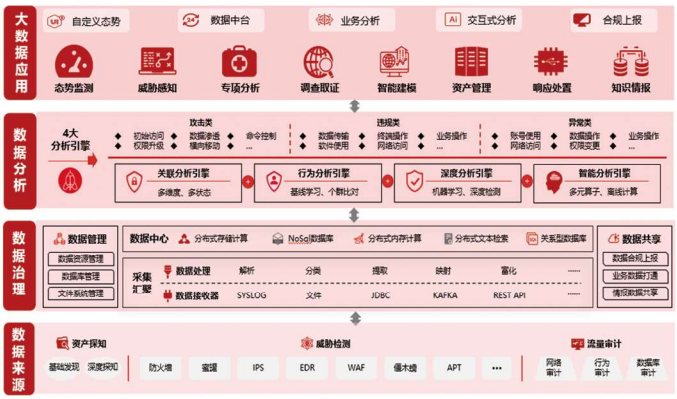
天融信大数据分析系统CISEE

www.topsec.com.cn

产品概述

天融信大数据分析系统（日志分析）v3（简称 CISEE）是一款面向海量安全数据的专业分析系统，提供数据治理、分析建模、数据可视化、人工智能分析等能力。系统基于大数据技术框架，对多源异构数据进行采集汇聚、清洗转换、信息富化，采用ETL机制进行信息抽取，建立多层次多主题数据仓库，通过丰富的分析算子库灵活组建数据分析模型，积累攻击行为分析识别的安全经验，提供丰富的数据展示图表组件，综合化展示数据分析结果，集成深度机器学习算法，增强数据分析智能性，能够从杂乱无章的安全数据中深入挖掘有价值的安全信息，提升安全运营效率。



产品特点

灵活的大数据框架

内置自研资源调度引擎，通过API、消息中间件代理等多种接口方式，灵活对接消息队列、分布式文件系统等开源存储计算框架以及腾讯、华为云等第三方存储计算框架；系统具备高达PB级数据存储能力，同时支持数亿条数据秒级检索响应。

纵深化的分析技术

关联分析通过数据之间的关联关系来发现威胁；行为分析从历史数据中学习或预测行为模式，进而发现当前数据的异常行为；深度分析则使用特定的AI算法来检测威胁。3种分析引擎形成纵深分析检测手段，内置多种分析模型，对网络安全威胁行为进行全面深入分析。

多元异构的数据接入

通过SYSLOG、文件、JDBC、KAFKA等主被动采集方式，实现多源异构的安全数据采集。支持天融信自有设备的对接以及非天融信厂家设备的灵活接入，接入设备类型包括但不限于抗DDOS、EDR、网络/数据库审计、防火墙、IDS、IPS、统一威胁管理、WAF等各类安全防护设备。

可自定义的分析展示

内置综合态势、资产态势、安全告警态势、网络攻击态势以及横向访问态势等多维度态势大屏，同时提供自定义大屏展示能力，内置多种类型图表，包括饼状图、关系图、散点图、折线图、树形图、雷达图等，利用拖拉拽的形式，支持自定义指标、图表、页面布局等元素。

典型应用

系统通常部署在客户单位运维管理区域的核心机房，需要与本区域及其它如办公终端、核心业务等区域的探针设备进行对接，支持从探针上获取系统所需的数据来源。常见的网络环境，如右图所示。

图中的管理平台默认带采集节点和分析节点功能，采集节点、分析节点支持集群部署、分布式部署以及横向扩展。