

2023年中国网络安全运营 市场研究报告

2023-11

数说安全研究院有限公司

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

版权声明

本报告由“数说安全研究院”出品（数说安全隶属于北京赛博英杰科技有限公司），报告版权归北京赛博英杰科技有限公司所有，报告中所有原创文字、观点、图片、表格均受中国知识产权法律法规保护。转载、摘编或利用其他方式使用本报告内容的，应向所有者取得书面授权，并注明“来源：数说安全”。违反上述使用的，我司将追究其法律责任。

免责声明

本报告中部分文字和数据采集于公开信息；市场数据通过CSRadar商业分析平台进行统计分析与模型估算获得；企业数据通过公开信息或访谈获得。数说安全对报告内容的准确性、完整性和可靠性尽最大努力的追求。由于研究方法和数据样本具有一定局限性，故在任何情况下，本报告中的信息或所表达的观点仅供客户作为参考，不构成任何建议。本公司不对报告的数据及分析结论承担法律责任。

- ◆ 在我国网安产业近三十年发展过程中，网络安全法实行超过6年、等级保护制度实行接近20年，这两项网安普适性法律法规已对企业网络安全建设产生重要且实质性的影响。目前看，多数企业已完成合规建设，基础安全体系搭建完成，未来将进入深耕细作、建设与运营并重的新阶段。
- ◆ 数字应用爆炸式增长导致企业安全风险暴露面不断扩大，网络威胁态势日益严峻。安全运营可以帮助企业将安全技术、安全人员与安全管理制度进行高效聚合，实现更为主动、快速、贯穿全局的防御能力。安全运营已成为海内外广泛认可的重要发展方向，未来也将成为绝大多数企业安全能力提升过程中的核心工作。
- ◆ 企业安全运营需求的快速释放也推动了安全运营市场蓬勃发展。安全运营涵盖范围非常广，主要由安全运营产品、安全运营服务和安全运营应用场景构成，不同应用场景所需要的安全运营产品、安全运营服务以及服务的模式可能存在差异。
- ◆ 本次研究主要针对安全运营服务市场，以市场需求最大的网络安全运营作为主要应用场景，非安全运营平台类产品和其它应用场景的安全运营不作为本次研究的主要内容。



目录

01

安全运营概述

02

安全运营技术与产品介绍

03

安全运营服务介绍

04

安全运营市场分析

05

安全运营市场优秀项目案例

06

安全运营市场总结与发展趋势

07

附录-安全运营厂商调研情况

安全运营概述

- ▶ 企业安全管理工作面临的挑战
- ▶ 安全运营的模式（甲方视角）
- ▶ 安全运营的定义
- ▶ 安全运营的价值
- ▶ 安全运营在网络安全体系中的定位与价值
- ▶ 安全运营利好政策
- ▶ 安全运营与安全运维的区别
- ▶ 安全运营法律法规

- ◆ **缺乏安全运营的静态防御模式无法有效应对不断演进的网络安全威胁：**国内大多数企业在构建安全体系时主要以满足合规要求作为第一导向，采购大量安全产品并堆叠部署已成为常态。然而，在这种背景下，各安全产品间常常孤立运转，缺乏有效的协同联动能力，企业整体安全策略与防御姿态长期处于静止和被动的状态，难以有效应对日益复杂和精细化、平台化、自动化的网络攻击，企业迫切需要建立动态、主动的安全运营体系，以达到有效防护的目标。
- ◆ **攻防不对等性导致企业难以实现100%绝对的安全：**攻击者在暗而防守者在明，防守方需要耗费大量资源部署长长的防线来保护庞大的网络资产，攻击者只要在100次攻击中成功1次，就可以抵消防守方在99次成功防守中所付出的努力。因此，企业在构建安全防线时，盲目的建设防线并不是最优的选择，更好的办法是在安全运营过程中时刻感知威胁与风险，采用更具针对性、动态的安全策略，并不断加强防御系统的韧性，保证即便发生攻击或系统被攻破，也能够及时发现、阻断攻击并快速恢复业务。
- ◆ **企业在网络安全投入上面临预算压力和资源限制：**对于一些企业来说，很难衡量网络安全投资的回报率（ROI），这导致它们在网络安全方面只拥有有限的预算和资源，同时也可能限制其采购和实施最新的安全技术和措施。因此，企业需要找到一种平衡，通过建立高效的安全运营体系，帮助企业最大程度提高系统的安全性，同时实现在有限资源下进行有效管理。

中国网络安全审查技术与认证中心（CCRC） 安全运维服务资质简介

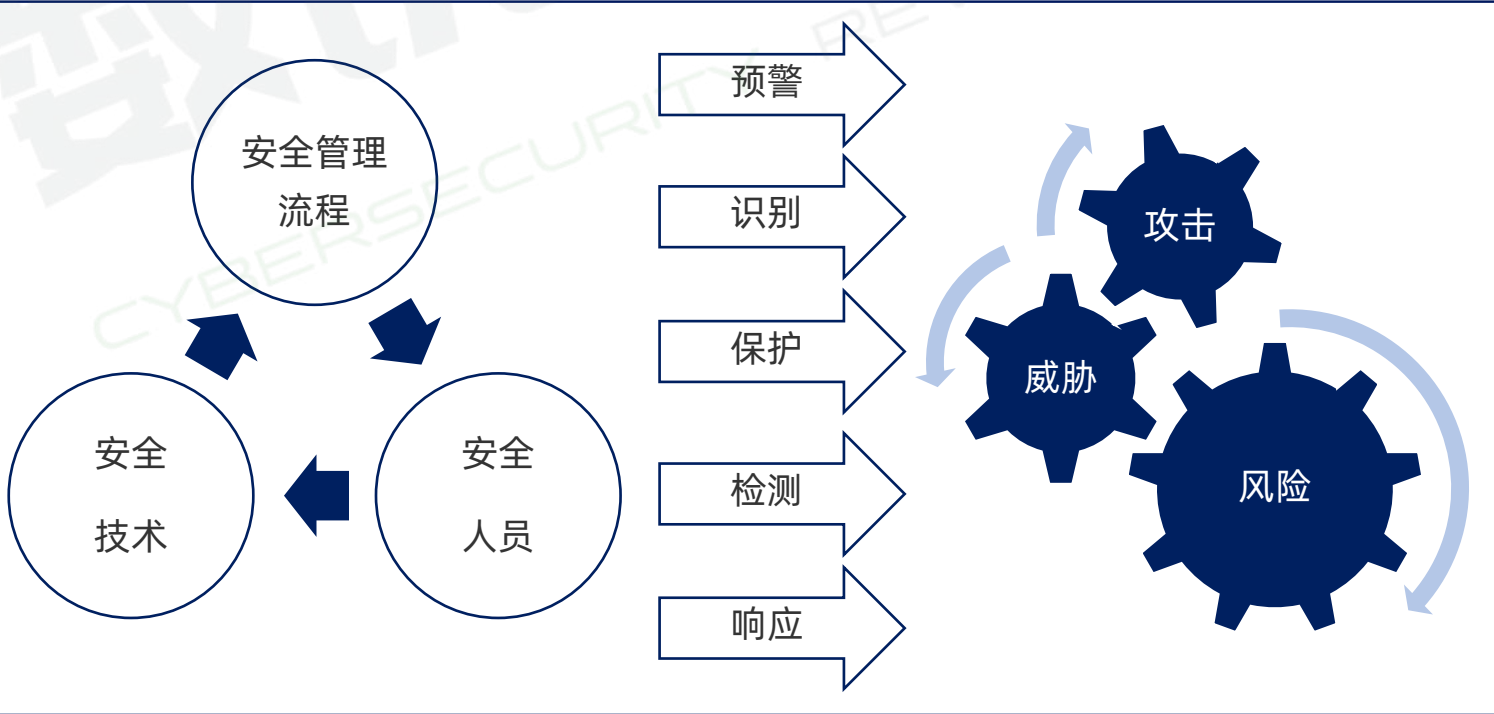
通过技术设施安全评估，技术设施安全加固，安全漏洞补丁通告、安全事件响应以及信息安全运维咨询，协助组织的信息系统管理人员进行信息系统的安全运维工作，以发现并修复信息系统中所存在的安全隐患，降低安全隐患被非法利用的可能性，并在安全隐患被利用后及时加以响应。

中国信息安全测评中心（CNITSEC） 安全运营服务资质（安全运营过程能力要求）

安全意识和安全技能培训；资产识别和管理；脆弱性识别和管理；应急响应及处理能力；深度威胁检测、研判和管理；安全事件预警与取证分析；风险评估的能力；内部审计和威胁情报处置；态势感知和趋势分析；维护安全运营中心（SOC）工具生命周期；安全性协调的能力；检验并证实整体安全性。

数说安全对安全运营的定义

结合行业主管部门对安全运维的定义和安全运营能力过程要求，数说安全对安全运营定义如下：
安全运营是通过统一和协调组织内安全人员、安全技术和安全管理流程，对组织面临的安全风险进行预警、识别、保护、检测、响应的过程。安全运营的目标是发现组织已存在或未来可能会出现的安全风险，并利用高效的安全防控措施来主动化解风险，以此不断改善组织的安全状况。







完全自建模式

- ◆ 组织具有成熟的安全体系，安全管理流程、安全人员、安全技术均由组织自建自筹；
- ◆ 组织CSO（首席安全官）对本组织的安全运营情况和效果负责；
- ◆ 组织具备充足的安全预算，已建成体系化的安全架构，拥有专业的安全运营团队，安全运营是保障组织业务发展的重要因素。
- ◆ 目前在市场中，采用完全自建模式的客户比例不超过3%。

产品体系自建+采购驻场运维服务模式

- ◆ 组织通过安全集成的方式购买安全产品并建立安全防护体系，但组织内安全人员有限，需要以人力外包的方式补充安全运营人员；
- ◆ 组织CSO（首席安全官）对本组织的安全运营情况和效果负责；
- ◆ 组织安全预算相对充足，但预算优先投入安全技术体系建设，拥有相对成熟的安全管理流程，但受限于组织体制、技术能力与人员编制控制等原因，无法自建完整的安全运营团队。

安全托管模式（MSS）

- ◆ 组织建立了安全防护体系，但没有独立的安全运营团队，也不具备安全运营能力，需要将安全运营工作委托给外部专业的安全公司；
- ◆ 受委托的安全公司针对组织面临的安全需求，制定组织安全管理流程、配备安全运营人员、提供安全运营工具，以云端/远程的交付方式实现对组织安全运营工作的全面托管，并对最终的效果负责；
- ◆ 组织安全预算有限，短期内不具备自筹自建安全运营体系的能力。

托管检测与响应模式（MDR）

- ◆ 除基础安全运营工作外，组织更关注自身面临的网络攻击与威胁，但组织不具备相应的技术能力，需要将威胁检测、威胁分析、威胁响应等工作委托给外部专业的安全公司；
- ◆ 受委托的安全公司为组织提供面向威胁视角的托管式安全服务，包括部署威胁检测探针、威胁分析和响应平台等基础设施，并在云端配备安全专家，为组织提供7*24小时的威胁检测与响应服务。

安全管理指标化

成熟的安全运营将打破传统网络安全管理的模式，在管理制度和管理流程基础上，进一步采用科学的数字化管理指标，通过风险平均检测时间（MTTD）、平均确认时间（MTTA）、平均遏制时间（MTTC）、平均恢复时间（MTTR）等多项指标量化安全运营过程和结果，从而达成更精细、可度量的安全管理能力。

安全能力实战化

安全运营通过威胁情报预测、主动监控、安全测试等多样化手段，提前发现企业可能面临的安全风险和威胁，自适应调整对抗策略，降低企业发生网络安全风险的可能性。同时，在风险发生时，安全运营可以实现快速的风险定位，通过体系化的安全运营流程来化解风险，在减少企业损失的同时不断强化实战能力。

安全成本最小化

国内以合规为导向的市场供需关系导致企业购买了很多安全产品，但并未通过技术有机结合形成有效的体系化能力，安全运营可以在弥补企业管理能力与技术能力的同时，合理规划安全需求与安全投入，实现物尽其用，减少冗余和重复性投资，以此降低企业整体的安全成本。

安全价值最大化

企业安全投入与产出不匹配是我国网安产业一直以来面临的突出矛盾，其主要原因在于长期形成的堆叠式安全体系，在没有良好的管理和运营的情况下，无法带来令人满意的安全价值。2016年开始的实网攻防，其目的也是解决让企业看到安全价值的问题，安全运营未来将进一步加速这个价值平衡的过程。

《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》 十三届人大四次会议 2021.3

- ◆ 第十八章第三节：加强网络安全保护，健全国家网络安全法律法规和制度标准，加强重要领域数据资源、重要网络和信息系统安全保障。建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。加强网络安全风险评估和审查。加强网络安全基础设施建设，**强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力**。加强网络安全关键技术研发，加快人工智能安全技术创新，提升网络安全产业综合竞争力。加强网络安全宣传教育和人才培养。

《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》 工信部 2021.7

- ◆ 第4条 创新安全服务模式
 - ◆ 加强安全技术产品的云化能力，推动云化安全产品应用，鼓励综合实力强的安全企业发展弹性、灵活的云模式网络安全服务。
 - ◆ **发展集约化安全服务，鼓励企业提供集防火墙、用户身份认证、数据安全、应用安全等一揽子整体解决方案。支持开展威胁管理、检测响应等安全托管和咨询服务。发展地区级、城市级、行业级安全运营服务，提高运营自动化、流程化、工具化水平。**
 - ◆ 鼓励基础电信企业、大型云服务提供商，并充分发挥网络和基础资源优势，输出安全服务能力，同时升级改造基础设施，支持安全企业嵌入安全服务能力。
- ◆ 第9条 推动关键行业基础设施强化网络安全建设
 - ◆ 推动能源、金融、交通、水利、卫生医疗、教育等行业领域加强资产识别、设备防护、边界防护、身份认证、数据安全、应用安全等技术手段建设，提升重要系统、关键节点及数据的安全防护能力。
 - ◆ **支持建立态势感知、通报预警、应急响应、安全运营等安全机制及纵深防护体系，不断提高风险防范和应急处置能力。**
 - ◆ 推进零信任、人工智能等技术应用，提升防护体系效能。
- ◆ 第10条 推进中小企业加强网络安全能力建设
 - ◆ **实施中小企业“安全上云”专项行动，建设网络安全运营服务中心，面向中小企业提供高质量、低成本、集约化的网络安全产品和服务。**
 - ◆ 引导中小企业通过网络安全产品服务一站式购买、租赁、订阅、托管、云端交付等方式，灵活部署网络安全产品和解决方案。支持开展多元化网络安全意识宣贯和技能培训，不断提升中小企业网络安全防护意识和能力。

中华人民共和国网络安全法（2017.6.1实施）

- ◆ 第二十五条：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。
- ◆ 第五十一条：国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。
- ◆ 第五十二条：负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

中华人民共和国数据安全法（2021.9.1实施）

- ◆ 第二十二条：国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。
- ◆ 第二十九条：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

关键信息基础设施安全保护条例（2021.9.1实施）

- ◆ 第二十四条：保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

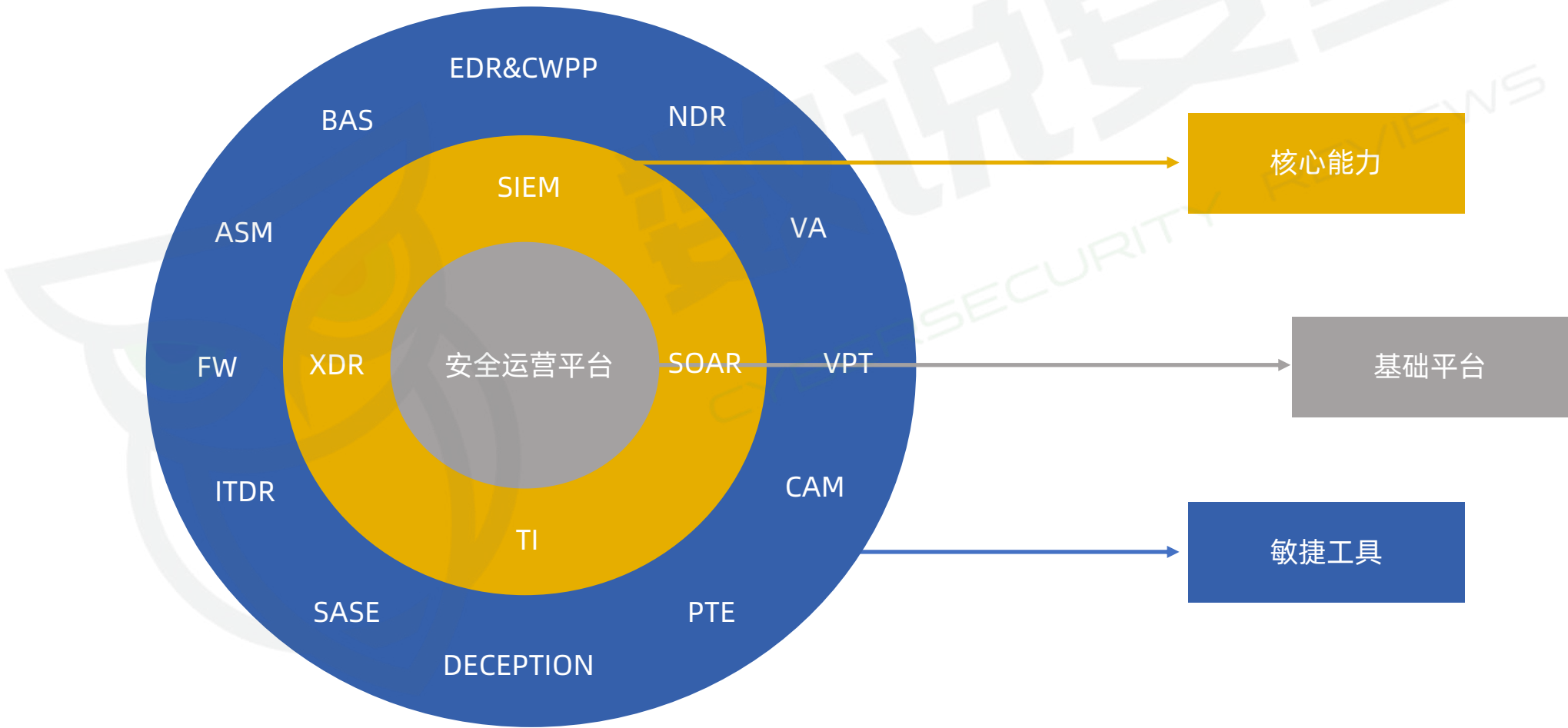
安全运营技术与产品介绍

- ▶ 安全运营方法论
- ▶ 安全运营关键技术-终端检测与响应（EDR&CWPP）
- ▶ 安全运营技术栈
- ▶ 安全运营关键技术-网络检测与响应（NDR）
- ▶ 安全运营核心能力-安全信息和事件管理（SIEM）
- ▶ 安全运营核心技术-入侵与攻击模拟（BAS）
- ▶ 安全运营核心能力-安全编排自动化与响应（SOAR）
- ▶ 安全运营核心技术-攻击面管理（ASM）
- ▶ 安全运营核心能力-扩展检测与响应（XDR）
- ▶ 安全运营核心技术-欺骗防御（DECEPTION）
- ▶ 安全运营核心能力-威胁情报（TI）

企业安全运营围绕以识别、保护、检测、响应、恢复为主要能力的安全体系框架，在原有纵深+静态防御基础上，可以通过扩展和强化识别、检测、响应3个维度的能力，向主动式、动态式防御效果进化。同时利用成熟、多样化的安全运营工具可以保障企业安全运营体系的高效运行，提升企业应对风险的能力，保证企业安全防护体系始终处于全局可视、自主可控、高弹性、自适应的积极对抗姿态。

企业安全框架	安全运营过程与目标			安全运营工具
识别	资产梳理	资产识别	通过工具/产品/技术识别组织内外部所有的IT资产	CAM
	脆弱性评估	漏洞评估	发现组织已存在的安全漏洞并根据优先级进行修复	VA、VPT
		风险评估	立足攻击者视角发现组织存在的安全风险，并评估风险优先级	ASM、PTE、渗透测试
保护	纵深防御		在识别企业所有风险因素后，在安全基础设施上设置对抗策略	FW、WAF、IPS、NAC
检测	威胁管理	威胁检测	在终端、网络、身份基础设施中采集信息以发现攻击	EDR、CWPP、NDR、ITDR
		威胁狩猎	通过伪造脆弱性、增加IT设施密度来发现和延缓攻击	DECEPTION
	安全检测	安全有效性验证	通过自动化方式对组织安全体系的有效性进行持续验证	BAS
	风险研判	威胁预警	通过接入实时的威胁情报数据，实现安全风险的感知和预警	TI
		态势感知	对全局安全态势进行动态、全面研判，为管理决策提供依据	态势感知/SOC/XDR/SIEM
响应	风险处置	风险缓解	攻击发生后通过协同联动安全基础设施来遏制攻击，处置威胁	SOAR
		溯源取证	通过还原攻击手法与攻击路径，找到攻击源头彻底排除隐患	溯源工具/全流量存储/人工
恢复	备份容灾恢复		系统被攻破后，通过多种技术手段恢复业务，保证业务连续性	数据容灾/备份/一体机/人工

网络安全技术的有效运用是提升企业安全运营效率、保障企业安全运营效果的核心手段。在安全运营技术栈中，安全运营平台是必不可少的基础性平台，除了承载企业安全运营管理的自动化流程，也是构建SIEM、XDR、SOAR、TI这4项安全运营核心能力的底座平台。SIEM是传统的安全信息和事件分析技术，XDR是更为先进的威胁检测技术，SOAR在安全运营事件的响应处置中不可或缺，TI是常态化安全运营状态下最重要的数据支撑。在构建基础平台与核心能力后，企业可以根据不同的安全需求，有选择性的使用十余种敏捷工具，来不断细化、落实安全运营工作，实现更自动化、智能化的安全运营体系。



安全信息和事件管理（ Security Information Event Management ）

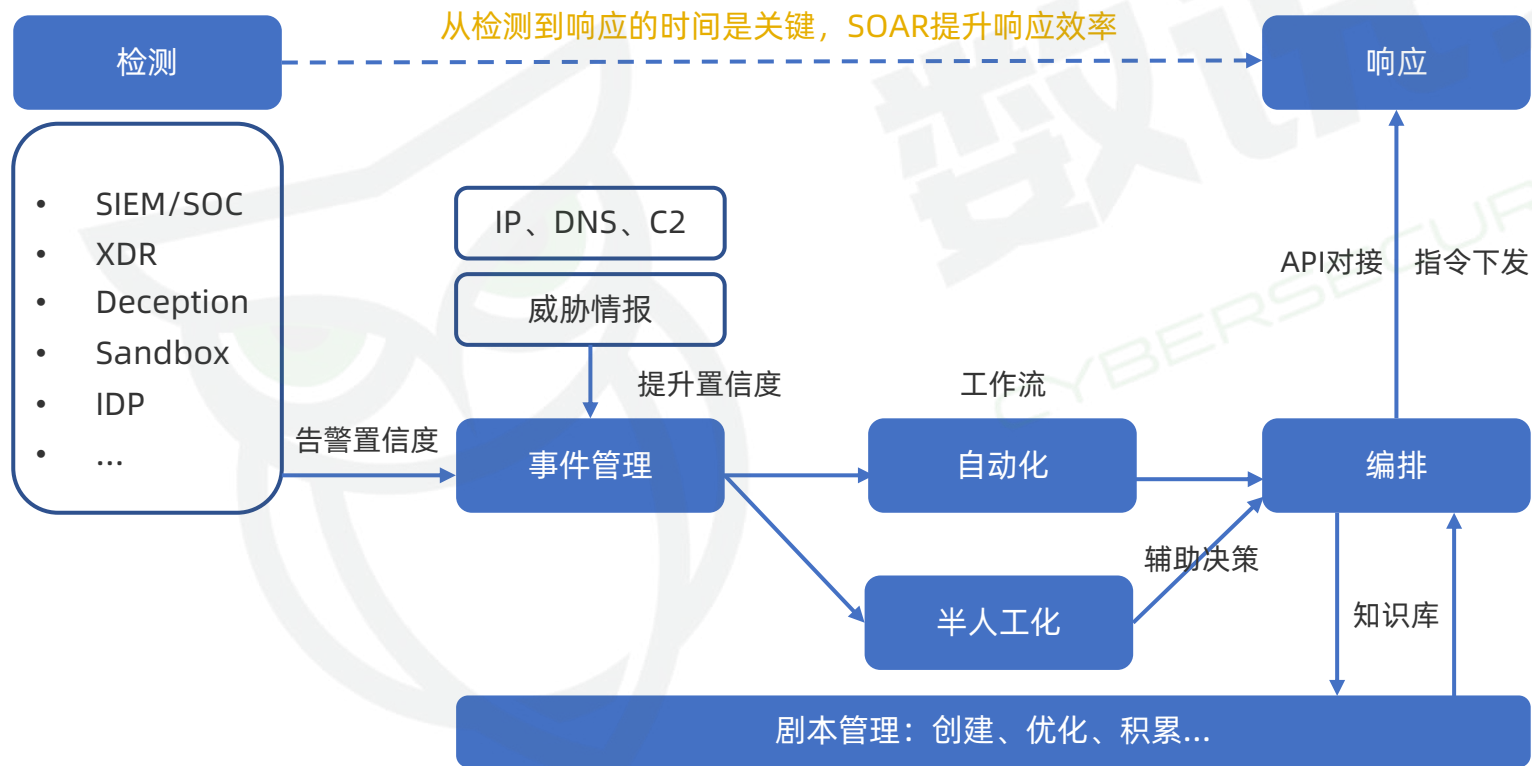
- ◆ 最初的SIEM平台是日志管理工具，结合了安全信息管理和安全事件管理，能够实时监控和分析安全相关事件，以及跟踪和记录安全数据以进行合规或审计。近些年SIEM不断发展，融合了用户和实体行为分析（UEBA）以及其他高级安全分析、人工智能和机器学习能力，用于识别异常行为和高级威胁。如今SIEM已成为现代安全运营中心中安全数据监控与处理的中枢，帮助企业实现更全面、精准的事件分析与管理能力。
- ◆ SIEM从本地和云环境中，采集包括用户、终端、网络、应用程序、云工作负载等多类IT和安全基础设施的数据，通过对这些多源数据进行聚合、富化、关联和建模，实现对威胁的调查，并生成准确的安全事件，为企业在安全数据层面提供整体安全视图和决策支撑。SIEM是企业构建安全运营体系最核心的底层能力。



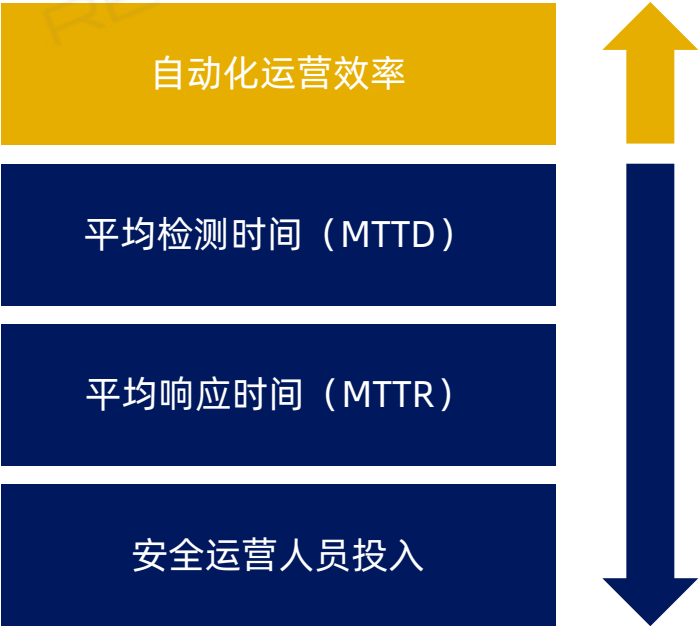
SIEM产品逻辑图

安全编排自动化与响应（ Security Orchestration Automation and Response）

- ◆ 随着移动办公、5G和物联网技术的发展，海量终端设备接入到网络，攻击面不断被拓宽，攻击事件呈现指数增长态势，使得安全运营团队承受着极大的压力。借助于SOAR产品，可以根据安全事件的分类/评估结果，关联不同类型的处理脚本，进行自动化的事件响应，帮助安全运营团队的工作效率实现指数级提升，有效应对不断攀升的漏洞和安全告警。
- ◆ 在安全运营场景下，SOAR是最重要的核心技术之一，通过接收高置信度的分析结果，SOAR可以将人工处理过程转化为自动化的剧本/工作流，大幅缩短从发现威胁到处置威胁的时间。



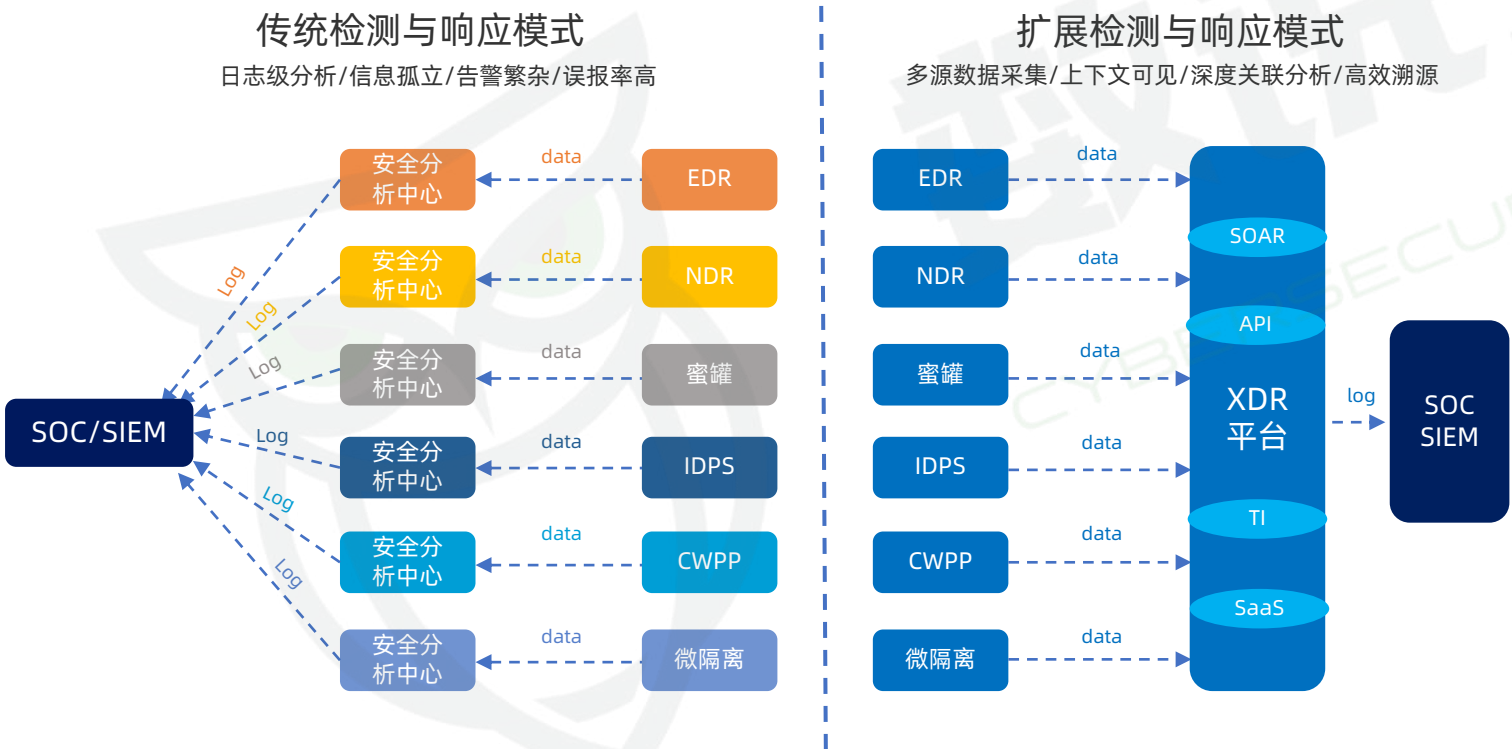
SOAR workflow 概况



SOAR应用价值

扩展检测与响应（eXtended Detection and Response）

- ◆ XDR平台可以跨区域收集来自多种安全设施的检测数据，并对其进行统一的集成、关联和上下文等事件化分析，以全局视角进行威胁研判，从而获得更准确和全面的检测结果。XDR旨在高效集成产品，打破信息孤岛，降低企业内的无效告警和安全运营成本。
- ◆ 在合规背景下，企业安全体系普遍存在产品碎片化、告警信息繁杂、事件响应流程混乱、人员能力不足等深层问题。如何通过安全运营体系一体化整合来提高安全运营效率，成为目前亟待解决的核心问题，XDR或在此方面形成技术突破，并对多场景常态化安全运营工作提供最直接的安全价值。



