

4.1 投标分项报价表

项目编号：ZFCG-G2020119 号

项目名称：许昌电气职业学院“网络安全体系建设(不见面开标)”项目

序号	名称	品牌 规格型号	技术 参数	单位	数量	单价	总价	厂家
1	安全态势感知平台	深信服 SIP-1000-B400	1、19 英寸标准机架式硬件设备，硬盘容量 32TB，CPU 16 核，内存 96GB，系统盘 128GB SSD。配置冗余电源。单台设备支持处理每天亿级实时日志分析， 3TB 数据量。 ▲2、本次配置 4 个千兆电口、2 个万兆光口、1 个串口、4 个 USB 口。提供设备连接所需的光纤跳线及光模块。 3、支持集群部署，集群节点 64 个。 4、所投产品全面支持 IPv6，支持 IPv6/IPv4 双协议栈功能，支持 IPV6 安全态势感知，实现 IPV4 环境下所有功能。 5、所投产品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，支持页面跳转到对应态势大屏。 6、所投产品支持大屏展示安全事件态势，包括安全事件、事件	台	1	127000	127000	深信服科技股份有限公司

		<p>等级分布、安全事件态势、安全事件 TOP5、威胁面最大的事件 TOP10、事件类型 TOP5、风险业务/终端 TOP5。</p> <p>7、所投产品支持感知业务/服务器资产，可定义 IP 地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并支持基于流量支持识别操作系统、开放的服务与端口。</p> <p>8、所投产品支持外部威胁感知展示，包含高危攻击、残余攻击、暴力破解、成功的事中攻击、邮件威胁、文件威胁、外部风险访问等。</p> <p>9、所投产品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。</p> <p>10、所投产品支持 DNSFlow 分析引擎，利用机器学习算法结合威胁情报，能够从大量的样本中进行学习，总结其伪装的规律，从而发现伪装的恶意 DNS 协议。</p>					
--	--	--	--	--	--	--	--

		<p>11、所投产品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深度检测引擎，支持定期自动升级或离线手动升级。</p> <p>12、所投产品支持 SMBFlow 分析引擎，能够发现主机传输可疑文件、恶意软件行为、文件或关键目录的可疑操作行为以及 SMB 暴力破解等。</p> <p>13、所投产品提供展示整体的安全状况统计和态势的摘要报告，内容包含总体摘要、安全感知详情、UEBA 行为画像、安全规划建设建议等，从整体展示安全状况，帮助为运维人员快速了解业务和网络的安全风险。</p> <p>14、所投产品可对安全探针和接入的安全组件（包括 EDR、上网行为管理、无线控制器、VPN 等设备）进行统一的升级管理，支持配置向导功能，通过系统检测功能，检测设备基础配置、设备资源、设备接入情况、设备流量等是否有异常，并导出上架检测报告，同时支持监控探针和各类安全组件的运行状态，包</p>					
--	--	--	--	--	--	--	--

			<p>含日志传输模式、日志传输量、最近同步信息等。</p> <p>15、所投产品支持大屏轮播，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、资产态势等态势</p> <p>16、所投产品具备挖矿专项检测，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；并支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计。</p>					
2	数据中心威胁检测探针	深信服 STA-100-D 642	<p>1、本设备为安全管理平台的配套组件，与本次采购的安全态势感知平台完全对接。</p> <p>2、19 英寸标准机架式硬件设备，CPU8 核，物理内存 8G，硬盘容量 1T，配置冗余电源。</p> <p>▲3、标配 6 个千兆电口、4 个千兆光口（光模块满配，类型按需提供）、2 个万兆光口（光模块满配，类型按需提供），本次提供设备连接所需的光纤跳线。</p> <p>▲4、吞吐量 3.0Gbps，包转发率 15Mpps。</p>	台	1	102000	102000	深信服科技股份有限公司

		<p>5、所投产品支持 IPV6/V4 双栈同时工作，支持 IPV6 流量分析，实现 IPV4 环境下所有功能。</p> <p>6、所投产品过旁路部署方式对全流量信息进行采集，支持探针同时接入多个镜像口，每个口相互独立不影响。允许将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。</p> <p>7、所投产品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。能够识别应用类型 1100 种，应用识别规则总数 3000 条，具备亿万级别 URL 识别能力，漏洞特征库规则数量 4000 条。漏洞特征具备中文相关介绍，包括漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号等。</p> <p>8、所投产品支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击。支持跨站请求伪造 CSRF 攻击检测。支持对 ASP, PHP, JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测。支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测。以上列出的攻击类型逐条响应。</p>					
--	--	---	--	--	--	--	--

