合同编号：

# 市委网信办2026年网络安全运维保障项目

# 合　同

项 目 编 号：DQA-2026005-CS

甲　　方：中共咸阳市委网络安全和信息化委员会办公室

乙　　方：咸阳秦云信息技术有限公司

甲方（采购人）：中共咸阳市委网络安全和信息化委员会办公室

乙方（供应商）：咸阳秦云信息技术有限公司

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定，按照平等、自愿、公平和诚实信用的原则，经甲方和乙方协商一致，约定以下合同条款，以兹共同遵守、全面履行。

## 一、甲乙双方信息

1．甲方信息：

单位名称：中共咸阳市委网络安全和信息化委员会办公室

统一社会信用代码：11610400MB29977130

开户行：建行咸阳渭阳路支行

账号：61050163520808190703

地址：陕西省咸阳市秦都区中韩产业园 A 区 103 号楼

电话：029-33210562

2．乙方信息：

咸阳秦云信息技术有限公司

开票信息如下

公司名称：咸阳秦云信息技术有限公司

地址：陕西省咸阳市秦都区渭阳西路北侧创业大厦 1 幢 4-08 室

电话：029-33260066

开户银行：陕西咸阳农村商业银行股份有限公司秦都支行

账　　号：270401010120100008516l

联 行 号：402795000025

**二、服务内容：**

运维服务内容详见附件 1

**三、运维服务期：**

服务期限一年（具体服务时间：自 2026 年 3 月 25 日起至 2027 年 3 月 24 日止）

**四、运维服务地点：**

中共咸阳市委网络安全和信息化委员会办公室。

**五、本合同总价为：**

人民币：1895000.00 元整（大写：壹佰捌拾玖万伍仟元整）

**六、付款方式和发票开具方式**

1．合同签订之日起 7 个工作日内，乙方向甲方提供合同总价款的 60%费用增值税发票，甲方见票后向乙方支付相应费用；

2．服务期满 6 个月后，并进行初步服务质量评估，合格后，乙方在 7 个工作日内向甲方提供合同总价款的 30%费用发票，甲方见票后向乙方支付相应费用；

3．最终服务期限前 1 个月由甲方进行最终服务质量评估，合格后，乙方在 7 个工作日内向甲方提供合同总价款的 10%费用发票，甲方见票后向供乙方支付相应费用。

4．乙方在甲方办理以上各期付款的支付手续前，向甲方出具等额的符合国家规定的发票。

5．所有款项应付至乙方以下账户：

单位名称：咸阳秦云信息技术有限公司

开户行:陕西咸阳秦都农村商业银行股份有限公司

账号:27040101012010000085161

## 七、运维服务要求

1．高效响应机制

7×24 小时全天候响应：设立专属服务热线与在线客服渠道，无论工作日、 节假日或凌晨时段，贵单位任何服务需求或系统故障反馈，我司将在 15 分钟内 做出响应，明确告知问题处理流程与预计解决时限。

分级故障处理：根据故障对贵单位业务影响程度划分等级，一般故障 2 小时 内解决，严重故障 1 小时内到达现场并启动应急方案，重大故障 30 分钟内组织 技术专家团队开展排查，确保最短时间内

恢复系统正常运行。

2. 专业服务团队

专属服务小组：为贵单位配置由项目经理、技术工程师、安全运维专员组成 的专属服务团队，团队成员均具备 3 年以上信息化系统运维与网络安全服务经验。

定期技能提升：每月组织服务团队开展 2 次的技术培训与案例研讨，内容涵 盖最新网络安全威胁态势、信息化系统运维优化方案、贵单位定制化系统功能升 级等，确保团队技术能力始终适配贵单位业务发展需求。

3. 数据安全保障

加密防护措施：对贵单位所有涉及敏感数据的传输、存储环节采用 AES-256 位加密技术，严格管控数据访问权限，建立“一人一权限、操作留痕迹”的访问审计机制，每季度出具数据安全审计报告。

