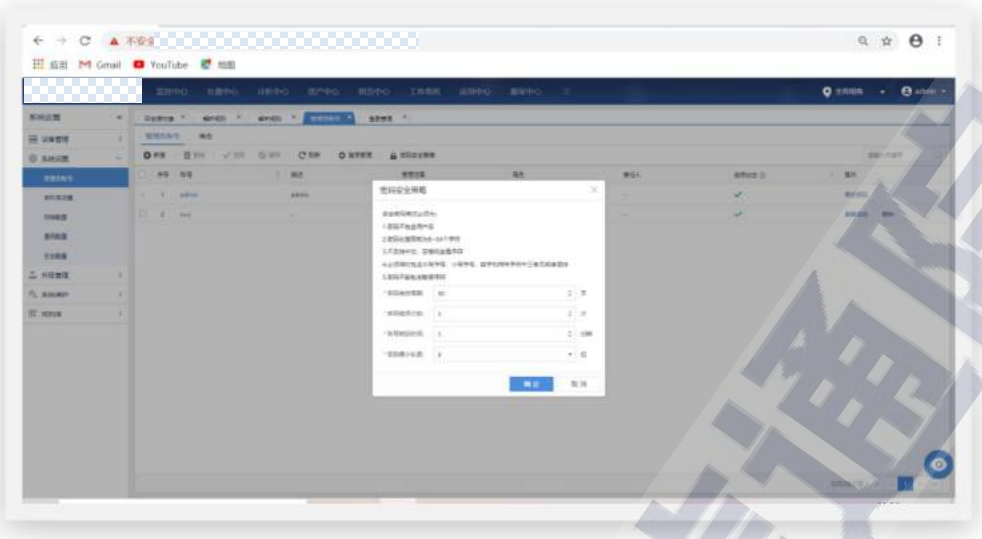


数据来源：中国信息通信研究院

图 27 安全治理数据功能

（四）系统自身安全管理功能完善

通过测试结果发现，几乎全部受测产品**在自身安全配置方面，均具备包括不限于用户标识、数据安全、身份鉴别、安全审计等安全配置功能。用户标识方面**，具备管理角色标识、鉴别信息、隶属组、权限等自定义用户安全属性，并具备用户属性初始化功能和用户唯一性设置。**数据安全方面**，具备数据安全管控机制，涵盖数据的创建、存储、使用、共享、归档、销毁数据全生命周期环节，涉及通过网络协议、接口、维护终端等多种途径进行数据访问、传输，保证在这些途径上的数据保密性、安全性和完整性。**身份鉴别方面**，具备提供授权管理员鉴别数据的初始化、鉴别失败处理、鉴别授权保护等功能。**安全审计方面**，具备对不同的安全行为进行审计记录的生成，并能够限制审计记录的访问。



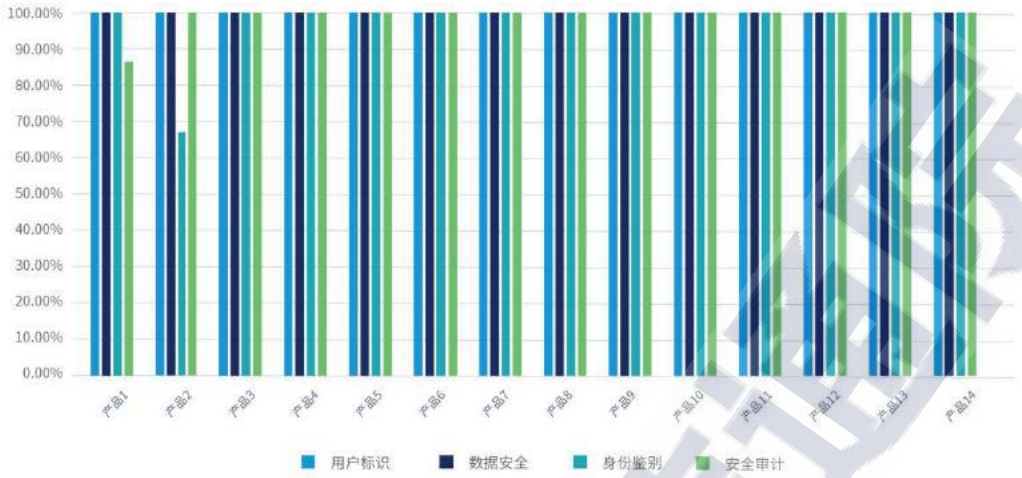
数据来源：中国信息通信研究院

图 28 自身安全管理配置功能示意图

数据来源：中国信息通信研究院

图 29 自身安全管理配置功能示意图

如图 31 所示，**绝大部分产品具有完善的自身安全管理能力。**其中 86%受测产品具备完善的自身管理能力，满足测试功能要求，14%受测产品在本次测试用例中存在微弱的差距。