			<p>9、所投产品支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。</p> <p>10、所投产品能够实时监控设备的 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。</p> <p>11、所投产品支持设备内置简单命令行管理窗口，便于基础运维调试。能够提供网络管理功能，可进行静态路由配置。</p> <p>12、所投产品支持用户初次登陆强制修改密码功能。多次登录失败将锁定账号 5 分钟内不得登录。</p> <p>13、所投产品支持在线升级和离线升级，并依托安全感知平台进行统一管控。</p> <p>14、所投产品支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级。</p>					
3	校园网 核心威胁检测	深信服 STA-100-F 842	<p>1、本设备为安全管理平台的配套组件，与本次采购的安全态势感知平台完全对接。</p> <p>2、19 英寸标准机架式硬件设备，CPU 10 核，物理内存 16G，硬</p>	台	1	108000	108000	深信服科技股

	探针		<p>盘容量 1T，配置冗余电源。</p> <p>▲3、标配 8 个千兆电口、4 个千兆光口（光模块满配，类型按需提供）、2 个万兆光口（光模块满配，类型按需提供），提供设备连接所需的光纤跳线。</p> <p>▲4、吞吐量 6.0Gbps，包转发率 16Mpps。</p> <p>5、所投产品支持 IPV6/V4 双栈同时工作，支持 IPV6 流量分析，实现 IPV4 环境下所有功能。</p> <p>6、所投产品过旁路部署方式对全流量信息进行采集，支持探针同时接入多个镜像口，每个口相互独立不影响。允许将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。</p> <p>7、所投产品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。</p> <p>8、所投产品能够识别应用类型 1100 种，应用识别规则总数 3000 条，具备亿万级别 URL 识别能力，漏洞特征库规则数量 4000 条。漏洞特征具备中文相关介绍，包括漏洞描述，漏洞名称，危险</p>					份有 限公 司
--	----	--	---	--	--	--	--	---------------

		<p>等级，影响系统，对应 CVE 编号等。</p> <p>9、所投产品支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击。支持跨站请求伪造 CSRF 攻击检测。支持对 ASP, PHP, JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测。支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测。对以上列出的攻击类型逐条响应。</p> <p>10、所投产品支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。</p> <p>11、所投产品能够实时监控设备的 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。</p> <p>12、所投产品支持设备内置简单命令行管理窗口，便于基础运维调试。能够提供网络管理功能，可进行静态路由配置。</p> <p>13、所投产品支持用户初次登陆强制修改密码功能。多次登录失败将锁定账号 5 分钟内不得登录。</p> <p>14、所投产品支持在线升级和离线升级，并依托安全感知平台进行统一管控。</p>					
--	--	---	--	--	--	--	--

			15、所投产品支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级。					
4	终端检测与响应平台 EDR	深信服 EDR	<p>1、本设备为安全管理平台的配套组件，与本次采购的安全态势感知平台完全对接。</p> <p>2、配置 20 个服务器终端授权。</p> <p>3、管理平台其操作系统为 64 位的 CentOs7 操作系统。</p> <p>4、终端软件（Agent）支持 32 位和 64 位的 Windows 系统和 64 位的 Linux 系统（包括 winXPsp3、7、8、8.1、10、2003、2008、2008R2、2012、2016，CentOS 5、6、7，Ubuntu 10.04、11.04、12.04、13.04、14.04、16.04，Debian 6、7，RHEL 5、6、7，Suse 12、Oracle Linux 等）。</p> <p>5、管理平台（MGR）能够提供适用于各类操作系统的所有版本的 Agent 软件下载。Agent 安装工具具有终端操作系统识别能力，自动选择合适的软件版本。</p> <p>6、无需安装任何其他软件和专用设备硬件，可直接部署于 X86 服务器和虚拟服务器。能够在虚拟化平台上通过虚拟机模板实</p>	套	20	1200	24000	深信服科技股份有限公司

		<p>现对虚拟机的镜像部署。</p> <p>7、可通过邮件、OA 等方式发布部署通知 Web 页面，终端用户只需点击链接自行下载 Agent 安装包进行安装部署。</p> <p>8、能够通过学校已有的上网行为管理系统，将终端 Web 访问请求重定向至 Agent 部署通知的 web 页面，实现终端 Agent 软件的强制推广部署。</p> <p>9、所投产品支持终端自动发现（管理员只需设置相应的 IP 段），并能够自动收集终端资产状况，包括：主机名、在线/离线状态、IPv4 地址、IPv6 地址、MAC 地址、操作系统、终端 Agent 版本、病毒库版本、最近登录时间、最近登录的用户名。</p> <p>10、所投产品支持录入终端所属责任人、责任人联系方式、邮箱、资产编号、资产位置信息，做到准确定位。</p> <p>11、所投产品支持实时监控终端上 Agent 对系统的资源消耗情况，包括 CPU、内存、硬盘等。</p> <p>12、所投产品支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置和 Windows 系统下信任区文件目录配置。</p>					
--	--	--	--	--	--	--	--