扩展检测与响应模式与传统检测响应模式的区别

传统检测与响应模式的局限性

- ◆ 各产品信息孤立，缺少关联分析，难以发现APT等高级威胁；
- ◆ 各检测点产生大量告警信息，安全运营工作效率低、负担重；
- ◆ 各品牌和各类型产品独立配置和维护，管理成本高。

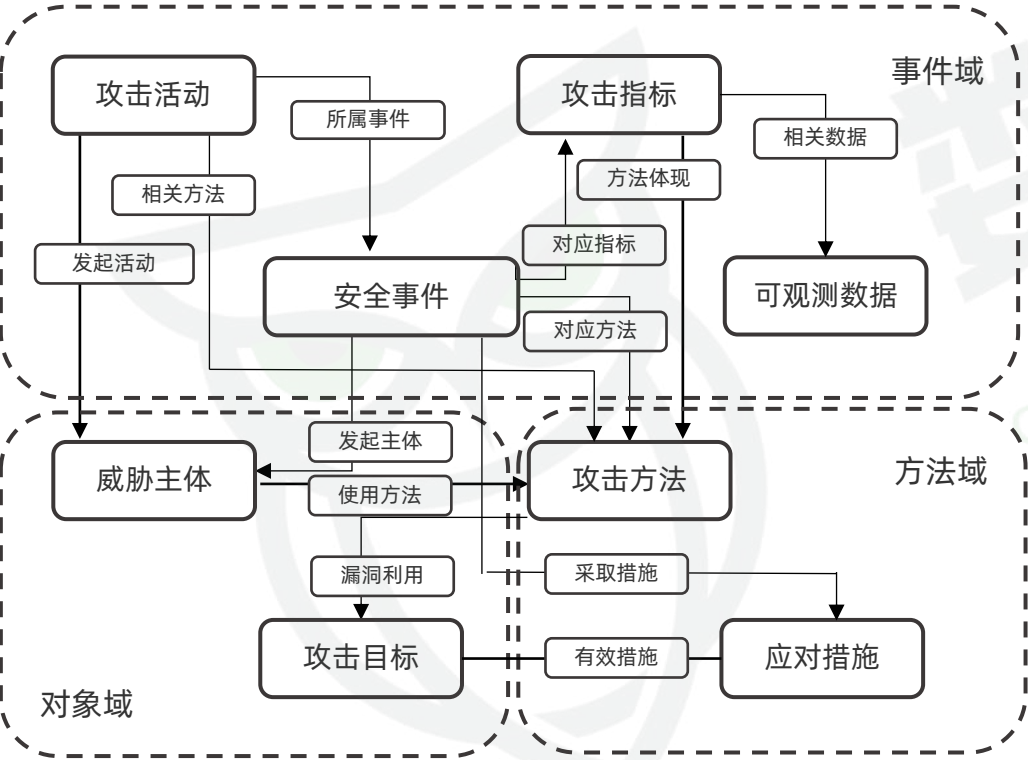
VS

扩展检测与响应模式的先进性

- ◆ 产品同品牌，各产品信息互通可读，由XDR平台统一分析；
- ◆ 摒弃繁杂的告警信息，而是精准少量的安全事件，效率提升；
- ◆ XDR平台可整合TI、SOAR等能力，并支持SaaS运营模式。

威胁情报（Threat Intelligence）

- ◆ 威胁情报是基于威胁知识、证据、技能和经验的信息集合，可以对已存在和正在出现的威胁和风险提供上下文、机制、可能产生的结果和应对意见等信息。这些信息可被用于及时响应和优化风险应对的决策。威胁情报可以帮助企业更好地洞察威胁形势和攻击行为，以及攻击者最新的策略、技术和程序，为企业提供决策依据和先发优势。通过广覆盖和高时效的威胁情报，企业可以主动、快速调整其安全防御策略，从而识别和抵御高级攻击、0 Day等安全风险。
- ◆ 在滑动标尺模型中，威胁情报定位于态势感知和积极防御之上，是填补已知威胁知识缺口并驱动积极防御的过程。威胁情报的posture，是覆盖面、时效性和可执行水平。

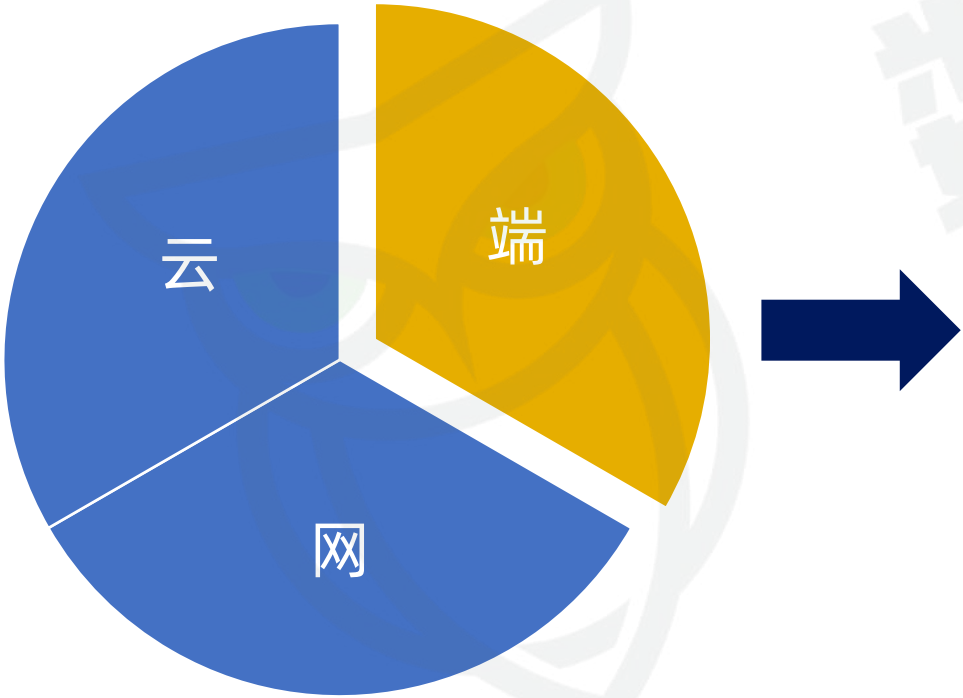


可观测数据			攻击指标		
DNS	邮件	文件	观测数据	攻击方法	攻击阶段
进程	网络访问	注册表	检测机制	潜在影响	应对措施
安全事件			攻击活动		
关系者	影响资产	影响评估	安全事件	威胁主体	攻击方法
预期效果	获取权限	发现方法	攻击活动	可信度	相关活动
攻击方法			应对措施		
攻击行为	攻击资源	攻击目标	阶段	类型	对象
攻击阶段	信息来源	攻击链	影响	成本	效果
威胁主体			攻击目标		
身份	动机	经验	漏洞列表	弱点类型	应对措施
预期效果	计划支持	可信度	信息来源	攻击目标	版本

网络安全威胁信息格式规范国家标准

终端检测与响应（Endpoint Detection Response & Cloud Workload Protection Platform）

- ◆ 终端检测与响应技术在IT端点部署轻量级代理采集终端信息并上传中心数据分析平台，通过大数据、机器学习、威胁情报、UEBA等新技术实现对终端安全态势的研判分析，是针对日渐多变的高级持续性威胁、0 Day等新兴未知攻击的主动性防御机制。
- ◆ 终端检测与响应技术在网络安全运营中同样扮演着关键的角色，其重要性和价值包括：实时监测终端上的活动，在快速检测和识别潜在威胁的同时可以将监控数据同步给安全运营中心，通过在终端采集的详细事件日志和活动记录，安全运营团队可以对安全事件做进一步根因分析。除此外，通过与SOAR、威胁情报等能力整合，终端检测与响应技术可以实现对终端风险的实时预警和快速处置。



面向PC终端（EDR）

- 办公操作系统
- 实时在线监控
- 恶意软件防护
- 威胁检测分析
- 用户行为分析
- 自动响应处置
- 加密流量识别
- 漏洞识别管理
- 威胁情报集成
- 事件调查取证

面向服务器终端（CWPP）

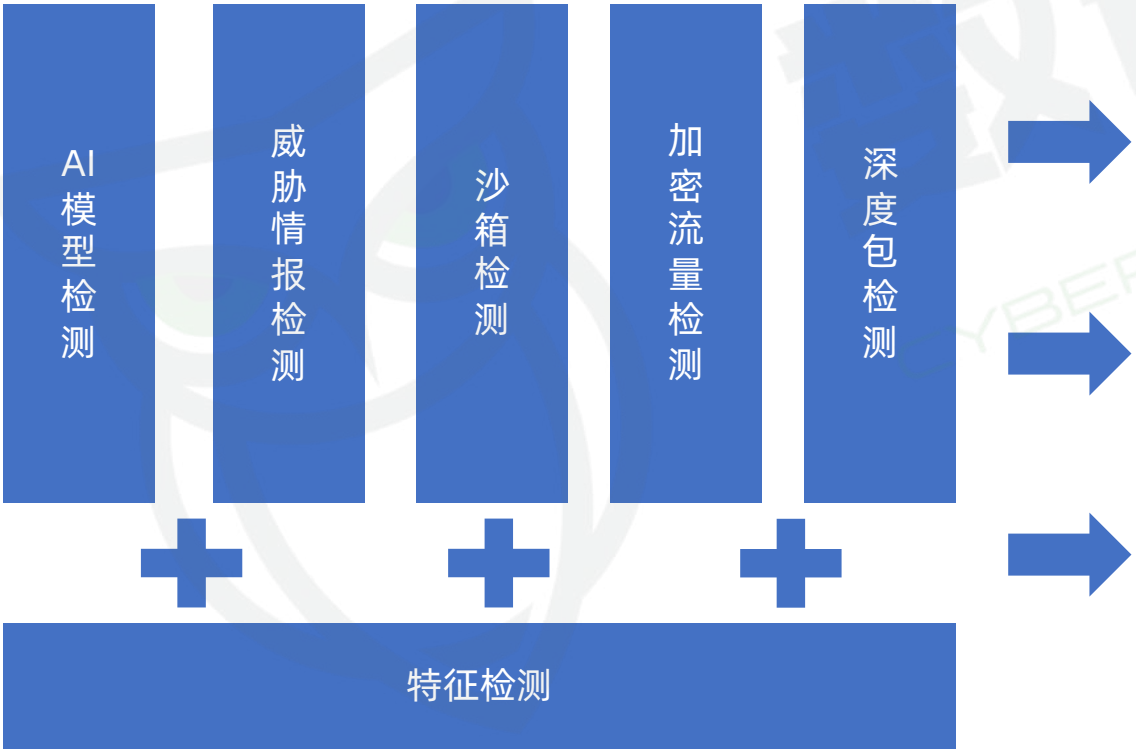
- 虚拟机/容器/无服务
- 自动资产识别
- 漏洞风险管理
- 微隔离/vFW
- 服务器加固
- 应用控制白名单
- 身份访问管理
- 系统完整性监测
- 主机入侵检测
- 恶意软件防护

终端检测与响应技术与在安全运营体系中的价值

网络检测与响应（ Network Detection and Response）

- ◆ 网络检测与响应NDR技术是在传统特征检测基础上，利用AI、ML、大数据等核心功能对网络流量进行建模和深度学习分析的过程，对识别到的异常行为进行流量还原、关联分析，并结合威胁情报来定位未知威胁，在网络层面实现对内网安全风险的实时监控，最终为安全运营处置提供信息支撑。
- ◆ 网络检测与响应与终端检测与响应技术的协同，可以大幅提升企业在安全运营工作中对未知威胁的识别与防御能力，也是未来支撑SOC、SIEM、SOAR等系统高效应用的重要前提。目前在企业安全运营体系构建中，已经有越来越多的客户使用NDR作为网络流量采集和检测的主要产品。

NDR产品主要技术路线



NDR在安全运营体系中的价值



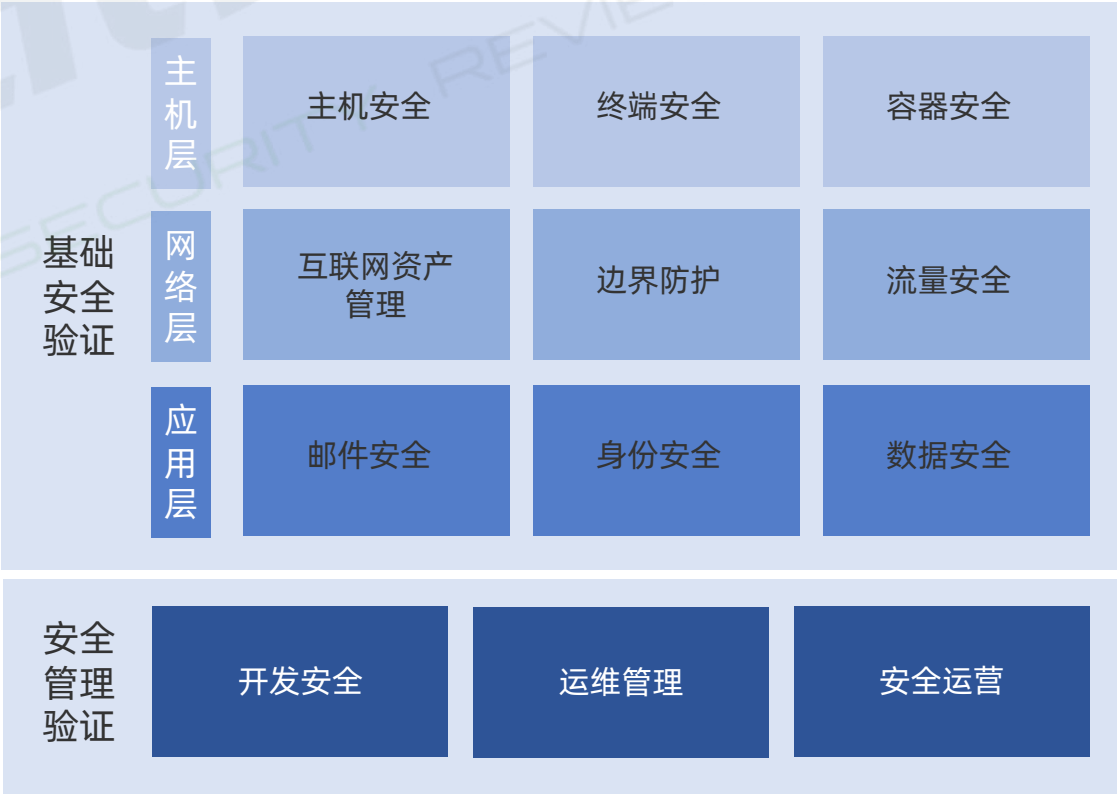
入侵与攻击模拟（Breach and Attack Simulation）

- ◆ 企业购买防火墙、防病毒软件、IDS、WAF、蜜罐等大量安全产品，设计严密的网络安全架构，但整套体系和设备是否如用户预期运行？如果网络攻击下一刻到来，管理者是否能看得见、防得住、抓的着？目前还没有一项完美的技术可以解决这些问题，但至少入侵与攻击模拟迈出了第一步。
- ◆ BAS通过主动验证+（半）自动化的方式，利用攻击者的战术、技术和程序来模拟杀伤链的不同阶段，持续测试和验证现有网络整体的安全机制（包括各安全节点是否正常工作、安全策略与配置的有效性、检测/防护手段是否按预期运行等），对企业对抗外部威胁的能力进行量化评估，并强化实战能力，最终实现安全运营工作降本增效。

BAS对日常安全运营常见问题进行自动化检测

安全产品	常见问题	归因分析
防火墙	安全策略异常	对重要系统设置权限过大的访问控制策略
NDR	告警延迟达30分钟	自身流量解析能力不足导致告警延迟
	不响应/无日志	产品无法达到宣称的性能，检测失效
	面对互联网攻击无告警	只接入电信运营商流量，漏接联通和移动
WAF/IPS	边界防护未覆盖资产	没有配置应该监测保护的资产
	边界防护策略不同步	同步策略未生效，防护失效
IDS	无任何告警或日志	策略配置后未生效，产品形同虚设
HIDS	日志异常	日志消息队列异常导致日志无法外传
	Webshell上传检测失效	Webshell检测告警失效
	反弹shell检测失效	反弹shell检测服务异常
蜜罐	蜜罐失效	大量节点蜜罐装置未正常工作
SOC	SOC告警日志丢失	日志漏包率达1%，远高于万分之一的预估

BAS安全有效性验证维度



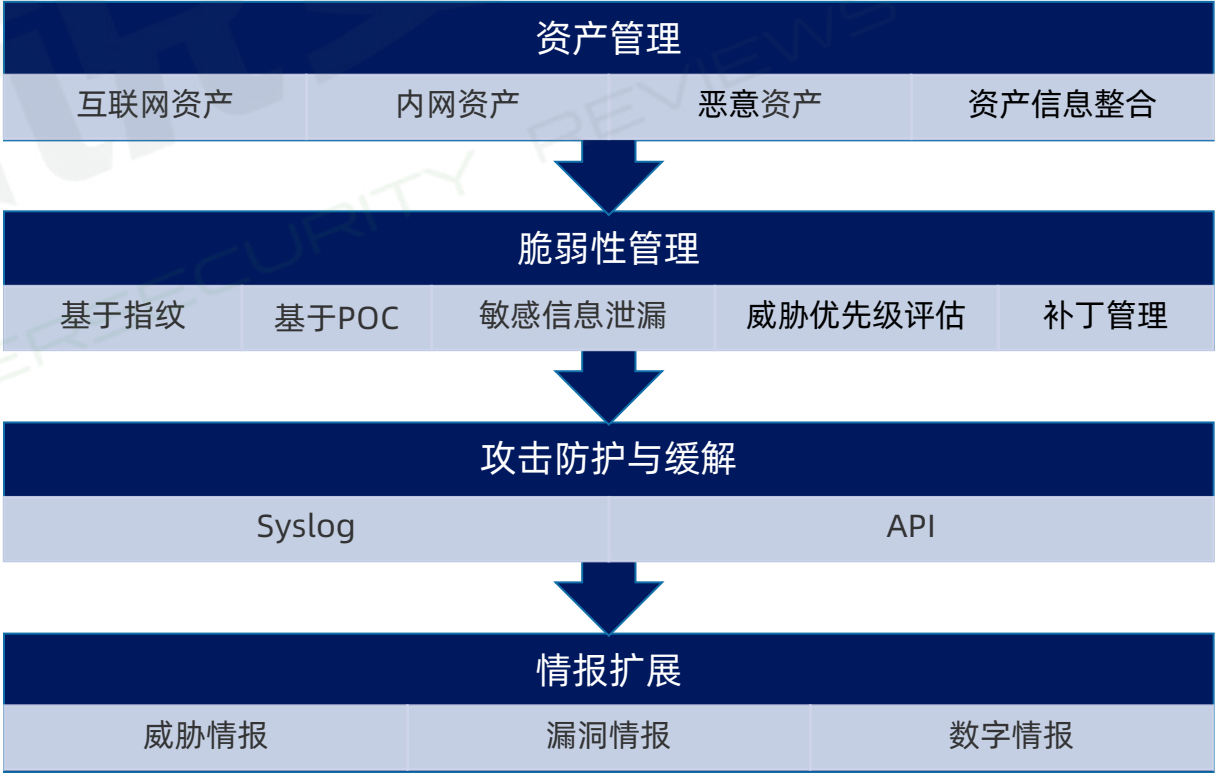
攻击面管理（Attack Surface Management）

- ◆ 攻击面是指企业所有可被利用的风险因素的集合，这些风险因素大多分布在物理面（例如端点、网络、服务器等设备漏洞）和数字面（例如企业数据泄漏、品牌侵权、个人隐私信息泄漏、网络钓鱼等）。攻击面管理旨在识别、分类这些风险因素，并对其进行优先级排序和持续监控。
- ◆ 攻击面管理是持续发现、分析、监控和评估内部和外部资产以发现潜在暴露面、攻击向量和风险，并进行优先排序、响应处置的过程。因为攻击面范围较为宽泛，按照企业管理者和外部攻击者两个不同视角，可分为网络资产攻击面管理（CAASM）和外部攻击面管理（EASM）两种。



攻击面=可被攻击利用的暴露面
可被攻击利用=可利用的机会 x 攻击能力

企业攻击面的定义
来源：未岚科技

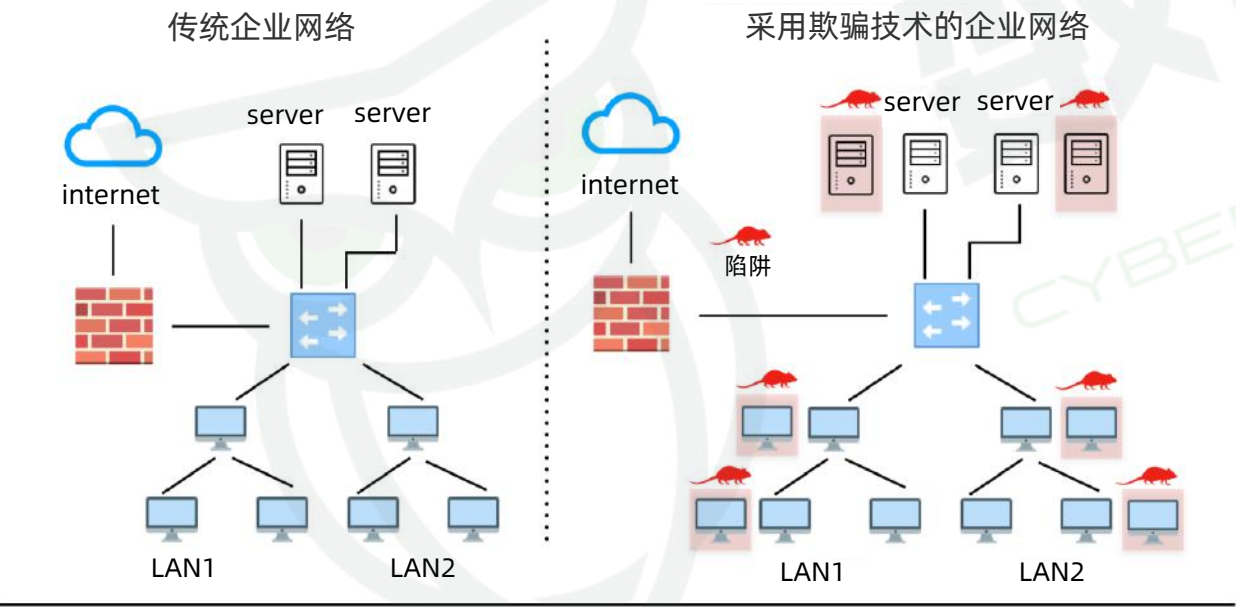


攻击面管理核心能力

欺骗防御（DECEPTION）

- ◆ 欺骗技术面向企业网络及横向移动下的威胁检测场景，通过对企业网络结构、操作系统、应用系统、文件、容器、微服务、甚至是IoT设备的高度仿真来增加企业IT设施的密度，最大限度增加被攻击者触碰的机会来诱导攻击者主动现身并陷入圈套，欺骗系统发出的告警信息，其置信度通常较高，是有别于传统检测手段、可以大幅提升企业安全检测能力的高级检测技术。
- ◆ 欺骗技术在安全运营中的主要价值包括误导并诱捕攻击者、攻击分析与研究、威胁情报生成、攻击溯源取证等，是高级别安全运营场景的重要技术。

必须监控来自欺骗工具的警报！



欺骗防御示意图

常态化内网安全监测

非传统IT环境下安全监测，如：IoT设备、医疗环境

终端无法部署检测探针，EDR或主机IDS无法使用

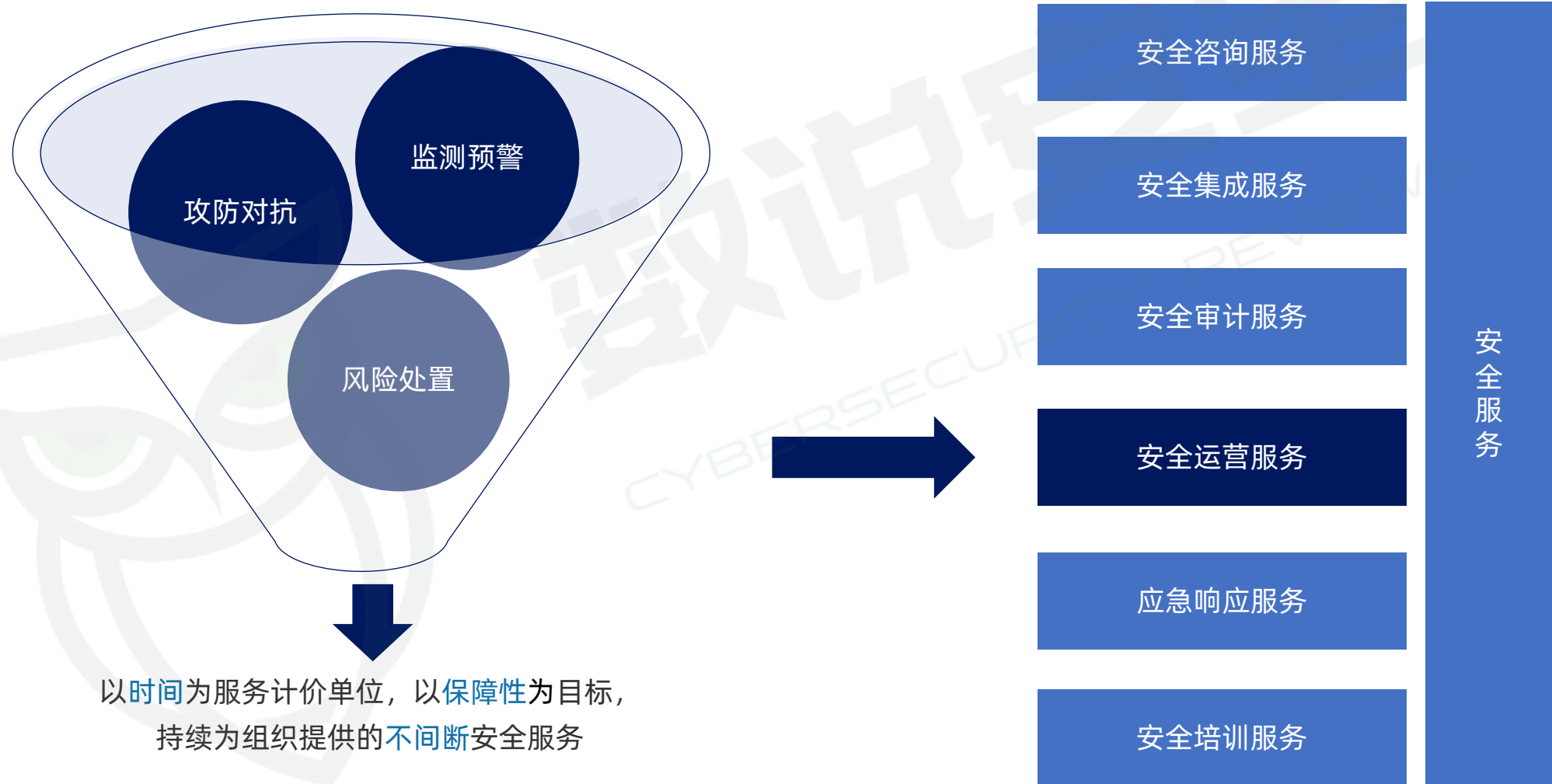
网络流量加密、传统检测手段失效

海量告警、管理成本较高、亟待降噪的分布式网络

欺骗防御在安全运营下的应用场景

安全运营服务介绍

- ▶ 安全运营服务与安全服务的关系
- ▶ 安全运营服务的主要模式（乙方视角）
- ▶ 安全运营服务商类型
- ▶ 安全运营服务的主要内容
- ▶ 安全运营服务-安全运维服务
- ▶ 安全运营服务-安全托管服务（MSS）
- ▶ 安全运营服务-托管检测与响应服务（MDR）
- ▶ 安全托管服务的主要模式
- ▶ 安全托管服务市场客户的特点
- ▶ 安全托管服务应用场景-城市级安全运营
- ▶ 安全托管服务应用场景-行业级安全运营



对比项	驻场运维服务	安全托管服务（MSS）	托管检测与响应服务（MDR）
服务地点	用户现场	非用户现场	
客户服务模式	1对1	1对多	
服务平台	无/甲方提供/乙方提供	乙方提供	
服务工具	以甲方现有产品为主	乙方工具+甲方现有产品	
服务交付方式	现场交付	远程交付	
服务交付物	人工报告	自动化周期性报告	
服务时效	5*8	7*24*365	
服务目标	保障企业网络安全基础设施稳定运行	通过化解网络安全风险来保障企业数字化业务稳定运行	攻击威胁检测与响应处置
服务客户类型	合规驱动	合规+技术驱动	监管+实战驱动

电信运营商/ 互联网厂商

主要面向使用自身“云”“网”服务的中小企业客户，在较强的网络资源、数据资源和算力资源基础上，通过生态合作、产品集成、自主研发等方式补充安全能力，形成“云网安”一体化服务能力，为中小企业提供轻量级的增值安全运营服务，在客户数量上远超其它类型的服务商。

网络安全厂商

在网安厂商中主要包含两类：第一类是具有成熟安全产品和安全服务能力的综合型安全厂商，针对不同的应用场景和用户需求，可以提供多样化的安全运营服务模式；第二类是以自研SOC/SIEM/XDR等平台为主的产品型厂商，在技术创新性、场景适应性、产品易用性等多方面具备优势，可以为市场主要的安全运营服务商提供能力支撑。

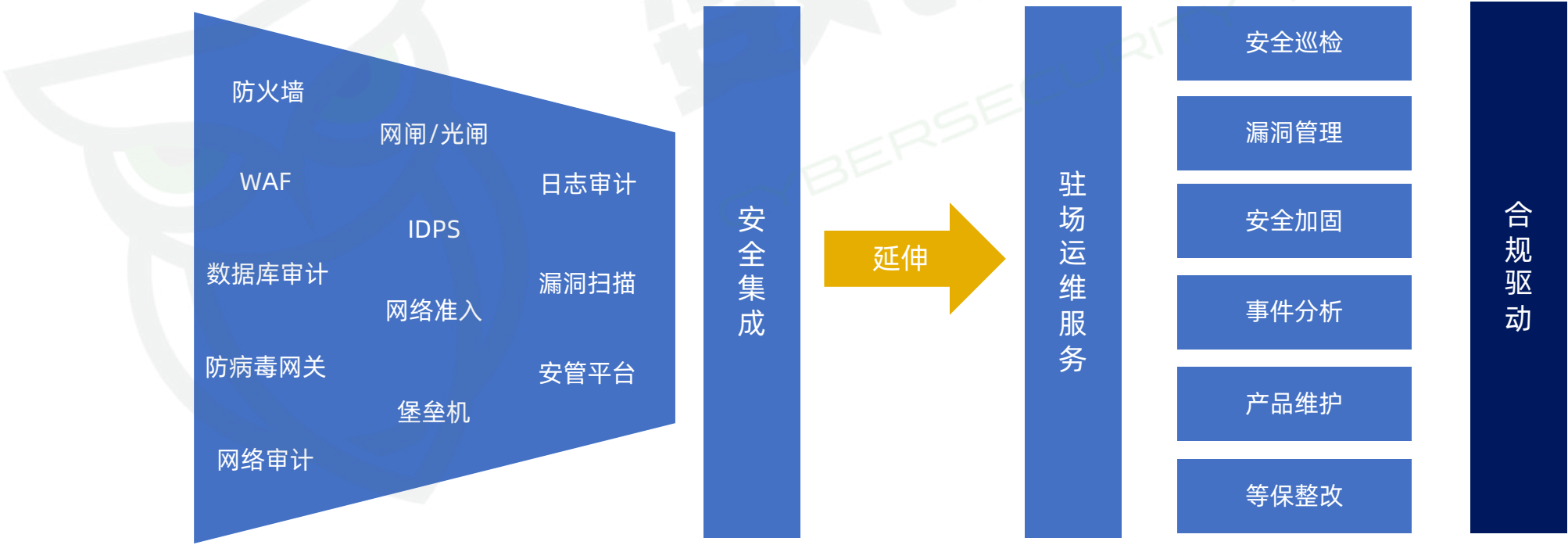
系统集成商/ 安全服务商

具备较强的一线经验，服务专业化水平高，保障用户最后一公里安全。在熟悉用户IT架构、业务流程、管理制度等情况下，可以近距离对用户的IT、网络、安全提供全方位服务，达成更好的服务效果和满意度。在安全运营服务市场供需关系中，系统集成商和安全服务商是重要的角色之一，同时也是MSS安全托管服务商主要的合作伙伴。

