AI驱动人社领域网络安全主动防御体系

构建项目需求方案

围绕网络安全核心需求，构建由中枢系统、支撑引擎、生态系统、管理体系及技术性能保障组成的完整体系，运用AI技术提升安全防护能力。

一、构建数据融合中枢

通过人工智能技术，构建“安全数据底座”，集成数据采集、清洗、转化三大核心能力，实现安全类、网络类、系统类以及接口类等多源异构数据的全生命周期治理。通过“数据搬运”模块，以实时采集技术快速汇聚分散在各终端、系统中的日志数据；“数据净化”环节运用清洗降噪算法，去除冗余信息，统一数据格式标准；“数据翻译”则深度解析日志内容，将非结构化数据转化为AI可识别的结构化语义特征，形成统一、规范的数据基座。由此，为安全事件预警、风险研判等智能化决策提供标准化数据支撑与高质量数据集。

（一）数据汇聚需求

**1.安全类日志数据**

汇聚防火墙、IDS等安全设备的攻击拦截、威胁告警日志；集成态势感知平台、SIEM等系统的风险分析与漏洞数据，支撑安全事件研判。

**2.网络类日志数据**

采集交换机、路由器等设备的流量元数据（五元组、带宽等），收录配置变更、链路中断告警及NAT日志，监控网络运行状态。

**3.系统类日志数据**

记录服务器、终端用户的登录、权限变更等操作行为，采集操作系统内核告警、服务异常及认证日志，保障系统运行安全。

**4.接口类日志**

记录接口调用全程数据用于调试追踪；统计性能指标与错误信息辅助优化；监控权限校验、限流熔断等安全管理数据，支撑接口迭代部署。

（二）数据治理需求

统一汇聚与标准化：实现多源数据实时接入并完成格式标准化，消除数据异构问题。

智能清洗与降噪：过滤重复告警、系统冗余等无效日志，合并同类事件，降低数据噪音。

（三）语义转化与AI适配需求

将清洗后的数据转化为机器可理解的结构化语言，提取安全语义特征，生成适配机器学习模型的标准化数据集。

二、构建数据融通中枢​

充分利用AI数据关联技术，打破数据孤岛，挖掘数据间潜在关系，实现安全数据的深度融合与智能分析，为网络安全态势感知与决策提供有力支撑。​

（一）数据关联分析​

利用AI算法对多源异构的安全数据进行深度关联分析，例如将安全类日志中的攻击告警与网络类日志的流量异常数据进行关联。通过机器学习中的关联规则挖掘算法，找出攻击行为与网络流量变化之间的内在联系，精准定位安全事件的源头和传播路径。同时，针对系统类日志中的用户操作行为与接口类日志的权限调用数据进行关联，判断是否存在异常权限操作引发的安全风险，为安全事件的快速定位与处置提供依据。​

（二）动态关联响应​

基于AI的实时学习能力，数据融通中枢能够对网络安全事件进行动态关联响应。当检测到新的安全威胁时，系统自动关联历史相似事件数据，分析其发展趋势和潜在影响。通过深度学习模型对关联数据进行预测，提前采取防御措施。例如，当发现某一类型的恶意软件攻击时，系统快速关联以往同类攻击的数据，预测其可能的传播范围和攻击目标，自动调整防火墙策略、加强关键系统防护，实现主动式安全防御。​

（三）数据可视化与决策支持​

通过AI数据关联技术处理后的数据，以直观的可视化方式呈现。利用图形化界面展示数据之间的关联关系、安全事件的演变过程以及网络安全态势的整体情况。安全管理人员可以通过可视化图表快速理解复杂的安全数据，辅助决策制定。例如，通过关联分析生成的攻击路径可视化图，帮助管理员清晰了解攻击的来源、经过的节点和可能的目标，从而制定更有效的防御策略，提升网络安全应急响应效率。

三、资产测绘中枢​

运用AI技术对人社系统内服务器、业务系统、网络设备等资产进行自动化识别与测绘，生成精准的“数字资产地图”。通过AI算法自动分析资产属性，为每项资产赋予“风险标签”，涵盖资产是否暴露于互联网、是否关联核心业务、存在的已知漏洞等关键风险信息。该地图以可视化方式直观呈现人社系统网络安全的关键节点与薄弱环节，助力安全团队快速定位高风险区域，为制定差异化、精准化的安全防护策略提供数据依据，有效提升人社系统网络安全防护的针对性和有效性。​

（一）资产自动化识别与测绘技术升级​

采用机器学习与深度学习相结合的技术，实现对人社系统资产的全面、精准识别。通过网络流量分析算法，自动发现隐藏在网络中的未登记资产；利用自然语言处理技术，解析业务系统文档与配置文件，精准识别资产功能与用途。同时，借助AI图像识别技术，对设备外观、运行状态等物理资产进行可视化测绘，确保资产信息完整覆盖物理和虚拟领域。​

