数世咨询
Digital World Consulting

能力白皮书

AI 原生 SOC



©北京数字世界咨询有限公司

数世咨询
Digital World Consulting

能力白皮书

AI 原生 SOC

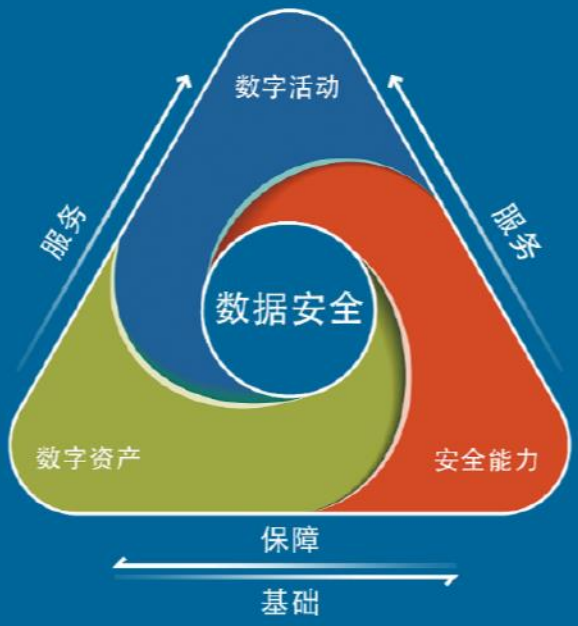
©北京数字世界咨询有限公司

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

数世咨询 刘宸宇

数世智库 数字安全能力研究院

版权声明

©2026［北京数字世界咨询有限公司］版权所有

本报告允许个人、学术、非商业场景完整引用，引用时请注明原文来源与作者。

任何商业转载、摘抄、二次改编、商用推广用途，须提前取得本公司书面授权，未经许可禁止商用，违者将依法追责。

目录

编者说明.....3

执行摘要.....3

第一章 安全运营的演进.....6

1.1 威胁演进：从个体黑客到智能威胁.....6

1.2 安全运营的四次跃迁.....7

1.3 产业数据：安全运营的市场与形态.....8

市场规模：连续三年下降，降幅收窄.....8

业务结构：产品与服务上升，集成下降.....9

安全服务占比：2025 年首次超过集成.....10

1.4 新拐点：从“外挂式 AI”到“AI 原生”.....11

第二章 安全运营的瓶颈与痛点.....12

2.1 数据：当前最突出的瓶颈之一.....12

2.2 人：安全运营的长期瓶颈.....13

2.3 架构：外挂式 AI 的天花板.....13

2.4 效能：“增产不增利”.....14

2.5 甲方真实诉求.....15

第三章 AI 原生 SOC 的定义与内涵.....16

3.1 两条技术路线.....16

3.2 数世咨询对 AI 原生 SOC 的定义.....17

3.3 四个判定标准.....18

3.4 概念辨析.....20

第四章 AI 原生 SOC 的核心技术架构.....21

4.1 数据层 21
4.2 核心架构层 22
4.3 智能层 23
4.4 应用层 24
第五章 落地路径与建设方法论 26
5.1 三类用户的切换路径 26
5.2 迁移挑战 27
5.3 高质量数据集与成熟度演进 27
5.4 建设原则 28
5.5 交付形态与合规 28
第六章 安全运营的未来趋势 30
6.1 人机协同关系将从“人在环中”转向“人在环上” 30
6.2 安全运营将走向按效果付费 30
6.3 安全运营将从 IT 视角拓展到业务视角 31
6.4 安全的价值标准将从“守底线”转为“提上限” 31
6.5 人才梯队建设的新难题 32
附录 AI 原生 SOC 代表性实践 33
Palo Alto Networks · Cortex XSIAM 33
CrowdStrike · SafeMind 34
微步在线 · OneSOC 35

编者说明

本报告为数世咨询基于公开资料、产业调研与行业访谈形成的第三方研究。报告中的数据主要引自数世咨询历年《中国数字安全产业年度报告》及《数智化安全运营报告 2025》等公开成果；涉及闭门讨论的内容，仅用于形成研究结论，不引用具体数据与引语。

报告对“AI 原生 SOC”这一方向做概念梳理与定义探讨，旨在为行业提供一份可讨论、可对照的参照。报告中提及的厂商实践仅作为行业案例的客观呈现，不构成数世咨询对任何厂商的推荐或评价。

勘误或合作，请联系本报告主笔分析师：刘宸宇 liuchenyu@dwcon.cn

执行摘要

数字化进程的持续深入，使网络安全的关注点从“建设”转向“运营”。当安全能力体系的基本框架逐步搭建完成，用户的关注点也从“有没有”转向“行不行”“好不好”——安全运营由此成为数字安全体系中价值最为集中、也最具挑战的环节。

过去数年间，安全运营的形态经历了从 SIEM 产品化、到服务化（MSS）、再到自动化编排（SOAR）的数次演进。2023 年以来，随着大语言模型等技术的成熟，“数智化安全运营”成为行业共识方向，即通过 AI 赋能与数据驱动，将

安全运营从成本中心升级为业务价值枢纽。数世咨询在《数智化安全运营报告2025》中提出的“1+1+1+N”框架，对这一阶段的能力构成做了系统梳理。

然而，产业现实与理想图景之间仍存在差距。《中国数字安全产业年度报告（2026）》显示，2025 年我国数字安全市场规模为 887.43 亿元，连续三年下降。在整体调整的背景下，安全运营呈现出“热度高、价值向上”的特征——安全服务收入占比达到 18%，为 2021 年以来首次超过安全集成；安全运营同时位列新质百强与融资热点赛道。但一个值得注意的事实是，产业统计至今没有统一的“安全运营”营收口径，行业对“安全运营是什么”尚未形成共识。

更关键的是，安全运营的效能并未随投入同步提升。数据层面，全量日志收不上来、多源数据语义不统一；人力层面，安全人才结构性缺口、告警疲劳长期存在；架构层面，将 AI“外挂”于传统 SOC 之上的做法，能接触到的数据有限，能力主要聚焦于告警降噪；产业层面，AI 虽提升了研发与办公效率，却未带来相应的商业收入增长，“增产不增利”成为较普遍的现象。

本报告认为，上述瓶颈的根源，是 AI 与安全运营的结合长期停留在“旁路叠加”层面。当“外挂式 AI”的能力触及天花板，“AI 原生”成为安全运营演进的新方向。AI 原生 SOC，是从架构层将 AI 作为核心能力植入，而非在传统 SOC 之上的旁路叠加——数据、存储、编排、语义等技术选型对 AI 友好，使 AI 能够深度使用底层数据能力。本报告提出“数据原生、语义统一、Agent 优先、架构重构”四个判定标准，用于界定一个 SOC 是否实现了 AI 原生。

在落地层面，不同类型的用户存在差异化的切换路径：尚无 SOC 的用户可直接构建 AI 原生 SOC；刚建成传统 SOC 的用户可先以外部 Agent 过渡；合约即将到期的用户则倾向直接替换。这一过程需要开放数据库与核心引擎，成本不亚于重做底座，因此并非功能的简单升级，而是一次架构级的重建。