- ◆ 安全运营服务是以时间为服务计价单位，为企业持续提供保障性安全服务的过程。下面列举了国内安全运营类招标项目中最为常见的用户需求，其中用户需求最高的服务有：应急响应、风险评估、漏洞管理、等保相关服务、驻场运维、基础安全服务。
- ◆ 在这些需求中，有一些已经可以通过自动化的方式实现，但仍有一些需求还需要人工现场参与。虽然安全运营服务在朝着集约化、智能化、低成本方向发展，但从当前多样化的市场需求来看，国内安全运营服务尚不能做到完全离场式的托管模式，到场的安全运营服务仍然占据一定比重。

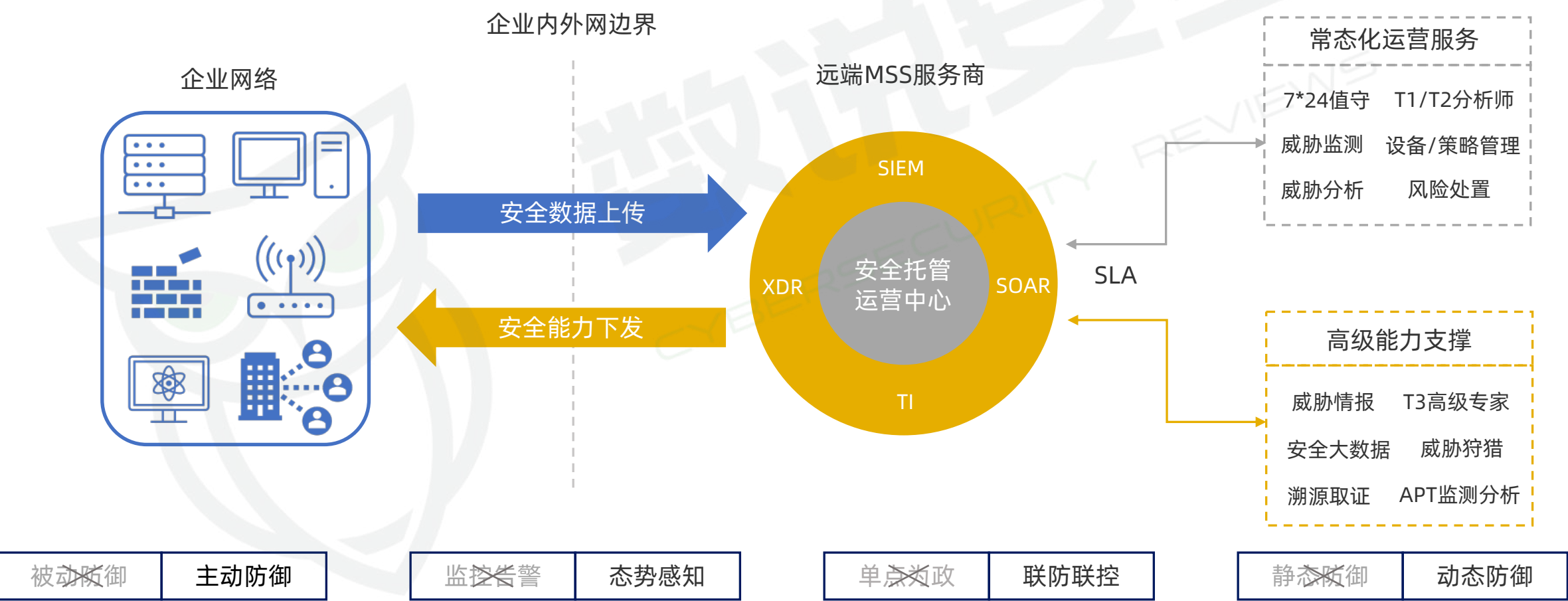


- ◆ 驻场运维服务是由传统安全集成业务自然延伸出现的服务形式，也是有安全预算、但苦于没有人员编制情况下甲方通常采用的形式。驻场运维服务是存量客户最多的安全运营服务子市场，对于以提供驻场运维为主的服务商来说，有以下4个共性特点：
 1. 劳动密集型：由于需要1对1和5*8驻场服务，服务商需要配备更多的服务人员，才能实现更好的客户覆盖；
 2. 跨区域服务挑战大：由于人员差旅、地域文化和工作方式差异，跨区域的项目可能不赚钱，服务商更聚焦于区域内用户，很少参与区域外的项目；
 3. 引入更多自动化平台和工具：因为“卖人头”模式投入产出比有限，服务商逐渐开始自研服务平台和工具，提高服务交付过程中自动化的比重，以达到更高的人效比，实现业务利润率提升；
 4. 服务要求细化升级：由于政策与监管力度持续加强，客户对驻场运维服务的要求也开始从被动防御、静态防御、监测告警服务级别向主动防御、动态防御、态势感知目标转变，并且愿意为这些增值的安全运营服务付费，服务商也在不断推动自身能力向安全运营服务能力转型。
- ◆ 虽然国内安全托管服务市场持续发展，但从国内客户使用习惯、接受度、核心需求、安全制度等方面来看，驻场运维服务仍可能是未来几年内市场中的主要需求。

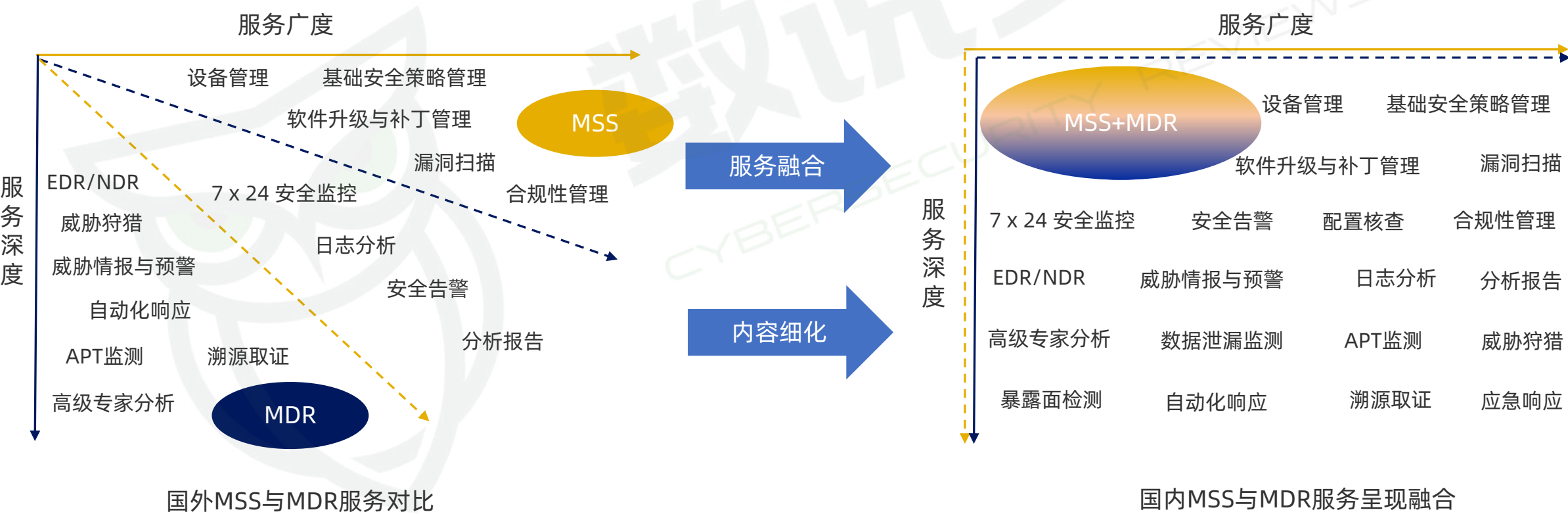


安全运营服务-安全托管服务（MSS）

安全托管服务（Managed Security Services, MSS）是一种新型的安全运营服务模式，企业委托专业的第三方MSS服务商全面管理其网络安全。典型的MSS模式依托于服务商可远程交付的安全托管运营中心，通过远程收集企业的安全数据，实现对企业网络安全风险的实时监测、分析、研判和响应。典型MSS模式不再依赖现场服务人员，而是以远程方式提供服务，可实现全年7×24小时的覆盖，并将服务商更专业的安全技术、安全人员和安全流程聚合到服务中，超越了传统现场服务、依靠个人能力的局限，给企业带来更高时效、更具性价比的安全运营价值。



- ◆ 典型的MSS服务侧重于管理和维护企业与安全相关的技术和产品，以保障企业IT基础设施稳定运行为目标，MDR服务则以更高的视角聚焦攻击与威胁，通过云网端数据共享与分析，提升企业在威胁检测与响应处置方面的能力。
- ◆ 从国内市场需求来看，由合规、实战和效果多驱动因素叠加，客户在选择MSS服务时，通常针对重要的IT资产和应用系统也会要求提供高级别MDR服务，而从供给侧来看，为了提升MSS服务价值，增强市场竞争力，MSS服务商也在不断细化和升级服务内容，推出配套的MDR服务。未来随着供需两侧的这种变化，MSS和MDR服务将延续融合的趋势，对于MSS服务商来说，也同时需要兼备MDR服务能力。



安全托管服务（MSS）在国内已有多年发展历程。随着客户的安全意识从合规转向实战，越来越多的客户逐渐转向购买安全服务而非仅购买安全产品，这使得MSS市场在国内得到了广泛认可。由于信任机制、安全制度、保密要求不同，国内安全托管服务呈现了3种主要服务模式，国外主流的、数据可出网的SECaaS运营模式在国内仍主要应用在中小企业和对安全数据外发不敏感的用户场景，国内网安头部和绝大多数政企类客户依然青睐在保证安全数据不出网前提下，采用远程托管或本地托管的运营模式。

SECaaS托管运营模式

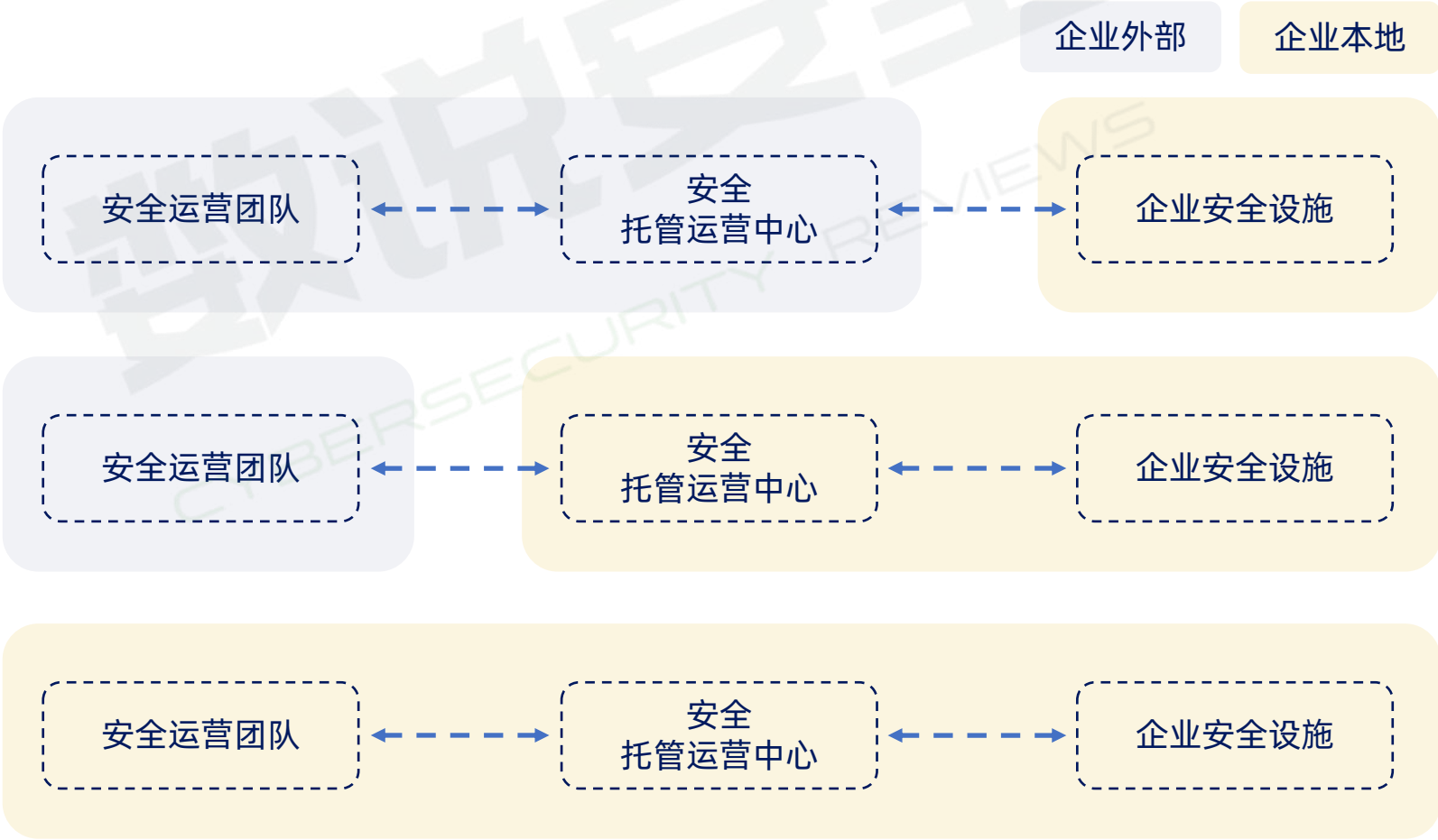
MSS典型服务模式，国外主流模式，即企业允许安全数据离开本地网络，远程接入到服务商远端的安全托管运营中心，并由MSS服务商安全运营团队实施远程管理，该模式应用的前提是企业安全数据可出网。

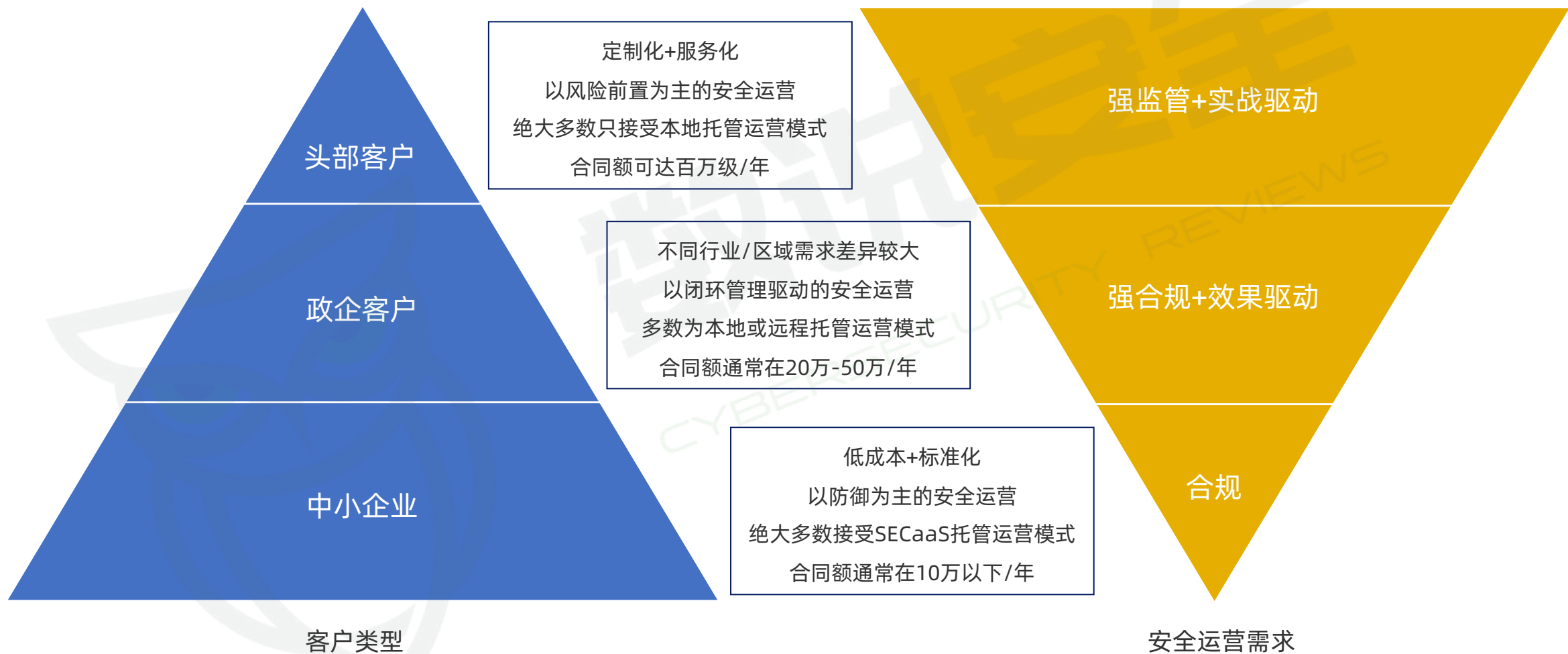
远程托管运营模式

企业不允许安全数据离开本地网络，MSS服务商将安全托管运营中心部署在企业本地，运营人员通过VPN、云桌面等方式接入进行远程管理。该模式既能满足企业安全要求，也能实现集约化运营。

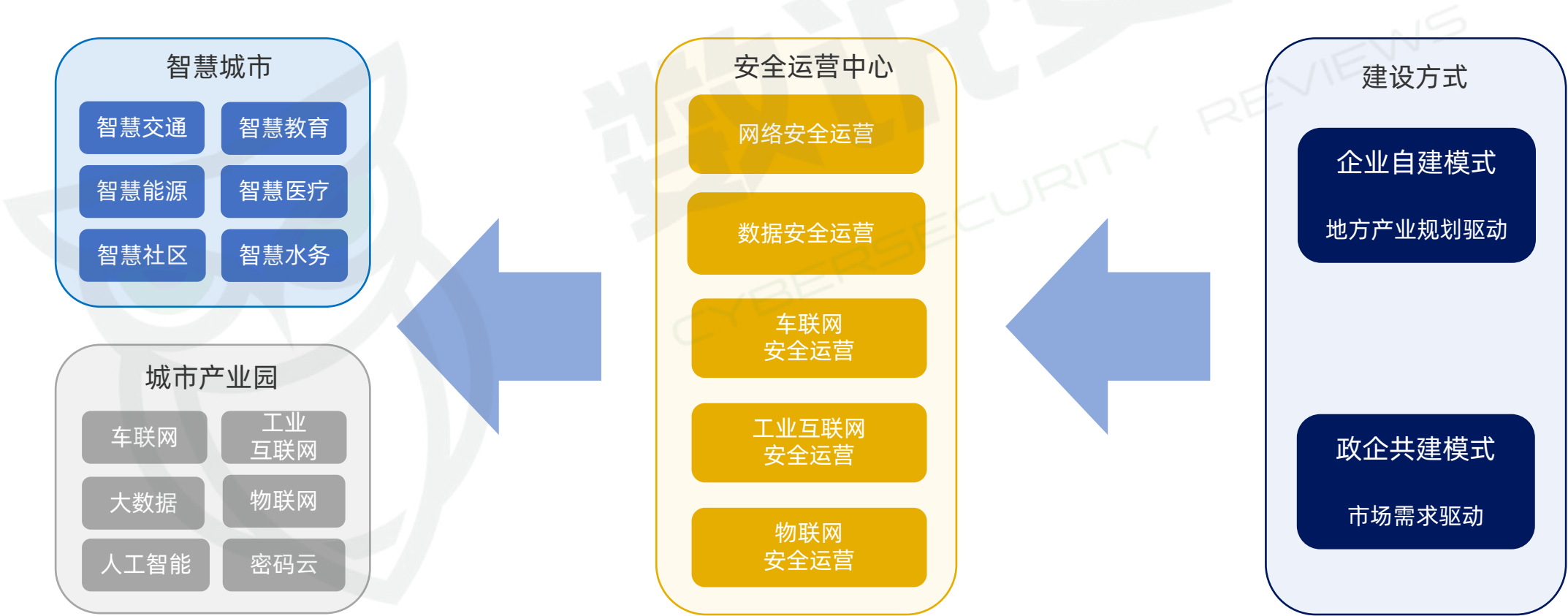
本地托管运营模式

客户对自身安全数据的保密要求较高，同时预算充足，也愿意为本地驻场安全运营服务付费，MSS服务商在客户本地部署安全运营中心的同时也派驻专职安全运营人员。

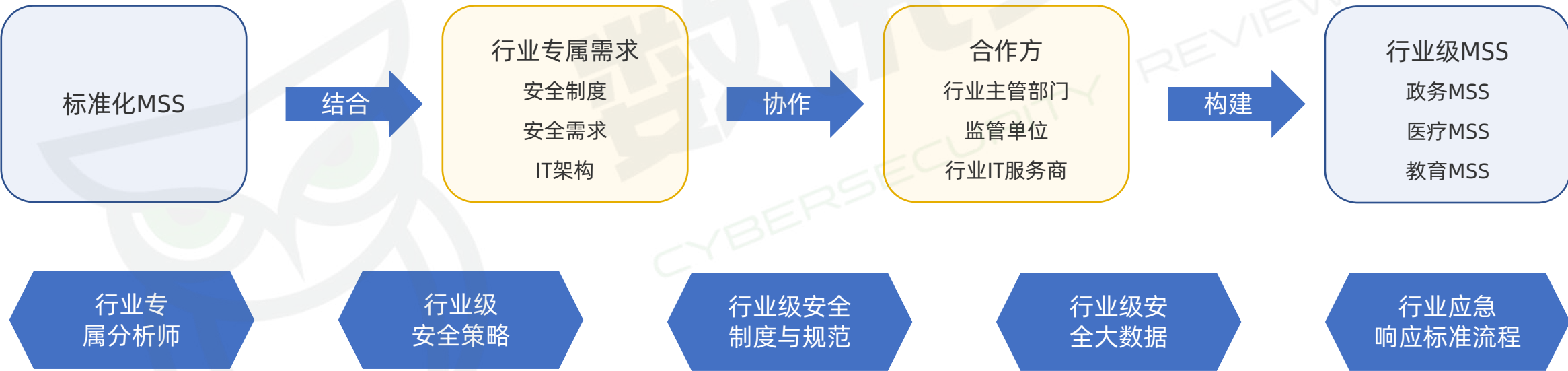




- ◆ 城市级安全运营是一个关键的网络安全枢纽，旨在为城市提供高水平的网络安全保护和响应能力，确保城市的网络基础设施和重要机构不受网络威胁的影响。这种安全中心的建立有助于提高城市的整体网络安全防御能力，以应对不断演变的网络安全威胁。
- ◆ 城市级安全运营主要面向两大类城市级业务场景，一个是面向智慧城市场景群的安全运营，一个是结合地方产业特点、面向各类IT产业园的安全运营。在城市级安全运营项目中，供需两端均具有较强的资源统筹和项目转化能力，但随着市场稳步深入发展，供给端竞争强度也在不断上升。
- ◆ 城市级安全运营中心建设模式主要有地方产业规划驱动的安全企业自建模式和市场需求驱动的政企联合共建模式，从实际情况看，企业自建模式逐渐减少，更多企业选择联合共建模式。



- ◆ 行业级安全运营是指针对特定行业量身定制的网络安全运营服务，不同行业面临不同的安全威胁和挑战，行业级安全运营可以结合各行业特点制定不同的安全运营策略和内容，并提供专业的服务以保障行业关键信息资产和数据的安全。行业级安全运营的核心在于深入理解各行业特性和核心业务流程，根据行业特点和不同监管要求，构建适合该行业特定环境的安全运营体系。
- ◆ 在安全托管服务市场中，政府、教育和医疗卫生行业是核心的客户群体，每个行业都有其特定的安全风险和需求。政府行业信息通常涉及国家安全和公共利益，因此其安全运营服务需高度本地化，以确保敏感数据严格限制在政府网络内部流转。教育行业，作为挖矿木马的高发区，迫切需要MSS重点关注内网的病毒感染及其横向扩散。医疗卫生领域则强调MSS应在保障其业务连续性的前提下，提升对勒索病毒的防御能力。



- ◆ 各行业精细化的服务需求难以通过一套标准的MSS服务来满足，也催生了行业级安全运营服务的兴起。行业级安全运营不仅适应了市场的需求变化，也代表了安全托管服务市场发展的趋势，即向着更加定制化和专业化的方向演进。

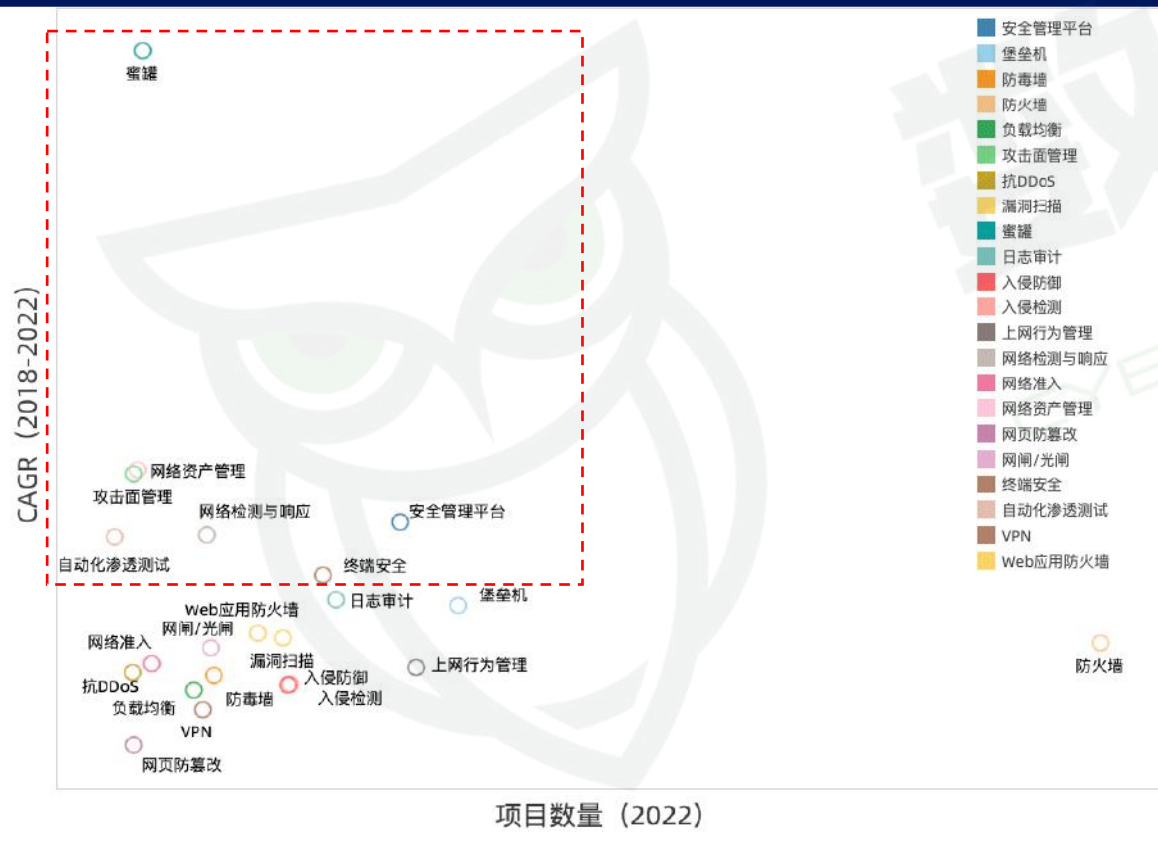
安全运营市场分析

- ▶ 安全运营产品全线快速增长，安管平台成为网安第四大单品市场
- ▶ 安全运营服务市场高增速放缓，但仍保持整体网安市场5倍以上增速
- ▶ 安全运营服务行业集中度高，政府/教育/医疗卫生/公检法司是核心行业
- ▶ 政数局、高等教育和医院是安全运营服务市场最大的客户群体
- ▶ 核心行业区域分布存在差异，30-50万是安全运营服务主流价格区间
- ▶ 应急响应/漏洞管理/风险评估/基础安全服务是安全运营服务市场刚性需求
- ▶ 广东/北京/浙江领跑安全运营服务市场，其余绝大部分省份也在高速增长
- ▶ 安全运营服务市场-行业TOP10服务商
- ▶ 安全运营服务市场-区域TOP10服务商
- ▶ 安全运营行业垂直政策与典型项目分析

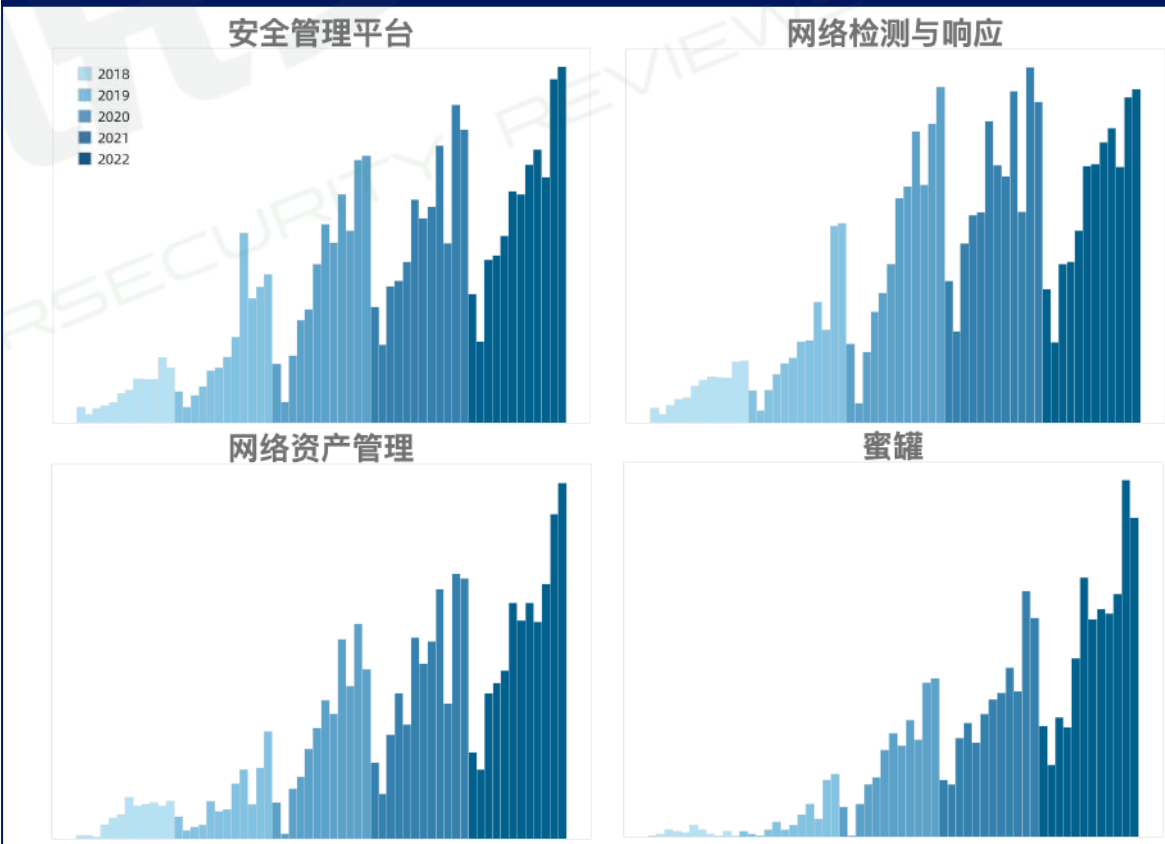
- ◆ 数据来源：数说安全CSRadar商业分析平台上跟踪到的市场公开招投标信息
- ◆ 数据范围：2018年1月1日至2022年12月31日
- ◆ 数据类型：采购安全运营类服务的服务型项目，采购安全运营类产品的产品型项目
- ◆ 局限性说明：所有市场分析内容基于市场公开信息，不包含不招标的商业市场和涉密市场。数说安全尊重市场客观发展规律，坚持中立的第三方观点，并对分析结论的准确性、完整性和可靠性尽最大努力的追求。由于研究方法和数据样本具有一定局限性，故在任何情况下，本报告中的信息或所表达的观点仅供客户作为参考，不构成任何建议。数说安全不对报告的数据及分析结论承担法律责任。

- ◆ 2018年-2022年，安全管理平台和其它具备较强安全运营属性的产品均呈现出较快的增长速度，5年复合增长率远超传统网安产品，且表现出抱团上升趋势，客户采购偏好发生显著变化。同时在2022年，安全管理平台市场需求非常旺盛，成为继防火墙、堡垒机、上网行为管理后的第四大单品市场。经过二十年发展，我国网安产业开始进入到建设与运营并重的新发展阶段。
- ◆ 在这5年间，安全运营产品也表现出不同的发展态势。其中安全管理平台有持续、明确的市场底量，近5年市场稳步增长。网络检测与响应市场在经历2020年高增长后近2年增长动能不足。网络资产管理市场进入到真正的连续上升期。蜜罐则从2019年Q4按下加速键，近3年高速增长，成为安全运营市场最受关注的产品。

