聚焦实战 合力构建更具韧性的智能安全防线

▶ 本报记者 张伟

8月21日，年度网络安全盛会CSOP 2025网络安全运营实战大会在北京市拉开序幕。本次大会以“新态势·新实战”为主题，吸引来自政府机构、国央企、科研院所、顶尖高校、运营商、大型金融机构、互联网头部企业等多位安全领域专家，共同探讨实战安全运营新策略，分享关键基础设施防护实战经验，合力构建更具韧性的安全防线。

新态势下的新实战

实战在网络安全中居于核心地位，是检验防御体系有效性、提升应对能力的关键标志和终极目标。

“我们的安全运营面临八大硬核难题，包括钓鱼攻击、漏洞管理、海量告警、高质量日志缺失、凭证泄露与滥用、加密流量检测、攻防时间不对称以及不断扩大的攻击面。”北京微步在线科技有限公司（以下简称“微步在线”）创始人兼CEO薛锋说，想要解决这些问题，必须回归安全运营的本质，通过提升基础能力而非盲目追逐热点，才能实现安全能力的质变。

实战的另一个表现是，攻击路径已经变得更复杂、更隐蔽、更出乎人们意料，想要在实战攻防演练中获得高分并非易事。对此，微步在线技术合伙人赵林林认为，必须要做到有的放矢，准确识别并防范供应链环节风险点，利用情报收集、厂商协同、快速响应层出不穷的0day（漏洞），并通过攻击行为与技术特征快速研判对手水平，消耗并压制对方攻势。

具体到办公终端，微步在线技术合伙人黄雅芳表示，面对钓鱼木马、漏洞攻击以及合法凭据、工具滥用，以EDR为代表的高级威胁对抗技术，也面临着理解复杂攻击行为不易准确理解、检测的实时性与准确性之间难以平衡、被致盲与绕过等困境，需要在安全运营中做到及时的检测响应、常态化的威胁狩猎、构建企业特有的检测能力。

从被动应对到智能防御

在实战化安全建设与运营过程中，许多嘉宾不约而同地提到“主动”二字。

“历年来，京东方信息安全工作都有总体方针指导。”京东方信息安全中心总监李楠说，京东方以资产安全为驱动，通过基础平台建设、功能完善、运营优化和效率提升4个阶段，构建了覆盖资产全生命周期的智能安全运营体系，驱动安全能力从被动防护向主动防御演进。

北京金山云网络技术有限公司企业安全负责人刘鹏介绍了企业安全在梳理、评估、布防、演练、保障等阶段的要点。在他看来，网络攻击的新态势是，攻击频率加快、规模扩大，攻击手段更加多样、隐蔽，攻击目标转向集权、核心系统，攻击流程更加自动化、智能化，只有通过“主动防御+纵深防御”形态构建才能更好地抵御网络攻击。

顺丰科技有限公司网络安全总监梁博分享了甲方视角下的威胁情报与狩猎。顺丰构建了以威胁情报为核心、威胁狩猎为关键手段的主动安全运营体系。基于XDR（可扩展检测与响应）理念，构建了检测响应安全工具链，在实战持续优化，初步形成安全运营驾驶舱，确保在攻防对抗中争夺并掌握制信息权，有效应对包括APT（高级持续性威胁）和0day在内的高级威胁，为企业业务保驾护航。

不过，在当前复杂的环境下，安全建设并非一蹴而就，而是要坚持长期主义。中信集团网络安全专家李显旭在分享《综合型集团企业办公防护体系建设探索》时表示，坚持安全长期主义，就是坚持可持续性的建设、可升级的安全体系和主动塑造的企业安全生态，围绕终端安全的“投递—执行—控制”三阶段实施三步防护策略，以实现经济、有效、可控的集团化安全防护，推动安全建设从威胁驱动转向风险驱动。

AI技术赋能降本增效

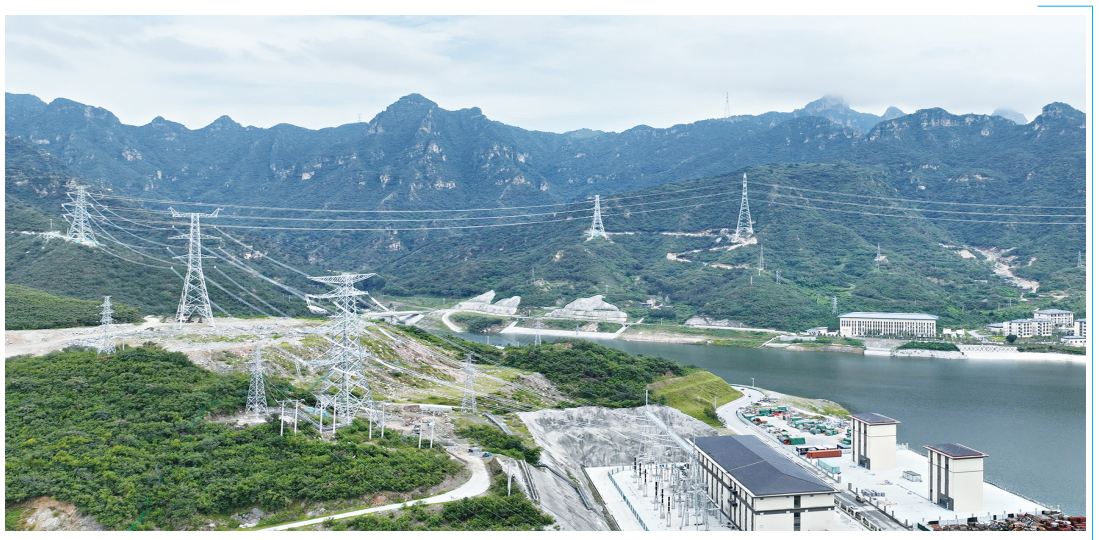
随着以人工智能为代表的新技术的广泛应用，攻防两端都随之发生改变，传统的网络安全防护思路在应对新型威胁时，或许已不再适用。

