**采购需求**

**一、为落实政府采购政策需满足的要求：**

|  |  |  |
| --- | --- | --- |
| **序号** | **政策名称** | **内容** |
| 1 | 政府采购促进中小企业发展 | 提供材料详见招标文件第六章“报价文件” |
| 2 | 政府采购支持监狱企业发展 | 提供材料详见招标文件第六章“报价文件” |
| 3 | 政府采购促进残疾人就业 | 提供材料详见招标文件第六章“报价文件” |

**采购标的对应的中小企业划分标准所属行业：**软件和信息技术服务业

**中小企业划型标准：**从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入50万元及以上的为小型企业；从业人员10人以下或营业收入50万元以下的为微型企业。

**二、采购资金的支付方式、时间、条件：**

|  |  |
| --- | --- |
| **▲履约保证金** | 1.合同签订后一周内，中标人向采购人提交合同总价5%的履约保证金，履约保证金在服务期内无违约等问题，服务期满后，于20个工作日内退还（不计息），逾期退还的，自逾期之日起，向中标人每日偿付合同价款的0.05%的违约金；  2.提交方式：支票、汇票、本票等非现金形式。 |
| **▲付款方式** | 按照年度支付，合同期满后，在中标人满足所有技术和服务要求条件且验收合格后，10个工作日内采购人向 一次性支付合同款的100%。 |

**三、服务及技术要求：**

**一、服务背景**

浙大城市学院积极响应国家网络安全改进号召，促进信息化建设、应用、管理和服务水平的持续提高，同时保障学院内部网络、信息系统的安全、稳定运行，将网络安全建设工作定位为非常重要的工作。目前，部署了大量的安全设备，然而安全防护往往并不止于安全威胁或安全事件的发现，更需要有效的安全威胁管理与运维。

随着安全设备的增多，安全事件发现能力提高，告警条数往往动辄上万条，管理人员不仅需要学习各类安全设备的管理运维方法，还需要依靠相关经验对安全事件进行分析响应，而由于存在误报的情况也不能轻易下结论，难以及时处置，导致安全事件虽然得到了发现，但却很难得到有效解决，同时还带来了巨大的工作量，安全设备的日常运维与安全事件的及时有效响应以及潜在威胁的高效阻断成为了棘手难题。

**二、服务目标**

通过专业人员驻场运维，最大化发挥安全技术采购效益，确保能够快速监测、响应、处置内外部攻击的攻击行为，通过技术人员现场信息安全值守，进行信息系统的安全保障工作，以发现并及时响应网络安全攻击事件，并在安全隐患被利用后及时加以响应。

1、降低整体风险。围绕业务系统逐步建立健全事前预警、事中监控、事后审计机制，更好的提升网络安全防护能力，降低系统运行风险。

2、增强安全防护体系。以总体安全技术防护策略为基准，持续开展风险和隐患排查、优化策略配置、减少互联网资产暴露面和网络攻击面，为信息化建设发展保驾护航。

**三、服务内容**

为采购人配备一名专业的技术人员驻场，驻场人员需擅长各种网络安全产品的原理及应用，可利用专业知识有效处置响应安全事件，热爱安全运维工作，具备较高的文档编写能力，同时有责任心，善于学习，沟通能力强，驻场详细服务内容如下：

1、网络安全运行状态监测分析

帮助采购人开展安全设备的性能指标、功能指标和硬件状态的巡检，记录指标值；

根据巡检记录，针对关键链路和节点设备的CPU、内存、磁盘使用率、网络连通性、网络会话连接数、网络流量等指标设置正常运行区间值、异常运行区间值及告警方式，一旦相关指标发生异常，及时进行安全告警；

针对监测指标产生的异常告警进行确认、分析，查找异常原因，提供解决方案，协解采购人完成安全整改和修复。

2、网络安全告警分析和预警

梳理网络和业务资产，针对网络收集的流量安全日志进行安全审计和分析，及时发现网络攻击和其它异常行为；

对网络安全设备产生的扫描探测、SQL注入、跨站脚本攻击、木马后门上传等各类网络安全告警事件进行溯源分析和风险验证，帮助采购人开快速完成安全响应；

通过先进的威胁狩猎思想，整合威胁情报、侦测技术、应急响应技术以及取证技术，采用人工分析和机器辅助的方法，针对网络数据和日志进行主动的和反复的检索，从而检测出逃避现有的安全防御措施的高级持续性威胁。

3、网络安全技术防护策略持续改进

实时对安全设备进行日志监控，在设备发现异常行为时，及时通过黑名单、访问控制列表等方式进行拦截处理施。对安全设备的系统版本、特征库、病毒库、威胁情报库和漏洞库等进行更新升级，对安全监测和安全风险检查的结果进行综合分析研判，识别网络安全风险、脆弱性和不合规配置项，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，协助开展策略配置调优，以持续提升安全运行和防护能力。

4、安全事件应急响应

在发现信息完全威胁后第一时间进行跟进处理，最大限度的降低安全事故带来的危害，减少安全事故带来的影响，将安全损失降到最低；

当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作；

然后再对入侵者进行追查，并对整个应急响应过程进行记录。对于紧急事件响应服务主要包括准备、识别事件（判定安全事件类型）、抑制（缩小事件的影响范围）、解决问题、恢复以及后续跟踪。

5、驻场人员要求

安排一名专业安全人员全年在浙大城市学院信息中心现场工作，国家法定节假日除外；驻场人员需具备CISP证书。

6、服务期

1年