

# T/CCIA

## 中国网络安全产业联盟技术规范

T/CCIA 005-2026

### 网络安全运营大模型参考架构

Cyber Security Operation Large Model Reference Architecture

2026-03-16 发布

2026-05-01 实施

# 目 次

前言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	2
5 网络安全运营大模型核心组件及架构 .....	2
5.1 概述 .....	2
5.2 用户界面 .....	3
5.3 模型推理单元 .....	3
5.4 知识库 .....	3
5.5 安全资源池 .....	3
5.6 数据湖 .....	3
6 网络安全运营大模型运营支撑功能 .....	3
6.1 概述 .....	3
6.2 威胁检测与识别 .....	4
6.3 安全告警关联分析 .....	4
6.4 漏洞评估与优先级排序 .....	4
6.5 自动化响应与处置 .....	4
6.6 智能报告生成 .....	5
6.7 持续学习与模型优化 .....	5
6.8 风险可视化 .....	5
7 网络安全运营大模型部署步骤 .....	5
7.1 确认部署需求 .....	5
7.2 定义度量指标与指标采集方法 .....	6
7.3 执行部署工作 .....	6
8 自身安全保障 .....	6
8.1 数据安全 .....	6
8.2 模型安全 .....	6
8.3 运行环境安全 .....	7
8.4 运维管理安全 .....	7
附录 A (资料性) 网络安全运营大模型工作流程 .....	8
A.1 对话驱动的工作流程 .....	8
A.2 实时数据驱动的工作流程 .....	8

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国网络安全产业联盟提出并归口。

本文件起草单位：深信服科技股份有限公司，云上（江西）安全技术有限公司、太原理工大学、中山大学、南昌大学、武汉大学、东南大学、复旦大学、华东交通大学、东华理工大学、四川大学、中国科学院信息工程研究所、南方电网数据平台与安全（广东）有限公司、北京珞安科技有限责任公司、杭州安恒信息技术股份有限公司、北京元支点信息安全技术有限公司、长扬科技（北京）股份有限公司、北京天融信网络安全技术有限公司、亚信科技（成都）有限公司、南京聚铭网络科技有限公司、蚂蚁科技集团股份有限公司、北京云弈科技有限公司、北京山石网科信息技术有限公司、北京长亭科技有限公司、北京神州绿盟科技有限公司等。

本文件主要起草人：游建舟、刘晨、訾然、杨柳、程寅、黄博正、陈永乐、何海涛、周辉林、夏正伟、胡轶宁、查德平、汤文亮、何月顺、李卫东、李兴国、赵智慧、张振礼、张涛、王建华、袁天伟、胡朝辉、张晓东、关勇、袁明坤、陈星、林建伟、马赛、赵华、王龔、安高峰、刘洞宾、唐开达、陈虎、白晓媛、张会源、钱志强、吴疆、何伊圣、王永振、殷杰、陈爱珍。

# 网络安全运营大模型参考架构

## 1 范围

本文件提出了网络安全运营大模型参考架构，给出了用户界面、模型推理单元、知识库、安全资源池、数据湖的功能及其关系的描述。

本文件适用于网络安全运营大模型相关产品的设计、开发、测试、部署、集成以及评估。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术 术语

GB/T 41867-2022 信息技术 人工智能 术语

GB/T 45288.1-2025 人工智能 大模型 第1部分：通用要求

GB/T 45654-2025 网络安全技术 生成式人工智能服务安全基本要求

## 3 术语和定义

GB/T 25069-2022、GB/T 41867-2022和GB/T 45288.1-2025界定的以及下列术语和定义适用于本文件。

### 3.1

#### 大模型 large-scale model

基于大量数据训练得到，具有复杂计算架构，能处理复杂任务，且具备一定泛化性的深度学习模型。

注：大模型的参数量由其功能和模态决定，一般不低于1亿。大模型训练使用的数据总量受参数量的影响，达到收敛的大模型的参数量的对数与其训练数据总量的对数成正比。

[来源：GB/T 45288.1-2025， 3.1]

### 3.2

#### 大模型服务 large-scale model service

开发、应用大模型及大模型系统的服务，以及以此为手段提供支持需求方业务活动的服务。

注：常见大模型服务内容包括大模型平台服务、大模型开发定制服务、大模型推理及运营服务。

[来源：GB/T 45288.1-2025， 3.2]

