服务需求一览表

序号	设备名称	技术参数	数量	备注
1	可管理的威胁分析与响应服务	1、功能要求 （1）、全流量分析服务 利用机器学习引擎和规则检测能力，及时发现网络安全事件线索，及时检测病毒木马、网络攻击等安全事件情况；开展全流量关联和取证，能够从多维度多角度进行长时间跨度的关联分析，同时提供渐进式安全事件分析和取证；可进行特定安全场景分析能力，能够快速实现客户提出的一些安全场景并进行场景分析。 （2）、事件场景分析 对事件告警进行关联分析并输出用户关注的重点事件，如热点事件、apt 攻击事件、Botnet 事件、恶意样本传播事件或是单次高危攻击事件等（webshell、隐蔽信道）。同时，用户也可以根据自身业务特点自定义事件类型进行输出，帮助用户从海量告警中快速发现需要处理的重点事件。 （3）、失陷资产排查 根据攻击方向、攻击类型等维度对失陷资产进行判断，从资产角度出发，结合攻击链模型向用户展示失陷资产的总体情况，帮助用户从海量告警事件中，快速定位需要关注和处理的资产。 （4）、攻击者画像 从攻击者的角度出发，为用户梳理出对网络最具威胁的攻击者，通过情报关联功能，追溯攻击者的相关信息，聚合攻击者在用户网络中的攻击行为和通信行为，增加攻击事件可信度，用户可以通过攻击者画像分析，回溯事件源头，从根本上处置类似攻击事件的发生。 （5）、数据回溯及 pcap 包取证 可通过情报或用户自定义规则，对历史流量数据进行回溯，提供 pcap 包取证服务。 2、技术参数 （1）、提供数据包 pcap 文件存储服务，提供在探针端存储数据包。并提供通过平台下载数据包。 （2）、提供提供融合模式匹配、协议分析、异常检	1	

		测、会话关联分析，以及抗入侵检测服务。 （3）、提供 WEB 攻击检测服务，检测服务提供自学习。 （4）、提供但不限于 HTTP 协议、DNS 协议、邮件协议、FTP 协议、TELNET、数据库操作、SSL/TLS 协商记录、登录记录、认证记录、ICMP 协议、TCP 会话、UDP 会话等元数据提取服务。 （5）、提供对存储的流量日志进行回溯查询，包括 tcp，udp 会话日志，dns 解析日志，web 访问日志，邮件日志，文件传输日志，ssl/tls 协商日志，数据库操作日志，社会账号日志，登陆日志，认证日志，icmp 日志服务。 （6）、提供网络中传输的文件的查询和下载服务，文件类型包括 doc，docx，wps，wpt，dot，rtf，ppt，pptx，dps，dpt，pot，pps，xls，xlsx，exe，bat，dll，com，zip，rar，gzip，tar，bz 等。 （7）、提供对历史上出现过通信行为的资产 ip 进行查询服务，记录其首次出现时间和最近出现时间。 （8）、提供对历史流量进行回溯分析服务，分析模式提供插件上传，规则配置和黑名单配置，提供回溯的历史数据的时间跨度的配置。提供回溯分析结果的查询和展示。 （9）、提供历史流量数据的自定义查询服务，提供自定义的 sql，提供查询条件的保存。 （10）、提供展示 dns 的响应码的分布服务，提供基于 dns 响应码对应的 dns 记录的数量进行统计排序。 （11）、提供展示 http 响应码的分布服务，提供基于 http 响应码对应的 http 记录的数量进行统计排序。 （12）、提供监控流量探针实际流量，并进行可视化呈现服务。 （13）、提供各会话通信时常统计服务，根据会话记录中的持续时间，展示各个”时间区间”的记录数量。 （14）、提供漏洞利用检测服务，提供入侵检测服务，提供 web 攻击检测服务。 （15）、提供从攻击者的角度，聚合单个攻击者相关的所有攻击信息，并结合情报展示攻击者的信息。 （16）、提供威胁情报联动检测服务，使用威胁情报		

