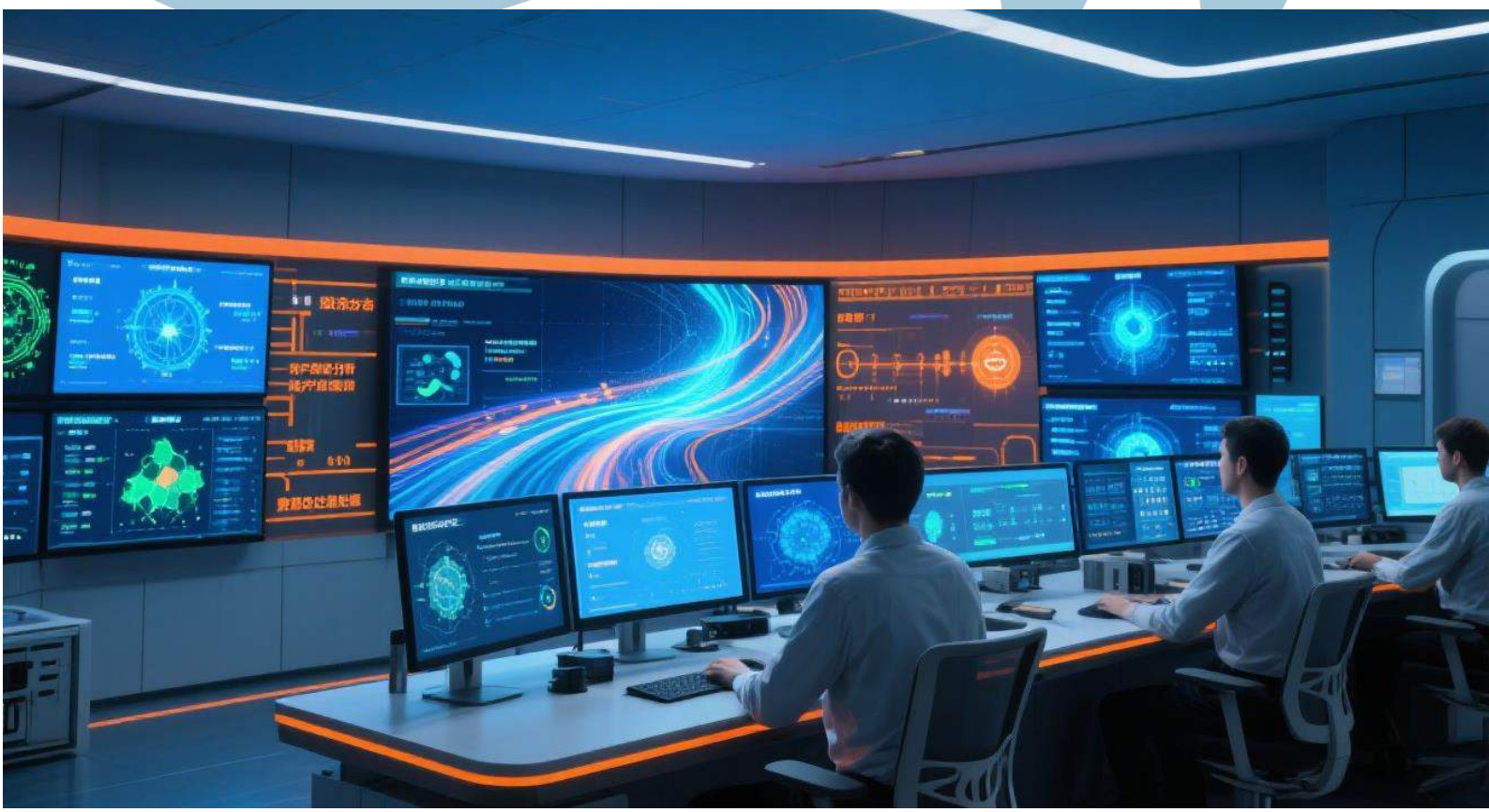
数智化安全运营报告

（2025）



数智化安全运营报告

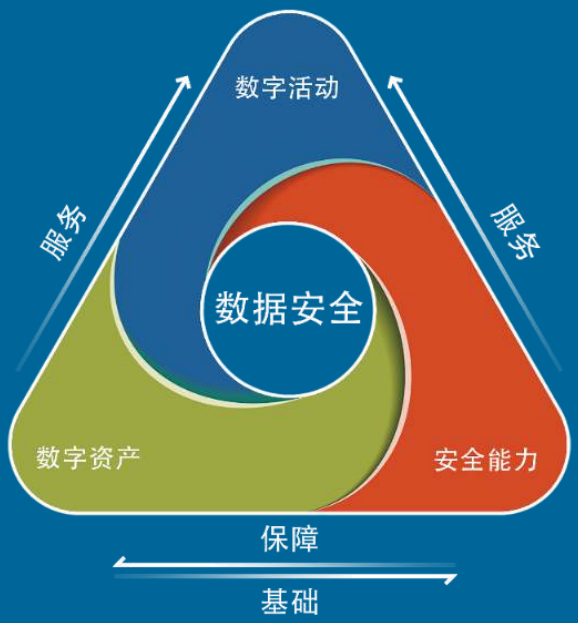
（2025 年）

数字安全是指，在全球数字化背景下，合理控制个人、组织、国家在各种活动中面临的数字风险，保障数字社会可持续发展*的政策法规、管理措施、技术方法等安全手段的总和。

这里的风险，不再局限于围绕数字化资产的攻防对抗，还包括了数字资产所承载业务的稳定性、连续性和健康性。这里的安全不再特指有意还是无意，天灾还是人祸，保安还是保险，而是更为广义的安全状态（SecSafe）。

*“世界环境与发展委员会出版的《我们共同的未来》报告中，将可持续发展定义为：“既能满足当代人的需要，又不对后代人满足其需要的能力构成危害的发展。”

——数世咨询，2023 年 11 月



以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核的“数字安全三元论”。

“数字安全三元论”由“网络安全三元论”（数世咨询于 2020 年提出）更新迭代而来，旨在匹配数字中国建设的进程，保障数字基础设施稳定、可持续运行，保障数据有效流动、激发数据要素价值。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构 ．网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

主笔分析师：靳慧超 数世咨询 战略分析师

分析团队：数世咨询 数字安全战略研究院 观安信息

报告审核：李少鹏 数世咨询 首席分析师

目　录

前　言

安全运营，以往通常是具备一定规模的组织才能承担和开展的工作，原因有二。一是因为安全运营工作价值不易显现，只有规模或收入达到一定量级，并且数字化程度较高的组织才有内驱动力为安全运营投入人财物。二是因为安全运营工作专业度高，需要数据分析、网络攻防、管理沟通等专业和复合型人才，并且工作压力大、时间长。

但随着数字化转型进程的不断深入，组织的核心业务与数字化的依赖程度逐渐走高，组织所拥有和产生的数据作为生产要素也在逐渐展现出自身的经济价值，使得越来越多的组织需要凭借安全运营支撑数字化业务的发展，保障数据安全、有效、高效流通。同时由于网络安全威胁态势的严峻形势以及我国监管合规的整治力度逐渐加码，国家和社会层面加大了对网络空间安全教育的投入，具备安全专业技能的复合型人才需求逐步得到解决。

基于这种趋势和需求，安全运营已经具备广泛且成熟应用的条件，成为组织数字化转型的有力保障，支撑数字化业务发展。但什么样的安全运营才能真正符合数字化组织的需求，才能够有效的帮助组织完成安全目标、体现安全运营的真正价值，这是摆在产业界面前的一道必答题。

为了回答这个问题，数世咨询对产业界进行了持续的调研，对符合数字中国的安全运营相关思想、技术、市场进行了整理与总结，并联合观安信息，基于其在安全运营工作中的技术实力与行业经验，绘制了数智化安全运营框架，希望可以为组织提供有益的参考和帮助。组织可以根据数智化安全运营框架，结合自身数字化环境和业务特点，开展匹配自身业务发展目标的安全运营工作。

关键发现

- ✓ 越来越多的组织认识到，安全与业务不应该是割裂的，安全运营本质上也是组织的一项业务，同样需要数字化。只有数字化后的安全运营才能与数字化业务深度融合，只有匹配数字化业务流程的安全能力才能得到组织的持续资源投入，只有具备安全性的数字化业务才能得到良性发展。
- ✓ 作为一项业务，安全运营的数字化需要从组织经营视角，以体系化和管理化思维切入。不单单是一些技术平台的上线，更重要的是在组织文化、管理、流程中融入安全。
- ✓ 安全能力的有效性要靠安全运营维持，而安全运营的高效性要靠 AI 的合理应用与高质量的安全数据实现。
- ✓ 由于大部分安全运营工作都具备场景化、流程化的特性，并且执行单一性任务的安全 AI Agent 已经开始应用于各类安全工具，安全运营与 Agentic AI 的结合将会赋予安全运营更深度的智能化。
- ✓ 安全数据是提升安全运营成效的核心要素。对于安全数据的归集、标准化以及计算能力是安全运营涉及的各类技术平台的基础。尤其是多模态安全数据的识别和汇聚，将会大大提升 AI 应用的多样性以及效果。

第 1 章 安全运营驱动力

1.1 威胁态势不断升级的挑战

自 1994 年我国全功能接入国际互联网以来，到现在 30 多年的时间，网络威胁的方式和手段不断升级，组织对抗网络威胁的方法在不断变化，同时组织对安全运营的要求也在不断调整，以不断应对威胁态势带来的挑战。

◆ **网络威胁的演变**

大致在 1994 年到 2000 年的这一时期，全球互联网处于起步阶段，网络安全意识薄弱，缺乏系统化防御体系，个体黑客开始崭露头角。网络威胁以技术探测为主，攻击者多为单纯的计算机极客，主要目标是破坏系统或展示技术能力。这一时期，组织的安全运营工作通过使用第一代防火墙（包过滤）技术产品，配合防病毒网关进行防护，工作内容更多的在于对安全设备的简单维护。

2000 年到 2011 年左右，全球互联网飞速发展，由于网络应用的普及，网络黑产开始浮出水面。这一时期网络攻击组织化、商业化特征凸显，网络钓鱼、金融诈骗成为主要动机。这一时期，组织的安全运营工作新增了 IDS、IPS 等网络攻击检测设备，并开始通过 SSL/TLS 协议为网站加密。由于等级保护的要求，组织开始建立自己的安全管理体系，包括安全责任、管理制度、技术要求等方面，严格划分和控制内外网界限，以边界访问控制设备作为主要技术手段。

2012 年到 2022 年左右，由“棱镜门”事件为导火索开启了全球网络空间争夺的序幕。云计算、移动互联网和物联网的普及使攻击面指数级扩大，网络攻击开始影响物理世界，由国家力量组成的网络部队将关键基础设施列为重点目。

这一时期，组织的安全运营工作开始接收威胁情报对网络攻击进行预警，通过零信任等新概念对技术手段重新调整。在网络安全体系建设方面，完善覆盖资产保护到事件处置全流程的管理体系，包括风险评估、应急演练、合规审计等。技术侧开始转向纵深防御体系的构建，从边界、应用到软件供应链形成多层次多防线的安全运营体系。

