**上海市公安局长宁分局数据安全监测预警能力提升项目**

**采购需求文件**

**一、项目概况**

**1.1项目背景**

2024年，长宁分局认真贯彻国家、公安部的政策精神，按照市局部署要求，通过建设数据安全态势感知两级平台，实现了基础的资产发现和风险感知等能力。

当前，随着分局数据中心架构的不断完善，数据中心虚拟化环境中的数据资产日益增多，数据流动日益频繁，因此需要加强对数据中心虚拟化环境中的数据安全管理。同时，随着数据安全需求的日益复杂，分局在数据安全运营智能化方面存在明显的提升空间，需要引入智能算法等技术，对数据安全事件进行准确的语义理解、智能降噪、智能分析，提高数据安全运营的效率和准确性。

**1.2项目目标**

通过本项目建设，逐步构建一套完善、高效的数据管理与安全运营体系，健全和完善数据资产发现、数据流转、自动化处置和数据安全运营管理的核心能力。实现虚拟化环境中各类数据资产的自动化、全面扫描与精准识别，形成详实的资产清单，并建立起实时管理机制，确保资产信息的准确性和完整性，为开展深度数据治理提供坚实基础。对虚拟化环境中API资产的访问和东西向流量进行全面管理，深入挖掘影子API资产，清晰描绘数据流转的依赖图和访问路径，对数据库攻击、API脆弱性等安全风险进行提醒。引入先进的智能技术，对数据安全态势感知平台进行升级，提升平台的智能化水平。通过自然语言交互、异常行为检测、GJ分析、报告生成以及知识库等功能的强化，实现数据安全态势的智能感知、快速响应和精准处理，为分局的数据安全提供有力保障。

**1.3主要建设内容**

本项目内容包括：

**1.3.1 虚拟化环境中数据资产扫描发现和识别能力**

对虚拟化环境中的数据库服务、文件服务、消息中间件等类型的数据资产进行自动化扫描和识别。对扫描到的数据资产进行识别，提取关键信息；为数据资产添加标签，便于数据的快速定位和分类管理。

与长宁分局数据态势感知两级平台进行对接，能够将采集信息报送至数据态势感知两级平台，供其开展分析和展现；能够与分局数据态势感知平台两级平台进行联动，接收和执行平台下发的管理指令和策略。

**1.3.2 虚拟化环境数据流转管理能力**

对虚拟化环境中API资产的访问和东西向流量进行管理，形成API资产清单。能够基于东西向流量测绘API服务的依赖图和访问路径；能够基于东西向流量，对数据流转（数据库、文件、消息、API）关系和路径进行测绘，能够管理数据库攻击、API脆弱性等传输行为。

对扫描到的API资产进行识别，提取关键信息；为API资产添加标签，便于数据的快速定位和分类管理。

与长宁分局数据态势感知两级平台进行对接，能够将采集信息报送至数据态势感知两级平台，供其开展分析和展现；能够与分局数据态势感知平台两级平台进行联动，接收和执行平台下发的管理指令和策略。

**1.3.3 数据访问控制能力**

部署数据访问控制系统，提供数据访问权限申请审批功能，面向访问数据库的用户，为不具备权限的用户提供权限的申请和审批；能够对高危操作、数据泄漏、数据导出、注入攻击、越权访问等行为作出GJ和阻断处理，并且能够对数据库访问进行细粒度的访问控制，以及对特殊数据进行处理。

**1.3.4 提升数据安全运营能力**

为进一步提升数据安全运营能力和效能，提升数据安全态势感知平台的智能化水平，对分局数据安全态势感知平台进行升级，通过引入智能技术，提升平台的智能交互、异常行为检测、GJ分析、报告生成、知识库等方面的功能。

