面向运营商网络的APT一体化监测体系研究

Research on APT Integrated Monitoring System for Operator Networks

韦峻峰，陈　晨，杨　莉（中国联通河南分公司，河南 郑州 450000）
Wei Junfeng，Chen Chen，Yang Li（China Unicom Henan Branch，Zhengzhou 450000，China）

摘　要：
随着数字经济的发展，运营商网络面临的APT攻击日益组织化、复合化与隐蔽化，传统防御机制面临实时检测与协同响应等挑战。基于广义安全控制系统理论，构建了“数据融合—智能决策—协同响应—态势掌控”的闭环控制机制，形成面向APT的一体化监测运营体系。通过在省级运营商网络中的应用，该体系显著提升攻击发现率至98.7%，平均响应时间缩短至8.3 min，成功阻断多起境外渗透，避免经济损失超2.3亿元，为关键信息基础设施防护提供支撑。

关键词：
高级持续性威胁；运营商网络；监测运营；网络安全防护
doi：10.12045/j.issn.1007-3043.2025.09.012
文章编号：1007-3043（2025）09-0063-07
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
With the development of the digital economy，operator networks are increasingly facing organized，compound，and stealthy advanced persistent threats（APTs），posing challenges to traditional defense mechanisms in real-time detection and coordinated response. Based on the theory of generalized security control systems，it constructs a closed-loop control mechanism comprising “data fusion，intelligent decision-making，coordinated response，and situational awareness”，forming an integrated APT monitoring and operational system. Through implementation in a provincial operator network，the system significantly increases the attack detection rate to 98.7%，reduces the average response time to 8.3 minutes，successfully blocks multiple overseas infiltration attempts，and prevents economic losses exceeding 230 million yuan，thereby providing critical support for the protection of key information infrastructure.

Keywords：
Advanced persistent threat（APT）；Operator networks；Monitoring and operations；Network security protection

引用格式：韦峻峰，陈晨，杨莉. 面向运营商网络的APT一体化监测体系研究[J]. 邮电设计技术，2025（9）：63-69.

0 引言

5G、云计算以及边缘计算等新兴技术在通信行业的深度融合使运营商网络已演进为涵盖核心网元、智能传输平面及云化业务平台的多层异构复杂系统。据国家互联网应急中心监测数据显示，2022年针对我国基础电信网络的APT攻击事件同比增长67%，攻击者平均驻留时间达112天，标志着采用特征匹配、行为分析、模式识别等技术手段的传统防御体系[1]面临着攻击隐蔽性增强带来的实时检测挑战、攻击驻留周期延长带来的防御时效性挑战、多阶段攻击复杂性带来的协同处置挑战等诸多挑战。

为解决上述问题，本研究结合广义安全控制系统（Generalized Security Control System，GSCS）理论框架，

收稿日期：2025-08-01

提出运营商场景下的APT一体化监测运营体系，通过构建“数据融合—智能决策—协同响应—态势掌控”的闭环控制机制，实现网络安全防御从静态防护向动态运营的范式转变。本研究在以下3方面实现了创新突破。

a）理论模型创新。将GSCS理论框架引入运营商网络安全领域，为解决运营商网络环境下APT攻击监测难题提供了全新的理论视角，突破了传统防御体系的局限。

b）技术融合创新。融合基于LSTM-GRU的异常流量检测模型和基于图神经网络的跨域关联分析引擎等形成了覆盖核心网元、传输平面及云化业务系统的立体化感知网络。

c）应用创新。在真实运营商网络环境中设计实施了APT一体化安全运营指挥平台，通过与现有网络设施和安全设备的深度融合，为运营商网络的安全运营提供了可视化、一体化、全方位的支撑能力。

1 相关工作

近年来，APT攻击呈现目标精准化、技术手段复合化、驻留方式隐蔽化等显著特征，给APT攻击检测与防御带来了极大的挑战[2-4]。近年来APT攻击相关的研究一直都是热点话题，重点集中在威胁检测、溯源推理、安全编排等3个方面。

a）在威胁检测方面，近年来研究的热点集中在利用AI实现APT攻击检测。Liras[5]等人针对APT攻击链中的恶意软件构建了4种机器学习模型来提取静态和动态特征进行综合识别；Han[6]等人设计实现了一种基于溯源图的运行时APT检测系统，根据上下文知识来智能识别可疑的APT行为；成翔[7]等人提出一种面向零日攻击检测的APT攻击活动辨识方法（APTIZDM），可有效辨识出被入侵检测系统漏报的零日攻击活动。

