**威胁情报检测与阻断系统技术参数**

|  |  |
| --- | --- |
| 指标项 | 参数要求 |
| 硬件要求 | 标准1U或2U机架式设备，内存≥32G；硬盘≥1T；配置4个千兆电口、4个万兆光口；配置bypass功能；配置冗余电源；  服务期内包含硬件免费维保、换新服务；  可单机实现全部功能，无需其他设备配合 |
| 性能要求 | 设备吞吐量≥4Gbps，支持带宽≥2Gbps，网络并发连接数≥500W，网络新建连接数≥50000； |
| 软件服务 | 主要情报库至少每日更新一次，服务期五年;  具有与设备情报相匹配的情报社区，可供用户查询威胁详情;  包含设备全部授权及功能，设备中不存在其他需额外购买授权;  支持系统软件更新 |
| 功能要求 | 具备高级威胁攻击检测、零日漏洞攻击防护、扫描防护、勒索、钓鱼、威胁情报检测能力，实现威胁情报检测与阻断通报治理能力。 |
| 具备灵活的部署模式，支持旁路部署、串接部署、虚拟线部署。支持部署引导，用户可直接根据引导进行配置，快速完成部署。 |
| 支持对多种类型的网络入侵行为进行防护，包括侦查、漏洞攻击、病毒攻击、建立通信隧道、网站后门&shell、连接远控地址、木马远控、远控流量工具、挖矿、僵尸网络行为、蠕虫攻击、勒索、数据窃取、尝试下载恶意文件、钓鱼、对外攻击、攻击持久化操作。 |
| 支持应对外部攻击IP高频扫描的扫描防护功能，可自定义设置IP在特定时间内扫描次数超过某个阈值后判定为扫描IP，自动支持IP封禁动作，并支持自定义封禁时间。 |
| 支持高危零日漏洞攻击的检测和防护能力，支持零日漏洞防护数量不少于200个，具备零日漏洞防护专项，单独展示检测和防御效果。 |
| 支持针对勒索攻击的网络威胁进行专项防护，对勒索病毒挂马的各类主机反连行为进行实时检测和自动化防护，具备勒索攻击防护场景下的安全策略设置、检测防护效果专项页面。 |
| 支持针对钓鱼攻击的网络威胁进行专项防护，对通过各类钓鱼链接发起的主机反连行为进行实时检测和自动化防护，具备钓鱼攻击防护场景下的安全策略设置、检测防护效果专项页面。 |
| 支持针对APT攻击的网络威胁进行专项防护，支持对APT组织攻击行为的检测和拦截，具备APT攻击防护场景的安全策略设置、检测防护效果专项页面。 |
| 失陷类威胁情报数量不低于200W，且能够保持分钟级频率更新。 |
| 支持通过Syslog日志对接的方式联动三方设备，设备能够接收三方设备提供的Syslog日志并进行自动解析，从而进行设备黑名单封禁操作，实现威胁自动化联动封禁。 |
| 支持灵活黑名单配置。支持通过Http Header字段中URL、Referer、User-Agent、Cookie、Http请求方法等字段或自定义Http Header字段进行出入站黑名单配置，支持IPV6黑名单封禁。 |
| 支持在国家级攻防演练场景下，自动获取重保攻击情报更新，检测且主动拦截攻击行为。 |
| 提供资产管理能力，支持对资产分组进行管理，支持自定义资产类型，支持手动录入资产或文件批量录入资产，支持资产信息一键导出功能。 |
| 支持通过API接口调用的方式进行防护策略配置，支持通过API接口实现黑白名单的增、删、改、查功能，支持通过API接口进行资产及资产组的增加、删除、查询功能，支持通过API接口进行设备运行状态查询。 |
| 支持通过DNS日志转发工具实现和DNS日志的对接，支持设备告警屏蔽关联DNS服务器的告警并展示真实的失陷主机告警。 |
| 支持外部攻击事件聚合展示，可实时查看外部攻击检测及拦截/放行情况，支持通过攻击IP、威胁事件、受害主机进行攻击事件模糊搜索，支持通过受害资产、威胁类型、检出和拦截次数进行攻击事件精确搜索。 |
| 支持恶意外联事件聚合展示，可实时查看恶意外联检测及拦截/放行情况，支持失陷主机、威胁事件、外联目的地址进行攻击事件模糊搜索，支持通过资产组、威胁类型、检出和拦截次数进行恶意外联事件的精确搜索。 |
| 支持绑定资产组进行威胁防护策略配置，支持按照流量方向、威胁严重级别、威胁类型等维度进行自定义开启或关闭拦截策略。 |