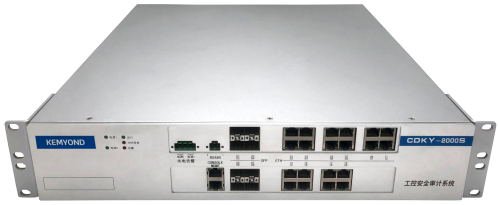
KEMYOND

CDKY-2000S

工控安全审计系统



特性及优势

- 对网络、系统的流量和日志数据进行监视和分析
- 识别已知的攻击活动并告警；
- 异常行为模式加以统计；
- 旁路形式，不影响原有的网络结构；
- 同时支持 4 路及以上镜像流量数据分析。
- 通过公安部安全与警用电子产品质量检测中心检测

介绍

利用 DPI、DFI 等技术对采集到的流量进行识别、解析和检测；通过对流量的威胁检测、溯源分析、流量还原、会话还原、文件还原帮助企业对安全事件进行快速溯源取证，分析结果支持上送到态势感知平台。该款产品可广泛应用于各种工业控制系统和工业设备，如 DCS、SCADA、PLC、RTU、继电保护等。

主要功能

功能项	参数详情
采集对象	支持对主机、网络设备、安全设备（包括工业防火墙、工业网闸、态势感知采集装置、入侵检测系统（IDS）、运维操作审计系统、防病毒系统等网络安全设备）等流量和日志数据进行数据采集
采集方式	支持主动采集方式，包括：SNMP、Agent、ICMP、SSH、网络主动扫描； 支持被动采集方式，包括：SNMP Trap、Syslog、流量嗅探。
审计数据采集	系统支持自定义采集策略，采集策略主要包括源目的 MAC 或源目的 IP、传输层协议、目的端口等。系统将根据采集策略及时生成审计数据，包括工控协议的审计数据。
审计数据还原	支持对 HTTP、SMTP、POP3、TELNET、FTP 等传统协议的审计。 支持对工控协议 modbus、mms 的识别和深度解析。
审计事件识别和分析	系统支持自定义白名单规则，支持基于 IP 或 MAC 定义网络通信白名单，以及基于功能码、寄存器地址等定义工业控制协议通信白名单。并基于白名单对审计事件进行识别，对网络中出现白名单以外的信息记录异常审计数据。
事件响应和报警	系统支持自定义报警策略，通过定义事件级别及告警方式，对产生的异常操作行为进行报警，通知管理员进行重点关注。

审计记录	生成的审计记录支持按事件主体、客体、时间、协议等字段进行筛选，通过筛选功能能够快速准确的获取到需要的信息，减少管理人员查询的工作量。 支持对审计记录进行数据汇总，并输出报表。根据统计报表能够直观的展现被审计工控网络数据的事件和级别的分布情况，了解工控网络数据当前的安全态势。

性能特性

性能参数	系统采集信息吞吐量不小于 1000 条/s； 支持监测对象数量不小于 1000 个； 整机最大吞吐率≥10Gbps，最大并发连接数≥100 万，每秒新建连接数≥10000； 最高支持千兆采集能力，且不丢包； 对于系统中的告警日志事件至少需要保存 180 天。

订购信息

名称	型号	CPU	内存	硬盘	网口	电源	机箱尺寸
工控安全审计	CDKY-2000S-A	4 核	16G	512G	8 千兆电口	双电源	1U
工控安全审计	CDKY-2000S	24 核	16G	1T+256G	20 千兆电口 +8 千兆光口	双电源	2U

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