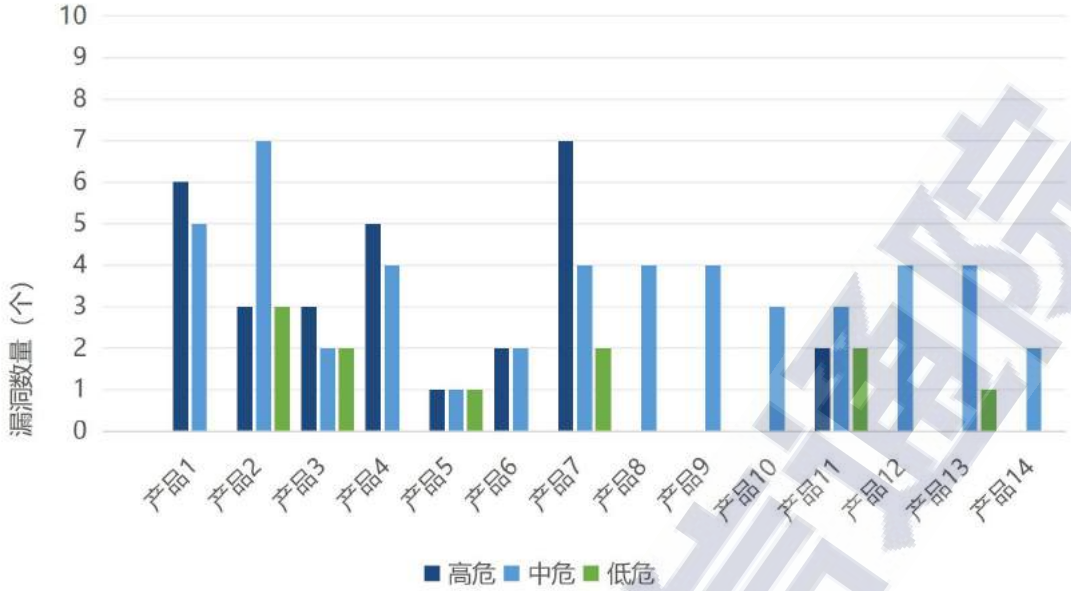


数据来源：中国信息通信研究院

图 30 产品自身安全管理功能结果比例图

（五）Web 和业务安全漏洞均有存在

通过测试结果发现，**全部受测产品均存在应用安全漏洞**。本次测试过程中，通过系统漏洞测试、应用安全测试、口令破解、数据包分析等不同工具和方法，对受测产品的 Web 应用和业务安全进行了测试，测试内容包括不限于对 Web 应用进行安全扫描监控，查看 Web 应用是否存在安全漏洞、利用业界知名安全扫描工具/开源扫描工具扫描和人工渗透测试尝试发现 Web 应用是否存在的安全风险、对系统业务逻辑进行分析和测试，查看业务逻辑是否存在漏洞（越权、数据泄漏等）。在本次全部受测产品中，均存在 Web 和业务安全漏洞。所有产品的高危漏洞占总漏洞数的 33%，中危漏洞占 55%，低危漏洞占 12%。其中，有 8 款产品均存在不同危害程度的高危漏洞。如图 32 所示各产品漏洞数量。



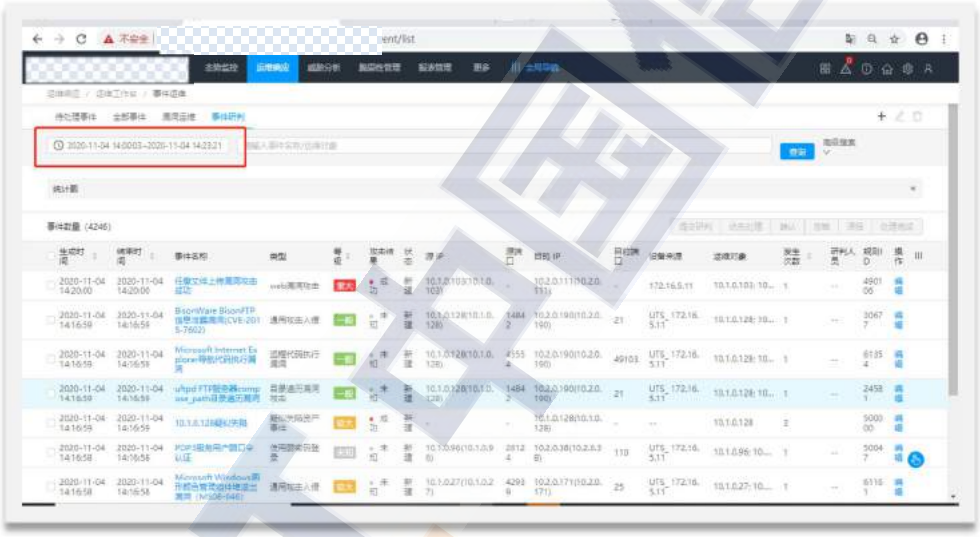
数据来源：中国信息通信研究院

图 31 受测产品应用安全漏洞情况

六、SIEM/SOC 类产品威胁识别能力分析

（一）各类网络攻击发现和分析的能力

在本测试中，利用流量发生器构造了近 5000 条漏洞利用攻击，包括但不限于远程代码执行、破壳漏洞利用、SQL 注入、HTTP PUT 方法任意写文件、暴力破解、端口扫描、非法权限获取、挖矿、木马后门通信、中间件漏洞等，用于验证受测产品的网络攻击识别和分析能力。

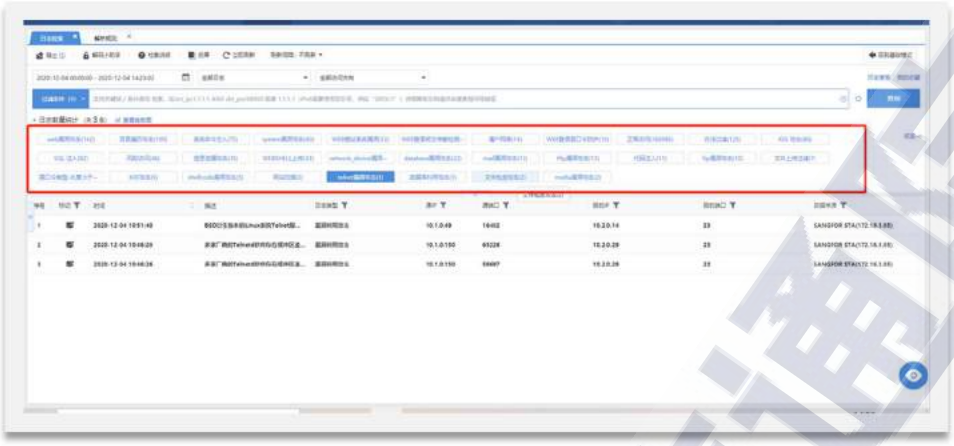


数据来源：中国信息通信研究院

图 32 网络攻击识别能力示意图 1

通过测试结果发现，**绝大部分受测产品可实现对网络攻击的基本识别，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。