### 3.3

#### 网络安全运营大模型 cyber security operation large model

一种结合网络安全专业知识和海量数据以实现安全事件分析、威胁识别、事件研判、响应处置等自动化、智能化运营功能的大模型服务。

### 3.4

#### 用户界面 user interface

用户与网络安全运营大模型应用交互的接口。

注：支持用户输入指令、查看模型分析结果及模型状态等各类智能化安全运营任务交互。

### 3.5

#### 模型推理单元 model inference unit

基于大模型技术，负责执行推理任务的核心组件。

注：根据用户输入或数据湖推送的告警信息触发推理过程，结合安全资源池和知识库提供的相关信息，完成对网络安全威胁的分析和处置响应的生成。

### 3.6

#### 知识库 knowledge base

专门用于存储和管理语义知识的数据库。

注：为模型推理单元提供知识检索能力，通过嵌入法律法规、运营制度等特定知识，辅助模型推理，提升推理结果的准确性和合规性。

### 3.7

#### 安全资源池 security resource pool

为模型推理单元提供安全运营相关的查询、命令执行以及能力调用等支持，实现对网络安全威胁的有效处置响应联动，整合了多种安全能力和资源的集合体。

注：包括但不限于各类安全设备的控制接口、安全工具的调用接口以及安全服务的接入接口等。

### 3.8

#### 数据湖 data lake

负责采集、整合、存储和管理来自不同安全设备、不同厂商的实时网络安全数据的平台。

注：包括如安全日志、原始流量数据、用户行为记录等数据，为模型推理单元提供数据基础。

## 4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口 (Application Programming Interface)

IP：互联网协议 (Internet Protocol)

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

SOAR：安全编排与自动化平台 (Security Orchestration, Automation and Response)

## 5 网络安全运营大模型核心组件及架构

### 5.1 概述

网络安全运营大模型的核心组件包括：

- 用户界面：支持用户进行提问或操作，向用户展示网络安全运营大模型的状态和分析结果；
- 模型推理单元：接收用户界面的提问或实时接收告警作为输入，结合知识库、API 资源池的检索或查询等服务，利用大模型自动化完成威胁分析和处置响应；
- 知识库：为模型推理单元提供知识检索能力，可嵌入特定知识用于增强推理效果，如法律法规、运营制度等；
- 安全资源池：为模型推理单元提供命令执行的自动化操作能力，实现有效的处置响应联动，如防火墙封禁、主机隔离等；
- 数据湖：负责对接不同安全设备、不同厂商的实时网络安全数据，如安全日志、原始流量数据、用户行为记录等。

网络安全运营大模型架构如图 1 所示。

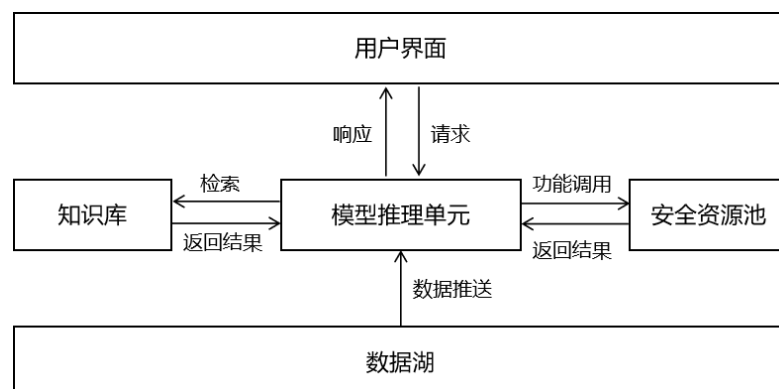


图 1 网络安全运营大模型架构图

## 5.2 用户界面

用户界面是用户与网络安全运营大模型交互的门户，提供友好的交互方式，允许用户提交查询请求、查看分析结果、进行模型配置和管理。用户界面功能包括：

- a) 支持多种交互模式，包括但不限于自然语言问答、图形化操作界面；
- b) 实现统一的用户身份认证和权限管理；
- c) 支持用户对分析结果进行反馈，以持续优化模型性能；
- d) 自然语言问答类交互支持文字、图标等安全运营数据展示能力；
- e) 自然语言问答类应用支持提供基于安全实时数据的响应和交互能力。

