

# 渭滨区人民法院网络安全入侵检测系统建设项目

## 合同书

甲方：宝鸡市渭滨区人民法院

乙方：陕西柏云电子科技有限公司



# 渭滨区人民法院网络安全入侵检测系统建设项目 合同书

采购人：宝鸡市渭滨区人民法院（以下简称甲方）

供应商：陕西柏云电子科技有限公司（以下简称乙方）

根据《中华人民共和国民法典》等相关法律法规之规定，本着平等互利、诚实守信的原则，甲乙双方就渭滨区人民法院网络安全入侵检测系统建设项目供货及安装事宜，经协商一致，签订本合同。

## 一、项目概况

项目内容：网络安全入侵检测系统。

地 点：宝鸡市渭滨区人民法院。

## 二、项目金额及结算方式

1、合同总价：人民币 132000.00 元，大写金额：壹拾叁万贰仟元整。

2、合同总价包括：完成合同内容所需的全部费用，包括设备的供应费、运杂费（含保险）、安装调试费等。

3、付款方式：

设备到货安装调试完毕，验收合格后，甲方在 10 个工作日内一次性支付乙方全额合同款。

## 三、交工

1、工期： 20 日历日。

2、质保期： 3 年。

## 四、质量标准和检验

如甲乙有一方对检验结果持有异议，则由甲方和乙方共同检测，到有资质的检验机构重新检验，检验费由乙方负担。

## 五、服务和责任

1、乙方的权利和义务：

乙方施工过程中所产生的一切费用由乙方自行承担。

2、甲方的权利和义务：

(1) 甲方应将需求计划提前 2 天通知乙方。

(2) 甲方负责验收，并做好记录，详细填写《验收单》，出现问题由有关人员承担责任。

(3) 甲方有权监督乙方执行合同情况。

## 六、违约责任

1、乙方必须按合同规定质量标准及时组织施工，如果不能按规定质量组织施工，一经发现，甲方有权拒收。

2、如果乙方在供需合同有效期内，不能按合同条款履行责任，工期不及时或质量不合格，给甲方造成不良后果或损失，则由乙方承担一切责任。

3、如果由于乙方的违约给甲方造成损失，则由乙方全额赔偿。赔偿款从其工程款中扣除，不足部份另行赔偿。

## 七、不可抗力

1、不可抗力指下列事件：战争、动乱、瘟疫、严重火灾、洪水、地震、风暴或其他自然灾害。

2、一方因不可抗力不能履行本合同规定的全部或部分义务，该方应尽快通知另一方，并须在不可抗力发生后三日内以书面形式向另一方提供详细情况报告及不可抗力对履行本合同的影响程度的说明。

3、发生不可抗力事件，任何一方均不对因不可抗力无法履行或迟延履行本合同义务而使另一方蒙受的任何损失承担责任。但遭受到不可抗力影响的有责任尽可能采取适当或必要措施减少或消除不可抗力的影响。遭受不可抗力影响的一方对因未尽本项责任而造成的相关损失承担责任。

4、双方应根据不可抗力对本合同履行影响程度，协商确定是否终止本合同，或是继续履行本合同。

## 八、争议的解决

1、合同双方应通过友好协商解决，因解释执行本合同所发生的和本合同有关的一切争议。经协商不能达成协议，则双方同意在甲方住所地有管辖权的人民法院提起诉讼。

2、在诉讼期间，除了必须在诉讼过程中进行解决的那部分问题外，合同其余部分应继续履行。

### 九、合同的补充、修改的变更

- 1、双方协商一致，可以对本合同进行补充、修改或变更。
- 2、对本合同的任何补充、修改或变更必须以书面形式进行。
- 3、双方签订的补充协议以及修改或变更的条款与本合同具有同等法律效力。

### 十、合同的生效

本合同签署的所有内容应当符合本次项目最终采购要求，经双方签字盖章后，方可生效。

### 十一、其它约定事项

- 1、本合同的附件均为本合同不可分割的部分，与本合同具有相同的法律效力。
- 2、一方当事人未经另一方书面同意，不得将其在合同下的权利和义务全部或部分转让给第三人。
- 3、本合同一式肆份，甲方执贰份，乙方执贰份，均具有同等法律效力。