2022 安全运营类产品项目数量与近5年复合增速



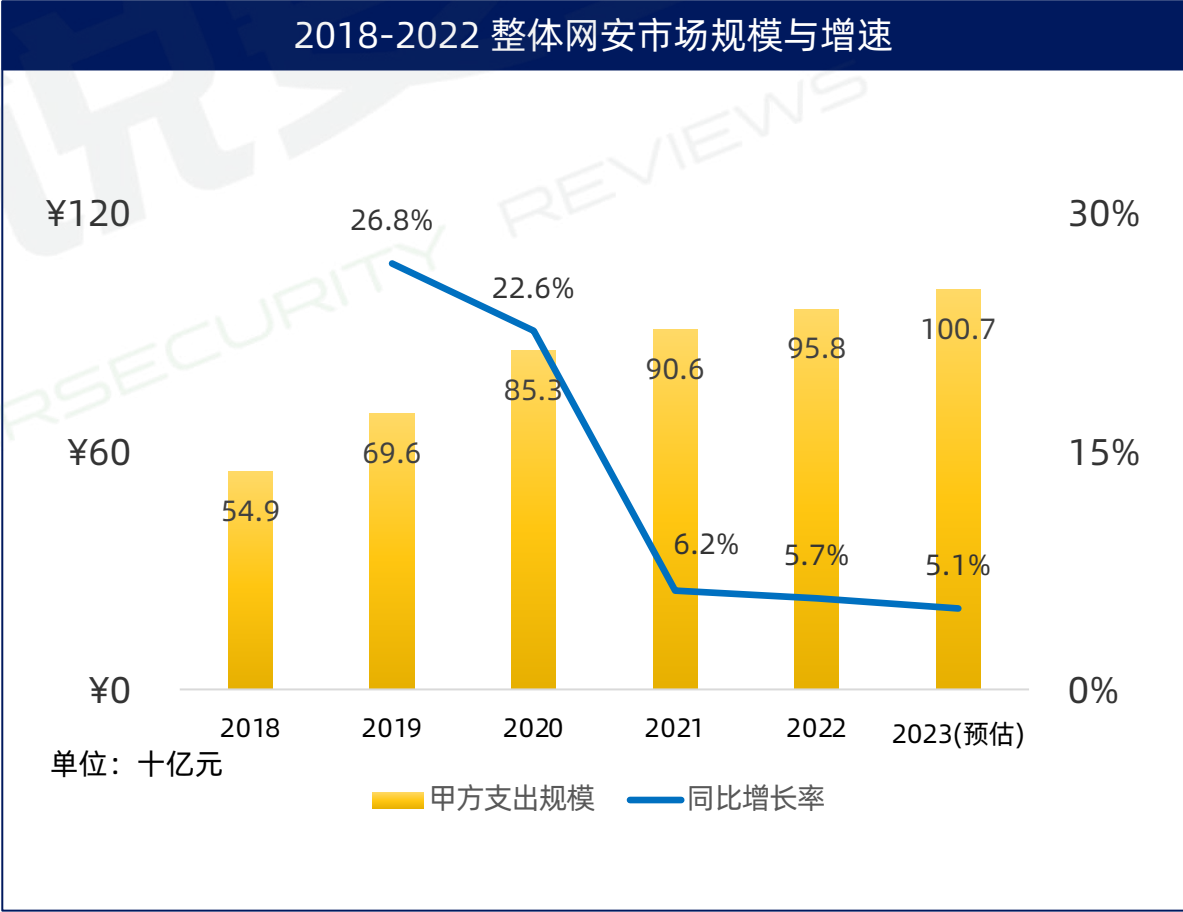
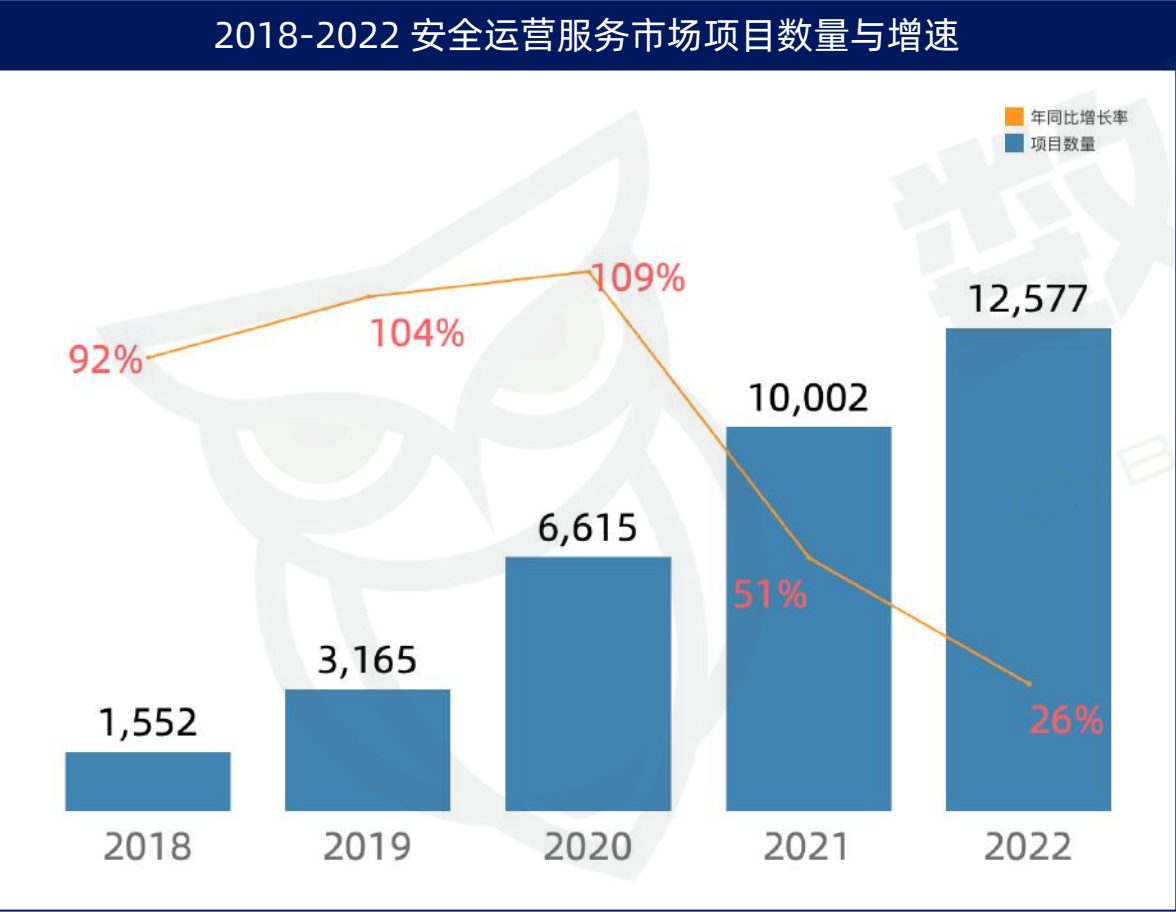
2018-2022 主要安全运营产品市场热度趋势



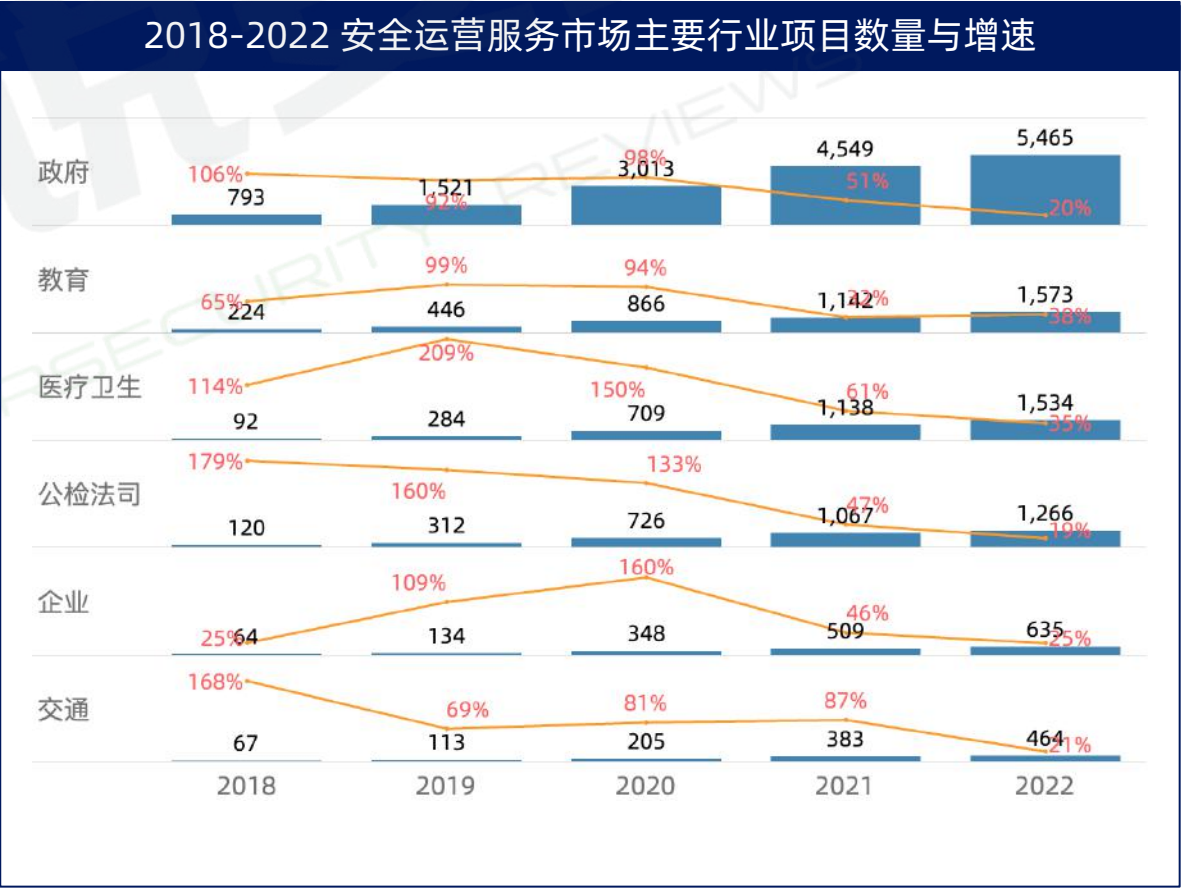
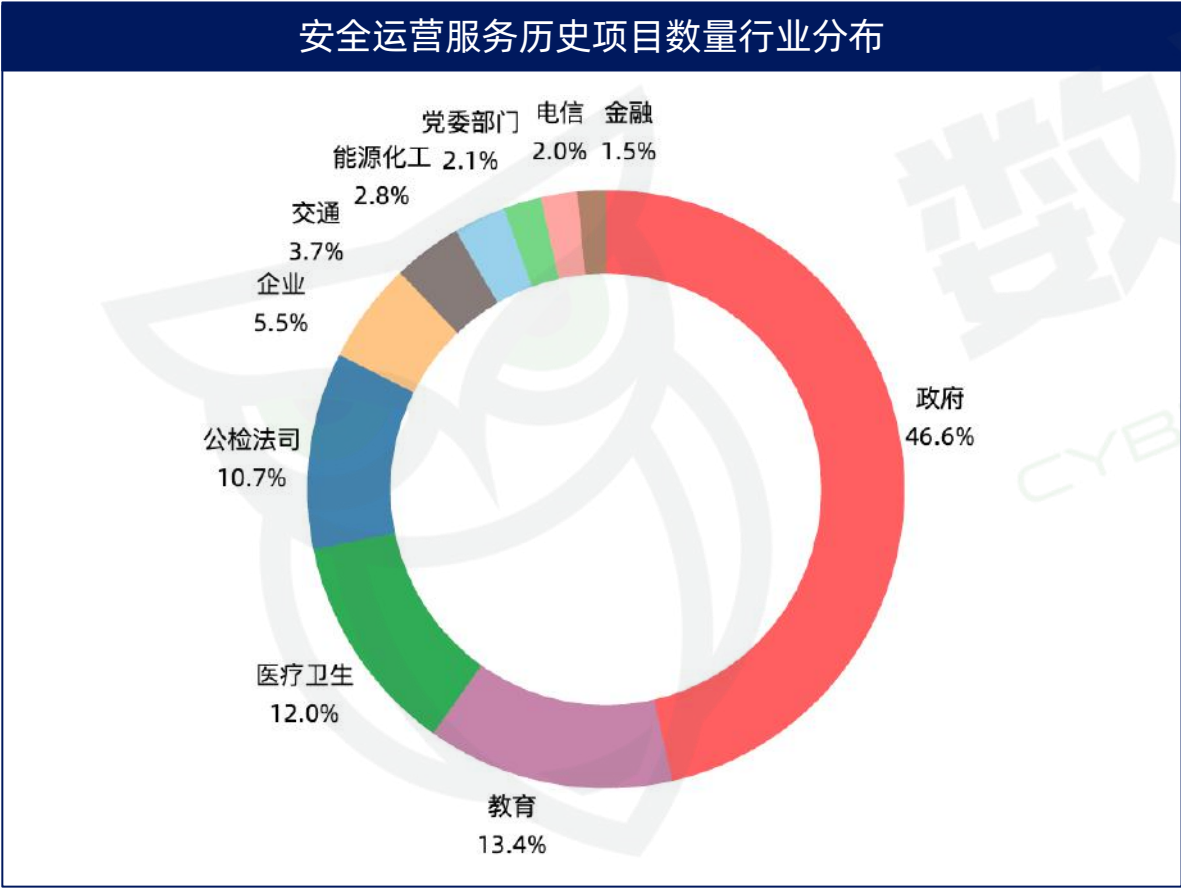
安全运营服务市场高增速放缓，但仍保持整体网安市场5倍以上增速



- ◆ 安全运营服务市场从2018年开始呈现非常高的增长态势，受疫情影响，2021年市场增速出现大幅下滑，2022年增速继续下降至26%，成为过去5年增速最低的一年。
- ◆ 过去5年虽然与整体网安市场保持着平行同向走势，但安全运营服务市场的增长速度还是非常亮眼。无论是高增长阶段还是增速下降阶段，市场增速始终远远高于同期整体网安市场，即便是情况最糟糕的2022年，也保持整体市场5倍以上的增速。

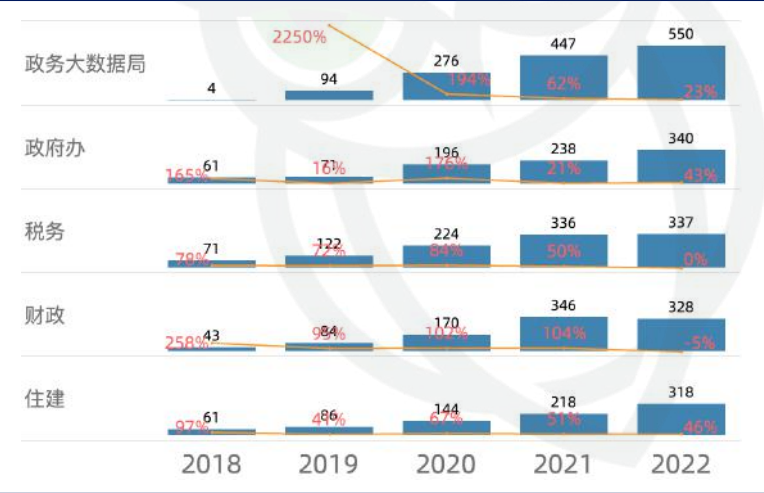


- ◆ 政府、教育、医疗卫生、公检法司行业占比均超过10%，4行业占比合计超过80%，是安全运营服务市场中的核心行业。其中政府行业由于机构数量庞大，有着更为急迫的安全运营服务需求，其项目数量已接近市场总量的一半，达到46.6%。
- ◆ 4核心行业在过去2年均出现增速的持续下滑，但教育和医疗卫生2022年的增速依然高于整体市场增速，其未来2年的发展情况值得关注。
- ◆ 金融和电信是网安行业头部客户，但在安全运营方面大多采用自建方式，采购安全运营服务采购需求较少，仅从项目数量来看，其并不是安全运营服务市场的主要客户。

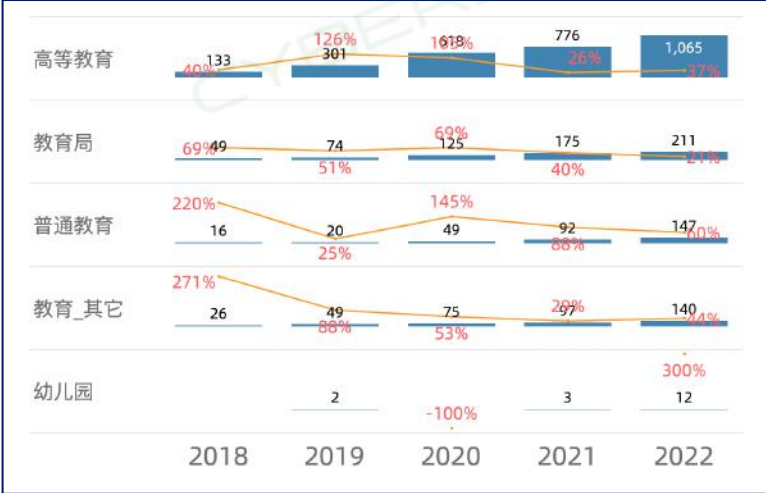


- ◆ 政府行业：
 - ◆ 数说安全将政府划分为39个二级行业，对安全运营服务需求最大的5个二级行业分别为政数局、政府办、税务、财政和住建，项目数合计占比33%，其它二级行业项目分布则非常分散，绝大多数占比不足2%，因此政府行业对安全运营服务的需求普遍存在于各个政府机构和单位。
 - ◆ 全国各地政数局在2019年前后陆续成立，对安全运营服务有迫切需求，从2019年开始项目快速增长，是非常值得关注的政府行业之一。
 - ◆ 政府行业安全运营服务个性化需求主要体现在3方面：基础性驻场安全运维服务、政务云安全运营与保障、政府门户网站群7*24安全监测。
- ◆ 教育行业：教育行业市场需求集中在高等教育，占比接近70%，增速稳定。其中高职高专、省属高校需求较大，项目特征主要表现为等保合规建设和智慧校园作为前导因素所延伸出的安全运营服务需求，大多数以基础安全运维为主。在成熟度高的用户中，已在整体或局部业务上采用MSS安全托管服务模式。
- ◆ 医疗卫生行业：医院作为医疗卫生的核心市场，占比超过70%，其中整体上三级医院占比较高，区县级医院开始呈现上升趋势，其中福建和四川在2022年出现比较快的增长。医院对安全运营服务需求更为细致，但业务连续性保障和勒索防护仍然是目前最核心的诉求，同时有部分医院在门户业务上已经开始采用MSS安全托管服务模式。

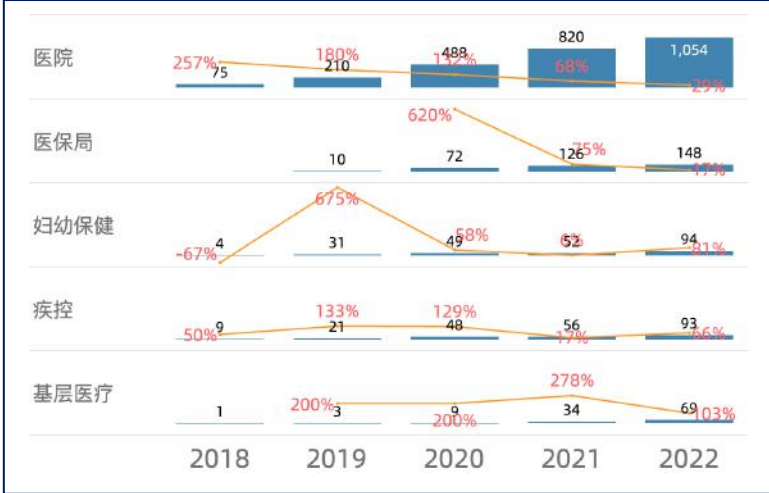
2018-2022 政府主要二级行业增长情况



2018-2022 教育二级行业增长情况



2018-2022 医疗卫生主要二级行业增长情况



核心行业区域分布存在差异，30-50万是安全运营服务主流价格区间



- ◆ 4大行业项目主要分布在传统网安市场的核心区域，包括北京、浙江、广东、江苏，且保持稳定增速。福建、湖南、四川在2022年，在4大行业上呈现出高增长态势，项目数量已逼近核心区域。
- ◆ 在非核心行业中，广东交通、广东企业、广东能源化工、北京能源化工、内蒙古能源化工，是具备一定项目底量、且在2022年保持快速增长的区域市场，其余还没有增速突出的大体量区域市场。
- ◆ 4大核心行业中，由于政府和公检法司对驻场运维有较强需求，因此项目金额中位数已接近50万，显著高于教育和医疗卫生30万的水平。

2018-2022 各行业区域历史项目数量与22年增长率

省份	项目数量									
	政府	教育	医疗卫生	公检法司	企业	交通	能源化工	党委部门	电信	金融
北京	-8%	30%	41%	39%	35%	-14%	108%	0%	36%	18%
浙江	11%	24%	3%	13%	35%	-8%	200%	-21%	39%	33%
广东	19%	38%	12%	-39%	86%	63%	67%	-11%	83%	38%
江苏	15%	73%	13%	13%	76%	-17%	80%	-13%	243%	0%
福建	24%	76%	64%	169%	-8%	7%	20%	275%	120%	-79%
湖南	31%	37%	72%	118%	-29%	3%		14%	-25%	25%
四川	66%	58%	106%	102%	-30%	-50%	-7%	20%	-40%	0%
山东	-1%	1%	47%	17%	-36%	32%	5%	11%	-40%	-18%
安徽	20%	25%	-4%	103%	-48%	43%		-50%	50%	0%
黑龙江	121%	413%	200%	114%		225%		1000%	0%	0%
广西	-39%	-41%	-23%	-35%	24%	19%	-75%	200%	-71%	
湖北	-13%	36%	3%	-47%	-5%	100%	-43%	50%	-100%	-50%
新疆	176%	233%	169%	108%	200%	500%	70%	733%	100%	-100%
宁夏	97%	63%	40%	144%		125%		-33%	250%	
内蒙古	209%	175%	67%	38%	500%	67%	414%	100%	200%	-67%
河南	31%	6%	27%	-44%	-12%	150%	80%	700%	133%	300%
山西	8%	13%	105%	33%	-50%	500%	400%	-25%	-100%	
江西	6%	-49%	-8%	0%	-33%	-23%	900%	-83%	100%	-67%
上海	-26%	-38%	59%	-60%	133%	120%	400%	-100%	-67%	-25%
重庆	11%	233%	-8%	-47%	0%	220%		-33%	0%	
贵州	10%	-24%	111%	-9%	75%	-43%	150%	-100%	-50%	400%
河北	80%	178%	175%	200%	256%	-25%	-100%		-75%	-67%
陕西	37%	60%	18%	30%	-33%		29%	-14%	-33%	150%
甘肃	0%	-16%	-61%	0%	-64%	100%	-70%	400%	0%	
云南	19%	180%	-13%	-25%	3%	-25%	50%	100%	33%	-100%
天津	48%	233%	14%	13%	50%	40%	233%	150%	400%	0%
辽宁	-32%	75%	333%	-44%	-11%	0%			60%	0%
吉林	6%	288%	33%	-44%	-17%	0%	-25%	-100%	0%	0%
西藏	-5%	0%	150%	600%					200%	
海南	-26%	0%	-40%	150%			-33%	100%	100%	700%
青海	-3%		33%	13%	-50%	0%	100%	0%	200%	-100%

2018-2022 安全运营服务项目金额中位数（专项）

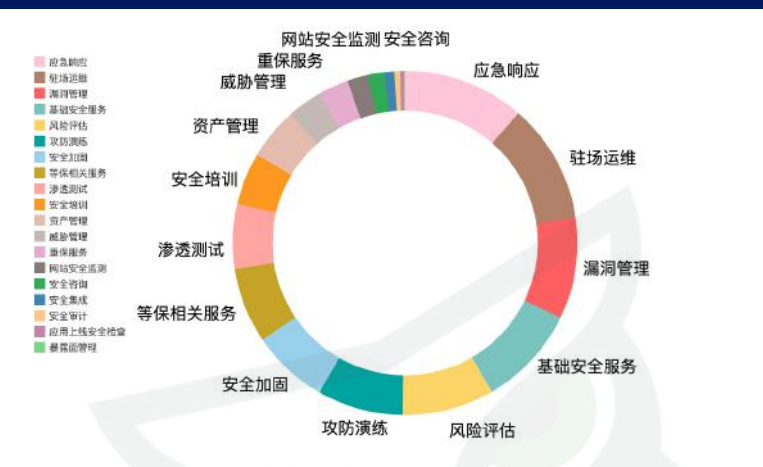
	2018	2019	2020	2021	2022
政府	460,000	500,000	550,000	575,000	490,000
教育	400,000	400,000	426,000	368,600	366,000
医疗卫生	347,000	346,000	620,000	400,000	298,000
公检法司	796,400	510,000	399,000	505,000	469,600
企业	250,000	380,000	398,000	470,000	395,000
交通	300,000	500,000	496,000	355,000	400,000
能源化工	520,000	97,500	413,000	891,800	475,000
党委部门	532,200	500,000	290,000	496,000	292,000
电信	650,000	550,000	500,000	735,849	480,000
金融	686,500	478,000	1,410,000	954,000	927,000

应急响应/漏洞管理/风险评估/基础安全服务是安全运营服务市场刚性需求

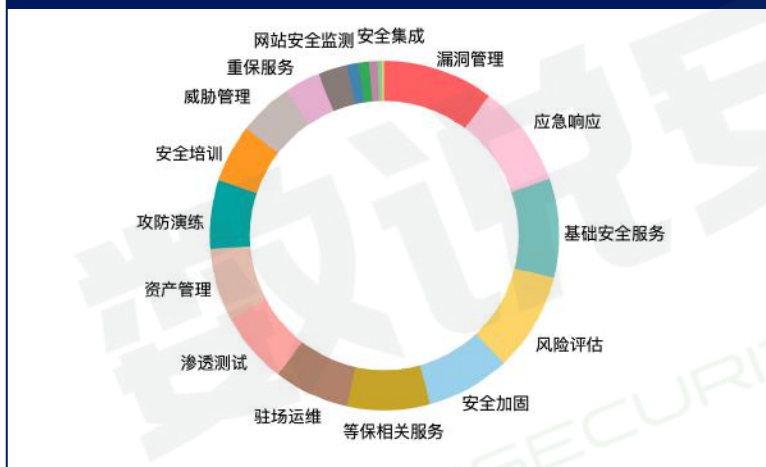


通过对招标采购需求做详细梳理与分析，得出不同行业对安全运营服务需求的分布：应急响应是4大核心行业（政府、教育、医疗卫生、公检法司）的普遍需求，政府和公检法司偏爱驻场运维，教育比较关注漏洞管理，医疗卫生则对风险评估和等保相关服务需求较大。

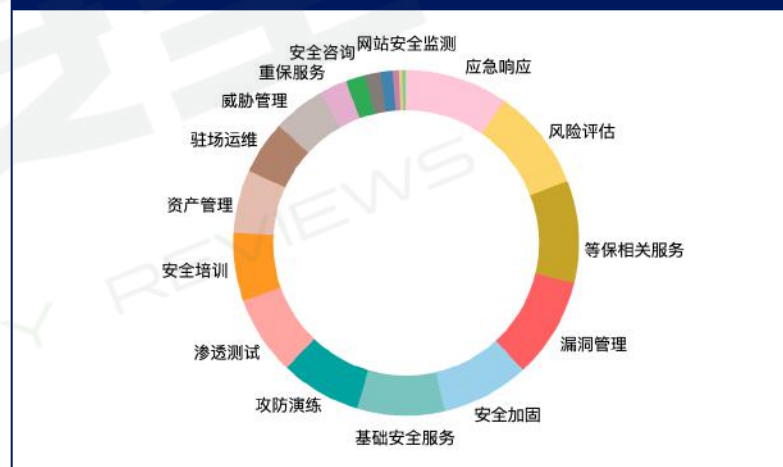
2018-2022 政府行业安全运营服务需求分布



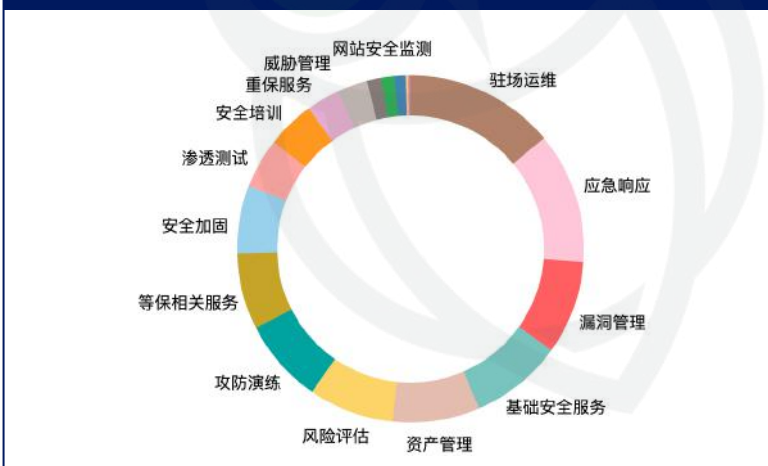
2018-2022 教育行业安全运营服务需求分布



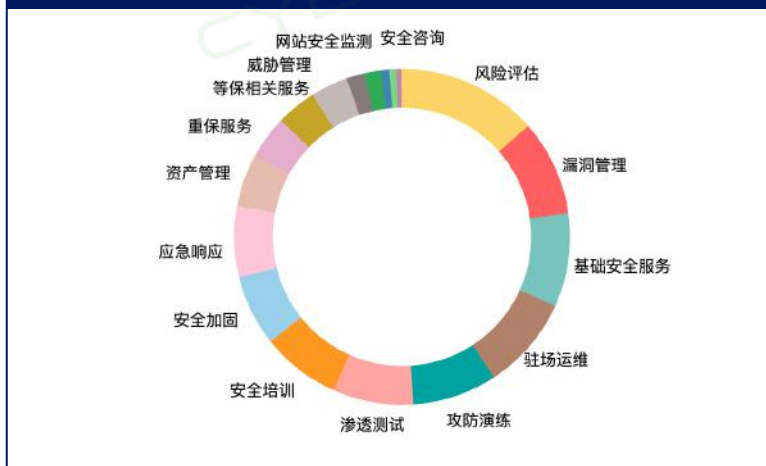
2018-2022 医疗卫生行业安全运营服务需求分布



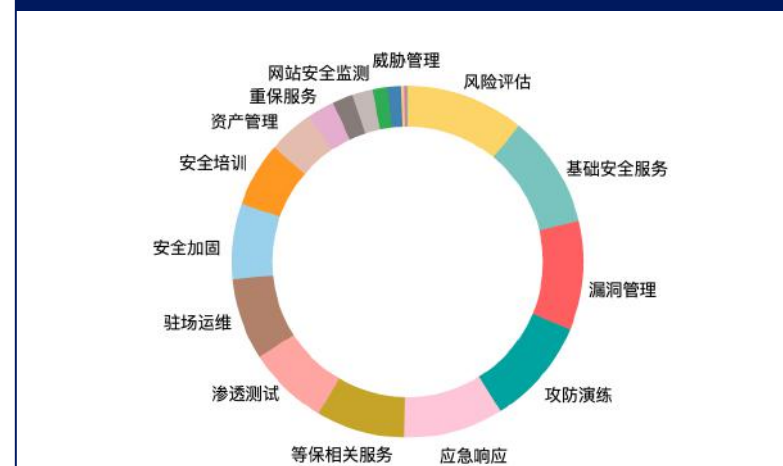
2018-2022 公检法司行业安全运营服务需求分布



2018-2022 企业行业安全运营服务需求分布



2018-2022 交通行业安全运营服务需求分布



广东/北京/浙江领跑安全运营服务市场，其余绝大部份省份也在高速增长



- ◆ 广东、北京、浙江是安全运营服务需求最为旺盛的3个省份，区域项目量超过3000；2000项目量级的省份包括福建、江苏、湖南、四川；达到1000项目量的省份包括山东、安徽、湖北，这10个区域是安全运营服务的核心区域市场，合计项目数量达到整体市场的三分之二。
- ◆ 在增速方面，31个区域，除了天津和海南，其余29个区域均呈现出全面高速增长的态势，5年复合增长率平均值接近80%，其中TOP5区域增速均超过50%，部分小体量区域甚至超过100%，由此看，无论是经济发达地区，还是经济发展中地区，安全运营服务在近些年受到客户的广泛认可，市场需求持续释放，从客户覆盖率的角度看，未来3-5年市场仍存在较大上升空间。



