|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| 序 号 | 名称 | 功能描述 | 单 位 | 数量 | 质保期 |
| 1 | 大数据智 能安全平台 | 基于实时流数据为用户提供安全分析能力和 风险告警及多维度可视化展示。为企业安全 提供决策依据、提高企业信息安全的纵深防 御能力。包含以下引擎和模块：1、智能化威 胁检测引擎 2、多维度攻击溯源引擎 3、场 景化威胁感知引擎 4、集成化联动响应引擎 5、启发式威胁狩猎引擎 6、安全运营工作台 模块 7、可视化模型编排引擎 8、重大活动保障模块 9、资产管理模块。 | 套 | 1 | 3年 |
| 2 | APT流量探针 | 1.对网络中传输的文件进行分离和检测 2.对 各种WEB攻击进行检测 3.对邮件社工类攻击 进行检测 4.通过识别DGA域名请求、异常流 量等全方位发现失陷主机 5.通过识别内网中 横向扩散等行为发现可疑主机 6.对检测对象 的会话特征进行多维度监控7.对流量中的资 产进行分析，主动发现网络资产 8.提供多个 智能报表，方便快速总览网络威胁情况 9.提 供综合管理和关联分析能力，同时可提供云端高级分析服务。 | 套 | 1 | 3年 |
| 3 | 堡垒机 | 1、产品类型：信创堡垒机2、产品功能：具 有强大的输入输出审计功能，为用户内部提 供完整的审计信息，通过账号管理、身份认 证、 自动改密、资源授权、实时阻断、同步 监控、审计回放、 自动化运维、流程管理等功能增强运维管理的安全性。 | 套 | 1 | 3年 |
| 4 | 技术服务 | 1、安全威胁分析研判服务:专业安全服务人 员结合本次采购的大数据智能安全平台、AP T流量探针的告警数据、原始日志数据等进行安全事件分析研判；2、应急响应处置服务：遇到突发的网络安全 问题如：发生网络恶意入侵事件、病毒木马 感染、因上级通报安全事件等，开展应急处 置措施，包括事件响应、安全事件入侵追踪和取证。 | 套 | 1 | / |

|  |  |
| --- | --- |
| 2 | 大数据智能安全平台（ 一套）：1、★基础配置 软硬一体机设备（使用国产化CPU及操作系统），例CPU：飞腾，鲲鹏，海光等主流 CPU,操作系统：麒麟，统信等主流操作系统），冗余电源；千兆电口≥4个，万兆光口≥2个（含光模块），CPU≥2颗，单颗≥24核，内存≥256GB ，硬盘≥48TB；数据采集和处理性能≥12000EPS，≥200个日志源；提供3年软硬件维保及特征库升级服务。 |
| 3 | 2、安全态势：支持安全态势的可视化呈现，以安全态势大屏的方式从攻击事件、资产安全、追踪溯 源、运行监测、重保方案等多个维度进行可视化展示，提供不少于10块大屏展示界面，并可根据“组织架构”筛选大屏展示数据范围，支持自定义大屏轮播时间和大屏轮播顺序。 |
| 4 | 3、分析模型：平台须内置包括规则模型、关联模型、统计模型、情报模型等安全分析模型，同时用户可根据实际需求对上述模型进行添加、编辑、删除、复制等，用于提高平台安全管理效率； |
| 5 | 4、威胁情报：支持对接威胁情报中心，支持情报离线更新及在线更新，支持查看情报源中有效情报 数、最近更新条数、最近更新时间、今日更新情报数、昨日命中情报数等；支持以APP导入的方式对 接第三方威胁情报平台，至少支持对接奇安信、天翼安全、微步等厂商的威胁情报，支持对情报接口进行设置，设置内容包括情报查询、IP碰撞和域名碰撞接口的启用、请求频率限制； |
| 6 | 5、归并处置：支持用户自定义配置归并场景，支持场景名称、归并条件、归并字段、场景描述的配 置，其中可根据字段过滤配置归并条件；支持归并场景的开启、关闭，亦可拖动方式调整归并序列优先级顺序。 |
| 7 | 6、告警监控：平台的告警监控支持查看告警的攻击链、攻击流向、攻击者或受害者列表，以及查看 攻击者和受害者两个视角的ATT&CK矩阵视图，ATT&CK矩阵视图展示支持中文或英文的语言切换，布局支持侧面或下拉两种方式、并支持选择全部技术或子技术的展示等； |
| 8 | 7、告警管理：支持用户对告警级别的调整，平台通过自定义配置过滤条件对告警级别进行调整，并 支持选择适用不同的组织架构；告警级别支持相对级别的升降和绝对级别的高、中、低，规则可选择长期生效或定期生效。 |