**二、项目要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **系统** | **模块** | **子模块** | **功能要求** |
| 软件系统 | 数据扫描 | 消息总线发现模块 | 主动发送探测包，在网络中主动探测并识别Kafka等消息总线资产信息。 |
| 云存储发现模块 | 主动发送探测包，在网络中主动探测并识别云存储、对象存储等消息总线资产信息。 |
| 消息SM检测模块 | 提供消息总线连接器，可以在获得授权后连接消息总线进行消息读取，能够读取消息头、消息键、消息值、时间戳；能够解析字符串、Avro、JSON等格式的消息内容，并基于关键字、字典和规则匹配方式识别MG特殊信息，对消息数据进行标签化。 |
| 云存储SM检测模块 | 提供云存储服务连接器，可以在获得授权后连接云存储服务，能够读取云存储中的各类文件，对文件中的文本数据进行内容识别，包括文件名、文件属性、文件哈希值、文本内容。能够基于关键字、字典和规则匹配方式识别MG特殊信息，对消息数据进行标签化。 |
| 云数据资产漏洞检测模块 | 能够扫描云服务器上的所有数据资产漏洞，包括文件系统、数据库、消息总线、应用程序等。系统能够自动检测开放端口、错误配置和已知漏洞，并生成详细的漏洞报告。 |
| 开放接口模块 | 系统提供API、Syslog、SNMP开放接口，能够基于南北向接口向第三方系统报送日志、资产、风险等信息。 |
| 数据流转JC | 云网流量采集模块 | 系统支持SDN引流和云主机轻代理Agent方式采集云网流量。采用高性能的数据采集和分析技术，实时JT云主机上网卡的网络流量，捕获进出的数据包，并支持对捕获的数据包进行解析，提取关键信息，如源/目的IP、端口号、协议类型等信息。 |
| 云网流量可视化模块 | 能够构建云内数据流转的详细图谱，还支持对捕获的网络流量进行统计分析，包括总流量、各协议类型的流量分布、特定IP或端口的流量情况等。通过可视化技术，直观展示云网络流量的空间分布、流动情况、异常状态等信息。 |
| 流转风险JC模块 | 实现对云网数据流转的全面JK和风险识别。对数据在流转过程中的安全威胁和潜在风险，包括但不限于数据泄露、非法访问、篡改等，维护云网环境的稳定和安全。系统基于预设的安全基线和异常行为特征模型，对数据流转过程中的风险进行实时感知和YJ。一旦发现异常或潜在风险，立即向相关人员发送GJ信息。 |
| 数据泄漏溯源模块 | 通过内存插桩技术，不需要SSL证书也可以获得HTTPS接口服务的请求数据和响应数据，包括请求的URL、请求头、请求体以及响应状态码、响应头、响应体等，能够检测SM数据的流转情况和流转路径，在发现异常操作或潜在的数据泄漏风险时，能够实时进行响应，阻断恶意行为，防止数据进一步泄漏。在事后，能够SM数据流转提供溯源支持。 |
| 开放接口模块 | 系统提供API、Syslog、SNMP开放接口，能够基于南北向接口向第三方系统报送日志、资产、风险等信息。 |
| 数据访问控制 | 报文处理模块 | 通过DFI和DPI技术对数据包进行处理，包括验证IP地址是否有效、端口号是否在允许范围内等，以确保报文的合法性和正确性。 |
| 解析模块 | 对输入的SQL语句进行结构上的分析和理解。通过解析SQL语句，将SQL语句分解为一个个的词法单元（Token），包括关键字、标识符、操作符、字段值等。通过识别选择列表、表名、连接条件、过滤条件等，匹配访问控制规则。 |
| 访问控制模块 | 基于用户账号通过数据权限管理系统的鉴权服务来检查执行该语句的用户是否具有相应的权限，以及是否具有访问表、字段的权限。 |
| 风险检测模块 | 在用户访问数据库过程中会进行持续的风险检测，包括SQL注入攻击、高危命令、特定SQL函数、机器访问行为、SQL长度异常、返回行数过多、口令暴破、恶意文件上传、缓冲区溢出、数据拖库、特殊数据未处理等异常行为。 |
| 数据TM模块 | 在数据库访问过程中，能够对MM数据进行实时TM处理。在不影响原始数据的前提下，系统根据用户角色、权限、分类分级等条件，对查询结果中的MM数据进行遮蔽、替换或变形，以保护数据隐私和安全。 |
|
| 数据源管理模块 | 支持对数据源进行添加、删除、修改、命名管理；提供数据源列表展现，可以按照数据源的类型进行分类过滤和展现；提供数据源的查询功能，可以按照数据源的类型、IP地址、名称等信息进行查询。 |
| 阻断GJ模块 | 检测到异常或风险行为时，支持会话阻断，可准确定位和记录风险来源并阻断会话请求。 |
| 数据授权模块 | 系统支持精细化灵活的权限管控，可根据不同用户设置不同级别的数据访问权限，权限控制可配置到数据库、数据表、字段级、DDL/DCL/DML，实现对数据的安全防护。 |
|
| 权限审批模块 | 面向访问数据库的用户，为不具备权限的用户提供权限的申请和审批。用户可以通过系统提交权限申请，明确说明所需的权限范围、目的和有效期等关键信息。权限申请提交后，将触发审批流程，按照审批规则进行流转。权限申请获得批准后，系统支持自动和手动方式为用户分配相应的权限。 |
|
| 开放接口模块 | 系统提供API、Syslog、SNMP开放接口，能够基于南北向接口向第三方系统报送日志、资产、风险等信息。 |
| 数据安全运营 | 智能技术引擎模块 | 引入智能技术，为公安数据安全态势感知和数据安全运营提供赋能支持和提升。 |
| 智能知识管理模块 | 面向公安数据安全领域构建知识库，并提供知识库的全面管理、维护功能。并可以基于知识创建和管理智能应用。 |
|
| 智能应用管理模块 | 提供智能应用的创建、配置、发布、管理等功能。 |
| 智能知识问答模块 | 结合智能技术引擎的能力，将知识导入系统后，设定的应用将形成基于有关知识的业务知识库，可直接根据知识库中的内容对用户问题进行解答。 |
| 智能训练服务 | 提供数据训练和模型调优人工技术服务。 |
| 密码应用改造 | 密码应用改造 | 按照商用密码应用改造。 |
| 硬件系统 | API探针 |  | 2U机架设备；CPU≥16核，内存≥64G，硬盘容量≥8T，网络接口≥6个千兆电口+4个万兆光口，支持扩展；冗余电源。三年软硬件质保。提供流量采集解析、API资产管理、API资产识别、特殊数据检测、API风险探测、统计报表、日志审计、南北向接口功能模块。 |
| 智能 GPU服务器 |  | CPU：Kunpeng920 5220（48C,2.6GHz）\*2以上；NPU：至少 Atlas 300i Duo 48G\*8)；内存：DDR4 2933MHz 32GB \*8及以上；系统盘：SATA SSD 256GB（Raid1）\*2及以上；数据盘：SATA SSD 3.8TB（单盘Raid0）\*10及以上；冗余电源； |

