1.1 案例三：工业互联网企业安全综合防护系统——打造工业互联网企业全流程、全领域的综合安全保障体系

1.1.1 方案概述

本方案方案应用于国内一家大型化工集团央企，总部位于上海，但是集团和各分厂、厂区遍布全国（18 个省、直辖市），核心需求是实现集团与各分厂的安全风险和威胁实时检测，掌握总体安全态势，支撑安全决策和规划，同时满足工业互联网企业安全分类分级工作的管理需要。

1.方案背景

为深入贯彻落实《国务院关于深化“互联网＋先进制造业”发展工业联网的指导意见》（国发〔2017〕50 号），2022 年 3 月 31 日工网安函【2022】235 号关于征求开展工业互联网安全深度行活动意见建议的函，2022 年 5 月《工业和信息化部办公厅关于开展工业互联网安全深度行活动的通知》工信厅网安函【2022】97 号推动在全国范围内深入实施工业互联网企业安全分类分级管理的要求。

本方案实施在某大型化工集团企业，厂区和分公司遍布全国，实现企业（包括各分厂）安全风险和威胁检测，掌握总体安全态势，支撑安全决策和规划。通过方案方案实施为化工企业提供分类分级全生命周期安全服务，包括工业互联网企业分类分级综合管理、企业安全防护能力建设、企业态势感知呈现，对接省工业互联网安全监测与态势感知平台，实现 IT 与 OT 的融合分析，提供安全监测和预警通报、威胁溯源、公共安全服务技术手段，实现工业互联网相关企业安全态势可感、可知、可监管，为工业互联网发展保驾护航。

2.方案简介

方案目前已经验收并在企业实际工作中产生了效益，解决企业：

（1）各地域设备和系统的数据孤岛问题严重

在分厂与总部、厂区内各设备和系统的安全数据没有统一汇聚和分析，安全数据和分析结果没有打通和共享，各自为战。

（2）工控威胁和异常行为检测能力缺失

生产网（OT 域）缺少安全检测手段和能力，生产网络的安全状态不可知。

（3）威胁溯源分析无从下手

缺少安全数据关联分析和威胁溯源的技术手段，针对发现的攻击和威胁不能进行行为回溯和威胁画像，以及快速定位和确定所有被攻击资产和影响范围，并对威胁处置进行有效支撑。

（4）威胁处置无法聚焦，效率低

集团总部和各厂区每天产生的安全时间数量平均达 10 万多条，安全管理和运营人员完全无法有效分析和处理海量的安全事件和报警。

（5）安全态势不可视

集团和各厂区的安全态势做不到可知可控，不清楚安全风险和威胁的当前状态、影响范围和发展趋势，威胁信息也无法共享。

（6）不能满足工信部分类分级省企对接合规要求

作为三级联网企业，未按照分类分级管理要求与省级安全监管平台对接，也不清楚如何实现对接。

通过本方案建设工业互联网企业安全综合防护系统，为该化工行业企业提供工业网络安全综合防护平台能力和与省/市工业互联网安全态势感知平台对接等安全服务，形成了企业安全监测、预警通报、威胁溯源、安全服务能力，实现了工业互联网相关企业安全态势可感、

可知、可监管，为工业互联网发展保驾护航。

3.方案目标

本次方案重点方向为搭建工业互联网企业网络安全综合防护平台，围绕工业控制系统安全、工业生产网络与管理网络安全、工业数据安全等，建设工业互联网企业安全综合防护系统，构建包括资产管理、漏洞检测、配置核查、边界防护、入侵检测、态势感知、病毒防范、安全审计、数据保护等的一体化动态综合防御体系，形成工业互联网企业安全综合防护能力，全天候全方位监控关键生产设备及重要业务系统安全状况，及时发现、处置、阻断各类网络安全隐患风险，并支撑溯源取证，为中化总部和21个分厂提供安全保障和满足分类分级管理需求。

1.1.2　方案实施概况

根据经信委专家评审建议，结合工信部方案的管理要求，方案在2021年以公开招标的方式完成工业互联网企业网络安全综合防护平台方案的采购工作，目前方案已完成实施并取得很好的应用效果，实现了总部和分厂多源异构全安全数据接入，构建工控网络威胁检测能力和安全事件回溯能力。通过安全告警解决海量安全事件处理失焦问题，同时构建企业全领域态势感知能力，并按照工信部分类分级管理要求，实现了省企对接，满足分类分级合规要求。