			<p>13、所投产品本产品制造商建有云安全服务平台，及时将 IOC 情报推送给本产品。本产品能根据 IOC 情报数据快速进行全网威胁定位分析，及时发现和响应最新的热点事件，并且根据历史行为数据进行溯源分析。</p> <p>14、所投产品支持场景化的配置向导功能，可以选择不同的终端部署方式以及使用场景，实现产品的快速实施。</p> <p>15、所投产品支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等。</p>					
5	网页防篡改	启明星辰天清Web应用安全网关系统 V7.0 WAG-WS	<p>1. 系统架构：C/S 架构，可以支持多个客户端管理，根据用户网站群架构与数量进行实际安装部署；</p> <p>2. 所投产品支持操作系统：支持 Windows Server2000/2003/2008/Unix/Linux/Solaris 等。</p> <p>3. 所投产品支持 WEB 发布类型：IIS、Apache、Weblogic、Tomcat、WebSphere 等所有主流的 Web 服务器。</p> <p>4. 监测模式：采用基于文件过滤驱动保护技术、事件触发机制相结合方式。</p>	套	2	57000	114000	北京启明星辰信息安全技术有限公司

		<p>5. 日志功能：系统能够对用户操作、文件操作和修改、安全日志以及策略配置事件进行完整日志记录；系统支持日志记录查询及导出，支持 excel 报表导出查询；系统提供独立的日志统计分析软件, 根据操作类型, 篡改文件等提供数据统计；系统日志支持 SYSLOG 接口，与网管平台结合。</p> <p>6. 防篡改功能：支持各类网页文件的保护，包括静态和动态网页以及各类文件信息；支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码；支持篡改后的自动恢复功能，恢复不依赖访问事件，直接由篡改动作触发恢复机制进行恢复；系统能够与所有第三方发布系统无缝结合，做到全自动发布；系统配置完成后，系统后台运行，支持断线检测；系统支持在断线情况下对网页文件目录的防护功能；系统支持黑白名单设置功能，提供进程黑白名单设置；系统支持对服务进行监控功能。</p> <p>7. 同步功能系统管理：系统可以从本地或异地备份文件夹自动同步到监测目录内；系统支持手工文件同步功能；系统支持手工指定文件或文件夹从监测目录到指定目录的备份；系统支持</p>					
--	--	---	--	--	--	--	--

		<p>增量备份功能；系统支持通过管理端受限用户进行文件上传下载功能；系统支持添加许可路径，排除保护内容；系统支持手工文件同步功能；系统支持各种发布工具或发布方式；系统支持内容管理系统；系统支持网络异常的自动恢复；系统支持发布失败的自动重新发布；系统支持 SSL 安全协议进行通信和文件传输，保证通信过程安全性；系统支持多虚拟主机 / 目录的并发同步功能；系统支持跨操作系统平台的同步；系统支持文件变化自动同步到多个 Web 服务器；可支持对 web 服务器的远程维护管理功能，如远程接管、远程唤醒、远程关机、远程用户注销等；支持对各类网页文件分类；系统支持高效的一对多集中管理模式；支持对服务器性能实时监控功能，包括：内存、CPU 占用率等；支持对服务器实时信息监控，包括：实时进程，服务信息，系统日志。</p> <p>8. 用户管理：系统支持用户权限分级, 只有日志管理员才可查看管理员操作日志, 可以设立多个基于文件目录的受控管理员。</p> <p>9. 自身安全性：指系统各个模块之间、进程之间的通讯、交互和自身配置均采用加密传输和保护；卸载时提供管理员口令才</p>					
--	--	---	--	--	--	--	--

			<p>可执行；支持对系统关键配置信息进行加密保护；支持对备份目录文件的保护；支持系统安装文件保护功能。</p> <p>10. 报警方式：支持声音提示报警，对非授权用户篡改网页提供实时声音报警；支持邮件提示报警，对非授权用户篡改网页提供实时邮件报警提示；系统支持报警提示框，对非授权用户篡改网页提供实时报警框弹出提示。</p> <p>11. 响应时间：当网站文件遭到篡改恢复最短时间 2ms。</p> <p>12. 最多可保护对象：系统能够保护站点的最大文件和目录的数量不限。</p> <p>13. 最大保护目录深度：系统能够保护站点的最长路径 10 级。</p>					
6	数据库审计系统	启明星辰 天玥数据库审计系统V6.0 DA-1500-UR	<p>1. 标准 2U 机架式，双电源，配置 6 个 10/100/1000M 自适应 Base-TX，4 个 SFP 光接口插槽（含模块），硬盘存储空间 2T。</p> <p>2. IPv6：支持 IPV6/V4 双栈同时工作。</p> <p>3. 部署方式：支持混合模式部署，可在线和旁路方式同时使用，具备 BYPASS 功能。</p> <p>4. ▲处理性能：每秒入库 35000 条/秒，日处理事件数 25000 万条。</p>	台	1	143000	143000	北京启明星辰信息安全技术有限公司