◆ **智能威胁的冲击**

从 2023 年开始，由于 AIGC、量子计算、太空网络等前沿技术的飞速发展，网络威胁态势再一次产生了质变，催生出诸多未知风险。

2025 年 4 月 15 日，哈尔滨市公安局发布公告，追查到美国国家安全局的 3 名特工和两所美国高校，参与实施了针对亚冬会的网络攻击活动。国家计算机病毒应急处理中心发布报告披露了两组数字，哈尔滨亚冬会的赛事信息系统和黑龙江省内关键信息基础设施遭到境外网络攻击的次数分别为 27 万次和 5000 万次。从攻击代码研判来看，此次攻击采用了智能体技术进行网络攻击，部分代码明显由人工智能编制而成。

面对新技术带来的新挑战，国家开始大力建设 AI 和数据基础设施、推进量子计算发展、布局太空网络等，充分利用新技术来对抗新技术。

组织的安全运营工作同样如此，由于业务对新技术的引入，从而产生了新的暴露面和安全风险。面对这些新的威胁，传统的防御思路可能收效甚微，所以安全运营工作同样需要用 AI 对抗 AI、用量子抵御量子，构建由 AI 赋能、数据驱动的动态安全防护体系，来迎接新时代网络威胁的智能化冲击。

1.2 数字经济平稳运行的要求

新一轮科技革命和产业革命将人类带入数字时代，数据作为关键生产要素的价值日益凸显，深入渗透到经济社会各领域全过程。我国数字经济蓬勃发展，已经取得了举世瞩目的成就，经济规模总量以及数据总量和算力总规模稳居全球第二位。2024 年，我国数字经济核心产业增加值占国内生产总值比重 10%左右，达到 13.5 万亿。《数字中国建设整体布局规划》中明确指出，数字技术创新体系和数字安全屏障是两大支柱。牢筑数字安全屏障，就是要强化网络、数据等安全保障体系建设，建立健全数据安全治理体系，保障个人信息，强化数字经济安全风险综合研判。

《网络安全法》、《数据安全法》、《个人信息保护法》以及等级保护 2.0 等法律法规的相继出台，促使我国的安全顶层设计逐步完善，推动我国安全运营体系的建设过程。随着数据已经在我国被确立为生产要素，根据国务院《关于构建数据基础制度更好发挥数据要素作用的意见》，未来的建设和发展必定会充分利用数据要素价值。而数据的价值越高，其安全风险也会越大。为了系统性防范数据风险，根据国家发改委等部门《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》，明确到 2027 年底，规则明晰、产业繁荣、多方协同的数据流通安全治理体系基本构建，数据合规高效流通机制更加完善，治理效能显著提升，为繁荣数据市场、释放数据价值提供坚强保障。进一步推动了一体化安全运营体系的全面建设。

传统的安全运营目标主要是为了满足监管合规的要求以及保障基础设施的稳定运行，以支持业务的正常开展。而数字化时代的安全运营则需要在此基础之

上，同时保障数据安全、有效、高效的流动，以起到支撑数字化业务开展的核心作用。

数世咨询认为，在数字时代，数据即业务。保障数据即发展业务，数据驱动即业务驱动。

第 2 章 数智化安全运营概念

2.1 概念定义

为了保障和支撑组织的数字化转型，数智化安全运营需要在安全能力统一管理的基础上，通过安全数据互通掌握多源头、多模态、多维度的安全数据，利用 AI 和大数据处理技术，使安全能力匹配业务流程，根据不同安全场景需求做出相应的协同处置动作、实现安全能力动态化，以持续应对不断变化的威胁态势。

数世咨询联合观安信息对数智化安全运营做出如下定义：

数智化安全运营是基于数据驱动和智能技术的融合应用，以多来源、多模态、多维度的安全数据为基石，深度融合人工智能技术以驱动自动化分析、决策与响应，将数据洞察高效转化为精准安全能力的新一代运营模式。

数智化安全运营以 AI 赋能、数据驱动为核心，整体提升安全运营中涉及的平台、能力、管理、流程、人员的协同性和效率，充分释放数据价值，促进组织战略发展。在安全运营为组织数字化业务筑盾护航的同时，数智化安全运营自身也是一项重要数字化业务，其核心目标是将安全能力从防御工具升级为驱动业务增长、创造商业价值的核心引擎。在此数字化进程中，组织对安全能力进行量化、对安全水平进行度量，以持续有效安全的实现推动安全运营从传统“成本中心”向“数字化业务价值枢纽”的转型愿景。

2.2 关于安全数智化

数智化安全运营的核心是数智化，即 AI 赋能、数据驱动，也就是将各类安

全运营平台和安全能力（安全产品、服务）与 AI 技术相结合使其具备更深度的智能化，然后利用多来源、多模态、多维度安全数据的汇聚和分析能力驱动具备 AI 能力的各类安全运营平台和安全能力，持续提供可用、准确、实时的分析数据，最终推动安全运营向更高阶的智能化方向发展。

AI 赋能以深度学习、自然语言处理、计算机视觉等人工智能技术为基础，数据驱动以大数据处理为底座、大数据分析为内涵。AI 赋能、数据驱动可充分释放安全数据的潜在价值，准确去除告警中的噪声干扰、快速锁定威胁源头、高质量预测风险，有效提升安全运营工作效率。AI 赋能和数据驱动可充分激活安全能力的防护效果，打造专业可信的安全大模型、协同联动各类安全能力、优化安全策略和流程，持续保持有效且高效的防护能力。

数智化安全运营通过 AI 赋能、数据驱动的方式，可极大增强安全运营平台和安全能力的数据分析能力、模式识别能力和自动化能力，从数据汇聚、AI 应用以及检测到处置的全流程优化安全运营工作。

◆ 更全面的数据汇聚

AI 的智能化能力来源于算法，而 AI 的智能化效果则来源于数据。数智化安全运营的重点在于 AI 的智能化应用效果，而这一目标是由多来源、多模态、多维度安全数据的汇聚作为基础实现的。

数智化安全运营具备汇聚组织多来源、多模态、多维度安全数据的能力：

1.多模态安全数据：将不同类型的数据，如文本、图像、视频流等，通过数据预处理、特征提取、跨模态映射、融合推理等步骤进行汇聚，来增强数据处理

能力的鲁棒性和准确性。

2.多源头安全数据：将组织内所属的数字资产（如操作系统、应用软件、IP 地址、API 接口等）、安全日志以及全网威胁情报（如传统威胁情报、开源威胁情报以及暗网情报等）汇聚，增强分析数据的全面性。

3.多维度安全数据：针对每一种数字资产，从不同维度（如访问时间、身份认证次数、登录地址等）整合汇聚，形成全方位的可观测安全姿态，增强分析数据的多样性。

◆ **更专业的安全大模型**

大模型是 AI 技术的复杂应用，其核心之一就是数据，数据不论在大模型的训练阶段还是推理阶段都发挥着决定性的作用。数智化安全运营使用安全大模型，并持续优化安全大模型的应用效果。

安全供应商为组织提供了基础的安全大模型，组织可通过数智化安全运营将自身数字化环境产生的安全数据、安全经验、处置偏好进行数据标准化处理，转化成可应用于大模型指令调整的三元组，根据组织自身数智化运营偏好进行指令调整后的安全大模型将会更加“懂得”组织的安全策略，并且得到更准确的输出内容，提升大模型的应用效果。

除此之外，通过外挂安全数据库的 RAG（检索增强）技术，可以使安全大模型获得最新的实时安全数据，有了更加真实、准确的输入数据才能使得大模型输出更准确的信息，这样就可以使得数智化安全运营的结果切实匹配真实的数字化环境与业务动态需求，进一步提升安全大模型应用效果。

◆ **更智能的安全运营**

大模型的应用快速进化，从 GenAI、AI Agent 到 Agentic AI。现阶段的创新应用已经证实，Agentic AI 可以为安全运营带来更深度的智能化，是安全运营发展的未来方向。

Agentic AI 可基于目标主动制定策略并执行任务，无需持续人工干预。利用大模型的专业知识和 AI Agent 的执行能力，根据不同场景需求结合安全现状，通过多步骤推理和工具调用实现安全运营操作，可解决不同种类、不同场景下的不同安全问题。

通过 Agentic AI 升级的数智化安全运营，可以自主的充分使用多来源、多模态、多维度安全数据并借助检索工具获取所需要的信息，利用自动化编排能力根据不同的安全需求将相应的安全能力作用到对应的控制点上。并且在这种自动化的处置过程中，联合协作多个不同能力方向的安全 AI Agent，使处置过程中的每一个输入、输出都具备精确性、准确性，最终得到可靠的处置结果，为安全运营人员节省大量的繁琐工作并且提供高价值的分析信息，带来极大的帮助。

◆ **更精准的威胁检测**

传统的威胁检测技术主要依赖预定义的规则和签名库，难以应对新型攻击和高级持续性威胁。融合 AI 技术的安全能力可以从海量安全数据中识别异常行为，实现智能化的威胁检测。

UEBA（用户与实体行为分析）可以通过大模型的赋能，使用图神经网络构建实体关系图谱，检测横向移动、权限提升等 APT 攻击链特征。

融合 AI 技术的安全能力通过监督学习与无监督学习的混合建模，可以构建网络流量与用户行为基线。基于 LSTM（长短期记忆网络）的时序特征提取技术，可识别流量中的时间序列异常。采用随机森林和 XGBoost 算法对多维日志数据进行特征工程处理，可实现误报率降低的目的。生成式对抗网络（GAN）的引入，可以使系统模拟攻击流量的模式，提升对零日攻击的识别能力。

◆ **更高效的资源分配**

安全运营工作需要处理大量的安全告警，而且安全运营平台通常需要检测、汇聚所有可能的威胁信息（如全面覆盖诸如 MITRE ATT&CK 等框架），而没有根据组织特有的风险状况和现有的安全控制措施进行优先级排序，并且在购买新的安全能力时，没有很好的配置或集成这些能力。这种工作方式产生了大量的安全告警，然而其中许多是误报或低优先级的。

AI 赋能的安全运营平台则可以有效解决这一问题。通过机器学习可以分析大量历史数据，识别规律以区分真实威胁和误报。此外，安全运营平台可以利用 AI 工具分析环境和历史背景，过滤掉无关或重复的安全告警，并根据潜在影响或被入侵的可能性等因素，优先处理最关键的安全告警。当安全告警以这种方式进行分类时，安全运营人员可以更方便地做出关于资源分配的决策，从而提高他们应对威胁和保护组织的能力。

◆ **更有效率的事件响应**

对于安全运营平台处理的告警，安全运营人员需要研判其真实性、根源及必要的响应措施，研判速度越快、信息越充分，威胁对组织造成的影响就会越小。

安全运营人员可以通过安全运营平台的 AI 能力为事件响应决策提质增效。使用 AI 能力来分析告警上下文信息来确定威胁类型，并且还可以快速自动化的收集更多的辅助安全数据以便作出更准确的决策，最终推荐生成适当的响应处置措施。例如，检测与分析的结果是勒索软件攻击，则可生成隔离受影响的系统、阻止恶意 IP 地址或锁定终端设备的事件响应方式。

