# 采购内容及要求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **用途** | **数量** |
| 1 | 入侵防御系统 | 用于实时检测、分析和阻止网络中的恶意流量、漏洞利用和异常行为，保护网络系统免受攻击并提供安全警报。 | 1套 |
| 2 | 数据库审计 | 用于实时监控、记录和分析数据库的访问与操作行为，检测异常活动，确保数据安全与合规性。 | 1套 |
| 3 | 堡垒机 | 对运维人员的操作进行集中管理，对身份、访问、权限、审计进行控制。 | 1套 |
| 4 | Web应用防火墙 | 用于检测、阻止针对Web应用的恶意流量和攻击，保护Web服务器免受SQL注入、XSS等常见威胁，确保Web应用的安全运行。 | 1套 |

## 一、入侵防御系统

1、标准机架式设备；≥6个千兆电口，≥4个千兆光口，≥2个万兆光口；≥1T硬盘，≥1个扩展插槽（支持40GE接口扩展），冗余电源；性能要求：整机吞吐率≥15Gbps,最大并发连接数≥400万,IPS吞吐率≥5Gbps。提供不少于3年规则库升级许可，包含攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库。
 2、支持威胁分析功能，威胁分析展示包括：威胁事件的失陷/成功/尝试/失败等攻击结果、攻击事件级别、攻击类型分布、攻击阶段、事件详情等信息。（提供截图证明并加盖公章）

3、支持受害者视角分析，按照时间范围、受害主机、事件类型、处置状态、攻击结果、应用协议等条件综合分析受害者信息。（提供截图证明并加盖公章）

4、 系统可检测的入侵防御事件库事件数量不少于7000条，支持全面的攻击检测能力，可检测常见的Web攻击、缓冲溢出攻击、安全漏洞攻击、安全扫描攻击、拒绝服务攻击、木马后门攻击、蠕虫病毒攻击、穷举探测攻击、CGI攻击、视频流量防护等。（提供截图证明并加盖公章）

5、支持对多种应用类型进行攻击检测，包括：WEB应用、文件传输、邮件、数据库、远程访问、远程过程调用、工控、基础服务、加密等多种业务。（提供截图证明并加盖公章）

6、支持暴力破解检测，包括：邮件（SMTP、IMAP、POP3）、文件（FTP、SMB）、远程访问（TELNET、RDP、SSH）、数据库（LDAP、SQLServer、DB2、REDIS、POSTGRESQL、ORACLE、MYSQL、MONGODB）、WEB应用（HTTP）等17种协议类型进行暴力破解检测。

7、支持弱口令检测，包括：邮件（SMTP、IMAP、POP3）、文件（FTP）、远程连接（TELNET、RDP）、数据库（LDAP、SQLServer、DB2、REDIS、POSTGRESQL）、WEB应用（HTTP）等12种协议类型，能够按照弱口令字典、口令强度、密码长度等方式进行弱口令检测。（提供截图证明并加盖公章）

8、支持独立的僵尸主机检测引擎，涵盖11000种以上的僵尸主机规则库。规则库支持按照攻击类型、操作系统、风险等级、ATT&CK、攻击阶段等方式进行分类。

9、支持注入和WEBSHELL攻击检测，包括：SQL语法分析引擎检测、SQL注入智慧引擎检测、XSS攻击智慧引擎检测、命令注入智慧引擎检测、WEBSHELL上传智慧引擎检测、WEBSHELL行为检测。

10、支持与防火墙联动处置，实现基于五元组动态阻断，并可自定义阻断时间。

## 二、数据库审计

1、标准机架式设备，≥6个千兆电口，≥4个千兆光口，≥1个扩展插槽；≥2T存储空间，冗余电源，网络吞吐≥2Gbps，可审计流量≥600Mbp，峰值SQL处理能力≥15000条/s，日处理能力≥1500万条。

2、支持旁路部署方式，无须安装软件，对原有网络不造成影响。

3、支持匹配查询条件后的查询结果分析，分析结果支持在线查看报表导出。（提供功能截图证明并加盖公章）

4、支持数据库请求和返回的双向审计，支持审计SQL返回结果集、SQL语句响应时间、连接时长、表影响的字段、影响行数等内容。

5、支持用户数据库中敏感信息的自动发现和手动添加，可定位敏感数据所在数据库名、实例名、表名、列名，并形成针对敏感信息的检测规则。（提供功能截图证明并加盖公章）

6、支持数据库服务器弱口令扫描，扫描出的弱密码支持脱敏显示。

7、支持对针对数据库的XSS攻击、SQL注入、CVE高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。（提供功能截图证明并加盖公章）

8、支持SQL错误统计，多个维度展示错误占比及趋势，从源IP维度以柱状图展示SQL错误数（TOP10）；支持SQL错误分析，以列表形式给出出错原因、出错信息以及解决办法