展望未来，Agentic AI 的全面崛起、人机协同的新范式、交付形态的服务化，以及生态协同与实战化检验机制的深化，将共同塑造安全运营的下一阶段形态。

安全运营的革新之变，本质上是从“AI 赋能”走向“AI 原生”的范式切换。对用户而言，这不仅是技术选型问题，更是安全运营体系能否与数字化业务同步演进的问题。

第一章 安全运营的演进

1.1 威胁演进：从个体黑客到智能威胁

自 1994 年我国全功能接入互联网以来，网络威胁的形态经历了若干阶段的演变。

1994 年至 2000 年，互联网应用刚刚起步，威胁主体以个体黑客为主，多以技术探测为目的，攻击的规模化和组织化程度较低。

2000 年至 2011 年，网络黑产逐步组织化、商业化。以经济利益为动机的网络钓鱼、金融诈骗等攻击成为主要形式，攻击者开始关注可规模化的牟利方式。

2012 年至 2022 年，国家级力量介入网络空间，关键信息基础设施成为重点目标。攻击的组织性、持续性和破坏性显著上升，攻击目标也从个体和企业，扩展到关系国计民生的关键领域。

2023 年以来，威胁态势发生质变。AIGC、量子计算等前沿技术催生了“智能威胁”。以 2025 年哈尔滨亚冬会为例，赛事信息系统和黑龙江省内关键信息基础设施分别遭到 27 万次和 5000 万次攻击，部分攻击代码明显由人工智能编制。这一案例在一定程度上表明，攻击方已开始利用 AI 提升攻击的效率。攻击的来源，正从“人在攻击”向“AI 在攻击”演进。

威胁的升级，直接倒逼防御体系的变革。当攻击的频率、速度和复杂度超出

人工处置的极限，安全运营必须从依赖人力，转向依赖技术与数据的自动化、智能化能力。这是理解安全运营后续演进的基本背景。

1.2 安全运营的四次跃迁

面对持续升级的威胁，安全运营的形态也在不断演进。从技术与机制的角度，大致可以观察到四次跃迁。

第一阶段（SOC 1.0），以 SIEM 产品化为标志，安全运营以工具和设备为中心。SIEM 系统实现了日志的集中采集与关联分析，但运营高度依赖安全人员的经验和人工操作，效率受限于人的能力。

第二阶段（SOC 2.0 / MSS），以服务化为标志，安全运营以托管和运维为中心。面对安全人才短缺的现实，托管安全服务（MSS）将部分运营工作交由外部服务商承担，在一定程度上缓解了人力压力。

第三阶段（SOAR），以自动化编排为标志，安全运营以流程和联动为中心。SOAR 对重复性、确定性高的运营任务进行自动化编排，提升了响应效率，但自动化范围受限于预定义流程，难以应对复杂多变的威胁。

第四阶段（数智化安全运营），以 AI 赋能和数据驱动为标志，安全运营以数据洞察为中心。深度学习、自然语言处理等技术开始应用于威胁检测、告警降噪等场景，安全运营从“成本中心”向“价值枢纽”转变。

数世咨询在《数智化安全运营报告 2025》中，将数智化安全运营定义为：

“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。”报告进一步提出“数智化安全运营‘1+1+1+N’框架”——1 种运营环境、1 组安全运营能力、1 套健康运营体系、N 类安全运营场景。

需要指出的是，数智化安全运营强调的是 AI 赋能与数据驱动的结合。在这一阶段，AI 更多地以“能力增强”的方式作用于既有安全运营体系，尚未从根本上改变安全运营的架构。这为后续“AI 原生”的提出留下了空间。

1.3 产业数据：安全运营的市场与形态

安全运营的演进，也反映在产业数据中。

市场规模：连续三年下降，降幅收窄

从整体规模看，数字安全产业自 2021 年起由高速增长转为增长放缓。据《中国数字安全产业年度报告》，2022 年市场规模达到历史最高的 981.2 亿元，此后连续三年下降：2023 年为 973.7 亿元（-0.76%，首次负增长），2024 年降幅扩大至 -7.4%，2025 年为 887.43 亿元（-1.5%，降幅收窄）。

