**湖南杂交水稻研究中心网络安全设备与服务采购项目需求清单**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **意向品牌** | **数量** | **单位** | **单价** | **合计** | **技术参数及功能要求** |
| 1 | 互联网安全访问服务 | 深信服、天融信 | 1 | 项 |  |  | 1、提供上网管控与安全防护融合的互联网安全访问服务，包含上网认证、访问控制、行为监控、外发管理、行为审计、统计报表、IPS、防病毒、SSL内容检测、恶意URL过滤、恶意IP过滤、恶意域名检测、威胁情报云查等功能以及特征库三年升级服务。2、带宽性能指标2.1、岳麓山实验室、杂优中心办公区使用≥500M性能的引流与云端安全分析服务。2.2、原水稻所办公楼、长沙县基地使用≥300M性能的引流与云端安全分析服务。3、平台部署要求：3.1、互联网安全访问服务平台应采用SaaS服务模式交付，提供SaaS统一门户，门户内服务目录包含但不限于：互联网应用审计与管控、入侵防御、病毒防护、准入与身份管控、带宽控制、威胁情报防护、数据泄漏防护等能力；即开即用，可随时根据分支单位实际需求灵活扩展。3.2、支持月度安全运营报告自动化导出，报告内容包括整体安全运营概览（威胁概况、风险终端）以及风险趋势，挖矿、木马远控、僵尸网络、黑客工具、恶意URL等类型的威胁拦截数；新型威胁最新动态及最新威胁情报TOP30；重点事件运营，包括TOP10威胁事件和TOP风险终端，展示全网具体的值得关注的风险事件。3.3、平台应具备统一运维管理能力，管理员可基于一次认证，在单一的管理界面实现策略的统一管理，策略配置包含但不限于：硬件与软件引流设备、上网安全能力、实时威胁情报查询与拦截能力等，并支持在单一的管理界面分析和展示用户的身份认证、安全策略配置和安全日志（提供产品功能界面截图，加盖公章）3.2、支持分权分域管理。其中平台内置超级管理员、安全管理员、系统管理员和运维管理员四类角色，整体实现不同单位管理员分级管理，权责划分一致。4、上网管控功能要求：4.1、支持网络安全边界防护，包括：IPS、防病毒、恶意URL过滤和僵尸网络等防护能力，支持对恶意流量进行自动实时拦截，阻断入侵活动；内置的漏洞规则库、URL数量防护库，支持识别并过滤SSL加密的钓鱼网站、非法网站等，以及将违规https访问重定向到告警页面；规则库均支持自动更新。4.2、支持检测终端的合规状态，为企业上网安全提供更好的防护。例如检查指定杀软/进程是否运行，是否有按照规定登录指定域等，对于不符合要求的终端，管理员可做出相应处置，例如提示用户、禁止上网等，同时支持配置精细化PC外接设备管控策略，防止文件泄密，保障企业数据安全（提供产品功能截图，加盖公章）4.3、支持提供全量威胁情报，POP点威胁情报至少千万+级别，文件MD5威胁情报数十亿级别，URL威胁情报千万+级别；支持DNS、IP、URL流量的实时检测与拦截，可有效应对挖矿、C2和恶意软件的威胁。5、网络边界安全防护5.1、支持IPS、恶意URL过滤、网关防病毒、威胁情报云查、全量加密流量检测、C&C等恶意域名、IP访问阻断能力。5.2、支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。5.3、支持僵尸主机检测功能，可识别主机的异常外联行为。 |
| 2 | 互联网出口安全网关 | 深信服、天融信 | 4 | 台 |  |  | 1、性能要求：引流吞吐性能≥1Gbps。提供三年硬件质保与软件更新服务。2、硬件参数要求：内存大小≥4G，硬盘容量≥128G SSD，接口≥6千兆电口。3、支持上网安全、实时威胁情报检测与拦截、威胁举证、行为管控、数据防泄露、身份认证等安全能力（提供同时接入两种引流模式的SASE平台截图和客户端安装包，加盖原厂公章）4、支持上报设备识别码、在线状态等信息，支持在管理平台批量下发路由、NAT、DHCP等网络配置5、硬件网关引流支持防火墙、SD-WAN CPE设备，设备与POP节点建立隧道连接，保证接入体验和效率，保障数据安全传输。 |
| 3 | 主机安全防护软件 | 深信服、天融信 | 1 | 套 |  |  | 1、提供：周密预防：系统漏洞扫描 、补丁修复、终端基线检查、资产主动发现、资产盘点；主机安全防护平台，安全防护授权数≥500.服务器防护授权数量≥10提供三年软件规则库更新服务。2、全面防护：文件实时监控、勒索诱饵防护；提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的恶意文件数量、已拦截可疑行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。（提供产品功能截图和关于“勒索防护”的软件著作书证明功能有效性，并加盖厂商公章）3、支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析；4、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、夜间登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户。5、支持勒索可疑行为检测，通过行为AI能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截。6、支持基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索，挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况。7、支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴。8、防护效果优异，满足单位需求，要求对流行病毒查杀率超过99.8%，误杀率小于0.01%。（需提供第三方检测报告并加盖厂商公章。）9、支持对Windows停更的系统提供专项防护，包括0day漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能10、同厂商的安全态势感知平台检测到某主机有僵木蠕毒的C2通信时，支持手动或自动化将恶意域名信息下发到本产品做C2通信的封锁拦截，实现精准防远控，且安全态势感知的此事件不再重复告警。 |