9、支持以用户名、源IP、部门、域名、主机名、邮箱、联系电话为条件的实名审计。

10、支持数据库操作类、表、视图、索引、触发器、存储过程、游标、事物等各种对象的SQL操作审计。支持对超长SQL语句的审计，支持对数据库绑定变量方式访问的审计。

11、要求采用安全操作系统采用冗余设计，可在设备命令行启动过程中选择主备系统。

12、基于NLP算法和嵌入模型技术对用户问题进行语义理解，以交互式对话方式，支持智能分析用户意图、快速图文响应用户需求。内置数据检索分析、高危操作检索、数据泄漏事件查询、攻击事件分析等问题，可直接点击问题获取答案。支持按自然语言形式输入自定义问题，即可快速获取用户关心的数据，数据可以饼图、柱图、表格、文字等形式提供。（提供功能截图证明并加盖公章）

13、统计图表展示数据库高危操作行为统计，可直观展示针对数据库删库、删表等高危风险操作，并展示受影响数据库详情。（提供功能截图证明并加盖公章）

## 三、堡垒机

1、标准机架式设备,≥6个千兆电口，≥4个千兆光口，≥2T存储空间,冗余电源,≥2个扩展槽位,≥200个主机/设备许可，图形并发≥500，字符并发≥600。

2、支持双因子认证；认证方式支持OTP动态口令认证、短信认证、数字证书认证、USB-KEY认证、人脸识别等多因素认证方式。

3、支持管控字符、文件传输、图形协议类型包括：字符协议类型SSH、TELNET，文件传输协议类型FTP、SFTP、SCP，图形协议类型：RDP、VNC，数据库协议类型Oracle、PostgreSQL、MySql、DB2、Informix 、SYBASE，Mssql、KingBase等。

4、支持资产的增删改查、锁定、解锁等操作，对资产进行全生命周期管理。

5、内置常见命令；支持自定义命令，命令级别分为：普通命令、敏感命令和高危命令。（提供第三方机构检测报告证明及功能截图）

6、通过IP网段扫描，快速发现指定IP地址范围内的资产，并自动识别IP和端口，方便管理员快速添加资产。

7、支持改密结果可通过邮箱、FTP方式外发；密码采用密码信封加密保存，以保证安全性；支持密钥加密和明文分段发送。

8、提供授权关系查看功能，图形化直观展示用户、用户组、资产、资产组、协议、账号的授权关系。

9、支持 Oracle、mysql 数据库代理功能。并支持SQL命令控制功能，支持对数据库的访问操作控制，可基于命令进行细粒度访问控制，包括：放行、审批、阻断和告警。

10、系统内置系统管理员、审计管理员、安全管理员三种角色，系统管理员可针对不同用户指定不同的管理权限，可设定用户（组）和资源（组）的管理范围。

11、支持操作记录视频回放时水印显示运维用户。

12、等价账号，可配置为等价账号的账号为同一资产不同协议的同名账号。等价账号主要用于账号改密，通过将同名账号配置为等价账号，可实现改密任务改密等价账号密码时，会将等价账号中所有不同协议同名账号的密码一并修改。（提供第三方机构检测报告证明及功能截图）

13、批量运维视图配置，支持标签/九宫格展示方式，便于用户查看运维资产信息。（提供第三方机构检测报告证明及功能截图）

## 四、Web应用防火墙

1、标准机架式设备，≥6个千兆电口，≥4个千兆光口，≥4个万兆光口，≥2T存储空间，应用层吞吐≥2.5G，网络层吞吐≥10G，并发连接≥200万，新建连接≥21000，≥3年规则库升级许可。

2、支持SQL注入及XSS攻击防护、跨站请求伪造（CSRF）攻击防护、爬虫防护、恶意扫描防护、Cookie安全、服务器信息伪装/过滤、缓冲区溢出、HTTP请求类型过滤、Webshell行为拦截，目录遍历等。

3、支持能够对SQL注入、CGI、跨站脚本（XSS）进行应用层漏洞扫描。

4、基于智能用户行为识别的动态防护机制，识别并彻底阻断黑客的攻击行为。

5、真实来源IP解析，解析通过代理服务器访问用户的真实IP地址，默认支持X-Real-IP或X-Forwarded-For字段的值作为真实来源IP地址，同时支持用户自定义字段名称。

6、支持透明模式、反向代理模式下的HTTPS协议防护，加载证书后由系统在本地完成HTTPS解密过滤再加密转发到服务器，无需服务器端做任何改动。

7、支持防CC攻击防护：Rerferer攻击防护，来源IP攻击防护，特定URL攻击防护，CC防护的访问控制。（黑、白名单）

8、支持敏感信息隐藏，身份证信息和银行卡信息中的部分位数用\*替代。（提供功能截图证明并加盖公章）

9、报表提供对防护Web网站中已经存在Webshell文件的告警功能。

10、主动阻断方式包括丢弃数据包、阻断TCP连接、禁止恶意IP的后续访问。

11、支持基线学习，可以自动学习用户http正常流量阈值模型，并给出推荐阈值配置项。（提供功能截图证明并加盖公章）

## 五、集成服务

**1.安全管理体系**

服务要求：服务方需针对我校实际情况更新、完善相关管理制度，协助学校制定安全管理体系，并定期对制度的合理性和适用性进行论证和审定，对存在不足或需要改进的制度进行修改。