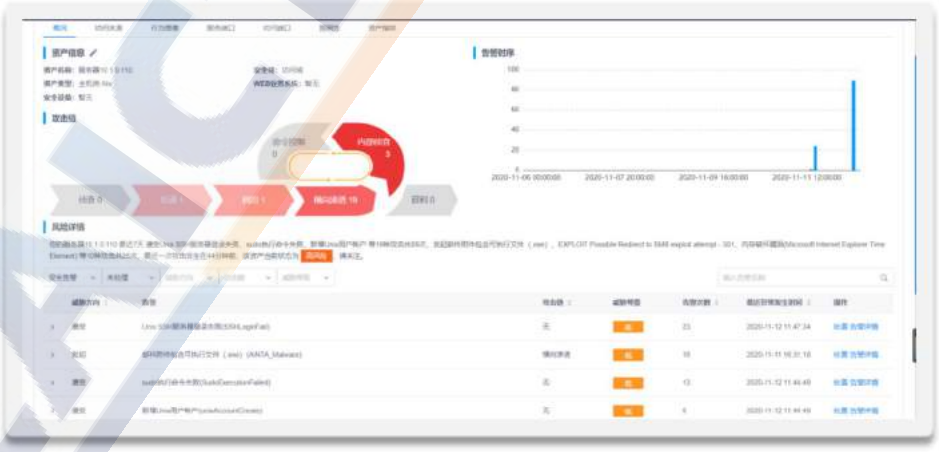


数据来源：中国信息通信研究院

图 33 网络攻击识别能力示意图 2

（二）多步骤攻击发现和关联分析的能力

通过测试结果发现，**绝大部分产品可以实现分析流量中的多步骤攻击链条**，包括基于攻击链模型的分析、攻击源追溯等功能。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。

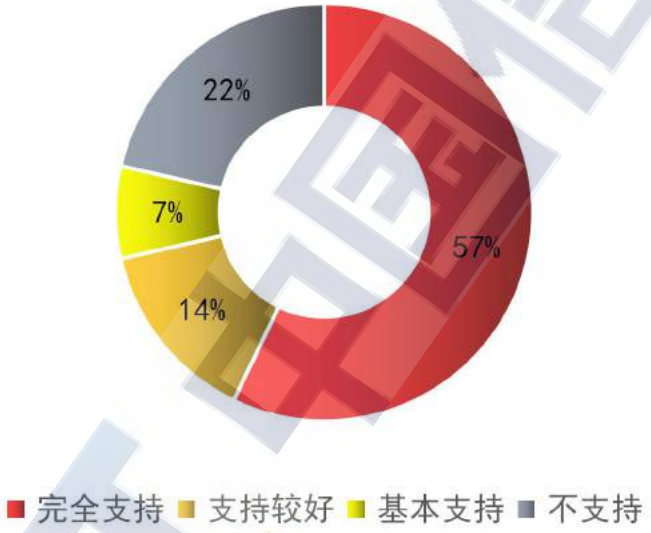


数据来源：中国信息通信研究院

图 34 攻击链识别功能示意图

ATT&CK[7]技术落地仍需完善。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，查看受测产品是否具备提供攻击链模型的安全事件监测的方法，是否能够直观呈现攻击者的抽象行为并提供攻击路径追溯等功能。

如图 36 所示，虽然绝大部门受测产品都可以识别出多步攻击链条，但是其中仍有 3 款产品不支持通过以 ATT&CK 为例的全过程告警功能，占全部测试产品的 22%。



数据来源：中国信息通信研究院

图 35 受测产品 ATT&CK 测试结果

[7] 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。

七、SIEM/SOC 类产品态势感知能力分析

态势感知能力，不仅是SIEM/SOC类产品对于数据分析的展示层，更代表一个系统对于网络中的资产、用户以及环境等各方面信息的深度理解和分析，从而形成全局视角，以用于决策支撑、应急响应和安全处置等。本次测试过程中分别对 SIEM/SOC 类产品的攻击和威胁态势感知能力、资产和运行态势感知能力、用户实体和 UEBA 能力等方面进行逐一测试，用来分析受测产品在态势感知方面的功能支持情况。

（一）攻击和威胁态势感知能力分析

根据测试结果，**大部分受测产品均具备一定的攻击和威胁态势分析能力**。其中，**攻击态势感知能力**主要能够实现显示攻击源国家 TOP n、显示不同时间段的攻击事件量、显示情报命中数、显示当前攻击状态值、显示当前攻击趋势值等内容。**威胁态势感知能力**能够实现潜伏威胁感知、外部威胁感知、威胁情报态势感知等方面的内容。

数据来源：中国信息通信研究院

图 36 攻击和威胁态势感知功能示意图

如图 39 所示，本次受测产品中，有 4 款产品在攻击和威胁态势感知的功能上完全满足测试要求，占全部受测产品的 29%；有 1 款产品完全支持攻击态势感知能力但威胁感知能力还需加强。其他产品均为基本支持或者较好的支持本次的测试用例，测试中未发现不支持此功能的产品。

数据来源：中国信息通信研究院

图 37 攻击和威胁态势感知测试结果

（二）资产和运行态势感知能力分析

根据测试结果，大部分受测产品均具备一定的资产和运行态势分析能力。其中，资产态势感知能力主要能够展示资产安全概览、展示业务系统和安全域 TOP n、资产价值分布、资产发现示意图、展示互联网资产暴露、展示操作系统版本、展示资产端口类型、展示资产来源、正常展示网段分布、展示资产分类统计信息和资产发现的来源等。运行态势感知能力主要能够显示全网安全状况及风险分布地图、安全域风险等级 TOP n、不同时间维度脆弱性、威胁和风险 TOP n、安全域价值等级分布、攻击关系图、威胁分布状况等等。

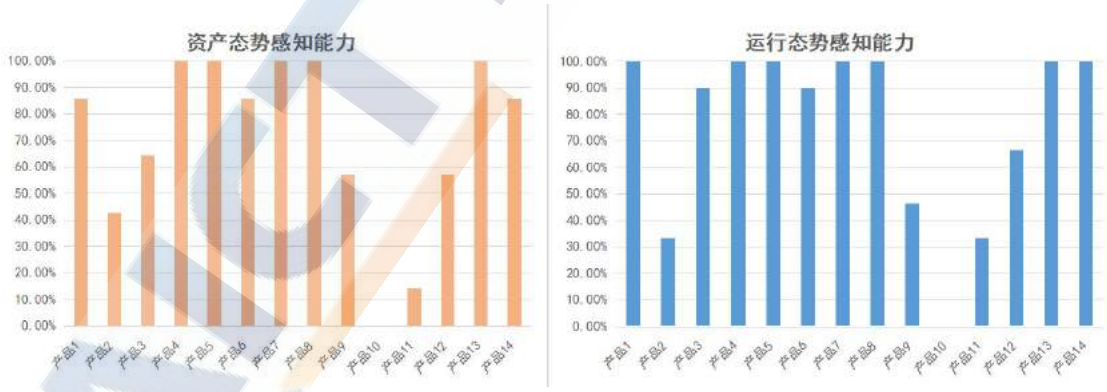
数据来源：中国信息通信研究院

图 38 资产态势感知功能示意图

数据来源：中国信息通信研究院

图 39 运行态势感知功能示意图

根据测试结果，本次受测产品中，有 6 款产品在攻击和威胁态势感知的功能上完全满足测试要求，占全部受测产品的 43%；有 2 款产品完全支持其中一项态势感知功能。仅有 1 款产品不支持此项态势感知功能。其他产品均为基本支持或者较好的支持本次的测试用例。



