头豹行业研读 | 2021/02

2021年
中国云安全托管行业概览：市场及技术初步观测

2021
Overview of China's Cloud Managed Security Service Industry: Preliminary Study of Market and Technology

2021年
中国のクラウドセキュリティホスティング業界の概要：市場とテクノロジーの予備的観察

报告标签：网络安全服务、云安全托管、SOAR、威胁检测与响应

头豹研究院

概览摘要

头豹谨此发布中国云安全托管系列报告之《中国云安全托管行业概览：市场及技术初步观测》行业报告。本报告旨在分析中国云安全托管行业市场概况及技术应等，技术主要集中于人工智能技术。2021年第一季度，头豹研究院对云安全托管服务领域核心产品进行了下游用户体验调查。受访者来自泛互联网、金融、医疗、教育、制造、物流等多个行业，所在公司规模不一，细分领域有别。

本报告所有图、表、文字中的数据均源自弗若斯特沙利文咨询（中国）及头豹研究院调查，数据均采用四舍五入，小数计一位。

- **MSS行业发展前景开阔**

2020年中国云安全托管服务（MSS）行业处于初步阶段；安全托管及运维托管概念相对超前。但由于中国安全即服务风潮、网安全人才缺口、等保政策趋严等因素将有望推动中国MSS行业概念普及、市场扩容。

- **运营流程自动化、技术智能化**

AI技术带动云网络安全托管所需技术短期效益提升，推动安全运营及托管的流程自动化、技术智能化发展，进一步降低威胁分析及响应周期、提升人力分析效率，为数字化时代下安全及服务和运营即服务夯实基础。

- **人力成本缩减、威胁识别精准提升**

2020年，SIEM与AI集成应用（AI&SIEM）仍处于识别及理解阶段，主要通过异常检测、线性预测等基础机器学习算法集成SIEM系统，实现人力成本缩减及威胁识别准确率提升。但距离AI@SIEM阶段仍存在差距。

- **编排流程自动化，威胁响应效率及精度双提升**

将以机器学习技术引入SOAR中能促进MSSP人机协同能力以实现流程、技术及人类智能三方整合。SOAR中较繁琐及简单重复的流程转移至机器分析，有效减轻分析师工作负载，实现响应时长及分析准度双提升。

目录

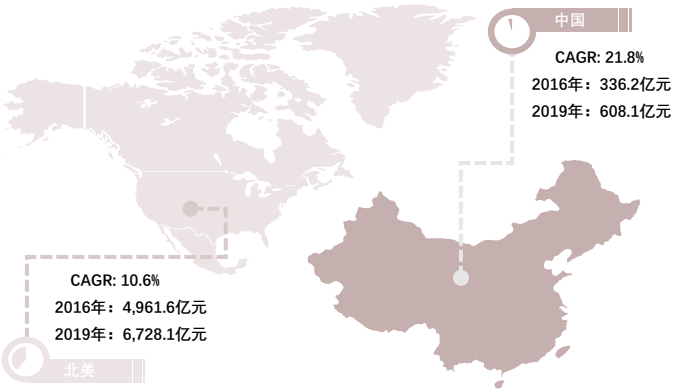
Contents

宏观网络安全市场概述——市场现况简述

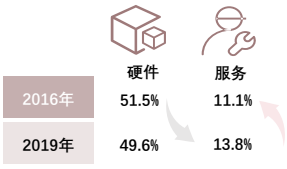
中国网络安全市场以网络安全硬件产品为主，整体市场空间及需求较大。伴随着网络技术持续迭代及云迁移需求释放，中国网络安全市场逐步掀起安全即服务风潮

网络安全市场对比，2016-2019年

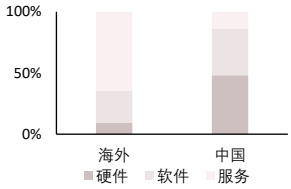
网络安全市场规模区域对比，2016-2019年



中国网络安全产品结构，2016-2019年



网络安全产品结构对比，2018年



中国网络安全市场发展前景开阔，未来有望领跑全球网络安全

网络安全是保护网络系统的硬件、软件和系统中的数据免受恶意攻击的技术。网络安全具体包括网络空间、物理空间、数据空间安全，涵盖网络系统的运行安全性、网络信息的内容安全性、网络数据的传输安全性、网络主体物理资产的安全性。

相较于北美网络安全市场，中国网络信息安全行业起步较晚、用户网络安全意识较为落后，整体网络安全行业市场仍处于上升发展周期，发展前景较为明朗。2017年起，中国网络安全市场规模增速及年复合增长率领跑全球网络安全市场。同时，中国IT支出规模逐步提升，位居世界第二，整体网络安全市场发展潜力较大。

传统网络安全市场以硬件产品为核心，“安全即服务”风潮推动中国网络安全从产品向服务转型

网络安全市场可划分为安全硬件、软件、服务市场。中国网络安全市场以硬件产品为主，其安全硬件产品占中国网络安全产品市场的48.1%。但2014年后，传统网络架构逐步向云计算演变，而传统的网络信息安全硬件产品难以满足日趋复杂的网络环境，网络安全服务重要性日渐凸显。中国网络安全服务市场占比从2016年的11.1%上升至2018年的13.8%。中国网络安全服务市场主要由托管安全服务、咨询服务、集成服务三大板块组成。其中，托管安全服务是网络安全产品及服务集成的表现。

来源：虎符智库，头豹研究院编辑整理

宏观网络安全市场概述——驱动因素

随着物联网及云计算市场快速扩容，信息安全暴露面加大，日常网络安全事件频发；同时国际争端加剧及疫情下远程办公形式创新进一步推动网络安全及相关服务需求持续释放

奇安信网络安全应急响应受攻击行业分析

2019-2020

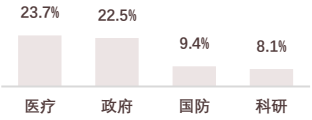
	2020	2019	2018
政府	146	132	63
医疗卫生	90	153	56
事业单位	61	118	30
金融	60	68	24
制造业	42	40	40
交通运输	34	54	23
IT信息技术	33	64	31
教育培训	33	51	35
公检	29	84	66
能源	18	26	-

疫情下网络安全概况

2020H1

中国安全漏洞数量同比增幅

中国高级威胁事件涉及行业分布



驱动一：日常网络安全事件频发，政府、医疗卫生、事业单位、金融为网络攻击的主要目标

伴随着网络技术的持续升级，在0 day攻击、ATP攻击、DDoS攻击等网络安全事件频发，中国政府政府及企业对网络安全的重视程度持续加深。根据奇安信2020年网络安全应急响应分析报告，奇安信集团安服团队2020年共接收到660起，政府部门、医疗卫生、事业单位及金融行业为2020年主要攻击目标；该四大行业应急安全事件处置数占安全事件处置总数的54.1%。

