项目采购需求

一、说明

1 总则

1.1 供应商应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由供应商自行负责。

1.2 供应商提供的货物和服务应当符合磋商文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

1.3 供应商在磋商前应认真了解项目的实施背景、应提供的服务内容和质量、项目考核管理要求等，一旦成交，应按照磋商文件和合同规定的要求提供相关服务。

1.4 供应商对所提供的货物和服务应当享有合法的所有权，没有侵犯任何第三方的知识产权、商业秘密、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。如采购人使用该服务构成上述侵权的，则由成交供应商承担全部责任。

1.5 响应供应商认为磋商文件（包括磋商补充文件）存在排他性或歧视性条款，自收到磋商文件之日或者磋商文件公告期限届满之日起七个工作日内，以书面形式提出，并附相关证据。

二、项目概况

2 项目基本情况

2.1 项目名称：网络安全基础服务

2.2 项目磋商概况：1.资产脆弱性管理服务，包含日志汇聚分析服务、漏洞管理服务、渗透测试服务、软件成分分析服务、安全监督检查服务、源代码安全审计； 2.常态化运营服务，包含重要节点安保值守、应急响应处置服务、应急演练； 3. 内网安全专项运营服务，包含政务外网流量威胁感知分析服务、网络准入服务； 4.互联网安全专项运营服务，包含网站安全实时监测服务、API 安全监测服务。

2.3 本项目服务期限：1年

3 承包要求

3.1 本项目不允许分包。

4 合同签订方式

4.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与磋商文件和成交供应商响应文件的内容一致，并互相补充和解释。

三、工作内容

5 项目总体要求

5.1 安全防护服务的过程中涉及的所有数据的拥有权及使用权均属于采购人，未经许可，响应供应商无权对其进行支配，所有与数据相关设备的维修、报废等处理需经采购人同意，并在监管下进行。若发现响应供应商未经许可对数据进行支配，采购人将对响应供应商采取惩罚措施并追究其法律责任。

5.2 响应供应商为服务本项目而采购的场地、环境、链路等硬件资源及各类软件资源，构成专门为采购人提供安全防护服务的设施资源，其拥有权属于成交供应商，使用权和产生的数据归属权属于采购人。

5.3 响应供应商在响应前应认真了解项目的实施背景、应提供的服务内容和质量、项目考核管理要求等，一旦成交，应按照采购文件和合同规定的要求提供相关服务。

5.4 响应供应商严格执行国家、地方、行业各项有关本项目的法律法规、制度和国家强制性标准，积极主动加强和服务业务及安全等有关的管理工作，并按规定承担相应的费用。响应供应商因违反规定等原因造成的一切损失和责任由响应供应商承担。

5.5 响应供应商确认的项目运营服务团队人员及数量，应与响应文件承诺一致，未经采购人书面批准不得随意调换或撤离，若自行更换或撤离，按照合同违约处理。

5.6 响应供应商明确安全防护安全管理方案，承担运营过程中环境安全、人员安全、信息安全、数据合规使用等相关各类安全责任。

5.7 响应供应商保证本项目所涉及的软件授权足量合规，满足知识产权方面的有关规定和要求。

5.8 响应供应商服务时所配套的工具，需符合现有网络环境，不可影响、破坏现有安全架构体系。

5.9 响应供应商承诺参与本运营服务的所有服务人员需严格保守与本运营服务有关的技术秘密和商业秘密，任何涉及采购人及使用单位的信息，包括但不限于数据、特有的功能需求等，未得到采购人及使用单位的书面同意，不得对任何第三方展示、举例乃至销售，否则响应供应商将承担由此产生的一切后果。