（二）动态风险标签体系构建​

基于资产实时状态与威胁情报，构建动态更新的“风险标签”体系。AI系统持续监测资产的漏洞修复情况、网络攻击暴露面变化，以及业务关联度调整，自动更新风险标签。例如，当某服务器关联的业务系统被纳入核心民生服务范畴时，系统自动提升该资产的风险等级；若资产修复了高危漏洞，风险标签随即降级，实现风险评估的实时性与准确性。​

（三）多维度资产地图应用场景拓展​

“数字资产地图”不仅用于直观展示安全风险，还深度融入人社系统安全管理全流程。在日常巡检中，安全人员可通过地图快速筛选高风险资产，针对性开展漏洞扫描与安全加固；在应急响应阶段，地图联动威胁情报与安全事件数据，直观呈现攻击路径与受影响资产范围，辅助制定高效的应急处置方案；在合规审计时，资产地图提供完整的资产台账与风险证据链，助力满足监管要求。​

（四）资产测绘与其他安全模块联动​

资产测绘中枢与数据融合中枢、数据融通中枢形成闭环联动。将资产测绘结果同步至数据融合中枢，为安全数据采集提供明确目标与范围；当数据融通中枢检测到安全威胁时，资产测绘中枢实时更新受影响资产的风险状态，并通过资产地图标注异常区域，实现安全防护的协同作战，全面提升人社系统网络安全防御能力。​

四、打造中枢支撑引擎

（一）行为基线引擎​

为用户和设备建立“行为档案”，基于历史操作数据，运用机器学习算法学习正常操作习惯，构建行为基线模型。实时监测用户和设备行为，一旦出现偏离基线的异常行为，系统立即发出预警，有效防范内部误操作或外部伪装攻击。

（二）弹性策略引擎​

面对新型攻击，AI智能算法能够自动分析攻击特征，实时生成防御策略。例如，当检测到恶意流量攻击时，系统自动切断可疑连接、清洗流量、暂时关闭风险接口等，实现防御策略的动态调整，无需人工干预。同时，支持防御策略的自定义配置与优化。​

（三）协同防御引擎​

建立异构安全设备之间的通信与协同机制，实现安全情报共享。当某一安全设备检测到威胁时，能够及时将情报传递给其他相关设备，触发全网协同防范，提升整体防御能力

（四）供应链安全引擎​

建立完善的供应链目录，对人社系统相关的软硬件供应商、服务提供商等进行全面管理。实时监控供应链各环节，开展风险评估和漏洞检测，确保供应链的合规性与可靠性，防范供应链攻击风险。​

五、培育“生态”系统​

（一）动态防御演练​

依托虚拟技术构建“攻防演练场”，运用AI模拟多样化的黑客攻击场景，包括常见攻击手段和新型攻击模式。通过定期开展实战对抗演练，暴露系统安全隐患，及时查缺补漏，持续优化防御体系。​

（二）新型威胁对抗​

针对黑客利用大模型的攻击手段，运用大模型技术模拟恶意行为，开展对抗训练。通过不断学习和优化，提升AI对新型AI威胁的识别和防御能力，精准识破攻击“伪装术”。​

（三）源头风险治理​

借助AI深度学习能力，对人社系统的代码进行深度分析，穿透代码底层挖掘潜在逻辑漏洞。从软件开发源头消除安全隐患，构建更稳固的数字安全基座。​

（四）业务安全融合​

将安全防护深度嵌入人社业务全流程，根据不同业务场景需求，定制“个性化”防护方案。确保安全防护与业务系统无缝集成，使安全成为信息系统的“内生基因”。​

六、软件供应链安全

（1）软件供应链安全管理平台建设

需要软件供应链安全管理平台，具体须具备四大核心功能：一是实现供应商管理及审查，通过创建目录集中管控企业软件供应商，并进行安全画像；二是开展资产管理与知识图谱测绘，识别各类软件 SBOM 及风险，绘制安全图谱以确定风险影响范围；三是进行软件供应链态势分析，以可视化大屏展示风险数据统计、态势及漏洞管理情况；四是收集处理安全情报，自动分析漏洞等信息并关联资产，及时推送风险情报辅助治理。

