|  |
| --- |
| **校园网大数据安全预警与态势感知分析平台** |
| 技术指标 | 指标要求  |
| 性能指标 | 硬件性能 | 2U/2物理CPU 12核\*2/内存256GB/硬盘4TB\*6/2GB RAID卡/冗余1+1电源模块/1G RJ45\*4/滑轨；支持通过多种类型的安全、泛安全类数据接入采集，应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员等数据。 |
| 软件性能 | ★平台中的安全数据，包括告警数据、资产数据、工单等至少20种可共享给第三方系统，实现数据共享和交换；[（要求提供截图或API接口文档并加盖厂商公章）](#证明材料1)；同时支持原始日志、标准化数据、告警数据≥3种数据的共享和交换。 |
| 大屏可视 | 安全态势可视化 | 支持大屏展示综合安全态势，包括资产风险态势、外部威胁态势、安全运营态势、业务资产外连态势、内网威胁态势、网站安全态势等，支持页面跳转到对应态势大屏，并具备大屏告警能力。 |
| 威胁感知 | 威胁感知模块 | 服务所依托的平台具备教育部门、CNVD、漏洞盒子等机构的第三方安全威胁接入和自动解析功能（需提供证明文件）；★可以实现与教育行业信息安全监测保障平台对接服务，以便于漏洞信息的及时发现和预警处理，提供满足实际要求的有效测试证明文件； |
| 安全应用和运营 | 资产管理 | 支持通过流量无侵入式自动发现资产，支持发现终端、Web服务器、DNS服务器、邮件服务器、FTP文件服务器等类型≥5种； |
| 系统引擎包含：大数据实时分析系统、用户异常行为分析系统、深度感知智能引擎、安全事件智能研判引擎、安全自动响应编排引擎；通过智能分析研判识别出真正有效的攻击和事件，结合校园网实际场景进行全面溯源与响应处置，实现安全运营和管理的闭环，提供上述系统引擎的详细描述并与学校网络架构相结合的价值呈现方案并加盖原厂公章； |
| 支持资产信息的全量导入导出，支持从资产管理平台同步资产。 |
| 智能检索 | 支持对原始日志数据、安全告警数据进行分类检索，从检索结果可关联威胁情报和资产信息并一键跳转；支持检索结果导出（不少于10000条），导出内容字段可自定义选择，支持excel或CSV格式。（要求提供截图并加盖公章） |
| 数据字典管理 | 支持管理系统中原始日志、安全事件、安全告警的所有字段和取值，每个字段均有清晰的说明； 支持数据标准管理，用户可以根据实际需求，对字典进行编辑，支持手动修改、增加或删除相应的字段。★实现实体间网络互访关系的多级钻取，支持>10跳的流量关联关系分析，支持通过端口、协议、异常访问类型过滤关联关系。（要求提供截图并加盖公章，验收时核对） |
| 安全域视角 | 支持安全域维度展示安全风险，包含安全域列表、安全域排名等信息 |
| 威胁情报 | 威胁情报 | 支持通过离线导入或手动编辑添加的方式，形成本地威胁情报，允许用户自建行业情报库，并实现情报库的增删改查、导入、导出功能；（要求提供截图并加盖公章）；支持统计情报源碰撞命中情报数量，针对任意单条无效情报可实现禁用。 |
| 安全分析能力 | 分析模型与指标管理 | ★平台应内置包括规则模型、关联模型、统计模型、情报模型、离线模型等在内的≥5大类安全分析模型，各类内置分析模型总条目数应不少于1400条，情报规则不少于870000条；（要求提供截图并加盖公章） |
| ★模型可通过串并联方式组合编排，前一个模型的输出可以作为后一个模型的输入，支持分析模型编排层级>10层。（要求提供截图并加盖公章） |
| 支持统计规则建模，通过统计规则建模，在指定的时间范围内，对符合过滤条件的日志中数字类字段进行求和，将其与阈值进行比较以发现异常威胁事件； |
| AI高级分析 | ★平台内置不少于8种机器学习分析场景模型，可检测发现勒索挖矿告警数异常、安全设备日志数异常、网络会话数异常、域名请求数异常等特定场景条件下的安全态势异常；（要求提供截图并加盖公章，验收时核对） |
