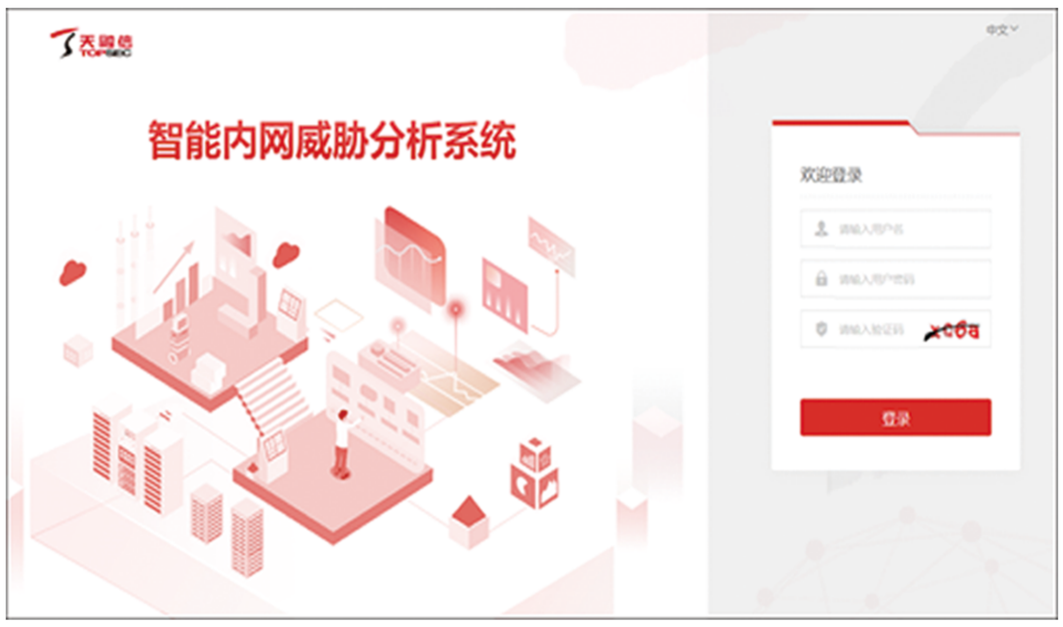
天融信智能内网威胁分析系统TopITA

www.topsec.com.cn

产品概述

天融信智能内网威胁分析系统（以下简称TopITA产品）基于大数据架构、采用AI智能设计理念，以发现内网失陷和内部违规为核心目标，全面收集终端、业务系统、网络流量三个方面的行为观测点的数据，融合关联分析、实体安全异常行为分析、AI分析形成纵深分析体系，辅予诱捕分析、流量分析、终端检测响应等技术支撑，通过构建行为模型和综合评分机制，捕捉政府、企业内网细微的行为异常变化，勾勒身份/资产行为轮廓，继而利用纵深分析对周期性行为进行判定，发现内网失陷和内部违规，最终挖出潜伏在内网高级威胁。



产品特点

全面的大数据机制

内置全面的大数据分析机制，采用分布式计算、分布式存储、数据仓库、分布式消息系统等组件，通过分布式消息系统和微秒级实时流分析引擎保证高性能的处理能力及强大的扩展能力，通过全文检索引擎保证大数据交互秒级响应能力，通过机器学习引擎提供智能分析能力。

纵深分析技术

产品搭载三种分析引擎：关联分析引擎基于多元组算子库进行自定义建模；行为分析可对海量数据进行深度学习，进行观察和统计；深度分析引擎对不符合简单逻辑关系规律的网络安全威胁行为进行深度挖掘分析，通过三种分析引擎，对网络安全威胁行为进行全面深入分析。

丰富的预置分析规则

预置300多种威胁分析规则，主要包括：攻击分析类、内网失陷类、数据泄露类、特权滥用类、业务异常类、异常访问类等，威胁分析规则构建应用了多种AI算法，如：时序分析、决策树回归、LSTM长短期记忆网络、K-means聚类、Ngram排名等。

可视化分析建模

提供可视化分析建模能力，通过行为索引建模技术完成行为仓库的构建，将分析能力场景化，通过可视、拖拽方式，将分析模块拼装成分析场景完成分析模型构建，可实现简单、灵活地自定义分析模型。

典型应用

整体部署方案包括四个部分：管理平台、分析节点、内网威胁探针、蜜罐探针。需要在核心交换域进行数据交换，采用旁路端口镜像的方式通过各探针实现实时的流量威胁检测，检测结果送至平台进行数据挖掘分析。常见的网络环境，如右图所示。

图中的管理平台默认带分析节点功能，分析节点、内网威胁探针、蜜罐探针支持横向扩展。