## 5.3 模型推理单元

模型推理单元是网络安全运营大模型的核心组件，负责执行威胁分析、事件研判、响应处置等核心任务。模型推理单元功能包括：

- a) 支持多种触发方式，包括用户主动查询、事件触发安全告警；
- b) 具备高效的推理引擎，能够处理大规模、高并发的推理请求；
- c) 具备与知识库、安全资源池等组件进行高效交互，获取所需的知识和执行能力。

## 5.4 知识库

知识库存储和管理网络安全知识内容，通常为向量形式，为模型推理提供知识检索能力。知识库功能包括：

- a) 提供高效的向量检索接口，支持多种相似度度量方法；
- b) 支持存储多种类型的知识，包括但不限于法律法规、安全规范、威胁情报、漏洞信息、攻击模式数据。

## 5.5 安全资源池

安全资源池提供对安全运营过程中各种安全工具和服务的访问接口，使模型推理单元能够调用这些工具和服务执行安全操作。安全资源池功能包括：

- a) 提供统一的 API 接口，屏蔽底层安全工具和服务的差异性；
- b) 支持安全事件响应处置，如 IP 封禁、主机隔离、进程终止；
- c) 支持安全数据查询和分析，如日志查询、流量分析；
- d) 具备访问控制和权限管理机制，确保安全操作的合规性和安全性。

## 5.6 数据湖

数据湖汇聚和存储来自各种安全设备和系统的原始安全数据，为模型训练和推理提供数据支撑，支持多种数据源的接入。数据湖功能包括：

- a) 接入的数据包括但不限于安全设备日志、网络流量数据、用户行为数据、威胁情报数据；
- b) 具备数据清洗、转换和预处理能力，为模型提供高质量的数据；
- c) 支持数据的长期存储和归档；
- d) 具备数据安全和隐私保护机制，符合相关法律法规要求；
- e) 提供数据访问接口，支持模型训练和推理的数据需求。

# 6 网络安全运营大模型运营支撑功能

## 6.1 概述

网络安全运营大模型的运营支撑功能包括：

- a) 威胁检测与识别：利用大模型对海量安全告警和日志数据进行深度分析，及时识别未知和已知的威胁活动。掌握正常与异常行为特征，发现潜在的安全风险与违规操作。结合多源威胁情报，实现威胁态势的感知；

- b) 安全告警关联分析：整合网络、终端、应用等多维度安全告警，通过大模型实现告警关联与溯源。追踪攻击路径，还原攻击链全貌，辅助快速定位安全事件根源；
- c) 漏洞评估与优先级：结合大模型对漏洞风险等级进行智能评估，优先级排序，实现主动防护。根据资产特征，识别潜在的安全薄弱环节，为修复提供决策依据；
- d) 自动化响应与处置：针对不同威胁，提供定制化的响应策略建议，增强安全事件的处理效率。配合安全设备和系统，自动执行检测、封堵、隔离等操作，提高响应速度；
- e) 智能报告生成：自动生成安全事件报告、风险评估报告等文档，提升管理层决策效率；
- f) 持续学习与模型优化：基于外部人员或设备反馈，持续收集和分析新出现的威胁信息，更新模型知识库。借助安全运营实践反馈，不断提升识别准确率与响应效率。
- g) 风险可视化：通过直观清晰的可视化手段，将复杂安全风险转化为易于理解的呈现形式，助力用户快速掌握全局安全态势并精准决策。

## 6.2 威胁检测与识别

网络安全运营大模型具备通过其强大的语义理解和模式识别能力，从传统的规则匹配提升至基于行为和意图的智能分析，在安全运营环节实现威胁检测与识别，主动、精准地从海量、异构的数据中发现隐匿的、高级的威胁活动。具体功能包括：

- a) 基于数据湖，汇集组织范围内的原始安全数据，包括但不限于网络流量日志、终端 EDR 告警、应用访问日志、云平台审计记录以及身份认证日志；
- b) 模型推理单元对经过预处理的原始数据进行深度的语义分析，理解日志条目所描述的语义逻辑；
- c) 模型推理单元通过预训练掌握正常业务操作行为基线，标记偏离安全范畴的行为；
- d) 用户通过安全资源池对异常的属性进行特征标记，特征存储在知识库，并用于实时威胁检测；
- e) 模型以自然语言总结威胁的关键点，提炼包含上下文描述的检测结果，并在用户界面体现。