驱动二：国际争端加剧及新冠疫情爆发，国际网络攻击目的主要集中于军事及医疗行业窃密

2020年国际争端加剧，国家之间网络攻击频率逐步提升，而网络攻击行动的主要目的集中于军事情报的泄密及新冠疫苗相关研究数据及成果的窃取。根据头豹研究院及虎符智库数据显示，2020年全球高级持续威胁攻击数量增幅高达23%，其中针对中国大陆的高级持续威胁攻击数量增幅则超过60%。纵观2020年高级威胁事件行业分布，医疗、政府、国防、科研四大行业板块占比共计63.7%。

驱动三：中国数字化转型及远程办公需求释放，网络端口数量增长、带来潜在网络安全隐患

中国新基建数字化转型，5G等数字技术得以进一步普及，智能家居、智慧工业、智慧城市等相关物联网设备数量实现爆发性增长。同时，物联网网络端口数量随之上升，从而提高信息泄露、物联网网设备漏洞等网络安全风险。此外，2020年疫情冲击下，中国远程办公需求爆发性增长，高峰期远程办公需求环比增长超过650%；而远程办公应用开放大量网络端口，企业重要数据资产保护及云上业务安全运营风险增加，中国网络安全需求持续释放。

来源：虎符智库，头豹研究院编辑整理

安全托管服务市场概述——市场现况简述

安全托管服务为集成安全运维、安全产品转售、安全管理咨询的第三方外包服务。中国网络安全托管服务业务范围较小，集中于安全运维，以中小型企业为核心目标客户；整体行业仍处于初期发展阶段

网络安全托管服务是安全产品、专业安防专家团队运维及企业安全管理策略咨询的集成性服务

网络安全托管服务（MSS）属于网络安全服务的典型代表，主要指将企业信息化的网络安全维护环节外包于第三方网络安全托管服务供应商（MSSP）；根据国际市场标准定义，托管安全服务供应商通过其安全运营中心（SOC）及相关服务水平协议（SLA）为客户提供全天候人工安全监控、威胁分析、预警情报、应急响应、快速系统恢复等网络安全产品集成、专业人员安全运维及企业安全管理策略咨询等服务。根据服务类型分类，网络安全托管市场涵盖客户本地驻场托管服务（MSS-CPE）、远程托管安全服务（MSS-Hosted）和云托管安全服务（CHESS）三大细分市场。

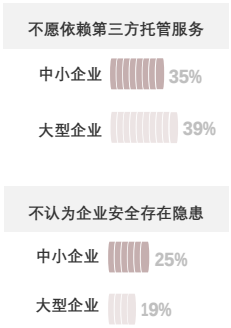
相较于海外市场，中国安全托管服务市场在成熟度、业务范围、目标客户等三个层面存在差异

从市场规模及发展进程的角度分析，截止于2021年，海外托管安全服务市场发展较为成熟，已成为海外网络安全服务中规模最大的子市场。根据头豹研究院数据显示，2019年托管安全服务占全球IT安全产品及服务市场的23%，同时其2019年的投资规模超出470亿美元。在中国网络安全市场方面，中国网络安全服务行业起步晚，整体发展进程较落后于世界平均水平；但2017年后，中国网络安全服务市场占比逐步提升；托管网络安全服务行业作为网络安全服务行业的典型代表，未来整体发展前景开阔。

就安全托管业务范围及目标客户层面分析，海外网络安全托管服务指网络安全产品、运维服务及安全管理咨询等集成整合服务，发展较为成熟，主要目标客户群体集中于海外中大型企业，整体利润空间较大。而中国网络安全业务范围较为小，主要集中于安全运维服务。此外，由于中国网络安全服务处于初级阶段，同时企业内部信息资产安全敏感度较高，安全托管服务市场需求接受度存在上升空间。此外，由于中大型企业安全运维成本敏感度较低，因而偏向于自发组织安全运维团队，中国网络安全托管中大型企业需求暂未完全释放，因此中国MSSP目标客户仍集中于中小型企业。

托管安全服务业务范围（常规）

卡巴斯基市场调研结果

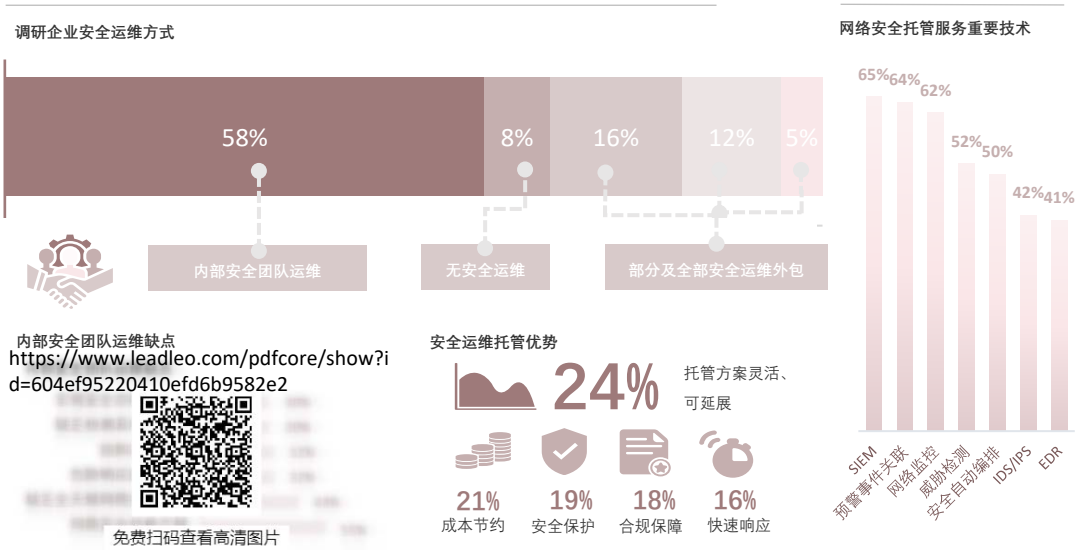


来源：卡巴斯基，头豹研究院编辑整理

安全托管服务市场概述——服务优势

安全托管服务在专业技术、运维成本、业务弹性等维度占据优势；2020年中国网络安全托管服务概念较为超前，随着云厂商对MSS业务的推动，MSS市场接受度有望持续提升

AT&T企业信息安全运维托管市场反馈调研，2018年



相较于企业内部IT团队运维，网络安全托管在专业技术、运维成本、业务弹性等方面具备优势

在安全保障及技术层面中，根据AT&T市场调研显示，企业自发组织IT运维团队仍为市场主流，但调研企业普遍认为内部团队运维在技术（55%）、监管时长（43%）、应急响应速度（32%）等方面有所欠缺。相较于内部团队，安全运维托管服务拥有更专业的安全维护团队、通畅的信息渠道、可靠的厂商支持，因而能有效解决部分企业安全技术和人员双重短缺的问题。根据市场反馈结果，SIEM（65%）、预警事件关联（64%）、安全监控（60%）为MSS中最具备价值的服务环节及技术。