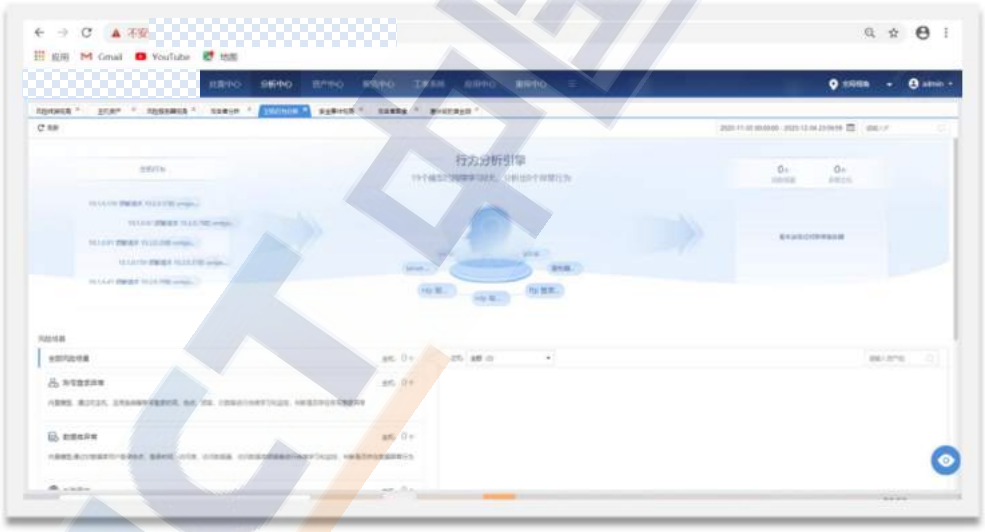
数据来源：中国信息通信研究院

图 40 资产和运行态势感知测试结果

（三）用户实体画像和 UEBA 能力分析

UEBA 是 SIEM/SOC 的关键功能，Gartner 曾预测，到 2020 年，

80%的 SIEM 产品都将具备 UEBA 功能。根据本次测试结果，**大部分受测产品均具备用户实体画像分析能力和 UEBA 分析能力，但在机器学习和深度分析上仍存在很大空间**。其中，用户实体画像分析能力主要能够添加设备的详细画像、能够在场景画像查看由于 UEBA 场景所触发的实体画像、能够在猎物画像看到威胁狩猎所触发的实体画像等。UEBA 分析能力主要是围绕用户和资产提供细粒度的行为分析场景，找出潜在的内部威胁与安全风险，并且可以查看异常行为场景的详细信息，进行深度分析操作，例如生成画像，进行威胁狩猎，产生告警，误报忽略等操作，同时对场景进行配置管理，包括场景的开启和关闭以及特征配置的调整。

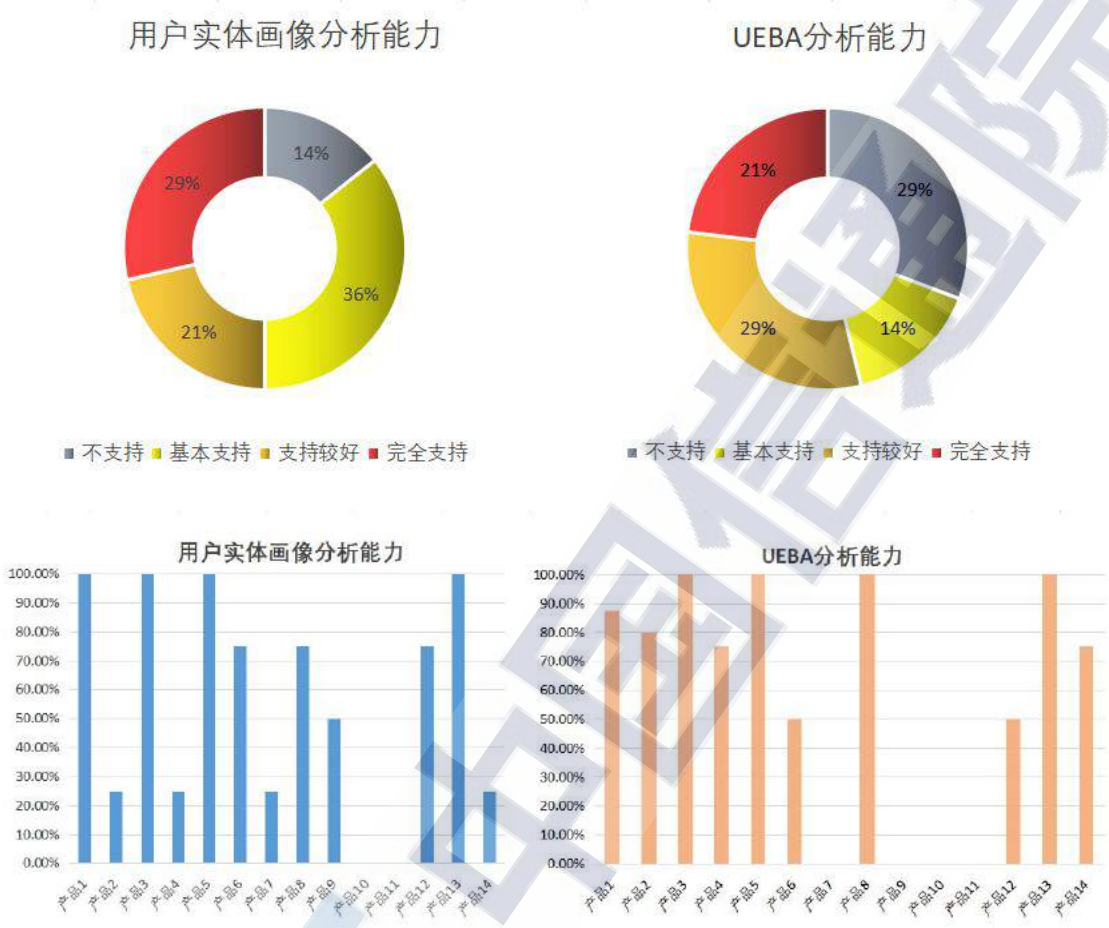


数据来源：中国信息通信研究院

图 41 UEBA 分析功能示意图

根据测试结果，本次受测产品中，有 3 款产品在用户实体画像分析功能和 UEBA 分析功能上完全满足测试要求，占全部受测产品的 21%；有 3 款产品完全支持其中一项功能。有 2 款产品不支持此项功