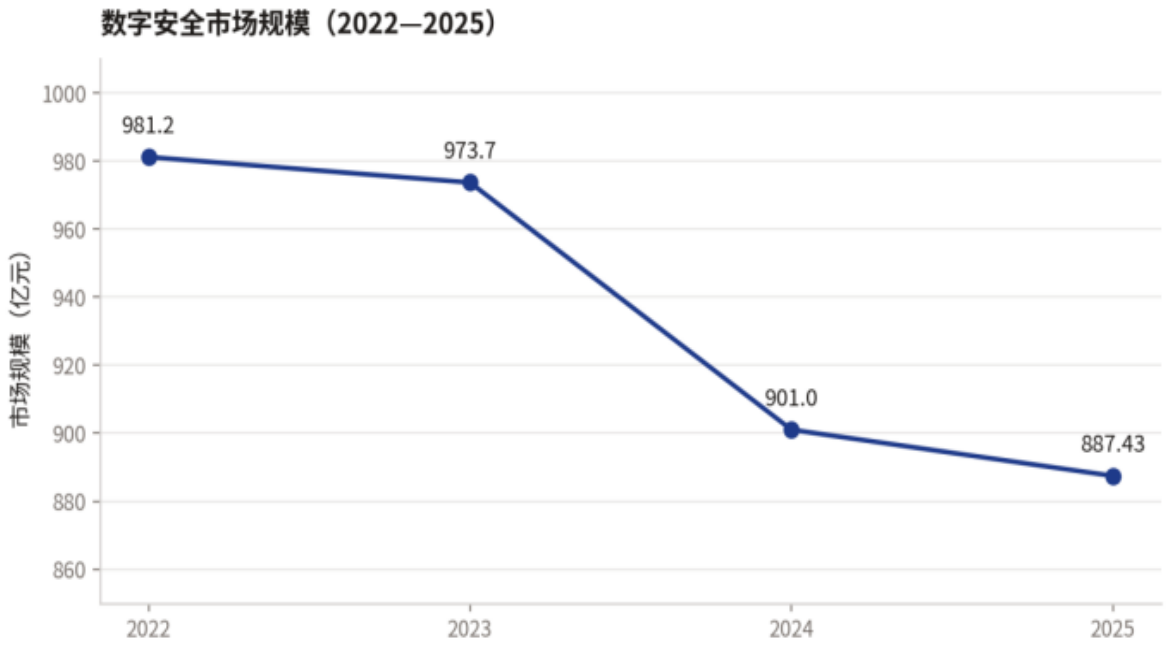


图 1 数字安全市场规模（2022—2025）

业务结构：产品与服务上升，集成下降

从业务结构看，三大业务（安全产品、安全服务、安全集成）中，安全产品与安全服务的占比上升，安全集成的占比下降。

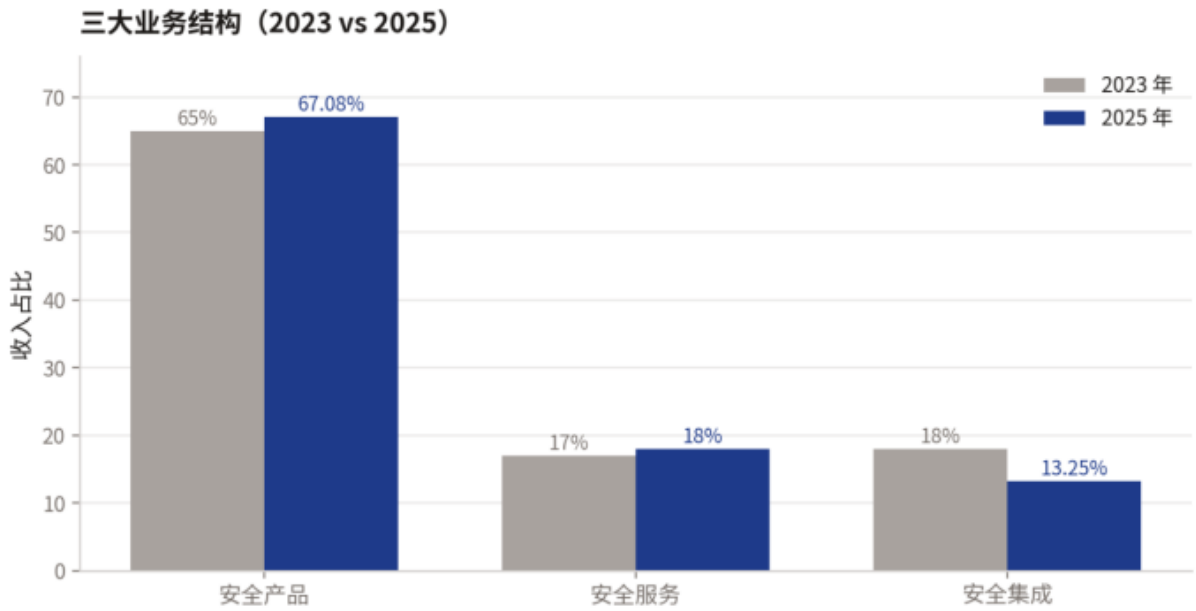


图 2 三大业务结构（2023 vs 2025）

安全服务占比：2025 年首次超过集成

2025 年安全服务收入占比达到 18%，为 2021 年以来首次超过安全集成收入（13.25%）。安全服务（含安全运营）占比的上升，从侧面反映出市场对运营类价值的关注度在提升。

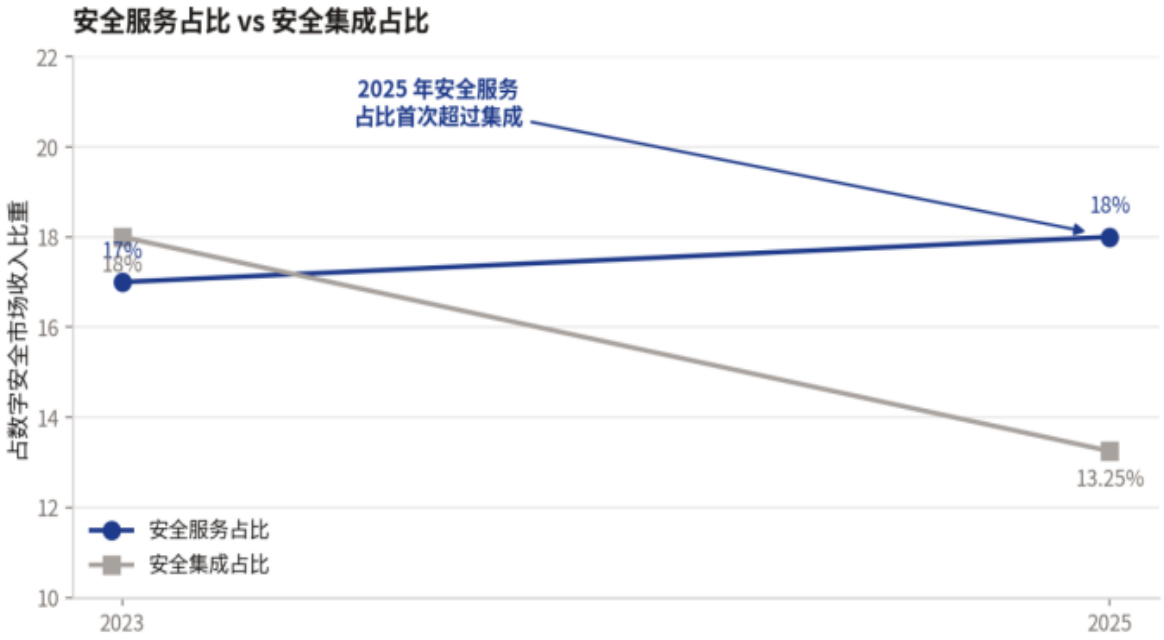


图 3 安全服务占比 vs 安全集成占比

从安全运营的形态看，数世咨询在“数字安全九大态势”中指出，不同场景、不同行业、不同规模的用户，对安全运营的理解和建设方式存在明显差异：头部客户倾向自建安全运营中心，腰部客户和数字化原生企业较适合安全托管模式，小型客户则选择公有云上的 SaaS 化服务。在认知层面，安全运营也大致存在三种理解：一是各类安全服务与运维，二是以统一管理平台为中心的探针集合，三是整个安全体系的规划、建设与运营。

一个值得注意的事实是：安全运营被列为热点赛道，但产业统计至今没有统

一的“安全运营”营收口径。这既反映出安全运营的内涵仍在演化，也说明行业对“安全运营是什么”尚未形成共识。从这个意义上说，对安全运营的重新定义，本身也是行业发展到一定阶段的必然需求。

1.4 新拐点：从“外挂式 AI”到“AI 原生”

当数智化安全运营逐步落地，一个新的问题开始显现：AI 在安全运营中的融入方式，进一步决定了其能力上限。

目前多数厂商的做法，是在原有 SOC 之上叠加 AI 能力（即“外挂式”），AI 主要通过 API 访问有限的运营数据。这种方式改造代价小、见效快，适合在既有体系上快速补充 AI 能力，但 AI 接触到的数据有限，作业面被限制在 SOC 已经开放的数据字段与场景之内，只能基于告警及其富化字段作出判断，而无法回到原始数据中重新求证，能力也难以超出既有场景。

与之相对，少数厂商开始从底层重构 SOC 的核心组件，将 AI 作为架构的一部分植入（即“原生”）。这种方式使 AI 能够更深入地使用底层数据能力，从而支撑传统架构难以实现的场景，但改造代价更大，对既有体系的兼容性要求也更高。

两条路线的分野，标志着安全运营正迎来一个新的拐点——从“AI 赋能”走向“AI 原生”。本报告后续章节将分别讨论这一拐点的背景（第二章）、内涵（第三章）、技术基础（第四章）、落地路径（第五章）与未来趋势（第六章）。