此外，安全托管服务在运维业务运维成本、外包运维服务灵活上具备相对优势。在市场调研中，24%的受访人员表示，所在企业更看重安全托管业务的灵活度及可延展性，以应对短期内重点网络安全防御部署需求。同时，运维成本缩减为企业（21%）采用安全托管形式的驱动因素之一。45%受访者表示安全托管模式能有效缩减10%-25%的安全运维成本。

2020年，安全托管服务概念在中国市场仍相对超前，但随着中国网络安全及服务风潮持续演进及腾讯、华为、阿里巴巴等云服务厂商的云上安全托管业务推动，安全托管服务技术、成本及业务弹性优势日益凸显，市场接受度有望得以提升。

来源：AT&T、中国电信、头豹研究院编辑整理

■ 安全托管服务市场概述——竞争格局

MSSP主要分布于三大阵营：云服务供应商、电信运营商及网络安全公司；其中云厂商具备天然MSS属性，通过云原生等技术将云安全业务外延至MSS，有效降低边际成本

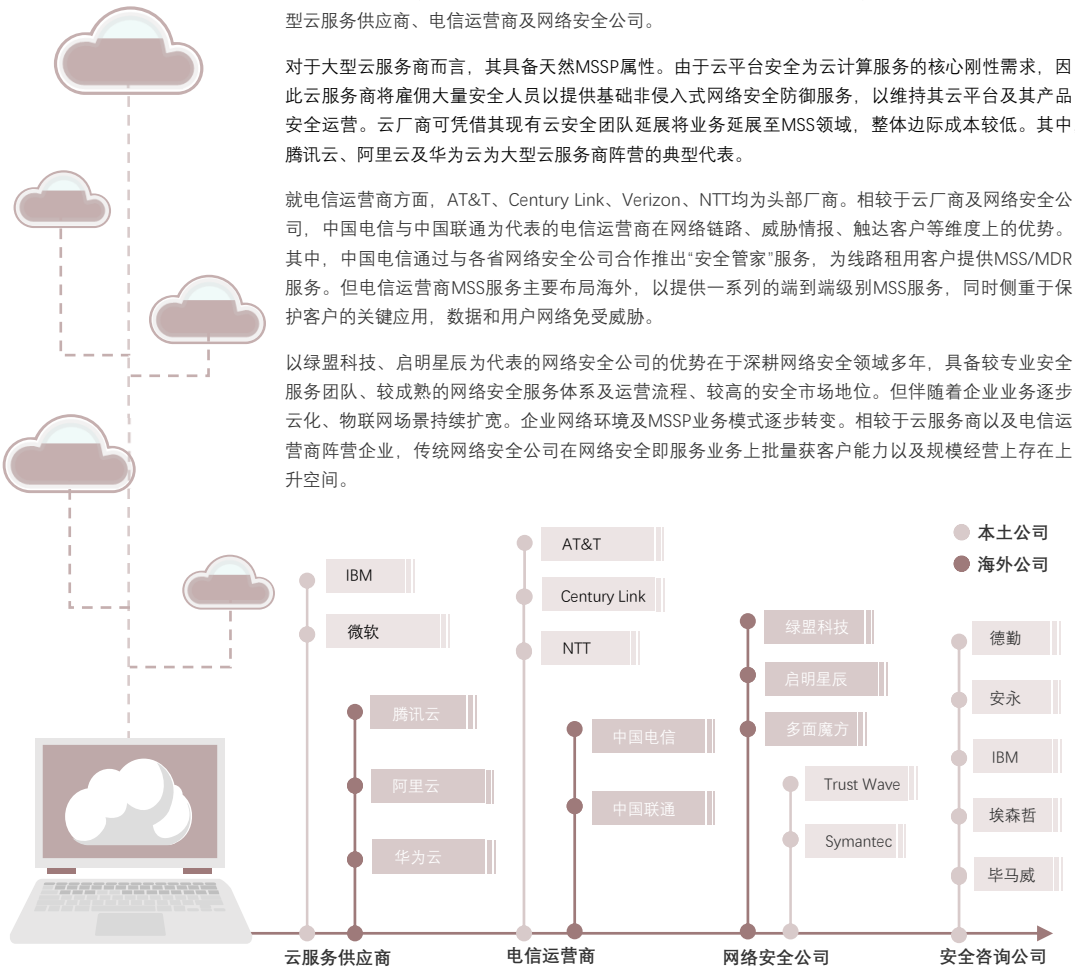
■ **安全托管服务供应商（MSSP）三大阵营**

除了以德勤、安永及埃森哲等传统的安全咨询公司，安全托管服务供应商主要分布三大阵营,涵盖大型云服务供应商、电信运营商及网络安全公司。

对于大型云服务商而言，其具备天然MSSP属性。由于云平台安全为云计算服务的核心刚性需求，因此云服务商将雇佣大量安全人员以提供基础非侵入式网络安全防御服务，以维持其云平台及其产品安全运营。云厂商可凭借其现有云安全团队延展将业务延展至MSS领域，整体边际成本较低。其中，腾讯云、阿里云及华为云为大型云服务商阵营的典型代表。

就电信运营商方面，AT&T、Century Link、Verizon、NTT均为头部厂商。相较于云厂商及网络安全公司，中国电信与中国联通为代表的电信运营商在网络链路、威胁情报、触达客户等维度上的优势。其中，中国电信通过与各省网络安全公司合作推出“安全管家”服务，为线路租用客户提供MSS/MDR服务。但电信运营商MSS服务主要布局海外，以提供一系列的端到端级别MSS服务，同时侧重于保护客户的关键应用，数据和用户网络免受威胁。

以绿盟科技、启明星辰为代表的网络安全公司的优势在于深耕网络安全领域多年，具备较专业安全服务团队、较成熟的网络安全服务体系及运营流程、较高的安全市场地位。但伴随着企业业务逐步云化、物联网场景持续扩宽。企业网络环境及MSSP业务模式逐步转变。相较于云服务商以及电信运营商阵营企业，传统网络安全公司在网络安全即服务业务上批量获客户能力以及规模经营上存在上升空间。

