

网络安全等级保护加固项目采购合同

重庆城市管理职业学院采购合同

(项目号: CSWU2021C-58)

甲方(需方): 重庆城市管理职业学院 计价单位: 元

乙方(供方): 重庆全意凡科技有限公司 计量单位: 台套项

根据《中华人民共和国民法典》、重庆城市管理职业学院网络安全等级保护加固项目校级竞争性磋商文件 (项目编号 CSWU2021C-58), 供方的《投标文件》及其相关承诺事项, 甲、乙双方同意签订本合同。详细技术说明及其他有关合同项目的特定信息由合同附件予以说明, 合同附件及本项目校级竞争性磋商文件、供方的投标文件等均为本合同不可分割的部分。双方同意共同遵守如下条款: 经双方协商一致, 达成以下服务合同:

品目	数量	主要技术参数及功能要求	单价	金额
1、日志审计系统 安恒 DAS-LOG-260	1	<ol style="list-style-type: none">1U, 1个 console 口, 配置6个千兆电口, 硬盘 2T, 内存 8G, 单电源, 日志处理能力 2000EPS。资产授权数量 55 个。支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP 协议日志收集; 支持阿里云 SLS 日志的采集。可通过接收协议限制日志接收速率, 包括 Http 接收、syslog 接收、SNMPtrap 接收、TCP 接收、WMI 接收、aliyun 接收。支持对 Agent 进行统一管控, 包括卸载、升级、启动及停止操作, 支持将日志收集策略统一分发。支持对收集到的重复日志进行自动聚合归并, 减少日志量支持将收集到的日志转发, 当原始日志设备无法设置多个日志服务器时, 可以通过本系统的日志转发功能将日志转发到其他日志存储设备。内置 5000+解析规则, 支持对收集的 5000+设备类型日志进行解析(标准化、归一化), 解析维度多达 200+, 解析规则可以根据客户要求定制扩展。可对日志进行细粒度解析, 解析后的日志根据具体日志包含但不限于: 日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息(公网情况)。具备安全评估模型, 评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等维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内置设备异常、漏洞利用、横向渗透、权限提	51500	51500

	<p>升、命令执行、可疑行为 6 大类 50+子类的安全分析场景。</p> <p>11. 具备三维关联分析功能：支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。</p> <p>12. 内置合规性报表 1000+ 种，内置 SOX、ISO27001、WEB 安全等解决方案包。</p> <p>13. 具备资产拓扑功能，可按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。</p>	
<p>2、APT 攻击检测系统 安恒 DAS-APT -800</p>	<p>1</p> <p>1. 支持检测 WEB 攻 2U，双电源，内存 16G，硬盘容量 2T，配置 6 个千兆电口，1 个空余接口扩展板卡，网络层吞吐率 1Gbps，应用层吞吐率 500Mbps。</p> <p>2. 击、恶意文件攻击、远程控制、WEB 后门访问、行为分析、非法数据、DGA 域名请求、SMB 远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP 欺骗、密码明文形式传输等。</p> <p>3. 支持详细展现风险等级、时间、威胁名称、攻击状态、攻击方向、客户端 IP、客户端 IP 所在地理位置、服务端 IP、服务端 IP 所在地理位置、报文、操作等信息，包含请求 URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息，并提供相应的数据包下载链接。</p> <p>4. 支持对内网主机进行主机威胁分析，详细展示具体的威胁等级、威胁次数、攻击开始时间、攻击结束时间、威胁性指数统计等。</p> <p>5. 可按攻击链阶段（弱点探测、渗透入侵、获取权限、命令与控制、数据盗取）详细展示主机相关事件数量。</p> <p>6. 支持对 IP、域名、恶意文件 SHA256 进行威胁情报检索，或跳转第三方链接（安恒情报分析、Whois、VirusTotal）进行检索。</p> <p>7. 支持 WEBSHELL 检测，可检测访问 webserv 的行为，包含具体对应的 URL、返回码、返回数据包内容等，可显示一句话类 webserv 后门是否植入成功。</p> <p>8. 支持对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接。</p> <p>9. 采用多并发沙箱检测技术，集成主流的操作系统 winXP、win7、win10、linux 等多种检测环境，拥有多项自主研发技术和专利。结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析。</p> <p>10. 支持通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到 APT 攻击中的 Oday 攻击。</p> <p>11. 支持动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险，对存在恶意行为的文件输出完整的二进制动态分析报告。</p> <p>12. 可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、返回结果、返回值等信息。</p> <p>13. 支持大屏展示风险事件，并进行攻击溯源，包括攻击主机个数情报事件 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）。</p> <p>14. 支持大屏展示失陷主机风险态势，包括失陷主</p>	<p>86500 86500</p>