		<p>5. 系统管理：采用分布式部署，可以通过统一的审计数据中心采集多个独立引擎的日志。总控制台能够适时监控分布式部署引擎的系统状态、策略和审计事件，审计日志统一存储、查询、分析、统计。</p> <p>6. 身份认证接口：支持静态密码、支持双因素认证方式；支持LDAP、AD 域认证方式；支持标准 radius 服务器的接口。</p> <p>7. 可审计和控制的操作系统类型：支持审计控制通过 RDP/VNC、Telnet、SSH、Rlogin、FTP、SFTP、SCP、Netbios、NFS、HTTP 等方式对数据库的访问；支持审计控制数据库操作，包括 Oracle、MS SQL Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、人大金仓、达梦、南大通用、神通、MongoDB 等数据库。支持审计网络邻居、NFS 协议的用户名、读写操作、文件名等；支持审计 Radius 协议的认证用户 MAC、认证用户名、认证 IP、NAS 服务器 IP；支持审计 HTTP 协议的 URL、访问模式、cookie、页面内容、Post 内容；支持对针对数据库的 SQL 注入、XSS 攻击行为进行检测。</p> <p>8. 操作日志内容：支持访问数据库的源主机名、源主机用户、</p>					公司
--	--	--	--	--	--	--	----

		<p>SQL 操作响应时间、数据库操作成功、失败的审计；支持数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等各种对象的 SQL 操作审计；支持 Select 操作返回行数和返回内容的审计；支持数据库存储过程自动获取及内容审计；提供对数据库返回码的知识库和实时说明，帮助管理员快速对返回码进行识别。</p> <p>9. 数据库访问控制策略：可实现基于访问 IP、用户账号、目标设备、目标服务、系统账号、具体操作、时间设定比较详细的访问策略。不符合访问策略的操作可以被阻断；对于数据库操作的阻断支持到命令级，保持会话不断开，仅阻断某一命令；对于数据库操作：能够定义数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物、响应时间、返回行数、操作成功失败等各种对象。</p> <p>10. 业务关联审计：支持自动方式建立 web 访问和 SQL 访问之间的对应关系，生成访问行为模型库；支持中间件环境下的 SQL 语句关联到 HTTP 操作，HTTP 操作关联到 HTTP-ID，实现中间件环境下的审计追溯；支持实时关联模式，可实时查看关联审计</p>					
--	--	---	--	--	--	--	--

		<p>结果，无须事后手工查询。</p> <p>11. 数据库异常行为智能审计：支持自动建立数据库操作行为基线；数据库操作行为基线包括数据库账号、操作类型（SQL 模板）等行为特征；对超出数据库操作行为基线的操作可自动识别，并及时告警。</p> <p>12. 操作响应：支持记录审计事件、Syslog 告警、SNMP trap 告警；支持命令级阻断，可只配置策略阻断单个操作命令，会话仍然保持；提供短信告警、邮件告警功能。</p> <p>13. 审计报表：支持生成各种格式的审计报表，包括 PDF、Word、Excel、HTML 等格式；支持报表按日、周、月自动生成，并且可自动邮件发送给相关管理人员。</p> <p>14. 标准联动功能：支持通过标准关联协议与校方现有 Web 应用防火墙联动，可对 WAF 上报的应用系统攻击实现场景还原展示便于运维审计分析预警；支持与 APT 检测产品联动，对于网络传输的文件不仅可以审计，还支持恶意代码检测，报告可疑的攻击文件。</p> <p>15. 大数据支持：支持审计系统扩展，可采用大数据平台存</p>					
--	--	---	--	--	--	--	--

			储和分析审计日志，极大扩展存储空间和分析能力。					
7	日志审计系统	启明星辰 泰合信息 安全运营 中心系统 V3.0 TSOC-SA-C DB	<p>1. 所投产品系统架构：基于大数据技术，采用 B/S 软件架构，具备高性能海量数据存储能力，根据校方需求，提供本地化现场展示页面与威胁日志可视化定制开发与范式化，▲实配 230 个审计对象授权。</p> <p>2. 所投产品日志采集：支持 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC 等多种方式完成日志收集功能。</p> <p>3. IPv6：所投产品支持 IPV6/V4 双栈同时工作。</p> <p>4. 资产管理：资产模块支持对资产的 ping、telnet 和远程访问等功能；系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表；能够根据收到事件的设备地址自动识别新的资产并自动添加到资产库中。</p> <p>5. 日志管理：对不支持的事件类型提供可扩展功能；支持长安</p>	套	1	167000	167000	北京 启明 星辰 信息 安全 技术 有限 公司

