政府采购合同

合同编号:_____

项目名称:改善办学条件-设备购置-网络安全等级保护实训中心建设项目其他不另分类的物品采购项目

货物名称:网络安全等级保护实训中心建设项目其他不另分类的物品采购项目

买　　方:北京市经济管理学校

卖　　方:北京昊汉软件有限公司

签署日期:2022年 6月14日

合 同 书

北京市经济管理学校(买方)改善办学条件-设备购置-网络安全等级保护实训中心建设项目其他不另分类的物品采购项目(项目名称)中所需网络安全等级保护实训中心建设项目其他不另分类的物品采购项目(货物名称)经中承国汇咨询(北京)有限公司(采购人)以 ZCGH-ZB-202205003 号招标文件在国内公开(公开/邀请)招标。经评标委员会评定北京昊汉软件有限公司(卖方)为中标人。买、卖双方同意按照下面的条款和条件，签署本合同。

1、合同文件

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下:

a. 本合同书

b. 中标通知书

c. 协议

d. 投标文件 (含澄清文件)

e. 招标文件 (含招标文件补充通知)

2、产品和数量

本合同产品: 详见后附清单

数量: 一批

3、合同总价

本合同总价为:¥2,472,000.00 元人民币，大写金额：贰佰肆拾柒万贰仟元整

分项价格:详见后附清单

4、采购资金支付

合同签订生效 7 个工作日内，卖方向买方支付合同总金额 5%的履约保证金¥123600.00 元人民币，大写金额：壹拾贰万叁仟陆佰元整；买方向卖方支付合同总金额 60%首付款，即¥1483200.00 元人民币，大写金额:壹佰肆拾捌万叁仟贰佰元整；全部货物交付并验收合格后 7 个工作日内买方向卖方支付合同总金额 40%尾款，即¥988800.00 元人民币，大写金额：玖拾捌万捌仟捌佰元整；验收合格日

起二年内，买方退还卖方履约保证金(合同款的 5%)，即¥123600.00 元人民币，大写金额：壹拾贰万叁仟陆佰元整。

5、本合同产品的交货时间及交货地点

交货时间:合同签订后 20 个日历日内完成送货、安装、调试

交货地点:北京市经济管理学校指定

6. 验收要求:

在交货前，卖方应对产品的质量、规格、性能、数量和重量等进行详细而全面的检验，并出具证明产品符合合同规定的文件。该文件将作为申请付款单据的一部分。产品运抵现场后，全部安装调试完成，买方应在 10 日内组织验收，并制作验收备忘录，签署验收意见。

卖方在收到通知后 7 天内应免费维修或更换有缺陷的产品或部件。

如果卖方在收到通知后 7 天内没有弥补缺陷，买方可采取必要的补救措施，但风险和费用将由卖方承担。

合同项下产品的质量保证期为自产品通过最终验收起 3 年。

7. 违约责任及解决争议的方式:

①违约责任

除不可抗力外，如果卖方没有按照合同规定的时间交货和提供服务，买方可要求卖方支付违约金。违约金按每周迟交产品或未提供服务交货价的 0.5%计收。但违约金的最高限额为迟交产品或没有提供服务的合同价的 5%。一周按 7 天计算，不足 7 天按一周计算。卖方违约导致本合同不能履行，买方有权随时解除合同。

②不可抗力

如果双方中任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间。受事故影响的一方应在不可抗力的事故发生后尽快书面形式通知另一方，并在事故发生后 7 天内，将有关部门出具的证明文件送达另一方。不可抗力使合同的某些内容有变更必要的， 双方应通过协商在 7 日内达成进一步履行合同的协议，因不可抗力致使合同不能履行的，合同终止。

③合同争议的解决

因合同履行中发生的争议，合同当事人双方可通过协商解决。协商不成的，可向买方所在地人民法院提起诉讼。诉讼费用应由败诉方负担。

8、合同的生效

本合同经双方授权代表签署一式肆份，买方执叁份，卖方执壹份，加盖单位印章后生效。

买　方：北京市经济管理学校

名　称：(印章)

2022 年 6 月 14 日

授权代表(签字)：

地　　址：北京市海淀区北洼路 83 号

邮政编码：100036

电　　话：010-68427106

开户银行：中国农业银行玉渊潭支行

帐　　号：11050301040000599

卖　方：北京昊汉软件有限公司

名　称：(印章)

2022 年 6 月 14 日

授权代表(签字)：

地　　址：北京市丰台区造甲街 110 号 31 幢一层 A1-258

邮政编码：100036

电　　话：010-57565859

开户银行：中国工商银行股份有限公司北京公主坟支行

帐　　号：0200004609200357746

中承国汇咨询（北京）有限公司
地址：北京市北京经济技术开发区万源街 22 号
电话：010-53383779

中 标 通 知 书

北京昊汉软件有限公司：

中承国汇咨询（北京）有限公司在此通知：通过评标委员会对改善办学条件-设备购置-网络安全等级保护实训中心建设项目其他不另分类的物品采购项目（招标编号：ZCGH-ZB-202205003）的认真评审和用户确认，贵公司为本项目的中标商。