		进行精准检测。提供对流量进行实时匹配，对命中的流量产生实时告警。提供对流量进行回溯检测，解决攻击漏检的问题。		
2	云防御服务	1、通过云安全管理平台进行统一管理。识别和阻断 SQL 注入攻击，Cookie 注入攻击，命令注入攻击；支持爬虫防护、扫描防护；支持文件上传、下载过滤；识别阻断跨站脚本（XSS）注入式攻击；识别和阻断应用层拒绝服务攻击，非法上传阻断，包括 WebShell 攻击防护，对网页请求/响应内容中的非法关键字进行检测、过滤；识别和阻断应用层拒绝服务攻击；识别和阻断敏感信息泄露、恶意代码攻击；控制网络扫描行为，提供多种威胁处理方式；返回错误码、重定向、监控、默认动作等；支持 Cookie 加密，支持 Cookie 篡改劫持，支持 Cookie 加固。 2、DDOS 防护 （1）DDOS 畸形报文过滤, 过滤 frag flood、smurf、stream flood、land flood、攻击 ip 畸形包、tcp 畸形包、udp 畸形包 （2）传输层 DDoS 攻击防护，过滤 syn flood、ack flood、udp flood、icmp flood、rstflood （3）连接型 DDoS 攻击防护，过滤 TCP 慢速连接攻击、连接耗尽攻击、tcp 新建连接限制等（4）攻击和 loic、hoic、slowloris、Pyloris、xoic 等慢速攻击 特征过滤，4 层 ip+port 过滤和 7 层 payload 部分内容过滤 3、WEB 应用防护 （1）源站隐藏 隐藏源站的 IP 地址，防止黑客对源站直接攻击 （2）服务器指纹伪装 伪装服务器指纹信息，降低基于服务器类型及版本的攻击利用 （3）注入攻击防护 防止 SQL 注入攻击攻取或篡改网页数据；防止通过 SQL 猜测、获取甚至修改数据库信息；防止通过特定的代码脚本获取服务器敏感信息；防止通过提交操作系统命令获取系统敏感信息；防止 LDAP 注入控制用于目录搜索服务的过滤器；防止通过文件注	1	0

		入获取操作系统文件信息；防止 SSI 注入攻击。 （4）跨站脚本攻击防护 防止提交恶意跨站脚本；防止通过 IE8 浏览器提交恶意跨站脚本。 （5）通用攻击防护 防止 HTTP 请求走私、HTTP 响应分割和 Session-Fixation 攻击 （6）Webshell 上传防护 通过检测文件内容对上传的 webshell 文件进行过滤 （7）信息泄露防护 防止目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露 （8）扫描工具防护 自动识别扫描器的扫描行为，并智能阻断如 Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、Watchfire AppScan 、N-Stealth、Acunetix Web Vulnerability Scanner 等多种扫描器的扫描行为 （9）爬虫攻击防护 防止恶意爬虫抓取 （10）第三方组件虚拟补丁防护 WEB 容器漏洞；开源 CMS 漏洞；WEB 服务器插件漏洞 （11）HTTP 协议规范性检查 检测 HTTP 协议报文合法性，如协议违规、报头缺失、HTTP 方法限制、畸形请求、文件限制、头部长度限制等 （12）CC 攻击防护 通过 URL 访问速率和指定 URL 访问集中度检测对可黑客发起的同行竞争、刷票、黄牛抢票、商业爬虫抓取敏感信息、大量恶意请求等应用层 DDOS 攻击进行防护，通过基于地理位置的识别，可设置不同地理区域的检测算法 （13）防盗链 支持多种盗链识别算法能有效解决单一来源盗链、分布式盗链、网站数据恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问 （14）访问控制		

		对客户端 IP 放行或阻断		

其他补充内容：

1、实施地点：学校指定地点；

2、实施时间：2019 年 10 月 1 日-2020 年 9 月 30 日；

3、服务期：2019 年 10 月 1 日-2020 年 9 月 30 日；

4、验收标准：中标方保证其服务质量及技术达到国家现行技术标准和合同约定标准或投标文件承诺标准。针对项目要求中的技术要求进行逐一验证，满足服务要求中的各项指标，并提供相关的技术文档、实施文档及学校要求的项目验收报告；

5、其他售后服务等：中标方应对服务响应时间、解决故障的所需要的时间做出承诺。