| 9 | 8、 日志检索：平台的原始日志或原始告警支持多种语法查询，语法至少包括但不限于AND、OR、N OT、==、!=、>、<、>=、<=、exist、notexist、in、notin、startwith、endwith，语法可任意组合并支持利用中括号和小括号的嵌套查询。 |
| 10 | 9、支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；支持将检索语句一键翻译为中文，提高可读性。 |
| 11 | 10、取证溯源：支持聚合场景下的四维自定义攻击流向图取证，攻击趋势取证、攻击链分布取证和实 体信息取证，展示攻击者和受害者的威胁情报与资产信息，可查看会话详情，会话详情包括检测、响应等基本信息，并支持查看会话关联告警情况，及添加白名单、发布预警、生成工单等操作。 |
| 12 | 11、支持实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取，通过“一键溯源”按钮进行威胁关系的自动拓展。 |
| 13 | 12、 自动化编排响应：平台支持内置自动化编排响应功能，支持通过任务看板查看自动响应任务的数 量、任务状态占比、任务趋势；以时间轴方式展示任务进行状态，并可查看每个阶段任务运行的详细信息。 |
| 14 | 13、平台的自动化编排响应功能支持将联动设备能力封装到APP ，通过导入APP的方式实现和不同产品的联动，支持设置3层递进阻断策略。 |

|  |  |
| --- | --- |
| 15 | 14、流量探针管理：对接入到平台的探针进行统一运维监控，平台上可查看探针注册时间、设备IP、 版本信息、许可证信息、数据上送条数、CPU利用率、内存使用率、磁盘使用率、网络流量大小、数据上送条数等，并支持许可的导入和导出。 |
| 16 | 15、资产管理：支持人工录入、流量自动发现、主动扫描、web自动发现、资产同步等不少于5种的资产数据接入方式。 |
| 17 | 16、安全态势感知：平台须具备外部攻击态势、横向威胁态势、外联威胁态势、资产失陷态势、Web业务系统态势、资产整体态势、威胁溯源态势等安全能力。 |
| 18 | APT流量探针（ 一套）：1、★基础配置 软硬一体机设备（使用国产化CPU及操作系统，例CPU：飞腾，鲲鹏，海光等主流CP U,操作系统：麒麟，统信等主流操作系统），冗余电源；网络层吞吐≥5Gbps ，内存≥64G，硬盘≥12T；千兆电口≥4个，万兆光口≥2个（含光模块），提供3年软硬件维保及特征库升级服务。 |
| 19 | 2、全流量检测：支持全流量数据包检测，支持风险数据包保存功能，以帮助用户还原攻击过程，进行取证和关联分析。 |
| 20 | 3、攻击行为检测：支持检测WEB攻击、恶意文件攻击、远程控制、WEB后门访问等行为。 |
| 21 | 4、攻击工具检测：具备30种以上的深度检测模块，可支持shiro反序列化、蚁剑、哥斯拉、冰蝎3.0 、冰蝎4.0等检测能力，且能识别如shootback、TunnaProxy、dnscat2、reGeorg、reDuh、CobaltStrike等隧道通信工具。 |
| 22 | 5、安全风险检测：支持检测WEB攻击、远程控制、WEB后门访问、SMB远程溢出攻击、弱口令、拒绝服务攻击、暗链、隧道通信、扫描行为、暴力破解、挖矿、恶意工具利用、漏洞利用等风险。 |
| 23 | 6、文件检测：支持 HTTP 、FTP 、SMB、SMTP 、POP3、IMAP 、NFS、TFTP 、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输文件检测。 |
| 24 | 7、弱口令检测：支持对HTTP 、IMAP 、SMTP 、POP3、Telnet、FTP等协议的弱口令检测。 |
| 25 | 8、动态沙箱：支持多并发沙箱检测技术，集成主流的操作系统winXP 、win7、win10、linux等多种 检测环境。内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析，提供第三方专业证明文件。 |
| 26 | 9、 日志管理：具备数据外送至第三方平台的能力，支持以KAFKA 、FTP 、SYSLOG数据接口输出风险信息。 |
| 27 | 10、产品资质：须提供中国国家信息安全产品认证证书(安全审计产品-增强级)，为保障产品未知威胁检测能力，产品名称须体现“APT”字样。 |