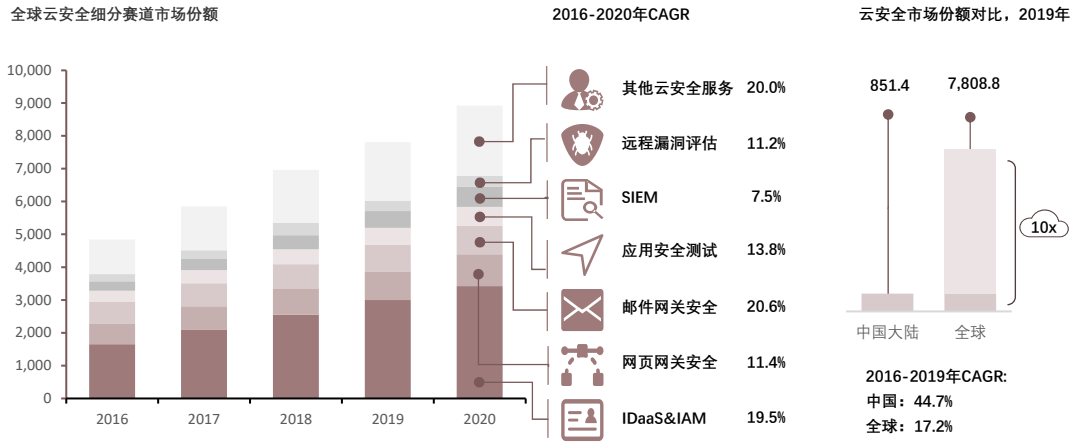


来源：安全内参、中国电信、头豹研究院编辑整理

云安全托管服务市场概述——市场现状简述

2020年中国云安全托管服务行业处于初步阶段。但伴随着云安全需求释放及SOAR等MSSP运维技术迭代及提升，有望推动传统MSSP业务向云端建构转型

全球云安全市场份额细分赛道及区域对比（百万美元），2016-2020年



- **MSSP从传统驻场安全托管运维服务转型至云安全运维，服务实现云安全风险事件快速响应、数据泄露及安全漏洞持续监控**

2020年，云计算、大数据、物联网及人工智能技术驱动下，企业数字化程度逐渐提升。企业信息安全防御关口逐步前移，从被动防御转向主动防御；同时，安全即服务风潮持续推动下，中国网络安全商业模式实现从“产品”到“产品+服务”模式转型。得益于SIEM、SOAR等网络安全产品及技术迭代及云计算需求释放，MSSP从传统驻场安全托管运维服务转型至云上远程运维环节。与传统网络安全托管服务相比，云安全托管供服务应商通过云上安全监管及运维服务实现安全风险事件快速响应、数据泄露及安全漏洞持续监控，确保企业客户关键业务数据资产在多云之间安全状态的一致性及无缝性。

伴随着中国社会数字化转型，大量企业将其业务迁移至云端。但由于上云企业的IT环境转变为混合云、多云的架构，其环境复杂性将大幅提高，网络安全暴露面加大，云安全需求持续释放。2016年后，全球云端应用安全监测、SIEM、远程漏洞评估等云安全细分市场持续扩容，2016年至2020年平均年复合增长率超过15%。纵观全球云安全市场，中国云安全市场体量较大，占全球市场1/10。整体增速高达44%。未来中国云上SIEM、远程漏洞评估及相关云安全运维等市场扩容将有望推动云托管服务行业向规模化、标准化发展。

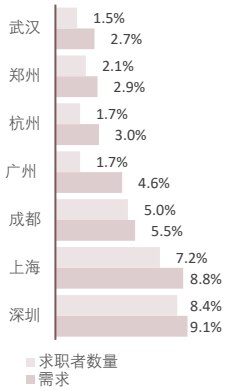
来源：中国银河证券、头豹研究院编辑整理

云安全托管服务市场概述——驱动因素

2020年，中国网络安全人才缺口及等级保护制度升级导致中小企业自主组织IT运维团队费用上升，网络安全运维外包需求释放，带动中国MSS市场进一步普及

网络安全人才供求对比

2019



驱动一：中国网络安全人才缺口及运维成本较高等问题加速中小企业MSS服务需求快速释放

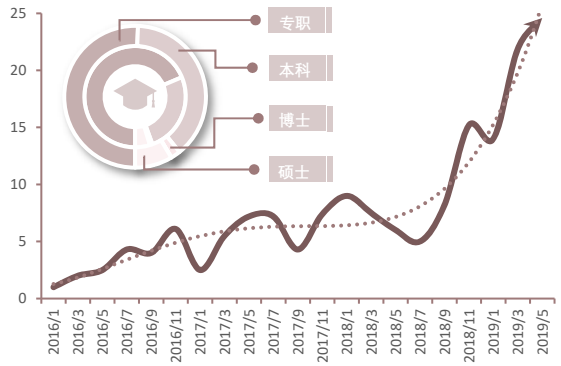
企业云迁移及后续云上安全运营需要企业内部安全团队必须同时掌握传统本地安全技术及更多基于云端的安全选项及技术。由于市场安全从业人员较为紧缺，人才短板问题日益加重。2020年至2019年，网络安全需求量整体增长25倍，深圳、上海、成都等[illegible]象。对于大型企业而言，其资规模较大、盈利能力较强，因而具[illegible]队。但中小型企业而言，人才培养难度较大、时间成本较高，同[illegible]后期运营费用，从而阻碍其云迁移进程。根据REEBUF数据显示，[illegible]为加速上云的最大阻碍，47%的企业表示缺乏合格安全人员为主要[illegible]应用云原生安全产品培养其技术团队，持续更新其SOC和NOC以[illegible]供灵活度较高的个性化安全服务。同时，中小企业可通过与MSSP[illegible]紧缺问题。

驱动二：网络安全法规驱严，等级保护制度升级推动云网络安全

相较于等级保1.0，等级保护2.0监管范围从单一信息系统延伸至网络[illegible]云计算等新技术领域，在风险评估、安全检测、威胁预警、数据灾备、[illegible]管要求。同时，企业网络安全定期要求及监管力度趋严，中小企业在防[illegible]理水平上存在短板，短期内难以实现等保合规，从而推动中小企业对MSS[illegible]

网络安全托管驱动因素

驱动一：网安全人才需求及2019年人员就业岗位学历供求分布（内/外：供/求）



驱动二：等保2.0与1.0对比

	等保1.0	
监管范围	信息系统	信息系统、数据、[illegible]
技术要求	物理安全、网络安全、应用安全等	物理环境安全、计算[illegible]
管理要求	安全管理制度及机构、人员安全管理等	安全管理制度及机构、[illegible]理人员、安全运维管理等
定级要求	自主定级	自主定级及网络安全等级保护专家评审
测评周期	三级：每年一次 四级：半年一次	三级及以上：每年一次
合规评分	60分	75分
新增要求	/	SOC、主动防御、态势感知、自主可控