这样就可以解放安全运营人员使他们能够将时间用于更具战略性和细微差别的决策任务。而且，还可以通过 AI 能力使安全运营平台持续从过往的研判事件和响应结果中学习，随着使用时间和事件数量的增长，可以进一步提高安全运营平台的事件响应效率，切实帮助安全运营人员。

◆ **更准确的风险预测**

传统的安全防御往往是基于已知威胁的被动响应，而 AI 赋能的安全运营平台可以通过预测性分析技术提前识别潜在威胁，并推荐生成相对应的安全防护措施。

安全运营平台可以利用 AI 能力通过时间序列分析和机器学习模型进行威胁预测，预测未来的攻击趋势和潜在风险。可以通过代码分析和漏洞数据库进行漏洞预测，预测系统中可能存在的漏洞。可以利用 AI 能力进行攻击模拟，模拟攻击者的行为路径，以便识别防御体系中的薄弱环节。

通过 AI 赋能的预测性防御使企业能够提前采取措施，防患于未然，从而大幅降低安全事件的发生概率和影响。

◆ **持续优化形成自适应安全体系**

数智化安全运营通过 AI 技术持续学习并且动态优化安全能力，实现推动安全体系从静态防御向自适应安全的转变。

安全能力通过持续学习和强化学习技术，可以不断优化其检测和响应模型，根据最新的攻击数据，动态调整其行为分析算法。

AI 赋能的安全运营平台可以根据实时威胁数据动态调整防御策略。当检测到新型攻击手法时，可以自动更新防火墙规则或调整访问控制策略。处置结束后通过事后分析和复盘，以不断改进检测和响应机制，优化安全策略和流程。

通过 AI 赋能的自适应安全体系使企业能够快速适应不断变化的威胁环境，始终保持高效的防御能力。

2.3 关于安全运营

数智化安全运营不仅具备原有的安全价值，即保障业务连续性、维持安全能力的有效性、满足合规监管的要求，同时也是组织的一项重要数字化业务，本质是由 AI 赋能、数据驱动的数字化服务。这种服务通过智能决策的安全中枢整合安全能力服务链，直接作用于数字化业务解决不同安全场景的需求，其本身就是一项可度量、可验证的数字化业务。

数智化安全运营的落脚点和价值体现是安全运营。关键所在，是利用 AI 赋能、数据驱动的方式升级安全运营 5 要素（平台、能力、管理、流程、人员），最终整体提高安全运营工作的协同效率。安全运营的数智化升级，关键在于 3 个方面，分别为平台功能性、运营成熟性和运营时效性。

◆ **增强安全运营各类平台的数据处理能力**

平台是为多系统提供支撑的框架或环境，使多系统可以进行相互协作。安全运营涉及多种类工作，需要不同的平台予以支撑。如身份认证平台，可以对接不同信息系统的身份认证流程，实现身份管理的一体化；如态势感知平台，可以将不同工具获取的信息进行集中分析，按照风险策略展示安全现状。

安全运营涉及的各类平台需要具备良好的网络架构以及对各种数据的处理功能，适应不同的业务环境。安全管理类平台需要具备对接和管控各品牌、各品类安全产品的能力，安全分析类平台需要将运营过程中产生的有效数据以用户便于接受的形式展现。

安全运营中涉及的多模态、多来源、多维度的安全数据，在数据规模、技术架构和应用场景上已经超越了结构化数据和中小规模数据集的范畴。安全运营涉及的各类平台的数智化升级需要从数据采集、分析、利用等全方位进行，使用支持实时流处理和分布式系统复杂性的大数据处理方式，才能将多来源、多模态、多维度安全数据进行快速、准确的处理。

数据采集方面，新出现对多模态数据进行识别的需求，需要将图像（如网络拓扑图）或视频信息（如机房监控视频）转化成可以被平台分析和利用的数据，为后续分析奠定基础。还有安全数据的标准化需求，原始数据往往包含噪声、缺失值或异常值，因此需要通过数据清洗与预处理技术，确保数据的准确性和一致性。

数据分析方面，需要利用 AI 机器学习算法和深度学习模型对数据进行分析。例如通过时间序列分析，可以增强预测网络流量趋势或设备故障概率；通过聚类算法，能够识别用户群体的行为模式；通过分类算法，可以判断潜在的安全

风险；这些数据分析的能力和结果不仅可以揭示安全数据背后的规律，还为趋势预测提供了科学依据。

数据利用方面，需要实现根据不同安全运营场景的特殊需求提供针对性决策辅助的能力，同时使用 AI 反馈机制学习不断产生的实时安全数据以持续优化和迭代，最终形成安全运营的 PDCA 循环。例如漏洞运营场景，需要综合漏洞级别以及对组织可能造成的真实危害，做到事前预警（如确认该漏洞对组织的真实影响范围等）、事中处置（如对哪些数字资产进行处置、利用哪些安全工具和能力、执行哪些具体措施等）、事后恢复（如数字化业务恢复顺序、程度等）、持续优化（如同类型漏洞或利用方式的验证、同类型事件发生后的流程改进等）。

◆ **推动安全运营的数字化转型**

数字时代，安全运营已经可以称之为组织的一种数字化业务，为了更好的保障其他数字化业务，安全运营自身也需要数字化转型。并且安全运营的数字化一定是运营过程管理的数字化，而不是运营过程的静态信息化记录。

升级安全运营成熟性，必须实现安全运营工作的数字化，就是要通过数字化的连接和 AI 能力，来助推安全流程高效运转，彻底提高 5 要素的协同效率。将安全运营流程与数字化业务流程深度匹配，使安全管理融入经营管理，根据不同数字化业务的针对性场景提供分门别类的安全应对措施，真正体现保障和促进组织发展的价值。

◆ **提高安全运营人员工作效率**

安全运营人员主要指安全运营工作中的安全分析专家、攻防对抗专家、运营

技术支持人员以及这些人员的安全工作经验，还有企业自身或者通过安全服务可以联系到的生态合作伙伴以及可协调的非自身安全人员。

传统安全运营中，安全运营人员常常被淹没在海量告警、信息搜集、威胁验证等重复性高、数量庞大的琐碎工作里。由于专业的安全运营人员本就相对稀少，如果不能使其充分发挥出核心作用，对于安全运营来讲就毫无效率可言。

对安全运营时效性的升级，就是要从繁复的工作中彻底解放安全运营人员，使安全运营人员将更多的精力和时间投入到更具战略性和高质量要求的高优先级工作当中，切实增强安全处置和应急响应时产生的实际效果。例如增强专家经验在业务环境中的实际应用效果、提高应急响应的及时性和应急处置的合理性、解决由新技术新业务带来的新安全需求。

第 3 章 数智化安全运营框架

根据数智化安全运营的定义（通过 AI 赋能、数据驱动的方式，链接安全运营中涉及的平台、能力、管理、流程、人员，提升安全运营的整体协同性和工作效率，最终达成满足监管合规要求和有效促进组织持续发展的目的），结合安全运营实际工作内容和流程，绘制出可落地应用的数智化安全运营框架。

数智化安全运营框架更加关注安全运营工作与数字化业务的匹配程度，强调以 AI 赋能、数据驱动的安全运营能力为核心，通过可持续评估、可持续优化的安全运营方式，以匹配数字化环境的安全运营场景为价值体现，最终达成满足监管合规要求、促进组织发展的目标。

数智化安全运营“1+1+1+N”框架，由 1 种运营环境、1 组安全运营能力（不同平台提供不同安全运营能力）、1 套健康运营体系、N 类安全运营场景组成。

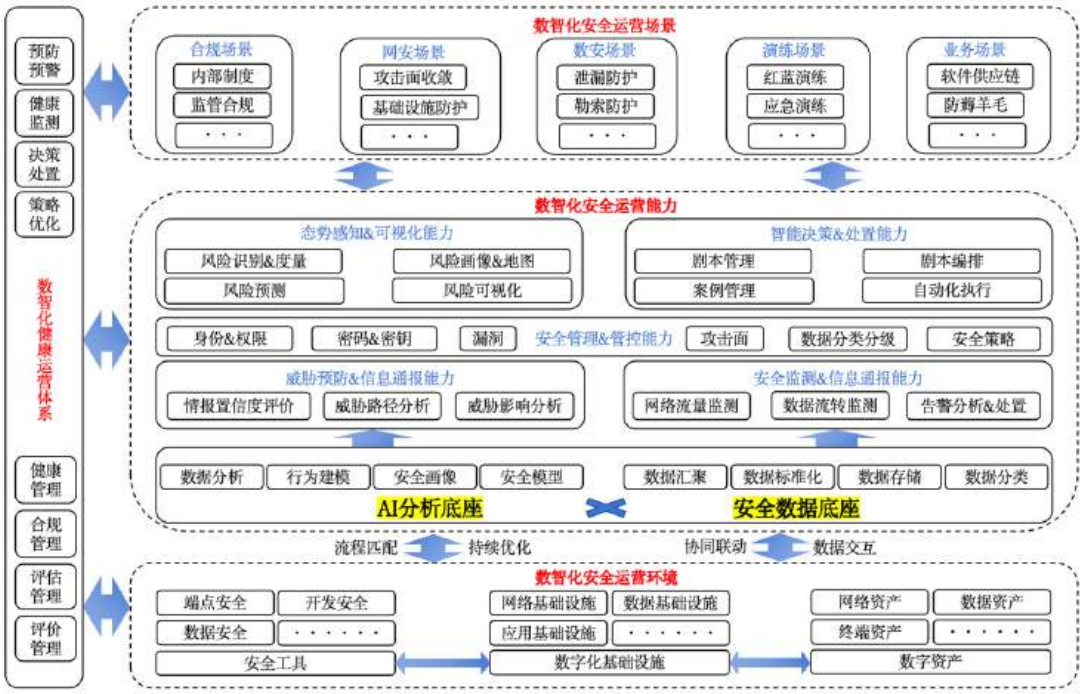


图 1 数字化安全运营框架 v3.0

数智化安全运营框架如上图所示，当前版本为 v3.0，框架会持续优化以匹配更多实际应用情况。

3.1 数智化安全运营组成

◆ **数智化安全运营环境**

组织的数字化业务依托于数字化环境开展，数智化安全运营的基础和对象也是同样的数字化环境。数智化安全运营环境主要包括组织的数字化基础设施（网络通信、算力支撑、数据湖仓、应用平台等）和数字资产（网络资产、终端资产、数据资产等）。

安全工具本质上也是组织的数字资产，依托于组织的数字化环境运行，作用于自身的保护对象，其同样需要运维、管理，属于数字化安全运营的对象。与此同时，安全工具还主要负责多来源、多模态、多维度安全数据的采集工作并提供相应的安全能力。如 EDR（端点检测与响应）是保护所有端点设备的综合性检测与响应技术手段，抗 DDOS 是保障网络服务稳定和可用的技术手段，隐私保护计算是促进个人信息和敏感数据流通的技术手段。

