

天融信工业互联网态势分析与安全管理系统TopISA

产品概述

天融信工业互联网态势分析与安全管理系统（以下简称TopISA产品）是对工业互联网进行安全监控与态势分析的大数据安全产品。系统收集流量、日志、设备运行状态等安全数据，经过处理、存储、分析后形成安全态势及告警，辅助客户了解所管辖工业网络的安全态势，并对告警进行协同处置。系统可全面掌握网络安全态势，监测漏洞、病毒、网络攻击，识别安全事件，预警重大安全威胁，达到快速应急处置目的，提升企业风险应对能力。



产品特点

强大的数据处理能力

TopISA产品采用大数据分析引擎，利用分布式文件存储及检索技术，可支持高达PB级的数据存储及检索，支持十亿级别数据秒级检索响应，同时具有横向扩展特性，客户可以根据实际使用需求，动态的增加系统的存储与计算性能。

全面的安全分析技术

TopISA产品支持汇总各类安全数据，运用关联分析、用户画像、业务安全基线、模型分析、威胁情报等安全技术，有效发现各类安全事件与风险隐患，识别漏报与误报的行为，提升安全运维工作效率，形成安全联动、动态感知的整体安全分析能力。

灵活的部署安全探针

TopISA产品支持丰富的探针类型，包括工控漏扫、工控防火墙、工控网闸、工控入侵检测与审计、工控监测审计、工控主机卫士等，同时支持第三方设备数据接入，客户可根据实际网络、预算情况选择安全探针进行部署，灵活组合不同类型的探针。

智能的识别工业资产

通过工业资产指纹识别技术，全面发现工业互联网资产，从工业设备、主机、应用、业务等多个维度构建资产库，对网内资产进行实时安全监控，呈现网络的风险、脆弱性等安全信息，为客户提供强大的资产管理与安全监控手段。

完备的安全知识大脑

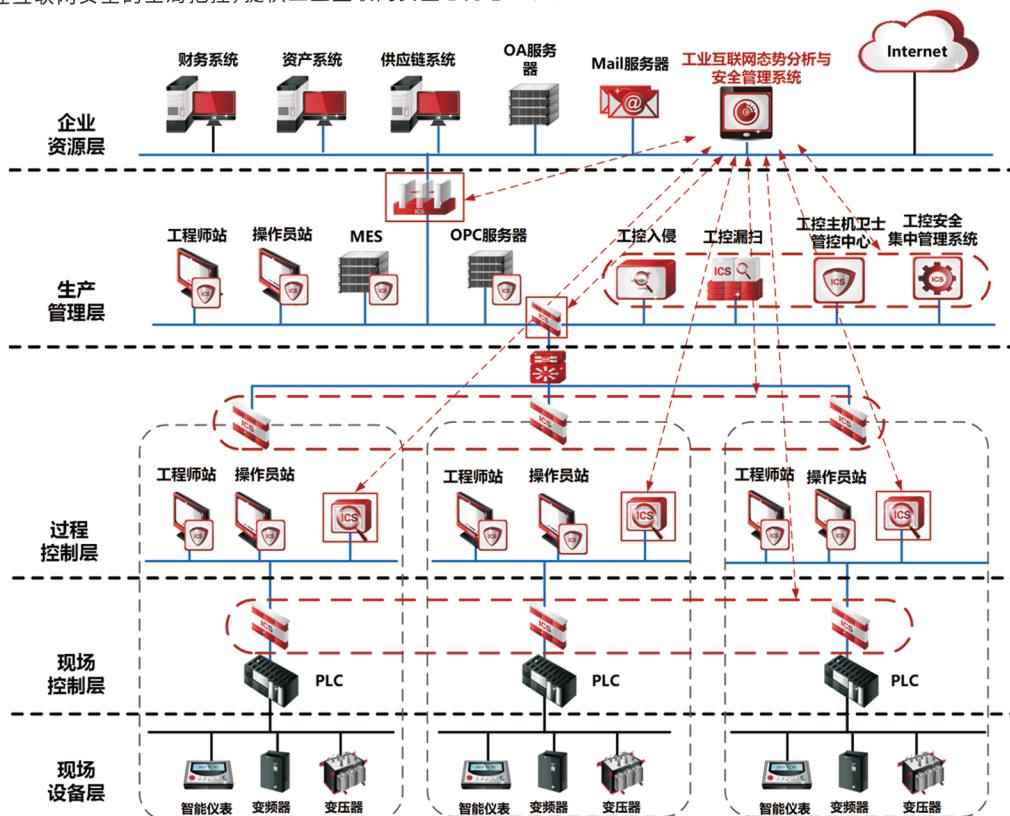
以工业互联网安全知识大脑为核心，包括工业资产指纹库、工业协议库、工业漏洞库、工业威胁特征库和工业设备库等，提供威胁情报、联动分析、合规分析、威胁追溯等安全分析服务，为客户持续输送安全能力。

全维度安全态势感知

从风险、攻击、资产等多个通用维度进行基本态势展示，从探针、追踪溯源等多个专项维度进行专项态势展示，并支持自定义态势展示。通过多种可视化态势感知技术，为客户提供友好易用的安全监控手段，进一步提升安全运维工作效率。

典型应用

TopISA产品部署于工业企业资源层,可全面收集网络设备、安全设备、主机设备等对象的安全数据,并进行关联分析,制定安全策略,联动网内各类安全设备,实现对工业互联网安全的全局把控,提供工业互联网安全态势感知和安全运营的全生命周期安全服务。



客户价值

安全探针统一管理

统一管理工业互联网中的安全探针,对网络中的流量全面分析,掌握IT和OT资产,形成资产画像、资产拓扑、策略基线、脆弱性分布等,帮忙企业以资产全局视角进行风险评估,满足业务需求,提升企业安全运营管理水平。

安全风险联动分析

通过关联内网各类工控安全数据及外部威胁情报,可以实现工控安全数据整合,消除信息孤岛,提升安全分析的准确性,降低误报漏报等情况,可以帮助客户识别和关注重点安全风险,形成动态安全策略,构建整体安全防御体系。

安全事件动态防御

联动网内各类安全设备,对发现的安全问题快速定位,并制定有效的安全防御手段,利用系统的安全策略集中管理能力,可以动态调整设备安全策略,快速封堵安全漏洞,及时处置安全事件,最大程度的降低事件影响范围。

安全态势可视化呈现

提供资产、告警、脆弱性、探针等多维度态势分析界面。通过可视化技术展示资产分类排行、资产漏洞排行、告警风险指数、攻击威胁排行、高危漏洞排行、告警事件类型分布等可视化模块,辅助客户完成安全决策,实现企业的安全态势感知可视化。