安全运营服务市场-行业TOP10服务商



统计2018-2022年各服务商直接中标的安全运营类专项项目数量，得出各行业安全运营服务商TOP10品牌，字体越大代表直接中标的项目数量越多。

2018-2022 政府行业TOP10安全运营服务商

中国移动 安恒信息
中国联通 启明星辰
绿盟科技 安信天行 奇安信
天融信 三零卫士 中国电信

2018-2022 教育行业TOP10安全运营服务商

安信天行 奇安信
中国电信 赛尔网络 中国联通
天融信 绿盟科技 中国移动 安恒信息
深信服

2018-2022 医疗卫生行业TOP10安全运营服务商

奇安信
安恒信息 中国移动 广东网安
安信天行 深信服 中国电信
三六零 优炫软件 中信网安

2018-2022 公检法司行业TOP10安全运营服务商

电科网安 中国电信 中国联通
安恒信息 天融信 中国移动 易聆科
嘉诚信息 启明星辰
奇安信

2018-2022 电信行业TOP10安全运营服务商

奇安信 亚信安全 启明星辰
保旺达 绿盟科技 华为
长亭 观安信息 美创 天融信

2018-2022 金融行业TOP10安全运营服务商

安信天行 中国联通 安恒信息
数字广东 绿盟科技 星维九州
奇安信 天融信 启明星辰 神州数码

安全运营服务市场-区域TOP10服务商



华南区域
广东东方思维科技有限公司
数字广东网络建设有限公司
广东网安科技有限公司
广州云峰信息科技有限公司
奇安信网神信息技术(北京)股份有限公司
北京天融信网络安全技术有限公司
北京神州绿盟科技有限公司
深圳市易聆科信息技术股份有限公司
北京启明星辰信息安全技术有限公司
杭州安恒信息技术股份有限公司

华东区域
杭州安恒信息技术股份有限公司
福建中信网安信息科技有限公司
江苏天创科技有限公司
奇安信网神信息技术(北京)股份有限公司
福建省海峡信息技术有限公司
北京神州绿盟科技有限公司
北京启明星辰信息安全技术有限公司
北京天融信网络安全技术有限公司
上海三零卫士信息安全有限公司
山东星维九州安全技术有限公司

华北区域
北京安信天行科技有限公司
奇安信网神信息技术(北京)股份有限公司
北京启明星辰信息安全技术有限公司
太极计算机股份有限公司
北京天融信网络安全技术有限公司
北京神州绿盟科技有限公司
北京禹宏信安科技有限公司
杭州安恒信息技术股份有限公司
深信服科技股份有限公司
首都信息发展股份有限公司

华中区域
奇安信网神信息技术(北京)股份有限公司
湖南省金盾信息安全等级保护评估中心有限公司
武汉云视科技技术有限公司
北京天融信网络安全技术有限公司
武汉安域信息安全技术有限公司
武汉吧哒科技股份有限公司
奇安星城网络安全运营服务(长沙)有限公司
上海三零卫士信息安全有限公司
湖南华测信息服务有限公司
智网安云(武汉)信息技术有限公司

西南区域
北京启明星辰信息安全技术有限公司
北京天融信网络安全技术有限公司
北京神州绿盟科技有限公司
奇安信网神信息技术(北京)股份有限公司
深信服科技股份有限公司
成都市数字城市运营管理有限公司
北京优炫软件股份有限公司
云南南天电子信息产业股份有限公司
重庆信安网络安全等级测评有限公司
成都奇点信安科技有限公司

西北区域
北京启明星辰信息安全技术有限公司
杭州安恒信息技术股份有限公司
西安德雅通科技有限公司
新疆天山智汇信息科技有限公司
北京神州绿盟科技有限公司
中电万维信息技术有限责任公司
上海纽盾科技股份有限公司
新疆联海创智信息科技有限公司
西安四叶草信息技术有限公司
甘肃安信信息安全技术有限公司

东北区域
长春嘉诚信息技术股份有限公司
黑龙江安信与诚科技开发有限公司
北京启明星辰信息安全技术有限公司
北京神州绿盟科技有限公司
长春市博鸿科技服务有限责任公司
奇安信网神信息技术(北京)股份有限公司
哈尔滨工业大学软件工程股份有限公司
大连惟远科技发展有限公司
沈阳欣欣晶智计算机安全检测技术有限公司
长春金阳高科技有限责任公司

以上统计2018-2022年各服务商直接中标的安全运营类专项项目数量，得出各区域安全运营服务商TOP10品牌。

安全运营行业垂直政策与典型项目分析

➤ 政府行业安全运营垂直政策

➤ 政府行业典型项目

- 1. 城市级安全运营; 2. 数字政府安全运营; 3. 发改委安全运营平台
- 4. 政务云安全运营; 5. 税务系统安全运维; 6. 省市数据一体化安全运营监测

➤ 教育行业安全运营垂直政策

➤ 教育行业典型项目

- 1. 等保建设与安全运维服务; 2. 智慧校园网络安全+运营体系建设; 3. 教育MSS安全托管服务项目集

➤ 医疗卫生行业安全运营垂直政策

➤ 医疗卫生行业典型项目

- 1. 面向等保/关保的安全运维服务; 2. 网络安全运营(+数据安全治理)服务
- 3. 医保信息平台安全运营体系建设; 4. 医疗卫生MSS安全托管服务项目集

《国务院关于加强数字政府建设的指导意见》 国发〔2022〕 14号

- ◆ 数字政府建设仍存在一些突出问题，主要是顶层设计不足，体制机制不够健全，创新应用能力不强，数据壁垒依然存在，**网络安全保障体系还有不少突出短板**，干部队伍数字意识和数字素养有待提升，政府治理数字化水平与国家治理现代化要求还存在较大差距。
- ◆ **建立健全动态监控、主动防御、协同响应的数字政府安全技术保障体系。充分运用主动监测、智能感知、威胁预测等安全技术，强化日常监测、通报预警、应急处置，拓展网络安全态势感知监测范围，加强大规模网络安全事件、网络泄密事件预警和发现能力。**

《山东省“十四五”数字强省建设规划》 鲁政字〔2021〕 128号

- ◆ 增强专业化安全防范能力。建立对全省数字政府政务信息系统、数据资源的安全监测和检测体系，准确识别安全风险，提升安全监测检测能力。实施全省重点行业点对点防护策略，加强智慧交通、智慧能源、数字水利等重要基础设施的安全防护工作，确保基础设施运行状态、风险隐患实时感知。**建设数字政府安全运营中心，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力。**
- ◆ **建设数字政府安全运营中心，成立安全运营机构。完善网络安全态势感知平台，扩大安全态势感知平台范围，推进其与业务系统的对接，与国家、网信、公安等平台完成数据对接，推进省市两级平台互联对接，形成全省一体化安全监测能力；**强化电子政务外网安全监测、政务云安全监管，加强电子政务外网监测节点部署，增加云上采集能力的部署和完善；加强政务网络整体的资产测绘及漏洞感知能力；加强平台AI分析能力。建设安全协调指挥平台，基于原有安全态势感知的基础数据能力，实现对网络安全整体工作的协调统筹指挥，实现对各类安全风险的统一管理。

《江苏省政务“一朵云”建设总体方案》 苏政办发〔2023〕 36号

- ◆ 建立具备纵深防御、态势感知和智能分析等能力的**全省政务“一朵云”安全防护体系**，从物理安全、云安全、数据安全和密码应用安全等层面进行立体防护。
- ◆ **建设包含感知监测、分析预警、指挥联动、应急处置、溯源分析、安全优化、外包管理等全流程的安全运维体系，提升响应效率，简化协同流程，高效保障业务安全可靠、持续稳定运行。**感知监测覆盖威胁告警、风险管理、漏洞管理等功能，实现资产清、位置清、态势清、异常清。分析预警将人工智能技术和监测数据有机结合，实现安全风险智能分析、秒级识别、动态预警。指挥联动实现横向到边、纵向到底、联动协同的自动化和智能化调度，提升日常态和应急态的安全协同能力。应急处置提升安全事件发生后的响应效率，加强攻防演练和重保看护，实现可演进的安全应对处置能力。溯源分析针对攻击事件进行调查取证，对攻击链条进行重新审视，确保通告及时、处理有效、责任到人。安全优化针对安全检测发现的安全漏洞等薄弱环节，进行持续安全策略优化、流程优化和技术加固。

《浙江省人民政府关于深化数字政府建设的实施意见》 2022.8

- ◆ 构筑公共数据全生命周期安全防护体系，推进数据加密、数据脱敏、数据水印、数据备份、数据溯源、隐私计算等技术能力全面应用，**强化网络安全主动防御能力、监测预警能力、应急处置能力、协同治理能力，全面提升云、网、终端、数据、应用防护能力。**强化个人信息保护，加强数据安全业务培训、技术防范和应急演练。

《广东省数字政府网络安全指数评估》 2020.12

- ◆ 为应对数字政府面临的安全威胁和严峻挑战，引导数字政府网络安全防护体系建设工作，持续提升数字政府网络安全防护水平，2020年广东省发布了国内首个数字政府网络安全指数。评估依托数字政府建设运营单位掌握的数字政府安全运营数据、网络安全监管部门掌握的数字政府安全监管数据、安全调研数据、网络安全厂商及互联网公司掌握的省域网络安全大数据、“粤盾-2022”数字政府实战攻防演练结果数据等，采用定量与定性相结合的分析方法，对全省各地市数字政府网络安全管理、安全建设、安全运营、安全效果等四个方面进行评价，客观科学地反映我省各地市数字政府网络安全整体防护水平。2022年广东省数字政府网络安全指数为百分制。其中，安全管理、安全建设、安全运营、安全效果4个一级指标分别占25%、20%、25%、30%。
- ◆ 安全运营指标用于评价数字政府网络安全保障体系在运行过程中的风险识别、安全监测及应急处置等能力，包含信息资产管理、日常安全运维、安全监测、应急处置、安全检查、安全审计、业务连续性保障、安全协同8个方面。重点通过摸清资产底数，及时发现风险隐患，采取相应的处置措施，形成联防联控的强大合力，确保数字政府网络安全防护体系稳定运行。

《广东省数字政府基础能力均衡化发展实施方案》 2022.10

- ◆ 齐头并进 全面推动数字政府各领域均衡发展：2019-2022年，省财政主要支持14个欠发达地市提升政务信息化基础设施、“一网共享”、安全保障体系等方面，《实施方案》与上一轮支持政策相比，支持领域和措施更加全面具体。网络安全方面，包括强化政务云基础安全保障和数据安全保障，推进政务领域商用密码应用等。

《河南省数字政府建设总体规划（2020—2022年）实施方案》 豫政办〔2021〕50号

- ◆ 强化安全保障。建设公共安全资源池、安全监管平台等，实现全程留痕和可追溯。落实信息安全等级保护、密码应用安全性评估及风险评估制度，定期开展信息系统安全风险测评和攻防对抗演练。建立数据风险排查和防控机制，发挥省政务服务平台枢纽作用，实现跨部门、跨地区数据共享全流程监管、追溯和数据异常使用预警。（省大数据局、公安厅、省委网信办牵头，各省辖市政府、济源示范区管委会、各省直管县〔市〕政府、省直各部门配合）。

《长沙市加快网络安全产业发展三年（2019—2021年）行动计划》 长政办发〔2019〕30号

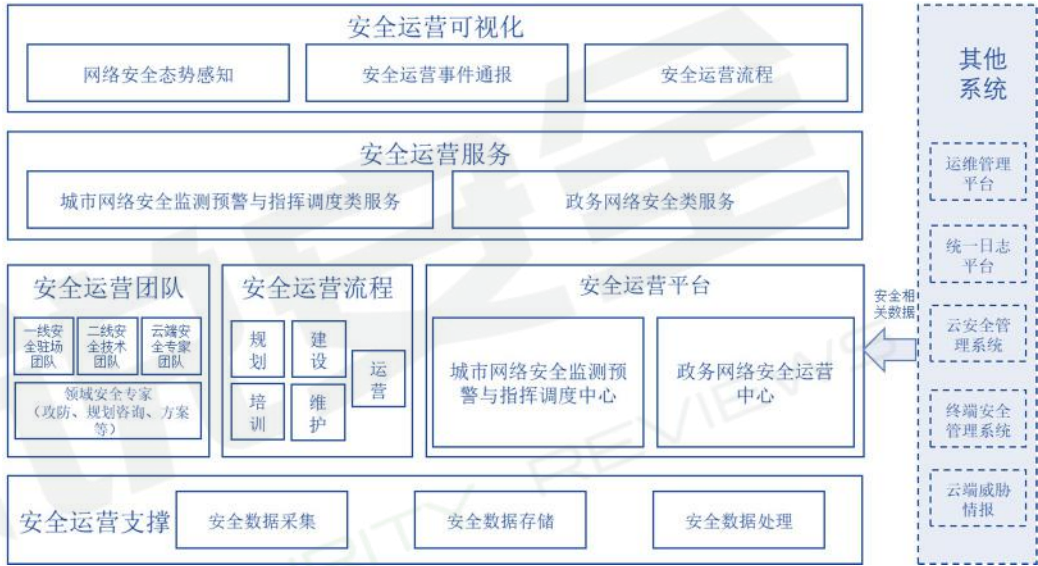
- ◆ 建设网络安全运营及应急响应中心。加大财政投入，搭建网络安全运营及应急响应中心，建立网络安全靶场、演练平台、实训基地和攻防实验室。面向企业提供安全规划体系论证、技术研发和验证、攻防演练演习、安全风险评估和安全培训等服务，定期组织大规模网络安全实战演练。建立跨部门、跨地区的应急处置平台，推动数据共享、联动响应，第一时间处置网络安全威胁，提升整体网络空间及重点行业安全能力，全面提升城市安全治理水平。（牵头单位：市委网信办，责任单位：市工业和信息化局、市公安局、市数据资源局）
- ◆ 支持研发创新平台建设。加快长沙网络安全研究总院、适配中心、测评中心、运营服务中心等重大公共服务平台建设，平台建成投产后，给予平台建设费用30%的补助，单个平台最高500万元。平台投入运营前三年，按实际产生服务费用给予全额补贴，单个平台最高500万元。（责任单位：市工业和信息化局、市财政局）

政府行业典型项目1-城市级安全运营



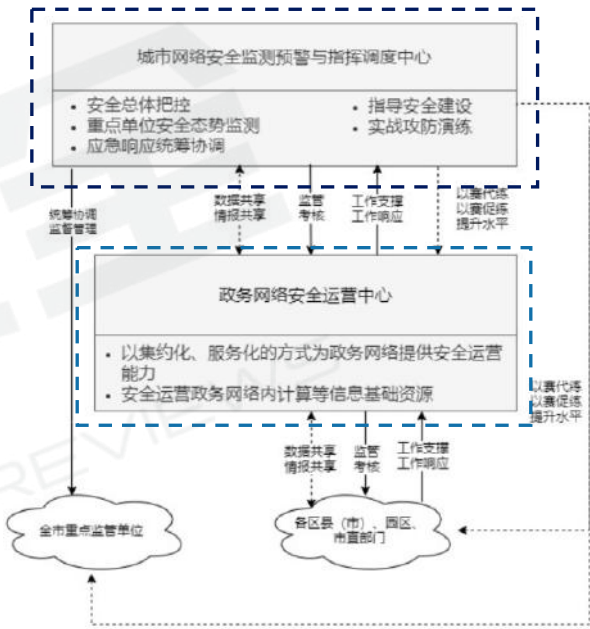
项目时间	客户名称	预算金额	服务周期
2021年	xx市大数据中心	5885万	3年
项目背景			
当前xx市正处于新型智慧城市和数字政府建设的关键时期，政务云底座、城市超级大脑、智慧交通、智慧医疗、智慧文旅等一大批数字基础设施和智慧应用服务建设正稳步推进。市委市政府为深入贯彻国家网络强国的战略目标，快速提升xx市城市整体网络安全防控水平和治理能力，助力城市数字经济发展和国家网络安全产业园区建设，保障xx市新型智慧城市示范城市和数字政府的高速安全稳定，制定并发布《xx市加快网络安全产业发展三年（2019-2021年）行动计划》，明确了建设xx城市网络安全运营中心，提升城市整体网络空间和重点行业安全能力，全面提升城市安全治理水平的工作任务。			
项目建设内容			
项目主要包括两部分： 1、面向市委网信办的城市网络安全监测预警与指挥调度：主要针对xx市委网信办的属地网络安全管理职责，侧重城市网络安全监管治理和应急响应； 2、面向市大数据中心的政务网络安全运营：针对xx市新型智慧城市和数字政府建设的各类信息系统，即xx市大数据中心自建和全市各委办局已上云的各类业务系统，提供网络安全运行保障和运营服务。 项目中涉及的部分信息化基础设施、软件平台及其配套的实施,采用租赁服务模式，服务中标人应形成本地化服务能力，为采购人提供持续服务。			

建设一级目录	建设二级目录	建设三级目录	建设模式(租赁/采购服务)
城市网络安全监测预警与指挥调度中心	城市网络安全监测预警与指挥调度平台及配套设施	包括数据融合系统、安全数据存储系统、业务应用支撑系统、安全监测感知系统、安全应急处置系统、统一指挥展示系统，以及相关配套的安全探针等配套硬件设施和互联网链路	租赁
城市网络安全监测预警与指挥调度服务	网络安全监管服务	包括人员驻场、安全检查、安全监测、安全通报等服务内容	采购服务
	实战攻防演练服务	包括演练组织、平台及场地租赁等服务内容	采购服务
	网络安全宣传教育服务	包括网络安全宣传周、网络安全意识教育、网络安全专项教育等服务内容	采购服务
政务网络安全运营中心	网络安全宣传服务	包括重点时期安全保障指导服务和特护期安全保障服务	采购服务
	政务网络安全运营管理平台	包括数据融合治理系统、系统安全管理系统、安全研判分析系统、安全协同处置系统、安全资源纳管系统、安全态势感知系统等，以及相关配套安全探针等硬件设施	租赁
基础网络和安全防护系统及配套设施	安全防护	包括防火墙、入侵防御、堡垒机、日志审计、漏洞扫描等符合等保三级要求的安全设备	租赁
	基础网络	包括IDC机房机柜、接入交换机、核心交换机等	租赁
政务网络安全运营服务	网络安全咨询服务	包括智慧城市网络安全顶层规划、安全政策制度、安全管理、安全技术、安全建设等方面的咨询服务	采购服务
	综合安全运营服务	包括人员驻场服务、APT威胁分析服务、高级渗透测试服务、安全监测分析、专项整治等服务内容	采购服务
	场景化的安全运营服务	包括各类场景下的重点时期安全保障服务	采购服务
	网络安全教育培训服务	包括网络安全运营技术培训、网络安全攻防技能培训、网络安全意识教育培训等服务内容。	采购服务



城市网络安全监测预警与指挥调度（市委网信办）	
平台建设	建设城市网络安全监测预警与指挥调度中心，导入外部安全监测数据，实现对城市网络安全事件的实时监测、威胁来源分析和组织情报分析。
前端探针部署	在全市60家政府、医疗、教育、交通、金融、传媒市政等重点行业和重点监管目标单位约130G的互联网出口，部署流量安全检测探针，实现对网络攻击、网页漏洞利用、病毒木马、APT事件等多种攻击行为的检测。
资产盘点	开展全市互联网资产信息测绘，建立全市互联网IP地址库、域名库和互联资产信息指纹库，掌握城市互联网资产暴露面。
网站监测	针对全市2000个重点备案网站进行实时安全监测，防止重要网站系统出现瘫痪及访问异常等不良情况造成的恶劣社会影响。
安全应急响应中心	建设城市网络安全应急响应中心，为城市网络安全应急指挥提供场地保障；开展7*24小时的城市网络安全运营服务以及定期的专项安全服务。
应急响应机制	开展城市网络安全应急演练，每年通过邀请攻击队，面向xx市重点行业和重要信息系统设施开展一次实战化网络安全攻防演习和网络安全现场检查，检验参演单位网络安全建设成效，检验并完善网络安全事件应急响应机制。
网络安全风险修复	通过实战攻防演练及时发现目标网络安全风险并提供修复指导。
民众网络安全意识	开展网络安全宣传教育，结合国家网络安全宣传周等场景，每年面向xx市民开展一次10个主题日的网络安全宣传活动。面向全市100家重点单位的网络安全负责人，开展网络安全应急、网络安全重保等工作的教育培训。

政务网络安全运营（市大数据中心）	
平台建设	建设政务网络统一安全管理平台，配套资产安全扫描、脆弱性扫描、基线核查、威胁检测、流量检测、文件沙箱、威胁诱捕等安全工具，实现对市电子政务外网、市政务云的网络安全监测数据的采集和集中存储，提供网络安全态势感知、安全数据采集、安全分析研判、系统安全管理、安全资源统一纳管等功能。
安全探针部署	在各区县（市）9个数据资源部门以及6个市直部门的政务外网和数据中心部署流量安全检测探针，通过对网络攻击、网页漏洞利用、病毒木马、APT事件等多种攻击行为的检测，实现对各区县（市）和6个独立机房市直部门的网络安全监管，并每月发布一次考核结果。
城市网络安全体系规划设计	结合《xx市新型智慧城市示范城市顶层设计》和《xx市新型智慧城市示范城市建设三年（2021-2023年）行动计划》，规划设计xx市新型智慧城市整体网络安全体系，编制《xx市新型智慧城市网络安全顶层设计》。
政务网络安全管理体系建设	结合xx市智慧城市建设现状，编制xx市智慧城市网络安全政策制度、技术规范和管理制度（数量不少于30个），面向xx市大数据中心的信息化建设全生命周期制定政务网络安全管理实施细则和技术规范，提供安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面的咨询服务。
政务网络安全运营	对市电子政务外网、市政务云以及各区县（市）数据资源部门、开发区/园区电子政务外网和数据中进行7*24小时安全监测分析，推进政务网络安全态势预测、事件分析、攻击防护和应急响应的安全运行闭环，完善网络安全应急预案，协助指导相关单位完成安全处置和安全整改修复。
常态化网络安全检查	面向市大数据中心自建的各类重点信息基础设施、信息网络和应用系统开展网络安全高级渗透测试、代码安全检查、攻击诱捕分析、APT高级威胁分析等，防范0day或其他高危漏洞暴露造成安全事故的发生。
场景化的网络安全保障	在重点特护时期如“二十大”以及重大节假日，或发生重大网络安全突发事件时，提供专业安全技术保障和应急响应力量，对重点特护对象开展重点保护工作，或者对重大网络安全事件提供紧急处置和溯源分析。
安全建设成效督检	对各应用开发商、云服务商、安全服务商的安全建设成效进行监督检查，并每季度发布一次考核评价结果。
网络安全技能培训	面向全市政务和智慧城市建设单位的信息化与网络安全开发维护人员提供专业的网络安全培训。



城市网络安全监测预警与指挥调度中心作为面向城市安全监管的技术支撑平台和总抓手，对全市重点单位进行网络安全监管，支撑“统筹协调、上下联动、数据共享、安全高效”的网络安全空间治理工作。政务网络安全运营中心作为可扩展的安全运营体系，通过安全监管、安全协同、安全保障确保政务业务连续性以及信息系统抗风险能力。平台间关系如下：

- 1、城市网络安全监测预警与指挥调度中心与政务网络安全运营中心分属于网络安全空间治理、网络安全防御管理的两个平台，平台之间通过共享数据，实行网络安全监测预警与指挥调度中心统筹协调、监督管理网络安全运营。围绕“平战结合”的网络空间安全治理需要，在监控预警的同时，开展实战化攻防演习，评估网络防御与应急处置能力，通过演习来评估其实战攻防抵御能力，从而达到提高网络安全意识，培养专业技术人员实战能力的目标。
- 2、政务网络安全运营中心向上为城市网络安全监测预警与指挥调度中心提供网络安全事件信息数据共享，向下为各政务单位信息系统应用提供联防联控的能力支撑，避免局部盲区而导致的防御体系失效；整体提升网络安全防护与突发风险应对能力，守住网络安全底线，筑牢网络安全防御屏障。

项目时间	客户名称	预算金额	服务周期
2022年	xx省大数据局	2500万	1年

项目背景
《xx省“十四五”数字强省建设规划》中明确指出“坚持总体国家安全观，聚焦数字基础设施、数字政府、数字社会建设等重点领域，支撑数字经济与生态的融合发展，打造“责任明晰、安全可控、能力完备、协同高效”的网络安全体系”。 参考国内外各类大型承载复杂业务的信息化系统运行模式，考虑建立我省数字政府安全运营中心，采用体系化的安全模式，按照持续运营演进方法，同时引入智能化的安全分析技术，提供自动化结合专家的安全处置手段，以及加强基于情报的事件研判机制，实现安全防御能力在数字政府领域的持续、真正落地。

项目建设内容
1、建立数字政府安全运营体系，在标准流程化的方式下完成省级数字政府基础设施及业务平台的安全运营工作，并向其他省级单位和地市大数据管理部门提供安全运营体系模板，让安全运行管理更加标准、统一。安全运营体系服务范围和省本级大数据管理部门相关云、网及应用。 2、建立大数据安全实训平台，实现网络安全领域政产学研全链条的有效衔接。在促进政企学研协同创新的同时，全面提升数字政府相关工作人员的安全创新和实践能力。

管理咨询服务
安全运营体系咨询服务-安全运营管理体系
安全运营体系咨询服务-安全运营工作机制
安全运营评价及安全有效性评估体系咨询-安全运营考核评价
安全运营平台
安全运营支撑平台
网络安全协调指挥平台
安全运营系统
用户行为分析安全系统
安全运营智能自动化运行系统
安全实训平台
网络安全仿真演练平台
红蓝攻防演习平台
网络安全应急演习平台
自动化渗透测试平台
源代码缺陷分析平台
人工智能实训平台

安全运营服务
安全运营管理服务
安全运营基础服务
安全运营技术架构维护服务
政务资产梳理服务
运营质量评价服务
安全能力有效性评价服务
电子政务基础设施仿真靶标运营
电子政务基础设施仿真靶标运营
电子政务基础设施仿真靶标运营
红蓝攻防演习平台运营服务
网络安全应急演习平台运营服务
自动化渗透测试平台运营服务
源代码缺陷分析平台运营服务
人工智能实训平台运营服务

安全运营支撑平台---核心功能要求

- ◆ 事件分析与处置：在数字政府安全运营工作中，包含大量针对安全攻击行为进行有效分析与跟踪的相关工作内容。为了改变分析过程以文档形式编纂导致无法对安全案例进行复盘及检索的弊端，系统在分析任务交叉确认的基础上，将完成有效性验证环节的分析成果进行卷宗化存储，便于安全决策人员对运营成果进行复盘及参考。
- ◆ 测试管理：在数字政府安全运营过程中，系统依据网络安全技术及管理要求，将渗透测试内容维护为细颗粒度的测试项，并将不同的测试项依照不同的测试场景组合为专用测试矩阵，规范安全运营人员在开展渗透测试过程中的测试流程及测试内容。
- ◆ 考核评价管理：在数字政府安全运营过程中，需要对安全运营人员的工作状态进行评价。通过收集各运营流程环节的工作数据，能够对运营工作的效率、准确性进行分析测定；对运营过程中发生的各项任务状态进行追踪，协助运营团队对安全运营工作内容进行指导和评价。
- ◆ 运营脚本：数字政府安全运营中心是以多级分析师协作的形态构建整体安全运营分析流程，但由于事件分析能力主要以高级分析师为主要输出来源，单纯以培训的方式向安全运营监测前线人数最多的一线分析师输出分析经验难免会产生遗漏，经常性的分析流程改进也影响学习连续性，并且无法对一线分析师的分析过程进行有效评价。为了完成上级分析师向下级分析师传递分析思路、处置思路、知识经验的目标，同时建立安全运营不同层次、不同角色间的工作内容及协同机制，平台需要具备“运营脚本”指导运营团队进行安全运营分析工作。
- ◆ 报告管理：在数字政府安全运营工作中，会产生大量的安全运营成果报告，因此需要系统提供自动化的报告统计编纂能力，减轻安全运营人员工作压力。

网络安全协调指挥平台---核心功能要求

- ◆ 政务资产管理服务：政务安全的目标是保障政务系统的完整、可用，为了确保政务系统的安全通畅，明确发生的政务系统安全问题的属主机构，有针对性地开展技术调度，同时对安全问题的处置状态进行跟踪。通过对政务资产进行汇总管理，从而“摸清家底”，明确政务体系安全防卫范围。
- ◆ 漏洞聚合管理：漏洞隐患对政务系统的影响情况是定期评估各地市政务系统安全状态及监管能力的关键要素，通过收集汇总各地市政务系统的漏洞数据，分析计算出周期范围内各政务资产脆弱性分值，并根据同比和环比的方式说明政务体系脆弱性安全现状，结合漏洞整改比率，对各地市大数据局实行安全风险提示及漏洞处置协调跟踪。
- ◆ 事件聚合管理：
 - ◆ 1、平台具备省级安全事件监测能力。通过依托省大数据局建立的全省政务外网监测体系的安全威胁监测能力，安全专家能够将发现的政务外网安全事件进行汇聚，并对安全事件的详细内容进行维护。监测到的安全事件通过协同处置服务模块发起事件协同流程，协助相关地市大数据局或属主单位完成事件的处置工作。
 - ◆ 2、平台具备地市安全事件上报能力。除漏洞外，能够汇聚各地市大数据局监测到的政务系统安全事件。检查管理：安全检查为省大数据局监督各地市大数据局安全工作的重要手段，需要定期或临时性发起各类安全检查工作，以评估真实安全状态。
- ◆ 热点应急管理：在安全管理工作中，数字政府运营中心需要对应急性工作进行支撑，应急性工作包括突发性安全专项问题、上级通报等。因此，系统需要具备热点应急管理功能对相关应急任务进行管理与归档。

项目时间	客户名称	预算金额	服务周期
2022年	xx省发改委	200万	1年
项目背景			
按照省数字化改革网络安全工作有关要求，建设数字化安全运营平台。本建设内容作为统一运营管理平台的网络安全模块，完成与统一运营管理平台的对接。安全运营平台接入范围覆盖省发改委重点信息系统。构建统一态势感知、统一通报预警，为持续提升委网络安全监测、预警、聚焦、处置工作水平提供有效支撑；落实常态化安全检测、安全监测、安全应急等工作，通过安全技术服务，发现网络安全隐患和漏洞，不断提升风险管理和应急处置水平，保障信创OA系统和发改大脑应用的安全运行。			

项目建设内容
建设省发展改革委安全运营平台。覆盖省发展改革委重点信息系统。实现政务云租户环境、经济信息中心机房的数据采集和处理、安全分析、态势感知、通报预警。将平台作为统一运营管理平台的网络安全模块，完成对接。 系统将满足信创适配要求，适配国产机及国产操作系统、浏览器等软硬件客户环境，如适配龙芯、鲲鹏等主流硬件架构，适配中标麒麟等主流操作系统，适配红莲花、360等主流浏览器。

安全运营平台主要功能模块	
数据采集和处理模块	将已有的、互相隔离的、分在政务云租户环境内、机房的安全数据打通，对于已有的安全数据，实现安全数据的统一汇集与利用。实现省发展改革委政务云租户环境、机房已有数据集成接入后的清洗、补全、关联、标准化、存储与处理，形成可用的数据字典、索引，支撑实现安全运营应用。
安全分析模块	利用安全数据对省发展改革委政务云租户环境、机房的网络日志、流量日志、安全告警等数据，应用、匹配安全分析模型，发现安全隐患，形成分析结果数据，支撑上层应用。
态势感知模块	实现省发展改革委政务云租户环境、机房整体安全状况可视化，提炼安全指标，有效提升工作效率的重要保障。统一安全可视态势感知的功能建设需求，需具备基于汇聚统一的安全数据的分析能力，能够展示出不同的安全视角体现省发展改革委不同安全域、不同系统的态势视图，反应全局的安全威胁、安全隐患与安全事件。
通报预警模块	将省发展改革委网络安全工作在政务云租户环境、机房整体串联、及时发现、有效处置的重要支撑，也是实现“数字化改革”中构建实战化重要节点安全防护体系、完善应急处置机制、提升应急处置能力的必要支撑。
对接统一运营管理平台	完成与统一运营管理平台的用户体系、数据接口、应用界面等的对接，应用页面与统一运营管理平台进行统一入口集成与页面集成，实现一屏展示的效果。

信创OA安全运行保障		
资产威胁探测服务	安全检测加固服务	安全运营服务
安全管理服务	应急响应服务	安全通告服务

项目时间	客户名称	中标金额	服务周期
2023年	xx市政数局	661万	1-2年

项目背景

“十四五”规划中明确提出，要提高数字政府建设水平，加强公共数据开放共享，推动政务信息化共建共用，以及提高数字化政务服务效能。在“十四五”期间，国家电子政务网络建设、集约建设政务云平台和数据中心体系，推进政务信息系统云迁移成为核心任务。政务上云已成为各地政府数字化转型的必选项。通过基于统一的政务云平台，加强数据共享互通。政务云已成为数字政府、数字城市建设的关键基础设施。