		<p>全事件格式；对日志设备类型、日志类型、日志级别等可进行重定义。日志可加密压缩传输，支持加密压缩方式转发，定时转发；支持对日志的过滤和合并；合并支持设定合并的时间范围；支持日志源管理功能，对断点日志源可以产生告警；提供基于日志查询任务模式的日志导出功能。</p> <p>6. 日志范式化：范式化字段应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源 MAC 地址、源端口、操作、目的地址、目的 MAC 地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；针对不支持的事件类型做范式化不需改动编码，通过修改配置文件即可完成。</p> <p>7. 日志分析：可以手工对选中日志进行告警或者加入观察列表中；可以对选中的日志提供在线/离线地图定位、源 IP 与目的 IP 分布走向的视网膜图展示、描述日志之间行为相关关系的事件拓扑图等多种分析工具；统计分析模式下支持柱状图、饼图等形式的统计信息可视化展示；根据统计结果可直接钻取符合条件的日志。</p>					
--	--	--	--	--	--	--	--

		<p>8. 日志全文检索：系统提供输入关键字从海量事件中获取匹配或部分匹配的事件，更方便的定位事件；提供基于正则表达式检索功能，为检索出更为复杂的事件信息提供有效支撑。</p> <p>9. 关联分析：系统具有日志关联分析的能力，能够对不同的日志进行相关性分析，发掘潜在的威胁信息；提供基于图形化方式的规则编辑器；规则可导入导出； 所有事件字段都可参与关联，规则可实时启用和停用。</p> <p>10. 资源自定义：可以将日志中的 IP 地址、端口、时间等信息进行资源自定义，为规则所引用；</p> <p>11. 防火墙设备联动：通过关联规则，发现安全隐患，如：DDoS 攻击、SQL 注入、XSS 攻击、口令爆破、违规访问敏感数据等，则日志审计与防火墙进行联动，实现自动化阻断功能；</p> <p>12. 所投产品威胁模型展示：提供威胁态势建模功能，支持建立一个事件到威胁的映射表，来获得威胁；根据 GB/T-20984 提供可感知的威胁类型；根据用户日志信息进行事件梳理，提供 60 项的威胁事件，事件内容包括事件名称、等级、威胁分类等；提供信息安全合规性威胁展示，用以显示被审计系统的违规行</p>					
--	--	---	--	--	--	--	--

		<p>为，威胁合规类应实现安全产品登录、服务器账号的登录时间和地址、交换机的登录、操作的统计等，提供 40 项合规性威胁模型；提供威胁攻击类模型 30 项，木马病毒类威胁模型 5 项；提供阈值威胁展示，提供 10 项阈值告警威胁模型；提供可用性威胁展示（可用性威胁指在 IT 服务中的一个无计划中断，或者 IT 服务本身服务性能的降低），提供 15 项可用性威胁模型；提供基础支撑性威胁展示，提供 15 项威胁模型；提供威胁建模的事件分类对应表，提供 100 项目。</p> <p>13. 现场定制开发：支持与多种数据源的连接，包括关系型数据库 Oracle、DB2、Postgres、Mysql，分布式 NoSQL 数据库 UDB、数据查询工具 Hive、Impala 支持 hadoop 架构数据源 Hbase、HDFS 分布式文件系统等；支持与第三方数据库对接，如 ODPS、ADS 等；定制开发的内容是动态数据展示，分析手段遵从大数据态势感知系统的功能要求，不应使用数据库报表工具、EXCEL、Tableau 等 C/S 架构的 BI 工具；数据挖掘 10 张大屏，每个大屏幕控件 6 个组件，组件包括折线图、热力图、玫瑰图、内外环、桑基图、3D 地图、散点图、饼图、世界地图、中国地图、省地</p>					
--	--	--	--	--	--	--	--

			<p>图、三维透视图等，数据展示的方式、内容、布局均满足用户需求，并能根据用户现场进行修改调整；所有定制开发服务的源代码是项目服务不可分割的部分，免费提供给用户方，代码包括：系统对接开发代码、平台调整代码、大屏展现代码、数据挖掘算法代码、数据挖掘数据实现代码等；根据代码更改需求，用户方获取平台源代码时，产品厂商无条件配合提供源代码。</p> <p>14. 日志存储保护隔离装置：保护器采用单片机架构，无操作系统，即插即用，无需安装驱动，无需额外电源供电，无需改变计算机系统的任何配置即可使用，可适配 Linux、windows 操作系统。设备基于电路通断的物理方法使攻击者无法通过软件漏洞、系统缺陷等方式绕过而窃取日志数据。</p>					
8	安全隔离网闸	启明星辰天清安全隔离与信息交换系统V2.6	<p>1. 系统架构：采用“2+1”系统架构，即由两个主机系统和一个隔离交换专用硬件组成；隔离交换矩阵基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为断开状态。</p> <p>2. 硬件规格：▲标准 2U 机架式，双电源，内外网主机各标配 6</p>	台	1	154000	154000	北京启明星辰信息安全