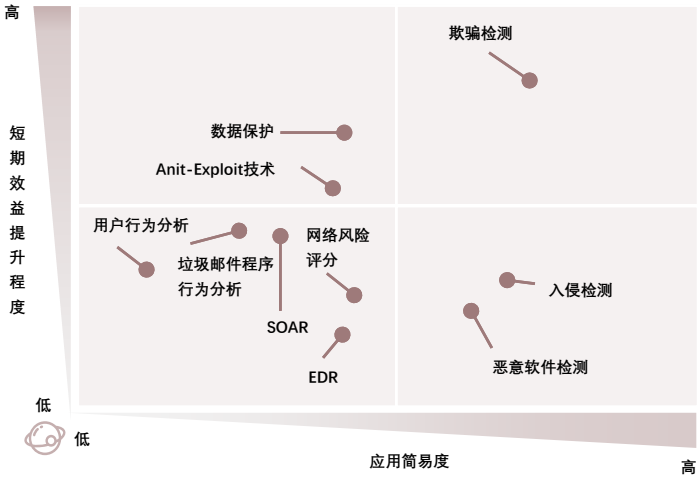
来源：REEBUF、奇安信、中国银河证券、头豹研究院编辑整理

云安全托管人工智能技术——人工智能应用概述

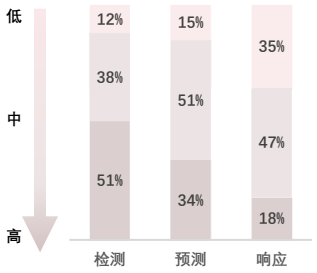
人工智能技术应用持续深化，现实网络安全防御精准把控、运维团队高效分析、时间及资金成本缩减等方面大幅提升；与MSS所需技术相融合，为行业自动化智能化发展夯实基础

人工智能技术于信息安全领域分析

人工智能技术与信息安全技术应用演进，2019年



Capgemini企业信息安全调研：AI应用程度



Capgemini企业信息安全调研：AI应用优势

■ **人工智能技术带动EDR、SOAR等MSSP必备技术升级，实现MSS运维效率及防御精准度双提升**

2016年后，得益于云计算及虚拟化技术的迭代升级及大数据开发应用，人工智能技术算力、模型精准度及稳健度得以持续提升，同时其应用场景持续扩展，涵盖金融、通讯、零售、保险、工业等行业。在网络信息安全及安全运维领域中，以机器学习为代表AI技术应用程度持续深化，提高企业在传统网络与云上虚拟环境的安全防御的准确性及运维人员分析的高效性，同时缩减企业在安全部署及运维中的时间及资金成本。纵观企业数字化安全防御三大环节，安全检测环节与AI技术结合应用程度及自动化水平相对较高，而风险预测及威胁响应环节中AI应用仍存在难度。根据Capgemini2019年企业网络安全及AI应用的行业调研数据显示，51%企业高管表示AI技术在企业风险检测环节应用程度较高。但在风险预测及威胁响应环节达到AI高度应用的企业仅为34%及18%。

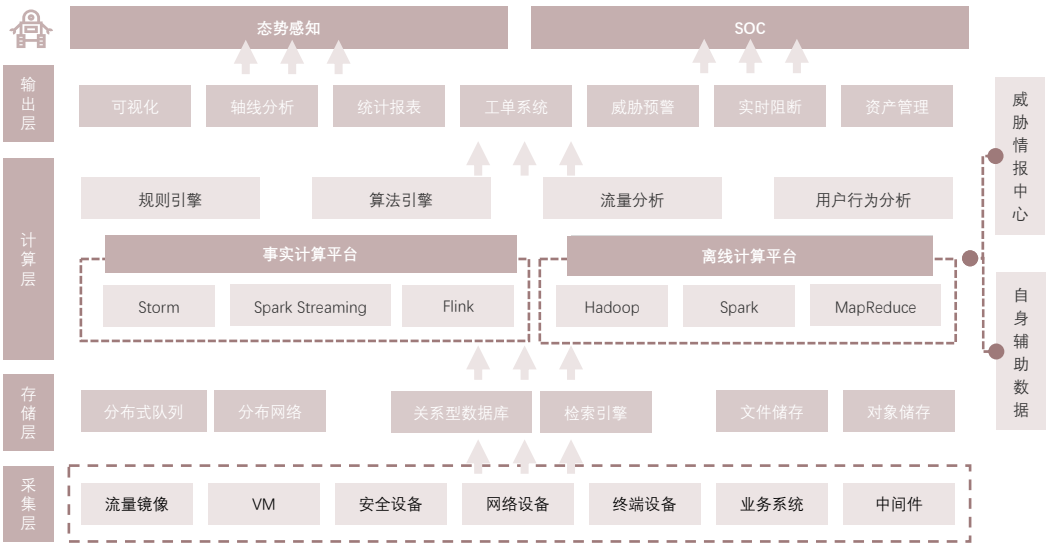
从AI应用网络安全技术演进的角度分析，随着AI技术持续升级，EDR、SOAR、恶意软件检测及入侵检测等云网络安全托管所需技术短期效益提升程度均有所增加，安全运营及托管的流程自动化、技术智能化成为必要发展趋势，进一步降低威胁分析及响应周期、增加人力分析高效性，从而为数字化时代下安全即服务和运营即服务夯实基础。

来源：Capgemini、绿盟科技官网、头豹研究院编辑整理

云安全托管服务人工智能技术——AI&SIEM

通过异常检测、线性预测等基础机器学习算法集成SIEM系统，实现人力成本缩减及威胁识别准确率提升；但2020年，MSS行业仍处于AI&SIEM阶段，距离AI@SIEM阶段仍存在差距

SIEM平台解构



■ **SIEM&AI有效实现MSS服务人力成本缩减及威胁识别准确率双提升**

SIEM（安全信息事件管理平台）为企业及MSSP网络及云安全运维基础与核心，负责收集汇总数据以结合威胁情报对企业网络及云资产危险进行判断与预警。SIEM系统平台架构可划分为五个层次，涵盖采集层、存储层、计算层、输出层及情报中心，分别负责数据采集与来源划分、储存信息数据及分析完成结果、运用核心算法逻辑对信息数据进行分析计算、按需输出及可视化结果、提供额外数据支持以提升威胁行为识别率。