1. 方案总体架构和主要内容

（1）方案总体架构

图 3-1　方案总体架构

平台的建设是整个方案的主要部分，主要包括如下内容：

➢ **数据采集接入：**实现对企业内外部多源异构数据的接入及汇聚，形成统一标准格式化数据。

➢ **数据处理及分析：**调用数据采集接入层形成的标准化数据进行分析及存储。通过 IT+OT 域研判结果汇聚、研判模型构建、事件智能研判及人工核验，梳理形成工业安全态势感知平台基础资源信息、联网设备及系统资产信息，形成基础信息库，安全技术库、知识库和规则库，为网络侧的安全监测分析提供数据支撑。

➢ **应用服务展示：**企业安全态势感知呈现，深度分析，日志检索，威胁溯源，资产管理，报表及策略管理，形成工业互联网企业安全综合防护能力，全天候全方位监控关键生产设备及重要业务系统安全状况，及时发现、处置、阻断各类网络安全隐患风险，并支撑溯源取证。

同时，平台与省级工业互联网平台对接，满足分类分级合规要求及数据共享，形成工业互联网网络安全的完整闭环。

（2）方案技术方案

➢ **资产画像：**通过主动探测、被动探测和静态导入等多种方式，全面探测全域资产，并通过自学习功能，收集业务访问日志，建立资产业务访问关系模型，实现精准的资产画像。

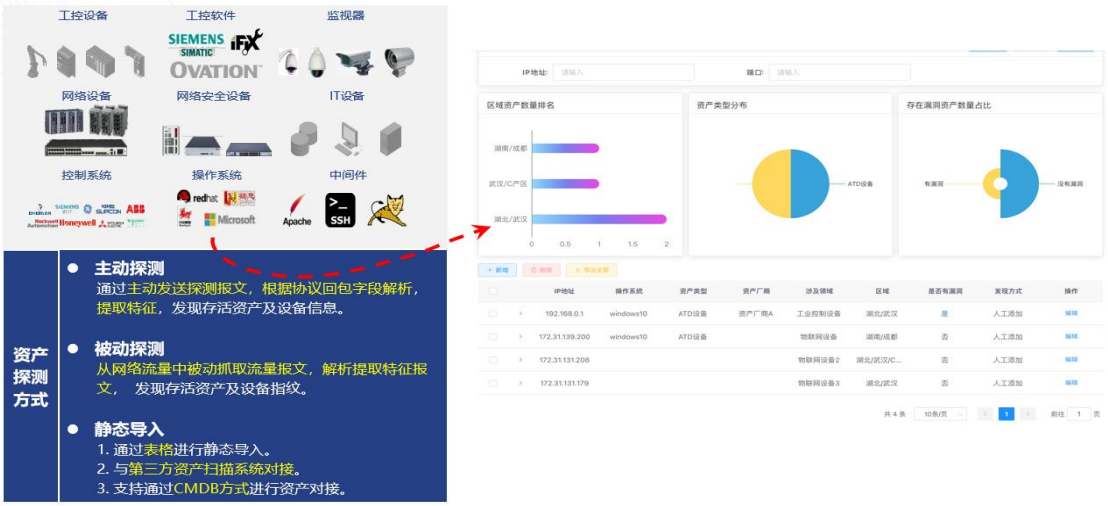

图 3-2　资产画像

➢ **多源异构数据灵活自动化配置接入：**通过人性化的设计和界面，为安全人员提供便捷的可视化安全策略配置功能，实现多源异构数据的快速灵活接入。

图 3-3　多源异构数据自动化配置接入

➢ **告警规则配置与运营：**依托海量现网安全数据汇聚和专家分析，积累网络安全告警规则并内置到系统，帮助客户快速建立安全能力。提供图形化、人性化的规则配置框架，通过时间段、威胁类型、发生频次等多维度，以及归并、去重等逻辑匹配规则的灵活配置，帮助安

全运营人员根据实际场景和阶段性关注重点，快速建立安全策略，提升安全运营效率。

➢ **全流程安全分析：**针对企业遭受的网络攻击进行实时监测，包括：密码暴力破解、拒绝服务攻击、勒索病毒、挖矿木马等。

图 3-4　全流程安全分析

➢ **安全深度分析：**根据企业客户业务需求，以及生产制造等领域的实际使用场景，挑选了 10 种工业协议，实现了这些工业协议的 100 多个字段深度解析，包括精准提取指令码、功能码、错误码等，工业协议的深度解析为工控通信异常，工控行为异常等工业威胁检测提供了基础和有力支撑。