4. 服务质量监督

月度服务报告：每月 5 日前向贵单位提交上月服务明细报告，内容包括故障 处理记录、系统性能优化建议、安全漏洞排查结果等，接受贵单位对服务响应速 度、问题解决效率、服务态度等方面的评价与监督。

满意度调查：每季度开展一次服务满意度问卷调查，针对贵单位提出的意见 与建议，在 3 个工作日内制定整改方案并反馈，确保服务质量持续提升。

## 八、项目验收

1．项目验收由甲方或其委托的专家或第三方机构对项目进行验收，验收时，乙方应无条件予以配合并提供所需的全部资料；

2．验收依据：磋商文件、磋商响应文件、合同文本、国内相应的标准、规范。

## 九、知识产权

乙方应保证其提供的服务不受任何第三方提出的侵犯其著作权、商标权、专利权等知识产权方面的起诉；如果任何第三方提出侵权指控，那么乙方须与该第三方交涉并承担由此发生的一切责任、费用和赔偿。

## 十、违约责任

1．除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式履行，那么甲方可要求乙方支付违约金，违约金按每迟延履行一日的应提供而未提供服务价格的0.5%计算，最高限额为本合同总价的5%;迟延履行的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；

2．除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，那么乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的0.5%计算，最高限额为本合同总价的5%;迟延付款的违

约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同；

## 十一、质量保证

1．乙方应建立和完善履行合同的内部质量保证体系，并提供相关内部规章制度给甲方，以便甲方进行监督检查；

2．乙方应保证履行合同的人员数量和素质、软件和硬件设备的配置、场地、环境和设施等满足全面履行合同的要求，并应接受甲方的监督检查。

## 十二、延迟履行

在合同履行过程中，如果乙方遇到不能按时提供服务的情况，应及时以书面形式将不能按时提供服务的理由、预期延误时间通知甲方；甲方收到乙方通知后，认为其理由正当的，可以书面形式酌情同意乙方可以延长履行的具体时间。

## 十三、转让

未经甲方事先书面同意，乙方不得部分转让或全部转让其应履行的合同义务。

## 十四、乙方履约延误

1．乙方应在规定的服务期内提供服务。

2．在履行合同过程中，如果乙方遇到妨碍提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的时间和原因通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意，以及是否收取误期赔偿费。延期应通过修改合同的方式由双方认可。

## 十五、合同中止、终止

1．甲乙双方不得擅自中止或者终止合同；

2．合同继续履行将损害国家利益和社会公共利益的，双方当事人应当中止或者终止合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，各自承担相应的责任。

## 十六、不可抗力

1．如果任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间；

2．因不可抗力致使不能实现合同目的，甲乙双方可以解除合同；

3．因不可抗力致使合同有变更必要的，甲乙双方应在 10 个工作且内以书面形式变更合同；

4．受不可抗力影响的一方在不可抗力发生后，应在 10 个工作且内以书面形式通知对方，并在 10 个工作日内，将有关部门出具的证明文件送达对方当事人。

## 十七、争议的解决

本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，可以选择下列 2 款方式解决：

1．将争议提交合同签订地仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决；

2．向合同签订地咸阳市秦都区人民法院起诉。

## 十八、通知和送达

1．任何一方因履行合同而以合同第一部分尾部所列明的约定送达地址发出的所有通知、文件、材料，均视为已向对方当事人送达；任何一方变更上述送达方式或者地址的，应于 3 个工作日内书面通知对方当事人，在对方当事人收到有关变更通知之前，变更前的约定送达方式或者地址仍视为有效。

2．以当面交付方式送达的，交付之时视为送达；以电子邮件方式送达的，发出电子邮件之时视为送达；以传真方式送达的，发出传真之时视为送达；以邮寄方式送达的，邮件挂号寄出或者交邮之日之次日视为送达。

## 十九、税费

与合同有关的一切税费，均按照中华人民共和国法律的相关规定缴纳。

## 二十、其他

1．乙方和乙方工作人员应对甲方提供的资料，以及对在项目实施过程中知悉的秘密(包括不限于国家秘密、科研秘密、商业秘密、群众个人信息等所有秘密)履行保密义务，不得就所涉及的秘密及敏感信息以单位或者个人名义公开披露和公开发表观点。