第二章 安全运营的瓶颈与痛点

在讨论“AI 原生”之前，需要先理解安全运营当前面临的实际困难。本章从数据、人、架构、效能四个层面梳理安全运营的主要瓶颈，并归纳甲方的真实诉求。

2.1 数据：当前最突出的瓶颈之一

安全运营的基础是数据，而数据恰恰是当前最突出的瓶颈之一。

其一，全量日志收不上来。 随着 IT 环境日益复杂，安全设备、系统、应用产生的日志种类和数量持续增长。受带宽、存储和成本限制，多数机构难以完整采集全量日志。而一旦采用“抽样”或“降量”的方式，就可能遗漏关键线索。数据的“收不全”，直接限制了后续分析的空间。

其二，多源数据语义不统一。不同厂商、不同型号的设备，其日志的字段定义、告警级别、时间格式各不相同。数据汇聚之后，往往需要大量人工进行归一化处理。数世咨询《网络安全态势感知能力指南》早在 2020 年即指出，“不同产品的对接成本高”是态势感知落地的难点之一——国内缺乏统一标准，不同厂商产品之间数据格式不同、接口难以打通。这一问题至今仍然存在。

其三，从告警（Alert）到事件（Incident）存在上下文缺口。业内有一种较为普遍的反映，安全产品在产生告警时往往无法同时提供研判所需的上下文数据，分析人员不得不转向业务系统、流量日志、数据库与操作系统另行取证，告警因

此难以被还原为可处置的安全事件。

2.2 人：安全运营的长期瓶颈

其一，安全人才结构性缺口。整个行业普遍缺乏安全人才，尤其是兼具行业经验和安全技术的人才。数世咨询《网络安全态势感知能力指南》指出，“态势感知体系离开了人，就变成了一堆无用的设备”。在部分大型机构中，安全团队规模与所辖资产规模严重不匹配：有的大型企业，其安全团队需要面对上千个系统，运营压力巨大。人才供给的不足，是安全运营长期面临的结构性约束。

其二，告警疲劳。随着安全设备数量增加、检测规则不断叠加，告警数量持续膨胀。分析人员大量时间消耗在低价值的告警筛查上，真正的高危事件反而可能被淹没。告警疲劳不仅降低了运营效率，也带来了漏判风险。

其三，人的价值面临重新评估。随着安全技术与工具的平权化，部分原本依赖个人经验的工作可以被工具承接。这并不意味着人不再重要，而是对人的定位提出了新的要求——从重复性的处置操作，转向更高层次的判断与决策。

2.3 架构：外挂式 AI 的天花板

在现有安全运营体系中，AI 的引入方式多为“外挂”，这带来了几方面局限。

其一，数据可见性受限。外挂式 AI 位于传统 SOC 架构之外，主要通过 SOC 封装的 API 调用方式访问数据。能接触到的数据类型和范围都受到限制，大量底层数据无法被 AI 直接使用；部分场景甚至需要通过"模拟读取页面"的方式间接

获取信息。

其二，能力止步于告警降噪。 受限于数据可见性，外挂式 AI 主要应用于告警降噪、知识问答等相对独立、边界清晰的场景，难以参与更复杂的检测与响应流程。

其三，难以增强检测能力。 由于无法接触底层数据，外挂式 AI 难以发现传统安全设备的漏检，也难以从多源数据中挖掘隐蔽的威胁线索。其价值更多体现在“减负”（降低告警量、减轻人工负担），而在“增强”（提升检测与响应能力）方面作用有限。

需要说明的是，外挂式 AI 并非没有价值。对于既有安全运营体系较为成熟的用户，它是一种务实、低成本的演进方式。但若要突破安全运营的能力上限，仅靠外挂难以实现。

2.4 效能：“增产不增利”

除技术与人的瓶颈外，安全运营在产业层面也面临一个突出问题。

数世咨询在《中国数字安全产业年度报告（2026）》中指出，AI 在研发和办公方面显著提升了效率，但效率提升未能有效转化为商业价值，企业的商业收入并未随之增长，形成“增产不增利”的局面。这一现象在安全运营领域同样存在：AI 的引入降低了部分运营成本，但尚未转化为可衡量的业务价值或收入增长。

造成这一局面的原因，一方面在于 AI 在安全运营中的应用效果尚不稳定，

不同场景下的表现差异较大;另一方面在于,安全运营的价值本身难以量化，“投入产出”缺乏统一的衡量标准。当技术投入无法对应到清晰的价值产出，用户在持续投入上难免犹豫。

2.5 甲方真实诉求

从甲方的角度，安全运营的诉求可以归纳为以下几点。

其一，高质量的数据集。AI 能否发挥效能，前提是拥有高质量的安全数据。数世咨询在数字安全产业年度报告中即指出，“缺乏高质量安全微调数据”是安全大模型面临的核心挑战之一。

其二，可观测、可解释的研判过程。 甲方希望 AI 的研判过程是透明、可追溯的——“降噪可观测、可解释”，而不是一个无法验证的“黑箱”。

其三，结论的可信度。 AI 给出的结论是否“敢直接使用”，是甲方关心的核心问题。在 AI 的能力得到充分验证之前，甲方往往倾向于让 AI 与人工“共同运行”，待准确率得到验证后，再逐步授予 AI 更高的权限。

其四，边界可控。 权限授出之后能否收回、AI 行为能否审计、出现误判由谁负责,这些是甲方在“敢用”之后必然追问的问题。预授权、可观测、可解释、可干预，是建立人机信任的一组必要条件。

这四点诉求指向同一个方向：安全运营的升级，不能仅靠 AI 能力的“叠加”，而需要在数据、架构与信任机制上做系统性重建。

第三章 AI 原生 SOC 的定义与内涵

本章在前两章的基础上，对“AI 原生 SOC”这一方向做概念界定：先梳理行业存在的两条技术路线，再给出定义、判定标准，并厘清其与相关概念的关系。

3.1 两条技术路线

从当前行业实践看，AI 与安全运营的结合存在两条技术路线。

路线一：在原有 SOC 之上叠加 AI 能力。 多数厂商采用这一路线。AI 以模块或功能的形式“外挂”于既有 SOC，主要用于告警降噪、知识问答等场景。这一路线的基本特点是价格与架构基本不变，改造代价小，能够较快地提供服务，也便于用户在其既有投资基础上平滑过渡。

路线二：从底层重构 SOC 的核心组件。 少数厂商采用这一路线。它们将 SOC 拆解为存储、编排、语义统一等组件，并让 AI 从架构层面参与其中，使 AI 能够访问更底层的数据能力。

两条路线在“AI 参与的深浅”上存在本质区别，主要体现在取数深度、编排方式和语义层级等维度：

- 在路线一中，AI 是位于架构之上的一个功能模块，AI 智能通过 SOC 封装好的接口进行取数，工作流程则是由人预先设定好，靠规则驱动，数据也仅仅停留在告警视角；

- 在路线二中，AI 则是贯穿架构的基础能力，AI 可以直接面对底层库表，按任务动态生成工作流，数据在存储层就完成了业务语义的统一。

需要说明的是，两条路线并非简单的优劣判断，而是适配不同用户需求与建设阶段的选择：对于既有体系较为成熟、追求稳步演进的用户，路线一较为务实；对于追求能力上限、愿意承担重构成本（或尚无历史包袱）的用户，路线二更具前瞻性。



