中煤集团山西华昱公司
网络安全威胁感知平台建设

技术要求

信息服务中心：2024.2.26

分管领导：2024.2.26

2024 年 2 月

一、总体要求

本次安全感知平台建设，厂家所提供的所有设备和软硬件系统应符合国家及行业相关标准和技术要求，乙方应在技术规格书中提供系统架构、设计、功能、品牌、规格型号、安全标准、质保等方面的具体说明，乙方应按照项目建设要求完成本系统，系统建设过程中所涉及的硬件、软件、模块、线缆及辅材等，如在设备清单中没有给出或在现场施工时数量不足的，均由乙方无偿按期提供。

所有硬件设备均提供三年的原厂质保服务及软件功能永久使用授权，提供三年的软件升级服务。

二、安全感知平台要求

1）安全感知平台

1、性能指标：国产化产品。标准机架式设备；CPU 性能：不低于 2 颗 hygon 5380 2.5GHz（16C）；系统盘：不少于 2*240GB SATA 盘；存储：不小于 48T；内存：不低于 6*32G；在带宽性能 1Gbps 时存储时长为 1500 天/1Gbps。接口：不少于 4 个千兆电口+2 个万兆光口；配置冗余电源，面板不可配置液晶屏防止关键数据泄密，与潜伏威胁探针组合应用，探针用于数据采集，平台用于数据分析和可视化呈现。专业的安全态势感知平台，能够做到检测、预警、响应处置，能帮助客户在高级威胁入侵之后，损失发生之前及时发现威胁；

2、支持安全态势的可视化呈现，帮助客户更直观的看清风险、看懂威胁，提供综合态势大屏、分支安全态势、安全事件态势、通报预警态势大屏、物联网安全态势大屏、全球网络攻击态势、资产态势、重大活动网络安全指挥调度大屏、设备运行态势、外联风险监控态势等不少于 12 块大屏展示界面证明；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置；

3、要求与现有下属所有矿探针进行对接，可实时收集下属单位安全信息，且可以联动下属矿探针及防火墙，支持将下属单位安全信息统一汇总接入，并实时分析展示，并可实时下发策略；

4、为实现安全事件的快速闭环处置，要求支持与现有品牌防火墙、行为管理、应

用交付等自有设备进行联动，实现效果包含联动封锁、访问控制、上网提醒、冻结账号等；

5、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；

6、支持自定义配置资产指纹识别规则，可基于流量行为细化资产类型，支持资产类型识别规则自定义和属性指纹特征自定义；

7、支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作；

8、支持 PPT 格式导出摘要报告，报告内容包括：网络安全整体解读、网络安全风险详情、告警及事件响应盘点，用户可直接通过导出的 PPT 报告进行工作汇报，高效体现工作价值。

9、支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH 漏洞、OpenLDAP 等操作系统、数据库、Web 等，页面上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；

10、支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力，综合运用威胁情报、IPS 特征规则和行为关联分析技术，如检测发现文件传输（上传下载）阶段的异常，对挖矿早期的准备动作即告警；

11、支持勒索专项检测页面，帮助客户更好的应对日益严峻的勒索风险，支持对勒索主题的安全告警进行统一展示和管理，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、威胁定性、勒索风险、威胁等级、受害者 IP、攻击次数等信息；

12、支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，

能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息；帮助管理人员及时了解威胁的影响，并找到攻击入口点；

13、支持通过网络侧（N）与终端侧（E）关联聚合，可以实现进程级取证，失陷主机定位更精准，并以可视化图谱直观清晰地展示出完整的攻击链，帮助用户快速找到症结，避免全盘查杀对业务产生影响；

14、支持随机生成临时管理员用户名和密码，供外援安全人员进行使用，随机用户名为临时自动创建管理员，只具备指定资产对应的：处置中心、脆弱性、日志检索的查看和操作权限，具备处置、上传附件等下级管理处置的权限；

15、支持综合安全风险、主机安全风险、脆弱性感知、外部感知、工单、摘要、处置报告多种方式呈现，也支持自定义时间导出 PPT 报告；

16、支持对 800+网络安全设备接入类型，接入方式支持文件、数据库、API、Syslog、FTP、Snmp trap、Kafka、WMI、webservice、winlogbeat 等方式进行日志接入，并支持用户对日志进行自定义解析规则；

报价人需提供功能截图证明并加盖原厂商公章。

2）潜伏威胁探针

1、软硬件一体化设备，与安全感知平台为同一品牌且均为国产化产品。硬件规格：1U，内存：不小于 16G，硬盘容量：不小于 480GB SSD，电源：单电源，不少于 6 个千兆电口+2 个万兆光口，要求设备处理性能不少于 2Gbps；

2、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；

3、内网资产：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；

4、违规访问：检测内网主机的访问情况是否符合规定，需要人工事先进行梳理好访问关系再进行配置。策略从上到下进行匹配，可以对策略优先级进行调节；

5、WEB 智能检测：支持命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等自定义配置启用、高检出、低误报模式；

6、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、Media 漏洞攻击、Shellcode 漏洞攻击、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、IPS 云防护、Web 漏洞攻击等服务漏洞攻击检测；