## 6.3 安全告警关联分析

网络安全运营大模型具备将碎片化的告警串联成完整的攻击链，揭示攻击全貌，实现从单点防御到全局溯源的跨越。具体功能包括：

- a) 模型推理单元基于时间、实体（用户、IP、主机、进程）维度，从数据湖中检索与初步识别的告警相关的上下文数据；
- b) 模型基于自身逻辑推理能力，构建告警之间的因果关系图谱，结合知识库存储的攻防知识，实现具备因果关系安全告警的聚合；
- c) 以可视化方式展示攻击时间线，串联不同告警形成攻击过程全貌，生成安全报告。

## 6.4 漏洞评估与优先级排序

网络安全运营大模型能够引入业务风险和攻击者视角，对漏洞进行智能化的评估与排序，形成修复建议。具体功能包括：

- a) 整合外部漏洞库、资产管理数据库、网络拓扑、业务重要性评级以及实时情报等安全资源；
- b) 模型推理单元基于获取到的漏洞信息，结合安全资源信息进行综合风险评估，以自然语言总结出漏洞的修复建议和优先级；
- c) 以漏洞为索引在用户界面展示漏洞基础信息和模型分析结果。

## 6.5 自动化响应与处置

网络安全运营大模型为安全编排与自动化平台（SOAR）平台提供策略，并实现自主或半自主地执行响应动作。具体功能包括：

- a) 模型推理单元根据已确认的高置信度安全事件的类型、严重程度和影响范围，参考安全资源池的响应剧本库，动态生成或推荐最优响应策略；
- b) 模型需要理解当前场景的细微差别，并对剧本进行调整，生成定制化的处置方案；
- c) 模型通过相似度匹配，借鉴类似事件处理的最佳实践，避免重复错误；
- d) 模型推荐的响应计划在用户界面以步骤列表呈现，并附带每个步骤的预期效果和潜在风险评估。

## 6.6 智能报告生成

网络安全运营大模型能够将复杂的安全数据和分析过程自动转化为专业安全报告,并能基于不同报告对象(例如企业管理层、技术团队、审计人员等)进行定制化。具体功能包括:

- a) 模型推理单元能够通过对话或人为操作触发,或基于定期的安全态势评估后自动触发,整合整个安全事件生命周期的数据,包括从数据湖中提取的原始证据、关联分析过程、处置措施和最终结果;
- b) 模型基于自然语言生成能力,编排结构化和非结构化的信息形成报告,并根据安全资源池中的绘图或制表工具等接口,丰富报告展示效果;
- c) 用户界面集成报告任务的查看、执行、删除等操作功能。

## 6.7 持续学习与模型优化

网络安全运营大模型具备持续学习和自我优化的能力,以保持其分析和响应能力的前沿性。具体功能包括:

- a) 模型推理单元能够通过实时推理调用,将安全资源池接入的威胁情报、持续沉淀的安全知识融入其研判逻辑;
- b) 收集通过用户界面收集分析师对模型的判断进行确认、修正或标记为误报/漏报的标注数据,连同事件处置结果,形成高价值标记数据集;
- c) 模型推理单元根据成功响应案例自动提炼、泛化,并转化为新的向量特征存入知识库,用于未来类似事件的快速识别和处置。
- d) 对模型推理单元进行定期或实时的微调,或通过强化学习来优化其决策逻辑;
- e) 定期基于大规模安全领域数据开展预训练迭代的内容,明确融合新威胁类型、攻击手法、漏洞特征等前沿知识,强化基础模型的泛化能力与场景适配性。

## 6.8 风险可视化

网络安全运营大模型凭借其智能分析能力,通过直观清晰的可视化手段,将复杂安全风险转化为易于理解的呈现形式,助力用户快速掌握全局安全态势并精准决策。具体功能包括:

- a) 依托大模型的威胁检测、告警关联分析及漏洞优先级排序等智能处理结果,通过图形、图表、仪表盘等多元可视化形式集成展示,构建全面动态的安全风险视图;
- b) 支持用户基于大模型的个性化推荐能力自定义可视化界面,灵活调整展示内容、布局与样式,适配不同场景的风险监控需求;
- c) 提供交互式探索功能,用户可通过自然语言对话、点击、筛选等操作,结合大模型的智能关联分析能力深入挖掘风险数据,精准识别潜在安全隐患与攻击路径;
- d) 结合时间维度,展示大模型分析得出的风险变化趋势与历史轨迹,辅助用户预测未来安全事件,制定针对性防范措施;
- e) 在可视化界面中集成大模型驱动的智能报警机制,当检测到高风险事件或异常行为时,以醒目方式实时提醒用户,并联动触发相应响应流程。

