睿航至臻
RUIHANG TECHNOLOGIES CO.,LTD.

睿航至臻产品手册

— 以智能安全为理念服务中国制造2025 —

目录

CONTENTS

PART
01

公司简介

公司简介

北京睿航至臻科技有限公司在工业互联网安全领域掌握多项前沿技术，拥有工业网络安全异常感知系统、工控日志审计系统、工业信息综合安全管理平台等覆盖工业互联网全生命周期的产品线，产品的应用覆盖了军工制造企业、电力核心系统等国家重要制造领域，正在研发推进的智慧城市建设项目，将公共基础设施的网络安全领域纳入了公司的核心产品应用范围。公司在杭州、嘉兴等地设有办事处，在长三角地区业务范围发展迅猛，逐步将公司品牌建设和市场开拓向全国方位推进。

防护

提前发现
消除隐患
消除不安全连接

控制

通过细分的访问权限策略来控制用户登录管理并进行分类记录

监控

连续监视、监测所有恶意攻击行为

响应

智能收集最新的态势感知情报实时进行排查

PART
03

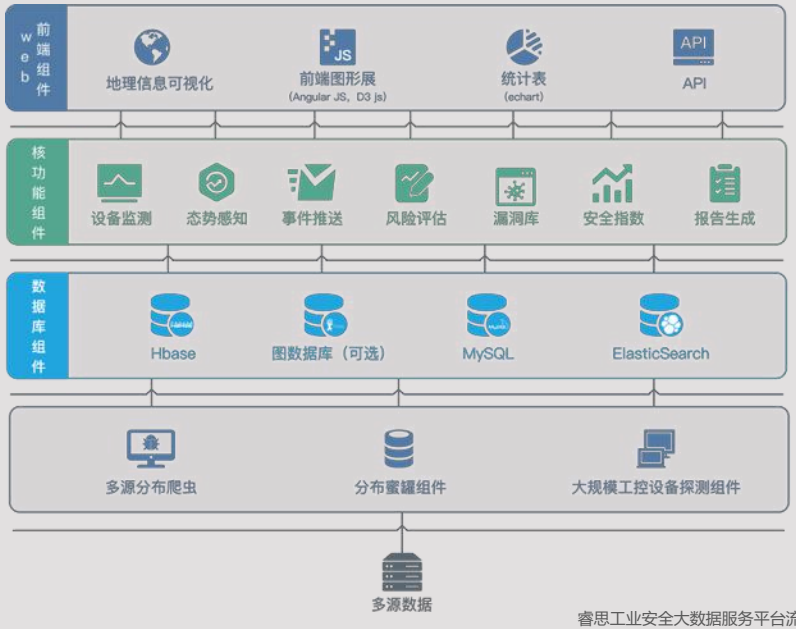
睿思工业安全大数据服务平台

睿思工业安全大数据服务平台

产品概述 | Product Overview

睿思工业安全大数据服务平台（Risdom） 是一个面向工业控制系统的安全监测与态势感知系统，其通过多种通道获取工控安全相关的各类数据，并基于此数据进行智能分析及可视化展示的综合系统。

Risdom提供了工控安全多源数据采集、工控设备扫描探测、基于工控蜜罐的态势感知、工控安全漏洞库以及工控安全指数等功能。本系统有助于政府部门、工业企业更好地掌握关于工控安全领域的安全风险情况、网络威胁信息、工控安全事件动态以及漏洞爆发情况等，有助于政府部门和工业企业从宏观上把握当前的工控安全态势，同时也支持对具体的工控安全事件和攻击活动进行微观分析。



睿思工业安全大数据服务平台流程图

睿思工业安全大数据服务平台

功能特点 | Features

工控安全多源数据采集

通过一个支持对多个数据源进行并发采集的分布式爬虫组件，对多种数据进行格式转换和结构化，从而建立了与工控安全主题高度相关的信息数据库。

工控安全指数

安全指数功能根据不断更新的工控安全事件数据、威胁数据、漏洞数据建立模型，计算安全指数，并建立一套学习训练模型，平衡历史数据波动，得到每日更新的工控安全态势指数，反映整体安全态势。