中标内容：网络安全等级保护实训中心建设其他不另分类的物品

中标金额：¥2,472,000.00

请贵单位在接到本中标通知书后 30 日内尽快与招标人签订政府采购合同，并将合同扫描件自合同签订之日起 2 个工作日内发送至邮箱 zhongcgh@163.com，邮件标题注明项目编号和项目名称，我公司按相关规定办理投标保证金退还事宜。

中承国汇咨询（北京）有限公司

2022 年 06 月 08 日

详细分项报价表

报价单位:人民币元

序号	货物名称	型号（规格）	品牌	制造商和产地	单价	数量	单位	总价
1	NF 防火墙（内置防毒墙模块）	型号：AF-2000-B2130 规格：网络层吞吐量：10G，应用层吞吐量：8G，防病毒吞吐量：1.5G，并发连接数：220 万，HTTP 新建连接数：15 万； 硬件参数：内存大小：8G，硬盘容量：128G minisata SSD，电源：单电源，接口：6 千兆电口+2 千兆光口 SFP。 功能和资质要求： 1.具有操作系统，支持多核并行处理； 2.支持对文件传输行为进行安全过滤，支持基于上传、下载、双向的文件内容过滤，内容过滤类型至少支持网页、脚本、压缩文件、图片、可执行文件、适配、文本等常见文件类型； 3.支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能； 4.产品支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御； 5.产品支持对多重压缩文件的病毒检测能力，支持 8 层压缩文件病毒检测与处置； 6.产品支持病毒例外特征设置，根据文件 MD5 值和文件 URL 设置病毒白名单，不对白名单进行病毒查杀； 7.产品支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果；提供省级或以上检测机构出具的有效检测报告；	深信服	深信服 中国	160000	2	台	320000

		8.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生； 9.产品支持 CC 攻击防护功能，为保障 CC 攻击的检测效果，提供省级或以上检测机构出具的有效检测报告； 10.产品支持与本地蜜罐联动，实现对 APT 攻击的防御功能； 11.产品支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP； 12.产品支持与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理； 13.产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议； 14.产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。						
2	入侵防御系统	型号：AF-2000-B2150 规格：网络层吞吐量：25G，应用层吞吐量：9G，IPS 吞吐量：1.8G，并发连接数：220 万，HTTP 新建连接数：20 万； 硬件参数：内存大小：8G，硬盘容量：128GB ，接口：6 千兆电口+2 万兆光口 SFP+。 1.支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能； 2.支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别； 3.访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式，支持长连接功能并可以配置连接时长；	深信服	深信服 中国	195000	1	台	195000

		4.访问控制规则支持模拟策略匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 5.支持记录策略变更项、新增、删除、修改操作，变更前后的策略内容和类型对比详细变更记录，并支持导出办公软件如Office可以打开的记录，且开启后不能在界面上修改记录内容； 6.支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制； 7.支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测； 8.支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机IP地址； 9.支持对终端已被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； 10.对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告； 11.支持通过NTA技术检测恶意外联行为，对失陷主机访问的恶意域名进行统计，管理员可以在界面定位到外联的域名，并将域名进行解析，展示IP归属地； 12.设备具备独立的入侵防护漏洞规则特征库，特征总数在7400条以上； 13.支持对服务器、客户端、口令暴力破解、恶意软件等漏洞攻击防护；支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能；						

		14.可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； 15.支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险； 16.支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证。						
3	上网行为管理	型号：AC-1000-B2100-H5 规格：网络层吞吐量（大包）：10Gb，应用层吞吐量：1.5Gb，支持用户数：6000，每秒新建连接数：14000，最大并发连接数：600000； 硬件参数：内存大小：8G，硬盘容量：128G SSD，电源：单电源，接口：6千兆电口+2万兆光口SFP+。 功能和资质要求： 1.支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略； 2.支持针对特权用户配置免认证key、免审计key、免控制key； 3.必须支持网关类型为HTTP协议时，发送国家码可配，适配海外用户认证需求； #4.支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证； 5.支持哑终端通过MAC认证的方式接入网络，必须支持在终端管理列表批量绑定设备IP/MAC快捷放通入网； 6.支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP	深信服	深信服中国	119000	1	台	119000

		表的工作量； 7.支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网； 8.无需安装客户端，通过流量状况检查10款以上主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复； 9.支持用户可以自定义产生根证书，导入包含秘钥的根证书； 10.支持审计用户的Webmail邮件外发行为，支持webmail形式发送的附件审计，并能精准到原始邮件；必须能审计用户通过SSL加密Webmail网站外发邮件的内容；支持审计用户外发Email邮件的正文及附件；必须能审计用户使用邮件客户端外发SSL加密邮件的邮件内容和附件，必须支持网易闪电邮、foxmail、钉钉邮箱； 11.支持telnet协议，可对登陆的账号、执行的命令进行审计；支持SSH/RDP协议，可对连接开始时间，连接结束时间，传输的流量大小进行审计；支持运维类应用的外发附件审计，包括Xshell，Pshell，MobaXterm，SecureCRT； 12.支持FTP协议上传、下载文件的审计，支持FTP传输客户端的外发附件审计，包括WinSCP、XFftp，FileZilla、SecureFX； 13.支持Teamviewer、向日葵、Anydesk、RDP的远程应用的外发文件审计； 14.数据中心可以对上网日志进行大数据分析，并支持多个大数据分析模型，包括泄密分析、离职倾向分析、上网态势分析、带宽分析、工作效率分析，可导出报表； 15.内置多套日志模板与日志平台对接，至少支持以下平台：派博、任子行、网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等；						