能。支持较好及以上的受测产品在用户实体画像分析功能和 UEBA 分析功能占比分别为 58%和 72%。



数据来源：中国信息通信研究院

图 42 用户实体和 UEBA 分析能力测试结果

八、SIEM/SOC 类产品趋势展望

根据 Gartner 的定义，安全信息和事件管理（SIEM）技术通过对来自各种事件和上下文数据源的安全事件的实时收集和历史分析来支持威胁检测和安全事件响应。在安全运营的发展历程中，SIEM 作为一种非常有效的技术解决方案，一直以来都是安全运营的关键输入，尤其是在安全响应（Response）版块发挥关键作用。而随着

安全数据、应用、场景量的激增，SIEM 的技术能力也在不断优化。

资料来源：FreeBuf.com

图 43 SIEM 技术快速发展

回顾 SIEM/SOC 发展演变的历程，我们可以看到其发展与安全运营的变化相契合，并不断优化以满足安全运营的需求。

（一）“智能 SIEM”将引领新一代 SIEM 能力发展

新一代 SIEM 从解决传统 SIEM 的告警爆炸、企业网络安全专业技能人才的匮乏等问题出发，能力集中在日志和事件融合分析、人工智能技术集成、关联分析、用户行为分析、安全编排自动化与响应、威胁狩猎等方面。我们将新一代 SIEM 定义为“智能 SIEM（Smart SIEM）”。

资料来源：FreeBuf.com

图 44 新一代 SIEM 的能力范畴

对比传统 SIEM 产品的技术能力，Smart SIEM 的能力发展趋势更多集中在**智能化、主动化、集成化**。

1. 智能化：AI+自动化驱动

随着事件数量的增加，使用旧 SIEM 解决方案的企业能够拥有大量的日志和事件数据，但无法智能地了解数据背后的原因。企业需要更智能的 SIEM，通过机器学习技术或自动化手段消除一些普通重复的任务，以确保有限的企业资源不会因警报疲劳而陷入困境。在此过程中，Smart SIEM 更强调应用用户行为分析（UEBA）和安全编排自动化和响应（SOAR）等能力。

基于机器学习的 UEBA 技术。用户和实体行为分析（UEBA）这项技术通常利用数百种机器学习模型来分析大量事件，并为每个实体

（用户/机器/打印机/IP 地址等）识别“正常”行为。对于每个实体，通过将其基线与新行为及其对等实体的基线进行比较，并将数百条线索之间的点连接起来，以评估是否产生风险分数异常行为预示着真正的安全风险。这样，数十亿个数据点就变成了少数优先的威胁线索，从而减少了警报，并使安全运营人员可以专注于调查对企业构成真正风险的威胁。UEBA 的机器学习类型通常分为两类：监督机器学习和无监督机器学习。

资料来源：FreeBuf.com

图 45 两种机器学习类型

监督机器学习依赖于大型标签数据集来训练模型，它非常适合识别具有已知攻击模式或危害指标（IOC）的已知网络安全威胁。例如，恶意软件检测是此类机器学习的用例之一，因为该行业具备数十年的恶意软件数据，可以提供用作训练模型的数据依据。

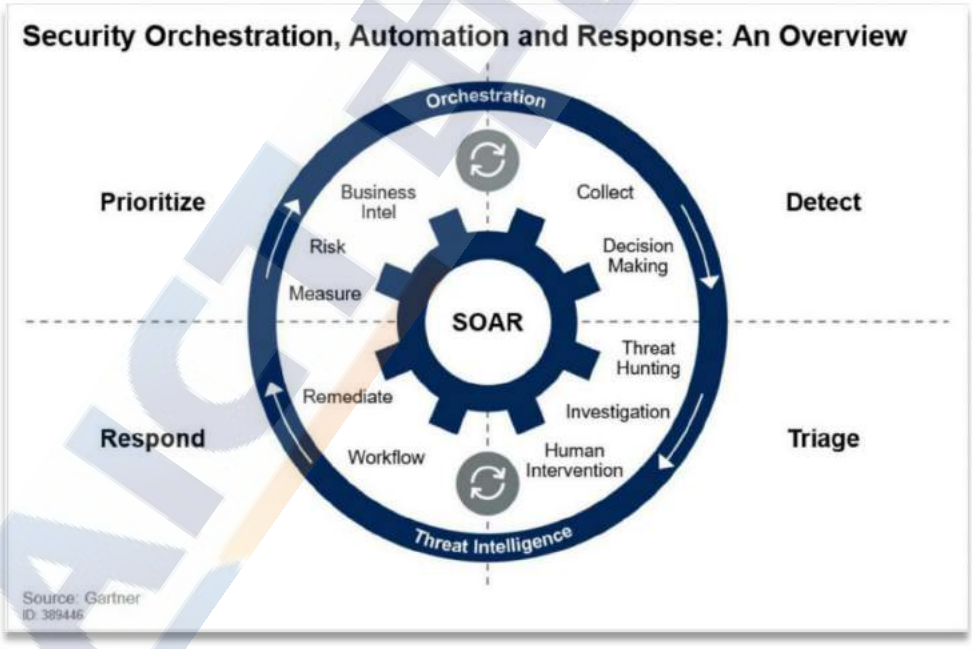
无监督机器学习通过查找数据集中的模式进行学习，因此非常

适合异常检测，在异常检测中它可以自动比较并查明异常行为，适应企业的数据并发现新的模式，无须人工指导机器寻找。

将 UEBA 与 SIEM 有效结合使用，可以提供一种分层的安全分析方法，快速、有效地找到已知威胁， 并帮助运营人员提高检测与响应效率。

安全编排自动化和响应（SOAR）技术

SOAR 的概念最早由 Gartner 在 2015 年提出，SOAR 的三大核心技术能力分别安全编排与自动化 （SOA，Security Orchestration and Automation）、安全事件响应平台 （SIRP，Security Incident Response Platform） 和威胁情报平台 （TIP，Threat Intelligence Platform）。