| 4 | 企业级数据备份与恢复系统 | 深信服、天融信 | 1 | 台 |  |  | 1、产品规格：2U机架式设备，性能指标：内存≥2\*32 GB。存储配置：本次配置系统盘≥2块240GB SATA SSD，数据盘≥3\*6T 企业级SATA磁盘。存储容量授权≥10TB接口：不少于2个千兆电口和2个万兆光口。2、配置10 TB备份容量授权许可，支持VMware vSphere、Sangfor HCI、H3C CAS、Microsoft Hyper-V、Citrix Hypervisor、RedHat RHV、ZStack、安恒、易讯通、WinHong、Halsign等虚拟化平台备份，支持Oracle、SQLServer（MSSQL）和MySQL数据库备份；支持Windows和Linux系统的文件备份，授权许可不限制客户端数量。3、为保证运维的便捷性，采用B/S架构和向导式的备份、恢复管理方式，支持各种类型用户管理；支持基于角色的访问控制，图形化报表显示等。4、支持虚拟机批量备份中应用关联的虚拟机备份的数据时间点一致（并行快照）。5、支持对虚拟机深度有效数据提取，只备份有效数据，排除交换分区、回收站等数据，有效节约备份空间。 6、支持一键检测功能，支持用户自行检测系统健康状态，检测包括CPU、内存、硬盘、网口等硬件故障、告警等问题，同时支持检测各类存储服务是否正常启动。针对问题能够提出解决推荐办法。7、支持备份系统可控制系统服务，支持对系统服务进行启动、停止等操作。 |
| 5 | 运维安全管理系统 | 深信服、天融信 | 1 | 台 |  |  | 1、硬件参数：规格：1U，内存大小≥8G，硬盘容量≥2TB SATA，接口不少于6千兆电口，包含资产授权数量(个) ≥50。2、支持unix资源、windows资源、网络设备资源、数据库资源、C/S资源、B/S资源。3、支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容。4、支持登陆控制台会话超时时间设置，用户在指定时间内无操作自动注销当前会话。5、支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。6、支持批量导入、导出资源信息；支持手动添加、删除、编辑、查询资源，支持变更默认运维端口。7、全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计。8、为了方便组织进行运维管理，内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴。 |
| 6 | 日志分析管理系统 | 深信服、天融信 | 1 | 台 |  |  | 1、性能参数：包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，可用存储量≥2TB（RAID1 模式），平均每秒处理日志数（eps）最大性能≥2500，2U设备，内存大小≥16G，硬盘容量≥128G minisata+2T SATA\*2，接口不少于6千兆电口+2万兆光口SFP+。2、为了方便查看，基于审计总览形式，展示整体的审计状况，包括当前存储空间、关联事件、审计事件、日志传输趋势；支持自定义设置可显示的模块。3、支持多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持日志进行定时刷新。4、通过接入序列号控制接入设备的个数，主要支持网络设备、安全设备、操作系统、中间件、数据库等设备的日志接入，可以获取到设备的传输日志量，设备同步数据状态等信息。5、支持以标准syslog等形式接收第三方设备的日志并存储；支持FTP、Webservice、JDBC的日志数据拉取接入方式；支持通过agent、wmi接口采集windows日志；支持对常见安全设备日志范式解析；支持通过SIEM日志解析引擎对第三方日志接入模块进行统一独立的升级维护（需提供截图证明并加盖原厂商公章）。6、支持750+第三方日志采集器。7、支持接入的全部日志、自身操作日志进行ftp备份；支持自动定时备份，自动同步到ftp服务器。8、可自定义设置日志存储天数，容量告警提示等；满足存储超过6个月以上的合规要求。 |
| 7 | 安全态势感知 | 深信服、天融信 | 1 | 套 |  |  | 1、性能参数：网络层吞吐量≥1Gbps。硬件参数：规格≥1U，内存大小：96G，硬盘容量：480GB SSD+4TB\*4 SATA，电源≥2，接口≥4千兆电口，≥4万兆光口SFP+。2、授权及更新：产品需至少包含三年产品质保，三年软件及特征库升级。3、支持安全态势的可视化呈现，以大屏的方式从全网安全态势感知大屏、安全事件态势、资产监控大屏、脆弱性态势、全球网络攻击态势、外联风险监控大屏、横向威胁态势等不少于7块大屏展示界面。4、支持大屏轮播投屏及自定义大屏顺序设置和大屏名称。支持自定义统计周期、资产组、展示风险、轮播时间间隔、实时告警等信息。5、为保障安全态势感知安全有效，需具备优秀的流量识别、安全分析和综合技术等能力，同时入围信通院《中国网络流量监测与分析产品研究报告》专业能力领域三大组：综合技术能力组、流量识别能力组、安全分析能力组，提供证明材料并加盖厂商公章。