2．本合同应按照中华人民共和国的现行法律进行解释。

3．本合同语言为简体中文，双方交换的与合同有关的信函均按此书写。

4．除技术规范中另有规定外，计量单位均使用中华人民共和国法定计量单位。

## 二十一、变更、中止、终止

合同一经签订，不得擅自变更、中止或者终止合同。对确需变更、调整或者中止、终止合同的，应按规定履行相应的手续。

## 二十二、本合同一式捌份

其中，甲方肆份，乙方叁份，采购代理机构壹份。签字盖章后生效，合同执行完毕自动失效。

甲方：中共咸阳市委网络安全和信息化委员会办公室

（盖章）

法定代表人或其授权的代理人：

（签字）

日期：2026.3.24

乙方：咸阳秦云信息技术有限公司

（盖章）

法定代表人或其授权的代理人：

（签字）

日期：2026.3.24

## 附件 1：运维服务内容清单

| 序号 | 服务项 | 项目 | 服务内容 |
|---|---|---|---|
| 1 | 日常安全运营服务 | 安全运维驻场服务 | 派驻 7 名专业安全运维工程师常驻客户现场，负责网络安全相关软硬件产品的基础运营与安全能力维护，实现故障即时响应，提供稳定的现场技术支持，执行日常巡检、运行及维护维修等任务。并参与安全运维体系的规划、设计与落地工作，协助客户系统化完善现有安全运维制度与流程；参与制定覆盖网络、主机及业务系统的全网业务连续性计划与灾难恢复方案；确保在重大会议保障、安全产品割接等可能对业务安全产生显著影响的关键时期，提供定制化、高可靠性的专项值守与保障服务。<br>上述安全运维工作，需自备专业安全运维系统，接入各类网络安全设备告警日志进行分析研判。 |
| 2 | | 网络安全体系建设咨询 | 提供从顶层设计到落地实施的全面网络安全体系规划，涵盖战略制定、架构设计、管理制度建设及持续改进的一体化咨询解决方案。 |
| 3 | | 线下安全检查服务 | 通过线下安全检查的方式，依据《网络安全检查评估工作指南》，抽查选取党政机关或企事业单位、学校和医院等开展网络安全检查线下检测，核查标准规范，指导被检查单位进行网络修复和加固工作，消除风险隐患，强化防护能力。 |
| 4 | 安全保障服务 | 重大活动保障 | 在大型活动、重要会议期间，提供覆盖重保前、中、后全周期的服务解决方案，在重大活动前提供资产梳理、安全检查及整改服务，活动期间提供监测值守、应急处置、ai 数据分析和威胁闭环等服务，为重保期间业务系统的安全稳定运行保驾护航。 |
| 5 | | 漏洞扫描 | 使用漏洞扫描工具，对主机、Web 应用、网络设备、安全设备等进行安全检测，快速发现安全风险并提供修复建议，防止攻击者利用漏洞植入木马、窃取核心数据等。针对整改情况进行复测，给出复测结果。 |
| 6 | | 协助安全加固 | 根据存在的网络安全风险，提供专业可实施的安全加固建议，协助进行加固建议落地，提供加固后的复测服务，输出安全风险复测报告。 |
| 7 | | 代码审计 | 需自行提供专业代码审计和软件成分分析工具，采用人工分析为主、工具分析为辅的方式，系统化的对源代码程序进行安全检查与审计，发现源代码缺陷引发的安全漏洞，输出代码审计报告及修复建议。检查内容包括但不限于：SQL 注入漏洞、跨站脚本漏洞、文件上传漏洞、敏感信息泄露等方面。 |
| 8 | | 渗透 | 在用户授权下，通过模拟黑客的攻击行为与分析方法对应用 |