资料来源：Gartner

图 46 Gartner 对 SOAR 技术能力的定义

SOAR 可以根据事先的预案（Playbook）进行编排和自动化，能

够有效地简化安全运营人员的手工作业，减少了单调繁重的威胁分析过程。**一是** SOAR 帮助安全分析人员更快地响应和调查攻击，使他们能够更快地开始缓解。自动化功能使他们能够采取措施将攻击风险降到最低,而无须人工干预。**二是**SOAR 自动化技术与机器学习(ML)和人工智能（AI）相结合，它们提供了更快的方法来识别新的攻击，并使预测分析能够得出统计推断，从而以更少的资源缓解威胁。**三是**利用 SOAR 的编排和自动化技术，安全运营人员可以在多个安全工具之间快速进行协调、从多个来源快速获取威胁源，并使工作流自动化以主动扫描整个环境中的潜在漏洞。**四是**安全运营人员通常需要花费大量时间来管理案例，创建报告并记录事件响应程序。SOAR 通过自动化操作手册、创建知识库沉淀，帮助企业保留安全运营经验并持续迭代学习。

将 SIEM 和 SOAR 结合后，能够大大缩短 MTTD（平均检测时间）和 MTTR（平均修复时间），解决安全运营人员短缺的问题，并降低 SIEM/SOC 中常见的告警爆炸问题，并通过自动化实现运营成本有效降低。

2. 主动化：威胁感知与主动防御

企业需要寻找通过预测和预期对手的下一步行动来具备主动竞争的能力，在此过程中，新一代 SIEM/SOC 需要具备威胁感知和主动防御的能力。将 SIEM/SOC 与威胁情报匹配，企业能够以敏捷和快速反应的方式应对不断发展的、大批量、高优先级的威胁。

通过威胁情报平台，企业可以汇总和合理化威胁数据，自动筛选出攻陷指标（IOC）作为可机读威胁情报（MRTI），并且使用现存的日志对比匹配以便轻松发现不常见的趋势或线索，并对其有效执行操作。通过将团队、流程和工具结合在一起，威胁情报平台指导安全响应并进行阻断，节省了追踪传统 SIEM/SOC 产生误报所花的大量时间。

资料来源：FreeBuf.com

图 47 威胁情报平台与 SIEM 等安全产品联动示例

如果将 SIEM/SOC 与威胁情报平台相结合，企业可以将所有人、过程和技术统一在智能驱动的防御背后，获得强大的安全运营增益效果。**一是日志、事件和数据的进一步分析。**将来自威胁情报平台的攻陷指标将自动发送到 SIEM/SOC 中进行警报，并将来自 SIEM/SOC 的特定事件发送回威胁情报平台来进行关联分析、数据挖掘和优先性排序，分析人员可以锁定恶意行为的所在位置。**二是建立企业自身威胁知识库。**综合性威胁情报平台可以作为企业的中央威胁信息

库。帮助企业了解网络犯罪分子的工具、流程、受害者和预期目标。**三是根据企业网络环境生成和优化情报。**威胁情报平台增加了上下文信息和关系丰富的指标，从而使企业能够更好地了解威胁的性质、对企业风险更有效地做出全面的反应。**四是主动防御。**威胁情报平台支持安全响应团队寻找线索和联系，这可以显示攻击企业的威胁与可能存在的威胁之间的关系，并发现新的相关的情报。使用这些信息，帮助安全团队变被动防御转为主动防御。

3.集成化：多元安全能力高效联动

随着 SIEM/SOC 的发展，Smart SIEM 的定义中逐渐集合了多种安全能力，例如前文提到的用户和实体行为分析（UEBA）、安全编排自动化和响应（SOAR）、威胁情报等多种能力。这些能力可以是单独的产品，但是对企业而言，集成化将是更好的选择。

事实上，在原有的企业安全建设中，常常面临的问题就是不同品牌、不同功能的产品并行在企业网络中。数量众多、品牌各异、功能不同的安全产品大大提高了安全运营工作的复杂度，对安全运营人员的要求也将更高。同时，不同安全产品产生的各类数据及事件繁杂且细密，致使安全运营人员深陷于事件风暴中，无法有效寻找梳理有效信息和及时处理安全警报。

在此背景下，新一代 SIEM/SOC 的需求逐渐被引导为各类安全能力的迁移和集成。例如，用于定义剧本和流程的编排和自动化工具或充当中央存储库的威胁情报平台、可以使用上下文的外部全局威

胁情报来聚合和丰富大量内部威胁和事件数据，方便企业可以了解并确定优先级采取行动。

此外，集成化的体现还包括 SIEM/SOC 对各安全品牌产品的兼容与多元化。企业战略集团（ESG）曾做过一项调研，数据表示，62%的受访者更愿意考虑从单个企业级网络安全供应商处购买公司所需的绝大部分安全技术。

对于企业运营人员来讲，管理不同品牌的安全产品更像是多维度的角力。不同品牌产品具备相异的技术架构、操作界面，甚至操作语言也会有所区分。这就对企业安全运营投入与技术能力提出了很高的要求，因此这也是大多数企业更愿意选择单一供应商的原因。换个角度，近几年各大安全厂商纷纷推出全行业全能力覆盖级解决方案未尝不是该需求的推动因素导致。

安全运营集成化更是“All-In-One”思维地接续传递，这种集成能力将安全团队、流程和技术整合到一个安全体系结构中，最大化提高效率和有效性，消除重复性任务，使得安全运营人员可以自由地专注于更高优先级的活动，不断赋能企业安全运营能力的提升。

4.MITRE ATT&CK 框架助推安全运营能力提升

MITER ATT&CK 矩阵的出现为企业安全运营提供了强大助推力，将 SIEM/SOC 的技术工具能力与其有效结合，将是企业应对安全风险的利器之一。

MITRE ATT&CK 将已知攻击者行为转换为结构化列表，将这些已

知的行为汇总成战术和技术。该列表相当全面地呈现了攻击者在攻击网络时所采用的行为，因此对于各种进攻性和防御性度量、表示和其他机制都非常有用。

资料来源：FreeBuf.com

图 48 ATT&CK 矩阵图

MITRE ATT&CK 的目标是创建网络攻击中使用的已知对抗战术和技术的详尽列表。简单来说，ATT&CK 是 MITRE 提供的“对抗战术、技术和常识”框架，是由攻击者在攻击企业时会利用的 12 种战术和 244 种企业技术组成的精选知识库。