工控安全漏洞库

目前已建立了包含5000+个CVE/CNVD来源的工控安全漏洞库。从爬虫组件获取最新的漏洞信息，对漏洞库进行扩充和维护。

工控设备扫描探测

设计并实现了面向互联网的大规模工控设备扫描探测器，对于全网工控协议端口进行快速大规模无状态扫描，获得疑似工控设备及控制系统目标信息。

基于工控蜜罐的态势感知

工控高仿真蜜罐模块通过对工控设备进行模拟仿真伪装成真实的工控系统，获取和收集外界对工控系统的探测和攻击行为，并进行本地记录和存储，从收集到的数据和访问序列中挖掘有价值的信息，例如攻击者画像、常见攻击手段等，来监测针对工业控制系统的嗅探、攻击态势，并对当前的风险和威胁情况给出评估和态势分析。

报告生成

报告生成功能基于以上数据和功能生成态势感知和风险分析报告，并提供在线阅读和离线下载两种方式，供用户选择。

睿思工业安全大数据服务平台

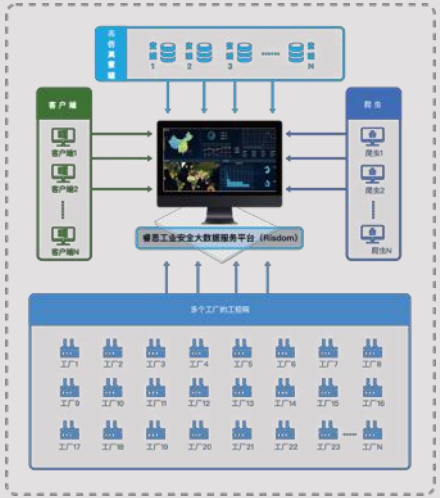
产品优势 | Product Advantages

工控设备快速探测和精准识别技术	采用TCP无状态扫描和零拷贝协议栈技术，大大提高了处理效率，并有效降低了带宽，与传统方式相比，效率提升达千倍以上。同时针对工控设备的精准识别问题，采用机器学习方法对工控相关的关键词不断进行重新的挖掘和筛选，并基于多模式匹配算法对关键词库进行更新。针对频繁更新引发的效率问题，提出了动态增量更新多模匹配自动机的算法，使得当关键词库发生变化后，无需再重新构建自动机，而是对原有自动机进行动态修改，大大提高了匹配系统在关键词频繁更新的情况下的反应敏捷性。
分布式高仿真蜜罐及恶意行为分析技术	针对当前高仿真蜜罐中缺乏工控相关属性的问题，在开源蜜罐系统上扩展并实现了多种工控协议，并进行高级别仿真，可有效躲避主流探测引擎的蜜罐识别功能。系统实现了完整且自动化的蜜罐信息收集、清洗、分析、展示工作流，覆盖了整个信息流的全生命周期。对蜜罐收集到的数据进行了深入分析和挖掘，针对蜜罐收集的网络行为日志，进行高效的数据清洗、降低了数据维度、合并了相似属性，接着对相似的访问序列进行聚类，得到有可能包含恶意序列的访问簇，进而分析出攻击行为组合。同时，系统还识别出了包含PLC拒绝服务、电表设备读写、加油站控制命令等多种攻击行为。

典型部署 | TypiCal Deployment

睿思工业安全大数据服务平台（Risdom）是一个面向工业控制系统的安全监测与态势感知系统，其通过多种通道获取工控安全相关的各类数据，并基于此数据进行智能分析及可视化展示的综合系统。

Risdom提供了工控安全多源数据采集、工控设备扫描探测、基于工控蜜罐的态势感知、工控安全漏洞库以及工控安全指数等功能。本系统有助于政府部门、工业企业更好地掌握关于工控安全领域的安全风险情况、网络威胁信息、工控安全事件动态以及漏洞爆发情况等，有助于政府部门和工业企业从宏观上把握当前的工控安全态势，同时也支持对具体的工控安全事件和攻击活动进行微观分析。