图 4 传统 SOC 与 AI 原生 SOC 架构对比

3.2 数世咨询对 AI 原生 SOC 的定义

基于对两条技术路线的观察，数世咨询将“AI 原生 SOC”定义为：**不同于**

传统 SOC 之上的旁路叠加，而是在架构层面将 AI 作为核心能力原生纳入构建的 SOC，称为 AI 原生 SOC。

这一定义包含三个要点。

其一，AI 的位置。 AI 不是 SOC 之外的旁路模块，而是 SOC 架构的组成部分。SOC 的数据存储、告警生成、工作流编排等技术选型，均优先考虑对 AI 的友好性。也就是说，不再以“人能否操作”为唯一约束，而是要以“AI 能否直接使用”为约束条件。

其二，AI 的能力边界。 由于深度接入底层数据，AI 能够使用比 API 更丰富的数据能力和操作能力，从而支撑传统架构难以实现的场景。举例来说，针对同一批数据，相比传统架构，AI 可以基于历史经验自主优化检测能力，跨多个数据源还原出完整的活动链路。

其三，区别的本质。 两条路线的本质区别，在于 AI 参与的深浅。所谓“AI 原生”，指 AI 作为架构内生的执行与决策单元，与架构的耦合已经达到难以分割的程度。这与业内目前普遍存在的“使用了 AI（却包装成 AI 原生）”具有本质不同。本报告给出这一判据的目的，正是为了让“是否原生”可以被对照，而不是停留在口号层面。下面我们来看四个具体的判定标准。

3.3 四个判定标准

为便于实践中的应用，本报告提出判断一个 SOC 是否“AI 原生”的四个标

准。

标准	含义	观察方法
数据原生	AI 在授权与审计约束下直接面对存储层的数据对象，而非仅经接口层取数	检查是否存在接口层的字段裁剪；检查 AI 的数据访问是否有独立的最小权限、只读/写分离与全量操作审计
语义统一	在存储层统一语义，从“告警视角”转向“业务视角”，还原完整业务链路	取一条告警，看系统能否在没有人工补数据的情况下回答“谁、在什么时间、对什么对象、做了什么、是否正常”
架构重构	面向 Agent 重构架构，全平台能力对 AI 原生开放，支撑安全运营自主闭环	选取安全事件，检验 Agent 能否自主组合调用系统能力，完成研判、处置、验证与结果反馈
Agent 优先	产品逻辑为 Agent 设计，而非仅为人类操作	方向性取向：产品是否具备面向 Agent 的接口、身份与权限设计

四个标准中，“数据原生”是基础，“语义统一”是前提，“Agent 优先”是产品逻辑，“架构重构”是组织方式。它们共同构成“AI 原生”的判定框架。

其中，“数据原生”不仅指数据的可及，也包含支撑海量数据实时处理与 AI 高频调用的计算能力——数据"看得到"与"处理得动"，共同构成数据原生的完整内涵。

此外，“Agent 优先”这一判断，反映的是 AI 原生 SOC 在产品设计上的取向——在使用者构成中，AI 智能体所占的比例显著提高，产品逻辑需要相应地为 Agent 而设计，而不只是面向人类操作者。

需要指出的是，这四个标准并不要求所有 AI 原生 SOC 完全一致，而是提供一个可讨论、可对照的参照。不同用户可据此判断自身所处的位置，以及演进的下一步。

3.4 概念辨析

AI 原生 SOC 与“AI 赋能 SOC”“数智化安全运营”之间，是进化关系，而非对立关系。

从 AI 的定位看，“AI 赋能 SOC”强调的是在既有体系中增强 AI 能力，这里 AI 是“工具”；“数智化安全运营”强调的是 AI 赋能与数据驱动的结合，这里 AI 是“能力”；“AI 原生 SOC”则进一步要求 AI 成为架构的组成部分，这里 AI 是“基础”。

从“赋能”到“原生”，是 AI 与安全运营结合程度不断加深的过程，也是安全运营体系随技术进步持续演进的过程。这一演进并非否定此前的实践，而是在既有基础上，进一步释放 AI 的价值。

第四章 AI 原生 SOC 的核心技术架构

上一章界定了“什么是 AI 原生 SOC”，本章进一步说明“AI 原生如何实现”。从技术架构的角度，AI 原生 SOC 自下而上可以概括为数据层、核心架构层、智能层、应用层四个部分。数据层提供统一的数据与上下文，核心架构层支撑实时处理与能力调用，智能层组织分析与任务执行，应用层面向具体安全运营场景。如下图所示：



图 5 AI 原生 SOC 技术架构

4.1 数据层

数据层是 AI 原生 SOC 的基础。与传统 SOC 相比，AI 原生 SOC 在数据层的核心特征，是数据对 AI 的“可及性”。

（1）流式数据接入。面对不同品牌、不同格式的日志数据，摒弃人工定义解析规则的传统做法，改为引入“数据接入 Agent”，接入企业侧已有的各类安全设备日志，对接调查、处置用的多个安全工具，由 AI 自动进行字段映射，设置高中低等映射级别，完成解析插件的生成，这样既将原本需要人工开发的工作压缩至分钟级，又充分发挥了企业已有的安全投资不浪费。

（2）统一语义。数据汇聚之后，需要在存储层建立统一的语义。这不仅是告警视角的归一，更是业务视角的重建——从多源数据中还原“谁在什么时间做了什么、是正常业务还是异常操作”的完整链路。统一语义的实现，通常由人定义业务术语、由代码实现规则、由 AI 按规则处理。有了统一语义，安全运营才能从零散的告警，走向对业务活动的整体理解。

（3）上下文关联。有了原生多源数据和统一语义之后，就可以将告警与资产背景、历史行为、漏洞情报等关联起来，为研判提供更完整的信息，并根据需要建立实体之间的关系或图谱。此时，通过统一的数据模型与查询接口，完成上下文关联后的高价值数据就能够被 Agent 和其他分析能力调取使用，进一步减少跨系统取数与理解的障碍。

4.2 核心架构层

核心架构层连接数据层与智能层，其价值在于支撑实时的数据处理、频繁的能力调用和多步骤任务执行，让 AI 得以推进实际运营工作，是“数据原生”得以成立的地基。而权限管理与审计贯穿始终，随数据进入、能力调用与任务执行同步生效，对关键操作进行人工审批，使 AI 在明确的边界开展工作。

（1）流式处理与实时计算。安全数据持续产生，相关处理也需要随即实时进行。通过流式计算，对接入的数据开展解析、富化和关联，为 AI 提供及时更新的上下文。这套实时计算由弹性、分布式的计算底座承担。技术上可以采用 Flink 等流式计算框架，具体组件根据系统需要选择。

（2）面向 Agent 的能力开放。将数据查询、情报检索、调查取证和响应操作等能力，以 API 或 MCP 等方式开放给 Agent，便于其根据任务需要发现和调用。其中，MCP 主要用于连接 Agent 与数据、工具能力，不承担底层日志采集和流式处理的作用。需要再次强调的是，MCP 直连数据源、AI 高频取数等能力，底层都依赖弹性并发的计算支撑；缺了这套地基，能力开放便无从谈起。