在网络安全事件分析中使用 ATT&CK 框架可以在不同的策略和技术之间建立联系。这有助于安全团队在完成攻击之前就识别出正在进行的攻击，并让安全团队很好地了解对手已经做了什么以及下一步可能会做什么。此外，ATT&CK 框架对于检测攻击特别有用，因为它是基于行为的模型，而不是基于签名的模型。因此 ATT&CK 可以预测常见的行为，避免被检测者破坏或基于签名的系统的其他弱点所欺骗。

总的来讲，MITRE ATT&CK 基于对网络杀伤链概念的扩展，从而将安全事件分解为阶段性的概念及应对措施，并可以与基于行为的检测方式相结合。无论是内置在企业检测和响应工具中，还是仅作为建设企业安全防护手段的标准方法论，MITER ATT&CK 矩阵都应该在企业的安全运营中占据一席之地。

对国内企业而言，安全重视程度和技术应用手段也在逐步提升。与之相对应地，忽视安全的代价也越来越高，例如客户流失、企业商誉受损、企业收入受影响等。大部分企业的安全建设取得了较大的进步，基本的网络安全防护已经不再是问题，而新的问题在于如何获悉安全事件的详细过程、如何全面掌握整网安全态势现状、如

何从纷乱繁杂的安全事件中抽丝剥茧命中高危安全行为。

SIEM/SOC 作为新一代安全信息和事件管理的技术，帮助安全运营人员从整个 IT 基础架构堆栈的各种系统中收集、关联和分析日志等数据，从而识别并报告安全威胁及可疑活动。

（二）多元安全能力组合成新趋势

SIEM/SOC 需要从海量冗杂的设备日志数据中有效梳理分析，通过融合更多有效的安全产品，形成采集、分析一体化平台，减少基础数据筛选和分析工作。在此背景下，安全运营需要智能化、主动化及高准确性的体系化建设，以达成内外部高级威胁检测和响应，而单一产品之间整合度较低、联动性较弱，无法高效处理安全事件，远无法满足用户需求，受此影响，安全运营从单一产品到组合型产品的转变趋势愈加明显。无论厂商侧还是用户端，均从产品技术导向和市场需求方面共同引导。从厂商侧来看，安全大厂纷纷布局该能力，主要采用收购单一产品能力厂商或整合新技术的方式，扩展安全运营产品生态，典型案例如综合安全厂商 360 收购 SIEM 能力厂商瀚思。从产品技术能力看，通过引入新的技术改进检测、调查、响应等功能不断优化 SIEM/SOC 的安全状态，例如 NTA/NDR 提升全网流量监控及威胁发现能力，UEBA 帮助运营人员深入了解安全威胁，SOAR 则大大提升了安全事件的补救效率，多元安全能力组合的转变越来越明显。

（三）AI&自动化驱动智能化转型

随着安全事件数量的增加，企业往往面临着大量日志和事件数据暴增却无力快速高效处理的状况。企业需要更智能的 SIEM/SOC 产品，以确保有限的企业资源不会因警报疲劳而陷入困境。

通过 AI 和机器学习技术驱动产品智能化转型成为 SIEM/SOC 的主流趋势。AI 技术可以帮助企业从海量的输入数据流信息中发掘威胁事件，并自动使用 AI 技术对不同业务、不同维度的数据进行智能关联，建立内在联系，并实现自动化威胁事件处置。目前部分新型 SIEM/SOC 已经集成了常用的 AI 算法，比如异常检测、线性预测等，这些算法以插件的方式集成进平台，企业可以选择基于算法分析自身庞杂的数据。

（四）云端部署能力持续扩展

随着云应用越来越普遍，企业必须确保包括云在内的整个 IT 基础设施的安全能力保障，云安全成为必争之地。因此，SIEM/SOC 需提供多种应用场景能力适配，除了硬件、软件等本地场景部署外，还需提供虚拟化或基于云服务的部署选项。

得益于企业对希望减少日志管理及安全事件监控成本的需求，“安全信息和事件管理即服务”模式逐渐增加。但是，有很多企业仍旧不放心把敏感日志信息发送到云端，而这也是 SaaS 服务商们需要解决的一个重要问题。

（五）需求落地向业务导向型转变

在以往 SIEM/SOC 的实际落地过程中，很多企业由于无法准确认知到真实的业务需求，往往盲目遵循“技术为先”或“架构为先”的惯性思维，便会出现产品部署后无法与业务架构密切融合甚至闲置为“花瓶”的状态。企业对于技术的追逐，虽然可以促进安全运营业务的发展，但是过于依赖技术，以为花大价钱购买了先进的技术就诸事大吉，其实更是一种误区。

随着企业安全业务的发展，对于 SIEM/SOC 的选择逐渐转变为业务导向型。即从业务架构角度出发，精准挖掘企业安全数据、安全应用等关联需求，匹配人员、技术和流程三大基本要素，只有训练有素的技术员工、核心技术平台 SIEM/SOC 与恰到好处的工作流，才能让安全运营这件事落到实处。

（六）多行业标准化交付能力待提升

由于 SIEM/SOC 涉及专业领域较宽，对使用者的安全能力要求相对较高，而大多数企业存在专业安全技能人才缺失、安全运营人员能力有限等普遍性问题，便会出现企业安全运营人员技术能力无法匹配产品运维的问题。

因此，随着 SIEM/SOC 的市场需求逐渐在各行业普及开来，安全厂商需要实现各行业标准化交付能力，简化产品运维，帮助提升 SIEM/SOC 产品的使用效率。此外，企业也需要注重培养安全运营人才，产品可以提升安全运营效率，但永远无法完全替代人的作用。

在此过程，从厂商及用户端共同促使 SIEM/SOC 有效落地。

九、SIEM/SOC 类产品能力分组

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。

基于测试结果，《2021 中国安全信息和事件管理类产品（SIEM/SOC）研究报告》对参与测评的产品进行产品专业能力划分，并输出九大能力组，以满足不同行业用户的需求，为其在网络安全产品选型过程中提供技术能力参考。