（2）静态代码分析能力

需要建立一套完整的静态代码分析体系，将其深度融入日常安全流程。该体系须具备主流代码语言检测能力，覆盖 Java、C/C++、Python、Go、C#、JavaScript 等主要开发语言；需针对 Java 语言支持字节码检测，可对.jar 和.war 格式的包进行无需源码的检测；需实现常见代码风险检测，涵盖安全缺陷、质量缺陷、编码规范三大类，支持 SQL 注入、反序列化等常见漏洞类型的检测；还需提供源代码编码规则检测、安全漏洞检测、度量统计、克隆检测、逆向架构图自动生成等功能，构建起源代码安全自主检测体系和能力。

（3）源代码软件成分分析

源代码软件须具备成分分析能力，面向源码文件检测，通过特征或代码分析识别开发人员有意或违规引用的开源第三方组件，利用应用组成分析引擎多维度提取开源组件特征，挖掘安全漏洞与开源协议风险。具体需覆盖Java、C/C++等主流语言组件检测；能识别应用内依赖组件的名称、版本号等成分信息；可检出漏洞并展示名称、CVSS评分等详情；还能匹配开源许可证特征，提供包括风险等级、兼容性说明等信息。

（4）二进制软件成分分析

二进制软件成分分析须具备面向二进制文件的检测能力，通过分析文件特征，识别成品软件中的开源组件及安全风险，助力供应链安全管理体系质量门禁建设。需支持 zip、jar 等常见压缩文件，Android APK、IPA 等移动应用文件，RPM、DEB 等安装包文件，以及 VDI、VMDK 等文件系统和磁盘映像格式的检测。

七、IPv6升级改造

为适应互联网技术演进趋势，提升网络兼容性与业务服务能力，需对省人社厅网络设备实施全面IPv6升级改造工程。通过部署双协议栈技术，确保核心交换机、路由器、防火墙等关键网络设备同时支持IPv4和IPv6协议，实现新旧网络协议无缝共存。改造后，人社厅网络环境将全面满足终端设备对IPv4和IPv6互联网业务的同步访问需求，有效消除网络访问限制，提升网络传输效率与服务质量。

八、管理强化需求​

（一）责任闭环管理​

利用AI建立全流程监管框架，涵盖安全责任分配、任务执行、过程监控到整改验收等环节。详细记录每个环节的操作信息和责任人，实现安全责任全程可追溯，确保责任落实到位。​

（二）智能考核评价​

制定基于AI的安全管理考核指标体系，将漏洞修复速度、应急响应效率、安全策略执行情况等关键要素量化成具体指标。通过系统自动收集和分析数据，实现对安全管理工作的客观、公正评价，使安全管理标准清晰明确。​

（三）自动化基础工作​

实现AI自动盘点资产，实时更新资产信息；对系统日志进行实时分析，自动识别异常行为；一键生成详细的风险报告，并根据预设规则触发相应的处置流程，大幅减少人工操作，提高工作效率。​

九、技术需求​

（一）AI技术应用​

综合运用深度学习、机器学习、自然语言处理等AI技术，支撑各功能模块的实现。如利用深度学习算法优化行为基线模型和威胁检测模型，运用自然语言处理技术辅助日志分析和安全报告生成。​

（二）大数据技术​

采用先进的大数据处理技术，实现海量安全数据的高效采集、存储、处理和分析。运用大数据平台和相关工具，支撑数据融合中枢的数据处理和资产测绘中枢的数据分析工作。​

（三）网络安全技术​

部署完善的网络安全设备和系统，包括防火墙、入侵检测与防御系统、漏洞扫描工具等，并确保其与“引擎”系统和“中枢”系统的有效集成，实现协同防护。​

（四）系统集成技术​

提供标准、开放的接口规范，确保各功能模块之间以及与现有业务系统、安全设备的无缝集成。采用成熟的系统集成技术和架构，保障系统的稳定性和扩展性。​

十、性能需求​

实时性：数据采集、分析和响应过程须具备高度实时性，确保安全威胁能够在最短时间内被发现和处理，关键操作响应时间控制在秒级以内。​

准确性：威胁检测、行为分析等功能的准确率不低于95%，误报率控制在5%以下，保障安全防护的有效性。​

扩展性：系统应具备良好的扩展性，能够适应人社业务的发展和网络规模的扩大，方便进行硬件扩容、软件升级和功能扩展。​

稳定性：系统须具备高稳定性，平均无故障时间（MTBF）不低于99.9%，确保持续可靠运行。​

十一、安全需求​

自身安全防护：对主动防御体系自身的关键组件和数据进行加密保护，设置严格的访问控制策略，防止被攻击和非法访问。​

安全审计：建立全面的安全审计机制，对系统内所有操作进行记录和审计，审计日志保存期限不少于一年，以便安全事件追溯和分析。​

合规性：项目建设符合《中华人民共和国网络安全法》、网络安全等级保护等相关法律法规和标准规范要求，确保系统在安全管理和技术防护方面满足合规性审查。