安全工具接受数智化安全运营的统一管理，执行相应安全运营场景的安全策略，在基础设施和数字资产上实现具体控制能力。

◆ **数智化安全运营能力**

✓ “AI*数据”双底座

数智化安全运营能力的核心是 AI 应用和大数据处理能力，二者缺一不可、是相乘的关系，任何一方面的能力欠缺都会造成实际应用效果的极大下降。

AI 底座提供安全数据的各类分析算法、数学建模能力并内置安全大模型，安全数据底座提供安全数据的汇聚、标准化、存储能力并根据不同需求对安全数据分类（如漏洞数据、告警信息等），双底座协同 AI 应用与大数据处理的基础能力为整个安全运营工作服务。

✓ 五大基础能力

数智化安全运营五大基础能力为风险预防&信息通报、安全监测&信息通报、安全管理&管控、安全态势&可视化和智能决策&处置，五大基础能力均由“AI* 数据”双底座支撑实现，形成由外部安全风险和内部安全动态共同驱动的数智化运营方式。

风险预防&信息通报能力的主要任务是根据全网威胁情报对组织自身的影响作出风险预警。通过置信度评价利用可信度高的威胁情报对组织进行模拟攻击，预测攻击路径与影响范围，将可能存在的各种威胁情形作为决策的支撑并可视化展现。

安全监测&信息通报能力的主要任务是从内部安全动态的变化中分析出安全风险并预警。持续对组织网络、数据、用户行为、合规制度的基线和特定阈值进行监控，分析出潜在的风险事件作为决策的支撑并可视化展现。

安全管理&管控能力的主要任务是整合组织分散的安全要求和能力，如组织的权限、密码、数据分类分级等，根据组织整体性要求和场景特殊要求，在统一

管控下实现整体性、系统性的防护水平。将组织面临的威胁和可能的风险所涉及的信息整合管理、分析，动态调整安全策略以持续维持整体性安全水平。

安全态势&可视化能力的主要任务是将组织相关的安全风险可视化呈现并作出相应预测为组织的整体风险决策提供参考。态势感知在组织整体风险策略框架下识别、度量安全风险，将业务流程中的相关风险信息进行多维度建模和量化分析，构建出动态化、可视化的风险特征模型。

智能决策&处置能力的主要任务是汇聚外部与内部安全风险，结合组织安全需求生成对应安全场景的处置方案。对各类流程剧本进行统一管理和编排，对不同安全场景中的特定案例进行统一管理并学习，利用双底座的能力根据处置经验不断优化决策结果。

◆ **数智化安全运营场景**

数智化安全运营场景是根据组织的数字化业务和经营发展的需求，通过数智化安全运营平台与数智化运营环境的协同，虚拟出的安全控制范围和运营工作流程。

合规场景主要包括监管合规的制度要求以及例行和突击检查所覆盖的安全控制点，将合规需求转化成对应的处置流程和安全基线进行自动化管理。如等保 2.0、内部敏感数据访问制度等。

网安场景主要包括管理和收敛组织的网络暴露面、保障数字化业务正常开展，面向网络架构和信息系统的稳定性需求。如漏洞管理和预防、网络攻击应急响应等。

数安场景主要包括组织内部数据处理全生命周期安全需求，以数据为核心围绕数据处理全流程形成针对性保障，促进组织内部数据流动和外部数据流通。如可信数据空间、数据防勒索等。

演练场景主要包括组织为应对网络攻击和提升安全保障水平所涉及的能力培养和验证需求。如内部红蓝军对抗演练、实网攻防演练等。

业务场景主要针对组织的数字化业务在开展过程中可能被利用的业务逻辑和安全漏洞，从软件开发到业务系统运营形成全方位保障。如开发安全、促销活动防薅羊毛等。

◆ **数智化健康运营体系**

数智化健康运营体系融入数智化运营环境、数智化安全运营平台和数智化安全运营场景，通过技术和管理双循环的管理和流程将整个数智化安全运营框架贯通，发挥出应有的安全效果。

数智化健康运营体系强调风险与业务的平衡、体现安全效果的动态性，不追求不切实际的安全目标，而要保证安全能力和策略持续匹配业务流程、满足合规要求，保障组织数字化环境的健康状态最终以支持企业健康发展。

技术方面，主要根据数智化安全运营平台的三大核心能力梳理出预防预警、健康监测、决策处置、策略优化的安全风险控制与处置体系，形成从预测到处置到优化的风险管理闭环。

管理方面，主要从数智化运营环境和数智化安全运营场景入手，根据组织数字化业务流程和经营发展需求，设立技术管控和合规管理的安全基线。根据安全

运营整体工作，设立评价和评估指标，使安全运营工作效果可考量、价值可呈现。

3.2 数智化安全运营特点

◆ **关注安全运营与数字化业务的匹配**

对于大部分组织来说，传统的安全运营之所以存在感低，很大程度是由于安全运营只对合规要求负责，工作绩效难以考量并且不会产生直观的收益，是一个纯粹的成本部分，这就导致了安全运营和业务“两张皮”的现象。

随着新时代网络法治和数字中国建设的不断发展，在两大方面对安全运营与业务融合提出了明确要求。一是合规监管不再只针对网络基础设施，而是更加关注数字化业务出现安全事件时对社会的影响，比如数据泄漏、个人隐私超限使用、不良信息和内容传播等。二是数字化业务深度渗透到了社会与经济的各方面，数字化业务出现安全事件会造成人身和经济的直接损失，比如智能驾驶被攻击导致的交通安全、大模型训练投毒导致的输出异常等。

这些新的变化和要求都是围绕着数字化业务的发展进行的，所以安全运营必须更加关注数字化业务流程与真实需求。

数智化安全运营就是要使用安全运营平台的 AI 应用能力来自动化的对接、匹配业务流程，并且在安全运营的过程中通过 AI 应用能力持续的学习，达到不断优化安全运营流程以持续适应不断变化的业务流程、助力业务发展的效果。

◆ **打造可持续评估的健康运营体系**

随着数字化的不断发展，安全能力体系进入实战化运营阶段，安全运营的效

果已经变成组织最关心的问题之一，即从“有没有”到“行不行”、再到“好不好”。

而“好的安全运营”并不是绝对的安全，而是根据组织自身发展需要、匹配业务流程的安全运营，是安全风险与业务发展的平衡，是一种动态的变化过程，是一种健康的状态。

为了达到这种健康状态，对安全能力的评估与验证就成为了组织对安全能力的新要求。打造一套可持续评估的健康运营体系实现数字化业务持续、健康的开展，就是应对新要求的最佳方法。

可持续评估的健康运营体系通过设立科学的评价与评估指标使安全能力持续有效，通过入侵攻击模拟（Breach Attack Simulation - BAS）、安全有效性验证（Cybersecurity Validation - CV）、持续自动化红队（Continuous Automated Red Teaming – CART）等手段帮助组织发现已部署安全产品、以及构建的安全纵深防御体系的有效点、失效点与空白点，以持续评估报告为安全运营提供可视化的成果汇报与可操作的整改建议，以量化评估结果为安全决策者提供进一步完善安全投入的合理化改进建议。

可持续评估的健康运营体系，是在预防预警、健康监测、决策处置、策略优化等技术能力的基础之上建立的新型安全威胁管控方法，它通过系统性的方式，构建了从预防、处置、恢复、评估、调优的完整安全能力闭环，帮助组织实现安全运营能力的全面提升。

可持续评估的健康运营体系，其核心逻辑和综合价值主要体现在四方面。一是系统全面性，涵盖了安全能力的各个环节，确保没有遗漏的安全盲区。二是主

动智能性，通过 AI 能力和安全实战经验的加持，提升威胁管控能力和准确性。三是动态持续性，持续的评估、调整、优化，确保安全能力能够适应不断变化的威胁环境。四是业务导向性，匹配安全能力与业务目标，确保安全防控措施有效保障、促进业务发展。

◆ 通过安全场景转化安全价值

数智化安全运营的实际价值主要体现在监管合规与组织发展两大层面。一是使组织满足监管合规要求，达成合法经营的先决条件，避免监管处罚导致的经营风险。二是帮助组织促进数字化业务开展，保障业务应用稳定、持续运行，保障数据安全、有效、高效流动。

不论监管合规还是业务发展，最终都会落实到一个个具体的安全场景。如等级保护年检、主管部门专项检查、重大活动安全保障，节日促销安全保障、数据防泄漏、数据防勒索等，每一个安全场景都有其特殊的安全要求，需要不同的处置与应急流程。

数智化安全运营需要通过 AI 与大数据的能力，持续生成、学习、优化不同安全场景的需求，有效匹配各种不同安全场景生成相对应的安全运营流程，这样一方面可以提高工作效率，更重要的是可以直观展现安全运营的工作效果。安全运营重在安全能力、难在运营效果，以有效性作为结果导向，才能凸显出安全运营的实际价值。

通过场景化的安全运营，还可以精准协同业务部门、安全部门、外部支持等多方人员共同开展工作，如策略核查、违规阻断、系统恢复、安全加固、最小授权等联合处置流程，发现数据泄露、数据勒索、用户异常行为等根本原因，还可

以有效应对暴露面收敛、攻击发现与阻断、日常攻防演练、威胁情报处置等安全应用场景，为后续组织的安全风险预测、研判、分析、预警夯实基础，真正形成有效和高效的安全防护体系。

第 4 章 数智化安全运营最佳实践

数智化安全运营的核心目标是通过数据驱动的智能化安全管理体系构建，实现对企业全域安全风险的实时感知、精准研判与高效处置，在保障数据资产安全合规的基础上，显著提升风险防控能力，优化安全资源配置效率，推动安全策略与业务需求的深度耦合，最终形成“风险可管、效率可升、协同可及”的安全运营体系，为企业数字化转型提供持续稳定的安全保障，实现安全能力向业务价值的有效转化。由此解决传统安全运营中“增量风险遗漏、存量治理低效、策略精准度不足、处置及时性低”等核心挑战。

通过构建数据驱动的安全运营中心，整合安全资产、运营流程及关键指标，实现安全能力的全局覆盖与动态优化：一方面，针对企业动态变化的网络空间资产，通过自动化手段实时感知增量风险并阻断，避免“风险窗口期”；另一方面，通过数据建模与指标量化，持续评估安全能力的实际效能，推动安全工作从“经验驱动”转向“数据驱动”，确保防御体系对真实威胁的持续有效应对。下面以某电子政务一体化网络安全运营建设和运营商行业一体化网络安全运营为两个案例，解析数智化安全运营框架在实际落地过程中遇到的挑战、解决问题的思路以及其成效。

4.1 某中心一体化网络安全运营

4.1.1 背景与挑战

2002 年《国家信息化领导小组关于我国电子政务建设指导意见》中正式提出中国电子政务建设的核心框架--“两网一站四库十二金”工程。其核心目的在

于通过信息技术重构政府服务与治理模式（政务内网、政务外网），实现行政效能与公共服务的双重提升。

数字化转型政务系统的功能具体表现为：**提升服务质量**，依托在线平台（一站）提供 7×24 小时政务服务，覆盖社保、医疗、教育等民生领域，减少群众办事跑动次数；**增强治理能力**，通过大数据（四库）分析辅助政策制定，同时利用人工智能等新技术实现精准监管与风险预警；**优化资源配置**，通过整合跨层级、跨部门、跨系统数据与业务流程（十二金），打破传统层级壁垒，实现高效服务模式；**促进政务公开**，通过政府网站、移动应用等渠道公开政策文件、办事流程，强化社会监督与公众参与。总体而言，政务电子系统正从向“智能化基础设施”转型，亟需在数据融通、安全保障、服务普惠等方面持续突破，以实现“用数据决策、用数据创新”的现代化治理目标。