**三、服务要求**

如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

保密期限由保密内容提供方确定，保密期限届满后，保密内容公开时，应书面征得保密内容提供方同意。

甲方委托开发软件的知识产权归甲方所有。乙方向甲方交付使用的信息系统已享有知识产权的，甲方可在合同文件明确的范围内自主使用。信息系统中所有文档资料和数据、收集和储存的个人信息所有权均属于甲方，未经甲方允许不得访问、修改、披露、利用、转让、销毁。

**四、其他要求**

**4.1项目验收**

4.1.1本项目实施期限为合同签订之日起3个月，开发根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的10个工作日内，确定具体日期，由双方按照合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，第三方验收费用全部由甲方承担，对此乙方应当配合。

4.1.2如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

4.1.3甲方根据合同的规定对服务验收合格后，签署验收意见。

**4.2售后服务与质保要求**

供应商应针对本项目提供所供货硬件设备、软件系统的原厂售后服务，质保期为三年（自项目验收之日起）；

在系统运行维护阶段，供应商应提供应用平台和应用软件的升级更新服务；

质保期内，供应商应提供定期的巡检维护技术服务，如每季度巡检一次。巡检中发现系统运行问题或潜在问题，应及时向用户报告，提出解决方案和措施建议，并与用户协商解决。

供应商应制定应急恢复方案，并在出现应用系统宕机、应用程序无法访问等紧急状况时，立即响应，快速分析问题和解决问题。

当故障涉及到多方设备，用户无法进行准确故障定位时，供应商应立即响应，协助用户进行准确的故障定位。

一级故障（重大故障）：系统瘫痪或服务中断时，供应商应在15分钟内响应，并在1小时内抵达现场，4小时内解决故障。

二级故障（主要故障）：影响服务性能时，供应商应在20分钟内响应，并在2小时内抵达现场，4小时内解决故障。

三级故障（次要故障）：其他障碍时，供应商应在0.5小时内响应，并在2小时内抵达现场，4小时内解决故障。

**五、人员要求**

本项目实施团队人员应配备充足、合理且职责分工明确、架构清晰合理。

管理人员应至少配备1名项目经理，且项目经理应满足以下要求：

1. 本科及以上学历，提供学历或学位证书；
2. 近3年在供应商单位的工作经验，提供社保证明或劳动合同证明材料；
3. 持有PMP证书且有丰富的数据安全、网络安全类技术能力、实施经验。

项目团队（除项目经理外）应配备技术负责人（不可以同时为项目经理）、技术实施人员、运维保障人员且应满足以下要求：

1. 项目团队人员不少于5人；
2. 项目团队人员应持有本科及以上学历，计算机、电子信息、软件工程、网络与信息安全相关专业，提供学历或学位证书；
3. 项目团队人员应拥有近2年在供应商单位的工作经验，提供社保证明或劳动合同证明材料；
4. 项目团队人员应同时持有CISP、CDSP证书且具有2年以上网络安全、数据安全相关工作经验。

**六、服务期限**

**1、服务期限：**合同签订后3个月完成。

**2、服务地点：**上海市公安局长宁分局

**七、付款及验收方式**

1、付款方式：

合同签订后，支付135,200.00元作为项目预付款，乙方完成全部工作，并验收合格后，招标方支付至合同价的50%。审计全部完成后支付剩余合同款。

付款条件备注：服务提供方应当在采购方每次付款前提前至少10个工作日向采购方提供有效发票。

对于满足合同约定支付条件的，采购人原则上应当自收到发票后10个工作日内将资金支付到合同约定的供应商账户，鼓励采购人完善内部流程，自收到发票后1个工作日内完成资金支付事宜。采购人和供应商对资金支付产生争议的，应当按照法律规定和合同约定及时解决，保证资金支付效率。

2、验收方式：采购人自行验收。

**十、投标单位资质要求（详见本项目招标公告）：**

1、供应商应当符合《中华人民共和国政府采购法》第22条所规定的条件；

2、供应商及其投标的产品和服务符合国家法律法规及强制性规范所规定的条件；

3、供应商在本市有完善的服务体系，能够提供良好的技术与服务支持；

4、本项目不接受联合体投标；