		GAP-6000-2620BD-RP	<p>个 10/100/1000M Base-TX 网络接口；设备提供液晶面板实时显示设备工作状态及配置信息，提供健康指示灯与声音报警装置。设备处于异常状态下，能通过指示灯报警，且能通过报警装置发出声音报警。</p> <p>3. 性能：网络吞吐量 1Gbps；并发连接数 100000。</p> <p>4. 系统：内外网主机系统分别支持双系统引导，并可在 WEB 界面上直接配置启动顺序，在 A 系统发生故障时，可以随时切换到 B 系统；且支持系统(包括配置)备份；</p> <p>5. IPv6 环境支持：支持纯 IPv6 网络环境，能够在纯 IPv6 网络环境下正常工作，具备 IPv6 Ready Phase-2 认证证书（已提供相关证明材料）。</p> <p>6. 强制访问控制：所投产品支持 WEB 认证方式和专用客户端两种认证方式；可对用户的客户端版本和进程进行检查，进行准入控制。</p> <p>7. 文件同步：所投产品支持 NFS、SMBFS 等文件系统；文件服务器可以是 Windows、Linux/Unix 等系统平台；支持文件传输方向可控，实现单向或双向传输；支持文件格式特征过滤；并</p>					技术有限公司
--	--	--------------------	---	--	--	--	--	--------

		<p>能提供文件类型判断工具以帮助用户识别不常见文件类型；重名策略，接收端客户端支持对重名文件的控制策略，提供“覆盖”、“丢弃”、“重命名”等重名策略；可根据异常条件进行报警，如 MD5 校验失败、内存占用过高等条件；支持邮件报警方式。</p> <p>8. 数据库同步：所投产品支持 Oracle、SQL Server、Sybase、Db2、MySQL 等主流数据库；数据库同步客户端支持 Windows、Linux 等主流平台；支持同种数据库间（同构）和不同种数据库间（异构）的同步；支持灵活的数据库冲突处理策略，当关键字数据发生冲突时可选择：覆盖/丢弃；支持数据库同步客户端的双机热备技术，为用户提供更高的冗余技术支持；支持数据容错处理，当数据同步失败时，用户可以查询、恢复、删除未能正常传输的数据；支持客户端与网闸间的数字证书方式的身份认证。</p> <p>9. 数据库传输：实现对多种（如 MySql、SqlServer、Oracle、DB2、Sybase）主流数据库系统的安全访问；提供数据库访问用户的过滤和控制；支持数据库 SQL 语句过滤功能；支持用户身</p>					
--	--	--	--	--	--	--	--

		<p>份认证。</p> <p>10. FTP 访问：实现安全的 FTP 访问，支持对访问用户、访问协议命令、上传下载文件类型等访问过滤控制；支持访问时段策略；时间可以设置为一次性或者周循环方式；支持用户身份认证。</p> <p>11. 邮件传输：所投产品支持基于 SMTP 协议的邮件发送和 POP3 协议的邮件接收；支持邮件主题及正文的关键字过滤，以及收件人、发件人地址黑白名单；支持对邮件附件大小进行控制；支持附件类型过滤；邮件收发支持时段访问控制；时间段可以是一次性执行、周循环两种方式；支持用户身份认证。</p> <p>12. 安全浏览：所投产品支持访问源地址、目的地址、目的端口的访问控制；支持页面关键字过滤，支持 MIME 类型过滤；支持网页下载文件类型过滤；支持 URL 过滤；支持上网时段控制策略，时间策略可以是一次性或者周循环模式；支持用户身份认证；支持 HTTP 请求头部大小限制。</p> <p>13. 定制访问：实现特定 TCP、UDP 协议的数据隔离交换，可合作定制开发针对特定协议的安全检测，实现如黑白名单控制、</p>					
--	--	--	--	--	--	--	--

			<p>关键字过滤等；支持源地址、目的地址、目的端口的访问控制；支持用户身份认证。</p> <p>14. 安全通道：所投产品支持 HTTP/HTTPS/FTP/SMTP/POP3 等应用协议；支持 H323/H323_GK 等多媒体协议；支持多种访问控制，比如 IP 地址和端口访问控制，连续端口范围控制等；支持时间策略访问控制；支持 SYN、UDP FLOOD 阈值设置。</p> <p>15. 病毒检测：所投产品支持病毒检测及入侵检测引擎。</p> <p>16. 安全管理：所投产品支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输；内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等；支持配置文件以加密的方式导出。</p>					
9	安全监测预警服务	启明星辰 启明星辰 安全服务	<p>1. 风险评估与渗透测试:从漏洞、配置弱点两个维度发现资产的脆弱性，包括漏洞的脆弱性和配置暴露的脆弱性。从校内、互联网等位置利用各种手段对某个特定网络进行测试，以及发现和挖掘系统中存在的安全问题，然后输出渗透测试报告及修复建议。</p>	套	1	162000	162000	北京启明星辰信息安全