（3）工作流编排与并发支撑。安全调查往往需要多次查询，调用多个工具，并根据返回结果循环处理。工作流编排与弹性、并发的计算能力这些任务提供运行支撑，使 Agent 的动态分析能够与既定流程衔接，也为持续运营提供基础。

4.3 智能层

智能层是 AI 原生 SOC 的“大脑”。

（1）模型底座。 当前安全运营所用的模型，多基于通用大语言模型，而非安全厂商自研的垂域大模型。原因在于，通用大模型的参数规模和能力已明显超出基于开源模型微调的垂域大模型，后者的投入产出比不具优势。这一选择反映了行业的一个重要判断：在安全领域，通用大模型的能力已经能够覆盖相当比例的需求，自研垂域大模型的必要性正在下降。

（2）Agent Teams。 单个 Agent 的能力有限。为处理复杂的运营任务，AI 原生 SOC 采用“Agent Teams”的方式：由主 Agent 统一调度多个辅助 Agent 与技能，协同完成任务。这种方式使 AI 能够应对需要多步骤、多工具协同的运营场景。

（3）自进化与记忆管理。 自进化使 AI 能够根据运营反馈持续优化研判策略与处置方法；记忆管理则沉淀资产背景、历史事件与处置经验，供不同 Agent 和后续任务复用。二者结合，使 SOC 的运营经验转化为可持续积累和改进的能力，减少重复试错，提升研判与响应质量。

4.4 应用层

应用层是 AI 原生 SOC 的能力出口。

（1）数字员工。 将安全专家的经验转化为可复用、可定制的“数字员工”，是 AI 原生 SOC 在应用层的重要方向。数字员工可以承接告警研判、调查取证、

设备巡检等运营任务，使用户可以按业务流程定制 AI 能力，实现对具体场景的适配。数字员工的意义，在于把原本依附于个人的经验，沉淀为组织可持续使用的能力。

（2）运营场景。 AI 原生 SOC 的能力最终落到具体场景：告警降噪、失陷主机调查、跨设备告警关联、钓鱼邮件分析等。与传统 SOC 相比，AI 原生 SOC 在这些场景中的参与更深，具备更强的上下文理解与关联分析能力。

（3）自然语言交互。通过自然语言发起任务、查看进展、补充业务背景和获取结果，降低使用复杂平台能力的门槛。人员可以围绕同一任务持续参与，在需要时调整目标、补充信息或完成关键审批。

第五章 落地路径与建设方法论

明确了 AI 原生 SOC 的定义与架构之后，本章讨论落地问题：不同用户如何切换、面临哪些挑战，以及建设过程中可依循的方法。

5.1 三类用户的切换路径

从传统安全运营向 AI 原生 SOC 迁移，因用户基础不同而路径各异。基于行业观察，大致可分为三类。

第一类：尚无 SOC 的用户。 这类用户没有既有投资的包袱，可以直接构建 AI 原生 SOC。实践中，这类用户（多集中于腰部及以下）对 AI 原生 SOC 的接受度较高，直接采用的比例也较高。

第二类：刚建成传统 SOC 的用户。这类用户建成传统 SOC 不久（1—2 年），短期内难以推倒重来，通常选择先以外部 Agent 的方式补充 AI 能力，作为过渡。这既保护了既有投资，也为后续的原生演进预留了空间。

第三类：传统 SOC 合约即将到期的用户。 这类用户在合约到期时，倾向直接替换为 AI 原生 SOC，并允许半年至一年的"双轨过渡"期，逐步完成切换。

三类路径中，从改造代价与收益比看，第一类用户是当前建议关注 AI 原生 SOC 的重点：他们没有历史负担，一步到位采用原生架构，能够更充分地发挥 AI 的价值。

5.2 迁移挑战

从技术角度，从传统 SOC 切换到 AI 原生 SOC，并非功能的简单升级，而是一次架构级的重建。

首先，需要开放数据库与核心引擎。AI 原生 SOC 要求 AI 能够访问底层数据，这意味着既有的分层逻辑需要重构，成本不亚于重做底座。

其次，需要同时满足“人”与“Agent”两类使用者的需求。传统 SOC 的产品逻辑主要面向人类操作者；在 AI 原生 SOC 中，Agent 成为重要的使用者，产品设计需要相应调整。这要求在产品逻辑上做增量设计，而非简单改造。

因此，迁移的难度主要不在单个功能，而在整体架构。这也解释了为什么“外挂式”路线在现实中更为常见——它的迁移成本更低，对既有体系的冲击更小。

5.3 高质量数据集与成熟度演进

AI 原生 SOC 的效能，最终取决于数据质量。数世咨询在数字安全产业年度报告中指出，“缺乏高质量安全微调数据”是安全大模型落地的核心挑战之一。高质量的安全数据，既包括高水平的标注，也包括标准化的日志字段。如何在新的技术条件下，快速补充高质量安全数据集，并将这些数据与 AI 能力有效结合，是 AI 原生 SOC 需要解决的问题。

从建设节奏看，安全运营的智能化难以一蹴而就，通常分阶段推进——从辅助感知，到智能驱动，再到体系融合，最终走向原生智能。数世咨询在《持续评

估定义安全运营》中提出，应“使不同发展阶段、不均衡发展状态的各类机构用户都具备安全运营的下限”。这一理念同样适用于 AI 原生 SOC 的落地：与其追求一步到位，不如先建立可用的“下限”，再持续提升。

5.4 建设原则

AI 原生 SOC 的建设，需要把握以下原则。

其一，确定性优先，逐步智能化。确定性的问题，优先用规则和流程解决；复杂的问题，再交由 AI 分析。这种“分工”可以在保证稳定性的同时，逐步扩大 AI 的应用范围，避免因过度依赖 AI 而引入新的不确定性。

其二，人机分工与信任机制。AI 的能力需要一个被验证、被信任的过程。实践中，通常让 AI 与人工“共同运行”一段时间，在准确率得到验证之后，再逐步授予 AI 更高的权限。预授权、可观测、可解释，是建立人机信任的关键。

其三，以效能最大化为标准。无论是确定性方案还是智能方案，选择的标准都是效能最大化。数世咨询在《持续评估定义安全运营》中提出，安全运营应通过持续的评估与验证，不断提升自身的“下限”与“上限”，实现从“小作坊”到“工业化”的进阶。这一思路同样适用于 AI 原生 SOC：持续的评估与验证，是保障其长期有效的重要手段。

5.5 交付形态与合规

AI 原生 SOC 多采用 SaaS 化交付，数据需要出域至云端处理。这带来了新

的安全与合规考量：如何在数据出域的前提下保障数据安全，如何满足行业与地区的合规要求，是 AI 原生 SOC 落地必须解决的问题。

交付形态的选择，因此不只是商务决策。对数据敏感度较高的用户，可能暂时选择本地化（私有化）部署，或在过渡期采用混合方式。随着合规框架的完善与用户信任的建立，SaaS 化交付的接受度有望逐步提升。