5.10 本次项目需指定专职项目经理1 名，协调工具实施，安全服务等相关服务内容，定期汇报工作，优化服务流程。

5.11 响应供应商不以实施项目为名，侵害本项目各参与单位的技术、商业秘密或者知识产权。

5.12 本采购需求书仅作为响应供应商响应依据，未经采购人书面许可，不可转发第三方或随意传播。

5.13 响应供应商如为大型集团本地分公司/全资子公司，需提供与集团公司的关系证明，保障服务质量。

6 项目技术需求

6.1 日志汇聚分析服务

响应供应商应完成所有日志汇聚并提供不少于700台设备的全量日志（包含网络设备、服务器等）分析服务，每季度完成一次全量日志审计分析并输出日志分析报告。

提供不少于4套符合用户现场环境的专业设备软件用于日常全量日志分析，所用软硬件设备工具获得公安部计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具的产品检验报告。所提供的产品检验报告须符合《信息安全技术 日志分析产品安全技术要求 GA/T 911-2010》（第三级），并提供完整的检测报告复印件（行标三级）。日志分析工具需要支持 Syslog、SNMP Trap、HTTP、FTP、SFTP等协议日志收集；日志分析工具应支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等设备日志采集。日志分析工具应能设置日志存储备份策略，包括系统日志保存期（天）、磁盘使用率百分比等策略；支持日志本地备份及恢复；支持日志备份自动传送到远程服务器，日志至少保存 180 天。

需提供4次日志分析报告和1份日志接入清单等涉及本项目的所有文档。输出物包括但不限于：

输出物	输出物标准
日志分析报告	对采购人相关设备产生的日志进行全量分析
日志接入清单	对采购人汇聚接入的情况进行记录

6.2 漏洞管理服务

针对采购人指定的信息系统开展160次漏洞扫描服务，响应供应商应提供不少于 4 套采用具有自主知识产权的漏洞扫描工具对服务范围内各种软硬件设备进行网络层、系统层、数据库、应用层面的全面扫描与分析，扫描设备检测规则库及知识库应涵盖 CVE、CNCVE 、CNVD、 CNNVD 等标准。

扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提出准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案，协助用户进行处置，反　馈漏洞处置情况，实现漏洞闭环管理。

需提供160份漏洞扫描报告等文档。输出物包括但不限于：

输出物	输出物标准
漏洞扫描报告	对采购人的系统主机等资产进行定向扫描，对发现的风险点进行问题描述、问题分析，并提出建议处置方法。

6.3 渗透测试服务

针对采购人指定的信息系统采用模拟黑客的攻击方法，综合运用人工渗透测试、专业测试工具和人工智能自动化渗透测试能力，对系统和网络进行非破坏性质的渗透测试，服务期内为采购人指定的信息系统累计开展40 次渗透测试服务，以此来检验系统是否存在一些隐性的安全漏洞和风险，并及时提醒相关人员完善相应的安全策略。渗透测试可用于验证网络是否真实地达到了预定安全目标、遵循了相关安全策略、符合安全合规的要求。人工智能自动化渗透测试应与人工测试相结合，人工智能生成的测试任务及发现的安全问题须经专业渗透测试人员复核确认，响应供应商应对最终测试结果负责。

（1）响应供应商测试方案内容包括测试对象、测试人员、测试IP、测试日期安排、测试工具、测试手段、异常应对措施等。测试期间若测试IP 有变化，需立即向采购人报备。测试手段包括但不限于注入、认证欺骗、弱口令、文件上传、命令执行、反序列化、逆向、反编译、暴力破解等。

（2）响应供应商需在测试开始前告知采购人并获得允许后方能开展测试。在测试过程中应按照测试方案规定的测试时间、测试方法（如能否使用扫描工具）进行测试，若未经允许在非规定时间内开展测试而触发采购人安全警报，需立即向采购人进行情况说明。

（3）响应供应商应协助采购人完成漏洞的修复，提供漏洞修复后的复测验证直至漏洞被确认修复，对于远程和现场复测的漏洞均不限复测次数。

（4）响应供应商应配有自动化的渗透测试工具自动发现子域名。域名信息包括域名、DNS 解析（A 记录、CNAME 等）、网站信息、响应码。（提供证明材料）

（5）响应供应商应配合提供至少 1 套扫描工具，满足信息系统、办公系统、网站应用等系统的安全扫描。同时要兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准，并提供CNNVD 兼容证书。（提供证明材料）

（6）响应供应商需提供的工具应具备弱口令扫描功能，支持常见协议弱口令扫描，包括但不限于FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典。（提供证明材料）