		16.能够与同品牌下一代防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；						
4	威胁分析系统	型号：YJ-1000-B1075 授权：系统漏扫授权 IP 数：100，WEB 漏扫授权 URL 数：20；性能指标：主机漏扫最大并发 IP 数：75，WEB 漏扫最大并发 URL 数：5； 硬件参数：内存大小：8G，硬盘容量：128GB SSD+ 2TB SATA，电源：单电源，接口：6 千兆电口+2 千兆光口 SFP。 功能和资质要求： 1.支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情； 2.支持全局风险统计时段自定义，展示近 3 个月、6 个月、1 年或自定义统计区间的风险分布和详情，时间跨度不限制； 3.支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行； 4.支持检测的漏洞数大于 19000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准； 5.内置不同的系统漏洞模板，包括高可利用系统漏洞、原理检测系统漏洞、中间件漏洞、数据库漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览，支持报表形式展示漏洞模板详情，包括漏洞总数、漏洞名称、漏洞类型、风险等级等信息； 6.支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等； 7.内置不同的 WEB 漏洞模板，包括高可利用 WEB 漏洞、通用应用漏洞、	深信服	深信服 中国	314000	1	台	314000

		SQL 注入漏洞、XSS 注入漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览，支持报表形式展示漏洞模板详情，包括漏洞总数、漏洞名称、漏洞类型、风险等级等信息； 8. WEB 漏洞扫描支持高级配置功能，可支持 fuzz 测试启用、WEB 访问策略、WEB 爬行策略等配置功能。支持并发线程数、超时限制、目录深度、链接总数自定义配置； 9. 支持域管理功能，系统默认内置数据域、终端接入域、运维管理域等，可根据客户实际情况进行自定义管理； 10. 支持业务系统登记功能，保护等级支持第二级和第三级，可根据不同域类别添加资产到业务系统中； 11. 提供检测结果综述分析，按照等保 2.0 的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况； 12. 按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认； 13. 支持统一管理所有业务系统的合规情况，合规报告可导出。业务系统差距报告量化、可视化整改前后的符合情况和安全问题； 14. 产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表。						
5	安全审计设备	型号：LAS-1000-A600 性能参数：包含主机审计许可证书数量：50，可用存储量：2TB（RAID1 模式），平均每秒处理日志数（eps）最大性能：1200； 硬件参数：6 千兆电口，内存 8G，硬盘容量：64GB minisata+1TB SATA*2，	深信服	深信服 中国	193000	1	台	193000

		USB 接口 2 个，串口(RJ45)1 个，电源：单电源。 功能和资质要求： 1.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等 720 种日志对象的日志数据采集； 2.支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射； 3.支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用； 4.支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志； 5.支持 TLS 加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量； 6.支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件； 7.支持日志检索数据的投屏；支持日志查询结果的统计与导出，支持历史备份文件导入查询； 8.支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括 base64、Unicode、GBK、HEX、UTF-8 等； 9.支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析； 10.支持网站攻击、漏洞利用、C&C 通信、暴力破解、拒绝服务、主机						

		脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上，支持自定义关联分析规则； 11.支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件； 12.日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量； 13.支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析。 14.支持自定义首页卡片，支持实时监控系统日志传输量和日志留存的合规情况； 15.支持个性化定制，支持全系统更换logo与系统名称，支持一键恢复默认； 16.支持POC测试工具一键生成数据。						
6	Web应用防火墙	型号：AF-1000-B1810 性能参数：网络层吞吐量：12G，应用层吞吐量：4.4G，全威胁吞吐量：650M，并发连接数：200万，HTTP新建连接数：8万； 硬件参数：内存大小：8G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP。 功能和资质要求： 1.产品支持IPSec VPN智能选路功能，根据线路质量实现自动链路切换； 2.产品支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求； 3.产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控	深信服	深信服 中国	210000	2	台	420000

		功能； 4.产品支持对常见 Web 应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义 Web 应用漏洞特征库超过 3320 种； 5.产品支持对请求报文头的 X-Forward-For 字段检测，并对非法源 IP 进行日志记录和联动封锁； 6.产品支持 CC 攻击防护功能； 7.产品支持未知威胁检测能力； 8.产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生； 9.产品支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制； 10.产品支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP； 11.产品支持与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理； 12.产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理； 13.产品支持管理员双因素认证功能，用户通过用户名/密码和 Key 等不同方式登陆产品管理界面；						
7	安全运营中心	型号：NTA-100-B620 规格：网络层吞吐量：1.5Gbps；硬件参数：内存大小：16G，硬盘容量：128GB SSD+2TB SATA，电源：单电源，接口：6 千兆电口+2 千兆光口 SFP。	深信服	深信服 中国	380000	1	台	380000

