采购招标项目参数要求

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项目名称 | | | 安全感知运营中心建设项目（1台/套） | | | | | 采购编号 |  |
| 供货时间 | | | 2020.09.30 | | | | | 供货地点 | 吉林大学珠海学院 |
| 售后服务要求 | | | 3年 | | | | | 安装调试要求 | 有现场培训和演示 |
| 项目概述：吉林大学珠海学院信息中心在现有安全体系上进行升级建设，从防御层次向“持续检测、快速响应”步进，打造一站式的“预防，检测，响应，加固”的四维服务，真正做到“安全态势可感知、安全威胁可预警、异常行为可监控、安全价值可呈现”。1）对全网业务系统核心资产进行识别，梳理分支用户与核心资产的访问关系；  2）对绕过分支边界防御的进入到内网的攻击进行检测，以弥补静态防御的不足，第一时间发现已发生的安全事件；  3）对内部用户、业务资产的异常行为进行持续的检测，发现潜在风险以降低可能的损失；  4）对业务资产存在的脆弱性进行持续检测，及时发现业务上线以及更新产生的漏洞及安全隐患；  5）将全网的风险进行可视化的呈现，看到全网的风险以实现有效的安全处置；  6）建立流程化的通报预警机制对网络安全风险进行通报，并以工单的形式实时下发， | | | | | | | | | |
| **重要技术参数（必填）** | | | | | | | | | |
| 安全感知平台参数 | | | | | | | | | |
| 技术指标 | | | | | 指标要求 | | | | |
| 硬件性能 | | | | | ★尺寸:2U架构,硬盘容量≥32TB,CPU≥16核心,内存≥96G内存,接口数量≥4个千兆电口、1个串口、3个USB口,电源:冗余电源 | | | | |
| 大屏可视 | 综合安全态势大屏 | | | | 支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势、设备运行态势；支持页面跳转到对应态势大屏，并具备大屏告警能力。 | | | | |
| 资产态势 | | | | 支持大屏展示资产态势，包括服务器操作系统分布、服务器开放服务TOP5、最新资产动态、最近变动资产。 | | | | |
| 3D网络攻击态势 | | | | 支持3D地球大屏展示网络攻击态势，包括攻击次数、遭受攻击资产组、攻击源地址、攻击源IP、攻击手段排行、遭受攻击服务器排行；支持境外、境内切换。 | | | | |
| 横向威胁态势 | | | | ★支持大屏展示横向威胁态势，包括业务与终端访问、发起威胁终端TOP5、遭受威胁业务TOP5、访问趋势图；支持不同颜色标注横向攻击、违规访问、可疑行为、风险访问等行为（需提供截图证明并加盖原厂商公章）。 | | | | |
| 大屏轮播 | | | | ★支持不同视角展示全网安全态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势、正常横向访问监控态势、正常外连监控态势、设备运行态势等13个独立的大屏展示功能；支持大屏轮播，可自定义播放顺序（需提供截图证明并加盖原厂商公章）。 | | | | |
| 资产中心 | 总览 | | | | ★支持对全网资产总览分析，包括资产概览、服务器运行状态、资产统计，其中资产概览包括7天即将退库资产、全部资产数、核心资产数、资产组数、服务器数、终端数；服务器运行包括服务器离线TOP5、服务器开放端口TOP10、服务器应用TOP5；资产统计包括资产组TOP5、资产来源TOP5、设备类型TOP5、操作系统分布、7天内即将退库资产；（需提供截图证明并加盖原厂商公章） | | | | |
| 脆弱性感知 | 脆弱性总览 | | | | 支持业务脆弱性风险分布展示，包括不同严重级别业务分布，漏洞类型分布，漏洞整体态势等。 | | | | |
| 弱密码 | | | | ★支持检测20类以上常见协议的弱密码，包括FTP、LDAP、VMWARE、ORACLE、REDIS、Elasticsearch等协议，检测信息包含账号、密码、服务器、所属分支和业务、类型、最近发现时间等；支持筛选管理员账号与是否登录成功，并支持导出弱密码报告（需提供截图证明并加盖原厂商公章）。 | | | | |
| 漏洞报告 | | | | ★支持流量实时分析漏洞功能，漏洞类型包括配置错误漏洞、OpenSSH漏洞、OpenLDAP、数据库、Web应用等；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（需提供截图证明并加盖原厂商公章）。 | | | | |
| 分析中心 | 威胁分析 | | | | 支持外部威胁分析，包括高危攻击、残余攻击、暴力破解、成功的事中攻击、邮件威胁、文件威胁、外部风险访问。 | | | | |
| 支持横向威胁分析，包括横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包括发起横向威胁主机TOP5、遭受横向威胁TOP5、横向威胁类型分布、横向威胁趋势。 | | | | |
| 挖矿专项检测 | | | | ★支持挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计（提供产品功能截图）。 | | | | |
| UEBA异常行为分析 | | | | 支持服务器行为分析建模，具备独立页面展示行为引擎学习的天数、异常行为与异常服务器数量，并对异常行为进行举证描述；支持对业务服务器内网横向被访问、横向主动访问、外连等建立行为基线，包括访问流量趋势、访问次数趋势、自定义非正常时间段、常见访问源网段、访问源主机、应用TOP5、目的端口TOP5等，提前发现未知异常行为 | | | | |
| ★支持不同场景下数据库异常模型的算法编辑，可选择稀有值检测算法、ZScore异常检测算法、箱线图异常检测算法；可将不同类型的算法应用到不同的资产（需提供截图证明并加盖原厂商公章）。 | | | | |
| 横向访问分析 | | | | ★支持横向访问服务器流量分析，包括TOP5应用流量趋势、TOP5协议趋势；支持服务器视角和来访分支视角，其中服务器视角可展示服务器IP、总流量、源IP数量、应用TOP10、协议端口TOP10、连接失败数、最大并发，并支持以表格形式导出数据（需提供截图证明并加盖原厂商公章）。 | | | | |
| 重保中心 | 外网暴露面梳理 | | | | ★支持内网对外服务器外网暴露面分析，包括内网IP、资产名称、所属资产组、域名/URL、外网IP、策略已开放、实际被使用、关联防火墙、关联应用策略、存在风险、处置状态等，并支持导入与导出（需提供截图证明并加盖原厂商公章） | | | | |
