**基于GPT技术的网络安全体系关键技术研究及应用**

**项目申报指南**

**一、需求目标**

项目围绕河北高速集团数字化转型面临的网络安全、国产商用密码应用的总体体系架构缺失、关键建设任务不明朗、试点应用经验不足、成熟应用推广匮乏等问题，设计注重信息共享和自主可控且集网络安全、国产商用密码应用、信息技术应用创新“三位一体”的全场景、全流程、全链路、自主可控的保障体系和产品，贯穿河北高速集团组织和数字化转型全生命周期。通过研究河北高速集团网络安全与国产商用密码应用的面临形势、当前现状和差距，为河北高速集团找准方向奠定基础；提出基于国密和信创的河北高速集团网络安全体系架构、关键建设任务和关键举措，为河北高速集团明确未来一段时间的行动路径；选取紧急且重要的关键任务进行技术攻关和试点，探索总结经验、形成试点样板，为河北高速集团未来全面推广奠定基础，如基于国密自主可控的增强型端侧可信身份及安全防护技术攻关和试点、基于GPT技术重构安全管理与运维服务流程，形成全国交通领域首个“网络安全机器人”和“国密可信安全链路”原型产品，并可在市场应用推广。

**二、产品指标**

1、网络安全机器人

（一）功能指标

面向集团网络安全领域应用，形成网络安全机器人产品，构建具备网络安全常见知识和最佳实践流程的专用大模型平台，重构集团安全管理与网络安全运维服务流程。

基于自然语言的交互式安全运营，依托于各类数据模型、语料与数据集，结合高速实际场景和安全数据进行预训练训练，构建安全大模型基座平台。通过采集集团来自终端、网络中海量网络安全威胁数据，以及其他合法来源的网络安全百科知识等，进行数据清洗、数据扩充、数据配比融合，形成高质量完备的安全数据。经过数据进行增量预训练和指令微调，打造具备安全问答、上下文理解、产品数据联动、服从合规原则的安全原始大模型。同时，将安全检测、事件研判、排查检索、值守处置涉及的安全业务进行建模和嵌套，使得安全大模型衍生业务思维逻辑，进一步扩展对终端安全、安全态势感知、安全运营平台、防火墙等产品联动处置能力，具体功能如下：

资产查询与统计：基于对话框的模式，对现网内的资产进行各个维度的统计、查询，以MarkDown、表格、饼图的方式进行输出，对查询到的数据，能够以自然语言的方式进行描述与总结。

安全数据解读：支持以自然语言的方式对HTTP告警数据包、威胁情报、恶意文件进行解读，并支持对告警解读的内容进行多轮追问与解答，支持分析恶意文件并支持虚拟执行返回专家解读结果，并支持将结果导出pdf文件，同时针对IOA安全告警可直接通过GPT完成解读。

漏洞管理：支持对全网的资产进行漏洞排查，并将存在特定漏洞的资产与相关字段关联起来。

安全告警研判：支持安全管理员通过对话框对特定时间内的告警进行查询与统计分析、解读安全告警后会出现各类推荐问题，基于这些问题的点击会逐步指导用户完成安全告警的研判、分析、处置等闭环动作。

安全事件解读：支持以故事线、自然语言的方式进行讲述、帮助管理员看清当前事件的来龙去脉。支持统计一段时间内的安全趋势情况。

平台具备安全百科知识解读能力，能够对平台上的专业词汇进行解读。

支持对java代码注入、命令注入、sql注入、java反序列化、php代码注入、xss注入、webshell上传、系统信息泄露、目录穿越等类型网络安全攻击进行检测与研判，对攻击手法进行剖析、解释、还原，并给出对应的处置建议，支持对语法混淆、多层编码、协议异常等多种组合攻击方式的检测，弥补传统防御技术的缺陷。

支持实时告警分析，可实现思维链处置过程追溯，24小时不间断自动分析，实时值守，可结合数据包解读、周期检测、资产分析、威胁情报分析和基础信息分析等维度输出研判处置思考过程，针对人工决策告警支持自动给出具体处置建议，针对自动处置告警支持直接实现自动处置并展示处置状态。

（二）性能指标

|  |  |
| --- | --- |
| 可用于预训练网络安全语料数据规模 | >=1TB |
| 用于微调安全领域专属任务的数据集 | >=1000000条 |
| 安全GPT模型参数规模 | >=35B |
| 上下文长度 | >=8192 |
| 值守时间 | 7\*24小时 |
| 实时生成网络安全告警分析报告时间延迟 | <=3分钟 |
| 误报率 | <=5% |