安全运营全局规划建设在电子政务的应用面临着行业特有难点。一体化政务大数据体系建设要求数据跨部门流通，但早期政务系统以垂直部门为中心进行建设，存在信息孤岛现象，在跨部门流通过程中的数据权属不清、隐私保护机制不完善可能导致泄露风险，导致跨部门协作开展困难、群众公共服务相关办理效率低下。近年来通过政务云进行资源整合信息孤岛现象得到极大改善，中共中央 22 年发布的“数据二十条”也对数据确权问题做了一定高度的指导，但在实际落地过程中，仍存在跨层级、跨区域、跨系统数据共享不及时，跨部门协同效率低的问题，应进一步通过细化的多层级制度和权责管理明确安全责任边界与强化协同治理，建立数据共享流通制度、构建完善安全大数据底座平台，为各层级提供合规安全原子能力。随着政务云、大数据平台、移动政务等新技术的普及应用，系统架构从传统本地化部署转向“云、网、端”融合架构，定义了“云、

网、数、用、端”的新安全防护目标。而多云环境、微服务、容器化应用等技术栈的融入，使安全防护边界变得模糊，传统基于边界的安全防护体系难以覆盖全链路，需建立默认安全治理体系，在应用系统上线前处置已知风险、加固安全控制，同时建立安全纵深防护体系规避运行时风险事件的发生。政务数据涵盖公民个人信息、地理信息、行业监管数据等敏感内容（四库），需满足《数据安全法》《个人信息保护法》及等级保护 2.0 等法规要求，然而部分系统因历史遗留问题难以满足合规标准，因此数据资产治理和数据流转安全管控成为政务系统安全运营核心任务和重要运营场景之一。

4.1.2 安全运营体系设计及技术方案

电子政务的一体化安全运营建设以“依法合规、统一监管、保障业务、安全可信”为目标，统筹建设“制度、管理、技术”三道防火墙：制度上保障各部门的网络和数据安全工作有章可循；管理上深化安全管理工作机制，加强组织内各部门运营协同管理覆盖各部门信息化基础设施、安管平台及重要信息平台，以“身份管理、统一认证、监测预警、流程管理、资产运营、运营分析、攻击面管控”为重点，全面实现统一运营门户入口、统一用户管理认证、统一业务受理分发、统一流程总线服务、统一资产运营、统一运营数据入湖和统一运营数据分析；技术上建立“云、网、数、用、端”安全纵深防护体系，实现安全整体可控。通过整合策略、技术、人员和外部资源等多个维度，构建全方位、多层次、协同高效的网络安全防护体系，以应对日益严峻和复杂的网络安全挑战。

（一）制度一把握

建立网络和数据安全组织架构，以数据防护为重心，建立健全网络和数据安

全制度体系运行机制，保障集团安全工作有章可循是“制度一把握”的重心。安全制度建设以支撑业务良好运转为核心，通过“合规监管规范化、制度流程落地化、组织职责明确化、检查评价常态化”四步强化管理整合，依托多级安全组织与多层制度规范，推进“跨层级、跨部门、跨系统”安全工作，以 PDCA 循环法构建闭环管理，从管理与制度层面保障安全工作从规划到落地的全流程实施。在组织架构上实行统一领导、分级管理、逐级负责，建设有效安全工作机构并明确机构与关键岗位安全职责。建立决策层、管理层、执行层三层制度体系：决策层与管理层从战略高度对风险治理、风险防护、威胁感知与响应及安全运营团队建设、安全培训作出定义与预期，执行层则针对系统建设、系统运行、应急响应三大环节做好工作分配与制度建立。制度文件采用四级体系：一级为顶层方针政策，是信息安全工作的纲领性文件；二级为管理办法，在安全策略指导下规范各项安全管理与技术制度、办法和准则；三级为实施细则与流程，包含实施细则、管理技术标准等内容以支撑二级文件实施；四级为记录表单，作为符合一、二、三级文件要求的客观证据记录活动实行情况。通过宣贯培训提升安全意识与防范能力，涵盖政策法规及指南解读、安全意识与技能培训，开展“网络安全周”活动，并设置靶场及培训考试模块。同时强化安全工作评估机制，优化安全绩效考核，确保安全制度有效落实与持续改进。

梳理业务逻辑线需以业务目标为导向，从流程解构、数据流转、角色协同三个维度切入，确保运营流程遵循就近原则且不影响正常业务开展。首先，纵向拆解业务全链条，明确从需求输入到价值输出的核心环节，标注各环节的关键动作与依赖关系。其次，横向分析数据在业务系统间的流动路径（如用户数据从前端采集到后端数据库存储、分析的轨迹），识别数据交互的节点与格式。还需厘清

不同角色在业务中的权责边界及协作流程，形成业务逻辑图谱。安全制度的建立与业务逻辑呈“镜像映射”关系，业务逻辑中的每个节点均对应潜在安全风险，安全制度需针对这些风险点设计控制措施。电子政务安全制度需围绕“公共信息服务”、“电子身份认证”、“电子税务”、“电子社会保障服务”、“电子民主管理”、“电子医疗服务”、“电子就业服务”、“电子教育和培训服务”、“电子交通管理”的核心业务逻辑，制定加密标准、权限管理办法、身份认证管理办法、数据共享管理办法及运营流程制定等安全制度，使安全要求嵌入业务操作的每个步骤，真正做到三同步。这种映射并非简单叠加，而是通过业务逻辑分析定位安全痛点，如，数据流转中的跨域传输环节需匹配合规制度，角色权限交叉处需建立特权访问管理制度。从而形成业务逻辑驱动安全制度设计，安全制度规范业务逻辑运行的闭环。当业务逻辑因需求迭代时，安全制度需同步更新，确保安全与业务始终同频共振。

（二）管理一手抓

在一体化安全运营建设中，安全管理和安全运营并重，通过一体化运营平台将预警、应急和服务支撑有效整合，实现统一预警通报和应急指挥与协同处置，支撑政务内外网建设稳定运行。在网络安全发展初期，各政府企业常以满足基本合规为目标进行安全工具选型，导致实际防护效能与业务需求存在偏差。后期虽强调以安全运营目标倒推工具能力，对威胁检测、漏洞管理等对抗类工具实施技术主导采购，但部分政务云平台仍存在安全产品授权过期、规则配置不合理、审计功能未启用等配而不用现象。电子政务一体化安全运营应以政务战略为方向，通过人和工具（平台、设备）发现安全问题、验证问题、分析问题、响应处置、解决问题并持续迭代优化。在这一过程中，需明确安全责任范围、安全体系的合

理性与完备性、安全资源投入度与重点风险的匹配度、安全能力与风险的匹配度以及安全能力覆盖率。

政务系统作为国家关键信息基础设施且政务业务涉及大量敏感数据，是境外 APT 组织的重点目标，需防范 0Day 漏洞、社会工程攻击、供应链攻击等高级持续性威胁，同时需确保安全防护体系对电子政务的日常业务运行和服务效率没有产生明显影响。因此和对安全与效率的兼顾是在进行电子政务一体化安全运营建设的主要挑战，管理构建安全体系的目的在于通过系统化和架构化的方法实现电子政务的安全目标，在集约化前提下提高效率和安全水平。

以 IPDR（识别、防护、检测、响应）为网络安全防御体系方法论，全面覆盖攻击暴露面、重要业务。在资产运营方面，力求消除任何死角，做到全面且无遗漏；通过网端结合的方式，有效对抗各类风险。同时，实现网数融合，进一步丰富感知能力，以敏锐捕捉潜在的安全威胁。分级安全运营实现集约赋能，能够充分发挥资源整合的优势，集中调度各类资源，以统一的手势和规范应对复杂多变的网络安全局势，从而全面提升网络安全防御的效能和水平，为数字化时代的网络环境提供坚实可靠的保障。

1. 资产一本账

资产一本账即全域资产统一管理，依据资产管理办法和细则结合系统等保级别和数据量计算资产价值，并对信息化资产进行发现、识别、入库、认领及审核工作，同时对各分子公司的信息化资产情况进行考核。依据部门职责划分资产类型，包括信息系统资产、云网主机资产、组件资产等。数据资产识别和治理模块能够识别多种资产类型和指纹信息，包括 Web 服务器、邮件服务器、数据库、

终端等等。本功能不仅提供手动登记，更具备主动扫描、系统同步、流量识别及代理测绘等先进技术。在支持主动探测方式来发现资产的同时，也能实现基于流量、日志、脆弱性等数据进行资产无侵入式被动发现及纳管。新入网终端在 30 秒内即可被识别并加入未纳管资产管理。信息化资产（包括主机及组件资产）入库后，将会自动推进分组织认领及审核流程。后续跟进对资产的价值评估和脆弱性量化评分，同时提供基于设备、应用等多维资产视角。凭借全信息化资产安全管理制度，依托一体化综合运营平台，能够高效有序地开展信息化资产生命周期管理，实现资产识别、审核入库、状态更新、资产脆弱性评估等流程。通过季度检查以及年度考核的资产信息管理考核办法定期考察各组织资产填报的完整性及准确性，压实信息化资产运营的责任落实。

2. 漏洞一个库

漏洞一个库即资产漏洞统一管理，凭借资产一本账的全域资产管理基础，联动漏洞扫描器和第三方漏扫报告，发现各类资产的脆弱性及网络攻击暴露面，展现数据资产目前的网络安全、数据安全盲点。通过定期检查、安全众测、红蓝对抗、风险评估等手段，实现组织资产漏洞早发现、早预警和早处置及网络攻击暴露面的早管控和早收敛。在安全运营中结合资产、责任人、系统、部门，给出全面的资产风险评估、漏洞跟踪分析。在组件漏洞安全运营方面，支持软件供应链漏洞扫描、管理，支撑对代码或二进制制品进行脆弱性检测、组件依赖管理并生成软件物料清单。细粒度资产管理和全面漏洞运营实现了资产漏洞关联、组件版本和情报关联，实现资产的脆弱性管理和漏洞的统一运营，实现资产与漏洞信息的下发、修复、验证等漏洞运营闭环功能。

3. 风险一屏观

一体化运营在数据采集接入上，支持多种方式，包括 20 多种日志数据接入、流量数据解析、资产数据发现识别和威胁情报第三方对接。其多层次挖掘模型检测内置丰富的安全规则和算法模型，涵盖众多检测类别。智能安全分析模型应用 ATT&CK 攻击链，支持多种攻击场景和用户异常行为模型，基于自研分析模型引擎可自定义探索深度异常威胁行为。基于此，多维安全态势呈现通过内置多种态势大屏，从网络安全风险监测、数据安全风险监测、告警处置情况、资产入库情况、漏洞管理情况、异常行为、风险管理、各分子公司安全风险监测、风险专题等维度对组织安全情况可视化展示。