		功能和资质要求： 1.提供安全分析大屏，能够展示资产分布，看清内网风险终端和风险资产概况，能够提示终端和服务器资产数据，能够展示风险终端和服务器数量。能够基于资产展示 web 明文、弱密码等脆弱性概况。能够展示风险终端和服务器 top5 安全事件； 2.提供安全分析大屏，支持大屏投放，能够看清内网互联网，业务服务器和终端之间的流量大小，能够展示内网资产 ip 和名称，能够展示服务器和终端之间的访问关系，基于时间维度展示安全事件态势，能够对热点安全事件进行播报展示，能够对事件等级分布进展，能够下钻分析，下钻提供安全详细事件举证； 3.支持待处置安全事件描述、事件标签、攻击阶段、事件分类、失陷确定性、威胁等级、风险主机统计、发生时间、处理状态以及自定义待处置事件； 4.支持对主流挖矿协议、矿池地址识别检测，挖矿病毒下载行为进行检测，挖矿配置文件下载识别等手法，针对主流的挖矿病毒的恶意流量通过智能分析进行聚类并提取相关指纹进行检测支持各大挖矿家族的变种识别； 5.针对挖矿做专项性分析，比如挖矿的币种分布，威胁趋势分析； 6.支持对僵木蠕的安全告警做专项性分析，比如僵木蠕威胁常用的攻击手法以及威胁趋势分析。将发生的所有安全事件默认按照处置状态，威胁等级，确定性等级，攻击结果、事件类型等维度进行筛选展示，并结合攻击阶段、事件统计和事件趋势等进行统计和显示、可实时监控发生的安全事件； 7.支持对勒索病毒的安全告警做专项性分析，比如中了勒索病毒的风险主机分布、威胁趋势分析，将发生的所有安全事件默认按照处置状态，威胁等级，确定性等级，攻击结果、事件类型等维度进行筛选展示，并						

		结合攻击阶段、事件统计和事件趋势等进行统计和显示、可实时监控发生的安全事件； 8.支持对隐蔽隧道的告警做专项性分析，比如攻击者利用哪些协议进行隐蔽通信以及威胁趋势分析，将发生的所有安全事件默认按照处置状态，威胁等级，确定性等级，攻击结果、事件类型等维度进行筛选展示，并结合攻击阶段、事件统计和事件趋势等进行统计和显示、可实时监控发生的安全事件； 9.支持对威胁情报的安全告警做专项性分析，比如通过情报匹配的风险主机分布、威胁趋势分析，将发生的所有安全事件默认按照处置状态，威胁等级，确定性等级，攻击结果、事件类型等维度进行筛选展示，并结合攻击阶段、事件统计和事件趋势等进行统计和显示、可实时监控发生的安全事件； 10.针对网站威胁的安全告警做专项性分析，比如网站攻击类型的分布以及威胁趋势分析。将发生的所有安全事件默认按照处置状态，威胁等级，确定性等级，攻击结果、事件类型等维度进行筛选展示，并结合攻击阶段、事件统计和事件趋势等进行统计和显示、可实时监控发生的安全事件，能复制攻击 IP、XFF 代理，并展示事件域名、http 状态码辅助进行事件分析； 11.支持邮件威胁分析，可展示收件人 TOP5、发件人账号 TOP5、恶意邮件类型分布、危害和处置建议；支持对恶意邮件详情分析，包含收件人账号、恶意邮件数量、发件人账号、附件名称、病毒名称、恶意链接名称等，并支持导出分析结果； 12.支持文件威胁分析，可展示文件分析过程、文件检测趋势、恶意文件 TOP5；支持恶意文件的详情分析，包括支持记录恶意文件感染的主机、所属 IP、文件名、病毒名称、传输协议等；支持导出文件威胁分析结果；						

		13.支持沙盒文件检测，能够对 exe 可执行文件、dll 应用程序扩展、BAT 批处理文件、PDF、office、VB 脚本、PHP 网页脚本、PY 脚本等进行检测； 14.支持安全检测日志、审计日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS 攻击、邮件安全、文件安全、网络流量、DNS、HTTP、POP3、SMTP、IMAP 等； 15.支持检测 7 类以上常见协议 FTP、LADP、mysql、POP3、SMTP、TELNET、WEB 等的弱密码，支持镜像流量检测业务系统中的弱密码，检测列表包含账号、密码、服务器、所属分析和业务、最近登录源 IP、类型、最近发现时间等信息，密码星号显示需超级管理员才可查看，并支持储存数据包内容； 16.支持联动同品牌 EDR 对主机下发全盘/快速扫描，且可对发现的威胁文件进行隔离/信任等操作； 17.支持与同品牌防火墙进行联动响应，支持系统下发安全策略到防火墙上，阻断攻击流量。						
8	运维安全管理系统	型号：OSM-1000-B1150-S3 规格：包含运维授权数：50，最大可扩展资产数：150，图形运维最大并发数：100，字符运维最大并发数：200； 硬件参数：内存大小：8G，硬盘容量：2T SATA，电源：单电源，接口：6 千兆电口。 功能和资质要求： 1.支持通过动作流配置提供广泛的应用接入支持； 2.内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴； 3.支持 RDP 安全模式（RDP、NLA、TLS、ANY）设置； #4.支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，	深信服	深信服 中国	216000	1	台	216000