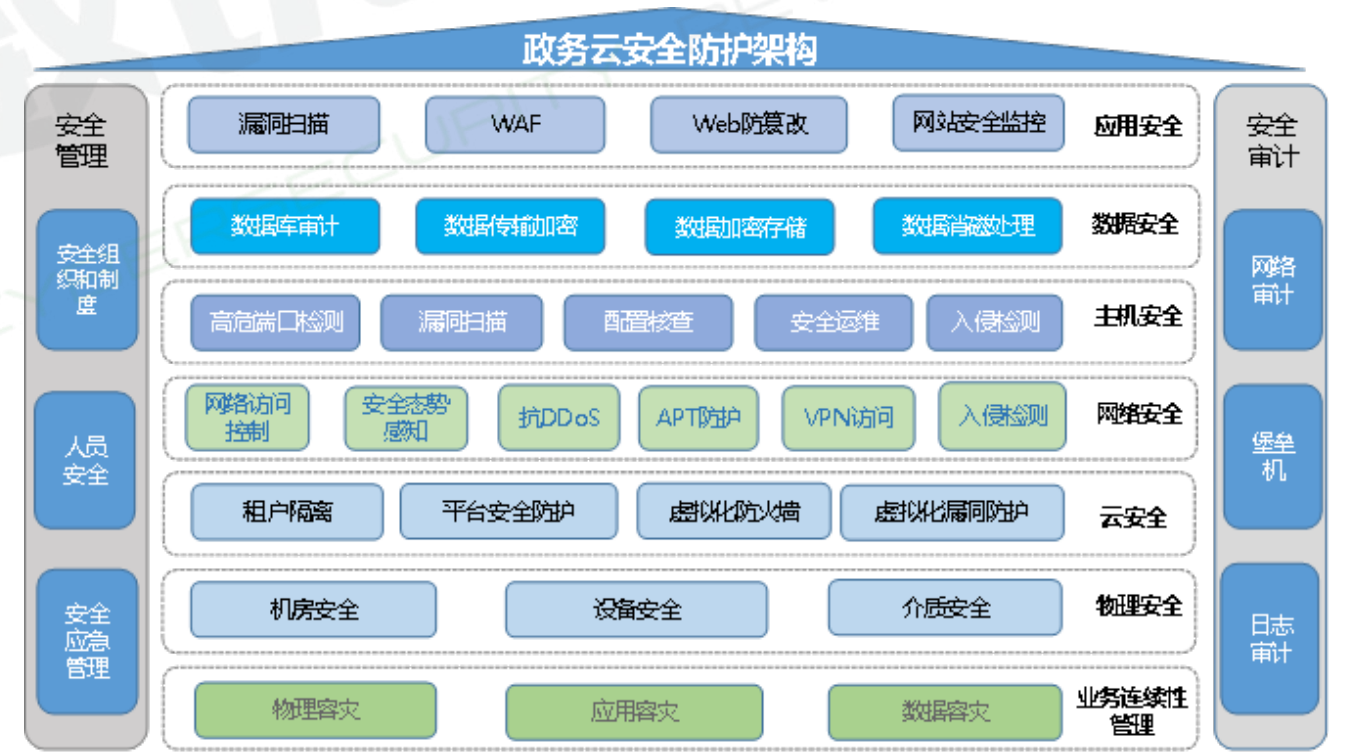
xx市政务云平台节点是省级政务云的安全边界和延伸，是保障地市政务信息系统安全可靠运行的重要载体。根据全省一体化安全标准的要求，地市政务云平台节点应该实现与省级政务云一致的全能力安全保障。

为贯彻落实《国务院关于加强数字政府建设的指导意见》工作部署，按照全省“一盘棋”的原则，统筹规划和布局数字政府基础设施和平台支撑体系，以各地级以上市为建设主体，从2022年起分三年完成数字政府基础能力均衡化发展指标任务，有力夯实数字政府建设根基。要求完善政务云基础安全保障体系。各地要统筹开展本地区政务云平台网络安全设备改造升级、攻防演练与安全测评，巩固提升政务云基础防护能力和安全运营支撑能力，推进本地安全运营平台与省级安全运营平台对接。《xx省数字政府基础能力均衡化发展指标任务执行标准》明确了健全政务云基础安全保障体系的工作要求，一是各地建成“云管端”一体、管理与技术防护并重的网络安全体系，覆盖网络攻击发现、通报、处置、溯源、打击全流程。二是各地利用大数据分析、自动化编排等技术，开展集中化、自动化、智能化的安全运营，提供覆盖全生命周期的安全服务能力。

项目目标

本项目将从原有安全设施运维服务、新增安全设施服务和安全运营服务三个方面为政务云平台xx市节点提供安全保障，完成我市分节点平台安全设施保障及安全运营平台运营工作。实现xx省“数字政府”省市一体化安全运营的目标，满足“全局统筹、跨网联动、多维感知、智能闭环、安全可视、合规运行”的网络安全新时代要求。

服务类别	安全运营平台软硬件设施维保服务	新增安全设施服务	安全运营服务	其他安全服务
服务周期	21个月	13个月	21个月	24个月



服务类别	服务内容概要
安全运营平台软硬件设施维保服务	安全运营配套硬件设施运维服务：主要提供安全态势感知服务器、地市节点专用交换机、地市节点专用服务器等配套硬件设备运维服务。 云平台安全设备基础设施运维服务：主要提供网络入侵防护系统(IPS)、DDoS防护设备、主机安全防护系统云镜服务、堡垒机、网络安全审计、集中日志审计系统、APT检测系统、云平台Web应用防火墙服务、云平台漏洞扫描服务、云平台基线配置核查服务等。 安全资源池运维服务：包括虚拟下一代防火墙组件、虚拟VPN、虚拟漏洞扫描、虚拟基线核查、虚拟堡垒机、虚拟数据库审计、虚拟网络安全审计、虚拟日志审计、虚拟增强型网页防火墙和虚拟网页防篡改等虚拟化安全资源组件，为租户上云提供满足等保2.0等安全合规要求的安全能力，为本市云平台节点提供全能力的安全防护服务，同时为省市一体化安全运营平台服务提供安全数据源。 智能网络流量检测运维服务：通过镜像端口的形式对政务外网网络流量进行检测，可检测数据中心内部存在的安全威胁及恶意流量，同时能够识别网络协议、租户网络行为，根据网络行为智能判断攻击威胁并采取对应行为。本期为智能网络流量检测软件服务提供运维服务，包括日常在线响应用户使用过程中遇到的问题，对软件进行日常更新运维，日常排检等内容。 省市一体化安全运营平台及态势感知服务：基于运营中心原始日志数据、安全分析数据，结合外界(国内外)互联网安全态势总体情况对当月的安全运营态势进行分析研判并在大屏显示。
新增安全设施服务	新增安全设施服务包括堡垒机授权、抗DDos服务、智能网络流量检测系统(攻击阻断)、入侵防御、政务云业务网站监测服务、威胁情报服务、省市一体化平台自动化编排服务、资产发现与风险管理平台、VPN与堡垒机国密改造、主机安全防护系统云镜升级版服务、主机安全防护系统云镜升级版授权等。
安全运营服务	安全运营支撑：加强地市安全运营团队建设，组建省市两级覆盖威胁监控分析、攻击防护处置、风险预警通报、应急演练的安全运营团队，优化运营规范制度，实现本级云网常态化7*24小时(省中心远程和地市现场结合)网络安全运营安全。 重保服务：通过现场值守、应急响应、突发事件处理等方式，为机关单位提供重大事件期间重要信息系统安全技术服务，确保各单位在重大时期能够及时应对各类信息安全突发事件，保障网络与信息系统安全稳定运行，做好重要时期的信息安全保障工作。
其他安全服务	上线安全测评服务：提供系统上线安全测评服务，服务包含编制测评方案、安全渗透、端口扫描、弱口令检查、基线配置检查、编制报告等内容。 网络安全指数评估服务：支撑和指导xx市系统梳理2022年和2023年指数评估情况和现状，识别差距，找出关键问题，提出2023和2024年xx市数字政府网络安全改进建议和方向，制定整体提升方案，并指导xx市政数局及各市直部门落地实施，提升xx市数字政府网络安全整体防护水平。

项目时间	客户名称	预算金额	服务周期
2023年	国税xx市税务局	433万	1年
项目背景			
近年来，税务总局在金税四期网络安全规划建设中，将建设智能安全运营中心列为一项重点工程，将其作为网络安全工作的重要支撑和有力抓手，力争实现安全防护自主可信，安全态势可知可见，安全现状可管可控，安全事件闭环运营。			
项目内容			
购买网络安全运营服务，完善我局的网络安全运营服务体系，协助我局提升安全整体规划管理，完善安全管理制度，优化安全管理流程。以整体安全运营的理念将网络安全服务、CDN网络加速、SSL证书服务、互联网高危漏洞检测挖掘和众测服务、数据安全运营服务以及14个系统的数据安全风险评工作等安全服务进行全面整合，达到全面提升网络安全监控、预警、响应、处置、应急等综合能力。			
人员要求：驻场团队至少4人，其中3名网络安全运营驻场工程师+1名数据安全运营驻场工程师；攻防演习防守团队需1名安全专家+2名高级安全工程师；应急支撑团队需要5人，按不同角色需保证1-2小时内到现场；重保服务团队需配备9名现场保障人员。			

日常运维服务			
信息资产管理	安全管理监控	互联网预警监控	安全加固技术支持
配置策略优化	网络威胁数据分析	基线配置检查	网络拓扑梳理
安全检测服务			
互联网暴露面发现（每年4次）	外部漏洞挖掘（每季度1次）		
安全专项检查（每年2次）	内部安全扫描（每季度1次）		
病毒查杀（每季度1次）	安全日志分析（每季度1次）		
安全审计服务（每季度1次）	代码审计（1600万行）		
安全检测服务			
威胁建模服务	威胁通告服务	威胁处置服务	威胁狩猎服务
应急响应服务			
重要时期保障服务			
网络攻防演习（监管/行业/市各1次）	重要时期保障		
网络安全宣传服务	SSL证书服务		
CDN加速服务	互联网高危漏洞检测挖掘和众测服务		
数据安全运营服务（含数据安全风险评估）			
安全服务配套工具			
网络流量探针	APT攻击检测	基线配置核查	威胁狩猎系统
数据安全平台		敏感数据发现	数据库审计

政府行业典型项目6-省市数据一体化安全运营监测



项目时间	客户名称	预算金额	服务周期
2023年	xx市数据资源管理局	800万	3年

项目背景

根据《全省一体化数据基础平台迭代工程等四大工程工作方案的通知》要求，开发建设xx市安全运营（监测）平台，保障省一体化数据基础平台xx市级节点的稳定运行，将技术、管理、人员和服务进行有机结合，实现网络安全事件监测、响应、指挥调度以及对云安全、网络安全、密码安全、应用安全、数据安全的监控，建成上下级平台贯通的全链路防护、检测、预警、处置、反馈体系。平台明确各类业务数据在数据全生命周期各个业务场景下保障要素，以合规为基线，以业务流程为导向，结合制度规范，建立完善的数据生命周期的为安全保障和监管措施。同时建立安全监控预警、信息通报和应急处置机制，逐步实现从“基于威胁的被动保护”向“基于风险的主动防控”转变，形成网络安全和数据安全的保障闭环。

项目需求

流量探针	网络流量溯源分析系统	县区采集清洗节点
日志探针	资产探针	漏洞探针
蜜罐探针	DNS解析	
安全数据仓库	安全能力中台	安全业务中台
安全运营门户		
信创环境部署	省级平台对接	50%性能冗余
高时效并发性		



省级建设
地市复用

地市新建

安全运营 服务内容	资产更新服务	安全专项服务	风险评估服务	安全加固服务	安全检查服务
	安全监测服务	安全保障服务	安全管理服务	安全事件跟踪	安全咨询服务
	安全应急、攻防演练服务		安全监督服务	安全培训服务	驻场运维服务

《国家智慧教育公共服务平台接入管理规范（试行）》 教科信厅函〔2022〕33号

- ◆ 接入国家智慧教育门户的平台应纳入教育部统一运行监测的范围，统一部署运行监测手段，通过对接方式自动获取用户访问、资源目录、使用评价、网络安全等方面的数据，建立基于大数据的平台评价机制。
- ◆ 教育部网信办建立平台网络安全监测预警通报机制，及时发现平台的网络安全隐患，并指导平台主管单位进行修复。定期组织智慧教育平台开展攻防演习，提升网络安全保障水平。平台主管单位应密切关注平台安全状况，发现平台运行故障、页面篡改等网络安全事件应及时按照《教育系统网络安全事件应急预案》进行报告，并采取有力措施及时处置，将影响降到最低。

《山东省教育信息化“十四五”规划》 2022.5

- ◆ 虽然我省教育信息化建设取得了显著进展，但由于顶层设计不够、资源投入不足等原因，存在基础设施支撑水平不足、优质教育资源供给能力较弱、信息化环境下教育教学模式创新不够、网络安全保障能力有待提升等问题。
- ◆ 持续完善网络安全防护体系，全面落实《网络安全法》《数据安全法》《个人信息保护法》等法律法规要求，严格遵循网络安全等级保护技术标准。重点保障教育系统关键信息基础设施，提升国产密码在网络安全防护中的应用水平，优先选用具有自主核心技术的安全可控产品和服务。推进教育系统全域网络态势感知系统建设，增强感知能力、保障绿色上网、推动可信应用，提升网络安全事件监测、研判、预警和应急处置能力。
- ◆ 提升省级教育网络和数据安全水平，健全基于全流量分析的安全监测处置中心，配齐用好网络安全设施设备，全面加强安全技术防范措施，开展数据全生命周期安全管理，保护教育行业关键信息系统和重要数据。定期开展全省教育网络安全检查和攻防演练，通过攻防对抗、沙盘演习等方式，提升网络安全防护能力和应急响应水平。

河南省教育厅《2023年教育信息化和网络安全工作要点》 教科技函〔2023〕99号

- ◆ 提升网络与数据安全水平。健全网络安全监测和事件应急处置体系。通过建立中枢、整合平台、对接数据等方式，扩大监测范围、提高监测深度，构建“一点发现、全网防御”的主动型网络安全防御格局，变单个学校独立防御为全省教育系统协调联动、联防联控。建立常态化网络安全应急响应及支撑服务团队，构建统一指挥、多级调度、协同处置的网络安全联动响应机制。常态化开展网络安全攻防演练。（责任单位：厅机关有关处室）

《中共陕西省委教育工委 陕西省教育厅2023年教育网络安全和信息化工作要点》 2023.3

- ◆ 完善网络安全防护体系。健全网络安全责任制，加强关键信息基础设施保护，开展信息系统网络安全等级保护工作。持续开展网络安全监测预警，完善全省教育系统网络安全通报机制，提升网络安全态势感知能力。建立智慧教育平台全天候保障机制，保障平台安全运行。加强教育数据全生命周期管理，探索建立健全数据分类分级管理制度，重点保护个人敏感信息和未成年人信息，维护教育数据主权。组织开展全省教育系统网络安全攻防演练，提升网络安全攻防对抗和纵深防御能力。深入开展委厅机关和教育行业国产化替代工作，摸清底账，制定替代工作方案和推进计划，开展检查督导工作。

项目时间	客户名称	预算金额	服务周期
2020年	xx市职业学院	148万	4年

项目背景

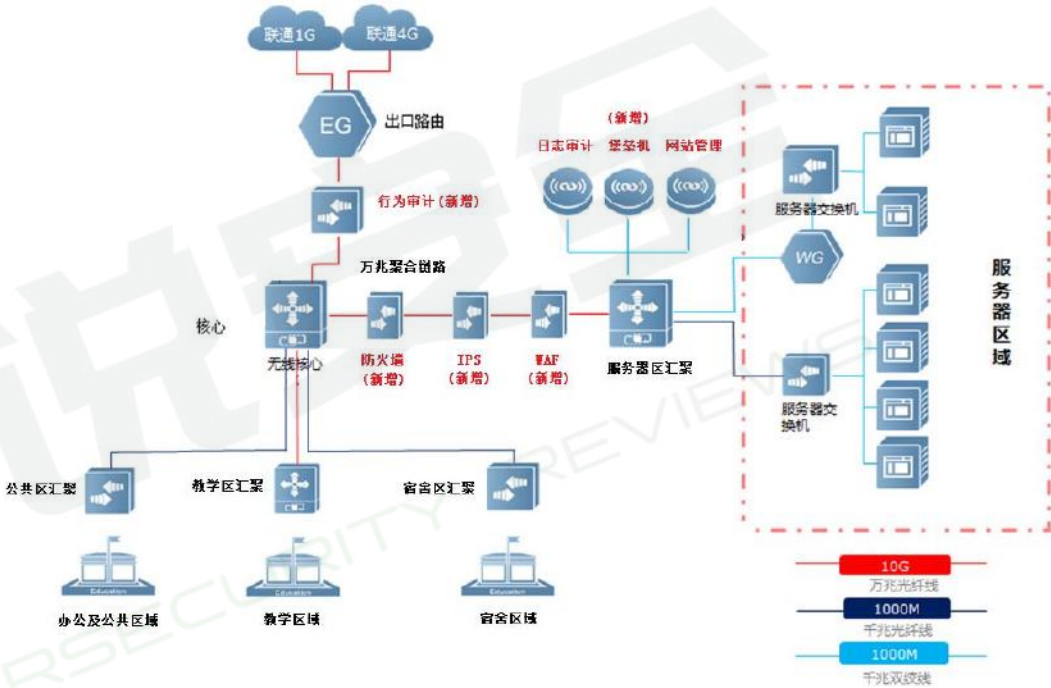
学校数据中心承载着我校大量的业务系统，如站群系统、数字化校园、智慧校园、一站式服务大厅等业务系统等，由于我校目前网络安全建设非常薄弱，缺乏有效的安全防护技术措施、安全管理制度以及安全审计措施，网络安全隐患越来越突出，随着国家实行网络安全等级保护制度2.0，依据《中华人民共和国网络安全法》，国家实行网络安全等级保护制度，我校需要实行网络安全等级保护制度，建设有效的安全体系抵御外来和内在的安全威胁，如安全漏洞、网站篡改、数据泄密等情况。

项目建设内容

据我校网络安全现状结合等保二级要求，完善校园网络安全建设，要求必须通过等级保护测评。第一由于缺乏专业的安全设备导致无法建立完善的安全防御体系落实网络安全等级保护制度。第二由于缺乏专业网络安全技术人员，导致安全工作落实不到位。介于以上情况，拟通过采购网络安全建设运营服务的方式落实校园网络安全等级保护建设与安全运维工作。在合同服务期限内，采购产品服务和安全服务：

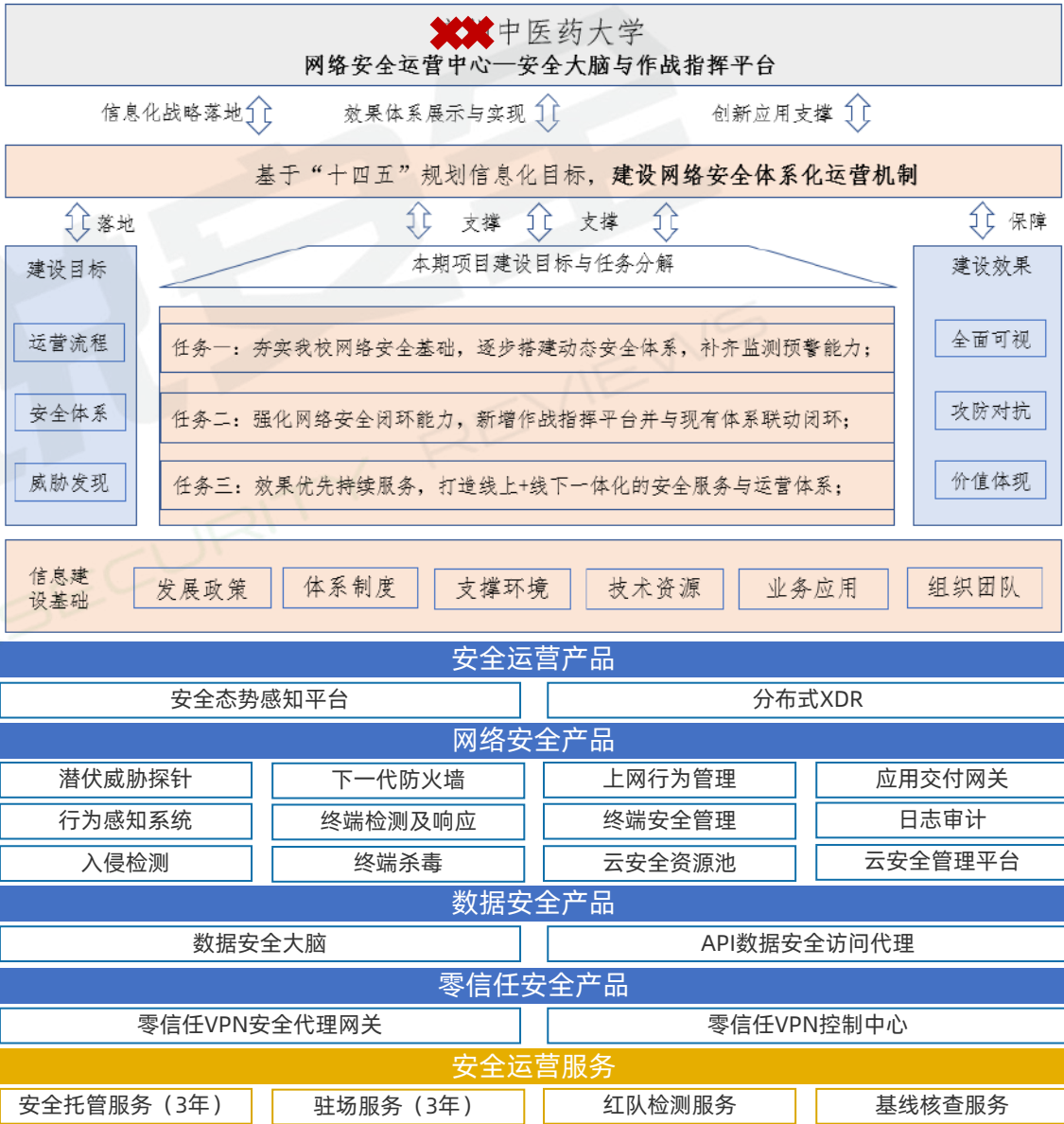
1、等保建设必要的安全设备实施部署、维护、升级服务，要求提供的安全设备必须保证校园网稳定运行，设备故障免费更换备件。

2、采购资产梳理、漏洞评估、安全维护、安全加固、网站监测、应急响应、安全预警等安全服务，并采购专职安全工程师5*8小时驻场服务。



产品服务需求		
防火墙边界防护服务（10G吞吐）	IPS入侵防范服务（10G吞吐）	Web安全防护服务（4G吞吐）
网站应用升级服务（100个网站）	上网行为审计服务（10G带宽）	堡垒机服务（100个资产）
安全日志审计服务（100个资产）		
安全服务需求		
资产梳理服务（12次/年）	漏洞扫描服务（12次/年）	渗透测试服务（2次/年）
安全加固服务（按需）	安全维护服务	网站监测服务（100网站）
安全预警服务（7*24）	安全应急响应服务（7*24）	重要时期安全保障（7*24驻场）
安全咨询与管理制度支持	安全培训服务（4次/年）	驻场工程师服务（5*8）

项目时间	客户名称	预算金额	服务周期
2022年	xx市中医药大学	4810万（IT+安全）	3年
项目背景			
xx中医药大学办学基础为创立于1924年的xx中医药专门学校，是新中国首批四所高等中医药本科院校之一。2020年成为xx省人民政府、教育部、国家中医药管理局共建单位。在未来，xx中医药大学按照国家高级标准学校，拟通过对校园信息化系统的全盘规划和统筹升级建设，从数字校园向智慧校园阶段迈进。所以学校应建立配套的常态化、长效化新型安全运营指挥技术和管理体系，通过自动化手段实现安全事件处置、隐患发现，完善应急指挥机制，建立设备资源、人力资源、管理资源之间的高效协同，对安全事件进行及时有效处置，实现统一的网络安全协同运营，保障学校网络安全稳定运行，业务系统持续安全运转。			
项目建设目标			
本次服务项目以学校服务器、核心业务系统等IT资产为保护对象，依据网络安全法、等级保护和相关标准规范，践行安全“实战化对抗、安全有效，由基本合规式安全转为实战化安全”的理念，定位于构建常态化的网络安全实战攻防对抗能力，同时围绕业务建设的驱动力，实现“体系合规、常态保护、实战有效”的效果。 第一，将以往经验式运维调整为针对学校业务风险针对性部署安全策略； 第二，强化学校网络防御基线检测，改变传统被动防御形式，加强高级攻击的检测能力； 第三，基于威胁可视性和运维自动化技术缓解当前阶段普遍存在的滞后式安全事件响应行为，提升学校日常安全运营效率。			



教育行业典型项目3-MSS安全托管服务项目集



项目时间	客户名称	客户类型	预算金额	服务周期
2023年	xx海洋大学	省属高校	18万	1年
采购需求				
30个主机资产7*24安全托管服务、7个自然日的重保服务、1次敏感数据泄漏监控服务、1次钓鱼演练服务、1次渗透测试服务（1次包含4个业务系统）、按需应急响应服务、4次主机和应用漏扫服务。				
项目时间	客户名称	客户类型	预算金额	服务周期
2023年	xx外国语学院	市属高校	28万	1年
采购需求				
供应商需在服务期内提供统一安全运营平台，主要服务内容包括：不限资产提供7*24威胁监测、7*24安全托管运营，自动化渗透测试工具订阅服务，重保现场值守服务，资产暴露面检测服务，应急响应服务。				
项目时间	客户名称	客户类型	预算金额	服务周期
2022年	xx大学	部属高校	10万	1年
采购需求				
采购数据中心安全托管服务，实现云端安全运营平台与学校现有安全态势平台、防火墙、主机安全检测平台联动对接，涵盖学校不少于50个IP资产7×24小时安全运营服务，服务内容包括：资产核查、资产安全评估、资产脆弱性与威胁管理、安全问题处置、重大活动和攻防演练保障。				

项目时间	客户名称	客户类型	预算金额	服务周期
2023年	xx城市学院	市属高校	45万	1年
采购需求				
7*24网站云监测云防护（1级域名≥ 6个、2级域名≥ 60个）、7*24威胁检测、流量威胁分析服务、态势感知运营服务、4次渗透测试和风险评估服务（20个以上系统）、1次应急演练服务、按需应急响应、2次安全培训服务、1人驻场服务。				
项目时间	客户名称	客户类型	预算金额	服务周期
2020年	xx学院	部属高校	49万	1年
采购需求				
网络运维服务（每季度开展定期网络巡检，网络故障响应，网络问题分析）、互联网安全托管服务（7*24网站防篡改监测和处置）、本地托管服务（每季度风险评估）。服务工具租赁：安全资源池（包含数据库审计、堡垒机、日志审计、漏扫与基线、SSL VPN功能授权）、全流量威胁分析系统、EDR（PC授权≥100、服务器授权≥25）、防火墙硬件维保与软件升级。				
项目时间	客户名称	客户类型	预算金额	服务周期
2023年	xx开放大学	市属高校	17万	1年
采购需求				
出口防火墙升级服务（升级智能化安全运营服务、云情报网关服务）、威胁检测运营平台服务（接入流量≥1500Mbps、接入端点侧数量≥50个、可容纳180天审计数据）、7*24安全托管运营服务（10个资产）				

《医疗卫生机构网络安全管理办法》 国卫规划发〔2022〕 29号

- ◆ 第二条：坚持积极防御、综合防护。充分利用人工智能、大数据分析等技术，**强化安全监测、态势感知、通报预警和应急处置等重点工作**，落实网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施。
- ◆ 第七条：各医疗卫生机构应依托国家网络安全信息通报机制，加强本单位网络安全通报预警力量建设。**鼓励三级医院探索态势感知平台建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判**，及时通报预警和处置，防止网络被破坏、数据外泄等事件。
- ◆ 第九条：各医疗卫生机构在网络运营过程中，应每年开展文档核验、漏洞扫描、渗透测试等多种形式的**安全自查**，及时发现可能存在的问题和隐患。针对安全自查、监测预警、安全通报等过程中发现的**安全隐患应认真开展整改加固**，防止网络带病运行，并按要求将安全自查整改情况报上级卫生健康行政部门。自查整改可与等级测评问题整改一并实施。
- ◆ 第二十六条：各级卫生健康行政部门应建立网络安全事件通报工作机制，**及时通报网络安全事件**。
- ◆ 第三十条：各医疗卫生机构应保障开展网络安全等级测评、风险评估、攻防演练竞赛、安全建设整改、安全保护平台建设、密码保障系统建设、运维、教育培训等经费投入。**新建信息化项目的网络安全预算不低于项目总预算的5%**。

《国家医疗保障局关于进一步深化推进医保信息化标准化工作的通知》 医保发〔2022〕 8号

- ◆ 各级医保部门要强化网络和数据安全组织领导，压实安全责任，统筹工作部署，建立健全网络和数据安全保护规章制度。加强网络安全智能预警能力建设，实时监测系统运行情况，提升安全威胁信息汇集和研判能力，加强网络和数据安全防护信息共享和通报预警。**推进安全运营管理队伍建设，强化日常监管，开展常态化医保数据安全专项检查，做好安全风险处置演练，做好重大活动期间安全保障，加快形成责任明确、层级清晰、保障有力的安全运营管理体系。**

《国家医疗保障局关于加强网络安全和数据保护工作的指导意见》 医保发〔2021〕 23号

- ◆ 到2022年，基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制。到“十四五”期末，医疗保障系统网络安全和数据安全保护制度体系更加健全，智慧医保和安全医保建设达到新水平。
 - ◆ 网络安全水平显著提升。主体责任明晰，监督管理机制完善，基础设施完备，网络安全技术能力、**态势感知、预警能力、突发网络安全事件应急响应能力显著提升**，网络安全有效保障。
 - ◆ 数据安全有效实施。数据安全审批制度全面建立，分级分类管理及重要数据保护目录全面落实，数据实现全生命周期安全管理，数据安全评估机制日益完善。
- ◆ 加强网络安全和数据保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施，**推进全国医疗保障信息系统网络安全和数据保护态势感知、预警能力建设。加强网络安全和数据保护信息的汇集、研判，建立健全网络安全和数据保护信息共享和通报机制，健全完善上下协同的通报预警机制。**

医疗卫生行业典型项目1-面向等保/关保的安全运维服务



项目时间	客户名称	预算金额	服务周期
2023年	xx疾控中心	80万	1年

项目背景

疾控核心业务系统始建于2003年，至今已建立起完善的国家、省、市、县、乡镇用户管理体系，先后建设了用户认证与授权管理系统、基本信息、基础编码、公共卫生数据交换服务平台等多个应用支撑系统，逐步完善了信息安全管理机制。2009年做了网络直报系统迁移改造，2019年启动了全民健康信息化保障项目疾控信息系统建设。已运行的核心业务应用系统覆盖全国各级各类医疗卫生机构，授权用户32.5万多人，系统要求7x24服务不中断稳定运行。同时建成了疾控中心本级及十一个直属单位的协同办公平台和各省级疾控中心节点。根据国家信息安全等级保护要求，xx疾病预防控制中心现有系统中的xx控制信息系统、协同办公平台等为网络安全等级保护三级系统，中心网站、公共卫生数据共享网站等为网络安全等级保护二级系统。

项目建设目标

供应商需配合xx疾控中心，按照《网络安全法》、《个人信息保护法》、《网络安全等级保护要求》、《关键基础设施保护条例》及《数据安全法》等国家法律法规相关要求，完善现有数据中心的安全运维管理，为xx疾控中心提供专业技术人员驻场，开展系统安全保障服务、态势感知平台驻场运维服务、国家重大节假日及xx疾控中心重大活动安全保障服务、攻防演练技术支撑服务、二线专家咨询服务、企业版防病毒运维服务、非法外联监控服务、安全培训服务。

系统安全保障驻场服务

提供合同期内5×8小时1名人员驻场服务(国家重大节假日及xx疾控中心重大活动安全保障除外)，协助采购人进行网络和信息安全管理，网络与安全设备安全配置策略维护、病毒查杀、安全设备运行状态检查、故障处置等事项，并对全年运维服务进行总结，编制《驻场安全运维服务总结》。