（三）技术一底座

电子政务安全运营目前处于“全面防御”与“精准聚焦”的战略转型压力。在安全运营刚刚开始建设的阶段，大部分工作可以凭借经验构建逻辑线条，虽未充分考虑安全规划问题，但这个阶段的工作多是重点工作，因此成效显著。下一阶段，安全运营工作试图补齐所有短板，覆盖所有潜在风险点，但受限于安全需求与业务逻辑脱节、安全人才储备不足、供应商技术方案滞后等现实问题，导致资源分散、响应效率低下，反而出现核心风险管理不善的困境。部分地区通过政务云平台建设和安全托管服务尝试优化风险管控模式，但整体仍未摆脱“被动响应”的路径依赖，亟需向最小自洽循环模式升级，即优先聚焦入侵响应、漏洞修复、攻防验证等核心环节，通过资源分级管理实现安全效能最大化。电子政务安全运营的发展正处于补齐短板阶段向最小自洽循环模型迈进的过程。安全运营流程管理中，传统标准化作业流程（SOP）逐渐失效、完全自动化响应转型受阻。

由 SOP 定义的操作规范标准化强，但因安全工作专业性强、覆盖范围广，导致 SOP 编写成本高、执行转化层级多，加之安全人员对流程的遵从度和理解度不足，实际落地效果不佳。当前安全运营已开始探索全自动化转型，通过安全运营自动化系统（SOAR）将专家经验转化为可执行的剧本，实现关键流程的闭环管理，但受限于技术成熟度、数据接口兼容性及数字底座覆盖度，安全运营自动化程度不足，大量非核心流程仍依赖人工协作，形成核心流程自动化与人工协作流程并存的过渡态。后续的技术建设需通过引入具备持续运营能力的供应商和融合 AI 技术的智能工具，逐步构建技术赋能、动态迭代、持续安全的纵深防御体系。

技术一底座即一体化安全技术底座以“全场景协同、集约化赋能”为核心，构建覆盖网络安全、数据安全、应用安全的通用技术能力体系，通过统一架构设计与资源整合，为安全运营提供标准化支撑。在网络安全领域，底座集成蜜罐诱捕、漏洞扫描、下一代防火墙（FW）、网络流量分析（NTA）等能力，实现对网络边界、核心链路的全流量监测与威胁阻断，结合威胁情报的实时关联分析，形成“攻击面收敛-威胁检测-异常响应”的闭环防御。数据安全能力体系围绕数据全生命周期构建，通过数据分类分级、流转监测、脱敏处理、水印溯源、数据库审计（DBA）等技术，实现重要数据从产生、传输到存储、销毁的全场景管控，配合分层响应机制与多部门协同研判，快速定位数据泄露、越权访问等事件的根本原因。应用安全能力则整合应用漏洞扫描、代码审计、软件供应链安全管理、API 监测等模块，深度融入软件开发生命周期（SDLC），从源头防范注入攻击、逻辑漏洞等风险。

底座通过 IDaaS（身份即服务）、DaaS（数据即服务）、EaaS（加密平台

即服务）、AIaaS（人工智能即服务）的服务化封装，实现能力的标准化输出与灵活调用。IDaaS 统一管理用户身份认证与权限分配，支撑“最小授权”原则落地；DaaS 聚合多源威胁情报（含漏洞情报、APT 情报、恶意 IP/域名等），通过情报融合处理与关联分析，为威胁预警、事件响应提供数据支撑；Eaas 提供标准化加密能力；AIaaS 依托机器学习算法，对安全事件进行智能分类、风险研判与攻击预测，提升威胁分析的自动化与精准度。

通过基础安全技术平台的统建模式，一体化底座打破传统安全能力的碎片化建设困局，形成“资源集中管理、能力统一调度、策略全局协同”的运营体系。该模式不仅降低各级机构的安全建设成本，避免重复投资与资源浪费，更通过标准化能力输出与协同机制，推动安全防护水平的整体提升，实现从“单点防御”向“体系化联防”的转型，为数据安全事件处置、威胁情报应用等场景提供技术支撑。

4.1.3 成果与价值

在制度层面，基于某电子政务安全顶层规划，构建了覆盖一二级核心制度、三四级执行细则的分层制度体系，发布多项关键安全管理制度，推动分子公司与部门完成配套制度建设，形成顶层设计、中层管理、基层执行的制度闭环，为安全运营提供规范化依据，实现安全工作从经验驱动向制度驱动的转型，强化了安全管理的标准化与合规性。在管理层面，通过构建三级联动安全运营架构，打通总部、分子公司与相关部门的协同链路，显著提升集中监测、统一报障、应急处置等工作效率，实现安全事件的分层响应与闭环管理。同时，以管理和技术双轮驱动推进资产一本账工作，完善资产管理流程与考核机制，形成系统、主机、组件

三级联动管理模式，结合常态化安全检查、渗透测试及重保任务实施，构建“以检促建、以改促防”的管理闭环，提升资产风险管控与应急响应能力。在技术层面，依托一体化安全运营平台的持续迭代，整合终端安全管理、特权账号管控、数据安全监测等技术能力，实现资产、漏洞、风险情报的集中管理与联动分析。通过引入多源威胁情报融合技术，强化实时攻击监测与预警响应，结合平台功能模块的智能化升级，推动安全运营从人工处置向自动化、智能化转型，为政务系统安全运行提供技术支撑，提升整体安全防护的精准性与时效性。

4.2 某运营商一体化网络安全运营

4.2.1 背景与挑战

随着数据安全上升为国家数字经济战略核心，企业数据保护、隐私安全及跨境传输监管强化，监管机构对数据全生命周期安全管理提出更高要求。运营商行业手握巨量国民个人信息及敏感数据，又为国家关键信息基础设施之一，其面临的挑战更为严峻，安全风险更为尖锐。

某运营商在安全运营中暴露出传统安全架构与新型风险场景的能力错配问题，表现为标准化防护的“技术孤岛”、运营支撑的“流程断层”、智能化应用的“效率瓶颈”以及新技术场景的“能力真空”。安全标准化防护存在结构性短板：流量防护技术上存在重复建设、告警过载问题，且各模块技术标准未完全统一，导致安全防护效果参差不齐；安全能力模块间缺乏有效联动和防护效果主动验证机制，难以形成场景化防护合力，虽已建设多层级防护体系，对难场景新技术仍然存在安全风险管控缺口。安全运营支撑能力存在机制性缺陷：IT 资产与敏

感数据纳管不充分，安全数据汇聚加工不充分，导致安全分析缺乏有效数据支撑，风险研判精准度受限；跨设备及平台的安全事件协同依赖人工介入且通过碎片化接口实现，流程跟踪控制缺失，难以形成闭环管理；缺乏业务侧资产资源实时同步机制，全量资产清单动态更新困难，导致安全策略与实际资产状态脱节。智能化安全能力显著不足：安全监测、审计及处置环节自动化水平低，人工参与度高，应急响应效率低下；对 AI 驱动的新型攻击缺乏智能化检测模型，传统规则引擎难以识别复杂攻击模式，防护手段滞后于攻击技术迭代。新技术场景下专项能力缺口突出：数据泄露风险管控手段不足，难以满足数据安全战略及监管要求；云原生漏洞检测与修复能力薄弱，且对供应链风险缺乏全链路监控，技术依赖导致系统性风险累积。

数智化安全运营打破传统安全运营的人力依赖与技术瓶颈，推动安全防护从被动应对向主动防御转变。在改进方向上，一方面利用自动化手段实时感知增量风险，通过智能监测与分析快速识别新出现的安全威胁并及时阻断，有效解决增量风险遗漏问题；另一方面，借助数据建模对安全运营过程中的各类要素进行标准化处理，通过指标量化精准衡量安全效果与风险态势，从而持续优化存量风险治理策略、提升安全防护策略的精准度，实现网络安全运营效能的全面提升。

4.2.2 安全运营体系设计及技术方案

（一）两级安全建设架构

某运营商构建总部与省公司两级统一安全运营架构，强化纵向协同管理机制：通过安全运营管理中心统筹两级职能，实现重要数据在数据中心的两级同步协同，同时各安全专业平台履行专业领域内的纵向管理职责。在任务调度层面，

制定统一的安全工作流两级接口标准，依托安全运营中心实现跨层级工作流的无缝互通，确保安全策略与执行任务的上下对齐。数据支撑方面，建立两级安全数据通道接口规范，基于安全数据中心实现总部与省公司的数据双向流通与共享，为风险研判与决策提供数据基础。针对安全业务协同，各支撑平台根据专业场景需求（如网络安全、数据安全、云安全等），定制化确定纵向协同交互方式，形成覆盖策略制定、执行落地、效果反馈的全链条纵向协同体系，有效提升两级安全运营的一致性与联动效率。

（二）两中心数智化横纵联动协同

1. 安全数据中心

安全数据中心通过数据集中存储、分类、标识、处理及开放共享的系统化设计，构建全域数据治理与服务中枢，实现安全数据的全域治理与价值释放。

数据集中存储致力于多源异构数据的统一承载，构建标准化存储体系以解决数据分散与格式异构问题，整合网络流量日志、终端操作记录、安全设备日志等多源数据，支持关系型、列式、时序及图数据库等混合存储架构，通过分布式集群部署实现 PB 级数据弹性扩展，保障数据存储的完整性、可用性与高效性。**数据集中分类**依托基于企业内部标准的精细化数据治理，建立分类分级体系实现安全数据有序管理，进行主题分类（用户数据、业务数据等）与安全分级（核心敏感数据、重要数据等），自动化分类工具结合人工审核对非结构化、半结构化及结构化数据进行智能分类，形成数据目录，为数据安全策略制定与访问控制提供基础凭据。**数据集中标识**聚焦全域数据资产的唯一身份体系构建，通过统一标识机制解决数据关联混乱与溯源难题，为各类数据资产分配唯一标识并建立“数据

-资产-业务”关联映射，实现全链路溯源，为安全事件分析提供精准数据关联能力

数据集中 ETL 构建一站式接入体系，借助对 20+接口种类、100+设备类型的支持及 30+处理算子能力，完成多源异构数据的统一采集、清洗转换与无感化接入，形成全域安全数据“统一入口”。通过标准化处理流水线确保数据可用可信，借助 ETL 工具链实现多源数据清洗转换，抽取阶段支持多种数据源接入，转换阶段完成时间格式统一、IP 标准化及敏感数据掩码处理，加载阶段按主题存入安全数据集市（包括资源数据集市、安全告警集市、日志数据集市和威胁情报融合等），为上层分析应用提供有效数据和关联特征输入。**数据开放架构**通过标准化服务接口支撑跨层级跨系统数据流通，设计 REST API、消息队列等多模式接口支撑安全可控的数据共享体系，实现总部与省公司数据双向同步及安全能力平台数据调用。同时，在数据共享过程中进行权限管控、流量控制及数据加密，在保障安全前提下支持数据按需共享。