b）在溯源推理方面，Alrabaee[8]等人通过分析APT组织使用的二进制文件编译过程中遗留的特征来溯源二进制文件的作者，黄克振[9]等人利用攻击事件线索和威胁情报追踪溯源APT攻击组织，Hossain[10]等人则在因果依赖关系的基础上利用溯源图实现APT攻击场景的快速重构。

c）在安全编排方面，李若彤[11]构建了一种多层次的综合防御策略集，并使用安全编排算法对综合防御策略集进行安全编排与自动化响应；Winterrose[12]等人从自适应攻击者角度出发，提出了一种基于不完全信息的博弈模型，并对比了随机性MTD和多样性MTD 2种防御策略的效果；Zhang[13]等人提出了一种基于不完全信息的随机博弈模型和一种具有奖励量化的Nash-Q学习算法。

虽然现有研究已经取得了良好的效果，但由于运营商场景复杂、庞大，现有研究在运营商场景下的应用仍然存在数据融合度不足、策略动态性欠缺等局限。

2 监测框架

本研究通过深入跟踪分析运营商网络架构，从全局的角度提出了一种面向运营商网络的APT一体化监测体系框架。该框架采用四层协同架构，通过“数据融合—智能决策—协同响应—态势掌控”的闭环控制机制，实现APT攻击的全生命周期管控（见图1）。

具体来说，本文所提出的框架包括4个层级。

a）数据融合层。基于Flink+Kafka的流式架构，采用多源异构数据融合技术整合网络流量、安全设备日志、终端行为（EDR）、威胁情报等12类数据源，实现高效的数据吞吐和数据标准化处理，为上层分析提供高置信度数据基底。

b）智能分析层。融合深度学习与攻击链推理技术，形成三位一体的分析体系。首先基于LSTM-GRU混合神经网络实现异常事件的发现，其次在离散化异常事件的基础上基于图神经网络进行跨域关联分析，挖掘其中存在的攻击链路，最后根据攻击过程中发现的统计特征、文本信息等关联威胁情报实现基于安全知识图谱的攻击者行为画像。

c）协同联动层。依托SOAR引擎构建智能化响应体系，集成78种预定义处置剧本与强化学习驱动的动态策略生成器。如供应链攻击处置流可实现代码签名验证，横向移动阻断流通过ACL实现策略自动下发与会话重置操作。

d）综合展示层。通过GIS热力图实时呈现APT攻击地理分布与强度态势，结合时间轴攻击链追溯看板完整复现攻击者战术、技术与过程（TTPs）。除此之外，综合CVSS 3.1漏洞利用系数、CWE Top 25资产暴露面评分及业务系统SLA等级，根据网络中的攻击态势实时进行动态风险评估。