PART
04

睿知工业企业安全态势感知平台

睿知工业企业安全态势感知平台

产品概述 | Product Overview

睿知工业企业安全态势感知平台，可对工业企业工控资产、人员和和网络进行在线监测，并对工控系统内的行为和活动进行收集，提取安全要素并进行分析，同时结合威胁情报，开展多源数据融合和关联挖掘，构建态势感知模型，以给出企业工控系统的整体安全态势，并就潜在的安全风险进行分析并给出预警,同时对安全趋势给出预测。 此外，工控安全态势感知平台还可以与工控网络审计和检测系统进行交互，获取异常事件和审计数据，形成统计报告和安全态势，对攻击行为进行分类等，对攻击的溯源和预警起到有效地支撑，从而形成一个完整的安全生态闭环系统。

睿知工业企业安全态势感知平台

功能特点 | Features

资产发现

对工控设备进行全网探测，通过无痕扫描等方式得到各资产的系统详细信息、位置信息和安全隐患等内容，并给出可视化展示。

安全预警

在实时发现、态势预测和离线分析过程中，发现安全隐患后将进行安全预警，提前让工作人员对威胁做出及时处置。

威胁感知

基于资产内容进行深入分析，发现工控资产存在的威胁点，并对威胁信息进行进一步判断，得到如弱密码，绕权等威胁利用特征。

追踪溯源

对资产发现及扩展性导入的数据，以大数据技术和关联性分析技术进行威胁的溯源追踪，更进一步识别攻击的发起点，并还原攻击路径。

态势分析

基于资产和威胁的多维度数据进行大数据分析，通过不同维度的趋势统计，以达到未来某特征的数据预测和分析。

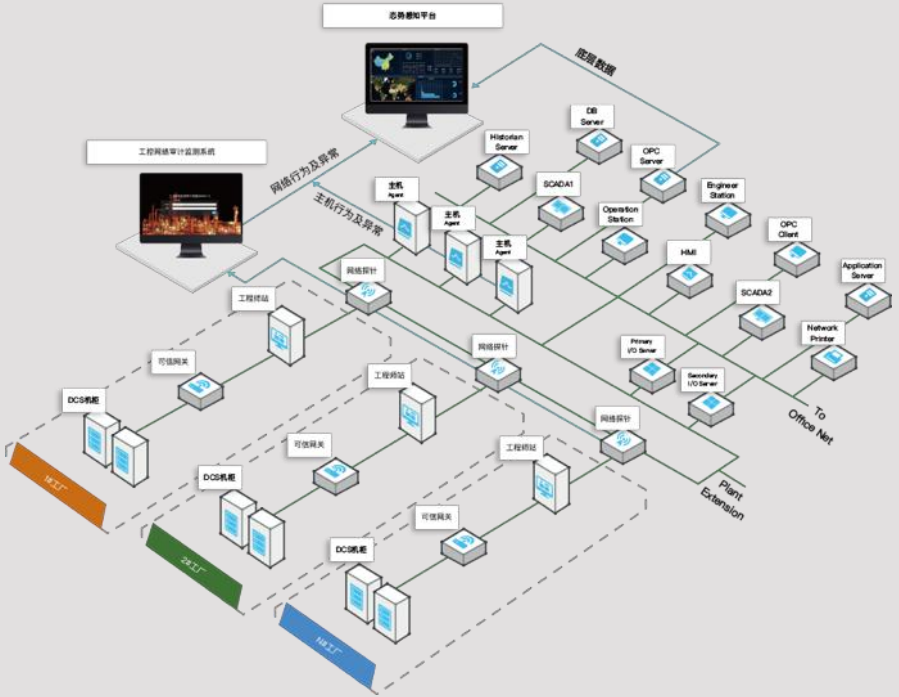
产品优势 | Product Advantages

多通道安全要素融合技术	汇聚多通道安全要素，依据要素间的内在逻辑关系对信息进行综合，为态势评估提供数据支撑。内在逻辑关系包括属性特征的相似性，预定义模型中的要素特征关联性，要素发生前提和后继条件之间的相关性等。
工控实体行为建模与风险评估	针对被监测实体（如操作员、主机、PLC等）等抽取实体属性，融合多元数据形成对象特征矩阵，基于对象模型分类器，识别存在风险对象，并给出当前的风险指数，并基于历史数据给出信誉值。
睿知工业企业系统安全态势感知	针对工控网络节点数量多、连接关系复杂等特点，根据网络节点、结构和安全事件间关联性建立统计学习模型，并给出相应的信息传播算法，以安全事件的发生为触发点，根据信息传播算法评估工控网络的安全风险及态势。