（7）针对网站应用系统的扫描应不限制WEB 服务器类型，支持如IIS、Websphere、Weblogic、Apache、Tomcat、Tongweb、Resin、Jboss、Nginx 等。支持扫描Access，达梦，Mysql, ORACLE, DB2, PostgreSQL, Sybase, Informix, sqlite, MSSQL SERVER 不同类型的数据库。

（8）使用针对主机、网络层、WEB 应用的自主研发的工具提供初步扫描服务、并提供相应的软件著作权和销售许可证书。

（9）响应供应商应配置人工智能自动化渗透测试能力，并结合人工测试对结果进行复核。所有测试及漏洞验证应在采购人书面授权范围内开展，不得影响业务系统的连续性、稳定性和数据完整性。

需提供40份渗透测试报告等文档，输出物包括但不限于：

输出物	输出物标准
渗透测试报告	应提供包含详细渗透步骤、漏洞发现的方式、漏洞证明截图以及修复建议，对于难以复现的漏洞提供及时的技术支持。

6.4 软件成分分析服务

配套提供软件成分分析软件用于对软件项目完成成分分析，并为采购人指定的信息系统累计开展20 次软件成分分析服务，在合同期内及时升级与维护。

软件成分分析工具支持对源代码、二进制文件及特征文件中开源组件进行静态分析。通过算法、策略、模型对项目中引用的组件及漏洞进行高效深层分析。支持检测可执行二进制的编译选项PIE、RELRO、 Canaries、NX、Symbols，有效避免常见的各类内存破坏类漏洞带来的风险。

软件成分分析工具支持对jar，war，pom.xml，build.gradle，package.json，package-lock.json，yarn.lock，go.mod，conanfile.txt，conanfile.py，composer.json，composer.lock，requirements.txt，configure.ac，configure.in，packages.config，project.json，csproj，build.gradle.kts，Cargo.lock，Podfile.lock，.apk，build.sbt，META.json，rebar.lock，project.clj，DESCRIPTION，deps.edn，Gemfile.lock，CMakeLists.txt 等特征文件进行分析。

需提供20份软件成分分析报告等文档，输出物包括但不限于：

输出物	输出物标准
软件成分分析报告	应提供包含组件信息、组件风险等级及修复建议。

6.5 安全监督检查服务

响应供应商应协助采购人完成共计 5 次的安全监督检查工作，工作内容包括但不限于安全管理检查、安全建设检查、安全运营检查、安全监管检查等内容。需运用人员访谈、文档核查和技术检查等方式，准确发现安全隐患，并提供风险分析与整改建议。为采购人提供专业检查知识和检查方法，提高网络安全检查工作的标准化、规范化和专业化水平。

需提供5份检查报告等文档，输出物包括但不限于：

输出物	输出物标准
检查报告	应提供包含检查结果及优化建议。

6.6 重要节点安保值守服务

按照采购人需求提供重大活动、假期和会议等重要节点期间的7*24 小时的重保服务不少于4 次，通过重保安全服务，借助安全运营平台工具，建立重要节点安全保障期间的安全保障机制，建立重要节点安全保障期间的威胁感知和预警体系。

（1）能够实时了解保障期间的信息安全状况、对发现的威胁行为进行及时管控，把控整体信息安全防护保障措施。

（2）控制发生信息安全事件的影响范围和行为，能够及时进行响应与处置。

（3）提供重要时期的现场防控与应急响应团队与组织，完成以下服务内容：漏洞扫描服务、主机评估服务、设备租赁服务、安全值守服务、日志分析服务、应急响应服务等。

根据重保活动情况，每次重保的输出物包括但不限于：

输出物	输出物标准
安全重保实施方案	需在其中明确保障工作要求及流程机制、系统相关部门工作职责和内容和要求。经客户评审得到通过后方可生效。
安全重保期间值守工作报告	以日报形式，每日编制安全重保期间值守工作报告，汇报当天安全保障情况，包含当天总体情况、值班情况、安全防护情况等。报告格式需符合采购人的要求。
重保安全风险处置单（如有）	响应供应商需对所保障各业务系统的网络安全监测预警，及时发现告警，第一时间通报至保障领导小组，提交对应事件的网络安全事件通报，并收集处置结果。需产生总结的完整告警处理记录。
安全重保专项总结报告	需要记录保障期间工作实施情况，需要对整个重保期间所有检测到的安全事件以及告警进行统计。要求做到对中高级告警及时处理，并在报告中完整体现。