2、国密可信安全链路

（一）功能指标

国密可信安全链路产品依据国密信创相关标准，充分考虑河北高速集团各类核心应用系统的兼容性匹配研发，该国密信创安全加密平台可以对集团各类信息化应用链路传输数据、视频等进行加密，同时支持签名验签及MAC功能的产品。部署在集团与各分子公司应用系统需求的两端，不改变现有网络拓扑结构，在“云-边-端”数据发出端加密、接收端解密，针对不同需求对报文不同的字段进行加解密，保证集团各类核心数据、视频传输安全，同时提供签名验证及MAC功能，实现一机功能多用。此产品市场应用场景广阔。

系统支持通过WEB方式对设备进行配置管理及查询，易用性高、管理方便。不改变原网络拓扑结构，支持多种加密算法，配置相关需要加密数据流策略即可对以太网的(L3：网络IP层)、(L4：传输层的TCP/UDP)加解密数据进行高性能加密和解密传输。

高安全性：产品支持国密算法，支持一链路一密钥进行加密，支持在线模式通过数字证书进行身份认证和密钥协商，支持离线模式密钥更新；

国密信创零改造周密考虑河北高速集团各类行业专线的多样性与复杂性，创新研发不需要IP地址即可实现透明加密传输，同时支持签名验证和完整性校验。

易用性不改变集团与各分子公司原网络拓扑结构，配置相关需要加密数据流策略即可对数据进行加密传输；

Web界面配置及查询操作简单易懂，适合集团与各分子公司技术人员上手操作，登录设备的管理IP地址，输入用户名和密码登录后，可以查看当前策略的配置信息，可对策略进行增、删、改、查的操作。

应用范围：对以太网(L3：网络IP层)、(L4：传输层的TCP/UDP)加解密：L3:对IP包的payload段进行加密，L4:对TCP/UDP的payload段进行加密

支持签名验签及MAC的功能，集团数据中心及各分子公司应用系统链路数据加密时能够灵活实现网络数据包“加密”、“解析”、“加密+解析”等多种组合的形式配置策略，实现一机功能多用的灵活性，最大限度贴合集团与各分子公司个性化需求；

旁路模式：产品部署在集团数据中心及各分子公司网络中不改变网络拓扑结构；产品支持旁路配置，当配置旁路模式时，数据不进行加密

（二）性能指标

加密算法种类指标：非对称算法：SM2;对称算法：SM4;杂凑算法：SM3支持在线模式周期自动更新密钥；支持离线模式手动更新密钥；

以太网链路加密性能：对对以太网(L3：网络IP层)、(L4：传输层的TCP/UDP)加密：对源IP、源port、目的IP、目的port和TYPE的精确和模糊匹配加密；

产品支持2048条业务加解密、加解密+HMAC策略匹配设置；

产品支持512条业务签名验签、加解密+签名验签策略匹配设置；

高性能测试指标

单向测试性能：

>=512Bytes大包数据，10Gbps

64Bytes小包数据，3Gbps

双向测试性能：

>=512Bytes大包数据，7Gbps

64Bytes小包数据，1.5Gbps

3、集团统一安全监管平台

（一）功能指标

1、数据采集：

具备网络侧和端侧流量数据采集能力，针对数据中心南北向威胁流量汇聚，数据类型包含但不限于：脆弱性、访问风险、服务探测、后门通信、账号爆破、攻击利用、Dos攻击、漏洞攻击、黑客工具、数据库攻击利用、访问恶意文件、感染病毒、流量异常、流量审计日志、Payload等内容；实时监测采集终端元数据及攻击信标数据，数据类型包含但不限于：网络连接、模块加载、进程与创建、DNS查询、文件创建与删除、注册表值设置、端口监听等内容。

具备将采集内容进行数据质量效果进行分析并评级功能，包含以下三级：

一级安全效果：

日志解析：所接入上报日志触发内置规则后能够生成安全日志，触发一次规则生成一条安全日志。

二级安全效果：

告警聚合：将多条同类安全日志聚合生成告警；告警融合：将不同来源设备所上报的日志融合生成告警；业务误报：能检测到告警是由正常业务访问行为触发，非攻击行为。

三级安全效果：

攻击成功：能够检测出告警的攻击结果为攻击成功；威胁定性：能够对告警的攻击行为进行定性，比如是否业务行为、病毒行为、定向攻击行为、扫描行为等；人为攻击：能够检测到告警定性为定向攻击；网端关联告警：网和端设备检测的告警能够关联成一条告警/事件；