		每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作； 5.支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批； 6.支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式； 7.支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人； 8.支持 RDP 协议的控制台登录控制； 9.支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用 SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP 等客户端工具实现单点登陆，不改变运维人员操作习惯； 10.图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放； 11.支持标准 SNMP v1、v2、v3 管理协议，支持 syslog 等标准日志格式外发； 12.全面支持 IPV6，设备自身可以配置 IPV6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登陆和审计； 13.支持从 WEB 页面设置多端口绑定，防止单网卡或单网线故障发生； 14.全面支持 Windows、linux、国产麒麟系统、Android、IOS、Mac OS 等客户端操作系统下的 H5 页面一站式运维，实现跨终端适应性 BYOD（Bring Your Own Device）；						

		15.提供等级保护咨询； （1）等级保护定级咨询。依据国家信息安全等级保护相关标准、文件要求和行业定级要求，协助系统定级，编写定级报告（按系统编写），依据《信息安全等级保护备案实施细则》制订系统定级报告，编制备案表并完成备案。 （2）系统预测评。提供 1 个系统的等保预测评，并提供相应文档； （3）等级保护差距评估服务。依据国家信息安全等级保护相关标准和文件要求，结合客户信息系统的安全保护等级，对信息系统安全等级保护状况进行安全评估，对信息安全管控能力进行考察和评价，确定信息系统安全保护能力是否达到相应等级基本要求的过程，以帮助客户及时发现信息安全风险。 （4）等级保护整改咨询服务。根据定级和等级差距评估的结果，进行总体分析，分析用户的安全需求，依据国家信息安全等级保护相关标准和文件要求，满足客户在技术和管理层面的安全需求的前提下，进行安全规划和设计；根据整改设计方案，进行技术整改（安全产品集成、安全加固）、管理整改，从而满足等级保护要求，并协助客户完成等级保护测评。 17.提供漏洞扫描服务； （1）Web 漏洞检测：利用专业的漏洞检测系统对 web 应用系统进行漏洞检测，并根据扫描结果提供扫描分析报告和整改建议。 （2）主机系统漏洞检测：利用专业的漏洞检测系统对操作系统、数据库、中间件、网络及安全设备进行漏洞检测，并根据扫描结果提供扫描分析报告和整改建议。 18.提供网站安全监测服务； （1）对风险评估报告中的高危漏洞进行专家验证，确保高危事件的准确性，并定期给用户推送云扫描报告。						

		（2）出现 0Day 漏洞时，主动对所监控用户业务做扫描发现，重要网络安全事件和安全漏洞快速预警通告和检测，检测结果第一时间定向推送到客户，能够支持微信端实时推送告警信息； （3）支持对目标站点提供网页敏感词检测能力。发现网页敏感词事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现； （4）支持页面响应监测，通过固定的频率模拟用户请求访问被监控站点，实时获取站点的响应状态和请求详情，精准的探测出网站的各种异常 3 分钟检测一次，当连续 3 次访问失败时判断为业务不可用； （5）支持网站存活监测，通过固定的频率探测被监控站点存活状态 （6）对目标站点的关键页面进行实时篡改监测，分钟级篡改发现，第一时间通过微信进行实时告警，并提供主动电话告警； （7）支持整站内容进行篡改监测，梳理并在首页展示站点结构图，显示网站各节点是否存在被篡改事件； （8）支持对目标站点提供网页黑链监测能力。发现网页黑链事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现； （9）支持以微信的方式对篡改、挂马、网站不可用等安全事件进行实时告警，支持微信端内容的及时推送； （10）支持邮件的方式推送安全事件报告、月报运营报告，便于站点安全的管理； （11）支持提供可视化的篡改监测界面，首页可直观展示篡改监测过程和监测结果，如正在监测哪一个页面，历史监测页面的安全状况等，便于实时掌握业务风险情况； （12）网站篡改事件应支持查看“举证图片”， 管理人员可通过微信及 web 登录界面，直观查看被篡改内容，便于第一时间掌握被篡改的情况。 19.提供安全测评服务。 提供一年的网站安全监测服务，提供 Saas 可视化自服务平台服务、黑						

		词/黑链检测、网站漏洞扫描、挂马监测、可用性监测、页面篡改监测、域名解析监测、敏感内容监测。通过网站安全监测平台对网站进行自动化监测，通过邮件进行及时报警，每月发送监测报告。						
9	终端安全系统	型号：HHV1.0； 规格：数量：300 个终端授权； 1.Windows PC 客户端支持:Windows XP/Windows Vista/Windows 7/Windows 8/Windows 8.1/Windows 10 ； 2.支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量（需提供功能截图，并加盖厂商公章）； 3.支持同时展示跟同品牌下一代防火墙、安全感知平台、上网行为管理，云端 SOC 平台，SAAS 化管理平台的联动状态； 4.支持安全策略一体化配置，通过单一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、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录； 5.支持资产登记功能，支持录入本终端所属责任人、责任人联系方式、邮箱、资产编号、资产位置信息，并可设置哪些为必填项，以便于进行终端资产管理； 6.支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、半夜登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户； 7.支持根据统计周期、终端名称、IP 地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，合规检测日志的查询和检测；	昊汉软件	昊汉软件中国	400	300	个	120000