2.1 基于LSTM-GRU的异常流量检测模型

为克服APT攻击手段复杂多变、隐蔽性强、持续

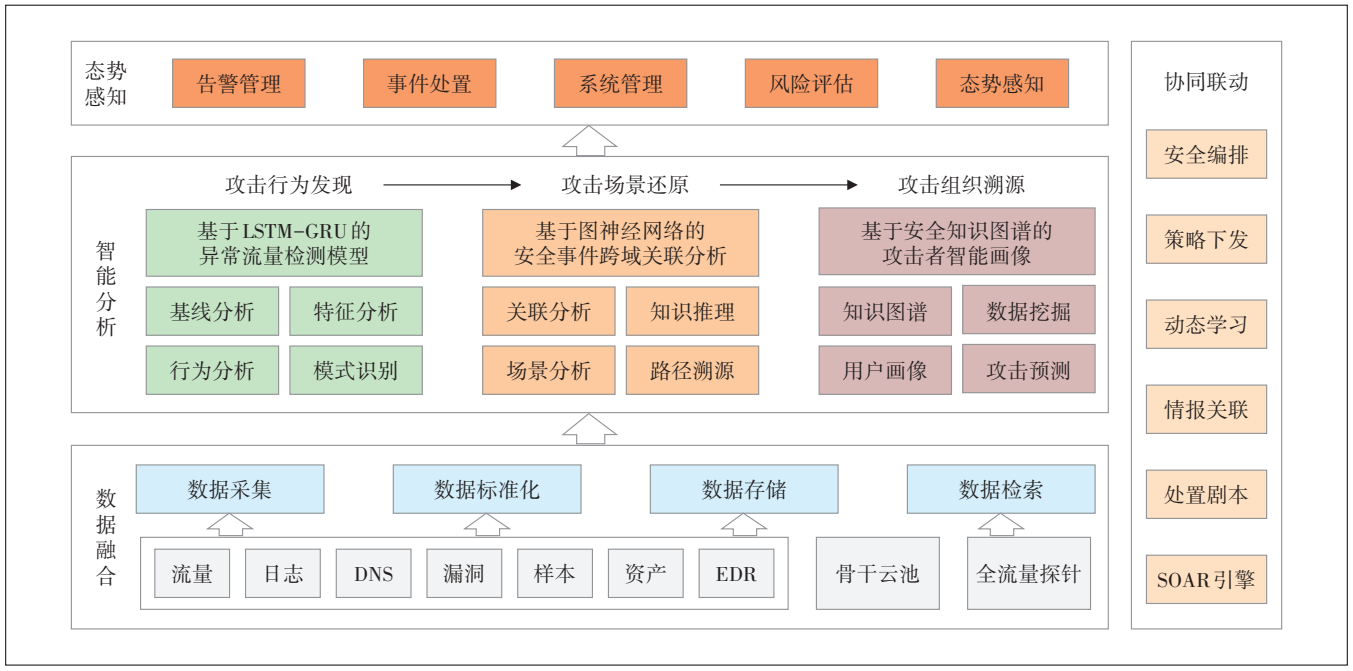

图1　面向运营商网络的APT一体化监测体系理论框架

时间长给传统基线分析、特征分析等检测手段带来的挑战，本文在监测体系中融合了基于LSTM-GRU混合神经网络的异常流量检测模型。该模型通过双门控循环架构与注意力机制的协同设计，突破了传统流量分析模型在时序特征捕捉与长期依赖建模方面的局限性。

本文所提出的基于LSTM-GRU的异常流量检测模型架构如图2所示，包括时序特征智能提取和注意力增强机制2个核心模块。

a）时序特征深度提取。采用LSTM单元捕获流量序列的长期依赖特征，通过输入门、遗忘门、输出门的协同调控，解决传统RNN的梯度消失问题。在5G网络切片场景下，针对NetFlow元数据中的会话持续时间、包长分布等23维时序特征进行建模。同时引入GRU单元增强短期动态模式学习能力，其简化门控结构可快速响应突发性流量异常。

b）注意力增强机制。设计层级注意力模块，对LSTM-GRU输出的多尺度特征进行动态加权。通过时间步注意力来识别关键时间节点，如DNS隧道建立阶段的查询周期异常；通过特征域注意力来聚焦高判别性特征维度，如SSL证书熵值突变、TCP窗口尺寸异常。