6.7 源代码安全审计服务

针对指定的5个系统，对采购人提交的源代码进行机器及人工联合审计，对审计出的风险点进行问题描述、问题分析，并提出建议处置方法，出具规范的代码审计报告。

（1）响应供应商应配备固定的代码审计人员团队，原则上不进行人员调整，因不可抗力因素导致的人员调整应经过采购人同意；响应供应商应根据采购人的相关要求明确审计时间、审计工具和审计方法；

（2）响应供应商应采用保密可控的、影响最小的和非破坏性的方法和手段对采购人的应用系统进行深入的代码审计；

（3）响应供应商应根据代码审计服务需求清单，在采购人指定地点开展代码审计工作，并出具审计报告、提出应用修复建议；

（4）在每次代码审计工作结束后，响应供应商均需清除本地测试机的源代码记录和检测结果报告，并提供修复漏洞的相关技术支持和免费复审服务。

（5）测试过程中若目标系统出现异常，须保证测试人员及时响应采购人的维护请求并及时赶赴现场解决问题。

需提供5份代码审计报告等。输出物包括但不限于：

输出物	输出物标准
代码审计报告	对采购人提交的源代码进行机器及人工联合审计，对审计出的风险点进行问题描述、问题分析，并提出建议处置方法

6.8 应急响应处置服务

在发生安全事件后，按照预防、情报信息收集、遏制、根除、恢复流程开展应急响应处理服务，帮助采购人快速响应和处理信息安全事件并从中恢复业务，协助采购人建设信息系统事件应急响应支撑服务体系，本次项目按照采购人需求提供专业团队开展 7x24 小时的应急响应支撑服务（包括7*24 小时远程在线支撑，现场应急支撑至少2 名专家1 小时内到达现场）；（提供承诺书）

（1）在系统出现恶意入侵、业务系统不可用、数据泄露等各类安全事件时，安全运维团队能在规定的安全应急时间内响应，对安全事件进行等级分析，并给出处置方案，事后对事件进行复盘，总结经验教训；

（2）当出现网络安全事件，造成系统无法正常对外提供服务时，安全运维团队应在服务要求中规定的安全应急响应时间内，派出应急响应专家协助完成包括但不限于：系统安全恢复，应用服务安全恢复，数据安全恢复，网络性能安全恢复，网络病毒灾难恢复等在内的灾难恢复工作；

（3）在系统出现各类型安全事件后，安全运维团队负责对安全事件进行分析，开展安全事件入侵追踪和取证、犯罪取证、事后安全分析和处置服务，并定期针对安全事件加强安全教育培训。

（4）应提供自主研发的应急处置工具箱用以支撑响应工作进行，支持主动扫描、被动扫描两种模式的深度扫描，支持多域名批量扫描；（要求提供截图）

根据应急响应情况，每次应急响应的输出物包括但不限于：

输出物	输出物标准
应急响应报告	针对发生的信息安全事件，开展处置、恢复等工作，出具相应的报告，描述事件的溯源、处置、改进建议等。

6.9 应急演练服务

参考 GB/T 38645-2020《信息安全技术 网络安全事件应急演练指南》、GB/T 20986-2023 《信息安全技术 网络安全事件分类分级指南》要求，根据采购人要求在有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件类型中选取场景开展1 次应急演练工作。

需提供应急演练文档等涉及本项目的所有文档。输出物包括但不限于：

输出物	输出物标准
演练方案	根据采购人制定合理的演练方案，对演练各个环节需要制定相关明细。

6.10 政务外网流量威胁感知分析服务

配套提供基于流量检测设备和日志分析能力的态势感知分析软件平台，并提供专业的流量收集探针等软硬件设备。完成采购人为期 1 年的全覆盖感知与分析政务外网流量威胁服务，提供1 年免费及时升级与维护服务，同时提供5*8 高级威胁技术分析服务。