		8.支持客户端的错峰升级或灰度升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴； 9.支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离； 10.支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截； 11.提供挖矿病毒巡检工具，支持通过内存、进程和启动项来检索病毒相关信息； 12.支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、最后攻击时间、发现方式、攻击内容、攻击历史； 13.支持基于IP（组）、服务和角色维度进行配置项设置，并且支持对配置项的备份以及恢复操作； 14.支持与同厂商的上网行为管理平台进行安全联动，支持管理员在上网行为管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息； 15.支持管理员在同厂商的上网行为管理平台界面下发一键隔离指令，对终端恶意文件进行隔离，防止病毒进一步扩散。						
10	信息安全等级保护课程资源包	型号：V1.0 规格： 一、内容要求 内容涵盖安全漏洞扫描工具的使用，以及网站安全监测工具的使用，包括Xsser扫描工具、Weevely扫描工具、同源策略、evel注入、文件上传、Wireshark流量监控、目录遍历、Wvs扫描工具、AppScan扫描工	昊汉软件	昊汉软件中国	195000	1	套	195000

		具等内容。课程内容按照等级保护测评工作流程进行课程内容设计。 二、数量要求 微课数量 20 个，总时长 100 分钟；动画数量 20 个，总时长 1200 秒。 三、技术要求 1.格式要求：PPT 课件，扩展名包括*.ppt、*.pptx；2.PPT 课件与微课视频相匹配；3.微课拍摄需组织具备丰富的人工智能教育背景经验，设计制作整理脚本完整内容制作；根据知识点需求拍摄制作微课视频；4.微课要求画面美观、画质音质清晰、信号稳定，无扭曲、晃动、抖动、闪耀等现象等；5.拍摄形式多样化，根据课程内容选择：实景拍摄、抠像拍摄、大屏拍摄、布景拍摄等；6.稳定性：全片图像同步性能稳定，无失步现象，CTL 同步控制信号必须连续；图像无抖动跳跃，色彩无突变，编辑点处图像稳定；要求声画同步；7.色调：白平衡正确，无明显偏色，多机拍摄的镜头，衔接处无明显色差；8.课程拍摄分辨率 1080p，1920×1080，25fps，PAL；9.配置专业无线耳机，全程收集教师声音，保证无杂音、噪音等；10.片头和片尾的总长控制在 10-15 秒；11.片头片尾可包括:学院 LOGO、课程名称、主讲教师姓名、单位等信息；12.采用广播级动画、特效制作及非编系统，如：Final Cut Pro 、Edius 非编系统、After Effects、3DSmax、CINEMA 4D、Audition、Photoshop 等软件进行制作，将视频演示、特效效果和实景素材串接，提高观赏性和感染力；13.单独制作字幕文件，字幕文件采用 srt 格式，字幕使用符合国家标准的规范字，不出现繁体字、异体字、错别字。					
总价						2472000	

详细服务分项表

序号	服务项目	服务项目详细说明	服务频次
1	安全测评	学校完成等级保护安全建设整改工作后，等级保护测评机构对学校的本次项目中的信息系统实施一次等级测评，确认现状测评过程中发现的高危风险问题已经通过整改工作得到解决，确保系统的安全防护水平达到国家信息安全等级保护相应等级的要求。	1 次
2	网站安全监测	域名数量 1 个 1、对风险评估报告中的高危漏洞进行专家验证，确保高危事件的准确性，并定期给用户推送云扫描报告。 2、出现 0Day 漏洞时，主动对所监控用户业务做扫描发现，重要网络安全事件和安全漏洞快速预警通告和检测，检测结果第一时间定向推送到客户，能够支持微信端实时推送告警信息； 3、支持对目标站点提供网页敏感词检测能力。发现网页敏感词事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现； 4、支持页面响应监测，通过固定的频率模拟用户请求访问被监控站点，实时获取站点的响应状态和请求详情，精准的探测出网站的各种异常 3 分钟检测一次，当连续 3 次访问失败时判断为业务不可用； 5、支持网站存活监测，通过固定的频率探测被监控站点存活状态 6、对目标站点的关键页面进行实时篡改监测，分钟级篡改发现，第一时间通过微信进行实时告警，并提供主动电话告警； 7、支持整站内容进行篡改监测，梳理并在首页展示站点结构图，显示网站各节点是否存在被篡改事件； 8、支持对目标站点提供网页黑链监测能力。发现网页黑链事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现。 9、支持以微信的方式对篡改、挂马、网站不可用等安全事件进行实时告警，支持微信端内容的及时推送； 10、支持邮件的方式推送安全事件报告、月报运营报告，便于站点安全的管理 11、支持提供可视化的篡改监测界面，首页可直观展示篡改监测过程和监测结果，如正在监测哪一个页	3 年