重庆全
合同
开户行：
账号：

重庆城
合同
开户行：中国建
账号：5000
800

	<p>机视角/横向攻击视角、失陷主机/黑客组织TOP5、风险类别排名、回连区域排名、失陷主机事件统计柱状图、最新事件、失陷主机数。</p> <p>15. 产品具备《计算机信息系统安全专用产品销售许可证 (APT 安全监测产品)》，提供证书复印件。</p> <p>16. 产品制造商具备 ISO/IEC 20000 信息技术服务管理体系认证证书和 ISO/IEC 27001 信息安全管理体系认证证书，提供以上证书复印件。</p>		
<p>3、主机安全管理系统 山石网科 SG-6000-CloudDis</p>	<p>1</p> <p>1. 配置 1 套管理中心，20 个 server 授权，10 个 PC 授权</p> <p>2. 操作系统兼容性：支持 Windows server 2003/2008/2012/2016/2019；支持 Windows XP、Vista、Windows 7/8/8.1/10；支持 Linux kernel 2.6 及以后版本；支持国产主流操作系统，包括中标麒麟、银河麒麟、深度科技等；支持 VMWARE ESX、Hyper-V、XEN 和 KVM 等多种虚拟化平台部署。</p> <p>3. 支持本地和远程安装部署，客户端软件完整安装包文件 6MB，运行后进程数量 2 个，客户端安装目录对磁盘空间占用总量 25MB。</p> <p>4. 安全探针部署在终端之后，无客户端托盘、无任何警告弹窗、无需终端用户做任何操作，所有操作均可在管理平台完成。</p> <p>5. 支持对未安装探针的 Linux 主机进行远程批量部署安装，可批量导入或单个添加 IP 和账户信息，支持选择要安装的探针版本，支持查看批量部署任务状态，可看到已执行和应执行的主机数量和详细列表，支持批量重新安装。</p> <p>6. 同时支持对 Windows 和 Linux 运行异常命令进行检测和阻止，避免攻击者利用系统合法程序执行恶意命令，达到对主机的攻击和破坏，支持区分 Windows 高危和低危命令并分别设定防护策略，可做阻止、仅记录和不处理的响应动作。</p> <p>7. 支持对主机主动发起或遭受系统漏洞攻击行为的检测和响应，包括永恒之蓝漏洞、RDP 漏洞等，可有效防止利用漏洞传播勒索和挖矿。能够精准记录展示攻击源目的 IP，关联并展示发起攻击的进程文件，找到攻击源。</p> <p>8. 支持 Windows 操作系统注册表中映像劫持、网络劫持、登陆劫持、开机自运行、任务计划、系统服务、驱动程序、浏览器插件的配置文件路径的检测，支持 Linux 系统关键文件变更记录，包括文件的详细路径、文件哈希、文件存在终端数量、最后更新时间，并能在线查看文件内容。</p> <p>9. 支持对主机运行的文件、存在的网络端口、系统服务等进行同组或全网主机横向分析对比，可显示覆盖的终端数量和终端列表。可对网络端口和系统服务关联到的进程名称和路径做展示，以及判断相关进程文件的安全性。</p> <p>10. 支持主机在线状态的检测，可实施检测终端主机异常离线的时间、终端名称、重要级别、通知源头、通知发送状态、概要和详情等信息。</p> <p>11. 支持异常登录监控，对违反规则的异常登录进行告警，监控内容包括账号、时间段、IP 地址段和监控目标。</p> <p>12. 支持对风险事件追溯分析，可记录事件发生时间、发生数量、关联主机名称、登录的用户账户、事件行为描述、事件关联文件详细路径、关联文件加载的模块信息、行为发生时的调用栈信息。</p>	<p>20000</p>	<p>20000</p>