2、可视化呈现

具备首页自定义按多维度时间周期展示功能：待办事项：待处置事件、风险资产、高修复优先级脆弱性和待处置工单等，基于资产安全事件和脆弱性，工单等基于评分规则，按照优、良、中、差等进行评分）；风险处置工作进展：事件处置数、事件处置率、遏制恶意域名、提效时长、处置文件数、工单处置数等；安全事件：严重、高危、中危、低危事件待处置情况与趋势呈现；智能响应：展示威胁实体处置数量、事件平均遏制耗时、事件自动遏制率、关键威胁响应等；资产概览：展示全部资产与核心资产数量与占比，风险资产发生趋势，脆弱性概览，资产体检等。

具备展示全网日志、安全告警、安全事件的数量，以及全网日志到告警的削减比例和全网告警到事件的削减比例，引擎告警和加白的数量，安全事件生成的方式分布以及多源检出、独报的占比等功能。

3、响应处置

具备针对事件执行处置剧本和动作功能。执行动作根据应用类型、动作类型进行动作设置，并按资源/标签选取执行组件，执行动作的响应对象包括不局限于：端点安全应用、网络安全应用、基础设施应用、通信应用、工具类应用、威胁情报应用，可选择处置、撤销、管控、通知、更新、备份、调查等执行动作类别。

具备通过拖拽方式灵活自定义编排威胁的响应处置流程，执行节点内容包括：动作调度、剧本应用、决策器、过滤器、人工审批、人工录入等必要的关键节点，通过对同网络安全设备的联动，实现对威胁的快速响应与处置，处置动作包含：封禁地址管理、隔离主机、信任文件管理、阻断进程管理、拦截域名管理。

4、资产管理

具备以资产组/业务组维度维度梳理资产详细台账功能，进行资产全生命周期管理（资产入库、审核、操作、退库等），可配置资产组的基本信息、资产组范围。业务组自定义可配置业务名称、业务所属上级、业务的资产范围、责任人、重要级别和备注等。

具备资产基础信息、关联IP、操作系统、设备信息、资产责任人统计功能，并梳理资产指纹以及统计硬件信息。

5、风险管理

具备以风险视角，对脆弱性风险进行展示，可对脆弱性类型、威胁标签、修复优先级、检测方式、脆弱性名称、数据源等标签进行筛选，并图形化展示整体脆弱性风险、高修复优先级脆弱性风险情况，并可点击脆弱性详情进行操作。

具备漏洞管理功能，统计分析漏洞详情，并在CVSS评分的基础上，结合漏洞可利用性、脆弱性端口暴露性、资产暴露面属性、资产重要程度和是否为热点漏洞，基于真实环境进行漏洞修复优先级评级。

具备安全事件、安全告警、攻击面风险等多角度呈现问题功能，结合ATT&CK矩阵更好发现风险资产已知威胁和潜在风险。

具备最新热点威胁趋势赋能条件，对热点威胁进行时间轴展示，披露漏洞名称、风险等级、CVE编号、可检测情况，影响资产、威胁标签、爆发时间。

具备对风险应用查看是否有资产关联安装该应用功能，并查看该资产上风险应用的数量及风险应用的介绍。

6、能力增长

与基于GPT技术的安全管理与运维服务流程重构平台对接，实现安全数据流量本地检测增强和告警解读能力，对接成功后能够通过GPT技术进行本地训练、微调，实现对话推理、自动化值守等安全管理功能。

（二）性能指标

|  |  |
| --- | --- |
| 可存储数据量 | >=100T |
| 可接入终端数 | >=5000个 |
| 可接入服务器数量 | >=500个 |
| 可接收处理日志处理能力 | >=6亿条/天 |
| 内置分析检测引擎 | >=50种 |
| 内置数据分析规则 | >=100条 |
| 攻击进程树纵向层级 | >=15层 |
| 自动化响应处置执行条件 | 脆弱性执行条件>=16个；安全告警执行条件>=29个 |
| 终端遥测源对ATT&CK框架中各种攻击类型的检测技术覆盖面 | >=370项 |

4、基于信创国密零信任架构下的数字云安全接入平台

（一）功能指标

采用“流量身份化”和“动态自适应访问控制”为核心的零信任创新技术构建数字云安全接入平台。通过平台网络隐身、终端动态环境检测、全周期业务准入、智能权限基线、多源信任评估等核心能力，满足新形势下数字云应用安全接入访问需求。平台采用SDP架构设计，由安全代理访问组件和控制器组件两部分组成，实现控制面和数据面的分离。控制器负责认证、授权、策略管理与下发，是整体的调度与管理中心，对接入的身份、终端、环境、行为进行信任评估，基于策略引擎配置的策略结果，决定允许或拒绝会话并让安全代理访问组件进行放通或阻断，具体功能如下：