AI技术于网络安全领域集成应用阶段可划分为识别、理解、反馈三个发展阶段。识别阶段是运用大量无监督及样本提取从而形成分类器。随着样本数据累积，分类器将样本数据样本进行机器学习训练、从而形成自动化识别及预测模型，生成识别结果。而理解阶段则是通过机器学习及部分深度学习技术将理解问题转化构建为识别问题。而反馈阶段则是实现真实人机交互、作业全自动化及智能化。SIEM于AI集成应用仍处于识别及理解阶段。通过异常检测、线性预测等基础机器学习算法集成SIEM系统，实现部分人力成本缩减及威胁识别准确率提升。但距离AI@SIEM（AI自动挖掘潜在威胁数据，对不同维度数据进行智能分类及关联，从而自发形成威胁响应及处理机制）阶段仍存在差距。

来源：CSDN（钱曙光）、头豹研究院编辑整理

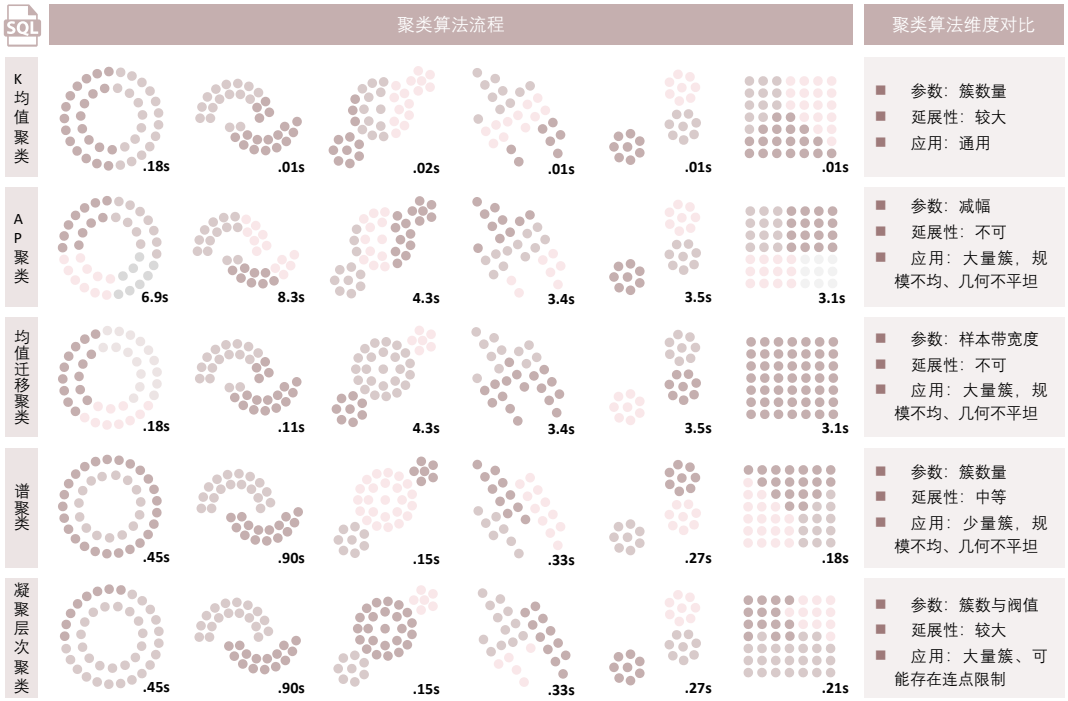
云安全托管服务人工智能技术——无监督学习与ATD

无监督学习通过聚类算法有效解决安全数据膨胀及信息杂乱等导致数据标注难的问题；在云上及传统MSS应用领域，其主要应用于ATD系统集成应用，实现快速及智能威胁识别

■ **无监督学习有效避免数据标注过程，从而提升ATD威胁识别效率**

由于数据膨胀及信息杂乱，网络威胁数据难以显现分类标注，导致系统计算层难以运用标准及准确样本进行机器学习。针对样本数据标注难等问题，无监督学习可摆脱数据标注依赖，通过将数据聚类法以实现无样本标注情景下的自主学习。根据聚类过程差异，无监督学习聚类可分为距离聚类、核密度聚类及层次聚类。其中，距离聚类算法应用最为广泛，主要通过对于距离中心点的持续迭代修正将样本归类于不同的样本簇。其实现关键在于数据事件及事件间距离的界定及初始簇的数量。而核密度及层次聚类则是分别根据初始密度及节点分层实现数据样本聚类。在云上及传统MSS应用领域，无监督学习聚类与ATD（深度威胁识别）系统集成应用，实现快速及智能威胁识别。