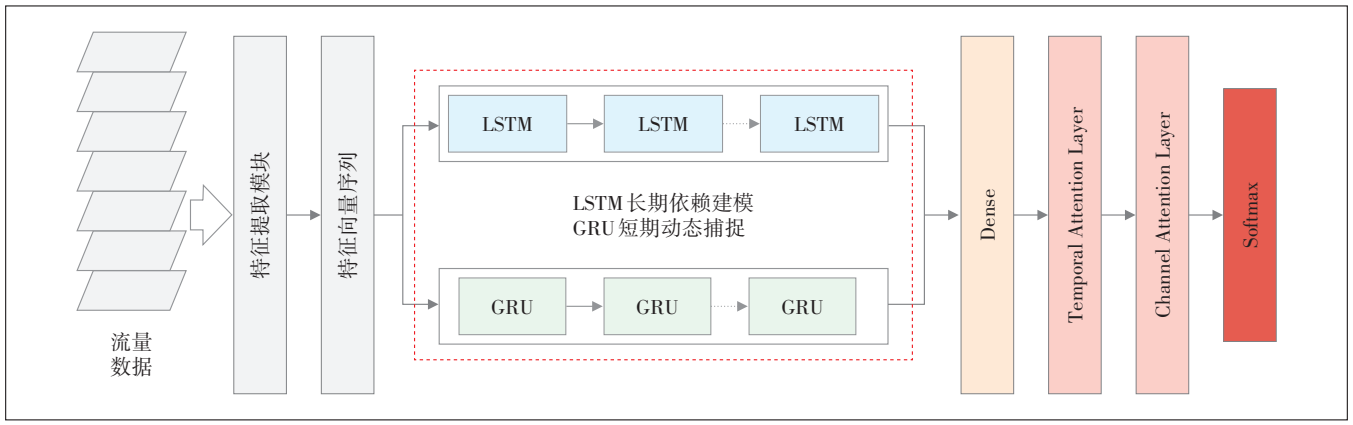

图2　LSTM-GRU神经网络架构

2.2 基于图神经网络的安全事件跨域关联分析

针对运营商网络中APT攻击呈现的跨域隐匿性与低关联性难题，本研究所提出的APT一体化监测分析体系中针对性设计了如图3所示的关联分析引擎，通过数据关联、场景关联、跨域关联等实现攻击链路的重建以及攻击场景的还原。

关联分析引擎内部采用基于异构信息图神经网络的跨域关联分析模型，通过多维关系建模与动态图推理技术实现攻击链的立体化重构。针对不同网络域中存在的主机探测、木马传播、非法外联、恶意样本等安全事件，提取终端行为指纹、用户实体、攻击对象、网络资产、攻击时间等多维度信息，并将其纳入统一图空间建模，创新性地定义访问关系、隶属关系、时序关系与语义关系4类边连接规则。具体而言，节点嵌入层融合NetFlow流量统计特征与威胁情报置信度，有效表征安全事件间的多维交互模式；在多关系图注意力网络的设计方面，通过节点级与关系级双重注意力机制，实现了跨域攻击链的精准推理。节点级注意力采用关系感知的权重计算方式，动态评估不同网络域中邻居节点的影响力，计算如式(1)所示；关系级注意力则通过可学习参数矩阵量化各类边连接的重要性，显著提升横向移动路径的识别准确率，计算如式(2)所示。为增强模型对抗APT组织反溯源的能力，在训练过程中注入基于ATT&CK战术生成的对抗性元路径，并引入Wasserstein GAN的梯度惩罚机制来稳定训练过程。

$$\sigma_{ij}^{r}=\frac{\exp\left(\mathrm{LeakyReLU}\left(\sigma_{r}^{T}\left[W_{h_i}\left\|W_{h_k}\right.\right]\right)\right)}{\sum_{k\in N_i^T}\exp\left(\mathrm{LeakyReLU}\left(\sigma_{r}^{T}\left[W_{h_i}\left\|W_{h_k}\right.\right]\right)\right)} \tag{1}$$

$$\beta_{r}=\frac{\exp\left(q^{T}\tanh\left(W_{\dot{r}}\bar{h}_{\dot{r}}\right)\right)}{\sum_{\dot{r}\in R}\exp\left(q^{T}\tanh\left(W_{\dot{r}}\bar{h}_{\dot{r}}\right)\right)} \tag{2}$$

在式(1)中，σ_{ij}^{r}为在关系类型r下邻居节点j对中心节点i的重要性权重；W是共享的权重矩阵用于线性变换节点特征；h_i和h_j是节点的原始特征向量；N_i^T是节点i在关系r下的邻居集合。在式(2)中，β_r是关系类型r在整个图中的全局重要性权重；q是查询向量，用于评估关系和当前任务的关联性；W_r关系r特有的权重矩阵；$\bar{h}_r$是关系r下所有节点的平均特征向量；R是图中所有关系类型的集合。