（一）综合技术能力组（8 家）

综合技术能力组（排名不分先后）	
厂家	产品
北京神州绿盟科技有限公司	绿盟安全管理平台
杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
新华三信息安全技术有限公司	安全威胁发现和运营管理平台
网神信息技术（北京）股份有限公司	奇安信网神安全分析与管理系统
深信服科技股份有限公司	深信服 FutureX 安全大数据平台
北京盛华安信息技术有限公司	CyberSky 安全态势感知与管理平台
任子行网络技术股份有限公司	网络安全威胁与事件管理平台
上海观安信息技术股份有限公司	观安安全态势分析系统

（二）日志采集识别与告警能力组（8 家）

日志采集识别与告警能力组（排名不分先后）	
厂家	产品
北京神州绿盟科技有限公司	绿盟安全管理平台
杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
北京安达亚科技有限公司	安达亚 AndaISM 大数据智能运维管理系统

亚信科技（成都）有限公司	MAXS 安全运营和态势分析平台
深信服科技股份有限公司	深信服 FutureX 安全大数据平台
腾讯云计算（北京）有限责任公司	腾讯 T-Sec-安全运营中心
网神信息技术（北京）股份有限公司	奇安信网神安全分析与管理系统
上海观安信息技术股份有限公司	观安安全态势分析系统

（三）威胁情报采集与安全分析能力（8 家）

威胁情报采集与安全分析能力（排名不分先后）	
厂家	产品
杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
网神信息技术（北京）股份有限公司	奇安信网神安全分析与管理系统
北京神州绿盟科技有限公司	绿盟安全管理平台
北京盛华安信息技术有限公司	CyberSky 安全态势感知与管理平台
深信服科技股份有限公司	深信服 FutureX 安全大数据平台
新华三信息安全技术有限公司	安全威胁发现和运营管理平台
腾讯云计算（北京）有限责任公司	腾讯 T-Sec-安全运营中心
北京神州泰岳软件股份有限公司	神州泰岳信息安全大数据态势感知系统

（四）态势感知能力（8 家）

态势感知能力（排名不分先后）	
厂家	产品
深信服科技股份有限公司	深信服 FutureX 安全大数据平台
北京神州绿盟科技有限公司	绿盟安全管理平台
杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
亚信科技（成都）有限公司	MAXS 安全运营和态势分析平台
网神信息技术（北京）股份有限公司	奇安信网神安全分析与管理系统
新华三信息安全技术有限公司	安全威胁发现和运营管理平台
北京盛华安信息技术有限公司	CyberSky 安全态势感知与管理平台
腾讯云计算（北京）有限责任公司	腾讯 T-Sec-安全运营中心

（五）ATT&CK 攻击链溯源能力（8 家）

ATT&CK 攻击链溯源能力（排名不分先后）	
厂家	产品
北京神州绿盟科技有限公司	绿盟安全管理平台

杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
新华三信息安全技术有限公司	安全威胁发现和运营管理平台
任子行网络技术股份有限公司	网络安全威胁与事件管理平台
网神信息技术（北京）股份有限公司	奇安信网神安全分析与管理系统
亚信科技（成都）有限公司	MAXS 安全运营和态势分析平台
深信服科技股份有限公司	深信服 FutureX 安全大数据平台
腾讯云计算（北京）有限责任公司	腾讯 T-Sec-安全运营中心

（六）安全治理能力（8 家）

安全治理能力（排名不分先后）	
厂家	产品
网神信息技术（北京）股份有限公司	奇安信网神安全分析与管理系统
杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
北京神州绿盟科技有限公司	绿盟安全管理平台
厦门服云信息科技有限公司	安全狗啸天-网络安全智能分析与安全管理系统
任子行网络技术股份有限公司	网络安全威胁与事件管理平台
新华三信息安全技术有限公司	安全威胁发现和运营管理平台
深信服科技股份有限公司	深信服 FutureX 安全大数据平台
上海观安信息技术股份有限公司	观安安全态势分析系统

（七）安全编排和全过程自动化能力（SOAR）（8 家）

安全编排和全过程自动化能力（SOAR）能力（排名不分先后）	
厂家	产品
新华三信息安全技术有限公司	安全威胁发现和运营管理平台
北京盛华安信息技术有限公司	CyberSky 安全态势感知与管理平
北京神州绿盟科技有限公司	绿盟安全管理平台
杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
上海观安信息技术股份有限公司	观安安全态势分析系统
中电福富信息科技有限公司	网络安全运营管理平台
北京安达亚科技有限公司	安达亚 AndaISM 大数据智能运维管理系统
北京神州泰岳软件股份有限公司	神州泰岳信息安全大数据态势感知系统

（八）用户和实体行为分析能力（UEBA）（8 家）

用户和实体行为分析能力（排名不分先后）	
厂家	产品
新华三信息安全技术有限公司	安全威胁发现和运营管理平台
北京盛华安信息技术有限公司	CyberSky 安全态势感知与管理平
北京神州绿盟科技有限公司	绿盟安全管理平台
杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
网神信息技术（北京）股份有限公司	奇安信网神安全分析与管理系统
中电福富信息科技有限公司	网络安全运营管理平台
任子行网络技术股份有限公司	网络安全威胁与事件管理平台
上海观安信息技术股份有限公司	观安安全态势分析系统

（九）安全运营与应急响应能力（8 家）

安全运营与应急响应能力（排名不分先后）	
厂家	产品
网神信息技术（北京）股份有限公司	奇安信网神安全分析与管理系统
杭州安恒信息技术股份有限公司	AiLPHA 大数据智能安全平台
北京神州绿盟科技有限公司	绿盟安全管理平台
深信服科技股份有限公司	深信服 FutureX 安全大数据平台
新华三信息安全技术有限公司	安全威胁发现和运营管理平台
亚信科技（成都）有限公司	MAXS 安全运营和态势分析平台
任子行网络技术股份有限公司	网络安全威胁与事件管理平台
腾讯云计算（北京）有限责任公司	腾讯 T-Sec-安全运营中心

关于

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始建于 1957 年，是工业和信息化部直属科研事业单位，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，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。

上海斗象科技有限公司简介

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。上海斗象科技有限公司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，呈现最专业地研究与咨询服务。

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