天融信工控日志收集与分析系统TopILA

www.topsec.com.cn

产品概述

天融信工控日志收集与分析系统是一款面向工业应用环境开发的日志审计类产品，系统采用主被动相结合的技术手段，通过Syslog、SNMP Trap、NetFlow、Telnet/SSH、WMI、FTP/SFTP/SCP、JDBC、文件等多种方式，对工业控制系统网络中不同厂家的安全设备、网络设备、工业主机、操作系统、上位组态软件、数据库系统等资产信息进行日志采集与分析，系统满足《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》与《工业控制系统信息安全防护指南》中对工业控制系统网络安全的对日志收集、存储、分析的要求，为工业企业安全生产提供数据支撑。产品广泛应用于能源、智能制造、钢铁、水利、轨道交通等行业。

产品特点

海量数据采集能力

系统支持至少26类350种安全设备、网络设备、服务器、工控应用系统日志等日志源进行采集，涵盖主流的安全厂商、工控厂商。采集具有多种方式，支持Syslog、Snmptrap、Netflow、WMI、FTP、SFTP、SCP、JDBC、文件等形式。通过日志进行采集、规范化管理、深度分析和可视化展示。

高效数据处理能力

系统采用大数据处理模式，对采集到的日志进行数据进行日志归一化处理、支持原始日志和归一化后的日志数据存储与查询，储存压缩比可达10:1，查询速度可达到百亿级日志查询秒级查询。直观展现安全事件的发生、访问源、危险等级以及影响范围的分别情况。

综合统计分析能力

系统支持管理员用不同角度对安全信息进行可视化分析，系统支持结果分析、日志挖掘、时间线、关系图、折线图、时序表、柱状图等形式，对流量分布情况、访问关系、端口访问关系、关联关系等进行分析，能够快速帮助客户发现安全事件源和目的，为事后溯源提供充足证据。

丰富可视呈现能力

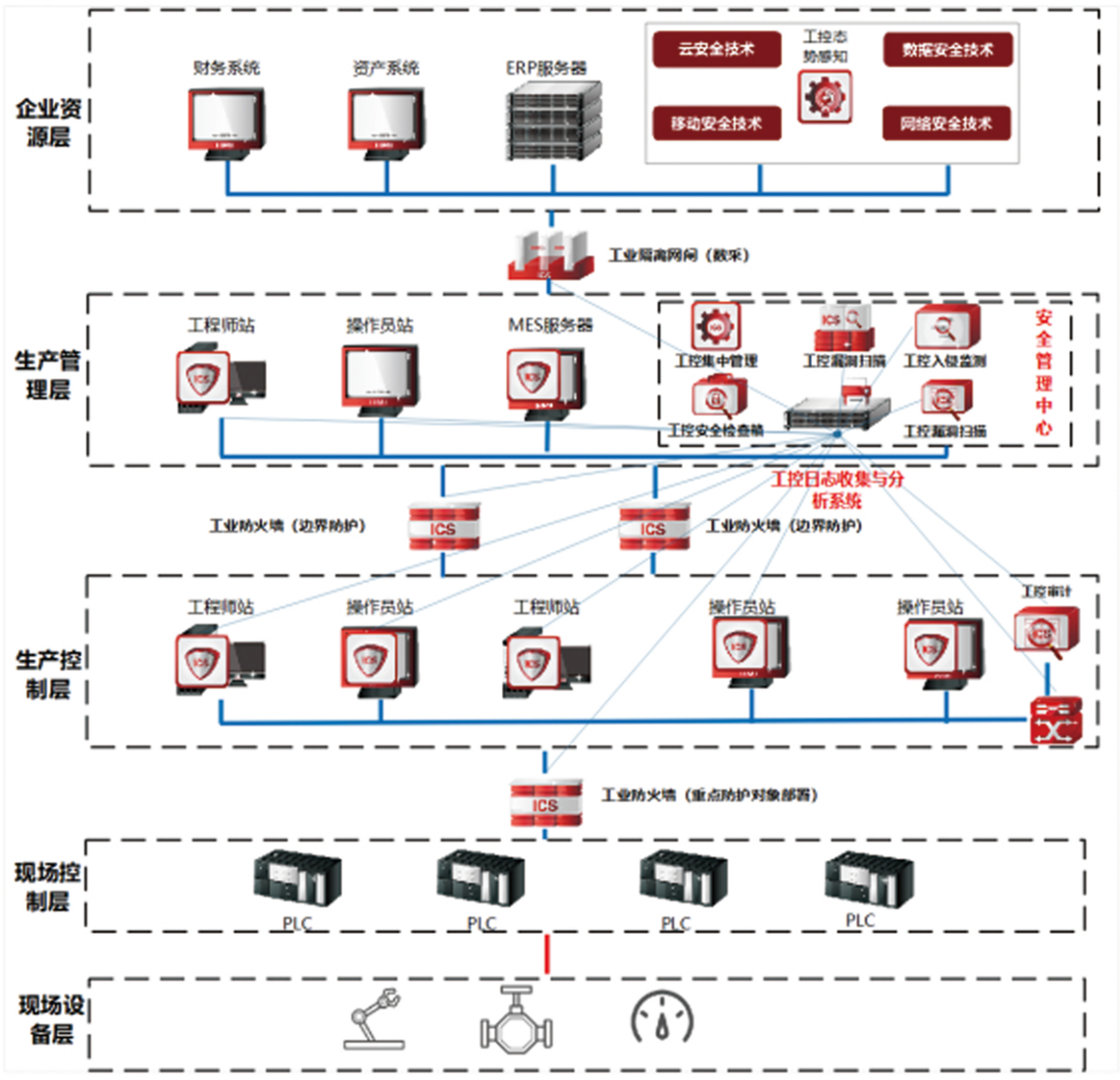
系统内置丰富数据展示模式，基于全球地图、全国地图、逻辑拓扑图、IP地址全球定位、饼状图、柱状图、曲线图、时间轴等，支持对日志查询结果快速自动分析，充分提升安全日志审计效率。同时支持将数据以PDF、WORD、EXCEL、HTML等方式不同格式进行导出。

