# 项目需求

## 1.项目需求

招标人采购一年的现有深信服网络安全设备维保服务及云端7×24小时安全运营服务。

1.1项目清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品型号** | **数量** | **服务过期时间** | **产品名称** |
| 1 | AC-1000-F640（出口行为管理） | 1 | 2024/9/20 | URL&应用识别规则库升级 |
| 2024/9/20 | 产品质保 |
| 2024/9/20 | 软件升级 |
| 2 | AD-1000-D620（出口负载均衡） | 1 | 2024/9/20 | 产品质保 |
| 2024/9/20 | 软件升级 |
| 3 | SIP-1000-B400（态势安全感知） | 1 | 2025/6/11 | 深信服安全感知系统平台特征库软件 V2.0版本 |
| 2025/6/11 | 产品质保 |
| 2025/6/11 | 软件升级 |
| 4 | STA-100-B2200（流量探针） | 1 | 2025/6/11 | 深信服安全感知系统探针特征库软件V2.0 |
| 2025/6/11 | 产品质保 |
| 2025/6/11 | 软件升级 |
| 5 | AF-2000-B2150（服务器防火墙） | 1 | 2025/6/11 | 深信服云智订阅软件（AF8.0.7及以上版本适用） |
| 2025/6/11 | 产品质保 |
| 2025/6/11 | 软件升级 |
| 6 | AF-1000-E420（运维防火墙） | 1 | 2025/6/25 | 深信服云智订阅软件（AF8.0.7及以上版本适用） |
| 2025/6/25 | 产品质保 |
| 2025/6/25 | 软件升级 |
| 7 | 安全运营 | 1 | 2025/6/30 | 云端安全专家团队与用户一同，采用“人机共智”模式构建持续（7×24小时）主动、闭环的安全运营体系，包含现状评估与处置加固、实时漏洞检测与修复指导、全网实时网络威胁监控与预警等 |
| 2025/6/30 | 网站监测4个（针对互联网网站暴露面实时防护，例如网页防篡改，WAF防护等） |
|

1.2技术指标参数要求

1.2.1安全运营服务

|  |  |
| --- | --- |
| 序号 | 技术规格 |
|  | **平台安全性：▲**投标人的安全托管服务平台应当通过国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部四部委联合组织的云计算服务安全评估，入选“通过云计算服务安全评估的云平台”名单（提供国家网信办官网发布的名单截图） |
|  | 暴露面梳理：投标人应使用安全工具对招标方服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险 |
|  | 安全现状评估：系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描 |
|  | **高危可利用漏洞防护：▲**针对服务范围内资产扫描到的高危可利用漏洞，投标人应当为招标方做好每一个高危可利用漏洞的防护工作，包括但不限于为招标方提供漏洞修复方案和安全设备防护策略，以及帮助招标方配置防护规则，保证招标方不因此出现重大事件和损失（提供服务平台具备高危可利用漏洞防护规则的证明，并且支持对扫描到的高危可利用漏洞能够自动匹配漏洞防护规则） |
|  | 受影响资产排查与加固：安全专家应当结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。（提供一个威胁情报的安全通报工单，工单内容包含威胁情报的基本信息和推送信息以及跟进记录，要求明确说明关联资产信息的排查情况） |
|  | 漏洞修复建议：针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案 |
|  | 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 |
|  | 威胁管理：实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件 |
|  | **安全策略检查：▲**投标人安全专家每月对招标方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。投标人云端服务平台应当具备丰富的策略检查工具（要求不少于40种策略检查的工具），支持排查安全设备防护策略配置的合理性（提供云端服务平台策略检查工具的截图证明） |
|  | 事件管理：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 |
|  | 服务过程透明化可视化：投标人需为招标方提供移动端服务过程展示门户（移动端Portal），支持直观地查阅服务推送的各种安全事件/威胁的详细专家审核研判过程，需包含安全事件详细的【基本信息】【入侵路径】【影响主机】【主机调查】【数据包分析】等内容（提供移动端服务过程展示门户中支持查阅服务推送的各种安全事件/威胁的详细专家审核研判过程的截图证明） |
|  | 安全规则管理：为了保证安全监测的效果，安全服务平台应具备检测规则的自定义功能，以满足日益复杂的安全趋势所带来的安全需求 |
|  | 平台管理：本项目使用服务工具支持将收集的安全日志上传到安全服务平台上，并支持在该平台上对服务工具进行管理 |
|  | 专属服务经理：为了保障服务质量和加强投标人与招标方的沟通，投标人应当承诺为招标方配置一名经验丰富的安全专家作为专属服务经理，并且实时响应投标人咨询的网络安全相关问题 |
|  | 通过SLA对服务水平作出承诺：1. 从安全日志上传分析研判到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15分钟，一般事件的通告时间少于30分钟；
2. 在配备投标人的边界防护服务组件和端点防护服务组件的情况下，重大威胁与事件的遏制影响完成时间少于15分钟，一般威胁与事件的遏制影响完成时间少于30分钟；
3. 安全事件经过投标人服务人员的确认后，通告给招标方的各类安全事件的准确率不低于99%（即误报不能超过1%）；
4. 投标人应当承诺攻击成功事件0漏报，服务人员至少发现攻击链路上的一个攻击行为。
5. 投标人应当承诺，服务范围内的所有安全事件的闭环处置比例达到100%。
6. 投标人应当满足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。
7. 在具备投标人的边界防护组件的情况下，要求招标方可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到99%。
8. 经招标方授权后，投标人服务人员协助进行安全事件的闭环，一般安全事件的闭环完成时间少于8小时，重大事件的闭环完成时间少于24小时。
 |
|  | **7×24小时威胁鉴定：▲**投标人应当具备云端检测和分析平台，通过采集招标方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为招标方提供7×24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；（提供云端服务平台告警审核功能界面截图，举证一个告警聚合分析的例子和一个告警详情展示具备上述能力） |