# 7 网络安全运营大模型部署步骤

## 7.1 确认部署需求

定义环境部署业务需求,包括但不限于:

- a) 功能需求和非功能需求,如性能指标要求、可靠性要求、安全性要求、可扩展性要求、易用性要求等;
- b) 安全性和合规性要求,如数据安全要求、模型安全要求、访问控制要求、审计要求、合规性标准;
- c) 现有安全基础设施和系统情况,如已部署的安全设备、安全平台、数据源等,以及与现有系统的集成需求;
- d) 预算和资源限制,如硬件资源、软件资源、人力资源、时间资源等。

## 7.2 定义度量指标与指标采集方法

定义关键性能指标，包括但不限于：

- a) 安全事件响应时间，从事件发生到完成处置的平均时间；
- b) 告警准确率，准确告警数量占总告警数量的比例；
- c) 告警降噪率，通过大模型降噪的告警数量占原始告警数量的比例；
- d) 误报率，被误判为安全事件的正常事件数量占总告警数量的比例；
- e) 漏报率，未被检测到的安全事件数量占实际安全事件数量的比例；
- f) 自动化处置率，通过大模型自动化处置的安全事件数量占总安全事件数量的比例。

## 7.3 执行部署工作

部署执行的过程包括但不限于：

- a) 资源准备，包括硬件资源采购、软件资源准备、网络环境搭建、安全资源配置等；
- b) 组件部署，按照实现视图的描述，部署模型推理单元、知识库、数据湖、安全资源池、用户界面等组件，并进行组件配置和集成；
- c) 测试验证，进行功能测试、性能测试、安全测试、集成测试、用户验收测试等，确保系统功能满足需求、性能达到指标、安全可靠；
- d) 服务开通，完成系统部署和测试后，进行系统上线和用户培训，正式开通大模型服务；
- e) 持续监控和优化，建立完善的系统监控和告警机制，持续监控大模型的运行状态、性能指标和安全状况，并根据监控结果和业务需求进行系统优化和升级；
- f) 数据接入和初始化，完成数据湖的数据接入配置，将安全日志、流量数据、资产信息、漏洞信息等数据接入数据湖，并进行数据清洗和标准化处理，为模型训练和推理提供数据基础；
- g) 模型部署和调优，配置模型运行所需的软件环境依赖，并进行模型调优和性能优化，确保模型推理的效率和准确性；
- h) 知识库构建和维护，构建网络安全知识库，包括威胁情报、漏洞知识、攻击技术、安全策略、合规要求等，并定期更新和维护知识库，保证知识的时效性和准确性；
- i) 集成与联动，将大模型与现有 SIEM、SOAR、威胁情报平台等系统进行集成，实现数据共享和功能联动，构建更完善的安全运营体系；
- j) 人员培训和组织建设，对安全运营团队进行大模型的使用培训和管理培训，提升团队的智能化安全运营能力，并建立与之匹配的组织架构和 workflows。

## 8 自身安全保障

### 8.1 数据安全

网络安全运营大模型数据安全保障能力包括：

- a) 输入输出数据内容安全：对输入数据进行恶意内容检测，拦截风险内容；对输出数据进行安全过滤，防范有害信息生成；采用加密传输协议保障数据传输过程安全，存储数据采用国密算法加密保护；
- b) 日志数据安全：规范日志数据采集范围，包含操作主体、操作行为、时间戳、资源信息等关键要素；日志数据异地备份、加密存储，备份保存期限不低于 6 个月；建立日志数据访问控制机制，防止日志篡改或泄露。

### 8.2 模型安全

网络安全运营大模型模型安全保障能力包括：

- a) 模型部署安全：采用模型加密、签名验证等技术，防止模型文件被窃取或篡改；部署过程中开启模型访问鉴权，通过 API 密钥、令牌认证等方式实现授权访问；对模型推理服务进行流量控制和异常请求检测，防范模型推理攻击；
- b) 模型迭代安全：建立模型版本管理机制，对模型迭代过程进行全程记录，支持版本回溯；新版本模型上线前需完成安全测试，验证其抗攻击能力及安全性表现。