| 支持时间序列、UEBA、Bayes、随机森林等长周期高级机器学习算法；  |
| 支持自定义部署AI机器学习模型，允许用户选用的高级机器学习算法不少于4种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助用户发现潜在的安全风险。（要求提供截图并加盖公章）； |
| 具备文件威胁鉴定模块,集成静态文件检测引擎和智能分析检测引擎，有效识别流量与邮件中的恶意文件并生成文件威胁分析报告 |
| 支持发现主机发送可疑附件的邮件行为、伪造发件人发送邮件、发送钓鱼网站邮件和垃圾邮件等行为；支持对恶意邮件详情分析，包含收件人账号、发件人账号、附件名称、病毒名称、恶意链接名称等。 |
| 仪表盘 | 支持可视化图表类型>=15种，包括但不限于时序图、饼图、柱状图等；可视化图表可通过拖拽配置组装成仪表盘，仪表盘不少于7种布局类型，每张仪表盘可包含>=50个可视化图表； |
| 可视化图表支持导出WORD、PDF； |
| 安全事件检测 | ★基于内置安全模型，实现如下安全事件与场景的检测： 拖库行为、0day攻击行为、弱口令、暴力破解、Web攻击行为、邮件攻击行为、文件威胁、木马回连、DoS攻击、SMB行为、违规登录行为、黑产黑链、隐蔽信道通信、FTP异常行为、恶意DNS通讯 、设备性能异常等。（要求提供截图并加盖公章） |
| 全流量审计与潜伏型攻击检测 | 支持全流量审计，包含网络第2-7层数据流量； 实现对关键字、数据来源等的自定义，通过内容深度匹配流量中的敏感信息，并对敏感信息快速定位，实现对敏感信息访问行为的有效监测；识别网络中WEB、QQ、迅雷等各种应用的登录行为，提取登录IP、登录账户、登录网站域名等登录信息。 |
| ★支持对可疑文件进行虚拟执行，支持文件上传检测，有效识别网络流量中的恶意文件（僵木蠕）、病毒等威胁并生成完整沙箱分析报告；（要求提供截图并加盖公章）支持SHELLCODE检测，可通过分析文件中的二进制代码，定位到文件溢出攻击的代码，并能定位到APT攻击中的0DAY攻击； |
| ★支持从 HTTP、FTP、SMB、SMTP、POP3等协议中还原>20种文件格式，包括但不限于doc, xls, ppt, swf, pdf, java, rar, zip, rar, exe, vbs, scr, html，js等文件格式。（要求提供截图并加盖公章） |
| 通报工单预警 | 通报总览 | 支持统一的安全运营工作台，在工作台可以集中查看当前用户的待办工单、最新通报预警状态； |
| 工单举证 | 工单详情与备注支持多种内容格式，包括但不限于文字、图片、超链接、表格、代码片段、附件等类型；支持工单举证信息一键溯源，工单处置人员可以直接定位到工单关联的原始信息进行查看；（要求提供截图并加盖公章） |
| 通告预警模块 | ★对学校整体的安全态势、通告流程等进行可视化展示；集资产梳理、监测预警、安全防护、通报考评、应急处置于一体，满足学校自身的安全管理。信息系统的安全管理可以开展二级监管模式，含已通告、待处置、待审核事件数量，单位安全事件整改率以及安全威胁分布等，以上须提供完整的功能设计方案和原厂省内教育行业案例合同复印件加盖原厂公章。 |
| 情报预警 | 支持通过安全告警自动派发工单到对应的安全管理员，支持自定义编辑预警信息内容；支持将预警信息直接转为内部通报，支持将通报内容作为工单定向指派。 |
| 报告中心 | 分析报告 | ★支持用户自定义编辑报告模板，根据实际的业务需求自定义统计分析的指标对象，生成有针对性的分析报告，安全分析中的所有字段内容，都可以作为报告的统计对象，并自定义时间范围实现报告导出。（要求提供截图并加盖公章） |
| 黑白名单 | 支持通过黑白名单功能对分析对象进行过滤筛选；支持通过任意字段进行组合，配置筛选条件并生成黑白名单过滤规则，支持规则数≥100条。 |
| 系统管理 | 运维监控 | 支持大数据平台本身的计算、存储资源利用率监控；支持数据集与数据索引健康度监控；支持对平台各组件运行健康状态的集中监控。 |