		<p>2. 安全加固:针对不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统的配置进行检查,并为系统制定安全的配置基线,便于进行配置核查。对网络安全设备进行策略的检查、梳理和修正,如防火墙的访问控制列表、安全策略有效性,进行策略调整调优,发挥已部署网络安全设备的作用。针对后期网络建设及调整,辅助完成网络安全规划及建设设计,提供安全建设方案。针对上线应用系统,从身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制、数据完整性和数据保密性进行安全功能有效性测试。</p> <p>3. 安全监控:对网络拓扑、网络设备、网管服务等进行相应的漏洞扫描和评估,并对网络日志、流量进行具体分析。按照上级机关各项安全检查工作要求,协助完成安全检查工作。提供最新的安全咨询信息,包括安全漏洞和补丁,包括国内知名的漏洞发布平台,将最新最严重的网络安全问题以最快的速度通报。</p> <p>4. 系统加固:针对数据中心不同类型的操作系统及服务器,部</p>					技术 有限 公司
--	--	--	--	--	--	--	----------------

		<p>署系统加固工具及组件，通过加固客户端对服务器系统进行加固，如外设控制，防止未授权 U 盘或其他移动存储介质随意插拔；主机防火墙，实现基于网络五元组的访问控制及进程管理；外联检测，服务器主动异常对外进行未授权连接时及时阻断并告警；应用管理，实现软件及进程的黑白名单安装管理；防病毒，能够对已知、未知病毒、木马、恶意程序等进行检测、清除，具备勒索病毒、宏病毒专杀能力；安全基线管理，客户端制定服务器安全基线标准，不符合基线标准要求的服务器，阻断接入。</p> <p>5. 安全测评：协助完成定级信息系统分析、定级系统边界划分、定级系统的等级确定、定级报告和备案编写。结合信息系统实际情况，进行系统性、全方位的分析信息系统安全，根据项目资金和时间规划，进行安全规划方案设计；同时提供具体落地的安全整改建设方案，用于指导安全建设。从安全技术（物理安全、网络安全、主机安全、应用安全和数据安全及备份恢复）和安全管理（安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理）两大方面进行与标准差距评估</p>					
--	--	--	--	--	--	--	--

		<p>分析，实施 3 个二级系统（门户网站、数字校园等）的等保测评工作，完成校等级保护测评备案工作，并取得备案证明。</p> <p>6. 网站安全监测预警：通过远程或现场方式，对网站定期进行安全检查，由安全专家进行专业分析，发现网站存在的隐患和漏洞，提供安全建议，帮助客户及时修复。通过 PING、GET 等方式对网站访问速度，响应时间，返回状态码进行监测，及时发现网站可用性问题并告警。对页面变化进行监测，发现疑似篡改情况，及时告警通知客户，避免由此带来损失。对被监控域名在各省主要运营商 DNS 服务器及授权域名服务器的域名解析情况进行监控，如发现域名解析异常及时报警并通知客户。</p> <p>监控范围包括：A 记录、MX 记录、NS 记录、CNAME 记录等。对网页中出现的敏感内容进行监测，如发现敏感内容及时通知客户进行处理。采用多种检测技术对网站挂马进行监测，发现网站被挂马后及时通知客户，减少风险。通过对被监测域名相似域名的检查，通过关键词对各主要搜索引擎搜索结果进行检查等方式对钓鱼网站进行监测，发现钓鱼网站后及时通知客户处理，避免造成经济损失。提供一台可信接入网关部署在校方数</p>					
--	--	---	--	--	--	--	--

			据中心，建立加密对接，远程集中管控、风险监测预警、安全事件通报与应急响应；收集和整理安全漏洞、安全事件、安全资讯等信息，使客户掌握当前互联网风险趋势，及时采取应对措施，降低风险，减少损失。收集和整理与客户网站、客户行业相关的漏洞信息、安全威胁等信息定期发送给客户，信息更贴合自身需求，可结合自身安全状况采取有针对性的措施和处理，处理更及时准确，可降低风险，减少损失。					
10	交互式智能大屏	希沃F75EC	<p>1、整机屏幕采用 75 英寸 UHD 超高清 LED 液晶屏，显示比例 16:9，具备防眩光效果。</p> <p>2、屏幕图像分辨率达 3840*2160。</p> <p>3、采用红外触控技术，支持在 Windows 系统中进行 20 点触控。支持在 Android 系统中进行 10 点触控。</p> <p>4、整机具有减滤蓝光功能，可通过前置物理功能按键，一键启用减滤蓝光模式。</p> <p>5、所投产品设备支持通过前置物理按键（为实现一键式操作，拒绝虚拟按键），一键启动录屏功能，可将屏幕中显示的课件、音频内容与老师人声同时录制。</p>	台	2	17100	34200	广州视睿电子科技有限公司