| | | | |
|---|---|---|---|
| | | 测试 | 系统进行全面的安全测试，需自行提供主机漏洞扫描、web 漏洞扫描、ai 自动化渗透测试等专业工具，识别目标系统中存在的安全风险，输出测试报告与修复建议，测试不得影响业务系统正常运行。针对整改情况进行复测，给出复测结果。 |
| 9 | | 安全培训 | 结合客户相关岗位的业务场景，以培训的形式分享可能因安全意识薄弱产生的潜在信息安全风险，从而提升企业信息安全意识能力；针对常见 Web 漏洞进行安全讲解（例如 OWASP TOP10 漏洞），以及常见安全工具的使用进行实操培训等。服务周期每半年 2 次，年度开展 4 次。 |
| 10 | | 安全检查与风险评估 | 通过安全服务团队对辖区重点关键基础设施单位进行安全巡检服务，包括以下服务内容：<br>1、巡检服务包含安全访谈、制度落实、漏洞扫描等内容；<br>2、对相关开发、管理等人员进行访谈，发现日常工作、流程、管理、制度等存在的安全隐患；<br>3、通过基线检查，发现网络、主机、系统、应用等存在的错误配置、不符合项、弱口令等问题；<br>4、通过漏洞扫描，发现网络、主机、系统、应用等存在的安全漏洞； |
| 11 | | 硬件维保及特征库和授权升级服务 | 提供威胁感知、网站监测和网络攻击阻断等设备的原厂售后服务承诺书，缩短设备故障导致的业务中断时间。定期为规划并实施设备操作系统的版本升级，获取最新的功能与性能优化，避免因版本过低导致的安全漏洞和兼容性问题。为相关设备及时更新病毒库、攻击特征库和授权服务，保障设备发挥安全防护能力。 |
| 12 | 应急保障服务 | 应急响应服务 | 以 “7×24 小时极速响应、精准处置、最小化损失、保障业务连续性” 为核心目标，提供远程 + 现场一体化处置服务。工作内容包括：安全事件分析、应急处置、协助加固、问题复测等。安全事件包括但不仅限于：勒索病毒、蠕虫事件、黑客入侵事件、数据泄露、挖矿事件等。 |
| 13 | | 应急演练服务 | 根据实际网络环境情况，按照监管及客户需求提供多种场景下的演练方案，以模拟演练、桌面推演、实战演练的方式检验应急预案的完整性、可行性，提高单位的应急预案实操性及应急处理能力。 |
| 14 | 403 专网网络维护服务 | 403 专网网络维护服务 | 保障甲方指定专网点位网络稳定运行、快速处置故障、降低业务中断风险。 |
| 15 | 网络安全攻击阻断 | 威胁情报赋能服务 | 1.支持威胁情报中心的引入，威胁情报中心要求集成有公安部的威胁情报源和不少于 5 家国内头部第三方安全厂商的情报集合，威胁情报包含正向攻击情报源、受控外联情报源、IP 画像情报源及自定义情报源等类型，并支持威胁情报行业 |