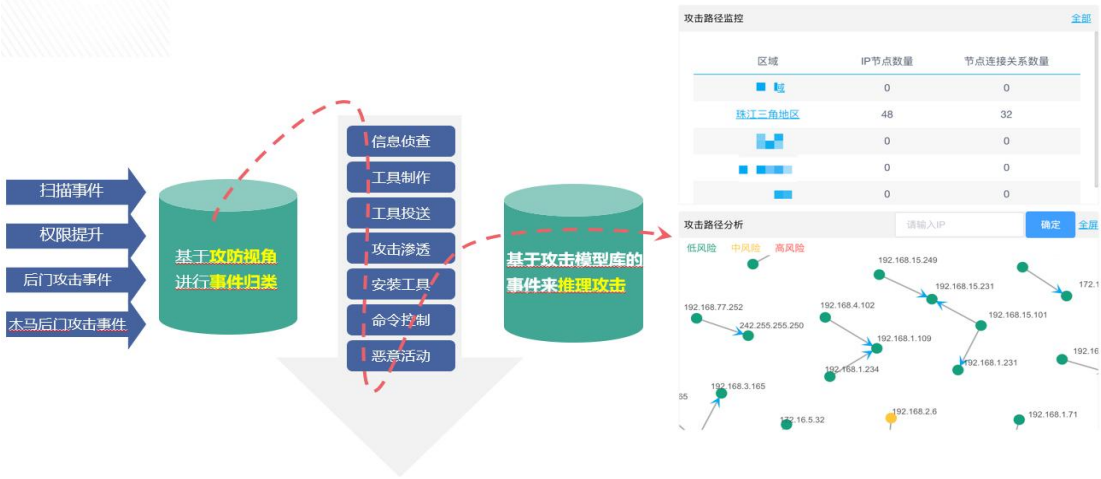

图 3-5　安全深度分析-攻击路径还原

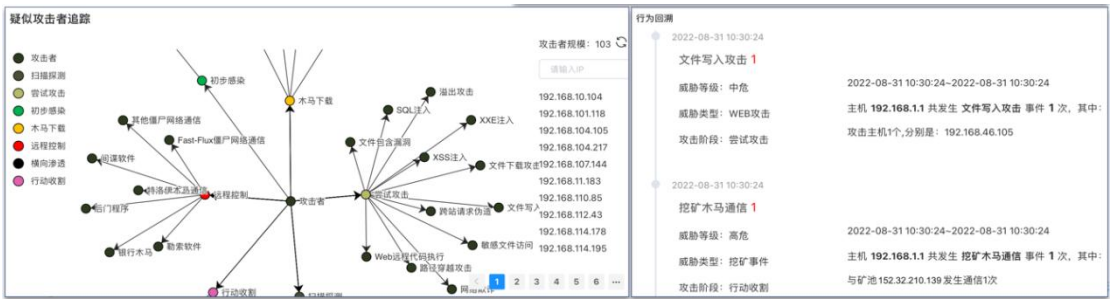

图 3-6　安全深度分析-风险主机画像

（2）方案主要功能

➢ 策略配置

策略配置包括区域配置、数据来源、范化策略和关联规则等功能模块，其功能是是实现多源异构数据的统一接入，以及安全分析规则配置和运营，为安全告警，深度分析和攻击行为回溯等功能提供支持。

数据接入策略

工业互联网企业中可能存在的大量不同类型，不同厂商的设备，例如网络设备，包括交换机、路由器等；安全设备，如堡垒机、防火墙、web 应用安全网关、入侵防御系统等；以及工业控制设备和系统等。这些设备和系统，都可以作为数据来源，态感平台通过范化策略模块，将不同的设备的数据进行归一化处理，统一接入到态感平台中。

安全告警规则

关联规则模块是安全分析知识库和规则库，通过规则的配置和运营，针对接入的多源异构数据进行多维度关联分析，产生安全告警和深度分析结果。在多源异构数据统一接入的基础之上，态感平台提供灵活、人性化的配置框架，帮忙用户进行规则配置和运营。