睿知工业企业安全态势感知平台

典型部署 | TypiCal Deployment

睿知工业企业安全态势感知平台采用B/S架构，客户端为浏览器，服务器端为Web服务器。其中，服务器端将汇聚来自工控网络审计系统（包含多个网络探针）、主机代理（Agent）和从OPC服务器采集的多类型数据，并进行数据融合和筛选，从中提取出网络安全要素（包含资产、人员和网络行为等多个维度），并基于安全要素对工控系统的安全态势进行刻画和评估，同时结合威胁情报信息对安全趋势进行预测。该平台将帮助安全负责人和管理人员对工控系统当前的安全态势进行评估，并对可能的威胁进行预警，同时有助于对工控系统安全态势进行持续、准确、实时的表征和预测。



PART
05

睿视工业网络异常监测审计系统

睿视工业网络异常监测审计系统

产品概述 | Product Overview

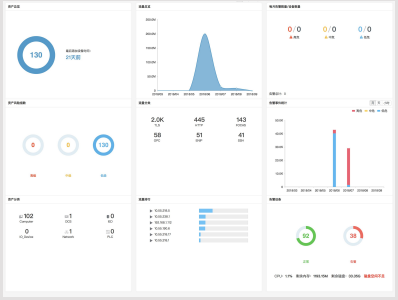
睿视工业网络异常监测审计系统（Rision），是专门针对工业控制网络的信息安全监控与入侵检测系统。它采用创新性的多级智能检测引擎，可有效发现网络异常和未知攻击，大大降低检测误报率和漏报率；实现了主动和被动相结合的设备精准识别和拓扑自动发现；支持面向网络拓扑和工业过程监控的双视图监控展示；支持面向工控协议的行为深度分析，可解析Modbus TCP、 西门子S7、DNP3、IEC 60870-5-104等工控协议，从中还原业务过程和指令操作行为；采用旁路部署，对工业生产过程“零干扰”，能够实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意攻击并给出实时报警，同时详实、准确记录工业控制网络中发生的各种行为和操作，包括设备间的网络通信和用户的网络行为操作，为事后分析、问题查找和事故追责等提供记录和依据。

