**亳州幼儿师范学校态势感知采购项目**

**设备技术参数要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **技术参数及产品性能要求** | **数量** |
|  | 态势感知设备和系统（软硬件一体，设备品牌：长亭科技） | 1 .2U标准机架设备，2\*8核CPU，96GB内存，240GB SSD，4TB数据盘，4个千兆电口（支持拓展万兆口），双电源，业务能力：最大实时分析流量≧1Gbps；  2.支持智能语义分析的漏洞检测，对跨站脚本攻击、SQL注入、命令注入行为进行语义分析检测，并输出安全事件。（提供功能截图并加盖投标人公章）  3.支持通过反弹 shell 检测模型，对执行代理工具shell等黑客发起的加密攻击行为进行深度检测，并输出安全事件。  4.支持 DNS 隧道深度检测；支持对dns2tcp、等DNS隧道构建行为进行识别，并输出安全事件。  5.支持通过Webshell攻击检测模型对常见 Webshell 工具发起的攻击行为进行深度检测，工具类型包含但不限于：蚁剑、冰蝎、哥斯拉等；  6.支持非 HTTP 代理下使用 Earthworm、frp、Ngrok、nps、Stowaway、Termite、Venom 等渗透工具进行远程代理攻击行为检测，并输出安全事件  7.支持 HTTP 代理下使用 ABPTTS、Chisel、reGeorg、Tunna、Neo-reGeorg 等渗透工具进行远程代理攻击行为检测，并输出安全事件  8.支持内网横移手段的检测，如Windows 通过 SMB/DCERPC 远程添加服务、Windows 通过 SMB/DCERPC 共享添加计划任务、通过 PsExec 进行远程控制等，并输出安全事件  9支持内网权限提升手段的检测，如Windows远程权限提升漏洞MS14-068、Zerologon利用漏洞 CVE-2020-1472、远程安装打印机驱动等，并输出安全事件。（提供功能截图并加盖投标人公章）  10.支持内网权限维持手段的检测，如Kerberos 万能钥匙（Skeleton Key），并输出安全事件。（提供功能截图并加盖投标人公章）  11.支持内网环境中敏感行为、危险调用检测，如Kerberos账户爆破、LDAP 敏感操作等，并输出安全事件。（提供功能截图并加盖投标人公章）  12.支持沙箱检测模式、支持windows、linux类型沙箱，支持自定义检测文件类型如文档文件、网页文件、压缩文件等；（提供功能截图并加盖投标人公章）  13.支持恶意文件专项检测，可实时查看恶意文件数量变化趋势；支持内置多个杀毒引擎；支持对恶意文件进行检测，检测的恶意文件类型包括但不限于：病毒、木马、蠕虫、钓鱼程序、黑客工具、漏洞利用代码、恶意宏文档等。检测结果须给出详细的恶意文件事件描述和解决方案，可查看恶意文件类型、文件MD5、文件路径、文件大小等详情信息，支持下载样本文件进行分析。（提供功能截图并加盖投标人公章）  14.支持webshell专项检测，可查看webshell攻击数量变化趋势，能够详细展示webshell文件路径、发现时间以及webshell文件详情信息，给出详细的 webshell 事件描述和解决方案。（提供功能截图并加盖投标人公章）  15.支持通过挖矿分析模型，对主机与矿池通信连接行为、协议等进行深度检测，检测矿池包含但不限于：XMRig工具、Stratum 挖矿协议等，并输出安全事件；  16.支持通过登录检测模型，对登录过程中输入的弱口令进行深度检测，并输出安全事件  17.支持通过 ICMP 隐蔽隧道检测模型，对未知 ICMP 隐蔽隧道进行分析，并输出安全事件  18.支持通过 DGA 域名检测模型，对黑客利用随机字符生产 C&C 域名逃避检测的行为进行深度检测；检测模型能够覆盖基于算数算法编码、基于哈希表示、基于辞典组合、基于排列组合等方式生成的随机域名及黑客行为，并输出安全事件。  19.