### 8.3 运行环境安全

网络安全运营大模型运行环境安全保障能力包括：

- a) 硬件环境安全：选用经过安全认证的硬件设备，开启硬件级安全防护功能；对硬件设备进行物理隔离和访问控制，防止未经授权物理操作；
- b) 操作系统与中间件安全：采用经过安全加固的操作系统及中间件，定期进行安全补丁更新；关闭不必要的服务和端口，减少攻击面；配置安全审计策略，监控系统级操作行为；
- c) 网络环境安全：构建边界防护体系，部署防火墙、入侵检测系统等安全设备；划分网络安全区域，实现不同区域间的访问控制；对网络流量进行实时监控，检测并阻断异常网络连接。

### 8.4 运维管理安全

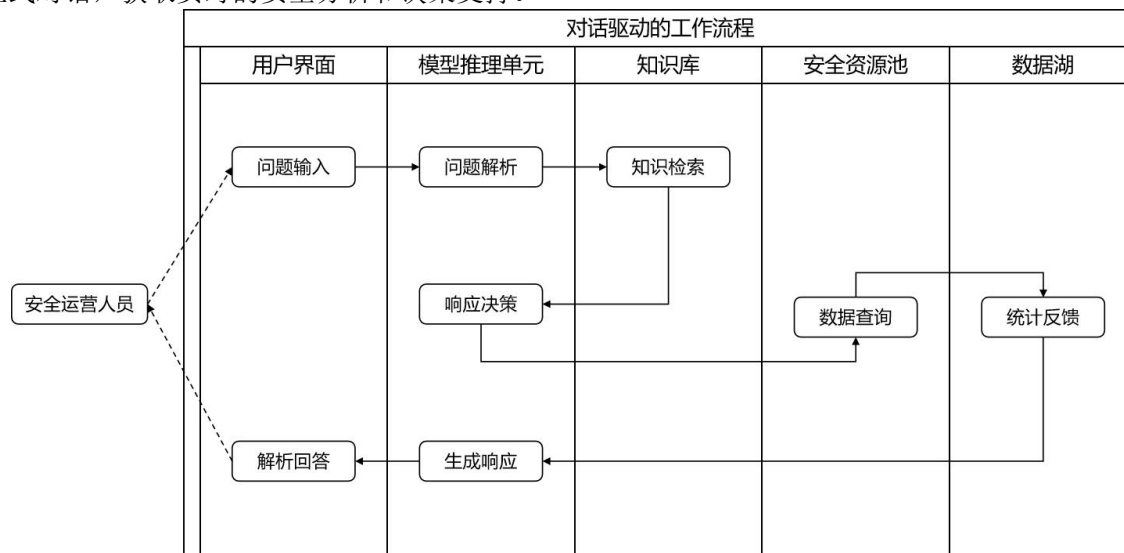
网络安全运营大模型运维管理安全保障能力包括：

- a) 身份认证与授权：采用多因素认证机制对运维人员身份进行验证；基于角色的访问控制分配运维权限，明确不同角色的操作范围；定期开展权限审计，清理无效权限；
- b) 运维操作规范：制定标准化运维操作流程，对关键操作实行双人复核制度；运维操作全程记录日志，确保操作可追溯；建立应急响应机制，针对安全事件制定处置流程和恢复方案。