无监督学习聚类算法对比

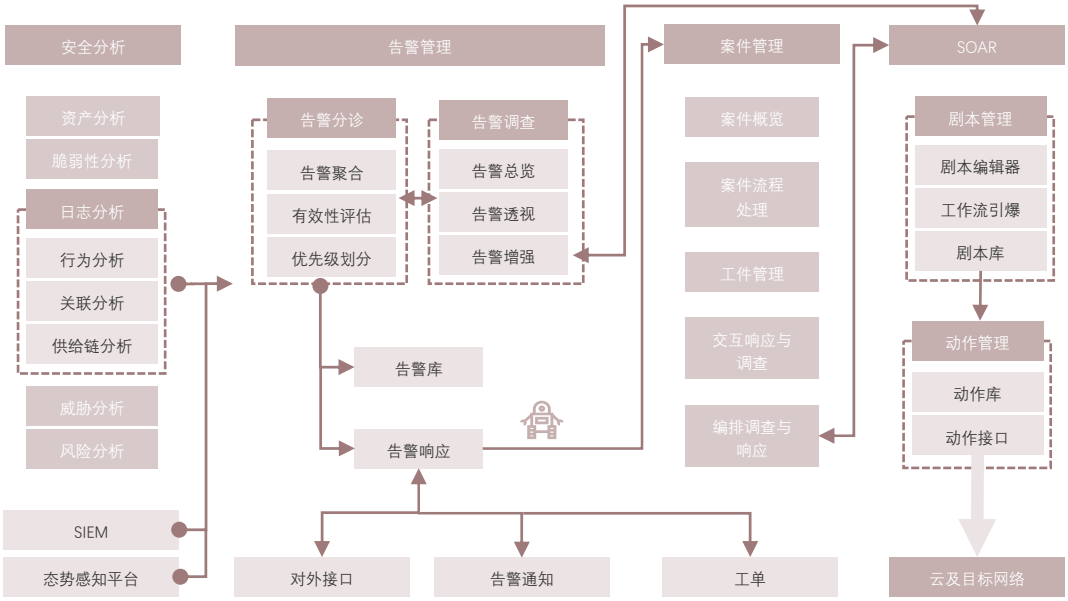


来源：CSDN（钱曙光）、Scikit Learn、头豹研究院编辑整理

■ 云安全托管服务人工智能技术——机器学习与SOAR

SOAR集成安全编排自动化、安全事件响应平台及威胁情报平台三种核心能力，以剧本的形式执行事件分类与分析，提升应急响应效率、实现工作流程自动化、标准化、智能化

SOAR流程



■ **SOAR集成SOA、SIRPs及TIPS三种核心能力以现实工作流程自动化、标准化及智能化**

2019年，得益于中国网络安全及云安全产品逐步完善，企业运维团队关联分析能力得以大幅提升，平均威胁检测时间呈现下降趋势，但企业消耗于安全应急响应时间仍过长。减缓MTTR（Mean Time to Response）的因素有三：（1）网络安全及运维专业人才短缺。根据MSSP服务龙头企业IBM2019年用户调研结果显示，77%的IBM企业用户难以雇佣一位具备安全分析能力得安防专家。（2）2019年后企业网络安全威胁事件快速频发，同时XDR、EDR等安全检测技术迭代升级，企业潜在及可疑网络安全威胁告警数量大幅增长，导致安全工程师安全分析任务负载过重。（3）网络安全自动化水平存在上升空间，安全分析效率难以提升。而SOAR作为安全编排自动化（SOA）、安全事件响应平台（SIRPs）及威胁情报平台（TIPS）三种核心能力的集成技术，为企业组织收集不同来源安全威胁数据并以剧本的形式执行事件分类与分析，提升应急响应效率、实现工作流程自动化、标准化，有效解决响应过程中人员短缺、警报分类质量和速度较低、安全人员工作负载过重等问题。

来源：CSDN、头豹研究院编辑整理

云安全托管服务人工智能技术——机器学习与SOAR

得益于机器学习与SOAR技术融合，提升云MSS服务人机协同效率。同时由于云安全需求释放，云部署SOAR占比持续提升，推动SOAR技术成为MSS行业大趋势

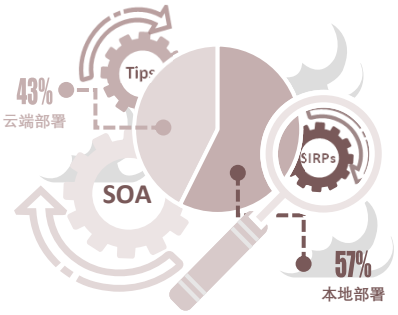
机器学习与SOAR促MSSP分析人员人机协同能力，实现流程、技术及人类智能三方整合

将以机器学习为代表的人工智能技术引入SOAR自动化编排中能促进企业安全运营团队及MSSP分析人员人机协同能力以实现流程、技术及人类智能三方整合。智能编排程序中较繁琐及简单重复的流程可有效转移至机器算法分析，有效减轻分析师工作负载，从而发挥其安全运维分技能及经验的相对优势，实现响应时长及分析准确度双提升。而根据头豹研究院及Capgemini数据显示，AI技术的应用有效缩减12%的检测威胁和漏洞总时间，SOAR补救漏洞或实施补丁等攻击响应所需的时间同时缩减13%。

SOAR云部署需求释放，进一步带动安全即服务行业持续扩容及AISecOpc应用场景逐步拓宽。

在云安全场景中，透过机器学习技术，SOAR技术能够较为精准响应密集网络攻击，涵盖零日攻击及无档案攻击等。同时，SOAR云端应用可通过云原生架构及容器化技术与企业网络系统整合，将安全编排及响应运用云平台，降低应急响应处置的边际成本，同时满足企业云业务安全及高效运营需求。

全球SOAR部署形式市场占比，2019年



2019年，全球云安全托管服务及SOAR龙头企业IBM为法国医疗保险公司提供SOAR相关服务。该企业整体体量较大，其数据涉及客户敏感信息，因而需对企业数据进行高效管理。IBM通过提升相关组件，将SOAR解决方案Resilient迁移至Saas，同时运用IBM QRadar Network Insight V1901及Securiity QRadar SIEM，大幅提升该企业威胁识别及安全响应效率，增强安全平台运维效率及企业内部协作效应。截止于2020年，随着企业信息数字化进程加速，云端部署SOAR占全球SOAR市场份额占比超过40%。长期来看，未来云安全托管服务需求释放有望推动SOAR云上部署市场份额提升，从而进一步带动全球安全即服务行业持续扩容及AISecOpc应用场景逐步拓宽。

SOAR为云MSS服务技术主要趋势

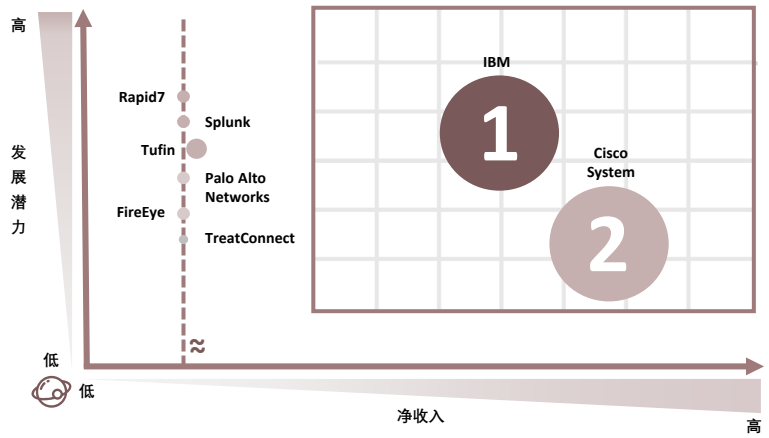
从编排自动化技术层面分析，智能化决策将有望成为安全编排发展趋势。现阶段而言，主要运用决策算法分为四类，涵盖有限状态决策模型、决策树模型、基于知识推理的决策模型及基于价值的决策模型。但系统算法对网络安全及攻防环境的感知不确定性较大，存在一定决策风险。伴随安全编排自动化及智能化程度提升，SOAR将有望通过累积过往安全分析专家处置评估安全事件数据，训练机器学习及深度学习模型与参数，从而提升智能系统对攻击的理解能力及自身脆弱性评估。编排系统将能透过具备分析当前安全态势，生成合理有效智能化安全决策方案，摆脱简单代码（续下一页）

来源：CSDN、HKT官网、 Capgemini、安恒信息、KBY、安全内参、头豹研究院编辑整理

云安全托管服务人工智能技术——机器学习与SOAR

智能化及自动化SOAR为云安全托管行业技术发展主要趋势；由于SOAR专业供应商以初创企业为主，IBM等安全大厂相继提出收购方案，导致SOAR产品主要向集成化、轻量化发展