2.3 基于安全知识图谱的攻击者智能画像

攻击者画像生成系统是APT一体化监测体系中的关键组件，它通过深度融合分析威胁情报、攻击行

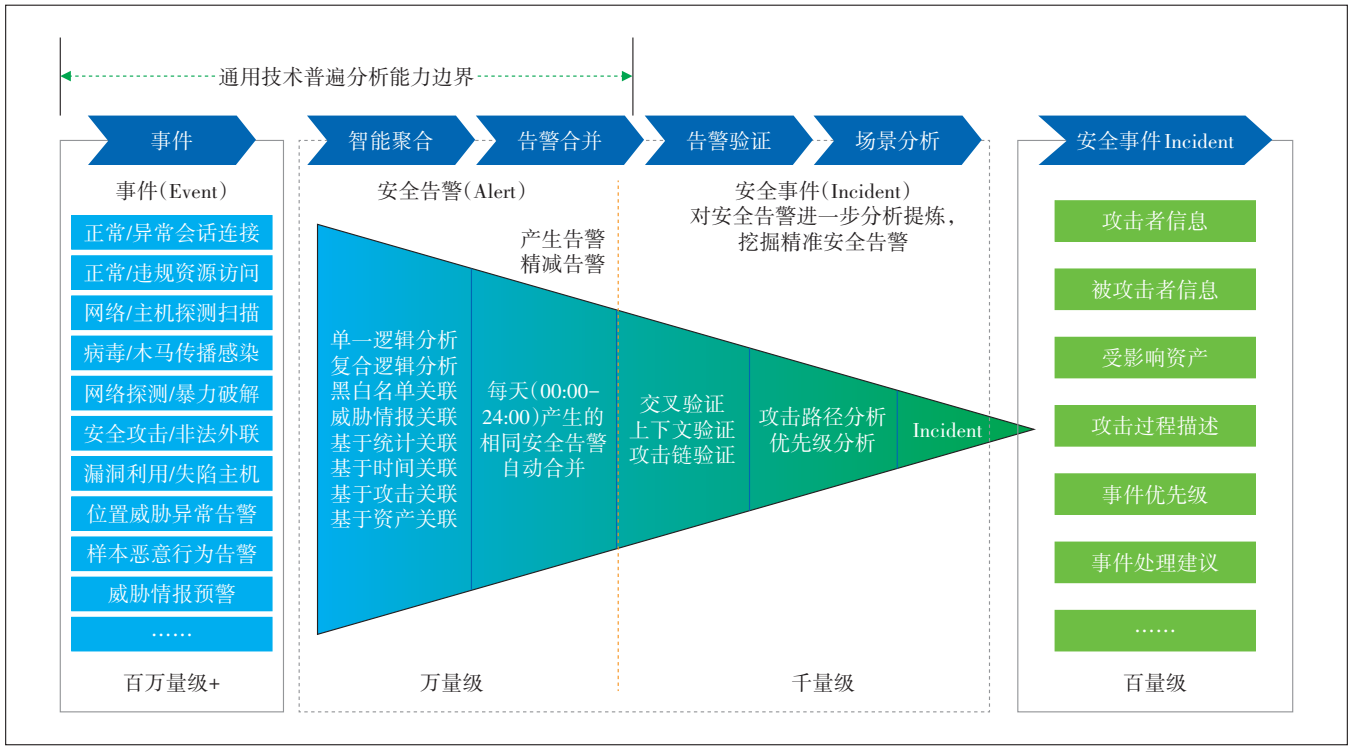

图3　安全事件跨域关联分析流程

为日志及网络资产数据，构建涵盖工具特征、TTPs模式、基础设施指纹、社交工程偏好、时间活跃规律、地理分布特征、漏洞利用偏好、加密通信模式、横向移动路径、数据外联渠道、伪装技术特征、反溯源策略等12个维度的知识图谱，精准构建攻击者画像。

具体来说，首先，利用安全知识图谱对攻击者的行为数据进行建模和存储，通过对安全事件数据的解析和特征提取，挖掘与攻击者相关的实体、行为，并将其映射到知识图谱中相应的节点和边上，形成攻击者行为的图谱表示。然后，采用机器学习和数据挖掘技术对攻击者的行为模式进行分析和识别。通过对历史攻击数据的学习，建立攻击者行为模式的模型，包括攻击者的工具使用习惯、攻击时间规律、目标选择偏好等。利用这些模型对当前的安全事件进行匹配和分析，判断是否与已知的攻击者行为模式相符，从而生成攻击者画像。

3 应用验证

基于本研究所提出的体系框架，在某运营商网络中设计实施了一体化安全运营指挥平台，并在某省安全运营中心进行了试运行。该平台通过构建全面、智能的APT攻击监测分析系统，利用网络流量监控、日志收集、数据预处理和特征提取等技术，结合机器学习算法和AI行为分析，深入挖掘潜在威胁。

