POC测试用例	
序号	测试项
1	内置有监督机器学习模型，支持从加密流量中识别shadowsocks流量、v2ray流量。须提供功能录屏及提供第三方测评报告
2	内置有监督机器学习模型，支持对冰蝎、哥斯拉、蚁剑等webshell加密通信进行识别和发现。须提供功能界面截图及提供第三方测评报告
3	针对 SSL 通讯中证书名称、证书颁发机构、证书状态、证书起始日期、证书结束日期、证书有效期、加密套件、加密套件长度、加密套件列表等关键通讯参数进行分析，发现 SSL通讯中的异常。须提供功能界面截图
4	内置个人敏感信息模板，包括客户编号、客户名称、网站账户、联系人姓名、增值税注册地址、联系人地址、法人地址、用电地址、联系电话、电子邮箱、微信账号、QQ 号、居民身份证号、军人证号、护照号、台胞证号、驾驶证号等。需提供功能录屏。须提供第三方测评报告
5	针对HVV高频出现的漏洞、弱口令、端口进行专项告警呈现，高危漏洞告警字段至少包括：告警时间、攻击IP/端口、受害IP/端口、告警名称、威胁等级、研判结果、攻击阶段、详情、pcap取证等；高危端口告警字段至少包括：发送时间、目的IP/端口、告警名称、端口服务说明、端口服务标签、发生次数等；弱口令告警字段至少包括：告警时间、攻击/受害IP/端口、告警名称/详情、威胁等级、研判结果、攻击阶段、pcap包取证等。须提供功能界面截图
6	支持对包含：TCP、UDP、ICMP、SCTP、HTTP、FTP、SMTP、DNS、POP3、LDAP、TELNET、SSL、RDP、SNMP、SSH、VNC、Rlogin、SMB、NFS、DHCP、SIP、TFTP、NNTP、Radius、Kerberos等常见协议的深度解析和还原。
7	支持数据库协议的解析，包含：MSSQL、Oracle、MYSQL、Postsql、DB2、Dameng、Kingbase、Gbase、Redis、SYBASE、MEMCACHED等协议。
8	支持还原的文档类型：doc/docx、xls/xlsx、ppt/pptx、pdf、rtf、 wpt、pot、wps、pps、mpp、et、dpt、dps、ett、dot。
9	支持常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、RDP、VNC、pop3S、Telnet）爆破检测。
10	支持多种抗逃逸攻击检测，检测类型包括：PDF漏洞利用规避攻击、 Adobe PDF JavaScript文件规避攻击、Metasploit PDF漏洞利用规避攻击。
11	支持针对主流Web服务器及插件的已知漏洞攻击检测。Web服务器应覆盖主流服务器：apache、tomcat、lighttpd、NGINX、IIS等；插件应覆盖：dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress等。
12	支持爬虫检测，具备对100种以上的爬虫特征进行识别和检测的能力,检测特征至少包括 ：WebInspect、穿山甲扫描、appscan、 burpsuite扫描 、长亭xray社区版扫描、Acunetix Web Vulnerability Scanner、netsparker。
13	支持对WEB服务器上的文件下载进行检测，检测的文件扩展名包括ini、sql、mdf、mdb、prm、conf、htpasswd、backup、bak、old、bash history 。
14	支持HTTP慢速攻击检测，检测模型支持最小会话时长、最小平均请求报文、最小平均响应报文读取长度等参数配置。
15	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。

16	支持语义引擎检测，基于上下文和语义分析的高级检测技术，理解 HTTP 请求和响应的上下文关系，拥有复杂的嵌套编码和变形绕过的解析能力，能够识别复杂的攻击模式和拥有更低的误报和漏报率。
17	支持对告警进行一键例外，快速屏蔽掉业务异常告警。须提供功能界面截图。
18	支持对检测的告警事件（包含入侵检测告警、WEB应用告警、威胁情报告警、恶意文件告警和WEBSHELL告警)结合双向检测机制、元数据、原始数据包和研判模型进行深层次研判给出告警事件的攻击结果：尝试攻击、高可疑攻击、攻击成功、失陷。
19	支持对实时流量采集的pcap包进行全流量存储，供追溯分析和取证使用。须提供功能界面截图。
20	支持不同条件检索告警日志，包含时间、威胁等级、攻击IP、攻击端口、受害IP、受害端口、规则ID、报文方向、研判结果、攻击阶段、置信度、CVE-ID、CNNVD-ID、URI、SUCI、SUPI、接口类型等。