第六章 安全运营的未来趋势

在前述讨论的基础上，本章展望安全运营的未来趋势。需要说明的是，趋势判断基于当前的产业观察，具有一定的不确定性，仅作为参考。

6.1 人机协同关系将从“人在环中”转向“人在环上”

安全运营中，人与 AI 的分工正在重构。当 AI 能够承担越来越多的日常运营任务，人的角色将从“操作者”转向“决策者”——在关键节点做出判断。安全运营的形态，将从“人在环中”（人贯穿全流程）转向“人在环上”（AI 自主运转、人在关键节点介入）。

这一转变并不意味着人的价值降低。相反，随着 AI 承接重复性工作，人的价值将更多地体现在复杂判断、策略制定等更高层次的环节。人机协同的关键，是找到人与 AI 各自擅长的边界，并建立顺畅的衔接机制。

6.2 安全运营将走向按效果付费

随着 AI 能力的增强，安全运营的交付形态也在变化。以往以“交付平台”为主的方式，可能逐步转向“交付服务”——即 MSS（托管安全服务）或 MDR（托管检测与响应）。用户不再需要自行搭建和运营复杂的平台，而是按需购买安全运营服务。

这一变化或将重塑安全运营的商业模式：从卖产品、卖平台，转向卖能力、

卖结果。最终引导安全运营走向“按效果付费”的模式。数世咨询在《网络安全态势感知能力指南》中曾指出，“托管服务化”是安全运营的重要方向；随着 AI 能力的成熟，这一方向的可行性正在上升。

6.3 安全运营将从 IT 视角拓展到业务视角

同样一次数据访问，是正常的批量作业还是异常的数据外发，只有在业务语境中才能判断。而 AI 原生 SOC 在数据层实现了语义统一，把分散的告警还原为可理解的业务活动。这为安全运营打开了一个新的方向：运营的基础，将从 IT 视角扩展到业务视角。这意味着，安全运营未来所依赖的，将不只是 IT 层面的技术数据，还包括业务层面的逻辑、流程、场景与数据。安全与业务的结合越紧密，运营的效果也就越接近业务真正需要的结果。

6.4 安全的价值标准将从“守底线”转为“提上限”

随着安全运营从 IT 视角走向业务视角，衡量其价值的标准也在发生扩展与外延。

以往，安全运营的成效多以 MTTD/MTTR 等技术指标衡量。这些指标刻画的是“守得住”——检测是否够快、响应是否及时，本质上对应的是安全的“底线”。而在业务视角下，衡量标准会进一步外延：安全运营能否帮助业务提效、能否降低业务的风险敞口、能否成为业务的支撑而非负担，这些更接近“竞争力”的指标开始进入视野。

这意味着，安全的价值不再只是“守住底线”，而是“提升上限”——不仅防范损失，也助力业务。当安全运营与业务数据打通、与业务流程协同，它就有可能从成本中心转变为竞争力的一部分。这将是安全运营价值的重新定位。

6.5 人才梯队建设的新难题

当 AI 承担起 L1、L2 层级的日常运营工作（如告警筛查、初步研判），一个此前较少被讨论的问题浮现出来：高水平安全人才的成长路径，正在变窄。

传统的安全运营人才，多是梯队式培养的——新人从 L1 的告警处理做起，在处理大量告警的过程中积累经验，逐步成长为能够独立研判、处置复杂事件的 L2、L3 人员。这一路径虽然漫长，却是经验传承与能力沉淀的主要方式。而当 AI 接管了 L1、L2 的大量工作，新人便失去了在实战中练手的机会，从新手到高手之间的台阶被压缩。

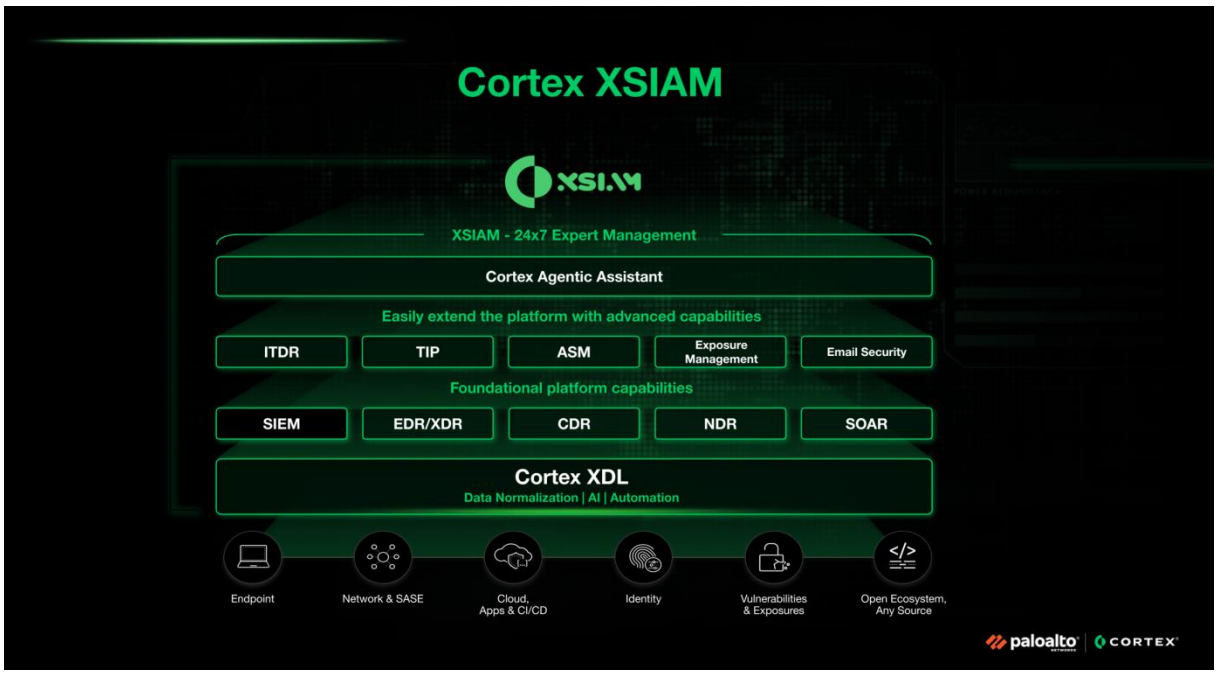
人才培养本就依赖实践机会的积累。如果 AI 承担了这些实践环节，那么未来的高水平安全人才从哪里来、如何成长，将成为安全运营面临的一个新难题。这一问题短期内未必显现，但从中长期看，它关系到整个行业的能力供给。如何在 AI 时代的运营体系中为人才保留成长空间，值得行业提前思考。

附录 AI 原生 SOC 代表性实践

本附录为数世咨询在调研过程中收录的行业代表性实践，仅作为行业案例的客观呈现，不构成对数世咨询对任何厂商的推荐或评价。

Palo Alto Networks · Cortex XSIAM

Cortex XSIAM 是 Palo Alto Networks 面向“AI 驱动 SOC”的平台产品。其核心思路，是将 SIEM、XDR、SOAR、攻击面管理（ASM）与威胁情报等功能融合到单一平台，以 AI 驱动检测、调查与响应，替代传统“以 SIEM 为中心、以人为主”的运营模式。



