附件 15

濮阳医学高等专科学校采购项目合同履约验收情况

<table>
<tr><td>项目名称</td><td colspan="2">濮阳医学高等专科学校基础网络铺设及安全运维项目（第二标包 安全运维）</td><td>中标单位名　称</td><td colspan="3">郑州云智信安安全技术有限公司</td></tr>
<tr><td>合 同 金 额</td><td colspan="2">485000.00 元</td><td colspan="4">大写：肆拾捌万伍仟元整</td></tr>
<tr><td colspan="2">政府采购项目编号</td><td colspan="5">E4109005080D03145</td></tr>
<tr><td rowspan="6">验收清单</td><td>序号</td><td>产品名称</td><td>规格型号</td><td>单价</td><td>数量</td><td>金额</td></tr>
<tr><td>1</td><td>明御综合日志审计分析平台</td><td>杭州安恒 DAS-LOG-120</td><td>81000.00</td><td>1</td><td>81000.00</td></tr>
<tr><td>2</td><td>AiNTA 流量审计分析平台</td><td>杭州安恒 DAS-ABL-SP800</td><td>77000.00</td><td>1</td><td>77000.00</td></tr>
<tr><td>3</td><td>AiLPHA 高级威胁检测与分析系统</td><td>杭州安恒 DAS-ABL-AXD R1800</td><td>193000.00</td><td>1</td><td>193000.00</td></tr>
<tr><td>4</td><td>安全托管运营服务 MSS</td><td>杭州安恒 MSS-P20</td><td>134000.00</td><td>1</td><td>134000.00</td></tr>
<tr><td></td><td>合计</td><td colspan="4">小写：485000.00 元</td></tr>
<tr><td rowspan="8">验收意见</td><td colspan="6">☑1、供应商提供货物的型号、数量、颜色等是否与中标内容及采购合同内容相符；</td></tr>
<tr><td colspan="6">☑2、供应商是否按照采购合同和承诺的时间、地点交货；</td></tr>
<tr><td colspan="6">☑3、货物安装调试是否完成；</td></tr>
<tr><td colspan="6">☑4、设备是否能够正常运行；</td></tr>
<tr><td colspan="6">☑5、供应商提供的发票是否真实；</td></tr>
<tr><td colspan="6">最终验收意见和需要说明的事项：
合　格 ☑
不合格 □</td></tr>
<tr><td colspan="6">验收小组负责人（签章）：
验收小组成员（签章）：
采购单位（公章）
验收日期：2024 年 3 月 13 日</td></tr>
</table>

1	日志采集探针	★1.硬件规格：标准1U硬件，1个console口，至少含6个千兆工作管理口(1管理口+1HA口+4审计口)，硬盘≥2T，内存≥8G，单电源 ★2.功能扩展： （1）采用解决方案包上传对产品进行功能扩展，无需要代码开发； （2）支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能，Kafka收发支持SSL加密。（提供界面截图） ★（3）支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配； （4）支持系统配置备份自动备份至远程服务器。（提供界面截图） 3.日志收集： （1）支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集； （2）支持使用代理(Agent)方式提取日志并收集，对Agent进行统一管控，包括卸载、升级、启动及停止操作； （3）支持将日志收集策略统一分发； ★（4）支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。（提供界面截图） 4.日志分析： （1）日志支持文本方式输出给第三方平台，进行数据共享； （2）内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展； ★5.支持分词算法的日志解析 （1）可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）； （2）内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景。 6.日志查询：支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 7.脆弱性管理：支持内置73000+条CVE漏洞数据知识库；支持内置数十项符合OWASP的Web漏洞数据知识库。 8.告警功能：支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警； 9.用户管理：用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户； 提供一键式故障排除功能； 10.资产管理：注册用户资产时，提供自动发现识别能力； ★11.支持在IPV6混合网络中进行审计日志资产识别。	1	台

