|  |  |  |
| --- | --- | --- |
| **要求类别** | **技术要求** | **招标要求** |
| 硬件配置要求 | 硬盘容量 | ≥ 250GB 固态硬盘、≥4TB机械硬盘 |
| 设备接口 | ≥7个10/100/1000BASE-T接口(其中2个管理接口，4个数据接口，1个BMC接口)，4个SFP插槽 |
| 电源 | 双电源 |
| 尺寸 | 标准2U机架式 |
| 流量采集能力 | 硬件部署要求 | 需支持旁路镜像部署、分布式部署等模式，至少支持4个端口镜像流量汇聚 |
| 网络流量侦测要求 | 网络流量侦测模块，要求对流量进行解析提取通用协议的全量字段，并将提取信息存储到后端数据存储端，使用高速索引技术，支持高效检索；支持实时在线分析能力 |
| 协议解析要求 | ★支持对网络协议数据进行协议日志与行为日志的分析。协议日志默认解析IPFIX(TCP/UDP)，HTTP，DNS，SSL/TLS，FTP，TELNET，ICMP，MYSQL等；行为日志分为邮件行为和登陆行为：登陆行为默认解析HTTP，FTP，MYSQL，NTLM，KERBEROS，SSH，SMTP，POP3，RADUIS等；邮件传输行为默认解析POP3和SMTP； |
| 威胁分析能力要求 | 检测范围及能力 | ★安全分析方法应包含基于特征规则、统计分析、机器学习等方式进行检测；支持风险事件按照攻击链模型分类和评级（需提供相关功能截图证明） |
| 检测范围包含但不限于：Web应用攻击、弱口令、暴力破解、扫描与爬虫、数据库攻击、敏感信息泄露、恶意通信流量、内网渗透、通用应用漏洞攻击（如勒索病毒等）、恶意软件、后门识别、异常协议 |
| ★支持内置多种风险检测模型：包含网络行为监测模型，监测HTTP协议与常见协议；智能机器学习模型；统计分析模型，对常见的端口扫描和暴力破解等行为进行检测；支持场景化策略配置，支持多个安全事件的关联分析；威胁情报模型，对恶意IOC监控，支持自行导入情报库（需提供相关功能截图证明） |
| 溯源分析 | 风险描述 | ★支持风险事件多维度检索，维度包含：风险等级、风险类别、自定义时间范围、风险名称、关键字、操作系统、服务器IP、端口及服务、来源IP、端口及服务、开发语言和框架，支持自定义风险关联模型（需提供相关功能截图证明） |
| 调查画布 | ★系统支持对安全事件进行溯源，提取各类网络IoC信标，如IP、URL、邮箱、域名、用户名、文件等，并以可视化的方式描述网络实体间的行为，绘制安全事件调查网络图（需提供相关功能截图证明） |
| 检测能力 | 恶意文件检测方式 | 支持对静态特征的分析，包括如PE文件特征、文件系统函数特征、注册表、异常服务等检测、多杀毒引擎检测、动态沙箱行为检测、动态API行为检测、文件网络行为分析，如主机行为通信、DNS通信、HTTP通信、SMTP通信、IRC通信等、信誉模型检测，包括敏感API检测、敏感字符串检测、基于机器学习的多模型融合计算分析。 |
| 运行环境 | 模拟window 32/64、Linux等常见操作系统，自适应运行环境 |
| 数据对接 | 风险上送 | ★支持级联部署方案下的风险数据上送功能，支持以syslog以及API形式进行风险数据上送，同时可根据实际需求配置上送策略，包含风险等级、风险名称、源目IP等（需提供相关功能截图证明） |
| 其他功能 | 操作日志 | 支持操作、登陆、升级等日志记录、存储和导出功能，支持CSV导出 |
| 支持操作日志详细记录，按操作用户、操作时间、操作IP、执行操作等 |
| 设备监控 | 支持对设备自身以及流量采集器的CPU、内存、磁盘空间、网络流量等参数使用状态以及可用性进行监控和报警 |
| 产品资质 |  | 《计算机信息系统安全专用产品销售许可证》 |
| 《中华人民共和国国家版权局计算机软件著作权登记证书》 |