资源发布：通过隧道模式，可以支持基于TCP、UDP、ICMP等协议代理访问业务资源，支持发布IP、IP范围、IP段、具体域名及通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面。通过WEB模式，可以支持基于http或https协议代理访问业务资源，支持发布IP或域名形式的后端服务器地址，可配置业务应用的具体访问URL路径。

客户端兼容性：零信任客户端应兼容主流国产与非国产终端操作系统，包括但不限于：Windows7（32位、64位）、Windows10（32位、64位）、Windows11（64位）、MacOS10、MacOS11、MacOS12、Android、iOS、麒麟V10、统信V20等。

客户端选路：对于多线路接入单网关访问业务的场景，支持时延优先的选路模式，首次接入时客户端以最低时延线路接入访问业务，后续客户端进行周期性探测线路时延，当时延超出设定值时判定为恶化线路。为排除线路探测时的临时网络波动，需多次探测为恶化线路时再进行线路切换，确认可切换后智能切换至当前最优时延的线路上。

认证管理：支持多种认证方式，包括但不限于支持以下认证方式：本地账号密码认证、LDAP/AD认证、OAuth2.0标准协议的票据认证、CAS标准协议的票据认证、Radius账号认证、HTTPS帐号认证、证书主认证、证书辅认证、短信主认证、短信辅认证、标准Radius令牌认证、第三方令牌认证、TOTP动态令牌认证等认证方式，并可与企业微信、阿里钉钉、飞书结合实现扫码认证，支持飞书用户或个人微信企业号通过H5接入。

增强认证：可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、闲置帐号登录、弱密码登录、异常时间登录、非常用地点登录等。

业务安全访问：支持配置动态访问规则，可配置化的ACL规则引擎，可以灵活地将终端环境、用户身份、处置动作等进行配置，为单位不同业务不同部门提供灵活丰富的访问控制策略。

暴露面收缩：支持单包授权能力（SPA），支持UDP+TCP组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口，不会出现敲门放大漏洞。PC端和移动端均支持通过安全码激活客户端为授权客户端，从而可进行SPA敲门和连接。

支持中国商用密码标准，支持加密算法SM2、SM3、SM4。

（二）性能指标

|  |  |
| --- | --- |
| 最大并发用户数 | >=3000个 |
| 加密流量 | >=480Mbps |
| HTTPS并发连接数 | >=48000个 |
| HTTPS新建连接数 | >=320个/秒 |

**三、成果与验收指标**

1、提交满足考核指标的系统平台，完成相关系统功能测试，形成2个原型产品并提供系统与产品使用说明书

2、提交《河北高速集团网络安全三年行动方案（含总体目标、关键任务和举措等）》报告1份。

3、提交《河北高速集团与分子公司网络安全技术要求》《河北高速集团分子公司网络安全管理与运维服务流程改造经验》《河北高速集团数字云安全动态接入经验》基础性、通用性技术规范3份。

4、申请发明专利1项，录用核心期刊论文2篇、软著2项。

**四、项目实施周期：24个月。**

**五、榜单金额：935.05万元。**

**六、揭榜团队要求。**

（一）揭榜团队须为在中华人民共和国境内注册、具有独立法人资格的企事业单位。

（二）揭榜团队应了解行业最新动态，具有信息化类技术研发、软件开发或相关项目承担经验。

（三）揭榜团队及项目负责人具备良好的社会信用，近3年无不良信用记录或重大违法行为。保证所提供申报项目信息的真实性，严格遵循科研诚信等有关规定，并对信息虚假导致的后果承担责任。

（四）揭榜团队及项目负责人需承诺揭榜后能够在指定期限内完成相应任务；承诺揭榜攻关期间积极响应技术需求方，提出攻克关键核心技术的可行性方案，掌握自主知识产权；具有相对稳定的技术支撑队伍与相关经验，能协助需求方完成技术应用落地实施。

（五）揭榜团队负责人应为项目承担单位在职人员，揭榜攻关期间原则上不得更换和调离。

（六）鼓励企业、金融机构、科技服务机构、高校、科研院所及新型研发机构等以联合体方式申报，牵头单位为1家，联合体成员不超过4家。