		面，历史监测页面的安全状况等，便于实时掌握业务风险情况； 12、网站篡改事件应支持查看“举证图片”， 管理人员可通过微信及 web 登录界面，直观查看被篡改内容，便于第一时间掌握被篡改的情况。	
3	等级保护咨询	**等级保护定级咨询：** 依据国家信息安全等级保护相关标准、文件要求和行业定级要求，协助系统定级，编写定级报告（按系统编写），依据《信息安全等级保护备案实施细则》制订系统定级报告，编制备案表并完成备案。 系统预测评： 提供系统的等保预测评，并提供相应文档； 等级保护差距评估服务： 依据国家信息安全等级保护相关标准和文件要求，结合客户信息系统的安全保护等级，对信息系统安全等级保护状况进行安全评估，对信息安全管控能力进行考察和评价，确定信息系统安全保护能力是否达到相应等级基本要求的过程，以帮助客户及时发现信息安全风险。 **等级保护整改咨询服务：** 根据定级和等级差距评估的结果，进行总体分析，分析用户的安全需求，依据国家信息安全等级保护相关标准和文件要求，满足客户在技术和管理层面的安全需求的前提下，进行安全规划和设计；根据整改设计方案，进行技术整改（安全产品集成、安全加固）、管理整改，从而满足等级保护要求，并协助客户完成等级保护测评。	3 年
4	安全漏洞扫描	**Web 漏洞检测：** 利用专业的漏洞检测系统对 web 应用系统进行漏洞检测，并根据扫描结果提供扫描分析报告和整改建议。 主机系统漏洞检测： 利用专业的漏洞检测系统对操作系统、数据库、中间件、网络及安全设备进行漏洞检测，并根据扫描结果提供扫描分析报告和整改建议。	按年服务，持续 3 年，每年 6 次漏洞扫描并提供漏扫报告

5	等级保护 2.0 安全运营服务	现状分析	网络拓扑	了解客户网络现状，需要了解客户网络中规划了几个区域，各个区域的功能，区域之间如何隔离、互联及防护，安全设备有哪些； 具体方式：了解客户出口设备，出口链路有几条，分别是哪几个运营商，带宽多大； 再了解出口到核心之间有哪些设备（安全设备、网络设备，设备功能、厂商、采购年限，尽量详细）各个设备从上往下如何互联； 再了解核心与各个汇聚交换机如何互联（条件可以的话可以详细到接入交换机）； 了解客户是否规划 DMZ 区域、服务器区域，若有了解区域之间是否有安全设备做防护，区域、安全设备如何连线；再了解是否规划安全管理区域，安全区域有哪些设备，如何接入主干网络。 根据和客户了解的情况以及现场机房理线的结果和客户现有的网络拓扑图进行对照，对客户现有网络拓扑图进行更新	一年 6 次，持续三年，提供《网络拓扑文档》
			机柜图	进入机房进行实地理线统计，对各个机柜的设备进行统计，包括设备处于机柜的位置，管理 IP，设备功能、厂商、型号、采购年限，若是服务器需标注承载的业务。 统计完成后整理形成机柜图。	一年 6 次，持续三年，提供《机柜图》
			资产	了解客户有哪些业务，各个业务的具体名称、功能、IP 地址，承载业务的服务器是实体服务器还是虚拟机，操作系统、中间件、数据库类型，业务负责人是谁； 通过核对这些信息整理出业务资产表。	一年 6 次，持续三年，提供《资产统计表》

			VLAN/网段	和客户沟通学校 VLAN 和网段是如何划分的， 具体：询问客户网络划分了多少个网段，VLAN 是多少，各个网段的用途（有线网段、无线网段、监控网段、服务器网段、管理网段等）；询问客户是否有现有材料，若有可以直接从客户处获取，若无通过登录核心汇聚交换机，查看配置获取。	一年 6 次，持续三年，提供《VLAN/网段统计表》
		安全基线	安全物理环境	物理位置选择：机房位置为防震、防风和防雨 物理访问控制：电子门禁系统 防盗窃和防破坏：设备固定+设备标签，线缆铺设隐蔽安全 防雷击：电路设计，有接地 防火：火灾自动消防系统，机房建设-耐火材料 防水和防潮：窗户、屋顶、墙壁的防水方法，可靠的排水通道，精密空调下部署水坝 防静电：防静电地板，设备合理接地 温湿度控制：机房空调/精密空调 电力供应：稳压器（UPS） 电磁防护：强弱电分开（电源线、网线）	一年 6 次，持续三年，
			安全区域边界	网络架构：有网络拓扑，根据网络使用和业务关系划分 VLAN，边界隔离，部署数据中心区域 通信传输：客户端到服务器、服务器到服务器之间要使用 SSL 等通信（SSH、HTTPS） 是否有可信验证机制	一年 6 次，持续三年，

			安全通信网络	边界防护：所有区域边界设置访问控制列表 访问控制：是否有 ACL 控制列表，是否最小化，设置边界访问控制策略，针对业务系统设置访问策略 入侵防范：是否有检测网络入侵行为（检查对象：入侵保护系统、入侵检测系统、抗 APT 攻击、抗 DDoS 攻击和网络回溯等系统或设备。） 恶意代码和垃圾邮件防范：（防病毒网关和 UTM 等提供防恶意代码功能的设备或系统）防御网络恶意代码 安全审计：记录用户上网行为，分析记录设备日志，外置数据中心、存储容量 180 天 是否有可信验证机制	一年 6 次，持续三年，

			安全计算环境	身份鉴别：设备设置登录认证功能；用户名不易被猜测，口令复杂度达到强密码要求（对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。） 是否具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施 远程管理是否使用 SSH、HTTPS 加密 访问控制：是否配置三权分立 安全审计：记录用户上网行为，分析记录设备日志，外置数据中心、存储容量 180 天 入侵防范：操作系统遵循最小安装原则 确认仅使用端口开放 操作系统配置终端接入方式、网络地址范围 系统配置项（如登录对输入框输入的内容进行长度、位数及复杂度验证等）； 漏洞加固 恶意代码防范：服务器和 PC 装终端杀毒 可信验证：如有加分项，无不做减分项 数据完整性：系统使用 HTTPS，SSL，保证重要数据在传输过程中的完整性 数据备份恢复：重要系统定期备份，容灾备份系统 剩余信息保护：利旧、报废设备信息删除（格式化或存储破坏） 个人信息保护：个人信息采集最小化，禁止未授权访问和非法使用用户个人信息	一年 6 次，持续三年，