| 用户管理 | 提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持根据对象属性自定义划分系统管理角色和一般用户角色，按照数据和功能分级灵活设置用户权限。 |
| 系统恢复 | 支持安全模型的启用状态恢复出厂设置；支持通过权限认证实现数据恢复出厂设置。 |
| 资质要求 | 厂商资质 | 为更好的提供相关定制和平台交付能力，原厂具有中国信息安全测评中心颁发的信息安全服务资质-安全工程类（三级）；★原厂具有CMMI能力成熟度模型五级证书；提供有效证书的复印件。 |
| 服务要求 | 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(官网上必须可查询到办事机构地址) ；提供平台日常维护、规则模型开发、安全事件分析研判及漏洞核验相关工作，须提供结合实际网络架构详细的测试运维及算法方案。 |
| 服务要求 | 原厂商应具有专业的大数据安全分析团队和云安全团队，需提供至少3份由中国信息安全测评中心认证的CISP-BDSA（大数据安全分析师）资质证书；原厂商提供至少3份中国信息安全测评中心认证的CISP-CSE（云安全工程师）资质证书。 |
| **2、综合日志审计模块探针（软件）** |
| 性能指标 | 性能指标 | 软件不依赖于设备或系统自身的日志系统；审计工作不影响被审计对象的性能、稳定性或日常管理流程；审计结果存储于独立存储空间；支持审计200个日志源； |
| 部署服务模式 | 旁路部署，日志源网络可达。支持与信息管理平台数据安全兼容；提供不少于三年的原厂7\*24小时上门现场服务支持；提供制造厂商CMMI L5认证证书；提供有效证书的复印件。 |
| 功能要求 | 采集方式 | ★日志采集方式应支持但不仅限于Syslog、kafka、ftp、部署代理等4种方式（需提供截图证明并加盖原厂商公章）；支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等（提供截图证明）。 |
| 采集内容 | 支持采集异构设备的日志数据，实现包括但不限于安全类、网络类、应用服务器类、操作系统类等接入采集。★内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等；5 大类 50 子类的安全分析场景（提供截图并加盖厂商公章）。 |
| 日志解析 | 支持接入应用服务器的性能类数据，包括但不限于CPU、内存和磁盘的使用状态数据；内置解析规则支持厂商>200家，支持解析日志设备型号>2000种；无需配置解析规则与设备日志对应关系，自动完成解析。 |
| 日志分析 | 支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以CVE、Bugtraq、OWASP公开协议和标准为为基础（提供第三方检测报告）； |
| 安全评估 | 具备安全评估模型，评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件（提供截图并加盖厂商公章）； |
| 日志发送 | 支持将采集的日志发送给安全感知平台以及第三方日志收集平台。★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；支持kafka日志接收转发、大数据安全域同步、沙箱报告转发等大数据联调功能；提供详细的配置方案和培训计划 |
| **3、安全溯源分析系统探针** |
| 性能指标 | 性能规格 | 软硬一体化2U标准机架式设备；电源：1+1冗余电源；接口数量：标配6个；MTBF 大于65000小时； |