## 附录 A (资料性) 网络安全运营大模型工作流程

### A.1 对话驱动的工作流程

对话驱动的工作流程如图A.1所示，以安全运营人员为代表的用户通过与网络安全运营大模型进行交互式对话，获取实时的安全分析和决策支持。



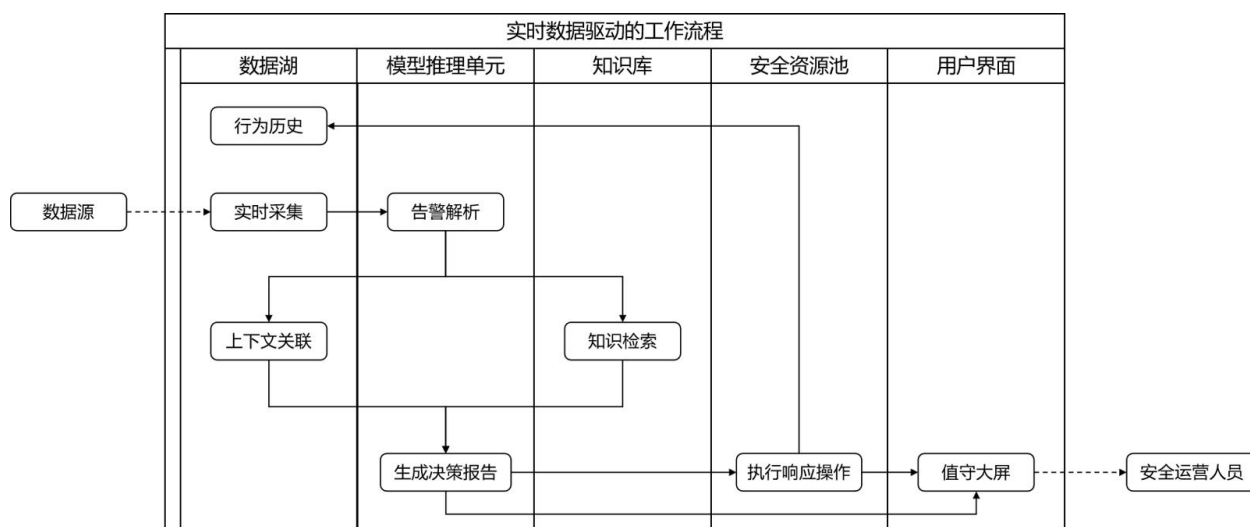
图A.1 对话驱动的工作流程

对话驱动的辅助运营工作流程，主要包括以下8个步骤：

- a) 问题输入：安全运营人员通过用户界面的聊天窗口，输入需要咨询的问题或内容；
- b) 问题解析：模型推理单元接收到问题后，利用大模型的自然语言理解能力，对问题进行解析，提取用于表示问题意图的语义向量；
- c) 知识检索：模型推理单元根据提取的语义向量，在知识库中检索相关知识，返回模型推理单元进行综合分析和决策；
- d) 响应决策：决策过程评估响应所涉及的外部工具，模型推理单元自动匹配安全资源池中合适的 API，并由大模型生成 API 调用命令所需的对象属性和范围参数；
- e) 数据查询：安全资源池发起 API 调用命令进行数据查询或其他操作；
- f) 统计反馈：数据湖执行查询任务，将结果数据反馈给模型推理单元，如告警列表、资产统计信息、漏洞统计信息等；
- g) 生成响应：结合实时安全数据信息，模型推理单元利用大模型生成详细的响应内容，包括威胁趋势分析、威胁主体调查、处置建议等；
- h) 解析回答：通过用户界面的解析，将回答中的特定信息以图表、排版展示给安全运营人员，安全运营人员可以根据大模型的响应内容继续进行后续问答。

### A.2 实时数据驱动的工作流程

实时数据驱动的工作流程见图A.2所示，实时采集和分析来自不同数据源的安全日志，自动完成研判及响应闭环，大幅提升威胁研判效率和分析范围。



图A.2 实时数据驱动的工作流程

实时数据驱动的自动化运营工作流程，主要包括以下7个步骤：

- a) 实时采集：数据湖持续收集和监控来自各种安全设备的实时数据，完成数据融合和标准化，并推送给模型推理单元；
- b) 告警解析：模型推理单元接收标准化后的告警信息，理解告警语义并提取告警关键内容；
- c) 上下文关联：根据提取内容关联数据湖中存储的上下文告警信息、资产信息、漏洞信息等；
- d) 知识检索：基于告警语义进行知识库检索，检索信息反馈给模型推理单元；
- e) 生成决策报告：结合上下文关联及知识检索内容，模型推理单元从攻击方向、关联资产、威胁情报、访问意图等维度生成研判报告，并制定相应的响应策略和措施；
- f) 执行响应操作：通过安全资源池执行特定的安全事件响应操作，并将操作行为历史记录到数据湖中，如隔离攻击主机、阻断恶意访问等；
- g) 值守大屏展示：全面展示告警降噪和自主值守情况，实时统计大模型的处置结论和威胁处置进展，帮助安全运营人员直观地了解当前的网络安全大模型的研判和处置结论。