支持沙箱行为签名检测，根据主机或网络行为判断其是否为恶意文件，支持显示沙箱内样本运行截图；（提供功能截图并加盖投标人公章）  20、支持还原邮件附件，对邮件附件进行文件检测。  21、支持从攻击者、受害者、威胁类型、威胁名称等多个视角对威胁事件进行事件自动聚合;支持在第一次聚合之后再按照攻击者、受害者、威胁类型、威胁名称进行二次威胁事件自定义聚合，支持根据攻击阶段和攻击结果等快速筛选查看。（提供功能截图并加盖投标人公章）  22、可对告警相关数据包进行在线解码分析，支持wireshark过滤语法对数据包进行过滤查询  23、支持告警快速筛选和高级筛选两种模式；快速筛选至少包含20个以上字段对告警进行快速筛选；高级筛选功能字段筛选逻辑至少包括等于、不等于、包含、不包含、模糊匹配、精准匹配多种方式，逻辑关系至少包含AND和OR，可以根据多条件组合方式对告警进行精细匹配查询（提供功能截图并加盖投标人公章）  24、支持双向流量检测规则配置，支持多种协议（HTTP、TCP、UDP 等）的逐流逐包检测，配置检测字段包括但不限于method、host、user\_agent、cookie、referer、header、body 等（提供功能截图并加盖投标人公章）  25、支持手动添加和文件导入资产；支持字段包括：资产名称、资产IP、资产类型、负责人、地理位置、重点资产和备注；并支持在告警列表的攻击IP和受害IP能够关联出相关资产信息。  26、支持命令执行成功研判，对攻击事件进行分析，判断此次攻击结果是否为失败  27、支持弱口令登录结果研判，对弱口令登录事件，判断弱口令是否有效  28、支持 SQL 注入成功研判，对 SQL 注入类事件进行分析，判断此次攻击结果是否为成功  29、支持反连成功研判，对反弹 shell、ssrf、jndi 等攻击，提取反连 IP/域名，分析受害主机是否连接该 IP/域名，判断此次攻击结果是否为成功  30、具备从流量中还原文件并进行威胁检测的能力，文件类型包括 doc、docx、ppt、pptx、xls、xlsx、wps、rtf、pdf、exe、zip、7z、rar、gzip、tar、pyc、py、html、swf、jpeg、jpg、png、pcap、class、jar、torrent、apk、chm、hlp、bz2、cab、flv、tiff、rpm、deb、msi、gif 等格式。  31、每年需和客户提前沟通好时间，配合好客户进行攻防演练2次，每月最少一次的安全设备巡检出具巡检报告。  32.可以联动现有网络安全设备，与联动设备一起可实现：支持所有线路应用流速趋势、流量管理状态、连接监控信息实时提供在线用户信息、应用流量排名、连接排名等；支持实时查看各带宽通道的使用情况；支持实时显示当天的安全状况、最后发生安全事件的时间、类型、总次数、源对象，Web 访问质量检测；（提供功能截图并加盖投标人公章）。  33、中标后7个工作日内需要投标方提供测试设备针对以上参数进行逐一比对，有虚假应标项，我校有权作废标处理。  34、为提升态势感知设备功能性和实际防护效果，要求所投产品的厂商具有中国通信企业协会颁发的通信网络安全服务能力评定证书-安全培训（二级）、具有中国网络安全审查认证和市场监管大数据中心颁发的信息安全服务资质-信息安全应急处理服务资质（一级）及信息安全服务资质-信息安全风险评估服务资质（一级）（请提供以上证书扫描件并加盖公章）。  35、该项目需提供不少于5年的免费运维及质保，项目运维及质保结束后，后续每年运维费用不高于项目中标价格的5%。  36、项目验收及项目运行后，有亳州市信息化专家库随机抽取至少3名专家进行验收。  37、项目安装运行后，需同时对我校所有信息化终端设备进行安全检查，并出具检查报告。  38、设备安装走线，不得存在跳线和飞线情况，每根线两端需有对应标签。  以上支持的所有功能无需定制开发，投标人必须保证应答真实有效，中标后7个工作日内要进行POC验证，与投标应答不符合，我校有权按虚假应标处理处罚。 | 1套 |