| 部署模式 | 旁路镜像模式部署，不影响服务器处理性能和网络架构；分布式部署：支持分布式部署，管理中心可实现告警统一管理，添加和删除探测器；自定义配置：支持根据添加探测器情况，自定义探测器名称、发送时间、发送目录等信息，并可显示不同探测器的IP、版本、状态和最近24小时的风险信息（提供截图证明）；支持IPv4和IPv6网络环境下的部署，可同时对IPv4和IPv6流量分析检测； |
| 功能要求 | 审计功能 | 支持全流量审计，包含网络第2-7层数据流量；可选择特定协议或IP地址自定义检测，自定义IP地址访问监测，并详细记录所有的审计数据包，可展现审计数据包的时间、客户端IP、服务端IP、应用层协议、报文、返回码、详细信息等； |
| 攻击溯源 | 支持大屏展示风险较为严重的事件，并进行攻击溯源，包括攻击主机个数最多的情报事件TOP10、威胁情报告警类型分布、3D攻击关系图、威胁活动（弱点探测、渗透入侵、获取权限、命令与控制、数据盗取）；支持按IP搜索关联的攻击事件，包括攻击拓扑图、攻击者基本信息、被攻击者信息、攻击过程（攻击过程列表内容包括时间、攻击者、被攻击者、攻击链阶段、风险标签、攻击次数），提供截图证明； |
| 敏感信息识别 | 支持对指定时间周期内HTTP、FTP、SMTP、IMAP、POP3等协议传输的文件进行分离并审计，并可对文件进行本地化存储或者发送至其他文件分析平台；敏感信息识别：实现对关键字、数据来源等的自定义，通过内容深度匹配流量中的敏感信息，并对敏感信息快速定位，实现对敏感信息访问行为的有效监测；登录信息识别：识别网络中WEB、QQ、迅雷等各种应用的登录行为，提取登录IP、登录账户、登录网站域名等登录信息；支持私网IP地址或网段的地理位置配置，在风险信息中按实际配置数据，展示对应IP地址的地理位置信息。 |
| 加密流量解析 | 支持对HTTPS流量的解析还原；流量代理分析：处理和分析第三方接入流量，满足用户对其他平台流量无法分析溯源需求（提供截图证明）； |
| 数据同步 | ★支持与信息安全管理平台进行数据同步，同步信息包括安全域、内IP等；支持前端可视化配置管理接口、监听接口，包括修改IP地址、启用禁用监听接口等（提供证明文件）； |
| 本地离线情报 | 内置离线高可信威胁情报库，应用远控类型的情报指标（IOC，Indicator of Compromise）对僵尸主机和僵尸网络进行精准检测。高可信威胁情报库还可以通过云端实时更新，始终保持最新状态，准确发现并定位失陷主机； |
| 一键排错 | ★支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。（提供截图证明）； |
| 告警方式 | ★支持kafka、短信、邮件、syslog、ftp、钉钉等告警方式，支持对kafka、syslog发送的风险信息进行AES加密传输，支持同时发送多人、单条发送、发送统计等高级告警功能（提供截图证明）； |
| 服务要求 | 提供24小时支持热线；本地应急响应时间<=2小时。[国家安全应急服务支撑单位证书](#_国家安全应急服务支撑单位证书)（国家级），提供证书复印件加盖厂商公章。提供2人次8x3学时现场安装部署培训，要求提供2人次8x3学时产品技术培训。具备中国信息安全测评中心信息安全服务资质证书（安全工程类三级）；提供重大事件应急响应预案，提供对于新发现的病毒、零日漏洞，厂商能够于2小时内作出响应。 |
| **4、安全服务** |
| 1、应急处置服务；学院安全管理员组织架构梳理与平台资产导入关联分析；2、通过资产识别、脆弱性识别、风险分析、威胁识别等规范化流程实现对业务系统安全风险评估；对学校指定业务系统进行风险评估与渗透测试，全面检测并整改系统的漏洞，并形成完整的评估报告，服务人员具备信息安全等级保护检查工具箱的操作服务能力；3、使用专业的具有自主知识产权的扫描工具，对校内主要信息系统的网站WEB漏洞扫描、操作系统漏洞扫描和数据库漏洞扫描三个层面进行脆弱性评估；配合学校在网络安全宣传周进行相关的网络安全攻防意识培训，提升学生网络安全意识、实践能力和防护技能。具备教育系统网络安全保障专业人员（ECSP）培训能力，提供不少于2个的培训名额。 |