**广东碧桂园职业学院网络安全态势感知系统采购需求书**

 **一、采购范围**

 1.数量清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备（货物）名称** | **单位** | **数量** |
| 1 | 安全态势感知平台（含硬件、软件、3年软件升级及原厂服务） | 套 | 1 |
| 2 | 探针设备（含硬件、软件、3年软件升级及原厂服务） | 台 | 1 |
| 3 | 安全运维服务 | 年 | 1 |

 2.供应商需完成如下事项：

供应商报价需包括设备及相关附件的采购、包装、送货、安装、验收、培训、税费、技术服务（包括技术资料的提供）、保修期保障、其它费用等一切支出。

**二、商务需求**

 1.对供应商的资格要求：

（1）对供应商的资格要求：国内（指按国家有关规定要求注册）注册资金500万元（含500万元）以上，具备独立法人资格；具有信息安全服务相关资质证书，具有履行合同所必须的设备和专业技术能力。

（2）投标人的证明文件不符合标“★”的任一项的，则视为未实质响应招标要求，取消其投标资格。

2. 硬件产品必须具备公安部颁发的安全产品销售许可证，软件产品必须拥有软件著作权登记证书，如是代理商投标则需提供产品制造厂商代理资质证书和厂商盖章的售后服务承诺函。

3. 实施要求：实施人员必须是经过专业培训的专业人员，具备设备原厂认证证书，实施技术及操作过程符合行业安全规范，实施过程将严格按照规范的程序实施，确保产品和周边设施的安全。