“传统SOC（安全运营中心）存在告警过载、响应延迟、标准化难度高及人才短缺等诸多痛点。”猿辅导信息安全负责人温飞表示，要建设基于大模型的智能运营三层架构：通过降噪层实现AI告警精准过滤，决策层构建人机协同研判机制，自治层执行安全边界内的剧本自动化响应。

对于AI的应用，中国科学院计算机网络信息中心高级工程师赵静表示，AI驱动的自演进网络安全不是简单的自动化或智能化，而是要构建一个以数据为燃料、以AI为引擎、以持续对抗为进化压力、以人机协同为控制中枢的动态有机体，能够自动优化监测策略，提升对高级隐蔽攻击的检测与智能处置能力。

面对巨大的双向流量、多样化设备以及广大师生用户，清华大学校园网网络安全负责人姚星昆将运营思路概括为“四化”，即复杂的事情简单化，简单的事情标准化，标准的事情流程化，流程的事情自动化，通过动态、智能、自动化的安全运营，实现“策略设定—发现问题—处置问题—处置确认—优化策略”的完整闭环。

据悉，本届网络安全运营实战大会在北京站点结束后，将继续在上海、深圳举办，博采众智，再造一届安全运营实战技术交流盛会。



8月26日，河北省重点项目——设计装机容量120万千瓦的易县抽水蓄能电站配套工程500千伏特高压送出线路并网投运。据国网河北省电力有限公司介绍，该能源送出线路全长49.937公里，将为易县抽水蓄能电站竣工投运后发挥调峰、填谷、调频、调相等作用提供支撑，助力太行山地区的新能源消纳和保障电网安全稳定运行。

图为8月26日拍摄的河北省易县抽水蓄能电站下水库附近的电站送出线路（无人机照片）。

新华社记者 杨世尧/摄

中国首个智能体产业合作组织正式成立

科技日报讯（记者 张佳星）8月21日，中国生产力促进中心协会智能体互联网分会成立大会在中关村国家自主创新示范区展示交易中心召开。

据了解，为解决当前智能体互联网的发展标准缺失、接口割裂、生态分散等问题，在北京邮电大学人工智能学院、北京浩瀚深度信息技术股份有限公司、中移互联网有限公司、拓维信息系统股份有限公司（以下简称“拓维信息”）、北京学霸在线科技有限公司、北京新流万联网络技术有限公司等发起单位的倡议和申请下，中国生产力促进中心协会批复成立“智能体互联网分会”（Internet of Agents Association，IAA），为智能体产业界构建一个开放、协同、共建共享的组织平台，整合上下游资源，推动智能体互联网的标准建设、场景拓展与产业落地。

中国生产力促进中心协会理事长申长江表示，希望分会能在人工智能产业的浪潮和机遇中快速发展，为我国人工智能事业做出最大贡献。中国生产力促进中心协会监事长韩丽娟宣读了协会对智能体互联网分会的成立批复，中国首个智能体产业合作组织正式成立。

中关村科学城管委会一处副处长王思野表示，基于海淀区的科技创新底蕴，分会将进一步发挥智能体标准和产业生态引领优势，在海淀区打造具有示范性和引领性的智能体互联网科技成果。

中国生产力促进中心协会智能体互联网分会主任张跃表示，将在协会领导下为分会成员单位做好服务，促进中国智能体产业发展。

在智能体互联产业发展论坛环节，北京邮电大学教授郭军介绍了智能体发展历史，以及北京邮电大学在智能体领域的科研历程和成果，并对智能体互联产业的发展给出了方向性建议。北京物资学院副院长、教授张闯从智能体与商业物流产业的结合角度阐述了智能体互联的必要性及发展趋势。

中国生产力促进中心协会智能体互联网分会首席科学家、北京邮电大学数据科学研究中心主任刘军以《智能体互联-人工智能进化新篇章》为题，介绍了智能体及智能体互联技术的发展将如何给人工智能产业带来新的变化。智能体互联国家标准负责人、中国电子技术标准化研究院信息技术研究中心工程师高歌以《智能体互联国家标准建设及推广》为题，为参会嘉宾介绍了相关国家标准制定的背景、进展和产业规划。中移互联网有限公司AI+联创中心副总经理孙立军以《打造AI智能生态通行证，实现智能体统一智联》为题介绍了企业在智能体互联产业的相关技术积累和产品服务。中铁电气化局集团有限公司信息技术中心副主任裴宁以《“中铁先锋”四电智能体大模型平台建设》为题介绍了企业在铁路建设与维护领域的智能体研发情况和规划。北京学霸在线科技有限公司教育行业总监朱苡嘉以《基于智能体的下一代智慧教育平台》为题介绍了企业在教育智能体领域的积累以及未来教育智能体互联的规划。

来自360、金山云、国金证券、拓维信息等行业代表公司、中关村科学城管委会、中关村国家自主创新示范区核心区发展研究中心等多家机构的专家学者参会。

作为全国第一个聚焦智能体产业的协会组织，中国生产力促进中心协会智能体互联网分会将秉承“连接产业各方，推动智能体互联网技术标准与应用生态发展，加速智能体时代的全面到来”的宗旨，构建智能体产业协作平台、技术交流平台、标准制定平台、应用推广平台和生态建设平台，致力于打造“开放协作、互信共赢”的智能体产业创新共同体。