KEMYOND

# KYSOC-5000

## 工控网络安全态势感知系统

### 特性及优势

•对收集数据汇总、分析、呈现，识别资产、告警、检测威胁

- 可识别协议多，支持 248 种协议解析
- 识别威胁类型多，支持 65 类威胁监视
- 长周期异常行为检测
- 海量原始流量的溯源和分析
- 采用闭环设计的安全事件的溯源和分析

## 介绍

按照“统一管控、分布采集”的原则，建设网络安全态势感知系统，将其作为网络安全中心。在中控室统一部署态势感知主站，在所有分区分别部署网络安全采集装置，采集装置对网络安全数据进行采集、分析处理，最后将采集的数据发送到主站，实现在主站的统一集中管控。实现工控网络安全实时监控，发现未知威胁、找出安全业务问题，实现事前预警、事中可知可控、事后可追溯的目的。

## 功能规格

| 功能模块 | | 功能详情 |
|---|---|---|
| 安全概况 | | 安全概览综合展示多个安全分区的流量和日志数据，仪表盘显示运行概览信息，包括采集装置资产统计、攻击地图、节点关系分析、威胁事件、安全事件、总流量趋势、文件还原数、应用层流量趋势、网络层流量趋势 |
| DashBoard | 总流量趋势 | 总体流量趋势反映采集装置采集的各区（办公网络、工控网络、管理信息大区）的入、出流量随时间变化的趋势 |
| | L2-L4 流量趋势 | L2-L4 流量趋势反映采集装置采集的各采集区的 L2-L4 流量随时间变化的趋势 |
| | 应用层流量趋势 | 应用层流量趋势反映采集装置采集的安全区域（办公网络、工控网络、管理信息大区）的应用层流量随时间变化的趋势 |
| | 用户流量趋势 | 用户流量趋势反映采集装置采集的安全区域（办公网络、工控网络、管理信息大区）的用户流量（具体 IP）随时间变化的趋势 |
| | 工控协议流量趋 | 工控协议流量趋势反映采集装置采集的工控网络区域的工控协议流量（具体 IP） |

| | | |
|---|---|---|
| | 势 | 随时间变化的趋势 |
| | 异常事件趋势 | 查询各分区异常事件类型统计比例图、敏感信息热力图、非法业务河流图、DDOS 攻击河流图 |
| | 关键业务 | 查询统计各分区 IM 业务、工控信息、视频信息、物联网协议、数据库业务、隧道业务信息。各类业务可按协议类型，并按小时/天/周/月统计流量和包数的 topN 的 ip。Top 值可通过系统参数进行设置 |
| **安全监视** | 流量监视 | 流量监视包括流量指标监控和通讯关系。流量指标监控按照不同安全区域显示网络流量指标数据；通讯关系按照不同安全区域显示区域内实时主机网络通讯关系。显示信息包含网络协议构成、对应协议每秒流量和总流量 |
| | 威胁监视 | 系统提供设备实时监视功能，实时展示所有威胁监视信息 |
| | 主机监视 | 主机监视展示主机登录情况，运行状态，端口使用状态等主机安全事件 |
| | 网络设备 | 网络设备展示网络设备如交换机、路由器等登录情况，运行状态，端口使用状态等设备安全事件 |
| | 安全设备 | 安全设备展示安全设备包括纵向加密设备、隔离设备、防火墙、采集设备的登录情况，运行状态，端口使用状态等设备安全事件 |
| | 组网结构图 | 显示厂级分析主站和采集装置的结构图，悬停每个采集装置图标可以显示其实时的状态（CPU、内存、磁盘、通信状态、关键进程状态），当通信状态为离线时，红色显示 |
| **安全审计** | 流量日志审计 | 提供网络流量日志的记录、查询等功能，包括网络统计日志、网络会话日志 |
| | 主机行为审计 | 提供主机登录操作信息的记录、查询等功能。包括主机登录系统用户名、登录时间、退出时间、操作命令、操作时间等信息，支持对相关操作行为关联审计及操作路径的回溯 |
| | 设备操作审计 | 提供对各类设备的操作行为的记录、查询等功能。包括网络设备和安全设备 |
| **溯源分析** | 应用访问 | 提供对业务会话、http、邮件、ftp、工业协议等各种应用访问的记录、查询功能 |
| | 记录取证 | 提供将网络流量生成 pcap 文件，并支持导出 pcap 文件的功能 |
| | 文件取证 | 提供将网络流量中的文件进行还原，并支持将还原文件下载到本地的功能 |
| **智能分析** | 图关系 | (1) 通过安全分区、IP 地址、开始/结束时间进行查询；<br>(2) 更换 IP 地址可查看指定 IP 的图关系；<br>(3) 点击节点，可对节点后的图打开和关闭；<br>(4) 图关系要展示的信息：上网网站、上网业务、节点关系通信关系对、设备操作行为、业务流量、异常告警信息。 |
| | 基线分析 | (1) 通过安全分区、IP 地址进行查询；<br>(2) 点击左上角的箭头按钮，选择不同的业务信息进行展示（上网网站个数、上网业务个数、通信关系个数、流量字节数个数）；<br>(3) 点击右上角的天、周、月分别查看往前推移（包含当天的）的 24 天、24 周、24 个月的数据（x 周表示时间、y 轴表示业务数据，默认横轴采样点数为 24，在系统参数中的基线参数表中可配置）；<br>(4) 当数据量大于或小于设定的基准线值（基线参数表中设置的值）时产生告警， |