7、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；

8、安全策略：支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况。支持通过白流量过滤的方式，过滤安全网站访问，提升性能；

9、高级检测：支持 5 种场景的日志传输模式,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；

10、对接第三方平台：支持与第三方安全分析平台 kafka 对接，将采集的数据上报至第三方安全分析平台；

11、探针管理能力：提供三权分立的用户管理能力：系统管理员、审计管理员、安全管理员、普通管理员四个角色相互独立；具备系统内用户的业务操作和运维操作；同时支持 IP 绑定的登录安全设置。普通管理员角色的权限可自定义模块页面的编辑和查看权限。

报价人需提供功能截图证明并加盖原厂商公章。

三、资质相关要求

1、报价人应在中华人民共和国注册并具有独立法人资格，有履行合同的能力的一般纳税人资格。（提供营业执照扫描件）

2、报价人需提供不少于三份 2021 年至 2023 年间同类项目合同关键页的扫描件（甲乙双方、供货清单、签字盖章页），要求必须为报价人业绩而非原厂业绩。

四、设备清单

序号	系统名称	技术参数	单位	数量	备注
1	安全感知管理平台	详见技术要求	1	套	
2	潜伏威胁探针	详见技术要求	1	台	

附件：

现有网络安全设备统计表

单位	设备名称	设备型号	品牌
华昱公司总部	应用交付管理系统	AD-1000 B1800	深信服
华昱公司总部	防火墙主	AF-1880	深信服
华昱公司总部	防火墙备	AF-1880	深信服
华昱公司总部	上网行为管理主	AC-1000 B1750	深信服
华昱公司总部	上网行为管理备	AC-1000 B1750	深信服
华昱公司总部	SSL VPN 专线设备	VPN-2050	深信服
华昱公司总部	中煤集团专线入侵防御系统	TI	天融信
华昱公司总部	中煤集团专线审计服务	IBM X3850	IBM
华昱公司总部	中煤集团专线防火墙	H3C F1030	华三
华昱公司总部	3600 入侵防御系统		网神
华昱公司总部	防火墙	WAF NX3	绿盟科技
华昱公司总部	堡垒机	网神 SecFox V5.0	网神
华昱公司总部	超融合合规一体机	CSMPv2.0-MGR-PS	奇安信
五家沟煤业	互联网防火墙	AF-2000-FH2100B-1K	深信服
五家沟煤业	煤炭专网防火墙	AF-2000-FH2100B-1K	深信服
五家沟煤业	流量分析设备	SIP-Y-1600-1K	深信服
五家沟煤业	日志审计	SIP-Logger-A600	深信服
五家沟煤业	堡垒机	OSM-1000-B1150-1K	深信服
南阳坡煤业	集团网防火墙	AF-2000-FH2100B-1K	深信服
南阳坡煤业	煤炭专网防火墙	AF-2000-FH2100B-1K	深信服
南阳坡煤业	流量分析设备	SIP-Y-1600-1K	深信服
南阳坡煤业	日志审计	SIP-Logger-A600	深信服
南阳坡煤业	堡垒机	OSM-1000-B1150-1K	深信服
元宝湾煤业	明御攻击预警平台	DAS-APT-800	安恒

元宝湾煤业	明御安全网关	DAS-NGFW690	安恒
元宝湾煤业	明御安全网关	DAS-NGFW690	安恒
元宝湾煤业	运维审计	DAS-USM280	安恒
元宝湾煤业	日志审计	DAS-LOG-260	安恒
元宝湾煤业	网闸		
水泉煤业	煤炭专线防火墙	AF-1000-B1120-OS	深信服
水泉煤业	互联网出口防火墙	AF-1000-B1510-NW	深信服
水泉煤业	数据中心防火墙	AF-2000-B2130-NW	深信服
水泉煤业	GAP 网闸	GAP-1000	深信服
水泉煤业	网络安全威胁分析设备		深信服
水泉煤业	日志审计		深信服
水泉煤业	数据库审计		深信服
水泉煤业	堡垒机		深信服
国兴煤业	集团网防火墙	AF-2000-FH2100B-1K	深信服
国兴煤业	煤炭专网防火墙	AF-2000-FH2100B-1K	深信服
国兴煤业	流量分析设备	SIP-Y-1600-1K	深信服
国兴煤业	日志审计	SIP-Logger-A600	深信服
国兴煤业	堡垒机	OSM-1000-B1150-1K	深信服
国强煤业	集团网防火墙	AF-2000-FH2100B-1K	深信服
国强煤业	煤炭专网防火墙	AF-2000-FH2100B-1K	深信服
国强煤业	流量分析设备	SIP-Y-1600-1K	深信服
国强煤业	日志审计	SIP-Logger-A600	深信服
国强煤业	堡垒机	OSM-1000-B1150-1K	深信服
白芦煤业	互联网防火墙	AF-2000-FH2100B	深信服
白芦煤业	煤炭防火墙	AF-2000-FH2100B	深信服
白芦煤业	安全态势感知	SIP-Y-1600	深信服
白芦煤业	堡垒机	OSM-1000-B1150	深信服

白芦煤业	日志审计	SIP-Logger-A600	深信服
白芦煤业	生产网与业务系统防火墙	AF-1000-B1310	深信服