| | | | |
|---|---|---|---|
| | 服务 | | 分类，至少覆盖金融、电力、能源、教育等30多个行业，支持IPv6格式情报数据。并且能够实时与公安部威胁情报中心联动，将威胁情报赋能给端点设备对网络攻击和恶意外联行为进行自动化的处置工作。 |
| 16 | | 网络攻击检测阻断服务 | 1.以威胁情报为核心，基于外到内的流量自动化检测，结合攻击行为特征分析、攻击语义分析、人工智能研判等手段，对不少于46种攻击类型防护可进行检测阻断，例如网络爬虫、主机扫描攻击、SQL注入、跨站脚本攻击、组件漏洞攻击、认证和授权漏洞、Webshell攻击、隐蔽隧道、后门攻击等。<br>2.满足多种网络检测环境，支持串联与旁路两种检测方式，支持802.1Q网络环境，支持对IPv6地址检测。<br>3.支持以IP黑白名单及访问控制的方式进行精细化攻击检测配置，并且能够以旁路方式自动化阻断攻击行为，阻断成功率要求≥99%。 |
| 17 | | 被控外联检测阻断服务 | 1.以威胁情报为核心，基于内到外流量的自动化检测，结合云中心威胁情报专家分析，对风险外联行为进行日常监测分析，按照外联APT组织、病毒木马、恶意程序、黑客工具等标签进行外联威胁分类分析<br>2.对被控外联检测环境的支持需与上述正向攻击行为检测保持一致，并且能够以旁路方式自动化阻断恶意外联行为，阻断成功率要求≥99%。 |
| 18 | | 弱口令隐患检测服务 | 1.基于对网络流量中应用协议的检测，能够对存在的弱口令登录行为进行监测分析，可自定义弱口令字典库，实现弱口令登录的实时监测，且能够对流量中存在弱口令的登录行为进行阻断处理。 |
| 19 | | 溯源画像分析服务 | 1.能够对威胁IP和域名进行基础属性画像，至少包含归属地、归属地、经纬度、运营商等属性，能够对威胁IP和域名的资产标签、组件标签、开放端口等进行自动化探测画像，并且支持对最近三个月的攻击轨迹溯源，至少包含历史攻击单位、攻击类型、被攻击单位所属行业等属性。 |
| 20 | | 防护联动处置服务 | 能够与当前网络中其它安全设备联动，支持将威胁情报中心监测分析受到的攻击和外联行为以syslog及syslog加密发送两种方式共享给其它安全设备进行处置，同时能够支持网络其它安全设备将检测到的威胁行为以API接口方式进行阻断调用处置。 |
| 21 | | 多维度安全事件分析服务 | 对正向攻击行为按照攻击检测告警、攻击IP分析及被攻击IP分析等维度汇总分析，对反向外联行为按照外联检测告警、外联检测分析以及外联域名分析等维度汇总分析，各维度均可按照需求进行监测分析。 |
| 22 | 威胁感知 | 流量采集 | 1、提供IPv4/IPv6双栈网络部署与流量分析检测服务，支持在IPv4和IPv6网络环境下部署，接口支持IPv4、IPv6配 |

| | | | |
|---|---|---|---|
| | 监管服务 | 服务 | 置，可对 IPv4 路由、IPv6 路由分别进行监控，同时实现对 IPv4 与 IPv6 网络流量的并行分析检测。(提供相关功能截图)<br>2、提供网络流量协议识别与还原服务，支持对 HTTP、DNS、DHCP、SMTP、POP3、IMAP、Webmail、DB2、Oracle、MySQL、MSSQL-DB、Sybase、SMB、FTP、SNMP、Telnet、NFS、ICMP、SSL、SSH、Redis、LDAP、RADIUS、Kerberos、NetBIOS、Modbus、NTP、IPv6 等常见协议进行识别及流量还原，可用于取证分析、威胁发现。<br>3、提供网络行为全维度记录与描述服务，支持对 TCP/UDP 会话、异常流量会话、SSL 加密协商、登录行为、域名解析、文件传输、FTP 控制通道、LDAP 行为、Web 访问、邮件行为、数据库操作、Telnet 命令、旁路阻断、MQ 流量、Radius 行为、Kerberos 行为、ICMP 流量、SYN 流量等各类网络行为进行完整记录与行为描述。 |
| 23 | | 流量过滤服务 | 1、提供流量文件还原服务，支持对 HTTP、FTP_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS 等协议流量进行文件还原。<br>2、提供规则化威胁检测服务，支持 13000+条检测规则，支持检测 WEB 攻击、Webshell 攻击、网络攻击、后门程序、僵木蠕、C2 外连、恶意通信、SMB 远程溢出攻击、文件上传、弱口令、暴力猜解、挖矿、黑客工具、明文密码传输、漏洞利用、ARP 欺骗、恶意扫描等安全风险。<br>3、提供流量抓包分析与取证存储服务，支持通过设备对流量进行抓包分析，可自定义配置抓包方向（双向/单向）、数据包数量、IP 地址、端口及协议类型；支持同时开启至少 16 个抓包任务，每个任务可独立配置抓包规则，抓取的原始流量包可本地保存，用于后续流量分析与安全取证。 |
| 24 | | 网内威胁监测服务 | 1、提供主机资产自动识别服务，可基于网络流量自动识别并归类主机资产类型，覆盖终端（PC、移动设备、其他终端）与服务器（代理服务器、数据库服务器、邮件服务器、Web 服务器、DNS 服务器、文件服务器、远程登录服务器、认证服务器、时间服务器、其他服务器）等多种类型，识别范围可灵活扩展。服务支持自动提取并生成完整资产字段信息，包括：IP、端口、服务、协议、WEB 框架、编程语言、办公系统、物理地址、操作系统、设备型号、厂家等关键属性。2、提供云端威胁情报联动检测服务，依托云端威胁情报库实现威胁实时检测，威胁情报库规模不低于 800 万条，覆盖 APT 事件、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒等主流威胁类型，支持实时检测与增量回溯。<br>3、提供内生情报生成服务，可基于文件动态检测，识别存在外联行为的 IP 与域名并自动生成可疑 IOC 列表，经人工确认后形成正式 IOC 情报。 |
| 25 | | 攻击 | 1、提供自定义线索拓线与溯源取证分析服务，支持对任意线 |