| | | |
|---|---|---|
| | | 如图中红色线条为告警数据。 |
| | 工控报文分析 | (1) 波形图分析；<br>(2) 通信关系图分析； |
| | 节点关系分析 | (1) 根据所属分区、开始时间、结束时间、IP 地址查询；<br>(2) 分别点击左上角的局域网 IP、广播 IP、组播 IP、公网 IP 可单独查看节点图，也可以全部展示查看。 |
| | 关联分析 | (1) 通过所属分区、威胁分类、开始时间、结束时间、源 IP、目的 IP 查询数据；<br>(2) 点击右侧的告警信息科展示与告警相关的图数据关系；<br>(3) 当点击某一条告警信息时，可以查询对应的日志信息（安全事件），通过关联源 IP、目的 IP、时间（取告警事件时间前后推 24 小时）。<br>(4) 当点击某一条告警信息时，可以查询对应的流量信息（通信对数据以及具体的 DPI 信息），通过关联源 IP、目的 IP、时间（取告警事件时间前后推 24 小时）。 |
| **智能报表** | 威胁事件 | (1) 通过分区和时间查询；<br>(2) 选择“导出报表”将数据导出；<br>(3) 选择“显示饼图”查看饼图信息。 |
| | 流量指标统计 | (1) 通过分区和时间查询；<br>(2) 选择“导出报表”将数据导出；<br>(3) 选择“显示饼图”查看饼图信息。 |
| | 通信关系统计 | (1) 通过分区、源 ip、目的 ip、目的端口、协议、时间查询；<br>(2) 选择“导出报表”将数据导出；<br>(3) 选择“显示饼图”查看饼图信息。 |
| | 非法业务信息 | (1) 通过安全分区、时间、非法业务名称、源 IP、源端口、目的 IP、目的端口进行查询；<br>(2) 点击“导出表格”将数据导出；<br>(3) 点击右下角的上一页、下一页和任意数字，跳转至对应页面查看非法业务数据；<br>(4) 点击左下角“当前显示”的数字下拉框可设置页面显示的数据量。 |
| | 非法主机信息 | (1) 通过安全分区、时间、IP、MAC 进行查询；<br>(2) 点击“导出表格”进行数据的导出；<br>(3) 点击右下角的上一页、下一页和任意数字，跳转至对应页面查看非法主机数据；<br>(4) 点击左下角“当前显示”的数字下拉框可设置页面显示的数据量。 |
| **资产管理** | | 提供资产信息的增加，删除，查看，编辑和配置变更完成（修改数据后点击此按钮，将修改的数据同步给采集装置）功能 |
| **规则管理** | | 检测规则主要由主站平台下发，本系统目前提供检测方法的查询。检测规则包括：可疑 IP 规格、可疑域名规则、特征值规则和行为模型规则 |

| | | |
|---|---|---|
| 系统管理 | 采集装置管理 | 采集装置管理提供对采集装置进行增删查改 |
| | 上送服务端管理 | 上送服务端管理提供对厂站侧分析平台管理上送主站配置 |
| | 用户管理 | 用户管理包括对用户的增加，删除，查看和修改操作。用户信息包括用户名、用户类型、有效期，启用状态等信息 |
| | 角色管理 | 角色管理（使用“安全员”用户登录）用于对不同角色分配不同权限，用户配置角色后就赋予该角色定义的菜单权限 |
| | 系统日志 | 日志管理（使用“审计员”用户登录）提供对平台自身最近 6 个月操作记录的管理，包括记录，查询、导出 |
| | 系统参数 | 系统参数提供参数设置，包括电厂名称、平台名称、LOGO 是否加载、安全统计时长、Dashboard 中的 TOP 值、经纬坐标、应用协议、工业协议 |
| | 分区管理 | 对分区进行管理，实现自定义分区名称，且对分区进行增删改的操作 |
| | 基线参数表 | 新增基线参数值，并对其进行编辑、删除、计算、查询等功能 |

## 订购信息

| 名称 | 型号 | 软件版本 | EPS | PPS | 吞吐量 |
|---|---|---|---|---|---|
| 工控网络安全态势感知系统 | KYSOC-5000 | V3.0 | 100K | 100K | 10G |

**上海宽域工业网络设备有限公司**

上海市宝山区园丰路69号3幢5层

189-1779-7159 (技术支持)　021-56561181 (座机)

189-1819-0263 (销售咨询)　zhouaixia@kemyond.com (邮箱)

**成都研发中心**

成都市高新区天府大道北段1480号孵化园6号楼105号

028-86263902 (座机)

**官方网站**

www.kemyond.com

宽域公众号