意凡科技
司专
民生银行重
152858
市管理职业
专月
105600005256
00117083

	<p>13. 支持 Windows 系统安全访问规则匹配日志记录, 可记录终端名称、访问时间、协议类型、出/入站方向、匹配次数、源 IP 地址、目的端口、关联主机进程、进程详细路径、进程安全级别等信息, 可快速将进程文件加入黑白名单。</p> <p>14. 支持查看主机磁盘目录, 可查看每个路径或磁盘分区下的文件夹, 以及每个文件夹内的文件信息, 可显示文件名称、路径、大小, 并能对文件进行隔离操作。</p> <p>15. 支持记录管理员操作日志, 可对比每次操作前后配置信息变化情况, 对违规操作进行追溯。</p> <p>16. 支持对指定路径下的指定文件在全网主机在线搜索, 可显示包含被搜索文件的主机列表, 包括主机名、文件描述、版本、HASH 值等信息。</p>		
合计人民币 (小写): ¥158000 (元)			
合计人民币 (大写): 壹拾伍万捌仟元整			
<p>一、服务要求</p> <p>(一) 交货/实施时间 签订合同后 15 个日历日内交货, 并完成安装调试。</p> <p>(二) 交货/实施地点 重庆城市管理职业学院</p>			
<p>二、质量保证与售后服务</p> <p>(一) 产品质量保证期: 自验收合格之日起, 其投标产品质量保证期达到 3 年。</p> <p>(二) 售后服务内容</p> <p>1. 我司和制造商在质量保证期内应当为采购人提供以下技术支持和服务:</p> <p>1.1 电话咨询 我司和制造商为采购人提供技术援助电话, 解答采购人在使用中遇到的问题, 及时为采购人提出解决问题的建议。</p> <p>1.2 现场响应 采购人遇到使用及技术问题, 电话咨询不能解决的, 我司和制造商应在 12 小时内到达现场 (远郊区 24 小时内到达现场) 进行处理, 确保产品正常工作; 无法在 24 小时内解决的, 应在 72 小时内提供备用产品, 使采购人能够正常使用。</p> <p>1.3 技术升级 在质保期内, 如果我司和制造商的产品技术升级, 我司应及时通知采购人, 如采购人有相应要求, 我司和制造商应对采购人购买的产品进行升级服务。</p> <p>2. 质保期外服务要求</p> <p>2.1 质量保证期过后, 我司和制造商应同样提供免费电话咨询, 并应承诺提供产品上门维护服务。</p> <p>2.2 质量保证期过后, 采购人需要继续由我司和制造商提供售后服务的, 我司和制造商应以优惠价格提供售后服务。</p> <p>(三) 备品备件及易损件 我司和制造商售后服务中, 维修使用的备品备件及易损件应为原厂配件, 未经采购人同意不得使用非原厂配件, 常用的、容易损坏的备品备件及易损件的价格清单已在投标文件中列出。</p>			
<p>三、验收要求</p> <p>1. 货物到达现场后, 我司应在使用单位人员在场情况下当面开箱, 共同清点、检查外观, 作出开箱记录, 双方签字确认。</p> <p>2. 我司应保证货物到达采购人所在地完好无损, 如有缺漏、损坏, 由我司负责调换、补齐或赔偿。</p> <p>3. 我司提供完备的技术资料、装箱单和合格证等, 并派遣专业技术人员进行现场安装调试。</p> <p>验收合格条件如下:</p> <p>3.1 设备技术参数与采购合同一致, 性能指标达到规定的标准。</p> <p>3.2 货物技术资料、装箱单、合格证等资料齐全。</p> <p>3.3 在系统试运行期间所出现的问题得到解决, 并运行正常。</p> <p>3.4 在规定时间内完成交货并验收, 并经采购人确认。</p>			

4. 产品在安装调试并试运行符合要求后，才作为最终验收。
5. 我司提供的货物未达到招标文件规定要求，且对采购人造成损失的，由我司承担一切责任，并赔偿所造成的损失。
6. 大型或者复杂的政府采购项目，采购人应当邀请国家认可的质量检测机构参加验收工作。
7. 采购人需要制造商对我司交付的产品（包括质量、技术参数等）进行确认的，制造商应予以配合，并出具书面意见。
8. 产品包装材料归采购人所有。

四、付款方式：

1. 成交供应商需在合同签订前向采购人缴纳合同金额的 5% 作为履约保证金（注明项目名称和编号），履约保证金汇到以下账户：
户名：重庆城市管理职业学院
开户行：中国建设银行重庆沙坪坝支行熙街分理处
账号：50001056800052500187
2. 验收合格后，供应商提供增值税发票后 15 个工作日内，向供应商支付合同全款；
3. 履约保证金在项目验收之日起至质保期满，无质量、售后和其它违约问题，由乙方提出申请，经采购人使用部门签字盖章后在 15 个工作日内无息支付给乙方。

五、违约责任：

1. 按《民法典》执行。
2. 乙方每延期一天，按照合同总额的千分之一收取乙方违约金；如甲方在验收合格并收到乙方发票后 20 个日历日内无故延期付款，每天支付给乙方千分之一的违约金。

七、其他约定事项：

1. 采购文件及其补遗文件、响应文件和承诺是本合同不可分割的部分。
2. 本合同如发生争议由双方协商解决，协商不成向需方所在人民法院提请诉讼。
3. 本合同一式伍份，需方肆份，供方壹份，具同等法律效力。
4. 其他：

<p>需方：重庆城市管理职业学院 地址：重庆市高新区大学城南路 151 号 联系电话：50001056800052500187 法人代表： 授权代表： 电话：罗小秋</p> <p>签约时间：2021.11.8 签约地点：重庆城市管理职业学院</p>	<p>供方：重庆全意凡科技有限公司 地址：重庆市九龙坡区石桥铺渝州路 18 号附 12-8 号 电话：023-68692314 传真：\ 开户银行：工商银行重庆高科技支行 账号：3100020419209423516 法人代表： 授权代表：林建峰</p> <p>签约时间：2021 年 11 月 8 日</p>
--	---