合规检查必备利器

通过对全面日志的高速采集、异构格式归一化、以及高效压缩存储（6个月以上）、快速查询、综合分析、可视化等技术满足GB/T 22239-2019《信息安全技术信息系统安全等级保护基本要求》要求二级及以上系统需要进行“安全审计”的合规性需求。

典型应用

单级单机部署是最简洁的系统部署模式，也是最典型的部署模式，适用于大部分网络环境。在这个单机部署场景中，用户仅需在一台服务器上部署审计中心系统。此时，审计中心可以直接采集管理对象的日志信息。系统使用者通过浏览器登录审计中心的WEB站点，即可依照相关的权限进行各种管理操作。



客户价值

海量日志全生命周期管理

天融信工控日志收集与分析系统充分考虑了大数据量处理的应用，因此系统已经具备了对大数据量的采集、存储特征，并应用了多项专有技术确保了系统在大数据量采集与存储方面的优异性能，全面应对大数据时代海量日志数据带来的管理挑战。

此外，通过部署天融信工控日志收集与分析系统，可以从海量日志采集、海量数据处理、海量数据存储、统计分析再到数据的备份与恢复等涵盖海量日志数据的全生命周期的统一管理，帮助用户提高日志管理能力。

满足合规性要求

国家主管部门为了加强网络安全建设陆续出台了《中华人民共和国网络安全法》、等级保护、分级保护等法律法规。系统不仅能够保障存储网络日志6个月，还内置基于等保、分保等合规性要求的分析场景，为用户开展合规性建设工作提供技术支撑。用户可以通过丰富的合规分析策略对全网的安全事件进行全方位、多视角、细粒度的实时监测、查询、统计、分析，动态了解系统的合规情况。通过系统对海量日志的采集、存储、分析能力，完全满足合规性要求。

日常运维有力支撑

天融信工控日志收集与分析系统对海量数据的自动化采集、存储、分析、统计，可以及时发现IT系统中的安全事件，解决了人工效率低下以及面对海量数据人工无法进行管理的难题，是运维人员日常运维中不可或缺的技术支撑工具。