		<p>6、整机支持机身前置物理按键，一键切换画面显示比例（4：3 与 16:9），可对不同页面比例的 PPT 课件实现全屏展示。</p> <p>7、整机内置非独立外扩展的摄像头，支持二维码扫码识别，可拍摄 500 万像素的照片。</p> <p>8、整机内置非独立外扩展的麦克风，可用于一键录屏对音频进行采集。</p> <p>9、整机内置无线网络模块，无任何外接、转接天线及网卡可实现正常网络连接。</p> <p>10、同一物理按键完成 Android 系统和 Windows 系统的节能熄屏操作，通过轻按按键实现节能熄屏/唤醒，长按按键实现关机。</p> <p>11、整机内置专业硬件自检维护工具（不接受第三方工具），支持对触摸框、PC 模块、光感系统等模块进行检测，针对不同模块给出问题原因提示，可对嵌入式系统运行内存、垃圾文件进行清理。支持直接扫描系统提供的二维码进行在线客服问题报修。</p> <p>12、整机具备 3 路前置双系统 USB3.0 接口, 双系统 USB3.0 接口，双系统 USB3.0 接口支持 Android 系统、Windows 系统读取外接</p>					
--	--	--	--	--	--	--	--

		<p>移动存储设备，即插即用无需区分接口对应系统。</p> <p>13、支持锁定屏幕触摸和整机前置按键，可通过遥控器、软件菜单（调试菜单）实现该功能，也可通过前置的实体按键以组合按键的形式进行锁定/解锁。</p> <p>14、具备智能手势识别功能，系统在任意信号源通道下可智能识别上、下、左、右方向的手势滑动并调用响应功能，支持将手势滑动方向自定义设置为快速返回、截图、冻结屏幕。</p> <p>15、主板采用 H310 芯片组，搭载酷睿系列 I5 CPU，内存：8GB DDR4 笔记本内存配置，硬盘：128GB SSD 固态硬盘。</p> <p>16、采用抽拉内置式模块化电脑，抽拉内置式，PC 模块可插入整机，可实现无单独接线的插拔。采用 120pin 接口。</p> <p>17、模块化电脑采用按压式卡扣方式，无需工具即可快速拆卸电脑模块。</p> <p>18、模块化电脑具有独立非外扩展的电脑 USB 接口：电脑上具备 4 个 USB3.0 TypeA 接口，1 个 USB TypeC 接口（支持 TypeC 接口的 U 盘插入使用）。</p> <p>19、整机端内置蓝牙：在 Windows 系统下，整机可通过蓝牙模</p>					
--	--	---	--	--	--	--	--

			<p>块与蓝牙音箱连接，通过蓝牙音箱播放整机音频。</p> <p>20、配置承载大屏的移动支架。移动支架在正负 10 度倾斜角度下不能翻倒；承挂 100kg，壁挂高度可调；整体高度 1597mm；托盘承重 25KG, 模具设置 U 型置物槽，方便触摸笔、遥控器等物品放置；支撑立杆采用壁厚 1.8mm 方通冷轧钢材质，表面黑色喷涂；脚轮为万向轮，聚氨酯（PU）材质，均带脚刹，直径 ϕ 75mm；脚轮中心距横向 1115mm，纵向 627mm。</p>					
11	服务器	超云 R5210	<p>1、2 路 2U 机架式服务器。</p> <p>2、配置 2 颗 Intel Xeon 4210，每颗 CPU 核心数 10 核，每颗 CPU 主频 2.2GHz。</p> <p>3、内存：配置 2*32GB DDR4 内存。</p> <p>4、硬盘：配置 5 块 2.5" 1.2T10K SAS 硬盘。</p> <p>5、硬盘控制器：八通道高性能 SAS PM8222 RAID 卡，RAID 0/1/5。</p> <p>6、网口：配置 2 个千兆网口, 支持 OCP 网络模块，支持 1Gb/10Gb/25Gb 速率。</p> <p>7、配置 2 个热插拔 550W 电源。</p>	台	2	32000	64000	长城超云（北京）科技有限公司

合计	大写：壹佰壹拾玖万玖仟贰佰元整 小写：1199200 元
----	---------------------------------

投标人（并加盖公章）：河南中网云科物联网科技有限公司