2. 安全运营管理中心

安全运营管理中心通过资产、策略、能力、流程、考核五大运营模块的系统化运作，实现全网安全资源统筹与运营效能提升，构建全要素协同的立体化运营体系。

安全资产运营覆盖基础设施资产与数据资产的全域管理，依托安全数据中心的标准化接口进行数据目录调取查询对资产全生命周期进行精细化管理。重点对资产进行风险分级与安全标签化，为策略制定提供精准靶向。同时，结合漏洞扫描结果、访问日志异常及资产脆弱性，实时计算资产风险指数并自动生成风险资

产清单，触发后续加固流程。

安全策略运营结合业务特性、风险场景及合规要求，构建“总部统筹-省公司落地”的分层级协同、动态化适配策略管理机制。安全策略运营基于资产风险评估、威胁模型及合规基线，生成差异化策略（如生产环境与开发环境的不同访问控制策略）。总部制定基线策略，借助标准化接口将策略下发至执行单元。省公司则通过策略引擎对总部基线策略与场景化策略进行冲突检测与优先级判定，确保策略体系的一致性与可执行性，并基于本地业务特性细化执行策略。最后，安全策略运营模块会定期开展策略合规性扫描与攻击面暴露检测，形成策略合规性及策略效果评估报告，保障策略的有效执行与持续动态调整。

安全能力运营聚焦技术融合与协同赋能，整合分散的安全能力，建立安全能力清单并明确各专业平台能力边界，实现能力按需调用。对安全数据集市、全网威胁情报服务、告警定位分析、资产智能测绘、数据水印溯源及脱敏、数据防泄漏等安全能力、攻击面管理能力进行标准化、服务化封装，为安全运营工作流程化编排及各安全支撑平台提供统一的服务化能力。在攻防实训及数据安全运营过程中，模拟 APT 攻击、自动化渗透、数据外发等难场景、新技术，动态验证安全能力的有效性，同时在攻防实战中沉淀威胁特征知识和专家防护经验以反哺安全能力的提升，形成安全能力迭代闭环。

安全流程运营以标准化驱动效率提升，构建端到端流程体系，编排安全事件处置剧本，完善策略变更、资产纳管等流程，通过安全运营中心统一制定的标准接口实现跨层跨域流程穿透，以形成“过程可管、进度可视、效果可评”的高效安全流程运营。安全流程运营通过调用标准化安全能力，实现重复性操作自动化

高效化、安全态势可知可感，最大程度将安全事件从发现、分析到处置全流程线上化，对剧本、案例进行有效性验证和实战优化管理。安全流程运营赋能安全运营从依赖人工低效模式到机器主导自动化范式的转变，在有效降低操作成本的同时，提升了安全响应的一致性、精准性与全局协同能力。

量化考核运营基于量化指标驱动实现持续改进，建立过程指标+结果指标双维度考核体系。其过程指标覆盖策略合规率、资产纳管率、流程自动化率等，其结果指标聚焦安全事件 MTTD/MTTR、数据泄露事件发生率、高危漏洞修复率等，结合业务影响评估形成综合评分，并以双维度考核指标推动运营效能的螺旋式提升。

（三）五大安全能力管理支撑

1. 安全威胁预警分析

安全威胁预警分析平台通过威胁分析模块和威胁处置模块的系统化构建，结合智能化技术与实战化需求，形成覆盖威胁检测、分析、处置的全流程安全威胁预警分析能力，推进全网安全威胁预警分析的智能化与实战化升级。

在能力建设层面，安全威胁预警分析平台构建了立体化威胁分析体系。围绕 ATT&CK 框架 14 个攻击阶段构建关联分析模型，将攻击路径拆解为可量化检测单元，结合资产权限推演潜在风险路径，建立包含技术点覆盖率、检测规则准确率、事件链关联度的三维评估体系，提升技术点覆盖面至 50%并新增 600 个细粒度分析模型及 70 个跨阶段事件链模型，实现攻击链全流程追溯。引入图引擎和安全知识图谱技术构建“实体-关系-属性”图数据模型，新增基于图特征的最优路径搜索、异常检测、行为相似度匹配、自定义子图匹配四大算法，配套长链

攻击、相似度攻击等攻击模式匹配检测，解决海量告警关联分析难题并深度检测复杂攻击场景。安全威胁预警分析平台构建覆盖“特征识别-事件聚合-攻击链路”的三层检测体系，实现单个攻击动作精准捕获、批量攻击检测灵敏度提升及完整攻击链自动生成，推动安全分析从逐告警研判转向链条式风险评估，形成“单点检测-链条关联-体系化防御”的递进式安全分析能力。

威胁处置基于威胁预警分析结果，以安全事件匹配预置剧本进行安全流程自动化响应，剧本编排支持跨平台联动执行终端安全策略下发、异常账号权限管控等止血操作。通过安全流程运营实现自动化处置，打通威胁检测与响应环节，应对流程碎片化与人工介入多的问题，提升安全运营的处置效率与协同能力。

2. 数据安全技防能力

数据安全技防能力体系以数据安全防护场景为导向，通过“安全防护筑基、支撑能力赋能、运营治理落地”的三维架构，构建与业务深度融合的立体化防护体系。运营商四大数据安全相关业务场景（数据共享开放，结算业务处理，营销运营数据统计和生产开发维护）间共性能力复用配合差异化适配，确保不同业务场景下的数据安全需求均能通过标准化安全能力与差异化策略组合落地，构建“识别精准、管控精细、审计全面”的立体化数据技防体系，实现数据安全与业务发展有机融合，支撑业务创新和数据价值释放。

四个主要数据安全相关业务场景的数据安全防护都离不开数据安全防护能力筑基。在数据安全资产管理方面，均通过数据资产智能测绘及数据分类分级引擎完成敏感数据定位，输出统一格式的安全标签。并依赖资产测绘及数据流转监测能力系统获取数据存储位置、业务关联关系，为策略制定提供资产上下文。同

时，在策略层面根据场景需求动态加载脱敏、审计、处置等细粒度策略，实现一处配置、多场景复用。统一提供商用加密密钥服务，支持不同场景的密钥生命周期管理（例如，开发环境密钥每日轮换、共享场景密钥按合作周期销毁等）。最后，在监控审计层统一收口，各场景业务日志统一接入安全数据中心，实现多维度检索，SIEM 系统内置场景化分析模型赋能跨场景风险关联分析（如，开发环境数据泄露与共享场景异常访问的联动告警）及基础数据安全防护能力度量优化。

上述四个数据安全相关业务场景的数据安全防护各有侧重点，在最大程度复用标准化数据安全防护能力的情况下，配合差异化安全能力组合及细粒度策略施行可以实现复杂业务场景下的数据安全技防最佳实践。数据共享开放场景重点在于确保共享数据在权限可控、内容合规、流转可追溯的前提下实现按需开放，避免敏感数据过度暴露或违规使用。在结算业务处理场景中，关键点在于保障交易数据从输入到输出的完整性、机密性和一致性，防范数据篡改、泄露及异常交易风险。而营销运营数据统计场景的核心是在用户数据统计分析中实现“数据可用不可见”，防止个人信息滥用及分析结果泄露。最后，在生产开发维护场景，重点在保护开发测试环境中的数据不被非法获取，避免生产数据因环境混用或操作不当导致泄露。

数据安全是网络安全运营的一个核心任务，而数据安全与业务安全高度耦合，实现数据安全的基础是实现业务安全。数据安全技防能力体系是数智化安全运营其中一个重要体系，可以推动数据安全从成本中心向价值转化中心转变，并为企业在数据要素市场化配置中构建安全竞争力。

3. 身份权限安全管控

身份权限安全管控以“身份为锚、权限为纲”，通过账号统一管理平台整合认证、授权、审计能力，构建覆盖“访问前身份校验、访问中权限控制、访问后行为审计”的闭环体系，实现“合法身份、最小权限、全程可溯”的安全目标。

身份认证体系融合聚焦解决身份认证碎片化问题，通过 FIDO 中台整合无密码认证、生物识别、硬件令牌等多因子认证方式，支持终端设备接入以实现动态组合认证，区分业务/运维，内/外人员的不同用户身份角色，在开户、登录环节实现身份“四照合一”，关键场景触发二次增强认证，推广无密码认证。访问控制融合围绕实现最小权限原则精准落地，依托账号统一管理平台打通 AD 域控、云账号、第三方系统的账号生命周期管理，借助自动化流程实现账号创建、权限分配、离职回收全流程线上化，基于 ABAC 模型结合用户角色、数据标签、访问场景动态生成访问策略以支持字段级权限、行级过滤及敏感表操作强制二次审批，对服务器、虚拟机实施文件级权限控制、命令级黑白名单并结合 UEBA 识别异常操作，避免“权限过度授予”导致的越权访问、数据泄露风险。能力服务融合整合分散的身份权限能力，通过统一身份服务中台提供标准化 API 接口支持业务系统快速接入并对接安全数据中心实现认证日志、权限变更记录集中存储与分析，利用策略引擎自动同步总部基线策略与业务线个性化策略，在零信任架构下结合终端安全状态动态调整访问权限，使未通过安全检测的设备仅能访问受限资源池、合规设备可访问全量授权资源，形成统一服务接口以支撑业务快速调用与安全策略下沉。涉敏行为管控旨在保障核心数据安全同时兼顾业务灵活性，对涉敏系统采用“访问申请-分级审批-操作审计”流程，通过堡垒机录制特权操作会

话并结合 OCR 技术识别屏幕截图中的敏感信息以对异常操作自动触发熔断机制，为涉敏岗位配备专用云桌面实现“终端设备与数据存储分离”并在云桌面内启用动态水印，借助机器学习分析涉敏操作模式以对低概率高风险行为触发增强验证、对高频正常操作简化认证流程，避免过度管控影响效率。

4. 安全审计

安全审计以安全数据中心（SDC）为底座，构建分析层、管理层、智能应用层与运营层协同的立体化架构，通过数据驱动、AI 赋能实现审计场景的全域覆盖与智能化升级。分析层以业务特征建模为核心，依托安全数据中心整合的多源数据，通过自然语言处理、词嵌入聚类等技术提取业务关键特征，并按照业务属性、风险等级进行标签化处理，形成业务特征库与标准化业务规则库。在此基础上抽象典型审计场景（如特权账号异常登录、敏感数据跨域流转），利用业务特征与标签对日志、操作记录等数据进行关联分析，实现审计对象的精准定位与风险特征提取。管理层聚焦审计流程的规范化与自动化，通过审计策略管理模块制定覆盖不同业务场景的审计规则，支持策略的分级下发与版本管控；审计任务管理模块承接分析层输出的审计场景，自动拆解为可执行的检测任务，并分配至相应安全平台；审计报表生成模块根据预设模板（如合规报告等）自动汇聚审计结果，支持多维度查询与可视化展示，为管理决策提供数据支撑。智能应用层通过三大模型实现审计能力智能化升级，基于数据泄露行为模型对文件外发、API 调用等行为进行建模，结合流量特征识别潜在泄露风险；基于账号权限操作模型分析特权账号登录时间、操作指令，通过行为基线检测越权访问、权限滥用等异常操作；基于访问风险研判模型整合设备指纹、地理位置、时间窗口等多维属性，动态评估访问请求风险。三大模型通过在线学习持续优化，实现对新增审计场景