2	流量采集探针	1. 硬件要求：内存：≥16GB；硬盘：可用硬盘容量≥2TB，千兆 RJ45 网口≥6 个 ★2.情报管理：支持显示情报基本信息、情报更新记录，支持查询同步到本地的情报信息。（提供界面截图） ★3.告警归并：支持展示高度聚合告警列表，对告警进行自动归并；支持多维度告警查询，支持威胁告警快速过滤，包括筛选、排除操作。（提供界面截图） ★4.组网划分：支持自定义添加组网配置，并可根据配置对资产信息进行组网划分。（提供界面截图） 5.流量采集 ：支持自定义流量采集策略，包括过滤策略和采集策略，支持根据 IP 和协议进行过滤，包括 DNS、FTP、HTTP、HTTPS、IMAP、KRB5、LDAP、POP3、RDP、SMB、SMTP、SSH、TELNET、TLS 等。 ★6.产品具备对维度深层次检测 APT 攻击方法的能力 7.弱口令检测： （1）页面支持多种类型弱口令策略可选，支持的口令字典库 50000 种以上； （2）支持自定义弱口令字典，可选不同格式弱口令，支持导入自定义弱口令列表； （3）WEB 登录参数灵活可配，支持字符串和正则表达式配置； （4）支持 Base64 编码弱口令和 md5 散列弱口令检测。 8.暴力破解： （1）支持 HTTP、FTP、Telnet、SMB、邮件（SMTP、POP3、IMAP）、RDP、MySQL、Oracle、SQL Server、PostgreSQL、Redis、Mongodb、SSH 等暴力破解检测，SSH 暴力破解支持爆破登录结果判定； （2）支持暴力破解检测策略自定义，支持添加暴力破解白名单功能。 9.扫描策略：支持端口扫描、主机 IP 扫描、Ping 扫射，支持自定义告警阈值。 10.域名检测：支持对 DNS 隐蔽隧道通信和 DGA 域名进行检测，用户可自定义域名检测域名长度和告警阈值，也可以选择是否检测 DGA 域名家族。 ★11.跨三层 MAC 地址获取： （1）支持跨三层 MAC 地址获取，用户可新增指定 SNMP 服务器，配置包括服务器 IP、ARP OID、获取时间间隔、每次获取最大个数、SNMP 版本（V1、V2C、V3）； （2）支持自动识别或手动添加交换机的 MAC 地址并进行识别排除，可自定义配置自动识别的个数阈值。（提供界面截图） 12.数据同步： （1）支持通过 Kafka、syslog 接口向态势感知平台报送流量审计数据与风险告警信息，Kafka 推送支持传输加密，支持 SSL、SASL 认证+SSL、Kerberos 认证+SSL 加密。 （2）支持通过 API 接口向态势感知平台推送资产信息。 （3）支持通过 API 接口向态势感知平台推送三层 MAC 地址信息	1	台
3	安全大数据智能分析平台（态势感知系统）	1.硬件要求：CPU≥2*16 核 32 线程、硬盘≥8T*4 、内存≥32G*8、网卡≥4 千兆电口，2 万兆光口； 2.行为审计与可疑通信检测：支持违规操作、违规访问、违规应用、违规外发等 300 种以上行为审计检测规则，可针对任意单条规则进行启用和禁用。 支持隧道通信、可疑内容、恶意 IP、恶意域名、恶意证书、远程控制等 2000 种以上可疑通信检测规则，可针对任意单条规则进行启用和禁用； 3.扫描探查检测：支持端口扫描、服务扫描、Web 扫描、扫描器指纹检测等 300 种以上的扫描探查检测规则，可针对任意单条规则进行启用和禁用。 4.漏洞利用检测：支持 SMB 漏洞、RDP 漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode 等 6000 种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用。 5.恶意文件检测：支持挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell 等 18000 种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。 6.配置风险检测：支持弱口令风险、明文传输风险、HTTP 配置风险、中间件配置风险、	1	台