			安全管理中心	系统管理：a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、 系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。（通过堡垒机访问，并审计） 审计管理：a) 应保证审计管理员通过管理工具或平台进行安全审计操作，并对这些操作进行审计；（设立审计管理员+所有管理设备审计） b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。（设立审计管理员+所有管理设备审计，定期进行日志分析与备份）	一年 6 次，持续三年，
		安全现状评估服务	安全巡检	设备安全检测：工程师定期进行设备巡检，同时进行系统安全检查，并根据检查结果，优化配置策略	一年 6 次，持续三年，提供《巡检报告》
			日志分析	日志分析：针对所有安全设备及业务系统的日志进行定期检查，并根据检查结果进行总结报告。	一年 6 次，持续三年，提供《日志报告》
			配置检测	针对网络设备、安全设备、操作系统、数据库、中间件等存在的不当配置进行检测，并提供安全配置检测分析报告及安全加固建议。	一年 6 次，持续三年，提供《配置检测分析报告及安全加固建议》
			策略检查	安全策略检查：针对 IT 环境中的服务器、网络设备、安全设备进行策略检查，并根据检查结果提供改进建议	一年 6 次，持续三年，提供《安全策略分析报告》

			安全设备管理	定期检查所有安全系统及设备的特征库版本，保持事件特征库为最新状态，有重大漏洞公布时，及时更新相应特征库；配合业务系统部署与调整，从安全角度给出部署建议，制定和更新安全设备的防护、检测策略；提供在安全设备故障处理过程中的协调和配合服务。	不限次
			安全通告	安全通告服务：为客户提供最新的安全动态、技术和定制的安全信息，包括实时安全漏洞通知、病毒、补丁升级、定期安全知识库更新等	不限次
			安全加固	安全加固:系统安全加固是指通过一定的技术手段，提高操作系统或网络设备安全性和抗攻击能力，经过加固的系统或设备，除了免除现有安全漏洞的威胁外，系统的抗攻击性也会有极大的增强，提供安全加固建议，以及安全加固方案	不限次
		入侵行为处置	入侵影响抑制	通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。	不限次，提供《入侵行为处置报告》
			入侵威胁清除	排查攻击路径，恶意文件清除。	
			入侵原因分析	还原攻击路径，分析入侵事件原因。	
			加固建议指导	结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。	
		渗透测试服务	渗透测试	结合采购人需求，通过现场或远程方式对采购人的内部系统、外部网站进行各种安全渗透测试，找出测试目标存在的安全问题，提出可操作的问题修补建议。	1年1次，持续三年，提供《漏洞扫描报告》
		安全应急服务	应急处置服务	应急响应：突发性安全事件发生时，第一时间进行响应，帮助客户及时有效的解决	不限次，提供《应急支撑记录》、《应

			安全事件处理	安全事件处理：在紧急事件或安全事故发生时，通过安全事件处理消除安全事件威胁，避免和减少事件的损失，打击非法入侵者，健全和改善信息系统的安全措施	急支撑报告》
			应急预案体系咨询	依据国家相关标准规范，结合组织管理要求和业务特点制订应急预案体系。	
		安全威胁处置	威胁处置	安全威胁处置服务，对安全威胁进行分析，及时处置安全事件，并对事件进行及时的溯源分析。再加上网络安全应急响应服务，将安全问题进行闭环处置。	不限次，每次处置提供《安全威胁处置报告》
		重要时期重保服务	重保保障	国家重要会议及活动、高考、中考期间，提供不少于 1 人的保障服务，负责单位安全设备及安全检测系统的日常运维，包括运行状态日检、检测，对安全设备及安全监测系统的策略调优、每天对安全设备日志信息和安全监测系统告警信息进行深入分析，及时发现安全威胁，并进行验证、处置及报告。	学校指定各重点保障时间点，每次提供《安保工作报告》
		模拟攻击和防御	攻防演练模拟	在专业的安全人员设计并搭建的网络及应用环境中进行模拟入侵及防御。模拟网络及应用的安全人员将同时设计一套可实施的、闭环的演练场景用以模拟安全事件。可以通过模拟的演练场景亲身参与到安全事件攻防之中，进而充分了解安全事件中攻、防双方的思路及实践方法。	根据客户需求，提供攻防演练报告
		安全培训服务	安全培训	安全管理、安全技术、安全意识等。安全培训：针对信息中心老师技术、管理和政策培训；以及学生的培训 提供安全小册子和小礼品。	每年 1 次，持续三年，提供培训素材和小礼品

		等级保护 2.0 安全运营服务	安全运营报告	等级保护 2.0 安全运营报告：等级保护 2.0 安全运营服务（一年 12 次的安全运营服务报告），每个月一次，每个月提供一本纸质版安全运营报告，全年共 12 本。每年提供上半年和下半年安全运营汇报 PPT。	一年 6 本，持续三年，提供安全运营报告和汇报 PPT