6、支持对接北信源、远望科技、网络空间测绘系统、哨兵云、AD域、城市热点、深澜等第三方资产数据源对接，支持立即同步功能。7、支持勒索专项检测页面，对勒索主题的安全告警进行展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP爆破、感染勒索病毒、黑客勒索攻击、勒索C&C通信等维度，支持展示受害资产以及受害资产攻击数Top5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、勒索风险、攻击阶段、威胁等级、受害者IP、受害者资产类型、攻击者IP、攻击次数、处置状态等。8、支持挖矿专项检测页面，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、挖矿阶段、攻击阶段、威胁等级、受害者IP、受害者资产类型、攻击者IP、攻击次数、威胁情报、处置状态等。9、支持本地威胁情报和云端情报检测，本地内置160W+检测情报IOC规则数，平台联网情况下每5分钟可获取云端最新热门威胁情报规则库，具备防御热点威胁能力，针对本地无法检测的可疑IP、未知DNS等信息可上传至云端情报平台，平台针对页面内容分析引擎、图关联分析、逆向分析、主动探测等技术进行检测，可实时播报威胁情报检测信息。10、支持与本次购买的主机安全软件、互联网安全访问服务平台等设备的联动，包含冻结账号、联动封锁、访问控制、主机隔离、上网提醒、隔离黑进程、DNS拦截、下发病毒扫描举证等。 |
| 8 | 潜伏威胁探针 | 深信服、天融信 | 1 | 台 |  |  | 1、 性能参数：吞吐性能：≤500Mbps。硬件参数：规格：1U，内存大小≥4G，硬盘容量≥128G minisata SSD，电源：单电源，接口：6千兆电口，要求和态势感知平台同一品牌。2、 支持对节点检测节点内部主机外发的异常流量进行检测。3、 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为。4、 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。5、 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。6、 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。7、 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。（需提供证明截图并加盖原厂商公章）8、 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。9、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） 10、为保障所投设备对内部数据流量收集的多样性，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）。 |
| 9 | 安全托管服务 | 　 | 1 | 项 |  |  | 1、服务资产数量≥50个，提供线上7\*24小时值守服务；提供线下值守人员，服务时长≥10天，需白天与黑夜轮流值守，本次安全托管服务需支持对接本次采购态势感知平台、主机安全软件、互联网安全访问服务。2、投标方需借助安全工具对IT资产进行全面发现和深度识别，确保服务内资产信息的准确性和全面性，便于攻防演习期间快速定位安全风险和加固。3、服务质量监控：投标方需为招标方提供的服务成果展示门户（或用户Portal）应具备服务质量可视化展示，投标方能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，以验证投标方所承诺的服务指标（或称为服务SLA）。（需提供服务成果展示门户中服务质量监控相关的截图证明，并加盖原厂公章）4、露面梳理：支持使用安全工具对服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。该工具应当支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向招标方举证，及对应暴露资产存在的漏洞。（提供服务工具具备以上暴露面梳理能力的证明截图，并加盖原厂公章）；5、高危可利用漏洞防护：针对服务范围内资产扫描到的高危可利用漏洞，投标方应当为招标方做好每一个高危可利用漏洞的防护工作，包括但不限于为招标方提供漏洞修复方案和安全设备防护策略，以及帮助招标方配置防护规则，保证招标方不因此出现重大事件和损失；要求招标方可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到99%。（需提供服务承诺函并加盖原厂公章）6、7\*24小时威胁鉴定：投标方应当具备云端检测和分析平台，通过采集招标方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为招标方提供7\*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示。7、攻击队情报共享服务，攻防演习期间，投标方支持获取疑似为攻击队IP的情报信息，支持批量导出查看，方便招标人进行快速封堵，实时攻防对抗。8、为保障攻防演练期间尽可能减少对正常业务访问造成影响，安全运营服务平台应能支持对待封堵IP和用户资产IP进行自动比对，当安全人员欲封堵的IP与用户资产冲突时给出自动提示，避免人为误拦截。9、为保障本次服务效果，具有丰富的漏洞发现能力，所投该服务厂商应具备成熟的漏洞库，同时在漏洞收集能力和原创漏洞挖掘能力有丰富的技术积淀，要求所投厂商为CNVD国家信息安全漏洞共享平台技术组成员和用户组成员，提供官网截图并加盖厂商公章。 |