3.1 体系建设

结合运营商网络已有的各类网络设施和安全设备，本研究所提出的监测体系在运营商网络中进行实施建设时主要带来了以下3点改变。

3.1.1 基础设施革新

基础设施革新包括增加APT攻击检测模块以及更新数据汇集与治理技术，完备运营商网络的基础安防能力和存储能力，具体实施如下。

a）部署涵盖数据采集、安全事件分析、异常流量检测模型等功能的高级持续性威胁全流量探针。该探针可以覆盖运营商网络中99%的核心链路，通过实时分析数据流来实现攻击检测、攻击成功检测、威胁情报检测等多维度的威胁监测，可精准识别如SQL注入、跨站脚本、命令执行、文件包含等多种Web攻击，也可检测木马、蠕虫、勒索软件、僵尸网络等攻击行为。

b）构建PB级安全数据湖，为安全分析提供完备的数据支撑。首先，通过标准化大数据预处理流程，在海量异构安全数据接入后，同步完成数据的过滤、解析、补齐、标签化；其次，通过构建数据分层存储模式来实现海量存储，保障功能、性能以及成本之间的三元平衡。真实运营商网络环境中适配设计的数据存储模式如图4所示。

3.1.2 能力中心完善

为充分赋能安全事件跨域关联分析、攻击者智能画像等核心能力，并保障其高效稳定运行，本方案在运营商现有安全运营中心的基础上，重点完善了威胁情报能力体系。

a）构建综合威胁情报中枢。通过深度集成5个权威情报源和三方威胁情报数据构建统一的威胁情报平台，提供独立的API实现情报数据的精准、高效、全面匹配。

b）强化情报治理与应用。平台按照高级持续性威胁情报信息库的相关标准对情报进行标准化处理与整合，建立了多层级威胁情报生产与上报、共享机制，可以逐步形成电信行业级高级持续性威胁情报知识图谱，并建立高级持续性威胁情报共享通路和机制。

c）保障情报生态多样性。为最大化情报价值，平台支持灵活接入商业情报、开源情报（OSINT）、监管机构情报以及自定义威胁情报。

3.1.3 运营机制创新

为有效支撑APT一体化监测分析平台的落地与高效运行，并充分发挥其联防联控潜力，本研究在运营商内部推动了深度的安全运营机制变革与创新，具体如下。

a）建立跨域协同的“联防联控”机制。打破传统安全运营中安全分析、威胁情报、应急处置等存在的壁垒，构建了跨部门、跨层级的协同响应流程。通过预设的自动化剧本触发告警，并依据威胁等级和影响范围自动派分至相应的专业团队进行并行处置。

b）推行“情报驱动、闭环管理”的安全运营流程。创新性地将威胁情报深度融入到日常安全运营的核心流程。情报平台不仅能够提供匹配结果，更能驱动主动狩猎任务。除此之外，将处置过程中发现的攻击者TTPs等线索闭环反馈给情报知识图谱，实现检测模型和情报质量的动态更新。