4. 合同签字生效后，以甲方发出书面通知之日起，15个工作日内将货物运达目的地并安装完毕。

5. 付款方式：

 （1）项目实施完成后，甲乙双方办理正式竣工验收及结算手续后，甲方于10个工作日内支付结算款的95%。

（2）余款5%作为质量保证金，甲方在3年产品质量保证期满后10个工作日内无息向乙方结清余下货款。

**三、技术规格和要求：**

1．总体要求

（1）为保护学院前期安全设备的投资，产品必须能够对接深信服防火墙、深信服EDR、深信服AC等设备，并实现联动。

（2）本项目产品功能及技术指标要求需提供相应截图并加盖产品原厂商公章证明。

2．技术参数要求

采购设备具体技术参数请见附表。

**四、服务需求**

1.乙方交付的产品质量保证期为3年，自该产品经甲方验收合格签字之日起算。

2.在质量保证期内，由供应商提供免费保修服务（另有特别说明的，按其要求执行），免费保修期届满后，如甲方需要乙方继续提供维护服务，由甲乙双方另行协商。

**附表：技术参数表**

**1、安全态势感知平台技术参数**

| **序号** | **功能及技术指标** | **详细参数** |
| --- | --- | --- |
| 1 | 硬件要求 | 国产品牌 标准2U机架式设备，双冗余电源，CPU数量≥2，内存≥192GB,具备独立的系统盘和数据盘，系统盘要求为固态硬盘，容量≥128GB，数据盘≥48TB，支持RAID5，接口≥4个千兆电口+4个万兆光口，数据吞吐量≥8Gbps。支持多节点设备组成HA集群，实现存储空间、处理性能弹性扩充；保证业务运行的连续性、可靠性 |
| 2 | 数据采集 | 支持从威胁探针、终端、安全设备（如防火墙、IDPS、WAF等）和第三方网络设备（通过标准syslog协议输出）处收集流量和日志数据。支持syslog、winlogbeat、wmi、jdbc、webservice、ftp、snmptrap格式的数据 |
| 3 | 全网安全态势大屏 | 支持不同安全视角展示16个独立的大屏展示功能 ，包括全网安全态势感知大屏、重点时期防护、安全事件态势、通报预警态势、资产态势大屏等。支持对安全事件、外部攻击者等维度进行自定义设置实现实时告警展示，支持大屏轮播，可在一个屏幕上自动切换轮播不同的大屏，所有大屏可自定义播放顺序。 |
| 4 | 资产管理 | 资产发现 | 支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、mac地址、主机名等。支持跨三层取mac地址，识别资产mac地址，并能够解决不同资产IP冲突问题，以及DHCP场景IP变更的问题。 |
| 资产全生命周期管理 | 支持资产多级分支管理，最多可至15级分支，支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等。 |
| 5 | 脆弱性管理 | 弱密码检测 | 弱密码识别支持主动扫描，支持加密协议的弱口令登录检测，支持SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL等协议。弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web空密码、账号白名单、密码白名单、txt文件格式导入。 |
| 威胁分析 | 支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web应用等 ，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。 |
| 6 | 威胁检测 | Webshell检测 | 具备基于AI的webshell通信流量检测，可检出加密（如冰蝎）的通信流量。，具备650+webshell规则检测，且覆盖webshell整个攻击阶段检测，包括webshell上传点探测、webshell上传下载、webshell通信。 |
| 事后异常行为检测 | 具备元数据行为分析引擎：httpflow、dnsflow、adflow、icmpflow、maillflow等, 通过异常行为分析，结合各类机器学习算法完成未知威胁检测。包括：内网穿透、代理、远控、隧道、反弹shell等事后检测场景。 |
| 挖矿专项检测 | 支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力。平台内置挖矿安全知识库，对常见挖矿行为和病毒木马等提供详细的背景介绍、感染现象、详细分析、相关IOC（MD5、C2、URL）、解决方案。 |
| 文件威胁分析 | 文件威胁分析支持平台内置的静态文件检测引擎、AI智能引擎、SAVE查杀引擎、webshellkiller引擎，利用LSA, AutoEncoder, LogicRegression, SVM, 随机森林，XGBoost等多种机器学习算法组合进行综合研判。支持采用AI技术针对无文件落地的恶意脚本进行检测。 |
| 邮件威胁分析 | 支持针对政企邮件混淆宏病毒威胁检测，可通过不断下钻的特征向量提取和聚类算法有效检出邮件威胁。支持对smtp、imap、pop3、webmail等邮件协议审计，提取邮件正文和附件中的流量，并对邮件附件、正文链接、邮件行为、发件人等多维度进行规则和机器学习检测，从而识别出钓鱼邮件、病毒邮件、垃圾邮件、鱼叉式钓鱼等恶意邮件。 |
| 第三方日志关联分析可视 | 支持SIEM日志关联分析结果的可视化展示。包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供每一台设备专项分析的页面。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析。 |
| 日志检索 | 支持安全检测日志、审计日志、第三方日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet等。 |
| 主机行为EBA分析 | 支持利用EBA技术进行资产的行为分析，对这些对象进行持续的学习和行为画像构建，以基线画像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。内建异常行为学习模型，并支持用户对EBA基线进行自定义调整，优化模型。 |
| 7 | 事件处置 | 告警消减 | 支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法。 |
| 联动处置 | 安全事件支持与深信服防火墙、终端安全响应系统、超融合联动封锁、访问控制，安全事件支持与终端安全响应系统联动一键查杀、进程取证，支持关闭深信服超融合上的中毒虚拟主机，支持对深信服超融合上中毒的虚拟主机进行快照。 |
| 8 | 外网态势感知 | 提供不少于5个域名的网站的云端漏洞主动扫描和持续监测服务。支持和SIP联动，定期对互联网业务系统进行漏洞扫描，将主动漏洞扫描和被动流量检测结合，实时发现内外网存在的安全风险，并通过邮件、微信公众号等方式进行主动告警通知；支持7\*24h的监测，及时发现网页篡改、敏感内容、挂马、黑链、断网等安全事件； |
| 9 | 攻防处置 | 实战攻防中心 | 具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理暴。实战阶段的实时攻击分析，实时展受害者IP、攻击者IP、XFF、攻击结果、攻击次数、事件类型、威胁等级、联动响应、状态码、确定性等级等20个以上类型。实战阶段的全过程可视溯源分析、总结阶段的值守报告等全过程流程。 |
| 威胁情报共享 | 支持云端与本地威胁情报共享，实时收集同步攻击者IP，并详细展示情报列表，包括IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动同品牌防火墙实现自动封锁。 |
| 溯源中心 | 支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息。 |
| 10 | 报表中心 | 全网安全态势报告 | 可快速生成月度、季度、年度PPT报表，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等，帮助用户高效汇报，体现安全工作价值。 |
| 告警推送 | 告警方式支持邮件告警、短信、微信告警方式。 |
| 11 | 应用中心 | 合规自检工具 | 支持同品牌防火墙、终端安全响应系统、上网行为管理等设备的配置核查并上报结果，提供自动化监测和配置引导。支持已合规基线管控业务安全，实时监测等保差距项和高风险项，避免策略变更导致不合规，有效应对网监不定期抽查和复测场景。 |
| 12 | 设备管理 | 基础特征库升级 | 具备IPS漏洞特征识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、URL库、应用识别库、恶意链接库、白名单库；支持定期自动升级或离线手动升级。 |
| 平台快捷控件 | 支持快捷菜单悬浮控件，平台全部功能可根据使用习惯自定义添加到快捷控件，方便使用，提高运维工作效率。 |
| 接入设备管理 | 支持流量探针统一升级管理，支持监控流量探针与安全组件的运行状态，包含日志传输模式、日志传输量、最近同步信息等。 |
| 管理员角色 | 支持管理员账号的新增、删除、启用、禁用等，支持免登陆及单点登录设置，支持可信IP设置。支持角色的管理范围及页面权限的收敛设置。支持系统管理员、安全保密管理员和安全审计员三个管理员角色。 |
| 13 | 产品资质 | 为保证厂家具备在用户核心业务在紧急情况下的应急响应能力，厂商为网络安全应急服务支撑单位证书（国家级） |
| 要求具备公安颁发的安全管理平台销售许可证要求具备ISCCC IT产品信息安全认证证书要求具备国家版权局颁发的软件著作权登记证书 |
| 14 | 售后服务 | 必须在省内有厂家直属的服务办事机构，提供7\*24小时快速上门服务和2小时内快速响应服务 |