| | | | |
|---|---|---|---|
| | | 回溯分析服务 | 索开展自定义拓线及溯源取证分析，可通过可视化分析画布呈现完整拓线过程，并支持结果快照导出；可针对指定线索展示溯源结果，涵盖攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等场景。<br>2、提供日志调查任务与结果导出服务，支持基于日志检索创建日志调查任务，并可将调查结果以 XLSX 格式文件输出。 |
| 26 | | 告警响应处置服务 | 1、提供 ATT&CK 攻击技术可视化关联展示服务，支持以可视化拓扑结构形式，呈现告警所命中的 ATT&CK 攻击技术及关联关系。<br>2、提供勒索告警专项分析服务，支持对勒索告警进行专项分析，可识别 Cerber、Tescrypt、Strictor、WannaCry 等主流勒索家族；威胁统计包括：活跃勒索家族（受害资产数）分布统计、勒索受害资产 Top10、勒索告警趋势图；勒索告警信息包括：最近发生时间、资产 IP、勒索家族、勒索阶段、告警次数、攻击结果、威胁级别、级联单位、资产分组、资产类型、告警来源、告警设备，以及对应的详细告警列表。<br>3、支持基于单条告警或符合告警查询条件多告警的手动，自动处置，处置支持包括 NDR 设备，邮件网关，终端设备，准入设备，防火墙设备，服务器安全设备，IPS。 |
| 27 | | 异常行为检测服务 | 1、提供网络日志专项行为分析服务，支持基于网络日志开展多维度专项行为分析，涵盖 DNS 行为、非常规访问、邮件行为、登录行为、WEB 行为、数据库行为、访问行为、旁阻行为等场景，分析子类不低于 23 种。<br>2、提供攻击带外检测分析服务，可对攻击成功后依据负载信息向第三方发起的二次攻击行为进行检测识别，并支持带外攻击趋势统计分析。<br>3、支持检测 HTTP、SOCKS 协议的产生可疑代理行为；支持检测 socks、http、reDuh、RegeoryTunnel、Tunna 等代理工具产生的流量特征并在页面上呈现可疑代理类型分布，可疑代理访问趋势。<br>4、支持反弹 shell 分析，通过对 TCP 流量特征的分析识别反弹 shell 行为，能够提取受害 IP、攻击 IP、端口等信息，并在页面上呈现反弹 SHELL 访问趋势，反弹 SHELL 受影响资产 TOP10。<br>5、支持检测 SMTP、POP3、SSH、RDP、FTP、MSSQL、MYSQL、REDIS、ES、ORACLE 等协议的异常登录行为；检测类型包括：非正常时间访问，特权帐号登录， 明文密码泄露。 |
| 28 | 站群及重点互联网系统信息安全 | Web 漏洞扫描服务 | 负责 350 个网站批量扫描执服务：<br>1、要求对咸阳市辖区内的重要业务系统每周进行安全漏洞扫描，实时发现安全漏洞并配合网信办进行通报<br>2、要求对咸阳市辖区内的重要业务系统每周进行 WEB 安全漏洞扫描，实时发现安全漏洞并配合网信办进行通报； |

