www.topsec.com.cn

天融信工控入侵检测与审计系统TopIDA

产品概述

天融信工控入侵检测与审计系统是一款专门针对工业互联网安全威胁的检测类安全设备。系统内置专业的工控入侵规则库，涵盖包括缓冲区溢出、扫描攻击、DoS/DDoS、SQL注入、蠕虫病毒、木马、间谍软件等多种类型的攻击特征；同时可根据业务功能需求制定白名单策略，采用攻击规则检测+业务白名单两种方式，对工业控制网络上捕获的数据包进行相应的行为匹配，及时发现来自生产网内外部攻击威胁，为客户提供直观、落地的安全防护建议，保障生产网络安全运行。

产品特点

多合一攻击威胁检测

系统集入侵检测、行为检测和数据库审计等多项安全检测技术于一身，依照特定的安全策略对工业控制系统运行状况进行实时检测，可有效发现基于网络或数据库层面的入侵攻击、异常流量、非法操作和SQL注入等安全威胁。

细粒度工业协议解析

系统内嵌协议深度解析引擎，针对工控协议数据包完整性、功能码、地址范围、值范围、变化趋势等多个层次深度分析，及时发现异常通讯行为。支持的工控协议包括Modbus、OPCDA、OPCUA、S7、Profinet、IEC104、DNP3、EIP、MMS等。

全方位业务行为审计

系统采用业务行为审计技术，对工业控制系统通讯内容的写操作、写频率、参数范围、变化量范围、变化率范围进行深度分析。解决了针对误操作、基于合法途径的非法操作、操控指令变更、PLC下装等破坏行为的精确识别。

全程数据库操作审计

系统采用数据库协议识别、特征检测和深度解析技术，针对登录用户、SQL语句、操作类型、操作对象等所有要素配置全方位的告警策略，记录针对数据库的所有操作行为，及时发现潜在威胁因素，快速精准定位安全事件。

多维度安全基线检测

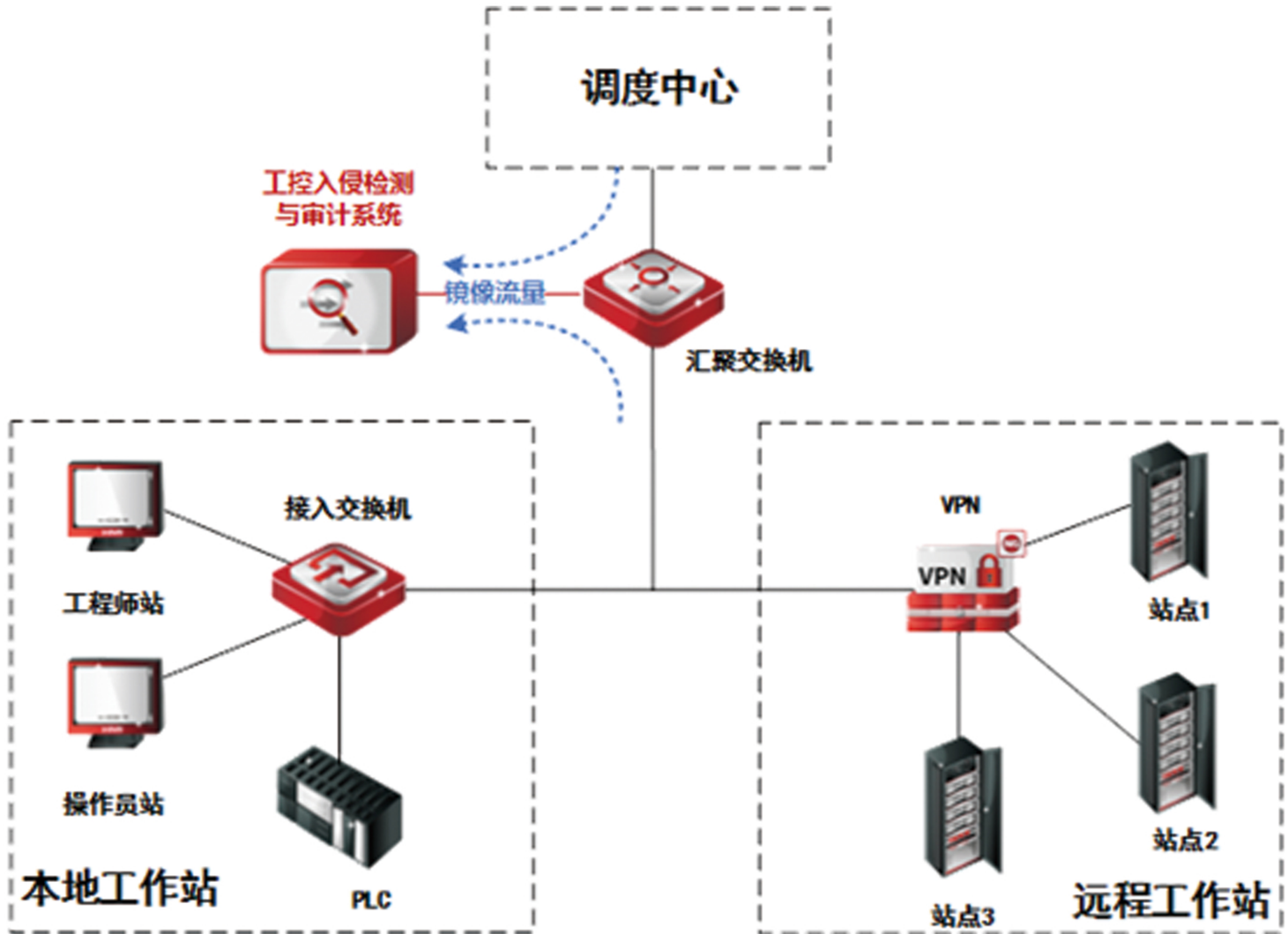
系统采用深度自学习技术，建立会话基线、流量基线和指令基线，并可根据工业控制系统业务需求进行自定义调优。有效检测非法外联、恶意程序和误操作等违规行为，帮助客户实时掌握网络中的运行状态，发现潜在安全威胁。

智能化工业资产识别

系统采用被动匹配技术，有效识别资产的IP地址、协议、端口、厂商信息、类型、型号、版本等信息，分析资产关系，自动生成资产拓扑，建立起完整的工业资产台账，帮助客户彻底摸清家底。

典型应用

天融信工控入侵检测与审计系统以旁路方式部署于控制网络区域边界，根据特有的工控入侵规则库及特定的安全策略，对工业控制系统的通讯内容进行行为匹配，可有效发现基于病毒、蠕虫、木马、DDoS、异常行为、异常流量、恶意程序等攻击威胁，进行实时告警，帮助工业企业客户及时发现安全威胁，保障生产网络安全运行。



客户价值

满足工业安全合规要求

可深入分析判断L2~L7层的网络入侵行为，精准发现网络中的攻击威胁，满足客户等级保护、分级保护以及相关行业政策的安全需求，提升工业控制系统安全防护能力。

预警工业入侵攻击事件

通过全面持续监测生产控制系统网络安全，建立起符合工业生产现场的安全检测规则，及时发现入侵攻击行为，并通知安全管理人员，降低安全事件造成的经济损失。

提升安全事故溯源能力

通过对网络攻击行为、违规操作行为等安全事件进行详细记录和报文留存，能够在发现问题时，方便用户对工业网络中发生安全事故的整个过程进

直观展示工业安全威胁

通过可视化展示技术，可以清晰、直观感知工业控制网络内部流量变化、通讯行为情况，帮助用户把控工业网络整体安全威胁。