1.2.2网站监测(以下技术内容应提供功能截图及加盖原厂公章）

|  |  |
| --- | --- |
| 序号 | 技术规格 |
|  | 服务内容：在安全托管服务MSS的基础上为用户网站提供持续网站监测增值服务，包括对网页篡改、网站挂码/黑链进行实时监测，同时运营中心还会帮助用户持续监控网站业务的可用性，帮助用户实时掌控网站的安全态势。 |
|  | **网站页面篡改监测：**▲对目标站点进行实时篡改监测，首页每5分钟一次，全站每3天一次，一旦发现被篡改第一时间通过微信服务群进行告警（提供网站监测服务网站页面篡改监测能力的证明截图） |
|  | **互联网漏洞检测：**▲支持模拟黑客攻击视角，从互联网对网站的web漏洞进行检测（提供网站监测服务互联网漏洞检测能力的证明截图） |
|  | **高危漏洞验证：**▲针对检测发现的高危漏洞，进行安全专家人工验证，并通过微信群实时向用户通告（提供网站监测服务高危漏洞验证能力的证明截图） |
|  | **业务可用性监测：**▲自动持续对网站的可用性进行探测，网站的首页url保持每10分钟探测一次，及时发现断网故障，微信专家群主动告警通知（提供网站监测服务业务可用性监测中的探测与告警能力的证明截图） |

1.2.3现网设备续保服务(以下技术内容应提供功能截图及加盖原厂公章）

|  |  |
| --- | --- |
| 序号 | 技术规格 |
|  | 出口行为管理 深信服AC-1000-F640：全网行为管理应用识别库升级、软件版本升级和硬件质保续保服务 |
|  | 出口负载均衡 深信服AD-1000-D620：应用交付软件版本升级和硬件质保续保服务 |
|  | 态势安全感知 深信服SIP-1000-B400：态势安全感知平台安全感知特征库升级、软件版本升级和硬件质保续保服务 |
|  | 流量探针采集 深信服STA-100-B2200：流量探针安全感知特征库升级、软件版本升级和硬件质保续保服务 |
|  | 服务器防火墙 深信服AF-2000-B2150：下一代防火墙安全特征库升级、软件版本升级和硬件质保续保服务 |
|  | 运维区防火墙 深信服AF-1000-E420：下一代防火墙安全特征库升级、软件版本升级和硬件质保续保服务 |
|  | 续保服务完成后，提供原厂续保时间有效期服务承诺函 |

1.2.4上述技术指标参数为投标人建议参数，若有部分参数无法满足，在评标过程中会根据评分标准扣除技术分；

1.2.4上述技术指标参数中，带有▲的为关键参数，若有三项关键参数投标人无法满足的，投标人响应文件作废。

1.3服务支持

1.3.1投标人应提供支持服务计划、安排等内容的说明；

1.3.2投标人应组建为本项目服务的武汉本地技术服务团队；

1.3.3投标人应提供7x24 小时快速上门服务和2小时内快速响应服务；

1.3.4在72小时内无法恢复故障提供免费的设备备机备件服务。

1.4服务时间：一年。

## 2.履约要求

2.1投标人应在合同签订生效之日起15个工作日内完成全部设备安装调试工作并交付使用。

2.2投标人应按招标人要求提供下列材料，若无法提供或提供不全按合同内相关违约条款处理：

（1）《安全服务运营报告》，提供频率：每月一次；

（2）《事件分析与处置报告》，提供频率：按需提供，不限次数；

（3）《安全通告》，提供频率：按需提供，不限次数；

（4）《年度汇报PPT》，提供频率：每年一次。