安全巡检服务	漏洞扫描服务	日志分析服务	应急响应服务
协助等保测评服务	互联网监控服务	堡垒机运营服务	

态势感知平台运营驻场服务

提供合同期内5×8小时1名安全运营人员驻场服务(国家重大节假日及xx疾控中心重大活动安全保障除外)，针对采购人现有的态势感知平台提供安全运维管理服务，包括：日常巡检、平台运行状态监控、系统升级、规则管理、知识库升级等工作内容、基础安全运营服务和二线专家技术支撑服务。依托态势感知平台开展资产管理、漏洞管理、威胁分析、预警通知等工作，通过持续开展运营工作可掌握数据中心的资产情况，及时发现面临的内外部威胁风险等。

资产管理	漏洞管理	告警监控分析	威胁分析
预警通知	日志解析	联动处置	二线专家技术支撑

国家重大节假日及xx疾控中心重大活动安全保障服务

国家重大节假日、xx疾控中心重大活动以及中心业务需要的重要信息安全保障时间内（不少于40天），需增派驻场工程师不少于1人，进行7×24小时驻场服务，协助采购人开展需要进行重点安全保障的任务，开展监控预警工作，及时处理各类信息安全事件，确保信息系统安全稳定运行。

攻防演练技术支撑服务

按照采购人攻防演练需求，协助采购人制定攻防演练工作方案，合理安排人员组建攻防技术团队，梳理安全措施有效性，排查安全风险和加固整改，组织攻防演练预演，以及在攻防演练过程中所需求的必要人员、技术支撑、安全检测等服务，演练结束后对演练效果进行总结并编写演练总结报告。

二线专家咨询服务	企业防病毒运维服务	非法外联监控服务	安全培训服务
----------	-----------	----------	--------

365*24热线电话---5*8内现场响应---5*8外15分钟响应、2小时到现场

医疗卫生行业典型项目2-网络安全运营（+数据安全治理）服务



项目时间	客户名称	预算金额	服务周期
2022年	xx医院（三甲）	120万	3年

项目背景

xx医院是国家卫生健康委员会直属医院，始建于1984年。现编制床位近2000张，集医疗、教学、科研、康复和预防保健等多项功能为一体，并承担中央保健医疗康复任务、国家卫生应急救援队任务，同时还是国家卫生计生委远程医疗管理与培训中心。

为更好地履行维护网络安全、意识形态安全和国家安全的使命，按照xx市和卫健委相关要求，开展网络安全服务建设工作，全面加强院内办公网络、信息系统的安全性，保障院内信息系统的安全稳定运行，提升医院整体安全防护水平。在安全运营建设过程中引入数据安全治理工作，保障医院数据的完整性、保密性、可用性。

项目内容

随着xx医院信息化业务的快速发展，业务系统日益复杂，业务关联性和架构复杂性、信息资产和数据总量逐渐增多，需要不断优化和提高安全能力，建立起持续运营的安全运营体系，从业务系统安全的角度出发，保障业务活动安全稳定。

乙方需结合甲方实际现状开展为期3年的安全运营体系建设与服务工作，使甲方具备在资产管理、检测与防护、威胁分析与响应、防御策略优化、威胁情报等方面具备相关能力，乙方需为甲方设计为期3年的安全运营体系建设规划。

同时在安全运营建设过程中引入数据安全治理工作，实现数据资产梳理、数据分类分级规范制定、数据分类分级策略、数据分类分级标识等。

网络安全运营服务要求

乙方应为本项目组建专职的服务团队，为甲方提供安全运营服务，甲方为本项目应至少配备专职项目经理、技术专家、3人驻场团队，项目组需具备相关能力资质证书、且具有在医疗领域参与安全运营项目经验。

服务交付

《漏洞扫描报告》	《渗透测试报告》	《新上线系统脆弱性评估报告》	《标准化管理制度》
《安全态势分析报告》	《安全通告及预警报告》	《安全运营月报》	《安全事件应急响应记录》
《安全保障期间工作总结》	《XXX安全培训》	《安全日志日报》	《安全日志及威胁分析月报》
《数据安全治理方案》	《季度工作总结报告》	《网络安全组日常工作规范》	《重保期间安全保障方案》
《新增和删除策略记录》	《安全运营工作手册》	《互联网暴露面检测报告》	《XX安全事件处置/溯源报告》
《XX应急演练方案》	《XX应急演练总结》	《攻防演练方案》	《攻防演练总结》

数据安全服务要求

数据资产梳理	针对xx医院业务范围不断扩大，数据类型逐渐复杂化情况，目前HIS系统、电子病历系统中存在海量的个人信息和健康医疗数据。医院需要通过相应的措施实现数据的分类分级管理，首先需要对数据资产进行统一的梳理，梳理HIS系统、电子病历系统的库表列信息，建立HIS系统、电子病历系统数据资产清单。
数据分类分级规范制定	为保证分类分级的顺利进行，需要建立分类分级规范指南，明确分类分级管理过程中各方责任、操作过程、原则和方法，形成可持续的分级分类业务指导要求。
数据分类分级策略	依据国家标准、行业标准，结合医院HIS系统、电子病历系统实际业务情况设计数据资产的分类分级策略，指导数据分类分级标记工作的展开。
数据分类分级标识	将数据分类分级指导方法进行实践，对HIS系统、电子病历系统开展数据安全分级，形成数据安全分级清单。

医疗卫生行业典型项目3-医保信息平台安全运营体系建设



项目时间	客户名称	预算金额	服务周期
2022年	xx省医保局	1148万	3年

项目背景

根据国家医保局《全国医疗保障系统核心业务区骨干网络建设指南》(医保网信办〔2019〕40号)和《xx省医疗保障局xx省政务服务数据管理局关于开展xx省医疗保障系统核心业务联网工作的通知》(x医保函〔2020〕106号)的要求,经过前期建设,省医保专网在2021年已初步建立。省医保专网采用树形网络结构,纵向由各级医疗保障部门按垂直的上下级模式连接成广域骨干网络,由国家医保局连接各省级医保局,并向下覆盖到市、县级医疗保障部门;横向以各级医疗保障部门为中心向同级信息资源共享部门辐射,并与医院、药店等相关单位连接,形成该级的城域接入网。

项目目标

针对省医保信息平台核心业务骨干网络的安全性和医疗保障数据防护要求,按照国家医保局“安全分区、网络专用、横向隔离、纵向认证”的原则,进一步完善纵向骨干网络结构安全、本体安全及基础设施安全,从终端安全、网络安全逐步提升省医保信息平台安全防护和安全运营能力。为满足国家医疗保障局对医疗保障信息平台的安全要求,本项目将协同省政务云平台医疗保障核心业务区共同构建云端-网端-终端的安全体系,推进省医保信息平台网络安全保护态势感知、预警能力建设。由省政务云平台提供云端安全保障,本项目提供终端和网端的自下而上的安全防护服务,实现省医保专网的安全防护和接入终端安全,同时通过安全运营服务,构建一套“技术先进、安全可靠、服务完备”的用户方安全运营体系,完全具备“威胁预警、协同对抗、可管可控”的安全运营保障能力,落实常态化的持续风险监控分析运维,结合省医保局的业务及防护能力情况进行7*24小时风险分析运营,避免发生安全事件产生重大影响。

基础设施服务要求

专业基础设施租赁服务	根据《国家医疗保障局关于印发加强网络安全和数据保护工作指导意见的通知》的网络安全指导意见,建立并完善省医保专网网络安全能力和接入终端安全保障,为省医保专网省节点租赁基于NFV、SDN、ATT&CK新型威胁分析、知识图谱和攻击链威胁分析及智能编排等新型技术的网络安全能力池。
------------	--

租赁系统要求

终端接入安全监控系统 (2套、网络层吞吐量3G)	下一代防火墙系统 (1套、网络层吞吐量3G)	网络入侵防御系统 (1套、网络层吞吐量3G)	网络防病毒系统 (1套、网络层吞吐量3G)
日志审计系统 (1套、150日志源、5000EPS)	全流量攻击溯源-文件监测系统 (1套、10万文件/天)	全流量攻击溯源-流量分析系统 (1套、检测能力3G)	全流量攻击溯源-威胁关联分析系统 (1套、检测能力3G)
蜜罐及欺骗统一管理系统 (1套)	集中预警展示系统 (1套、10000EPS)	一键威胁处置系统 (1套)	资产集中管理系统 (1套)

威胁情报分析系统(1套)

运行维护服务要求

针对所租赁的专业基础设施提供合同服务期限内3年免费维保服务(投标报价需包含相关费用),以确保安全基础设施稳定运行。具体包括设备故障保修、设备巡检、软件补丁、辅助故障定位等服务。

安全运营服务

安全规则/功能优化	日常实时安全监控	恶意攻击封堵处置
失陷事件专项排查	安全威胁预警及恶意样本捕获分析	重大活动保障专项策略调优演习协助
终端已知病毒查杀服务	终端新型病毒查杀服务	网络安全可视化服务

总体要求

数据与接口要求:本项目部署网络安全能力平台,采用私有云方式部署,网络安全能力平台采用虚拟化软件服务。为确保数据安全,网络安全能力平台与医保网络采用专线互联,并接入至现有的医保网络中,实现与医保网络核心区域的数据牵引、流量牵引和安全防护,并根据业务需求,输出业务所需要的外部数据和接口。
吞吐量要求:本项目规模涉及整个医保信息平台、服务参保人数共1.08亿、日均医保结算量120+万笔。需满足省级100个机构接入终端及支持21地市2万接入数量终端的流量分析,满足省医保专网50个网络设备及安全能力的日志分析。

医疗卫生行业典型项目4-MSS安全托管服务项目集



项目时间	客户名称	客户类型	预算金额	服务周期
2023年	县中医院	二级甲等	70万	3年
采购需求				
包括：20个资产授权的安全托管MSS服务3年（每年90000），EDR、安全感知管理平台、防火墙3年硬件维保与特征库、软件升级服务。				
项目时间	客户名称	客户类型	预算金额	服务周期
2022年	区医院	三级甲等	135万	3年
采购需求				
区医院外网等保三级建设项目拟采购链路负载均衡、下一代防火墙、安全态势感知平台、潜伏威胁探针、等保一体机、上网行为管理、隔离网闸、托管式安全运营服务（提供三年原厂服务）及测评服务（国家级测评机构）。MSS安全托管服务50个资产授权，中标价格180000（每年60000）。				
项目时间	客户名称	客户类型	预算金额	服务周期
2023年	大学附属医院	三级甲等	75万	1年
采购需求				
互联网资产发现服务（4次）、渗透测试服务（2次，每次30个应用系统）、漏洞扫描服务（4次）、风险评估（1次）、重要时期安全保障（HW、两会、国庆期间7*24服务）、威胁检测与响应服务（提供1个平台+2个探针、授权50个资产）、按需应急响应服务、网站7*24监测（5个网站）、红队评估服务（1次）、应急演练服务（1次）、策略优化和安管制度完善协助、主机安全加固服务。				

项目时间	客户名称	客户类型	预算金额	服务周期
2023年	省人民医院	三级甲等	30万	1年
采购需求				
服务期内针对xx省人民医院指定的至少20个系统开展渗透测试，协助院方进行漏洞修复并提供修复后的复测。提供1年MSS远程安全托管运营服务，资产授权≥100个，服务工具提供API数据接口，支持与其他平台进行对接。				
项目时间	客户名称	客户类型	预算金额	服务周期
2023年	省妇幼保健院	三级甲等	40万	1年
采购需求				
按照信息系统网络安全等级保护相关标准的要求，为xx省妇幼保健院提供为期1年的三级信息系统（5个）网络安全等级保护测评服务（1次）和7*24安全托管服务（10个应用资产），MSS后台监测系统必须支持与院方现有的态势感知系统进行流量对接。同时要求MSS服务支持通过SLA对安全事件服务水平、安全威胁服务水平、安全漏洞服务水平做出承诺。				
项目时间	客户名称	客户类型	预算金额	服务周期
2023年	市人民医院	二级甲等	76万	1年
采购需求				
安全风险评估服务（资产识别、基线核查、漏洞扫描、弱口令扫描、渗透测试）、安全加固服务（网络、主机）、云端安全托管服务（10个资产）、重保服务、安全培训服务、5*8安全驻场服务（2名一线工程师+2名远程二线工程师）。				

安全运营市场优秀项目案例

- ▶ 启明星辰---江苏无锡数据安全运营项目案例
- ▶ 深信服---某大型物流客户云网端安全运营项目案例
- ▶ 绿盟科技---某大型商业银行安全运营中心建设与服务案例
- ▶ 安恒信息---某知名三甲医院安全托管运营最佳实践
- ▶ 360数字安全---某制造业跨国企业安全托管运营服务案例
- ▶ 腾讯安全---某证券客户安全运营最佳实践
- ▶ 安信天行---省级政务云综合监管项目案例
- ▶ 众智维科技---某大型金融机构智能安全运营项目案例
- ▶ 星维九州---某企业托管式安全运营最佳实践
- ▶ 日志易---某银行信创安全运营与态势感知平台项目案例
- ▶ 长扬科技---全局管控、技管并重，构建某集团工控安全主动防御运营体系

基于国家数据安全要求，围绕政务云、政务外网及大数据中心，以数据安全技术保障为基础、以管理运营为抓手、以监测预警为核心、以协同响应为目标，全面建成城市政务数据安全运营中心，为中国政务场景下数据安全建设打出“样板”。实现：1、城市政府大数据中心数据资源分类分级覆盖率达到100%，实现敏感数据全局管控；2、城市大数据中心敏感数据100%实现安全存储与传输，实现数据管理从粗放向精细的转变；3、实现数据风险实时监控。

项目介绍



项目亮点

- 1、打造了中国首个政务场景下通过国标《数据安全成熟度模型》三级认证的城市政务数据安全运营中心；
- 2、成为城市政务数字化场景、数据安全、安全运营中心这三个业务方向的标杆和引领；
- 3、制定《市级公共数据分类分级实施指南》
- 4、获得：
 - (1) 城市大数据中心荣获中国信息产业商会人工智能分会“2019—2020年度数字政府建设卓越实践奖”；
 - (2) 无锡市公共数据开放平台获评贵阳数博会“2021数字政府管理创新奖”；
 - (3) 江苏省网络安全优秀实践案例。

深信服-某大型物流客户云网端安全运营项目案例

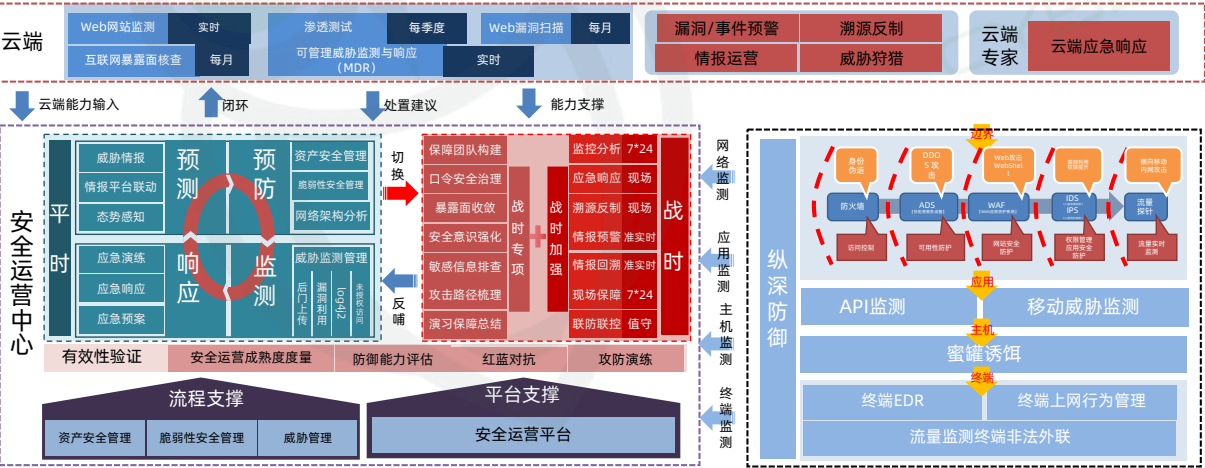


深信服科技股份有限公司成立于2000年，是专注于企业级网络安全、云计算、IT基础设施及物联网的产品和服务供应商，致力于让每个用户的数字化更简单、更安全。目前深信服在全球设有50余个分支机构，员工规模超过9000名。

深信服安全托管服务（MSS）通过云端安全运营平台和安全专家团队有效协同的“人机共智”模式，提升组织安全风险管控能力和安全工作效果，为用户提供持续、有效、省心、便捷的安全托管服务，一同构建7*24小时持续守护、有效预防和主动闭环的体系化安全运营能力。

项目介绍	项目亮点
◆ 项目背景 国家法律法规及行业监管要求明确要求邮政企业、快递企业应当按照国家网络安全等级保护制度的要求履行安全保护义务。随着攻防演练、安全监督检查的常态化，集团网络安全风险管理面临巨大挑战，曾发生多次安全事件并受到上级监管通报。 ◆ 客户痛点 1、网络架构复杂，网络安全管理难：大型物流企业业务体系庞大、分支机构众多。复杂的网络架构、繁多的资产、有限的时间精力让网络安全工作极具难度； 2、缺少专业运营人才，研判响应滞后：安全设备本身的配置和管理需要持续开展，企业缺乏专业人才，分析研判、响应处置能力不足，疲于被动响应； 3、攻击手法持续升级，难以对抗实战：企业对外业务系统多，暴露面大，而外部攻击手法持续升级变化，企业对新型威胁的检测处置不及时、难闭环，处于“攻防不对等”状态。 ◆ 方案设计 摒弃以往“缺人招人、缺设备买设备”的高投入、效果无法保障的安全建设方式，某物流企业选择与第三方专业安全厂商——深信服合作，选择以提升“安全效果”为导向的安全运营方案，导入MSS+SIP+STA+SAAS XDR(订阅) +EDR的云网端安全运营解决方案。	◆ 项目亮点： 在使用MSS期间在日常运营、威胁监测、攻击对抗多方面实现了安全效果的大幅提升，通过MSS从不间断的风险管控，实现风险“可知、可控、可管”。 1、7*24小时真守护，平均10分钟完成应急响应：两年服务期间内，主动响应并处置多起夜间攻击事件，平均响应时间10分钟。上线SaaS XDR及MSS 2个月后，帮助客户发现了一起“SQL注入-dnslog域名访问-外联下载bash-反弹shell-执行命令”事件，信息中心联动深信服安全运营中心，10分钟内还原整个攻击过程并完成应急响应、阻断攻击，处置闭环效率显著提升。 2、实战能力大幅提升，防守成绩优异：在多次重要时期、大型攻防演练的真攻真防下，MSS云端专家团队和信息中心默契协作、共同坚守下，没有任何一起攻击成功突破安全防线，最终取得了优异的防守成绩。

绿盟科技集团股份有限公司成立于2000年，总部位于北京，公司于2014年在创业板上市，是国内综合型网络安全厂商，公司客户覆盖政府、金融、运营商能源、交通、科教文卫等多个行业，可提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。近3年安全运营业务复合增长率超40%，安全运营服务在服客户超2000家。

项目介绍	项目亮点
◆ 项目背景： A银行为我国大型城市商业银行之一，随着网络安全逐年建设，A银行已完成基础架构安全建设，但是在日常安全运营过程中，依然有以下突出问题待解决： 1、安全设备种类多，日均告警上亿条，缺乏有效监测手段，安全事件难发现； 2、安全团队初建，人员能力不足，缺乏梯队建设，安全能力难以持续提升； 3、全工作没有整体规划设计，依赖个人经验和外部厂商能力，执行效果难保障； 4、安全工作涉及多个部门，依赖人工推动处置，效率低，处置难，风险长期暴露； 5、安全建设投入周期长，缺乏有效的量化评价手段，安全成效难凸显。 ◆ 建设方案： 通过安全运营中心建设，构建云地协同、平战结合安全运营体系，实现A银行安全运营工作规范开展，安全风险可管控，并借助有效性验证与运营优化，持续提升安全运营能力。 	◆ 项目亮点： 1、从无到有构建态势感知能力，核心区域监测100%覆盖 基于智能安全运营平台10000+检测规则，千万级病毒库，实现威胁集中监测，覆盖银行两地三中心三十余个安全区，安全风险一屏概览。 2、基于岗位定向开展人才培养，提升团队实战化能力 完成安全运营团队岗位架构及安全人员能力梯队设计（含5类运营岗位，3级运营专家），并基于岗位要求开展安全培训，构建实战化运营团队。 3、持续提升自动化能力，实现分钟级威胁检测与响应 贴合客户业务配置30多个SOAR剧本，实现威胁自动处置。封堵平均时间由建设之初的1.2小时下降至3分钟，整体MTTD降低至15分钟内。 4、执行效果量化可控，运营成果直观呈现 构建核心度量指标，结合安全运营成熟度评估与实战攻防演练，持续牵引安全运营建设，安全运营成熟度已提升至3级充分定义级别。 ◆ 客户价值： - 安全运营管理能力显著提升，实现安全风险可管可控，常态化到战时平稳切换。 - 威胁事件监测、处置能力显著提升，MTTD由以天为单位缩短至15分钟内，MTTR由48小时以上缩短至12小时内。

• 安恒信息-某知名三甲医院安全托管运营最佳实践



安恒信息成立于2007年，于2019年登陆科创板。安恒信息秉承”构建安全可信的数字世界“的企业使命，以数字经济的安全基石为企业定位，形成了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略，作为国家级核心安保单位，参与了近乎国家全部重大活动的网络安全保障工作，实现零失误。2020年11月23日，安恒信息正式成为杭州第19届亚运会网络安全类官方合作伙伴，这也是国际大型综合性赛事网络信息安全类最高层级合作。

安恒信息安全托管运营服务（简称：MSS）正式发布于2022年6月，目前拥有四个安全托管中心（杭州、北京、广州、西安），13个联合运营中心，为全国的政府、教育、医疗、企业、金融用户提供MSS安全托管运营服务。

项目介绍	用户收益
◆ 需求背景 XX市人民医院作为一家三甲医院，仅有运维人员，无法从专业视角分析海量的设备告警，安全设备始终无法发挥出全部价值。在发生安全事件时，缺乏及时有效的处置手段，无法确保事件均能闭环。自2023年起，医院再次加强对网络安全方面的投入，以增设态势感知平台+安全服务人员的方式提升安全水平。 ◆ 建设方案 1) 部署态势感知平台，对接云端安全运营中心，全网流量及安全日志实现统一汇集分析； 2) 部署资产与漏洞管理平台，持续开展资产与漏洞管理，安全检查工作常态化开展； 3) 引入外部安全服务专家服务，7*24小时实时进行威胁监测与响应。 	◆ 首月成果 1) 资产与漏洞深度管理：完成院内资产发现，梳理并录入资产与漏洞管理平台主机资产、域名资产、WEB资产共计5000余项、资产指纹信息24000余条（其中新增待确认主机资产400余台，WEB资产42项）。 2) 暴露面&攻击面管理：针对互联网资产：发现存在十余项高危指纹，协助收敛暴露面&攻击面并修复7个高危漏洞；针对内网资产，通过周期开展漏洞管理工作，共处置240余个高中危漏洞。 3) 安全事件快速响应闭环：发现并通报处理17起安全事件，包括3次紧急安全事件（挖矿病毒横向扩散、勒索病毒域名恶意通信、境外IP登录院内系统），均成功拦截并进行安全加固。 4) 自动化处置助力安全防护：完成8项响应剧本的编写与有效性验证，利用设备自动化处置能力有效提高了安全处置时效。

360数字安全集团(三六零数字安全科技集团有限公司)是数字安全的领导者，秉持“上山下海助小微”战略方针，以“安全即服务”为核心发展理念全面升级“360安全云”，将十多年被行业反复验证成功的数字安全运营体系框架，以云化服务化方式为国家、城市、大型企业、中小微企业构建应对数字时代复杂威胁的完整数字安全能力。

项目介绍	项目亮点
◆ 客户背景： 某中国500强上市公司是一家集制造、产品定制、产业互联网等为一体的国际化企业，产业分布在中国、美国、加拿大、英国、日本等多个国家。 ◆ 客户需求： 【需求一】利用360在互联网侧的能力 1.对企业部署在互联网侧的资产和业务进行梳理，找出非该企业的信息资产，特别是仿冒的网站及APP，同时协助企业对仿冒资产进行举报。 2.对互联网资产的漏洞进行排查，找出高危漏洞，并协助信息部门对漏洞进行修复。 3.对暴露在公共平台上与该企业相关的数据及暗网平台上涉及买卖该企业数据的行为进行排查。 4.对企业网站进行保护，防止网站被篡改。 【需求二】利用360的安全大数据和工程师能力 1.对办公网的攻击行为进行7×24小时监测，并协助客户完成威胁的处置。 2.对办公网的资产进行梳理，对漏洞进行排查，并协助信息部门对漏洞进行修复。	◆ 服务成果： 1.威胁事件发现率提高80%。 2.事件响应时间从30分钟降低到5分钟，业务流转效率提升500%。 3.事件研判时间从120分钟降低至20分钟，研判分析效率提升500%。 4.事件处置事件从96小时降低至24小时，处置效率提升300%。 ◆ 项目优势： 360数字安全运营服务基于360安全云在全网能力、运营平台、轻量探针、专家团队四大要素的优势，以及近20年积累的安全服务能力和攻防实战经验，帮助企业构建集合精准发现、及时响应、快速止损的一体化数字安全运营服务，真正做到为安全效果买单。 360 数字安全托管运营服务业务架构

腾讯安全作为互联网安全领先品牌，致力于成为产业数字化升级进程中的安全战略官。2023年，基于全球1500位CSO实战总结，腾讯提出了一套以“发展驱动”为核心的数字安全免疫力模型，助力客户构建数字安全体系，守护企业生命线！

腾讯SOC+智能安全运营与管理体系充分融合情报、攻防、管理与规划四大能力矩阵，包含NDR、SOC、威胁情报、安全数据湖四大产品矩阵，从安全形态、安全价值、安全思维等战略视角，更全面的审视安全问题，有效解决制约SOC建设过程中的诸多瓶颈问题。

项目介绍

◆ 客户业务诉求

近年通过实战攻防演练的方式来发现企业安全漏洞，提升企业安全防护能力的形式已经成为常规手段。企业也能够对抗中不断适应多种攻击手段，升级自身防护能力，并在最终的复盘中对攻击行动中的防御体系的识别、加固、检测、处置等各个环节进行审视，发现薄弱位置并进行优化。

该金融企业也是通过每年至少两次的实战化演练来促进网络安全建设。之前由于互联网暴露面还未完全收敛导致有部分高危组件对互联网开放，成为了防护的短板，通过实战化的演练发现问题，加速互联网暴露面收敛工作，通过把高危组件收缩至零信任网关，从而减少攻击面。

◆ 客户效果自述

基于企业对于安全建设工作的向基层落实以及安全能力的整体提升的需求，腾讯的安全运营中心可以建设集团化SOC方案，将其安全管理的能力输出并接入到企业安全建设流程中，通过集中集团的网络安全日志进行安全数据和信息集中统一管理、场景建设及事件闭环。

我们企业在安全运营能力建设方面有了更大的能力提升。我们企业本身业务范围比较广，包括投资银行、证券交易、融资租赁等等，同时也在积极地推进数字化建设，为客户提供更多样化、优质化的金融服务，这么多元的业务场景其实对自身的安全运营和管理也提出了挑战。

腾讯在安全给出体系（SOC+智能安全运营与管理体系），能够通过预测、防御、检测和响应实现安全事件的闭环，这跟我们企业的“主动响应和闭环”的安全工作理念是比较符合的。在实际落地过程中，腾讯的这套体系也有效帮助到我们的安全运营方面建设，特别是安全运营中心、安全编排自动化平台。

除此之外，腾讯安全做的一些关于ATT&CK的前沿技术研究，其实也给我们企业的攻防能力带来了启发和参考，同时以产品的形态让企业能够轻松地接入一些前沿的安全能力，真正帮助企业提升自身的安全水位。

通过腾讯的专家对安全运营深刻的认识，来建设丰富的安全场景，展现安全态势，从而帮助公司提高威胁检测能力，加快响应速度，赋能我们企业数字化能力。



[illegible]

3. 为云服务商考核审计, 使用单位效能评价提供决策依据。

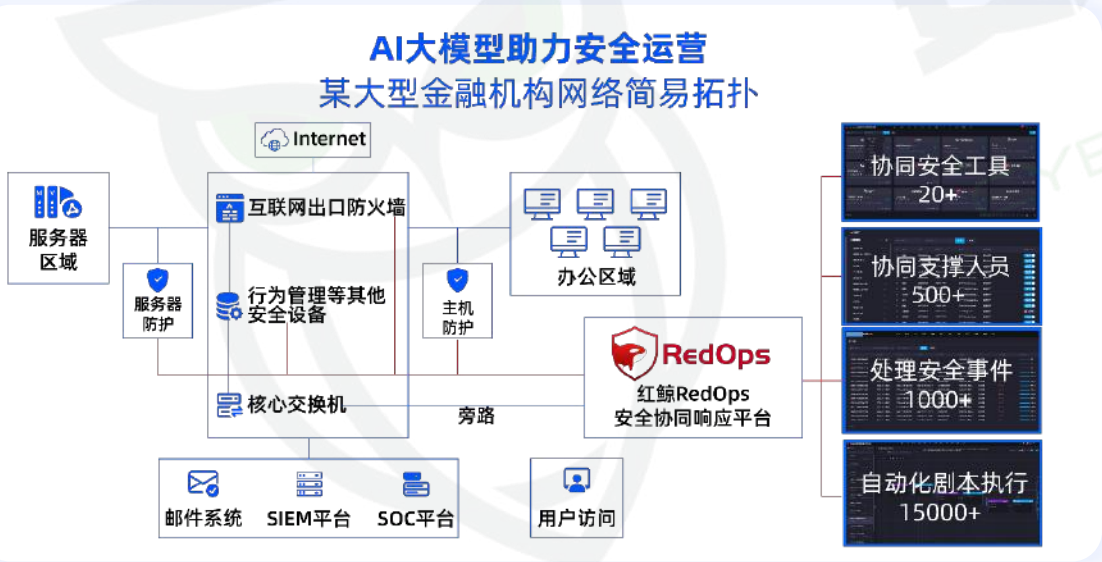
南京众智维信息科技有限公司位于金陵南京，是以国内知名的麒麟安全实验室（原OPENX实验室）为基础建立的新一代人工智能+机器学习驱动的网络安全运营解决方案商，拥有20+发明专利，50+软件著作权。公司深耕AISecOps赛道，将机器学习、自然语言处理和深度算法学习等技术应用于**企业级、城市级安全运营，重保对抗，协同作战**等场景，目前已与200+高质量客户达成合作与签约，覆盖金融、政务、运营商、能源、军工等行业龙头客户。

项目介绍与核心价值

◆ 需求背景

- 1.IT规模复杂且安全设备异构，1W+台安全设备及上百万台生产服务器。
- 2.长期面临合规及红蓝实战，承受重保期间现场600+作战人员管理压力。
- 3.日常安全事件处置过度依赖人工，重保对抗期间强度大、时间长。
- 4.企业安全网格、云化成熟，管理者对网络安全运营实战化发展定位明确。

◆ 建设方案



◆ 方案价值

- 1.构建企业级安全运营中台管理+网格运营化，摆脱安全“孤岛”困局。
- 2.全自动完成运营/重保场景下企业90%以上任务，降本增效显著。
- 3.全程AI辅助MTTR/MTTD考核，贯穿人-产品-流程实现重保“0”失分。
- 4.实现大规模企业级安全运营300+编排流程、600+人员、上百万IT资产。

◆ 方案成效

RedOps
红鲸RedOps
安全协同响应平台

- ✓ 重保、护网场景下自动化处置率90.3%
- ✓ 重保、护网场景下平均处置事件7s
- ✓ 沉淀多套内部安全运营经验
- ✓ 有效解决全局资源组织问题

AI机器人辅助运营决策、总结及作战墙知识图谱化

山东星维九州安全技术有限公司是以MSS\MDR（托管式安全服务）为核心业务方向的新型网络安全服务商和安全运营服务装备供应商，结合国内客户需求及业务特点，打破传统安全的纯产品交付模式，以安全数据不离场的方式帮助客户建立基于持续监测的安全运营体系以应对动态威胁。目前已接入大中小200余家远程服务客户，为客户监测业务数量26000+，监测IP数量11000+，日监测发现安全漏洞500+，累计监测发现漏洞421472个。星维安全运营中心依托中心侧安全运营支撑平台SOSS体系与客户现场侧前哨服务系统，通过安全运营分析用例、安全运营剧本、标准化运营流程调度一二三线安全运营分析师，以安全数据不离场的方式帮助客户完成资产安全治理、暴露面分析、威胁管理服务、脆弱性管理服务等标准化安全服务工作。