 **2、探针设备技术参数**

| **序号** | **功能及技术指标** | **详细参数** |
| --- | --- | --- |
| 1 | 硬件要求 | 和SIP同品牌，标准2U机架式设备，接口数量≥6个千兆电口、2个万兆光口；硬盘容量≥1T；数据处理性能≥2Gbps，冗余电源 |
| 2 | 部署模式 | 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响 |
| 3 | 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。 |
| 4 | 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意UR监测模式，可完成模式匹配并生成事件，可提取URL记录和域名记录。 |
| 5 | 网站攻击检测 | 支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞等网站攻击检测。 |
| 6 | 敏感信息检测 | 支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤。 |
| 7 | 漏洞利用攻击检测 | 支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Network Device、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击等服务漏洞攻击检测。 |
| 支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex等客户端漏洞攻击检测。 |
| 支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测。 |
| 8 | 异常流量检测 | 支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等（需提。 |
| 支持ICMP、UDP、SYN、DNS等协议外发异常流量检测，支持自定义阀值。 |
| 9 | 僵尸网络行为检测 | 支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测。 |
| 10 | 高级检测 | 支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 |
| 支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。 |
| 支持传输访问检测日志，包括正常访问、风险访问、违规访问。 |
| 支持传输协议审计日志，包括https协议日志、http协议审计日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志、AD域协议审计日志、WEB登录审计日志、FTP协议审计日志、Telnet协议审计日志、ICMP协议审计日志、LLMNR协议审计日志。 |
| 11 | 违规访问检测 | 支持IP，IP组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式。 |
| 12 | 沙盒对接 | 支持将流量还原的文件发送至沙盒分析；可支持第三方沙盒对接。 |
| 13 | 特征库 | 内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。 |
| 14 | 抓包分析 | 支持流量抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式。 |
| 15 | 管理功能 | 支持设备内置简单命令行管理窗口，便于基础运维调试（需提供截图证明）；可实时监控设备的CPU、内存、存储空间使用情况；能够监控监听接口的实时流量情况。 |
| 16 | 产品资质 | 要求具备公安颁发的网络入侵检测系统销售许可证 |
| 17 | 厂商资质 | 厂商具备软件开发成熟度CMMI 5级认证，提供证书复印件并加盖厂商公章；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；厂商需是中国反网络病毒联盟ANVA成员单位；厂商是微软安全响应中心的MAPP计划成员；厂商为国家信息安全漏洞共享平台CNVD用户组成员，提供CNVD官网截图证明并加盖厂商公章；厂商具备云安全成熟度成熟度模型CSA-CMMI 5认证，提供证书复印件并加盖厂商公章； |
| 18 | 售后服务 | 必须在省内有厂家直属的服务办事机构，提供7\*24小时快速上门服务和2小时内快速响应服务 |