		数据库配置风险、服务配置风险等 300 种以上配置风险检测规则 7.主机和账号异常检测：支持端口异常、主机对外扫描、主机对外攻击等主机异常检测能力，对任意单条检测规则支持启用和禁用。 支持登录异常、暴力破解、行为异常等账号异常检测能力，对任意单条检测规则支持启用和禁用。 8.Web 攻击检测：支持 Webshell 请求、XSS 攻击、SQL 注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE 注入、网页篡改、SSRF 攻击等 14 类、8000 种以上 web 攻击检测规则，对任意单条检测规则支持启用和禁用。 ★9.产品具备 CC 攻击的检测方法的能力 10.加密攻击检测 ：支持解密流量检测特定攻击 ★11.支持 AI 规则引擎、AI 智能新型引擎，检测加密流量攻击 12.资产指纹识别：支持 Web 应用类指纹信息识别，识别类型：Web 服务器（OA、企业建站系统、博客、门户、在线阅读等）、Web 组件、Web 中间件、邮件服务器等，识别 Web 应用类型指纹数量 18000+		
4	安全托管运营服务 MSS	1. 资产发现与服务范围内资产管理：服务提供方应通过主动扫描和被动流量识别的方式进行全网资产发现。服务提供方应在服务过程中持续对资产进行标签标记，要求平台具备标签类型、标签名称、标签权重、标签置信度等内容（提供界面截图） 2.互联网暴露面检测：服务提供方应在用户提供的根域名、IP 等信息的基础上，对用户在互联网上暴露的 IP 资产、指纹资产等信息进行搜集，并在人工检查整理后将报告发送至用户。服务提供方应具备专业的红队平台，在服务过程中能够自主选择暴露面搜集内容和深度，如选择全量或常见 CMS、邮箱、Github 信息等（提供界面截图） 3.互联网漏洞管理服务：服务提供方应支持 web 漏洞扫描结果+V 确认，表示该漏洞可靠性达到 90%以上，帮助用户快速的确认和处理漏洞。（提供界面截图）。服务提供方应具备 CVE、CNVD、CNNVD、EXP、POC 等不同标签的漏洞情报、需要关注的重视程度，并能够及时从包括安全客、freebuf、看雪论坛等平台获取安全资讯。（提供界面截图） 4.服务范围内资产威胁检测分析与处置：服务提供方应通过云端安全托管运营平台对服务内资产提供 7*24 小时威胁监测，并分析检测各项安全隐患，包括且不限于漏洞利用、弱密码、Webshell 写入、异常登录、木马回连等安全风险和异常行为。服务提供方应具备策略编排模块，能够及时针对用户提出的需求进行策略编排，包含策略模式、策略条件、策略类型、策略等级等内容（提供界面截图）。 5.安全运营知识库：服务提供方应具备专业内部服务知识库，提供包括攻击、威胁狩猎、风险管理、应急响应在内不少于 7 个维度的运营知识，要求储备内容不少于 3000 万字，方便时刻为用户提供所需的安全运营知识。（提供平台截图）。 6.服务范围：为 20 个核心业务资产提供全年的 7*24 小时安全托管运营服务； （1）含 1 年资产管理服务，基于设备发现的资产与资产台账，为资产重要性进行分级打标； （2）含 1 年 2 次的互联网暴露面检测服务，搜集暴露的 IP、域名、端口等信息。 （3）含 1 年 4 次的互联网开放系统漏洞扫描管理服务，对互联网资产验证与修复跟踪。 （4）含 1 年 7*24 小时的服务范围内资产威胁检测与分析服务。 （5）含 1 年的服务范围内资产事件处置与应急响应服务。 （6）含 1 年 4 次的服务组件调优服务。 （7）含 1 年的情报订阅服务。 （8）含 1 年 2 次的复盘汇报服务。 （9）含按规定频率提供的各服务项报告。	1	年
3 - 等保测评				