全球SOAR竞争格局，2019年



（承接上一页）if-then条件语句结构，从而避免攻击者改变相关变量绕过安全处置。

从SOAR产品及服务发展维度看，SOAR技术跟UEBI相似，均属于技术集成独立产品。但由于专业SOAR厂商以初创公司为主；SIEM及SOC安全大厂资金实力较强，均通过收购SOAR公司将编排自动化技术集成或整合成为旗下产品及相关组件，有效解决安全监测、安全响应组模块设备孤立及技术整合度较低痛点，从而实现综合分析能力及团队安全运营效率双提升。2016年IBM通过收购Resilient Systems，将其发展为SOAR产品。该产品可与且Qradar SIEM集成以形成SOAPA解决方案。此外，2018年LogRhym在其NG SIEM产品中集成SOAR组件SmartResponse。未来SOAR产品有望与SIEM和SOC等整合、向着集成化及轻量化产品及组件形式发展。

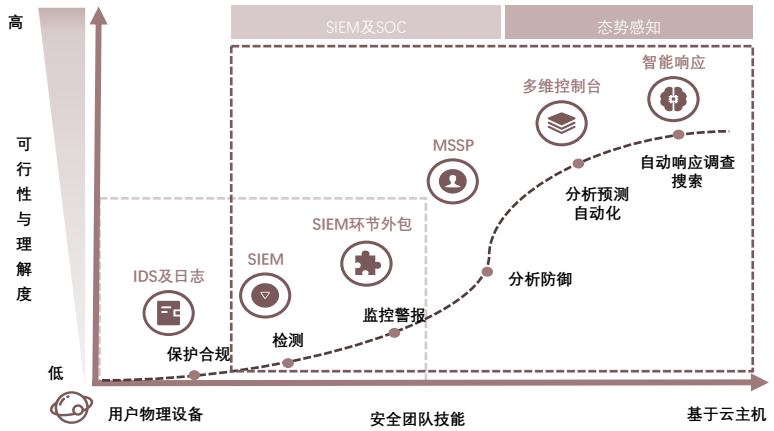
就全球市场竞争格局层面观察，由于海外安全运营及安全托管服务行业起步较早，发展较成熟，全球SOAR行业以海外厂商为主；2019年行业呈现以IBM及Cisco为主导的双龙头格局。就短期言，Cisco Systems整体盈利总额及企业规模均高于IBM。2019年，相较于IBM，CISO System的净收入及企业规模水平分别高出23.8%及10%。但长期来看，IBM于SOAR行业发展前景及竞争潜力较大。首先，IBM SOAR产品Resilient集成化程度较高，产品及解决方案组合较为灵活，可根据应用场景及企业定制化需求与其他IBM产品集成销售，整体利润上升空间较大。其次，在技术维度上，Resilient较强调其内部人工智能技术应用。由于智能化和自动化为SOAR行业必然发展趋势，人工智能技术集成水平决定IBM Resilient在同行业竞品中未来潜在核心技术竞争力。最后，IBM作为云服务商及龙头云MSS厂商，未来云上MSS模式需求释放将有望成为SOAR行业新增长点。

来源：CSDN、HKT官网、 Capgemini、安恒信息、KBY、安全内参、头豹研究院编辑整理

云安全托管服务人工智能技术——深度学习与态势感知

态势感知以全流量分析为核心，集成机器学习等技术，未来有望与深度学习及指示图谱等人工智能及大数据模型集成运用，帮助MSS对网络威胁事件的自动化精准预警及快速响应

网络安全托管发展方向



态势感知为集成检测、预警、响应处置的大数据安全分析平台，以全流量分析为核心

态势感知是一种基于环境的、动态整体的洞悉安全风险的能力，以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析及响应处置能力的一种方式，从而实现大规模网络环境中网络态势发生变化的安全要素进行获取、理解、显示以及最近发展趋势的顺延性预测，进而进行安全的相关决策与行动。在网络安全领域，态势感知为集成检测、预警、响应处置的大数据安全分析平台，以全流量分析为核心，集成威胁情报、UEBA、失陷主机检测、图关联分析、机器学习、大数据关联分析、可视化等技术，对全网流量实现业务可视化、威胁可视化、攻击与可疑流量可视化等。

从技术发展趋势角度分析，态势感知技术有望与深度学习及指示图谱等人工智能及大数据模型集成运用，对网络安全态势变化因素的精准把控，同时从已知威胁推演未知威胁，并对安全威胁事件的预测，从而帮助MSS实现对网络威胁事件的自动化精准预警及快速响应。

在云网络安全托管应用方面，针对SOC及其内部SIEM对网络安全数据缺乏分析、安全事件响应效率较低等问题，态势感知技术的提升网络安全托管服务的SIEM的日志整合分析以及SOC的统一管理能力，同时凭借人工智能、数据挖掘及数据关联等技术实现认知、理解和预测能力自动化，提升MSS运维团队效率。此外，随着云计算基础设施的大量使用，MSSP实现网络安全态势感知系统的基础平台云化，进而使其态势感知能力可以随着保护对象的规模变化而动态变化。

来源：CSDN、HKT官网、 Capgemini、安恒信息、KBY、安全内参、东方证券、头豹研究院编辑整理

方法论

- 头豹研究院布局中国市场，深入研究10大行业，54个垂直行业的市场变化，已经积累了近50万行业研究样本，完成近10,000多个独立的研究咨询项目。

- 研究院依托中国活跃的经济环境，从云安全托管、人工智能等领域着手，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。

- 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。

- 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。

- 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明

- 本报告著作权归头豹所有，未经书面许可，任何机构或个人不得以任何形式翻版、复刻、发表或引用。若征得头豹同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“头豹研究院”，且不得对本报告进行任何有悖原意的引用、删节或修改。

- 本报告分析师具有专业研究能力，保证报告数据均来自合法合规渠道，观点产出及数据分析基于分析师对行业的客观理解，本报告不受任何第三方授意或影响。

- 本报告所涉及的观点或信息仅供参考，不构成任何投资建议。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。在法律许可的情况下，头豹可能会为报告中提及的企业提供或争取提供投融资或咨询等相关服务。本报告所指的公司或投资标的的价值、价格及投资收入可升可跌。

- 本报告的部分信息来源于公开资料，头豹对该等信息的准确性、完整性或可靠性不做任何保证。本文所载的资料、意见及推测仅反映头豹于发布本报告当日的判断，过往报告中的描述不应作为日后的表现依据。在不同时期，头豹可发出与本文所载资料、意见及推测不一致的报告和文章。头豹不保证本报告所含信息保持在最新状态。同时，头豹对本报告所含信息可在不发出通知的情形下做出修改，读者应当自行关注相应的更新或修改。任何机构或个人应对其利用本报告的数据、分析、研究、部分或者全部内容所进行的一切活动负责并承担该等活动所导致的任何损失或伤害。

www.leadleo.com

https://space.bilibili.com/647223552

https://weibo.com/u/7303360042