流量威胁感知分析工具服务需支持双向全流量检测审计，能支持对请求和响应内容进行审计，支持IPv4 和IPv6 网络环境下的部署，可同时对IPv4 和IPv6 网络流量分析检测。对于风险数据包提供保存和数据包去重功能， 自动剔除重复数据包、存留会话的请求和相应风险数据包，帮助用户还原攻击过程，进行取证和关联分析；并支持系统内置wireshark 组件对数据包在线预览。

流量威胁感知分析工具应解析 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、 SMTPS、POP3S、IMAPS、KRB5、SNMP、NETFLOW V9、TFTP 等协议报文（HTTPS、 SMTPS、POP3S 、IMAPS 加密协议解析需要导入服务器私钥证书）；支持 COAP 、MQTT 等物联网协议解析和审计；支持识别 QQ、WEB、LDAP、FTP、TELNET、邮件、SMB、RADMIN、ORACLE、MSSQL、 SYBASE 、MYSQL 、DB2 、PostgreSQL 、REDIS 、MQTT 等登录行为；

流量威胁感知分析工具应支持 HTTP、SMB、SMTP、IMAP、POP3、FTP、TELNET、RADMIN、 SSH、 RDP、 ORACLE、 MSSQL、 SYBASE、 MYSQL、 DB2、 PostgreSQL、LDAP、 MQTT 等协议的暴力破解，能识别出登录次数、账户信息、爆破成功与否的攻击状态。同时支持 IP 、端口、SMB 、Radmin 、ICMP 、ARP 、传输层协议和漏洞扫描行为检测。支持 UDP FLOOD 、DNS FLOOD 、NTP FLOOD 、Chargen FLOOD 、SNMP FLOOD 、SSDP FLOOD、Memcached FLOOD、SYN FLOOD、RST FLOOD、FIN FLOOD、ACK FLOOD、HTTP FLOOD、 ICMP FLOOD 、SEANET_FLOOD 检测。支持以上行为模型的启用/禁用，并支持自定义配置模型的相关参数；

流量威胁感知分析工具应支持详细展现风险等级、时间、威胁名称、攻击状态、攻击方向、客户端 IP 、客户端 IP 所在地理位置、服务端 IP 、服务端 IP 所在地理位置、端口、报文、操作等信息，包含请求 URL 、请求类型、请求内容、请求头、Host 、User-Agent 、Accept、Accept-Language 、Accept-Encoding、Accept-Charset 、Keep-Alive 、Connection 、Cookie 、请求参数、响应码、返回长度、ATT&CK 矩阵等信息，并提供相应的数据包下载链接。

针对流量中的个人敏感信息进行识别分析，包括身份证、银行卡、手机号、港澳通行证等，并展示传输信息的协议、网站域名、URL 、客户端 IP 、服务端 IP ，便于用户发现敏感信息的传输安全隐患和处置。

根据政务外网流量威胁和感知分析情况，输出物包括但不限于：

输出物	输出物标准
流量威胁和感知分析月报	需在其中汇总当月流量威胁情况、研判分析情况，并视情况提出安全建议。
流量威胁和感知分析报告（如有）	出现真实攻击时需对事件情况、研判分析结论进行描述，并提出安全处置建议

6.11 网络准入服务

响应供应商应提供专业网络准入服务工具，为采购人完成不少于 500 个网络终端节点的政务网接入准入部署及定期检查服务，实时采集终端、设备、IP、MAC 等各类网络信息，实时掌握各社区居委网络接入情况；支持对接入网络的摄像头、打印机、瘦客户端、 自助终端、扫描枪、手持终端、探测器、视频会议设备、门禁控制器等基于 IP 的所有设备进行识别，发现信息包含接入状态、设备名称、设备 IP 地址、MAC 地址、设备类型、设备品牌、用户名称、部门名称、接入交换机、接入端口、接入位置等，并可对设备进行注册管理。

网络准入控制：根据用户或设备的身份和权限，限制其访问网络资源的范围和权限。支持对接入设备指定相应的绑定规则，根据接入设备是否符合接入规则来决定允许或拒绝其接入，防止仿冒终端接入，如基于计算机 IP/MAC、交换机端口、接入控制点设备等进行灵活绑定。