c）构建标准化、自动化的安全运营工作流。基于一体化平台能力，重新设计并固化安全事件发现、分析研判、响应处置、溯源取证以及报告总结的全生命

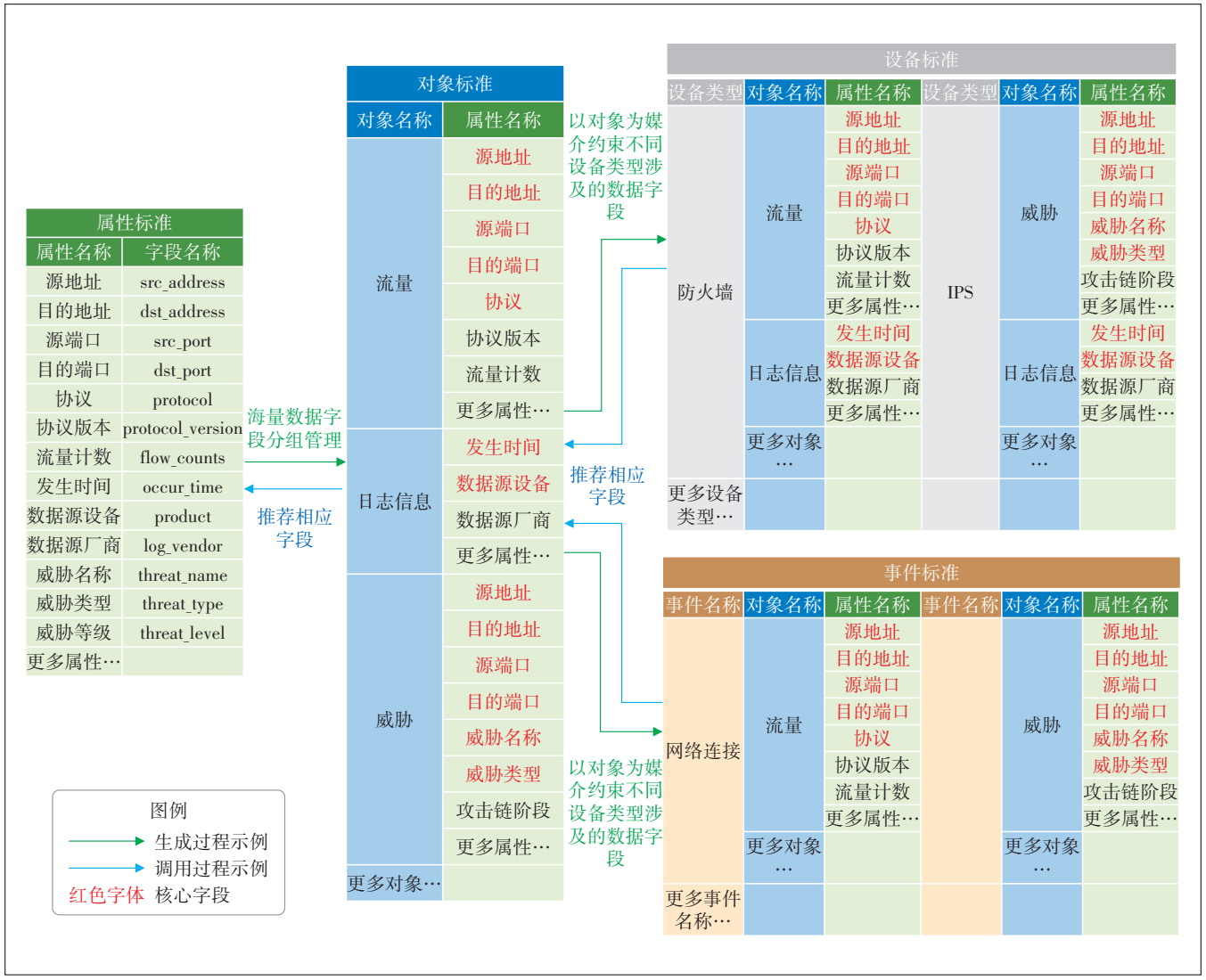

图4　真实运营商网络环境中的数据存储模式

周期标准化工作流，显著提升对高级威胁的响应速度和处置效率，减少人工操作失误。

在真实的运行过程中，网络与信息安全一体化综合指挥运营平台实时监控网络状态、运营数据和工作流程，面向运营商提供可视化、一体化、全方位的安全运营支撑能力。

3.2 实施成效

网络与信息安全一体化综合指挥运营平台经过6个月的试运行，给某省安全运营中心的安全指标带来了显著改善。

a）运营效率与处置能力跃升。省安全运营中心每日监控安全告警数十万起，研判安全事件近万件，实现告警100%当日处置闭环。对于集团级安全指挥调度平台下发的工单，平台实现100%及时响应与处置，进行恶意IP封堵、漏洞信息发布预警、安全事件排查等运营工作。

b）主动防御与协同成效显著。成功识别并通报处置多起弱口令、终端疑似感染病毒外连恶意域名等高危风险，并及时通知责任部门处理。积极与集团、地（市）、各专业线沟通协调，上下共振，左右同频，卓有成效地开展了日常运营工作。

整体来说，一体化运营工作成效显著，累计清理账号工号5.2万个，整治漏洞隐患507个，强化基线配置1.6万台，清理安装违规应用的终端6 353台，开展精准钓鱼测试15次9 311余人次。得益于平台的高效运行与上述举措，公司网络安全态势持续平稳，重大

网络安全事件保持“零发生”。

在试运行期间，典型的应用案例为平台精准识别某境外APT组织（关联海莲花）的攻击活动。通过深度关联分析样本行为特征、C2连接指纹及多源威胁情报，初步怀疑攻击已生效，平台随即启动全流程自动化响应。首先，快速定位：基于流量模型检测到目标区域峰值突增380%的异常流量；其次，攻击溯源：精准还原攻击链路，确认攻击者利用高危漏洞（CVE-2023-1234）进行渗透；最后，即时封堵：自动阻断恶意C2连接28个。该事件的成功处置，有效遏制了攻击扩散，将潜在损失降低约2.3亿元，充分验证了一体化平台在应对高级持续性威胁（APT）方面的强大实战能力。

