**技术规范书**

1、资质参数

* 投标方或生产厂商具备CCRC信息安全服务资质认证证书—信息安全风险评估服务一级资质。（需提供证书证明并加盖原厂公章）
* 投标方或生产厂商软件研发实力需通过CMMI L5认证和CSA CS-CMMI5认证。（需提供证书证明并加盖原厂公章）
* 投标方或生产厂商需是国家信息安全漏洞库CNNVD技术支撑单位。（需提供证书证明并加盖原厂公章）
* 投标方或生产厂商提供公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》网络版防病毒产品（一级品）资质证书。（需提供证书证明并加盖原厂公章）
* 投标方或生产厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位。（需提供证书证明并加盖原厂公章）

1. 技术参数

* 云端威胁：支持跳转链接至云端安全威胁响应系统，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。（需提供产品截图证明，并加盖原厂公章 ）
* 漏洞验证：提供漏洞验证服务，针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的漏洞，自动生成漏洞工单，安全专家跟进漏洞状态，各个处理进度透明，方便招标方清晰了解当前漏洞的处置状态，将漏洞处理工作可视化（提供服务工具漏洞工单截图，并加盖原厂公章，需展示当前漏洞的处置状态）
* 漏洞状态追踪：对发现的漏洞建立状态追踪机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况，使得招标方可做到漏洞的可视、可管、可控（提供漏洞管理功能平台截图，并加盖原厂公章，直观展示漏洞管理情况）
* 基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案（提供在服务平台申请主动响应的实际界面截图证明，并加盖原厂公章）
* 业务安全状态监控：需服务监控门户（或用户Portal，区别于安全感知大屏），在门户中招标方可查看业务和资产安全状态信息，使得招标方能直观感受到当前的业务和资产安全状态，展示纬度至少包括服务资产安全评级、服务运营状态及成果、安全风险概览、最新情报。（需提供截图证明，并加盖原厂公章）
* 服务质量监控：提供的服务监控门户（或用户portal）应具备服务质量可视化展示，能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，已验证所承诺的服务SLA。（需提供截图证明，并加盖原厂公章）
* 通过SLA对安全事件服务水平作出承诺：（提供承诺书并加盖原厂公章）

1）从安全日志产生到事件通告给招标方的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于30分钟，一般事件的通告时间少于1小时。

2) 在配备的边界防护服务组件和终端防护服务组件的情况下，运营服务对于重大安全事件的遏制影响和处置完成时间小于1小时，对于一般事件的遏制影响和处置完成时间小于4小时。

3）在未配备的边界防护服务组件和终端防护服务组件的情况下，运营服务对于重大安全事件的遏制影响和处置完成时间小于8小时，对于一般事件的遏制影响和处置完成时间小于24小时。

4）安全事件经过服务人员的确认后，各类安全事件的判断准确率不低于99%。

5）在配备了的边界防护服务组件和终端防护服务组件的情况下，安全事件的闭环处置比例达到100%。

6）对于重大事故应启动应急响应机制，工作时间15分钟之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应，省会2小时上门处置，省内8小时上门处置。

* 保障期间，需要提供7\*24小时持续专家服务，威胁发现及时响应（提供承诺书并加盖原厂公章）