| 28 | 堡垒机（ 一套）：1、★基础要求：软硬一体设备，使用国产化CPU及操作系统，运维审计资产数≥500，并发字符连接最大数≥200，并发图形连接最大数≥30；≥16G内存， ≥4T硬盘，冗余电源，管理口≥2\*千兆电，业务口≥4\*千兆电+4\*千兆光（含2个千兆光模块）；提供3年软硬件维保及特征库升级服务。 |
| 29 | 2、单点登录认证：支持标准化对接CAS、JWT、SAML2、OAuth2单点登录认证，且支持配置是否自动创建堡垒机中不存在用户。 |
| 30 | 3、双因子认证：支持域认证与双因子认证结合使用，如同时使用AD/LDAP用户名+AD/LDAP密码+手机APP动态口令登录堡垒机、同时使用AD/LDAP用户名+AD/LDAP密码+短信口令登录堡垒机。 |
| 31 | 4、支持的协议和应用：支持常用的运维协议：SSH、TELNET、RDP 、VNC、FTP 、SFTP 、rlogin 、X11；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL 、MySQL 、VMware vSphere Client、浏览器等客户端工具。 |

|  |  |
| --- | --- |
| 32 | 5 、数据库兼容性：支持DB2 、Oracle、MySql、SQL Server 、PostgreSQL 、KingbaseES 、DM、 GBase8a、GBASE8s的协议运维代理，可实现自动登录， 自动登录可直接调用本地windows系统的 数据库客户端工具（包括ssms 、sqlwb 、DBeaver 、mysqlcli、MySQLWorkbench 、MySQLFron t、DbVisualizer 、PLSQL 、SQLPlus 、Toad 、ToadforDB2 、db2cmd 、QuestCentral、pgAdmi n3 、psql、Ksql、Isql、DIsql、DMmanger 、GBaseDateStudio 、navicat系列等），无需应用发布前置机。 |
| 33 | 6 、数据库自动改密：支持对Web应用的自动改密功能，并且支持随堡垒机提供的改密插件录制向导, 通过改密插件自动生成web应用的改密脚本。 |
| 34 | 7 、专用客户端运维：支持Windows/macOS操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。 |
| 35 | 8 、 H5运维：支持ssh 、telnet、rlogin 、rdp 、vnc 、ftp 、sftp 、x11协议的H5运维，无需本地运维客户端工具。 |
| 36 | 9 、运维审计日志：支持对运维操作会话的在线监控、实时阻断；支持录像慢速/快速回放、支持记录 起止时间、来源用户、来源IP 、 目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。 |
| 37 | 10 、用户角色：支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理；支持自定义用户权限。 |
| 38 | 技术服务：★1 、安全威胁分析研判服务：由经验丰富的专业网络安全服务人员，通过登录评估大数据智能安全平台、APT流量探针设备，提取 日志、流量等数据进行人工安全分析，可以对考试院系统遭受到的攻击方式、频率、防御有效性等方面进行分析研判。针对网络攻击告警事件进行深入分析，研判攻击造成危害和影响；针对异常网络访问行为进行深入分析，研判攻击造成危害和影响；基于ATT&CK框架，针对海量日志进行人工检索、多维度关联分析。 |
| 39 | ★2 、应急响应处置服务：当遇到突发的网络安全问题如：发生网络恶意入侵事件、病毒木马感染、遭受DDos拒绝服务攻击或 因上级通报安全事件等，开展应急处置措施，包括事件响应、事件分析、安全灾难恢复、安全事件入侵追踪和取证。1）针对入侵成功的行为采取应急处置措施，包括阻断攻击源、阻断远控服务器、隔离下线受害主机等；2）针对入侵成功行为进行全面回溯分析，查找攻击路径、漏洞利用，并进行业务系统恢复操作；3）详细记录安全事件处置全过程，记录内容至少应包括：安全事件详细信息、应急处置全流程信息。 |