- **统一安全管理平台 SOC6000-XE6M-D6202 产品简介**

统一安全管理平台随着信息安全的不断发展，信息系统多样化导致日志量巨大、日志格式多样、用户无法进行重点分析、难以挖掘各类日志之间的关联关系等问题，为解决此类问题东软结合在网络安全领域多年的理论和实践经验特推出面向政府、企业和各类组织的日志审计系统，东软统一安全管理平台(SOC-XE)支持多种日志采集方式、日志支持种类多、扩展灵活，可智能关联各类日志信息，能够为用户从纷繁复杂的日志中萃取出具有价值的分类；

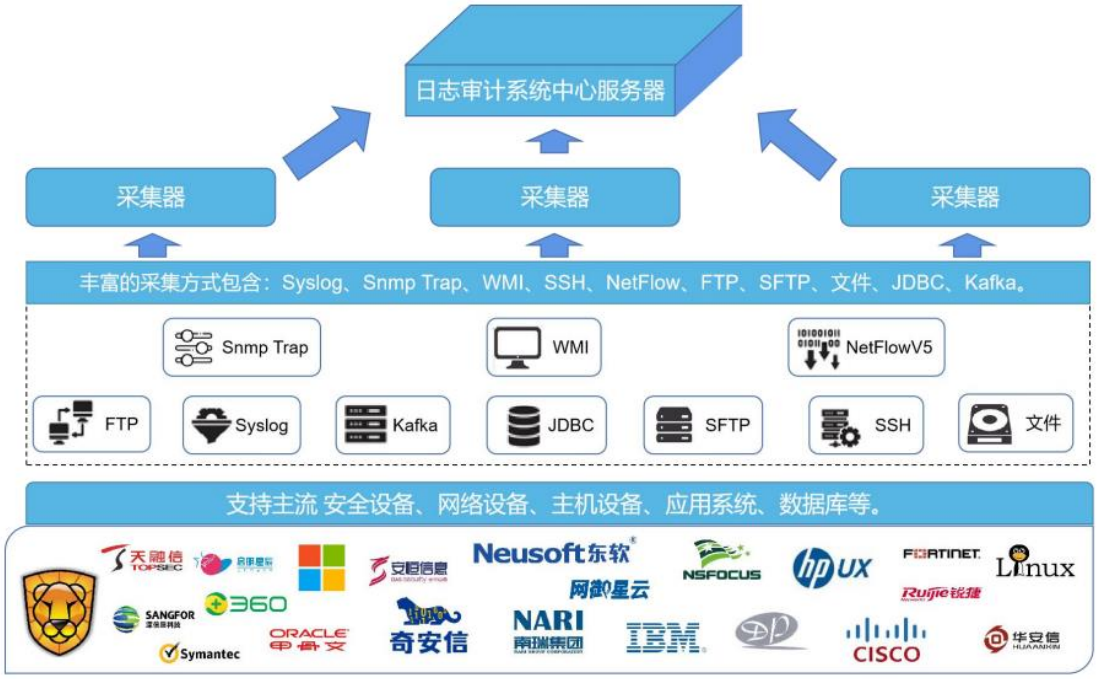
- **统一安全管理平台 SOC6000-XE6M-D6202 硬件配置**

采用标准 2U 机架式设备；交流冗余电源；具备 6 个千兆电口，6 个千兆光口，4 个万兆光口；设备具备液晶屏；

- **功能描述**

资产自动发现能力

东软统一安全管理平台具备完善的资产管理能，可通过资产自动发现能力，主动和被动收集采集网络中的资产信息，并可直接一键入库，方便大规模的资产录入。



可用性监控

- 网络链路、安全设备、网元设备监控

平台可以实时监控网络链路、安全设备、网络设备、集群、服务器等运行状态，进行历史状态数据统计分析。

- 日志收集、解析、存储、分析统计

平台支持多种方式采集设备日志，进行解析、汇总、存储、集中分析、统计，支持多种日志的可视化、自动化分析。

- 安全态势、安全事件

平台支持对安全事件、资产风险进行集中管控：包括病毒事件、恶意代码事件、威胁情报事件、异常行为事件、数据泄漏事件等。

工控协议检测

东软统一安全管理平台，支持主流工控安全协议检测（包括 Modbus、IEC）等；

部署能力

东软统一安全管理平台为了应对高并发，高吞吐场景，可支持单机或集群部署；

日志存储能力

东软统一安全管理平台针对网络安全法法律法规要求，可配置日志保存时间，

最低满足 6 个月的日志存储时间，存储空间不小于 2TB 硬盘；

知识库

知识库包括漏洞库等。漏洞库内置 CVE 漏洞库、CNVD 漏洞库、威胁情报库支持手动查询漏洞信息。

安全事件分析

本产品的核心价值之一，就是从来自单点安全设备的、海量的原始日志中，找出真正高风险的安全事件，减少用户处理误报的时间，使他们可以专注于其他保障业务系统稳定运行的工作。

本产品采用基于策略的分析模型，内置策略供用户选择，用户也可以自定义事件分析策略，对事件进行深入调查、取证和溯源。

日志采集

本产品支持从网络设备、安全设备、主机系统、数据库系统、中间件系统等 IT 基础设施采集日志，采用的协议和方式包括但不限于：Syslog、SNMP Trap、SSH、JDBC、FTP/SFTP、NetFlow、WMI、Kafka 文件导入等方式。