国家癌症中心

态势感知平台技术需求

## 1.采购产品一览表

态势感知平台1套，含1个流量传感器和一个威胁检测与分析系统。

## 2.采购需求

### 2.1 流量传感器要求

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标项要求** |
|  | 硬件配置 | 2U标准上架设备。≥6\*GE电口，≥4\*10GE光口（含光模块），≥4TB SATA 企业级硬盘，冗余电源。。 |
|  | 性能要求 | 应用层吞吐≥2G |
|  | 部署方式 | 支持通过流量镜像的方式旁路部署在网络中，可同时接入多个镜像口，每个镜像口相互独立，不影响原有网络架构和处理性能。 |
|  | IPV4/IPV6双协议栈 | 支持IPv4和IPv6网络环境下的部署，接口支持IPv4、IPv6配置，支持对IPv4路由监控和对IPv6路由监控，可同时对IPv4和IPv6网络流量分析检测。 |
|  | 离线流量采集 | 支持手动批量导入PCAP包对离线流量采集，单次总大小支持1个G；支持通过配置FTP方式批量导入PCAP包对离线流量采集；记录PCAP包导入记录及检测状态。 |
|  | 流量过滤 | 支持流量过滤策略，通过ip、ip段、端口、协议等进行流量过滤，过滤语法支持and、or、not等多条件过滤语句。支持通过配置BPF语法条件进行流量过滤。 |
|  | 网络协议 | 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、dhcp、smtp、pop3、imap、webmail、db2、oracle、mysql、mssql-db、sybase、smb、ftp、snmp、telnet、nfs、icmp、ssl、ssh、redis、ldap、radius、kerberos、netbios、modbus、ntp、ipv6等。 |
|  | 文件协议 | 支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk、bin等）、压缩格式文件（RAR、ZIP、GZ、7Z、tar等）、文档类型文件（word、excel、pdf、rtf、ppt、txt等）、多媒体文件（flash、jpg、jpeg、png、flv、swf等）、脚本文件（html、htm、java、mhtml、mht等）等类型。 |
|  | 数据库操作 | 支持常见数据库协议的识别还原，数据库行为的解析，生成流量日志：DB2、Oracle、SQL Server、MySQL、MSSQL 、PostgreSQL、Mongo DB等协议。 |
|  | 认证协议 | 支持LDAP、Radius、Kerberos等认证协议的解析，生成流量日志。 |
|  | 邮件行为 | 支持WebMail、SMTP、POP3、IMAP邮件行为解析，生成流量日志。 |
|  | 登录动作 | 支持识别FTP、SMB、Oracle、MySQL、MSSQL 、PostgreSQL、SSH、POP3、IMAP、SMTP、redis、 CouchDB、Membase、Mongo DB等登录行为。 |
|  | 隧道封装识别 | 支持VLAN 、VXLAN的网络流量的解析检测。云场景下，支持GENEVE协议双层隧道封装流量的解析检测。 |
|  | 威胁情报检测 | 支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒、其他恶意软件。支持基于流量实时IOC匹配功能，设备具备主流的IOC，情报总量500+万条。 |
|  | 规则检测 |  系统默认内置13000+条检测规则，支持检测WEB攻击、Webshell攻击、网络攻击、后门程序、僵木蠕检测、C2外连、恶意通信、SMB远程溢出攻击、文件上传、弱口令、暴力猜解、挖矿、黑客工具、明文密码传输、漏洞利用、ARP欺骗、恶意扫描等风险。 |
|  | 检测模式 | 支持检测模式的标准模式、精简模式、自定义模式的切换，支持自定义检测深度，支持DNS隧道检测、CS流量检测、MSF检测、暗网流量检测等十几种机器学习模型的自定义配置。 |
|  | Web攻击检测 | 支持检测针对WEB应用的攻击，如SQL注入、XSS、代码执行、系统配置等注入型攻击。 |
|  | 支持跨站请求伪造CSRF攻击检测。 |
|  | 支持其他类型的WEB攻击，如目录遍历、弱口令、权限绕过、命令执行、文件读写、信息泄漏、文件包含、文件写入攻击、挖矿等检测。 |
|  | Webshell攻击检测 | 支持基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等。支持基于 webshell 函数的攻击检测，如任意文件上传、任意函数执行后门、任意文件写入、任意文件包含、任意目录读取、命令执行后门、preg\_replace 代码执行等。 |
|  | 网络攻击检测 | 支持多种攻击检测，能更全面的从流量中发现威胁，如：SQL注入、XSS、信息泄露、间谍软件、协议异常、网络欺骗、黑市工具、代码执行、挖矿等。 |
|  | 异常流量检测 | 支持非TCP完整流、畸形包检测、数据包完整性检测、IP碎片攻击检测、编码绕过检测、高级逃逸 AET 检测等防逃逸检测能力。 |
|  | 暴力猜解检测 | 支持HTTP、SMB、FTP、IMAP、POP3、SMTP、MSSql、Mysql、Oracle、Sip 、Redis 、Ldap 、Nntp 、SSH、Telnet、Sybase 、VNC、RADMIN、RDP等协议暴力破解检测，能识别出尝试登录次数、账户信息、爆破成功与否的攻击状态。 |
|  | XFF提取规则配置 | 支持自定义NAT转换前的IP字段名和字段位置，支持对IP字段名进行优先级排序。支持配置代理白名单。 |
|  | 高级威胁旁路阻断 | 基于专用的高级旁阻阻断规则实现攻击行为事中实时阻断。支持观察模式，仅记录行为，不进行阻断，同时提供阻断行为分析，协助判断旁阻上线后的效果及对业务可持续性的影响。 |