睿视工业网络异常监测审计系统

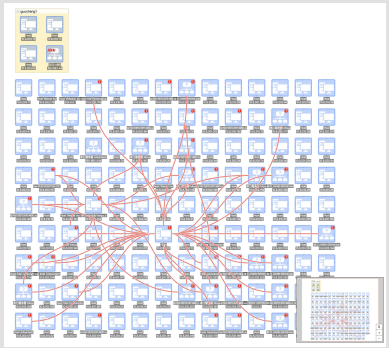
功能特点 | Features

可视化面板

从工控资产、审计活动和告警事件三个维度，对工控网络安全进行全面监控、展现和异常感知。



双视图监控



多级别智能检测引擎

网络行为审计和回溯

工控网络审计检测系统，支持对工控网络通信记录进行回溯，根据时间、IP地址、端口号、功能码等条件查询通信记录，为工业控制系统的安全事故调查提供详实的依据。

事件告警与分析

支持事件，分级告警。多个检测引擎产生报警，提供告警报文查看，对触发告警的报文，记录PCAP文件，方便查询原始报文。

关键事件检测

对工程师站组态变更、操控指令变更、PLC下装、负载变更等关键事件进行实时监控，下发的指令出现异常则告警等。

睿视工业网络异常监测审计系统

产品优势 | Product Advantages

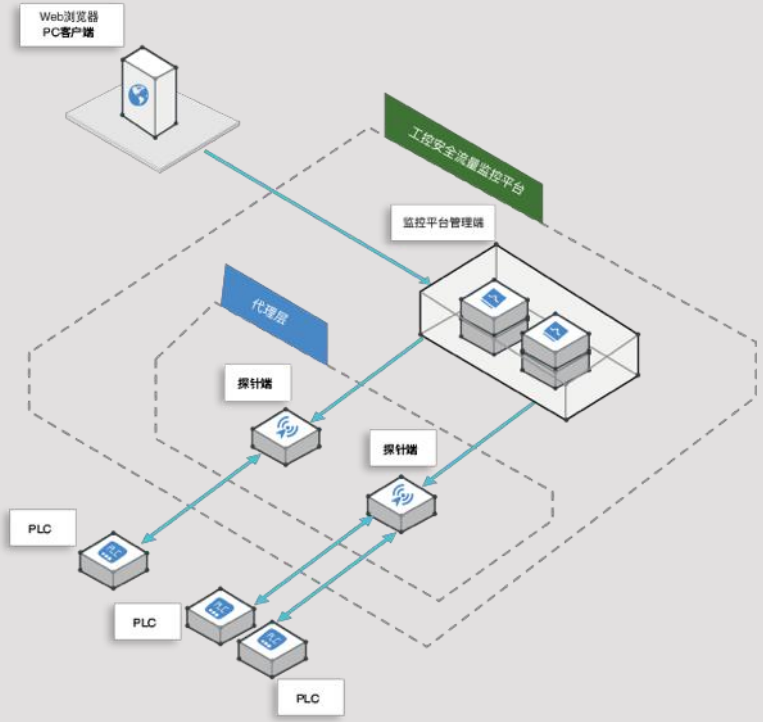
设备精准识别和拓扑自动发现	实现了主动和被动相结合的设备精准识别和拓扑自动发现。对于被动方式，采用流量旁路监听方式，可以通过网络流量监听识别工控设备、操作系统和型号等信息，同时可以发现设备间交互的网络业务流信息，同时建立了包含50多种设备和系统指纹的设备指纹库。对于主动方式，采用低交互拓扑自动发现技术，可精准发现工控网络拓扑以及设进一步详细信息。
多级智能检测引擎	创新性地提出了面向工控网络异常识别的多级智能检测引擎，基于概率状态图对工控网络正常行为进行精准建模，可识别业务流程和序列化操作和指令。设计并实现了面向网络流的智能检测引擎，采用人工智能技术，对网络通信行为进行建模，可支持对私有工控协议报文进行异常检测。针对不同的网络环境和负载可切换检测引擎模式，并支持各个引擎进行开关。
基于协议深度识别的网络行为分析技术	与市场现有产品相比，本系统不仅可以对协议进行深度解析和识别，还可以对协议中的工控指令和用户行为进行细粒度抽取，与业务和工艺过程进行关联，并进行对比分析，从而有效支撑对不符合业务流程的行为进行检测。
面向工控网络的双视图实时监控	实现了工业视图和网络拓扑视图相结合的双视图监控机制，可同时对工业过程情况和网络通讯指令及行为进行监控，并进行对比分析，从而更有效地发现异常行为和可能的攻击事件。

睿视工业网络异常监测审计系统

典型部署 | TypiCal Deployment

睿视工业网络异常监测审计系统的部署方案是有两部分组成：一是管理端，二是探针端（或称为代理端）。管理端负责呈现Web管理页面给用户，页面提供了功能操作的入口，当用户在页面操作指定的功能后，管理端会下发命令给探针端，从探针端搜集设备信息，流量信息和异常事件。探针端主要负责对流量的监测和异常检测，通过多层检测引擎对正常业务模式进行建模，对不符合正常模型的异常行为进行报警上报给管理端。 架构如右图所示：

此外，睿视工业网络异常监测审计系统还可以与睿知工业企业安全态势感知平台进行互动，态势感知平台再利用这些事件回馈验证其算法的准确度，调整算法参数让其更加智能，同时会把这些上报数据形成统计报告和攻击态势，对攻击行为进行分类等，对攻击的溯源和预警起到有效地支撑，从而形成一个完整的安全生态闭环系统。



谢谢观看

睿航至臻
RUIHANG TECHNOLOGIES CO.,LTD.

— 竭诚为客户提供优质化规范化的服务—