**3、安全服务技术要求**

| **序号** | **服务类型** | **内容及要求** |
| --- | --- | --- |
| **1** | 资产识别与梳理 | 投标方需借助安全工具对招标方资产进行识别和梳理，并在后续服务过程中根据识别的资产变化情况触发资产变更等相关服务流程，确保资产信息的准确性和全面性 |
| 投标方需结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新 |
| **2** | 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 |
| 弱口令扫描：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等 |
| 基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况 |
| 勒索病毒事件分析：投标方需分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断否存在勒索病毒攻击等 |
| 挖矿病毒事件分析：投标方需分析是否感染了挖矿病毒/木马；是否处于挖矿状态；根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等 |
| 蠕虫病毒事件：投标方需确认文件是否被感染，定位失陷的代码并进行修复 |
| 针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点 |
| 失陷主机分析：投标方需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议 |
| 潜伏威胁分析：投标方需分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C通道、隐藏外联通道等外联威胁行为 |
| **3** | 问题处置 | 投标方需对发现的问题进行处置，包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等 |
| **4** | 漏洞管理 | 漏洞扫描与验证：投标方需提供不少于每月一次针对服务范围内的资产的系统漏洞和Web漏洞进行全量扫描，并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 |
| 漏洞优先级排序：投标方需提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度 |
| 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 |
| 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 |
| 服务催单：针对服务平台生成的工单，招标方可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促投标方第一时间处理 |
| 漏洞复测：需提供漏洞复测措施，及时检验漏洞真实修复情况。投标方要支持招标方可按需针对指定漏洞，指定资产等小范围进行，降低漏洞复测时的潜在影响范围 |
| 漏洞状态总览：对发现的漏洞建立状态总览机制，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 |
| 最新漏洞预警与排查：投标方需实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。 |
| 最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。 |
| 最新漏洞复测与状态跟踪：由投标方对该最新漏洞建立状态追踪机制；跟踪修复状态，遗留情况。 |
| **5** | 威胁管理 | 结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单 |
| 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 |
| 实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型 |
| 投标方需针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户 |
| 结合威胁情报，投标方需排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固 |
| 投标方需每月主动分析病毒类的安全事件：提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家协助用户查杀病毒 |
| 投标方需每月主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置建议 |
| 投标方需每月主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置 |
| 投标方需每月主动分析失陷类的安全事件并协助用户处置，并提供溯源服务 |
| 策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新 |
| 策略定期管理：投标方需每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到有效的防护效果 |
| 通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗 |
| 通过全网大数据分析，发现有境外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为 |
| 实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。 |
| 针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助招标方快速恢复业务，消除或减轻影响 |
| 入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务 |
| 入侵威胁清除：排查攻击路径，恶意文件清除 |
| 入侵原因分析：还原攻击路径，分析入侵事件原因 |
| 加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵 |
| **6** | 服务水平协议 | 对安全事件服务水平作出承诺：1）从安全日志产生到事件通告给招标方的时间方面，按照国际标准对安全事件的分类分级指南，重大安全事件和较大安全事件的通告时间小于30分钟，一般事件的通告时间少于1小时。2）在未配备投标方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和较大安全事件的遏制影响和处置完成时间小于4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。3）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%。4）在配备了投标方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%。5）以上要求未达标的惩罚措施为：每不达标一次，服务时间延长一周。6）对于特别重大安全事件应启动应急响应机制，10分钟之内云端专家进行响应，同城2小时上门处置，同省4小时上门处置。7）服务期内若发生一次特别重大安全事件，投标方将扣除服务合同金额3%作为赔偿金。 |
| 安全威胁服务水平作出承诺：1）从安全日志产生到威胁通告给招标方的时间方面，高级威胁的通告时间少于30分钟，一般威胁的通告时间少于1小时。2）在未配备投标方的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的处置完成时间少于24小时。3）安全威胁经过服务人员的确认后，高级威胁和一般威胁的判断准确率不低于99%。4）在配备了投标方的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的闭环处置比例达到100%。5）以上要求未达标的惩罚措施为：每不达标一次，服务时间延长一周。 |
| 对安全漏洞服务水平作出承诺：1）在配备投标方的漏洞定期扫描服务组件的情况下，漏洞扫描的频率不低于每30天扫描一次。2）高危可利用漏洞从发现到完成闭环处置的时间少于7个工作日。3）高危可利用漏洞经服务人员确认后的准确率不低于99%。4）高危可利用漏洞的闭环处置比例达到100%。5）对于0day和最新漏洞，从发现漏洞到通告给招标方的时间少于8小时。6）在配备投标方的边界防护服务组件和终端防护服务组件的情况下，对于0day和最新漏洞，在发布相应的攻击POC之后，运营服务将在24小时内遏制漏洞的影响。7）0day漏洞经过服务人员确认后的准确率不低于99%。8）在配备了投标方的边界防护服务组件和终端防护服务组件的情况下，0day漏洞的闭环处置比例达到100%。9）以上要求未达标的惩罚措施为：每不达标一次，服务时间延长一周。 |
| **7** | 服务交付物 | 交付物名称：《安全服务运营报告》，报告频率：每周一次交付物名称：《首次威胁分析与处置报告》，报告频率：一次交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数交付物名称：《安全报告》，报告频率：按需触发，不限次数交付物名称：《综合分析报告/运营月报》，报告频率：每月一次交付物名称：《勒索风险排查报告》，报告频率：每季度一次交付物名称：《季度汇报PPT》，报告频率：每季度一次交付物名称：《年度汇报PPT》，报告频率：每年一次中标后招标方有权要求中标方严格按照上述频率要求提供服务交付物，确保满足招标方安全需求。如中标方未能按时提供，招标方有权终止服务合同，中间产生任何费用由中标方自行承担 |
| **8** | 服务频率 | 7\*24小时持续专家服务，威胁发现及时响应 |