### 2.2威胁监测与分析系统

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标项要求** |
|  | 硬件配置 | 2U标准上架设备。≥4\*GE管理电口；≥960G SSD+32TB SATA 存储硬盘；冗余电源。 |
|  | 性能要求 | 处理能力≥12000eps |
|  | 系统运行监控 | 支持以分析平台为中心，可视化呈现天眼安全设备的部署情况、运行情况、数据情况、联动情况 |
|  | 监测工作台 | 支持根据用户业务需要进行个性化监测工作台自定义，支持重点监测内容集中添加或单个页面随意添加，个人监测工作台模板导入导出等功能； |
|  | 告警列表 | 支持对全部数据来源的分享展示与汇总展示，支持告警页面自动刷新时间自定义配置；支持自定义告警高级检索场景；普通检索模式支持自动置顶参与检索的条件；高级检索支持AND和OR组合查询，高级检索 suggest 功能支持中文拼音识别；告警列表可以进行包括基本信息、规则信息、原始告警、攻击行为、资产详情、取证分析、ATT&CK分析、攻击带外分析等内容的详情查看，以及基于告警列表可以对告警进行联动处置和添加白名单操作； |
|  | 告警分析 | 支持告警的深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为 |
|  | 受害资产分析 | 支持以受害资产维度进行分析，分析内容包括失陷状态、受到的攻击类型、威胁级别、处于的攻击阶段、所属的资产分组 |
|  | 攻击者分析 | 以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产支持自定义过滤内网IP，以便高效定位外网攻击者 |
|  | 威胁分析 | 支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击带外分析。 |
|  | 支持挖矿行为的分析，分析内容包括挖矿阶段、币种分布、挖矿告警趋势以及挖矿告警信息 |
|  | 威胁情报维度分析包括：情报详情、影响资产列表、资产的行为（行为包含：DNS解析、TCP流量、UDP流量、WEB访问、文件传输） |
|  | 应用安全的细分维度包括：WEB安全、数据库安全、中间件安全、邮件安全 |
|  | 系统安全的细分维度包括：暴力破解、弱口令、未授权访问设备安全 |
|  | 支持根据不同类型设备进行筛选告警信息，并对筛选以图形与列表相结合的形式进行综合展示 |
|  | 云端联动 | 支持与云端威胁情报中心联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等 |
|  | 威胁情报 | 支持基于威胁情报的威胁检测，检测类型包括：APT事件、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒等。支持自定义威胁情报，自定义类型包括：IP 地址、域名、MD5、URL 等。 |
|  | 情报管理 | 支持汇总统计、查询、展示情报数据，包括内生情报、云端情报、自定义情报、情报白名单。内生情报：支持编辑、删除（批量）、停用启用（批量）、批量导出的管理功能；云端情报：支持云端情报的多条件查询功能自定义情报：支持新增、编辑、删除、批量停用启用、批量导入导出，支持自动同步自定义情报至采集设备（流量传感器、文件威胁鉴定器），支持批量更新自定义情报并保存情报的更新记录情报白名单：支持新增、编辑、批量删除、批量导入导出的管理功能 |
|  | 情报研判 | 支持情报内生，通过研判确认文件威胁鉴定器分析产生的内生情报从而达到情报内生的目标支持跳转文件威胁鉴定器查看内生情报来源详情 |
|  | 登录行为分析 | 支持暴力破解行为检测，检测内容包含：源ip、目的ip、使用协议、爆破次数、爆破成功与否等 |
|  | 支持异常登录行为检测，检测内容包括：源ip、账号、登录资产IP、使用协议、登录结果等信息，且能进行异常时间配置 |
|  | WEB服务器行为分析 | 支持非常用请求方法分析，展示源ip、目的ip、域名、访问链接、请求方法、状态码、最近访问时间等信息 |
|  | 支持可疑爬虫或扫描分析，能自定义web访问频率，且能设置源IP白名单。 |
|  | 数据库行为分析 | 支持对mysql、mssql、oracle、sybase等常见数据库高危操作行为分析，其能自定义规则 |
|  | 访问行为分析 | 支持外部访问分析，能展示源ip、资产ip、端口、协议、时间等详细信息，且能自定义源ip白名单支持资产横向访问分析，能展示源资产ip、目的资产ip、端口、协议、banner、时间等详细信息，且能自定义源ip白名单 |
|  | 告警全包分析 | 可基于告警数据进行全包数据取证分析并兼容wireshark过滤语法对全包数据进行查询 |
|  | 可视化展示 | 支持大屏展示网络攻击态势，包括整体网络风险等级、告警总数、攻击源国家/地区TOP5、攻击态势，并支持自动旋转的攻击全景地图展示支持大屏展示整体威胁事件态势，包括威胁类型分布、威胁事件TOP5、威胁事件趋势、最新告警事件、威胁星云图、威胁IP网支持大屏展示整体资产风险态势，包含资产矩形树结构、资产分类、资产概况、开放服务统计、资产风险状态 |
|  | 与现有防火墙联动 | 支持与现有防火墙进行联动，发现威胁事件后支持对攻击IP、恶意域名和受害资产的流量进行阻断（将策略下发给防火墙，由防火墙执行阻断） |
|  | 与现有终端安全管理系统联动 | 支持与现有终端安全管理系统进行联动，发现威胁事件后支持与控制中心进行指令下发执行终端隔离和扫描操作 |

### 2.3服务要求

三年维保服务；三年威胁情报与检测引擎规则免费升级授权；三年5\*8小时线上技术支持；三年不定期线下技术支持。