采购人（盖章）：宝鸡市渭滨区人民法院

供应商（盖章）：陕西柏云电子科技

地址：宝鸡市渭滨区公园路77号

地址：陕西省宝鸡市渭滨区滨河南路1号渭滨区互联网产业园1号楼1405室

委托代理人（签字）：

委托代理人（签字）：

电话：

电话：0917-3254618

开户银行：

开户银行：中国银行宝鸡陈仓园分理处

账号：

账号：102414997320

日期：2024年9月19日

日期：2024年9月19日



### 合同清单

序号	货物名称	品牌	规格型号	详细技术参数	单位	数量	单价	小计
1	综合威胁探针系统	绿盟	UTSNX3-HD4100-P	<p>2U 机型 SSD 为 64G 硬盘为 24T 管理口有 2 个 GE, console: 1 个 RJ45 接口, 8 个 10/100/1000M 电口, 4 个千兆 SFP 插槽, 扩展槽为 2 个, 吞吐量为 1.5Gbps。 包含流量采集、元数据提取、存储等功能 我公司投标产品完全满足流量采集要求; 支持导入 HTTPS 证书, 对流量进行解密和还原; 支持流量白名单, 过滤掉不关注资产流量, 白名单类型应包括 IP、端口、邮箱、域名。 威胁检测要求: ★应覆盖多种攻击特征, 可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测, 攻击特征库数量至少为 9000 种以上。要求提供攻击特征库数量截图证明。 内置 WEB 应用机器学习检测模型, 支持对 sql, xss, exec, phprce, ptravel 和 jeli 攻击类型进行分类检测和告警, 告警信息至少包括机器学习告警类型和威胁事件名称。 WEB 类告警详情中包含请求和响应信息, 在请求和响应信息中能标记规则匹配中的字段信息, 便于运维人员快速进行确认攻击事件。 内置恶意文件检测引擎, 支持对可执行文件、文档、压</p>	台	1	132000.00	132000.00

			<p>压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件类型、恶意文件家族信息和恶意文件变种信息。</p> <p>★支持自定义 TCP/UDP 行为检测模型，通过自定义内部资产对流量中的异常行为（包括内部向外部发起、内部对内部发起）进行检测和告警，告警信息包含检测类型和威胁事件名称。要求提供告警截图（包含告警类型和威胁事件名称）</p> <p>我公司投标产品完全满足回溯分析要求：</p> <p>应具备元数据提取、存储和检索的能力。支持元数据存储和展示，元数据类型至少包括 TCP&amp;UDP 日志、HTTP 日志、EMAIL 日志、FTP 日志、DNS 日志、ICMP 日志、文件还原日志。要求提供功能界面截图和日志截图。</p> <p>我公司投标产品完全满足响应：</p> <p>支持对入侵检测告警、WEB 应用告警、威胁情报告警和恶意文件告警中的攻击 IP 和受害 IP 发送阻断报文，进行旁路阻断。支持自定义一键封堵，配置策略包括 IP 类型（配置选项包括源 ip/源端口/目的 ip/ 目的端口）、域名类型、生效时间和失效时间。支持与大数据平台联动；提供 API 接口，由大数据平台通过接口下发一键封堵策略，探针执行封堵动作并将封堵日志信息发送给大数据平台。</p> <p>我公司投标产品完全满足取证（流量存储）要求：</p> <p>支持对采集的全部流量进行存储、检索和下载，检索条件包括源 IP、目的 IP、源端口、目的端口、起止时间。</p> <p>支持自定义规则抓取和留存可疑原始流量，自定义规则支持对原始流量的 payload 进行匹配。自定义规则内容至少包括：源 IP/源端口、目的 IP/目的端口、匹配类型（二进制、字符串、正则表达式）、匹配特征、会话数量、过期时</p>			
--	--	--	--	--	--	--

2	合计	大写：壹拾叁万贰仟元整		<p>间。</p> <p><b>资产识别要求：</b></p> <p>支持从流量中识别资产信息和展示,识别的信息至少包括资产 IP、资产 MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。我公司投标产品完全满足动态沙箱检测要求:</p> <p>支持样本虚拟化执行环境,具备 windowsxp、windows7、windows10 和 android 执行环境</p> <p>基于虚拟执行的动态检测技术,可以基于软件在虚拟环境的行为及通用漏洞利用特征(进行为,逃逸行为),分类识别各种加壳病毒及未知恶意代码;</p> <p>▲可记录文件运行期间的注册表行为、文件行为、网络行为等所有行为记录。支持文件检测内容包含恶意文件来源,恶意行为类型,恶意文件进程操作,文件操作,网络操作,注册表操作等可疑行为。</p> <p><b>厂商资质要求：</b></p> <p>厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书,提供有效证书的厂商盖章复印件;厂商为微软 MAPP 计划合作伙伴,提供证明材料。加盖厂商公章;</p> <p>厂商获得由中国信息安全测评中心颁发的信息安全服务(安全工程类三级)资质证书,提供有效证书的厂商盖章复印件</p>				132000.00
---	----	-------------	--	---	--	--	--	-----------