| | | | |
|---|---|---|---|
| | 运维监测 | | 3、要求对咸阳市辖区内重要业务系统网站存在的敏感信息泄露事件进行安全扫描服务，及时发现信息泄露的问题<br>4、要求对咸阳市辖区内重要业务系统中存在的附件，如 doc、docx、pdf、xls、xlsl、ppt、pptx、csv、markdown、md、txt 等附件进行安全监测服务，及时发现信息泄露事件。<br>5、要求对咸阳市辖区内重要业务系统存在的 oday 漏洞进行预警、通报；<br>6、针对漏洞扫描服务输出的报告，要求提供相对应的智能体实现对报告内容的自动解读；<br>7、支持网站附件中敏感信息泄露监测，附件类型至少包含：doc、docx、pdf、xls、xlsl、ppt、pptx、csv、markdown、md、txt<br>8、支持多引擎扫描网站存在的安全漏洞，默认每周检测一次，并支持自定义监测周期。 |
| 29 | | web 内容监测服务 | 全面监测 350 个网站内容安全风险：<br>1、要求针对咸阳市辖区内重要业务系统进行 WEB 内容监测服务，能够实时对违规内容（包括 FGFD、色情、暴力、恐怖主义、侵权、欺诈等信）进行监测，并配合网信办进行通报服务。告警响应时间为一分钟。<br>2、要求针对咸阳市辖区内重要业务系统进行 WEB 内容监测服务，能够实时发现首页源代码中出现的任何的变化，并进行综合分析，发现违规内容变更并配合网信办进行通报。<br>3、要求针对咸阳市辖区内重要业务系统进行 WEB 内容监测服务，能够实时发现业务系统全站内存在的任何页面篡改信息，并能够第一时间定位源代码篡改的位置和内容，并给出修复建议，并进行综合分析配合网信办进行通报；<br>4、针对 WEB 内容监测服务输出的报告，要求提供相对应的智能体实现对内容的自动解读；<br>5、支持可用性节点智能监测，可以配置最少监测节点数量并 |

| | | | |
|---|---|---|---|
| | | | 且每次随机选择节点进行监测<br>6、为了提高效率，支持设置可用性模版，模版可以快速用于多个资产的监测<br>7、可用性监测时支持设置请求参数，包括：HTTP 头、Cookie、用户认证（Basic Auth）设置，支持设置是否进行 SSL 证书验证。 |
| 30 | | 防冒网站（钓鱼网站监测服务） | 精准识别 350 个目标网站的仿冒/钓鱼风险，实现溯源处置与风险闭环，保障品牌声誉及用户权益，构建全流程监测体系<br>1、要求建立咸阳市辖区内全面的黑词、挂马、网页篡改、钓鱼网站特征库，并基于恶意特征实现对咸阳市辖区内仿冒网站的实时监测服务，能够在钓鱼/仿冒网站出现的第一时间实现告警，并配合网信办实现通报；<br>2、针对仿冒网站监测服务输出的报告，要求提供相对应的智能体实现对内容的自动解读；<br>3、基于已获取的全国范围内的 DNS 解析数据、10 亿终端监测数据以及 4000 万页面/天的实时监测技术，可在钓鱼/仿冒网站出现的第一时间通知到客户。<br>4、提供基于大数据支撑的黑词、暗链、空链、坏链发现技术手段，支持全站监测，可定位源代码的位置和内容，支持监测频率自定义，支持 AI 验证 |
| 31 | 办公场所视频监控系统运维 | 办公场所视频监控系统运维 | 主要负责市委网信办办公场所的视频监控系统日常巡检、故障排查与设备维护，确保前端摄像机、硬盘录像机、网络传输稳定运行；防范非法入侵与数据泄露，保障监控数据安全可控。 |