根据网络准入情况，输出物包括但不限于：

输出物	输出物标准
网络准入接入清单	需在其中汇总当前已经接入政务网的设备清单。

6.12网站安全实时监测服务

要求无需本地部署任何软设备，通过云端专业实时监测平台，完成为期1年的网站安全实时监测服务，监控对象按照采购人要求动态更新，监控内容包含漏洞、弱口令、安全事件、内容监测、站点断网等，网站监测能力不少于40个，不多于100个。（提供功能截图证明）

平台提供脆弱性监测服务，对网站存在的脆弱性进行探查，包括SQL注入漏洞、跨站脚本漏洞、开放服务漏洞、网站第三方应用漏洞0day漏洞等。（提供功能截图证明）

平台应具备针对广泛使用的开发框架或者中间件的0day漏洞发现能力，包含struts2、主流PHP环境、常见CMS等国际广泛使用的开发框架。（提供证明材料）

针对安全事件提供监测服务，支持黑链、黑页、webshell、网页挂马、JS挖矿脚本、图片篡改等安全事件的监测和查询，并进行专家审核。（提供功能截图证明）。

针对网站内容提供监测服务，支持对政治、反动、不文明用语、暴恐类、低质灌水等敏感内容进行检测，支持敏感内容自定义；支持错别字监测，支持错别字自定义设置。（以上均提供证明材料）。

针对站点断网情况提供推送服务，支持对断网时间、断网原因、当次断网持续时长、当前状态、恢复时间等情况进行监测并推送至相关人员（以上均提供证明材料）。

配套提供7x24小时的安全专家值守与分析服务，实时发现各类安全威胁，并对安全问题进行审核、验证和告警，第一时间安全告警通知。（提供值守专用电话和值班场地实景照片），同时每月应及时提交月度报告。

为保障服务稳定性与专业性，工具厂商在全国范围内具备至少10个云监测节点（提供证明）。

根据网站安全实时监测情况，输出物包括但不限于：

输出物	输出物标准
网站安全监测月报	需在其中汇总本月监测发现的断网事件、安全漏洞、安全事件等相关信息。

6.13API安全监测服务

响应供应商应提供不少于2套专业API安全监测工具，完成为期1年不少于30个互联网应用系统的API数据接口风险监测服务。通过对流量解析还原和敏感数据识别打标，帮助采购人自动识别梳理API以及业务系统用户，可自动检测API上存在的脆弱性，防止发生机密数据因API自身脆弱性造成的数据泄漏事件产生，并且系统可对各种违规使用数据行为进行监控告警，防止核心数据以违反安全策略规定的方式流出。

所使用工具支持根据策略自动识别划分静态资源页面和数据共享API，支持可视化多指标组合配置划分规则，配置指标维度包括：URL、请求用户代理、请求方法、响应内容类型、请求头、响应头、响应码、请求体、响应体。

同时工具可自动识别文件中包含的敏感数据标签。支持识别文件类型包括：doc、pdf、docx、xls、xlsx、ppt、zip、rar、tar、gz、7z、docm、pptm、xltm、xlsb、bz2、gzip、wps、txt、html、xml、csv、json。

支持监测API的生命周期变化，并可通过可视化方式修改生命周期的打标周期。并且能够对API生命周期、返回类型、数据特征分布等维度进行统计分析。

支持以IP、账号、IP+API、账号+API、数据维度进行行为风险配置。支持通过多种指标组合自定义配置新增风险策略，例如：请求数据标签、返回数据标签、下载文件、上传文件、访问频次、登录账号数、账号密码去重数、手机号验证码去重数、操作时间等。支持以滑动窗口计数方式匹配监测规则。

根据API 安全监测情况，输出物包括但不限于：

输出物	输出物标准
API 安全监测月报	需在其中汇总本月监测发现的资产情况、安全事件、安全漏洞等相关信息。

7 运营服务管理要求

7.1 运营服务要求

响应供应商向采购人提供响应文件中采购的所有内容的培训和维护服务，提供安全防护资源租赁服务，并负责安全防护服务所需要涉及的工具安装、软件集成、运维管理工作。若采购文件中所采购的服务等方面的配置或要求中出现不合理或不完整的问题时，响应供应商有责任和义务在响应文件中提出补充修改方案并征得本项目单位同意后付诸实施，所产生的费用由响应供应商负责。响应供应商需按照服务质量保证的服务标准和要求提供各种售后服务，负责对其提供的服务进行维护或升级。

