网络安全（数据安全）应急处置工具箱

功能需求参数

一、工具箱功能及内容

供应商应在规定的期限内交付网络数据安全检查工具箱，网络数据安全检查工具箱（以下简称“工具箱”）符合相关数据安全检查工具装备技术规范要求，满足网络数据安全和个人信息保护等网络数据安全风险检查、数据泄露应急处置，并能自动生成检查分析报告。主要功能如：

1.支持的数据安全管理检查模块应包含如下。

（1）检查工作台。包含检查方案管理、检查任务管理、技术检测管理、数据采集、数据分析。依据《网络安全法》《数据安全法》《个人信息保护法》《党委（党组）网络安全工作责任制实施办法》《关键信息基础设施安全保护条例》等法律法规，设置数据安全检查项及检查要点，包含但不限于数据安全组织体系、制度建设、数据分类分级、供应链及合作方管理、数据收集、传输、存储、使用和加工安全、数据提供和公开安全、销毁安全、交易安全、安全防护、现场检查监测预警、数据载体高危漏洞、弱口令、恶意外链行为、攻击入侵线索、数据安全审查及风险评估、数据出境安全等问询记录（提供原厂相关功能证明材料截图或复印件并加盖单位公章）。

（2）知识库管理。包含威胁情报库、数据分析规则库、流量特征知识库、漏洞知识库、弱口令库、日志分析规则库、检查模板库。检查工具应预置知识库集,与检测引擎联动以实现相关的检查能力；应包含为实现检查项所必需的知识和规则；应支持规则或模型的导入、调用、编辑、自定义配置功能；应支持自定义配置检查规则；应支持根据实际工作需要扩展。特别是可以根据不同行业的检查标准，自定义导入功能（提供原厂相关功能证明材料截图或复印件并加盖单位公章）。

2.支持技术检测功能包含资产识别功能、漏洞检测和弱口令检测功能、数据接口安全检测功能、数据和流量采集分析功能、日志分析功能、敏感信息发现功能等。

（1）资产识别功能。支持主机、数据库、网站应用系统、中间件、大数据平台、接口等识别，支持通过协议、证书、域名、端口等特征快速高效梳理特征资产。支持数据接口资产的发现并对其接口类型进行识别与分类，支持登录接口、上传接口、下载接口、一般服务接口等类型的自动分类。（提供原厂相关功能证明材料截图或复印件并加盖单位公章）。

（2）漏洞检测和弱口令检测功能。支持国内外主流操作系统（微软操作系统、麒麟操作系统等）、数据库、大数据平台、云平台、网站系统应用等漏洞检测，支持各类网站应用及中间件检测。（提供原厂相关功能证明材料截图或复印件并加盖单位公章）。

（3）接口安全检测功能。根据所给接口（外部系统与系统之间以及内部各子系统之间的交互点）开展针对接口的安全漏洞检测。（提供原厂相关功能证明材料截图或复印件并加盖单位公章）。

（4）数据和流量分析功能。应用程序编程接口安全分析、数据传输风险分析、传输通道安全分析（识别加密协议包括但不限于SSL、TLS、IPSec等）、文件敏感信息发现、分析、攻击威胁发现、支持镜像流量实时分析、离线流量上传分析。（提供原厂相关功能证明材料截图或复印件并加盖单位公章）。

（5）日志分析功能。支持主流操作系统中的多类型日志采集，包括操作系统日志、中间件日志、数据库、安全设备日志等关键日志的识别、采集、分析。支持非法外联检测，支持通过日志分析出被控外联线索。

（6）敏感信息发现功能。支持加密数据识别；支持个人敏感信息识别；支持发现敏感文件网络传输行为并自动提取文件，对其敏感信息发现情况进行标记。支持丰富的敏感数据识别技术，包括正则表达式、关键字典等先进技术自定义创建识别规则。支持内置敏感信息发现策略，包括敏感标签设置、敏感等级设置、发现策略设置、插件管理等。（提供原厂相关功能证明材料截图或复印件并加盖单位公章）。

二、 售后及服务要求

1.供应商提供本项目招标内容的实施方案，应包括工具箱的供货及调试、进度保障措施、质量保证措施。实施方案内容详实、可行性、操作性强、承诺完整详细、符合项目实际需求。

2.工具箱交付后提供不少于5年7\*24小时响应的本地化原厂技术支撑服务和质保服务，如遇重大事项满足2小时内现场服务，并根据采购方需求提供现场支撑服务，如工具箱使用中发生任何故障，提供免费维护保修及软件升级维护服务。在质保期内，由于硬件问题引起系统运行不稳定，承建方应免费提供硬件更换、硬件维护等工作；非承建方责任引起的设备损坏，承建方亦应负责修理，由此产生的费用由采购方负责解决。此项内容提供符合相应要求的承诺函。

3.质保期内，包括免费升级、功能完善、故障排除、性能调优、技术咨询等，并负责工具箱的开发、集成、处理、协调与其他系统的对接等。提供针对本项目的售后服务方案，售后服务方案中至少应包含售后服务承诺函、售后服务组织架构、售后服务人员组成等内容，为确保售后服务质量，应提供不少于2人的售后服务组，组员中具备CISP等网络安全、网络数据安全方向证书。

4.供应商需要提供培训承诺，质保期内每年厂家培训次数不少于1次，制定详细的培训方案，充分考虑本项目特点和用户需求，根据培训对象确定培训内容，根据培训方式（前期培训、现场培训、集中培训）制定培训计划和课时安排。培训方案详实科学、培训周期合理，同时，为确保培训讲师经验丰富，讲师应具备相关专业证书。

5.供应商承诺工具箱质保到期前确保软件升级到最新版本，做好软硬件的维保更新，提供承诺函。

三、工具箱性能要求

1.知识库管理：敏感数据规则（敏感标签内置规则不少于100条）；漏洞库（漏洞规则不少于20万条，支持支持兼容CVE、CNCVE、CNVD、CNNVD等标准）。

2.资产识别功能：支持20余种数据类型资产的发现识别，包含常见的mysql、Oracle、DB2、kingbase等数据库类型。支持非机构化文件扫描，支持本地、FTP、SFTP等。资产探测速度精准，5M带宽下扫描常用端口组，C类网段不超过15分钟，B类网段不超过120分钟，在线资产识别率应不低于90%。

3.敏感信息发现功能。支持Mysql、Oracle、POSTGRESQL、UXDB、MSSQL、HIVE、IMPALA、MARIADB、ELASTICSEARCH、CLICKHOUS、GREENPLUM、INFORMIX、SYBASE、HBASE、POLARDB、南大通用、人大金仓、达梦、高斯等20余种数据源类型；支持对终端、及存储中的数据内容进行离线敏感识别及安全检查，支持离线工具部署运行在Linux、Windows、Mac三种常用的操作系统，支持doc、docx、ppt、pptx、xls、xlsx、pdf、rtf、txt等办公或文本格式文档内容深度解析、多层压缩包解析、支持识别加密的Office类文档、RAR、ZIP、ARJ压缩包、PDF文档。（提供原厂相关功能证明材料截图或复印件并加盖单位公章）。

4.硬件性能。CPU：大于等于12核心；内存：大于等于32GB；硬盘不小于1TB，网口：千兆网口；工具箱重量不超过5KG。（提供工具箱实物图片或复印件并加盖单位公章）。