需提供交付成果：《安全管理制度》

**2.安全运维体系**

服务要求：

1）服务方需针对我校制定事件管理流程、问题管理制度、变更管理制度、资产和配置管理制度、访问管理制度、介质管理制度以及投标人管理流程等。其中包含：概述、目的、范围、流程等。

需提供交付成果：《事件管理流程》、《问题管理制度》、《变更管理制度》、《服务资产和配置管理制度》、《访问管理制度》

1. 梳理学院资产信息，提供自动化工具或设备对我校机房整体系统进行评估，检查系统整体脆弱性，提供风险评估报告。并对我校系统硬件建立详细的资产及配置档案。参考国内国际权威的系统安全配置标准，并结合操作系统安全评估及漏洞扫描、安全检测、日志分析和配置检测中发现的问题，对我校服务器、网络设备、数据库系统等安全漏洞进行修补，加强安全配置、安全加固处理。

需提供交付成果：《资产及配置档案》、《风险评估报告》、《安全加固方案》

**3. 项目实施及安全运维要求**

1. 项目实施

项目施工包含设备安装部署、设备所需光模块，辅材及人工等。

根据我校网络安全防护现状，建设全方位、动态化网络安全防御体系，需提供全域安全设备联动实施方案，通过构建集边界防护、流量监测、威胁感知功能的智能动态防御体系，实现多维度安全信息实时共享与跨设备协同响应，最终交付包含系统部署规划、安全策略配置的详细方案，以确保项目具备可落地性、可验证性与可持续优化性。

项目实施完成后，通过自动化工具或设备对我校信息系统安全保障能力进行评估，全面提升业务系统防护能力，提供具体实施方案。

1. 安全事件溯源分析

服务期内安全服务人员持续对安全事件提供深入调查分析，厘清安全事件损害范围、判断安全防御策略有效性、提供快速抑制攻击的措施。事件调查的过程，按照服务脚本和服务流程进行，产生告警和生成报告向相关责任人进行通知通报。每事件溯源分析事件不超过一周。

1. 安全事件应急响应

提供7×24小时的免费技术支持。支持范围包括产品的功能、配置、安装、调试、客户使用中遇到的各种技术问题的一般性咨询，并随时准备处理各种突发事件。

在我校发生各类网络安全事件时，第一时间提供应急响应和处置服务，按照安全应急响应预案，及时采取有效的应对措施，控制安全事件造成的影响范围，缩小损失，排查问题来源，恢复信息资产正常运行。

应急响应结束后，给校方提交《XX系统（事件）应急响应报告》。

1. 重保服务时间要求

在春节、劳动节、国庆节、开学时期等对系统设备稳定运行要求较高的特殊时段进行驻场值守，将值班工程师的时间表以及联系电话表以传真或Email的方式传送给客户方负责人，如果需要，根据实际情况安排工程师提供现场值班技术支持服务。

根据学校安排在春节、两会、国庆、开学时期等重要保障时期和重要的活动开展时期，为学校提供驻场服务。驻场服务时间不少于30天。

1. 设备巡检

每周提供定期的现场全面巡检，记录设备的运行状态，及时发现并排除系统故障，调整系统运行参数，保证系统运行在良好状态。及时响应学校的调试、优化及故障排除等服务要求，确保服务范围内设备无故障、稳定运行。每月底形成《月度巡检报告》。

1. 项目团队人员

投标人必须在本地（西安市）有固定的办公或售后服务机构场所（提供产权证明或租赁合同），整体实施服务内容是由投标人组建的专业技术支持团队完成（提供在所在单位近3个月的社保缴纳证明）。运维人员分为管理人员、技术支持人员，管理人员和技术支持人员均要求获得相关专业认证。项目团队人员配置根据下表，项目团队的工程师需具备以下证书：

|  |  |  |
| --- | --- | --- |
| 名称 | 人员证书要求 | 配置人数 |
| 项目经理 | PMP认证、信息系统项目管理师、CCRC信息安全保障人员认证证书CISAW  | 1 |
| 安全运维工程师 | CISP | 4 |

## 六**、**售后服务

所有软硬件提供3年质保。

售后服务机构健全，设备投标人在本地建立有完善的售后服务机构及服务团队，提供至少3年免费7\*24小时售后服务，提供售后服务承诺函。服务承诺内容为：设备出现故障1小时响应，2小时内到达现场，4小时内解决故障，如遇设备损坏等硬件故障，需提供备机。

## 七、交付期

交付期：自合同签订之日起 30 日历天内完成。

## 八、付款条件

项目整体验收合格后，一个月内，学校向中标单位支付合同总价款。