项目介绍	用户收益
◆ 需求背景 XX集团作为一家地方性的大型国有企业，近年来一直致力于数字化转型，作为支撑数字化建设的关键基座，网络安全建设是数字化转型的必由之路，目前企业网络安全方面存在以下短板：一是尚未建立动态信息资产管控机制。二是缺少统一安全监测预警和处置响应能力，缺少网络安全统一指挥和决策调度，难以及时发现处理出现的安全事件。三是网络攻击日益频繁，单靠自身力量难以形成全面防护，需协同多方力量共同应对。 ◆ 建设方案 1) 威胁管理运营服务(MDR)。包含威胁监测、事件分析与处置、安全机制有效性验证等服务内容，为用户提供持续性整体风险管理服务； 2) 脆弱性管理运营服务(MVA)。包含攻击面管理(ASM)服务、专项安全测试、专家安全测试、业务安全监测及安全意识评估等服务，通过不同服务的组合，针对性的提供有效的脆弱性管理能力； 3) 安全运营支撑服务。通过引入安全运营服务网关、资产探测、热点漏洞扫描等安全运营支撑工具，辅助安全运营工作的闭环管理。	◆ 运营成果 1) 资产与暴露面管理 资产管理10次，运营期间共计下线业务系统21个，上线业务系统24个，最新运营资产为196个 2) 脆弱性闭环管理 弱密码管理6次，共计发现2个业务系统存在弱密码账号59个，已全部完成整改；进行漏洞管理6次，共计修复高可利用漏洞81个，一般漏洞5个，剩余38个高可利用漏洞和42个一般漏洞修复中。 3) 威胁闭环管理 内外部威胁管理共计10006次。外部威胁分析进行9547次攻击对抗，策略调优6次，累计永久封锁恶意攻击源70次；内部威胁分析处置489次，隔离处置恶意病毒16起，信任文件27起，运营期间累计阻断恶意外连行为446起。

◆ 运营成果

1) 资产与暴露面管理
资产管理10次，运营期间共计下线业务系统21个，上线业务系统24个，最新运营资产为196个

2) 脆弱性闭环管理
弱密码管理6次，共计发现2个业务系统存在弱密码账号59个，已全部完成整改；进行漏洞管理6次，共计修复高可利用漏洞81个，一般漏洞5个，剩余38个高可利用漏洞和42个一般漏洞修复中。

3) 威胁闭环管理
内外部威胁管理共计10006次。外部威胁分析进行9547次攻击对抗，策略调优6次，累计永久封锁恶意攻击源70次；内部威胁分析处置489次，隔离处置恶意病毒16起，信任文件27起，运营期间累计阻断恶意外连行为446起。

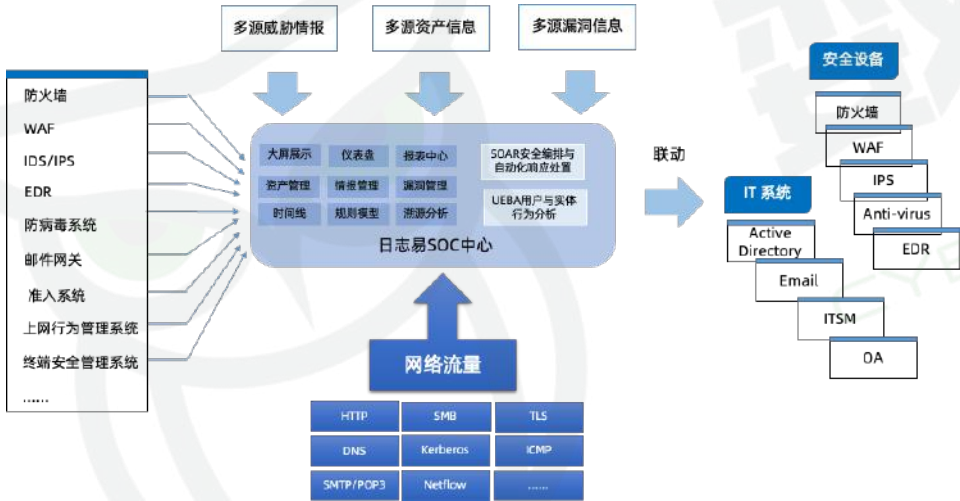
日志易-某银行信创安全运营与态势感知平台项目案例



日志易是国家级专精特新“小巨人”企业，国内领先的日志管理与分析平台开发商，基于自研搜索引擎Beaver和搜索处理语言SPL推出SIEM安全大数据分析平台、数据工厂（安全数据治理）、日志审计一体机、SIEM、UEBA、SOAR、安全态势大屏等安全系列产品，实现安全分析、威胁检测与响应、用户异常行为分析以及态势感知等场景，已服务金融、能源、运营商等重点行业近1000家大型机构。

项目介绍

某银行是国内最大的股份制银行之一，交易数据量大，并具有高度敏感性和价值性，对于网络安全、数据安全的重视程度远高于其他行业，其信息化建设的先进度也走在国内前列。日志易安全SOC运营中心作为行内唯一的安全运营中枢，帮助其实现了多种安全设备数据源的实时检测分析，以及跨不同来源关联分析挖掘潜在威胁的能力，建设以来为客户实现了护网0通报。同时，项目经验也成功复制到国内多个大型金融机构，形成了完善的安全运营平台及配套运营服务解决方案。



- 监测：通过SIEM进行威胁检测，**实时发现威胁**，并与威胁情报平台（TIP）进行关联，**提高告警精准度**；
- 分析：通过从NDR以及EDR对安全事件展开取证分析，**确认、追踪可疑攻击以及异常行为**；
- 响应：以SOAR为驱动，联动阻断设备/系统（抗D/边界防火墙/WAF/AD/堡垒机），对发现的安全事件进行响应（**封禁IP/锁定账户/其他**）

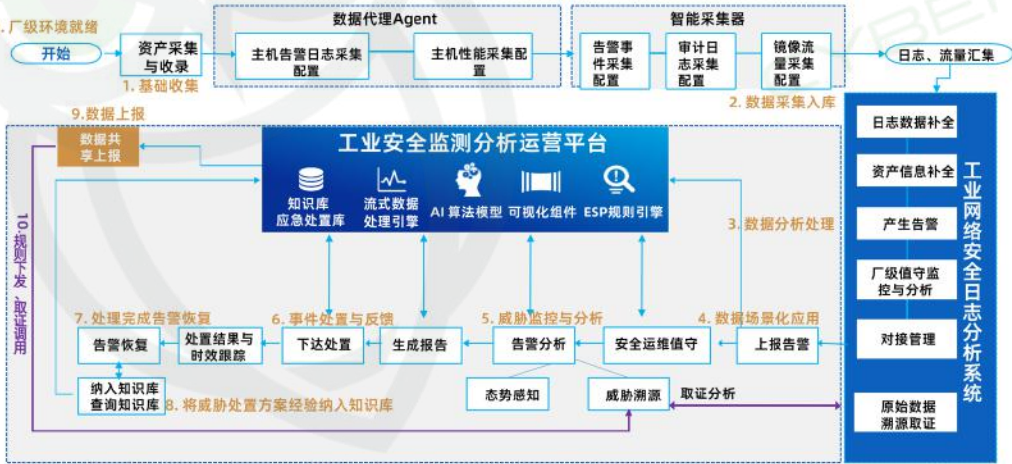
项目亮点

- **自研搜索引擎**：PB级存储搜索，**100亿**级别日志量**秒级**搜索。
- 数据解析能力**行业领先**：**支持数百种数据源**自动解析接入，内置数十种解析引擎，对于非内置解析规则的全新数据源做到快速解析。
- **Flink规则引擎**：分钟级创建并启用新监控规则。
- **SPL规则引擎**：对标Splunk，**300多种**函数、指令，支持复杂检测模型构建，大时间跨度数据分析。
- **丰富完善的威胁狩猎功能**：网络层取证、端点层取证、攻击链、时间线、溯源分析等。
- **数千个规则模型沉淀**，数十个成熟SOAR剧本，帮助用户一站式解决从威胁检测到响应的各种难题。
- **信创国产替代**：国内**最接近Splunk的国产化替换产品**，**信通院唯一认证信创日志分析平台**，已实施多个落地案例，无缝替换，更符合国内用户使用习惯。

使用前	使用后
每天人工搜索攻击次数较多的 十数个IP 查询威胁情报后处置，延时性和随机性都很高。	将 所有 安全设备的告警结合威胁情报进行分析，并运用 自动化剧本 处置， 一分钟 内处置完。
只能关注 高危 的漏洞攻击事件。	可以实现 所有等级 安全事件的分类处置。
精力有限， 选取个别 比较信任的设备数据进行查看。	将所有购入设备数据都 整合 在SIEM平台上，只需关注SIEM平台即可掌握全局安全情况。
每天 2、3千条 告警量，根本不可能每条核查。	通过SIEM对告警聚合、关联规则，告警量下降至 数十条 甚至更少。

长扬科技（北京）股份有限公司是一家国资监管下、市场化运作，专注于工业互联网安全、工控网络安全和工业互联网+安全生产的国家高新技术企业，公司以信创安全操作系统为安全底座，以工业安全靶场为能力提升手段，自主研发了近百款产品，构建工业互联网安全产业完整生命周期的集团级工业网络安全保障体系，广泛服务于电力、石油石化、轨道交通、城市市政、智能制造、钢铁冶金、教育等行业超过4000+家工业企业，满足等保2.0及关键信息基础设施安全保护条例要求。

项目介绍	项目亮点
某集团是以肥料、精细化工、新材料为主业的国有综合产业集团，长扬科技为其构建工控安全主动防御运营体系，落实集团网络安全制度要求，加强工控资产合规管理，实现基于网络安全态势感知的持续监控和分析，为集团及下属企业构建一个全局的、实时的、可预测的网络安全运营体系，全面提升集团的工控网络和信息网络的安全威胁监测感知与应急处置能力，让网络攻击和安全威胁无处遁形。 ◆ 解决方案： 1、安全规划方面，围绕集团和首批13家下属企业，依据“总体规划、分步实施、技管并重、适度防护”原则，深入一线调研，制定集团总体工控安全建设规划、工控安全集团标准，避免下属企业重复建设，投资浪费； 2、解决方案层面，通过技术、管理、运营三者结合，打造满足等保、分类分级、关保等监管要求，并通过持续运营，为智慧工厂的长期稳定发展保驾护航。	摸清家底 认清风险 加强集团工业网络安全集中管控能力，全面梳理集团下属企业的关键信息基础设施工控系统资产现状，查找安全漏洞，排查安全隐患与风险，切实增强工控系统网络安全管理水平及防护能力，提升了集团对全局工控系统资产和信息安全风险的管理水平。 纵深防御 联防联控 增强各企业对工业控制系统网络行为的合规性识别能力，切实提升集团工控系统安全检测与预警能力。实现工控网络安全风险实时感知、威胁精准研判，提升了集团网络安全整体防护水平。并通过内外部多级联防联控技术，提升了集团工控及网络安全应急响应与处置能力。 安全运营 降低安全威胁 通过构建集团级纵深防御与监测预警能力体系，有效改进工控资产管理手段，提高了工控网络安全运维与运营水平，有效的降低了网络攻击给企业带来的安全威胁和经济损失。 行业标杆 护航集团成为保障粮食安全的国家队 本项目对全国化工行业、全省众多企业将起到良好的带头示范作用，引领行业进步，促进相关标准的推进。制订的企业标准规范填补了省化工行业工控安全防护企业标准的空白，其考核标准更具有科学性，集团的工业互联网安全保障体系可护航集团公司发展成为保障粮食安全的“国家队”。



项目系统架构图

安全运营市场总结与发展趋势

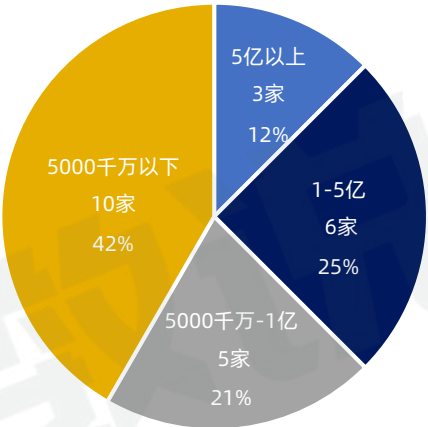
- ◆ 安全运营领域法律法规健全、政策利好明显，企业开始重视并推进安全运营体系规划与建设，安全运营已成为网安产业发展的重要方向。
- ◆ 近五年，国内安全运营市场快速发展，典型安全运营产品和服务过去五年市场复合增长率分别超过50%和70%，特别在最近三年特殊时期，安全运营市场表现出强劲逆势高增长态势，在整体网安市场发展起到了非常显著的带动作用。
- ◆ 安全运营需求增长推动安全运营技术发展进步，目前海内外公认、成熟的安全运营类技术已多达二十余种，在这些技术中，有一些是针对传统能力的升级，有一些则是拓展了新的安全视角，从实际项目来看，这些技术已经逐步被客户接受，实际应用程度在快速上升。
- ◆ 在目前安全运营市场初期发展过程中，仍然存在值得关注的问题，解决这些问题将更利于市场未来更有序、均衡的发展：
 - ◆ 中高级安全人才短缺对安全运营市场供需两侧产生一定制约。技术与产品提升安全水平，但安全人才决定最终效果。培养中高级安全人才对于实现人机共智、确保安全运营效果至关重要，这是安全运营市场可持续发展的关键因素。
 - ◆ 异构安全生态和低开放性对企业安全运营构成较大挑战，解决之道在于积极倡导开放的生态理念，建立标准和接口，促进不同安全产品的互联互通，从而提升企业安全运营的效率 and 效果，真正帮助企业实现安全运营工作进步与提升。

- ◆ 安全运营相关法律法规、行业垂直政策以及实网攻防活动的持续发展，从未来五至十年长周期看，安全运营体系建设将成为企业安全能力提升过程中的核心任务之一。这一趋势将进一步推动安全运营产品和服务市场需求的快速增长。
- ◆ 安全运营发展离不开技术和模式的迭代升级，以下方向的创新，将引领安全运营市场未来发展趋势：
 - ◆ AIGC在安全运营领域的深化应用。AI与安全运营的结合已经受到行业内高度关注，与AI+威胁检测不同，AI+安全运营可以实现快速的效果转化。ChatGPT最新成果所展示AI能力的巨大进步，会引起AI在网络安全运营的一系列尝试，并且结果可期，目前国内厂商已经在快速拥抱AI，并在AI助手、AI知识库等基础上向AI+告警降噪、AI+攻击溯源方向演进。
 - ◆ 将网络安全度量方法整合到安全运营体系中，以定量评估安全性能、风险和防御能力。这有助于企业及时发现自身问题，确保安全防御体系始终处于最优的姿态。在安全运营体系成熟后，网络安全度量将成为安全运营能力提升的重要方向，金融行业已积极探索在网络安全度量方面的应用。
 - ◆ 安全运营服务SECaaS模式的探索与应用。国外安全运营服务通过SECaaS模式创造巨大市场，但国内由于信任机制和安全制度差异，SECaaS模式应用范围受限，安全运营服务规模化发展始终面临较大挑战。在这个过程中，国内厂商开始采用在保证安全数据可控的情况下，开展行业或区域专属安全运营服务。未来国内安全运营服务市场SECaaS模式的发展路径和模式演变非常值得关注。

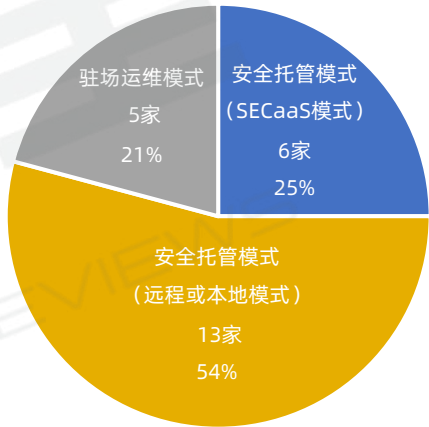
附录-安全运营厂商调研情况

- ◆ 安全运营业务收入过亿的企业全部为综合型安全厂商：该收入指以服务为主形成的安全运营业务收入，不包括单独销售的安全运营类产品。目前收入超过1亿以上的企业有9家，全部为综合型安全厂商，具有成熟的安全运营业务模式和安全运营产品，同时也具备规模化销售渠道和服务交付网络。产品型或服务型企业安全运营收入目前均没有超过亿元。
- ◆ 近90%的安全运营厂商过去3年业务复合增速均超过20%：在过去3年特别时期，市场中绝大多数企业能保持20%以上增长，是非常不易的，既印证了市场需求的火热，也说明安全运营是稳定、具有发展潜力的赛道。
- ◆ 安全运营服务由驻场运维向安全托管模式转型，但SECaaS模式目前还未成主流：出于客户需求和自身业务发展考虑，国内以驻场运维为企业开始考虑向安全托管模式转型，而在近80%开展安全托管服务的企业中，只有25%的企业采用SECaaS为主的服务模式，大多数企业仍以本地托管或本地+远程混合托管模式为主。
- ◆ 安全运营平台是企业开展安全运营业务的必备基础：无论哪种服务模式，安全运营平台都被企业看作是提升安全运营服务效率和价值的最重要支撑，90%以上的企业目前均研发了安全运营平台产品。

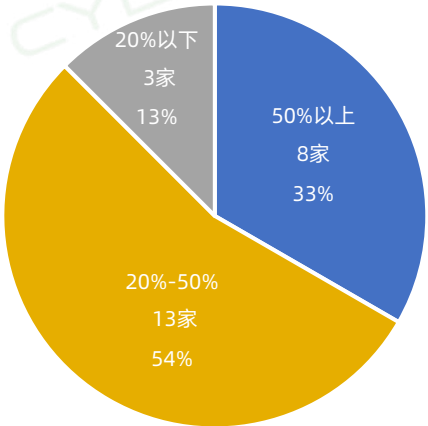
被调研企业2022年安全运营业务收入



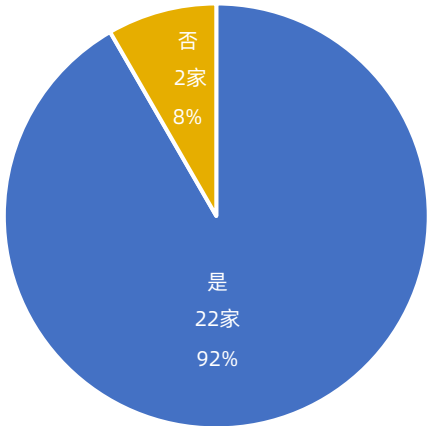
被调研企业安全运营业务主要服务模式



被调研企业2020-2022年安全运营业务年复合增长率



被调研企业是否自研安全运营平台 (SOC/SIEM/XDR/态感)



调研企业	安全运营业务简介
	作为“独立第三方安全运营”首倡者，启明星辰集团北斗立方安全运营中心围绕智慧城市以及关键基础设施行业客户对安全运营的迫切需求，为政务云、数据中心、关键信息基础设施及其他行业 and 中小企业提供安全运营中心建设及安全运营服务。根据不同用户的需求和建设进度，运营中心可加载如标准化远程/现场网络安全监控、数据安全运营、云安全运营、安全咨询和培训等运营业务模块，构建可持续扩展和装载新业务内容的安全运营模式，如：大数据AI安全运营中心、数据安全运营中心、云安全运营中心、工业互联网安全运营中心、态势感知运营中心、内网安全运营中心等。
	深信服安全运营中心建成于2018年，是国内较早的商业化云端安全运营中心。深信服安全托管服务（MSS）以网络安全“持续有效”为目标，围绕资产、漏洞、威胁、事件四个风险要素，通过云端安全运营平台和安全专家团队有效协同的“人机共智”模式，提升组织安全风险管控能力和安全工作效果，为用户提供持续、有效、省心、便捷的安全托管服务，一同构建7*24持续守护、有效预防和主动闭环的体系化安全运营能力，实现可视化、可衡量、可承诺的安全效果。目前深信服已建立面向教育、医疗、政务、企业四大行业的安全运营中心，在线服务客户数达到数千家。
	绿盟科技开展云安全运营、企业安全运营与城市级安全运营业务。云安全运营基于绿盟科技T-ONE CLOUD平台为企事业单位提供网站监测、网站云防护、威胁检测与响应、外部攻击面管理等订阅式安全运营服务。企业安全运营通过咨询规划、成熟度评估、平台建设、威胁建模、自动化编排等过程，结合云地数据协同方式，为客户达成全面的企业级安全运营能力。城市级安全运营则聚焦云计算、大数据、物联网、工业互联网等场景，从规划、实施到落地，帮助客户构建云-网-端体系化安全防护，并同步建设城市网络安全管理体系与运维体系，实现城市网络安全闭环运营管理能力。
	安恒安全托管服务（MSS）是利用安恒信息自主研发的安全托管运营服务平台，以用户资产全生命周期的安全需求为导向，参考IPDRO框架，将专业化人才梯队、标准化运营流程、智能化安全运营平台深度结合，从资产管理、攻击面管理、漏洞管理、威胁狩猎和应急响应五大核心攻防对抗域持续提供7*24主动、有效闭环的安全运营保障。安恒信息目前可以提供种安全运营服务模式，包括SaaS模式MSS服务、智慧城市安全运营服务、企业本地/远程安全托管服务等，目前累计服务客户数已接近上千家。
	奇安信安全运营服务是从客户业务视角出发，同企业安全部门共同进行安全运营架构、包括运营组织搭建，事件响应流程，运营平台及工具进行设计，通过外购或自研安全运营、流程管理等平台及设备、规划对应的工作场地，开展7x24小时的安全监测、综合分析、事件预警、深度分析、应急响应等服务，为客户侧的网络安全提供了有力保障。在圆满完成了北京冬奥会和冬残奥会网络安全保障工作，兑现了北京冬奥网络安全“零事故”的承诺后，对客户提供全面安全保障的能力又得到了大幅度的提升，并且将成功经验广泛复制。
	安信天行立足全局，植根行业，以提供专业的网络安全服务为核心，依托丰富的服务经验，以城市级安全运营中心为纽带，畅通技术与管理之间的鸿沟，赋能区域行业伙伴，实现深度化运营、全方位支撑、一体化交付等能力，建立从监视、预警、分析、运维、处置的安全闭环流程，构建综合服务平台和技术支撑平台，以权威的安全服务资质和专业化安全服务团队，提供体系化、全面化的安全运营保障服务，共建安全运营体系，为政务、卫生、纪检、教育、广电、企业等各领域千余家单位信息化建设保驾护航。

调研企业	安全运营业务简介
	“360数字安全托管运营服务”依托360安全运营数字化协作平台，将360云端数据、专家、能力、探针等建立多维度连接，为客户提供7×24远程安全实时监测，帮助客户“摸清家底、感知风险、看见威胁、处置攻击、提升能力”，实现安全事件全程可见、可管、可追溯。该服务可向用户提供弹性、持续化的安全服务，应对高级威胁。“360数字安全托管运营服务”基于被国家、央企客户验证有效的“360数字安全框架”，为用户提供强大的云上数字化安全运营平台。
	“SOC+安全运营体系”是腾讯安全面向产业数字化转型推出的新理念，强调以威胁情报运营和攻防对抗为基础，构建起“情报-攻防-服务-生态”的闭环安全运营体系。目前，腾讯SOC+集成了TIX威胁情报中心、SOC安全运营平台、NDR网络威胁检测与响应、MDR安全运营服务四大产品矩阵，可支撑政企机构建立起技术、人员、流程一体化的安全运营体系，全面提升安全防护能力和安全运营效率。
	星维九州是以MSS\MDR（托管式安全服务）为核心业务方向的新型网络安全服务商和安全运营服务装备供应商，通过建立专业的安全运营团队，依托中心侧安全运营支撑平台SOSS体系与客户现场侧前哨服务系统，通过安全运营分析用例（USECASE）、安全运营剧本、标准化运营流程调度一二三线安全运营分析师，以安全数据不离场的方式帮助客户完成资产安全治理、暴露面分析、威胁管理服务、脆弱性管理服务等标准化安全服务工作。目前已接入大中小200余家远程服务客户，覆盖金融、医疗、数字政府、企业等客户。
	日志易始终将自主创新作为公司可持续发展的核心战略之一，以对标SIEM领域巨头Splunk为目标，坚持研发自主可控的大数据分析技术，作为信创工委大数据组组长，在国产化适配互认与产品自主可控方面具有领先优势。日志易安全运营中心基于自主开发的纯国产搜索引擎Beaver，支持100亿条日志量级秒级检索返回，为用户打造集数据采集解析、规则预警、关联分析、威胁处置等全流程于一体的人工&自动化运营闭环。至今已积累了金融、制造业、高科技等多个垂直行业头部客户大型安全运营中心案例，并获得客户高度认可。
	长扬科技基于对国家工业互联网安全相关政策、法规与标准的持续研究和深度解读，总结超过32个行业领域、4000余家工业企业的安全服务经验，分析各行业、全场景业务流程和网络安全实战化需求，打造出一套“一站式、全行业、定制化”的工业互联网安全服务体系，体系涵盖安全咨询规划、安全实施交付、大安全运营和安全培训4大类、27项标准化服务产品，满足用户在合规咨询、顶层规划、方案设计、评估检查、安全加固、安全运营等方面的网络安全服务需求，并且基于用户不同的网络安全服务需求，提供模块化的服务组合。
	众智维科技以国内知名的麒麟安全实验室为基础，以AISecOps为核心理念，将机器学习、自然语言处理和深度学习等AI技术应用于安全运营，发展至今已形成智能化企业安全风险、安全资产管理、安全日志管理，以及安全自动化响应、自动化编排和自动化安全运营等15款模块化产品。依托国家级信息安全课题建立了众智维安全运营中心，以南京为中心辐射全国，为企业客户提供7*24安全托管和安全运营服务，实现“人+产品”的整体托管解决方案，帮助客户在安全运营方面实现降本增效。

调研企业	安全运营业务简介
 数字化解决方案领导者	新华三以主动安全3.0为理念，基于一切皆服务(XaaS)，以业务运营为驱动，打造涵盖“按需订阅、云上托管、交钥匙服务”等特色的新一代新华三云端安全运营中心。综合技术、流程、人员和平台等多个因素，通过技术手段和人文管理相结合的方式，实践出“咨询先行、能力交付、保险托底”的最佳运营模式，并逐步推出三层金字塔的业务模型，包含云端安全运营服务、行业级安全运营服务和城市级安全运营服务，覆盖百行百业，使企业安全防范体系更加完善、可靠和高效，助力企业实现降本增效。
	中国电信安全公司将云网资源禀赋与安全标品融合，打造出具有差异化优势的MSSP安全托管服务，形成了全网采集、全程防护、内外溯源的一体化解决方案。此方案通过对海量探针上报的日志进行降噪优化，算法训练得以迅速提升，有效保障关联分析结果的准确性。在响应处置环节，通过大量且较高的剧本命中率，专家无需进行二次研判工作。此外，电信安全L1-L3级云地协同专家提供1v1贴心服务，将客户体验放在首位。安全运营专家通过实战经验与行业融合，为金融、互联网、政务、公检法、教育、医疗等不同行业客户输出契合行业属性的最佳实践。
	广东网安依托18年网络安全服务经验与业界网络安全运营最佳实践，通过自研的网络安全运营服务平台，集成防御、监测分析与合规审计等专业网络安全工具，持续监控响应客户安全事件，自动化处置威胁；通过一线、二线与外部专家等组成的专业安全服务团队，为用户提升提升7*24小时网络安全运营服务。根据客户网络安全能力基础与工作目标，弹性提供托管式与专项安全运营服务，包括安全评估咨询规划、安全监控和事件响应、安全防护和漏洞管理、攻防演练、安全培意识训与安全合规和审计等服务，在政府与医疗行业积累了丰富的安全运营服务项目经验。
	华为乾坤安全云服务解决方案，使用全新云边端一体架构，云端提供整体分析能力，边侧通过天关设备提供边界防护能力、端侧通过EDR提供终端防护能力。面向客户提供完整安全集成运营服务，客户可实现按需订阅、快速能力部署痛点需求；云端通过云端专家+智能分析算法实现对边侧、端侧威胁告警快速自动分析响应、智能识别客户本地网络的潜在威胁，并完成告警自动化处置闭环，自动处置率达到95%，从而帮助租户简化本地运维，提升安全运营与防护实效。
	云纷科技以十年安全管理经验及安全研发能力为依托，结合自身对于安全的理解和知识，协同利用开发能力、调用各类自动以及半自动化工具，为客户提供最切合实际的安全运营及托管服务。其提供的下一代MSSP服务是充分运用了敏捷智能的新技术来应对海量增长的长尾用户群体，通过技术驱动和集中共享降低每个单一客户投入的成本以确保性价比。云纷科技自研云原生平台InsightX，运用人工智能AI算法、IXtra，UEBA等组件，将安全实践和安全理论知识快速工具化产品化，来提高安全效率降低企业成本，并对企业提供7x24全天候安全保障。
	保旺达运营中心SOC系统以AI和自动化编排为核心，充分采用技术手段，将人、技术和流程高度协同起来，将繁杂的安全运行（尤其是安全响应）过程梳理为任务和剧本，提供定制化的流程和控制，整合并加速有效网络威胁的调查与缓解,防护能力孤岛化，运营工作碎片化、无序化、重复化等问题，将安全管理工作融入到铁塔日常运营活动中，建立了技术、人员、流程一体化的标准安全运营体系。

调研企业	安全运营业务简介
 漠坦尼	漠坦尼托管安全服务（MSS）包含安全咨询、安全运营、安全评估、安全培训等内容，结合公司多年技术实战经验，致力于满足客户业务安全与监管合规需求。聚焦业务创新、提高运营效率、降低运营成本、解决实际问题，以全方位的规划设计、优质的解决方案和持续服务，面向企业安全需求提供专业化、定制化、个性化、低成本、长周期的网络安全服务。安全托管服务将帮助客户实施整体安全规划，全面提升客户安全管理和治理水平，最终实现合理运用外部资源的自主运营安全，更好地帮助客户解放IT生产力，将更多精力聚焦于业务创新本身。
 云盾智慧 iCloudShield	云盾安全服务团队前身为联通集成公司的内部安全服务团队，成立于2008年，拥有数十名具备安全等保测评师、CISP、CCIE、MCSE等专业资质安全攻防专家，承接联通集团信息化部、网络部、渠道运营中心、软研院等日常安全服务和重保值守等服务，2019年划入云盾智慧，服务范围扩大为常态化安全运营、风险评估、重保服务、攻防演练、数据安全评估等。慧势态势感知与安全运营平台以构建全局安全数据分析能力为核心，内置威胁分析智能引擎及安全运营工具。平台现已应用于中国联通集团总部，监测分析集团数十万资产的安全态势，是运营商行业内领先的态势感知平台。
 亚信安全	亚信安全MSS运营服务依托亚信安全XDR产品解决方案和安全运营专家团队，为企业、教育、医疗、政府、金融等行业客户提供巡检、按需和常态化安全运营服务。基于XDR的治理框架，根据用户不同的需求，提供了三大托管式安全运营服务模式，将安全产品、服务、流程以及人员进行深度打通和融合，帮助客户解决资产漏洞不清晰、真实威胁不可见、告警聚合效果差、产品联动效率低等问题，构建体系化、常态化和实战化的安全运营能力，将黑客入侵、病毒感染等安全风险降至最低。能够解决的不仅是当下的安全难题，还有适应未来需求的安全布局。
 Hillstone 山石网科	山石网科可持续安全运营服务构建了可持续安全监测、安全评估和响应能力。通过设置专业的技术人员岗位，明确岗位职责，通过制定标准工作流程，规范协同机制。依托山石网科全线产品，利用用户现场环境，开展安全合规、资产梳理、漏洞管理、安全事件监测、威胁分析、事件流程管理及通报、演示汇报等一系列日常运营工作。可短期快速提升用户安全能力，同时可借助山石网科专业安全服务团队帮助用户培养并建立自己的安全运营能力。
 Juming 聚铭	聚铭依托团队近20年安全运营平台开发运维经验推出的聚铭下一代智慧安全运营中心产品以“人机共生，智慧运营”为核心理念，依靠大数据挖掘、AI算法、智能降噪等关键技术，构筑全流程自动化的安全动态防御体系。结合用户实际安全场景和业务需求提供专业报告和安全指导，动态优化安全工作流程、组织架构和配套制度，做到弱人工化、重智能化的安全运营，最终实现安全设备、安全数据、安全管理“效能最大化”的目标。目前产品已服务全国超3000家客户。
 ANTIY 安天	安天常态化安全运营服务可根据客户自身的安全运营成熟度，将安天特色的能力运营支撑点融入到客户的安全运营流程体系中，以威胁对抗为核心，以持续性威胁猎杀为基础手段，结合现场的安全产品和平台，通过“运营体系建设”、“前置安全评估”、“常态安全运营”和“事件应急响应”四个方面开展日常安全运营，协助客户建设安全运营组织机构，建立并完善安全运营体系，健全安全运营管理制度体系和应急预案体系，强化关键环节的安全运营协同机制，确保客户的网络安全工作在安全运营组织机构的带领下能井然有序的开展。



以数据为基础的网络安全产业研究平台

ssaq@geniuscybertech.com

2023