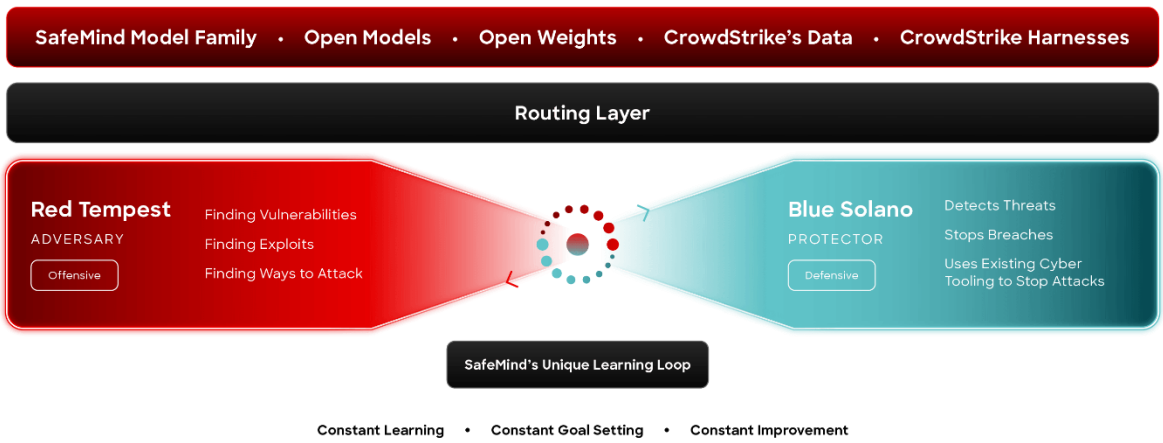
在数据层面，XSIAM 通过统一的 XDL 数据接入与归一化，将端点、网络、云、身份及第三方数据汇聚到同一数据底座；在智能层面，以因果引擎与智能拼

接把分散告警自动关联为事件，再由 AI 模型完成检测、调查与响应；在自动化层面，奉行“自动化优先”，2026 年起进一步主打“Agentic SOC”。

对照本报告的四个判定标准，XSIAM 在“架构重构”上尤为突出——它以平台融合的方式，重构了传统分散的 SOC 工具链。如果对照本报告 3.3 章节中的四个判定标准，其“数据原生”与“语义统一”体现较为明显，“Agent 优先”属方向性符合。

CrowdStrike · SafeMind

SafeMind 是 CrowdStrike 于 2026 年 9 月发布、与 NVIDIA 合作打造的面向网络防御的 AI 系统，原生运行于 Falcon 平台内。它并非一个完整的 SOC 平台，而是对应“AI 原生”中的智能层——以专为安全训练的前沿模型与智能体，承担攻防对抗的核心工作。



SafeMind 由两个模型构成闭环：进攻模型 Red Tempest 模拟 AI 驱动的攻击者，持续探测攻击路径、执行“机器速度的持续红队”；防御模型 Blue Solano

基于攻击活动记录，自动生成并验证检测规则、封堵缺口。两个模型在协作框架中相互对抗、持续进化。其训练基础来自 Falcon 平台的全量遥测、威胁情报与多年事件响应经验，模型基于 NVIDIA Nemotron 微调。

同样对照本报告 3.3 章节中的四个判定标准，SafeMind 在“Agent 优先”上表现突出，是典型的 Agentic AI；“数据原生”依托 Falcon 平台得以体现。需要说明的是，它重构的是“智能层”（模型与智能体），平台的数据层、核心架构层、应用层仍由 Falcon 承载，因此并非一个完整的“AI 原生 SOC 平台”。

微步在线 · OneSOC

OneSOC 是微步在线近期发布的以“多智能体协同”为核心构建的 AI 原生安全运营体系，对照四个判定标准，其在“数据原生”“语义统一”“架构重构”“Agent 优先”上均有明确对应，作为代表性实践入选本报告。

在架构上，其采用“企业侧轻量 Broker 接入 + 云端智能运营中心”的方式：Broker 收敛异构数据、执行调查与处置指令；数据层以湖仓一体承接、遵循 OCSF 数据标准，入库即统一语义，并以 Agent 原生友好的方式对外提供检索能力；核心架构层以 Kafka、Flink、图数据库与工作流引擎支撑消息总线、实时计算、关系存储与处置编排，其中图数据库将攻击链还原与多跳关联成为一次图查询，而不是查询期的临时拼合。



图 6　微步在线 AI 原生安全运营中心 OneSOC 架构图

在智能层，AI 架构层（XGPT）以多 Agent 协同承担研判、调查、处置等长任务链路，以攻击面和风险发现承担主动防御，以平台支撑 Agent 降低平台自身的运营门槛，并通过全局知识库与 Memory 沉淀历史事件与处置结论与资产语义，使系统的判断能力可复用、可累积。

业务场景层将上述能力以三种形态交付：自然语言交互、事件全生命周期的运营闭环（聚合—研判—调查—处置）、以及防御前置的攻击面梳理与风险发现。层与层之间以流式接口贯通。从流式接入、流式数据供给、AI 原生推理与计算到业务场景调用，四段衔接均由系统内部完成，不依赖报表导出与工单转派。

通过多智能体协作和上下文分析，OneSOC 将“设备报出了什么”进一步转化为“攻击结果如何、哪些线索值得优先调查”。安全人员据此结果推送复核关

键证据、确定响应优先级，并将确认后的经验沉淀为后续研判可复用的知识，结合治理层面，敏感操作经人工审批并全程留痕后，逐步形成持续改进的安全运营机制，最终达到以多智能体协同推动告警从规则命中走向结果研判闭环的效果。

数世咨询
Digital World Consulting



中国数字安全产业
独立第三方研究与咨询机构

Independent Research & Consulting for China's Digital Security Industry

第三方独立
- 完全第三方背景
- 独立分析师团队

调研对象
- 800+ 网络安全企业
- 年均500+深度沟通
- 年均2000+小时访谈时长

服务对象
- 国家、行业监管机构
- 行业客户及用户
- 网络安全产品与服务供应商

服务内容
- 国家、行业智库
- 细分领域研究报告
- 提供面对面咨询
- 为产业各方提供资源对接

合作方式
- 各类报告定制
- 年度企业观察列表
- 活动赞助
- 投资FA

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

撰写发布《中国数字安全大事记》《中国数字安全能力图谱》《中国数字安全价值图谱》《新质 中国数字安全百强》《中国数据安全50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，还为监管机构、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

数世咨询目前已对接国内网络安全企业800余家，并与400余家具备原厂能力的安全企业和100余家安全行业领先者企业，以及110余家有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。包括共同举办数字安全大会，投融资对接，安全产品与企业推荐，企业资源整合等。

行业咨询

经常性地为监管部门、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

数世咨询
Digital World Consulting

数字安全领域独立第三方调研机构