4 讨论与展望

4.1 面临挑战

本文所构建的APT一体化监测运营体系虽然在实践中取得了显著成效，但仍面临以下挑战。

a）加密流量分析瓶颈。随着加密技术的广泛应用，APT攻击者越来越多地采用加密通信来隐蔽其攻击行为，传统的检测方法在加密流量中难以有效识别威胁特征。

b）新型AI对抗攻击防御。APT攻击组织不断利用AI技术提升攻击的隐蔽性和复杂性，如GAN等技术被用于生成高度逼真的虚假数据，需要有效防御新型AI对抗攻击。

c）跨境协同处置机制缺失。APT攻击往往具有跨国界的特点，但目前国际间的情报共享率较低，跨境协同处置机制尚不完善，需要建立高效的跨境协同处置机制。

4.2 未来方向

针对上述挑战，未来的研究方向如下。

a）量子安全通信技术在防护体系中的应用。量子通信技术具有高安全性、抗窃听等特性，研究量子安全通信技术与现有防护体系的融合，探索量子密钥分发、量子随机数生成等量子安全通信技术在APT防御中的应用，可为运营商网络构建更加安全可靠的通信渠道。

b）构建基于数字孪生的网络攻防演练平台。数字孪生技术可以构建与真实网络环境高度一致的虚拟模型，为网络攻防演练提供理想的平台。通过在数字孪生平台上进行模拟攻击和防御演练，可以提前发现潜在的安全风险，优化防御策略，提高网络安全防护能力。

参考文献：

[1] 杨宇，陈一丁，赵荣，等. 网络安全主动防御研究综述[J]. 科学技术与工程，2025，25(7)：2654-2663.
[2] 杨秀璋，彭国军，刘思德，等. 面向APT攻击的溯源和推理研究综述[J]. 软件学报，2025，36(1)：203-252.
[3] 王郅伟，何晞杰，易鑫，等. 基于APT活动全生命周期的攻击与检测综述[J]. 通信学报，2024，45(9)：206-228.
[4] 吴寒，李晓东，成星恺，等. APT攻击检测技术研究综述[J]. 通讯世界，2024，31(2)：61-63.
[5] MARTÍN LIRAS L F，DE SOTO A R，PRADA M A. Feature analysis for data-driven APT-related malware discrimination[J]. Computers and Security，2021，104：102202.
[6] HAN X Y，PASQUIER T，BATES A，et al. UNICORN：runtime provenance-based detector for advanced persistent threats[EB/OL]. [2025-02-02]. https://www. ndss-symposium. org/wp-content/uploads/2020/02/24046-paper.pdf.
[7] 成翔，匡苗苗，严莉萍，等. 面向零日攻击检测的APT攻击活动辨识研究[J]. 湖南大学学报（自然科学版），2024，51(12)：153-164.
[8] ALRABAEE S，SHIRANI P，DEBBABI M，et al. On the feasibility of malware authorship attribution[C]//Foundations and Practice of Security. Cham：Springer，2016：256-272.
[9] 黄克振，连一峰，冯登国，等. 一种基于图模型的网络攻击溯源方法[J]. 软件学报，2022，33(2)：683-698.
[10] HOSSAIN M N，MILAJERDI S M，WANG J，et al. SLEUTH：real-time attack scenario Reconstruction from COTS audit data[C]//Proceedings of the 26th USENIX Security Symposium. Vancouver，BC：USENIX，2017：487-504.
[11] 李若彤. 新型电力系统APT攻击防御策略集的安全编排与自动化响应方法[D]. 保定：华北电力大学，2024.
[12] WINTERROSE M L，CARTER K M，WAGNER N，et al. Adaptive attacker strategy development against moving target cyber defenses[EB/OL]. [2025-02-02]. https://arxiv.org/abs/1407.8540.
[13] ZHANG H，ZHENG K F，WANG X J，et al. Strategy selection for moving target defense in incomplete information game[J]. Computers，Materials and Continua，2020，62(2)：763-786.

作者简介：
韦峻峰，毕业于西安交通大学，高级工程师，硕士，主要从事IT系统及网络信息安全相关技术及运营研究工作；陈晨，毕业于西安交通大学，工程师，学士，主要从事数通设备及网络信息安全相关的运营研究工作；杨莉，毕业于重庆邮电大学，工程师，硕士，主要研究方向为网络安全运营。