| 核心服务器梳理 | | | | 支持核心服务器暴露面分析，包括内网IP、资产名称、所属资产组、策略允许访问、策略已开放、实际访问、实际被使用、关联应用控制策略、存在风险、处置状态等，并支持导入与导出 | | | | |
| 联动响应 | 安全组件接入展示 | | | | ★支持接入云眼、潜伏威胁探针等设备；支持在页面中显示安全组件接入的数量和状态（需提供截图证明并加盖原厂商公章）。 | | | | |
| 云眼防护联动 | | | | ★要求必须支持本单位云眼（网站防护服务）数据接入平台。 | | | | |
| 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。 | | | | |
| 深度检测引擎升级 | | | | ★具备安全日志分析引擎、DnsFlow行为分析引擎、HttpFLow分析引擎、NetFLow分析引擎、MailFLow分析引擎、SmbFLow分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等；支持定期自动升级或离线手动升级（需提供截图证明并加盖原厂商公章）。 | | | | |
| 接入设备管理 | | | | 支持安全探针统一升级管理，支持监控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。 | | | | |
| 分支权限管理 | | | | ★支持自定义分支管理权限，分支管理员具备独立的管理页面，只能管理和查看所属分支资产的安全信息；具备完整的功能展示，包括监控中心、处置中心、分析中心、资产中心和报告中心；总部管理员支持查看全局的安全信息，支持页面跳转各个分支的独立管理页面（需提供截图证明并加盖原厂商公章）。 | | | | |
| 开放共享 | | | | ★支持通过RESTful API接口形成对平台数据资源的“开放”与“共享”，第三方平台可获取受监控IP组、资产信息、风险业务与终端、漏洞详情、弱密码和明文传输等信息，实现数据更大价值（需提供截图证明并加盖原厂商公章）。 | | | | |
| IPV6管理 | | | | 支持IPV6平台管理，审计日志支持IPv6。 | | | | |
| 潜伏威胁探针 | | | | | | | | | |
| 技术指标 | | 指标要求 | | | | | | | |
| 品牌要求 | | ★与安全态势感知系统为同一品牌 | | | | | | | |
| 硬件性能 | | 性能参数：吞吐性能≥1Gbps。 硬件参数：规格：1U，内存大小≥4G，硬盘容量≥64GB SSD，电源：单电源，接口≥4千兆电口+2万兆光口SFP。 | | | | | | | |
| 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 | | | | | | | |
| 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。 | | | | | | | |
| 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。 | | | | | | | |
| 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。 | | | | | | | |
| 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（需提供截图证明并加盖原厂商公章）。 | | | | | | | |
| 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、VNC等协议暴力破解检测。 | | | | | | | |
| 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（需提供截图证明并加盖原厂商公章）。 | | | | | | | |
| 支持ICMP、UDP、SYN、DNS等协议外发异常流量检测，支持自定义阀值。 | | | | | | | |
| 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。 | | | | | | | |
| 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（需提供截图证明并加盖原厂商公章）。 | | | | | | | |
| 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。 | | | | | | | |
| 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（需提供截图证明并加盖原厂商公章）。 | | | | | | | |
| 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 | | | | | | | |
| 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 | | | | | | | |
| 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（需提供截图证明并加盖原厂商公章）。 | | | | | | | |
| 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。 | | | | | | | |
| 部署 | | 支持多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台 | | | | | | | |
| 资质要求 | | | | | | | | | |
| ★售后服务要求 | | 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(官网上必须可查询到办事机构地址) | | | | | | | |
| ★产品资质 | | 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中国国家信息安全产品认证证书  要求具备国家版权局颁发的软件著作权登记证书 | | | | | | | |
| ★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  厂商具备云安全成熟度成熟度模型CSA-CMMI 5认证， | | | | | | | |
| 申报人 | | | |  | | | 单位负责人 | |  |
| 实验室与资产管理处 | | | | | |  | | | |