服务过程中使用的相关工具设备，需按采购人需求足量提供。

为保证服务响应效率，应对突发事件，供应商需保障相关人员及时到位处理相关风险，并承诺出现重大突发事件后，15 分钟内响应，30 分钟内可到达客户现场。

响应供应商应根据不同的安全防护服务任务的范围和要求，提出相应运营服务方案，包括但不仅限于处理流程、响应时间、管理体制、维护人员和工具配备等。响应供应商需按照方案中的事项安排相关团队制定详细的作业计划并执行。

未经许可不允许使用大规模自动化扫描工具及渗透工具，禁止上传木马、执行高危payload 等影响系统运行的操作。

在系统频繁出现故障或遇重大节假日等保障，需要提高系统维护等级的情况下，响应供应商应提供技术人员提供现场技术支持，及时处理各类故障。以上工作所产生的费用都由响应供应商承担。

7.2 服务团队要求

响应供应商应为本项目单独建立管理组织，配置相应团队，同时提供至少2 名5*8 现场常态化安全驻场服务人员，现场管理服务工具及支撑采购人开展其他安全相关工作。

所有服务人员均需提供资质证明、简历以及在职证明，服务人员必须满足以下要求：

（1）供应商应组建8 人以上的专业安全服务团队。且须具备相关工作经验，能满足项目所需要求，具有本科以上学历优先。

（2）项目经理须满足10 年以上信息安全服务工作经验，具备中国信息安全测评中心认证的注册信息安全专业人员（CISP）证书及中国网络安全审查认证和市场监管大数据中心认证的信息安全保障人员（CISAW）证书，并提供证书复印件。

具备10 个信息安全服务项目经验（需提供证明）。

（3）项目参与成员应熟悉行业安全规范、安全技术标准及常见的安全漏洞，熟悉各类常见安全缺陷的代码及解决方案。

（4）供应商在成交后应遵照采购人相关管理要求，履行对进场服务的驻点管理责任。落实现场服务商签订《保密承诺协议》等协议及工作规范，确保进场的驻点人员知情、认可采购人的各项管理流程制度及工作规范，并在服务过程中严格遵守。

（5）在采购人的驻场办公地点工作期间需遵守采购人的出入管理、行为规范、安全管理、出勤管理等相关规定。响应供应商需实施定期考核评估工作。若驻点人员违密义务、工作规范或有其他重大违规行为而被要求退场的，则不得再次使用。若因能力上不符合要求，而被要求退场的驻点则两年内不再使用。

8 知识产权承诺

本项目中形成的知识产权（包含需求分析、系统设计、软件程序、核心技术、数据标准、接口规范、知识库、专有方法、模板、培训材料、专有数据、技术文档、服务模式、运作模式等，但不限于上述形式）归采购人所有。响应供应商向采购人交付的信息系统已享有知识产权的，采购人在许可范围内合理使用。

本项目中形成的知识产权的申请权、所有权与利益（包括：专利权、商标权、著作权、商业秘密专有权等，但不限于上述权益的申请权）归采购人所有。未经采购人书面同意，响应供应商及其合作履约方不得以任何形式自行申请。

响应供应商不得以任何形式侵害本项目中形成的知识产权。未经采购人书面同意，响应供应商不得以任何形式提供或出售给其他单位使用。若发生侵害行为，响应供应商则全额赔付采购人本项目成交金额以及响应供应商通过侵害行为获得的全部收益。

没有采购人明示的书面同意，响应供应商不能作出关于本项目或者其条款的任何新闻公告、媒体宣传或其他形式的公开披露。

响应供应商提供的产品和服务等不得侵犯任何第三方的知识产权。若发生侵权行为，一切法律责任、后果及损失均由响应供应商承担，采购人不承担任何法律责任及后果，且保留追责权。