的自适应检测。运营层通过人员画像整合员工岗位权限、操作习惯、历史风险记录，通过账号画像关联账号生命周期与权限分配记录，通过资产画像汇聚资产类型、安全标签、漏洞状态等信息，形成立体审计视角。同时，运营层依托安全数据中心的关联分析能力，还原“账号登录→权限调用→数据操作→结果输出”的身份活动全链路完整轨迹。运营指标体系建立覆盖审计覆盖率、异常事件检出率等核心指标，为审计能力评估提供量化依据和优化方向。

安全审计发展目标围绕“场景化、智能化、一体化”持续演进，基于 SDC 数据底座不断丰富审计业务特征库，引入人工智能的建模分析预测能力，实现身份活动从登录认证到权限操作的全链路可视化跟踪。通过扩展审计对象范围，构建人员、账号、资产三类画像的深度关联模型，推动审计场景从规则驱动向数据驱动转型。同时，审计运营能力全面融入数智化安全运营，实现审计任务从“人工触发”到“自动化分派”的升级，最终形成数据贯通、模型智能、流程自动的一体化审计运营体系，为企业安全决策提供全维度支撑。

5. 安全评估检测

安全评估检测体系以基础能力协同为支撑底座，通过封装合规服务化能力形成标准化接口，供各个支撑平台调用，实现总公司与省公司在检测标准、基础数据（威胁情报、资产清单、策略模板）的两级协同。总公司统一制定安全评估检测规则框架，省公司基于本地业务特性补充细化，共享资产指纹库、漏洞知识库，避免标准冲突与重复建设。安全评估检测以服务化、自助化、国产化为目标，构建全网统一的安全评估检测能力调用平台，支持各省公司及业务部门通过 Web 门户自助调用漏洞扫描、基线检测、弱口令识别等安全能力。在漏洞基线

综合治理层面，通过与 SDC 联动构建全网漏洞一张图，整合资产暴露面、漏洞详情、威胁情报等基础数据，实现漏洞从发现、验证、修复到复测的全生命周期管理。同步生成全网健康评估一张图，按业务线、地域、资产类型展示基线合规率、漏洞修复率等核心指标，为漏洞考核提供实时数据支撑。场景化检测能力强化围绕“两高一弱”（高危漏洞、高风险资产、弱配置）治理、专项漏洞整治、POC 验证等需求，构建差异化检测策略。

安全评估检测自动匹配检测模板并生成任务工单，实现能力调用从“线下申请、人工分配”到“线上自助、智能调度”的转型。同步推进国产化技术适配，完成与国产漏洞扫描检测工具的接口对接，构建国产化漏洞库，确保检测能力全面兼容信创环境。

4.2.3 成果与价值

数智化安全运营架构通过技术创新与流程优化，有效应对传统安全运营的核心挑战及运营商行业面临的安全运营挑战。在增量风险遗漏方面，依托无侵入式被动发现技术，基于日志和脆弱性数据，实现入网终端快速识别并纳入未纳管资产管理，结合多资产类型与指纹信息识别能力，大幅降低新资产带来的未知风险；通过 ATT&CK 能力评估举证，全面评估检测能力对攻击阶段和技术的覆盖度，为检测模型优化提供方向，增强对新型攻击的发现能力。针对存量治理低效，架构构建自动化处置体系，利用剧本编排与自动化执行，将重复性安全操作的人工参与度大幅度降低，释放人力专注高级威胁研判；通过标准化运营流程和自动化执行，实现日常扫描任务、漏洞修复等操作的周期化自动处理，显著提升存量资产的安全治理效率。在策略精准度不足问题上，威胁分析预警平台整合多

源数据构建量化评估模型，输出资产风险评分、攻击成功概率等指标，为决策提供精准依据；身份权限管控平台基于 RBAC/ABAC 技术实现细粒度权限控制，并通过数据分类分级管理建立差异化防护基线，提升策略制定的精准性；同时，攻击链分析模型精准定位攻击纵深行为链路，结合图模型构建能力，可针对任意攻击特征定制检测策略，增强对复杂攻击的识别能力。对于处置及时性低，安全运营中心的自动化处置能力实现事件与剧本的自动关联，低危事件全自动执行处置流程，高危事件快速完成自动化预处理并推送人工研判，大幅缩短 MTTR；联动处置功能支持与安全设备实时联动，实现“通知-封堵-溯源-通报”的链式响应，针对高危攻击源即时阻断，确保安全事件得到及时处理；通过主动威胁感知和响应机制，实现对关键资产威胁活动的实时监测与快速响应，显著提升整体安全处置效率。

4.3 本章小结

数智化安全运营的实施需遵循三大核心原则：**数据先行，**预先梳理资产分类、数据接口及指标定义，构建统一数据底座以解决数据缺失与格式混乱问题；**场景驱动，**从变更管控、漏洞巡检等高耗时高风险场景优先部署自动化工具，再逐步向复杂场景扩展以降低实施难度；**组织协同，**建立跨安全、业务、IT、运维部门的协作机制，通过指标透明化促进跨部门共识，避免安全与业务脱节，实现技术与管理深度融合。

数智化安全运营通过整合风险感知、治理、防护、响应、检验等多维度场景，构建全闭环体系：依托安全产品运行数据、资产信息及运营指标的集成与多视角可视化，实现安全风险的全局可观测与精准追溯；针对增量与存量风险，借

助自动化扫描、巡检及策略优化技术提升治理效率与覆盖完整性；通过定期自动化巡检、智能策略生成及动态熔断机制，保障安全能力覆盖率与策略执行精准度；基于多源数据整合与预定义响应剧本，将威胁处置效率从小时级压缩至分钟级；建立标准化检验流程与统一资产模型，通过量化指标与趋势分析实现防御体系的持续优化，最终形成数据驱动、智能协同的立体化安全运营架构，全面提升安全防护的主动性、精准性与有效性。通过构建以安全运营中心为核心的一站式体系，整合数据驱动的风险治理、智能联动的风险防护、高效协同的威胁响应与量化检验的效果评估，实现从“被动救火”到“主动防控”的范式转型。

未来，需持续强化数据模型的深度应用与智能化工具的迭代创新，推动安全能力与业务需求的深度融合，为企业数字化转型构建可持续的安全免疫系统。

第 5 章 安全运营的未来展望

集安全能力统一管理、安全数据互通和安全防护协同联动于一体的数智化安全运营已经是现阶段乃至今后很长一段时间的安全运营终极形态。但就数智化安全运营本身而言，其智能化和数据化各方面的发展潜能还有待发掘，随着科技的进步和数字化应用的普及，数字化安全运营在可预见的未来会持续精进。

5.1 AI 赋能的安全运营将全面崛起

现阶段安全运营主要通过大模型的新兴能力（上下文学习、指令遵循、逐步推理），实现了知识问答、威胁检测、告警降噪和钓鱼邮件分析几个场景应用。目前虽然并不能保证 100%的准确率，重要事件还需要人工复核，但也在一定程度上减轻了繁重的日常工作，缓解了安全运营人力资源紧张的处境。

随着 GenAI、AI Agent 和 Agentic AI 应用的高速发展，尤其是我国 AI 技术的突破，类似 DeepSeek 更理解中文语境的大模型诞生，AI 赋能的安全处置和回答的准确率将会越发平稳，同时也会开发出越来越多的安全场景，并且利用多模态能力实现的图像（网络结构、数据流等）、视频（物理安全监测、危险操作等）等安全场景应用同样会极大的提高安全运营的效率。

并且在具身智能的发展下，尤其是我国在该方面的领先优势，未来的安全运营分析师和设备操作人员可能变为 AI 智能机器人，而这些都会直接成为安全运营的管控对象，为安全运营又提出了更加严格和细致的要求。

AI 的发展还会促进 SOAR 技术的升级。虽然 SOAR 技术已经在安全运营工作中应用多年，但在国内的应用效果和使用体验中尚未取得良好成绩，主要在于

安全运营整体自动化程度不足以及 SOAR 自身智能化构建多场景流程的能力欠缺。随着数智化安全运营的普及，结合 SOAR 动态匹配安全场景的能力加强，安全运营工作的自动化、智能化水平将得到长足的进步。

5.2 数字化程度加深，安全运营需构建生态协同环境

数字化是将现实世界与数字世界的映射，数字化程度越高，数字世界越丰富，数据源头和种类也会呈现迸发式的增长。掌握安全数据的全面性是数字化安全运营的基础、智能数据分析是数字化安全运营的核心驱动力，这两方面将会在未来持续发展。另外对于数据的开发和利用将会迎来新的阶段，数据要素的价值释放会带动全行业加速数字化转型，数据的价值越高其风险就越高，对数据的安全保障将会在法规和技术层面携手前行。

同时，由于数据的量级和数字化对数据分析的需求不断增加，量子计算的大量和高速数据分析速度、隐私保护计算对敏感数据的保障利用、边缘计算对数据分析的实时性优化，都会成为安全运营技术能力中增加的部分。而相应的新技术都会带来新的安全需求，需要根据新技术的特性调整安全运营的架构以及策略，以利用新技术带来的能力提升和保障新技术带来的安全问题。

基于此，由于数字化程度的加深，安全运营的管理范围和技术能力不断增加，并且组织也会根据数字化的发展衍生出不可计量的特性化安全需求。面对如此庞杂的安全运营需求，没有任何一家厂商可以提供全部能力支撑，安全运营应该构建起资源、能力、咨询互补互助的生态环境，切实帮助客户实现经营目标。

5.3 实战化检验机制将得到深度应用

安全工作不容易得到广泛认同的关键在于其经济价值的隐蔽性，安全工作成果不易直观展现以及经济收益无法衡量换算，是用户与供应商共同面对的难题，但这一现象在数字时代将得到质的改变。

数字时代将网络空间与物理空间深刻对接与融合，在数字社会、数字生活中，在不远的将来人类必将感受到数字安全威胁的切肤之痛。关键信息基础设施将成为网络攻击的众矢之的、业务数据和个人信息将面临全天候的破坏和窃取，安全事件的影响将会扩散到每个人身上，安全防护没有平时与战时之分，每一分每一秒都是真刀真枪的碰撞。

经过数世咨询的观察，不止是国内，在全球范围内，安全运营过程中的高级威胁分析、防护以及高级专家等实战性能力的认可比例正在稳步提升，这一现象进一步证实了数字安全威胁正在朝着实战化的方向演变。

基于此，包括靶场演练、模拟推演、实战仿真、武装对抗的实战化检验机制将为安全运营装上一副价值放大镜，将经济损失和品牌影响直观的摆到台面上，能否经受住实战检验将成为安全运营工作必要性和有效性的考核标准。

北京数字世界咨询有限公司（以下简称“数世咨询”）是国内数字化领域独立第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监督机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，以及150余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接，安全产品与企业推荐，企业资源整合等

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区天鼎218文化金融园东外110号 网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

小酒馆

数世咨询
Digital World Consulting

数字安全领域独立第三方调研机构