➢ 日志检索

提供接入的原始数据查询和检索功能。同时，通过对原始数据的统计和分析，向用户展示威胁事件分布，归属区域，攻击趋势，威胁等级，失陷主机等维度的分析结果。

➢ **深度分析**

基于 ATT&CK 安全分析模型，对威胁事件和攻击行为进行攻击链溯源和取证，如下图所示，通过对各类威胁事件基于攻防视角等多维度归类，依托安全分析模型和各攻击阶段的攻击路径和手法进行关联分析，为用户还原完整的攻击过程和攻击影响范围，并针对攻击者和被攻击者进行行为回溯和画像。

➢ **告警管理**

平台基于接入的多源异构数据和告警规则产生安全告警，从攻击方向（由外向内，内部横向和由内向外等）以及主机状态等多个维度，向客户展示资产的安全风险和面临的威胁状态，并进行预警。

➢ **资产管理**

平台的支持下列 3 种资产数据接入方式：

一是与客户已有的资产管理平台对接，接入资产数据。

二是与第三方资产扫描系统对接，接入资产探测结果。

三是手动录入，提供资产录入模板，实现资产数据的一键导入。

同时也接入资产的漏洞数据，并针对漏洞，从漏洞类型、危害级别、区域分布等多个维度，将资产与漏洞进行关联分析，对高风险资产向客户进行预警。

➢ **自动化报表中心**

形成企业安全自动化报表生成，提供安全报告生成和导出功能，为企业安全预警及安全决策支撑提供帮助。

➢ **企业安全态势感知**

通过实时安全事件监测，结合威胁情报和丰富的知识库进行分析和研判，帮助企业全面掌握安全状态和发展趋势。态势感知模块从监测对象，攻击方向，威胁类型等维度提供企业安全综合态势、资产态

势及威胁事件态势大屏呈现。

➢ **系统管理**

平台系统存储策略管理，操作日志及登录日志管理，保障系统安全及分权分域管理。

2. 网络、平台或安全互联架构

（1）系统部署全图示意

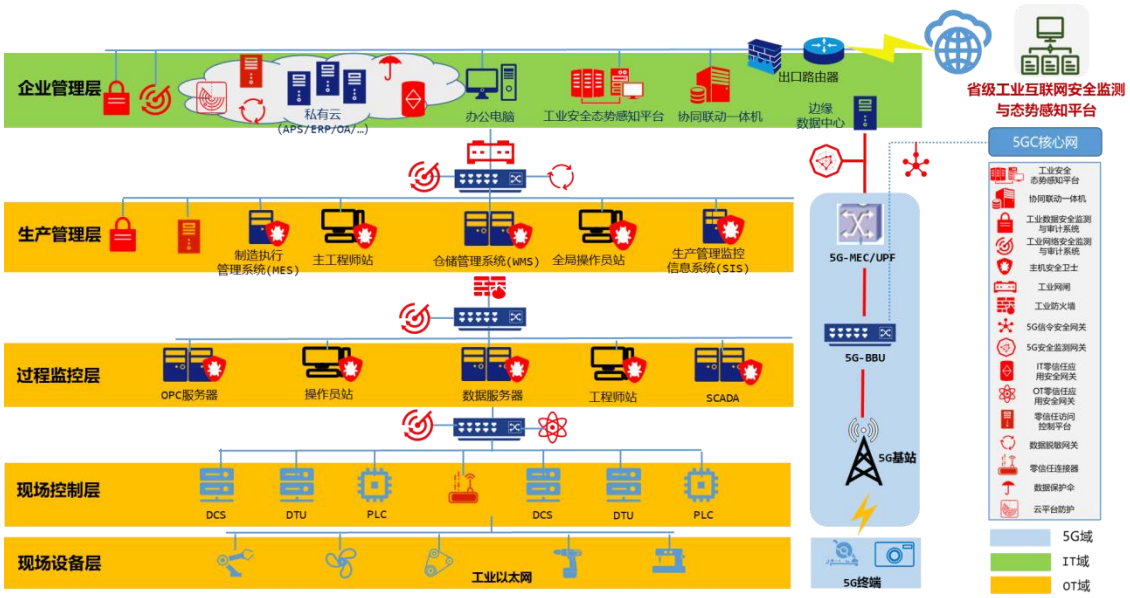

图 3-7　系统部署全图示意

通过在车间，工厂部署相应安全防护设备，实现对多源异构数据的采集分析，建设化工集团企业工业安全态势感知平台，同时通过企业安全协同联动一体机，实现与省级平台的数据对接及共享，满足分类分级要求。

（2）网络架构示意

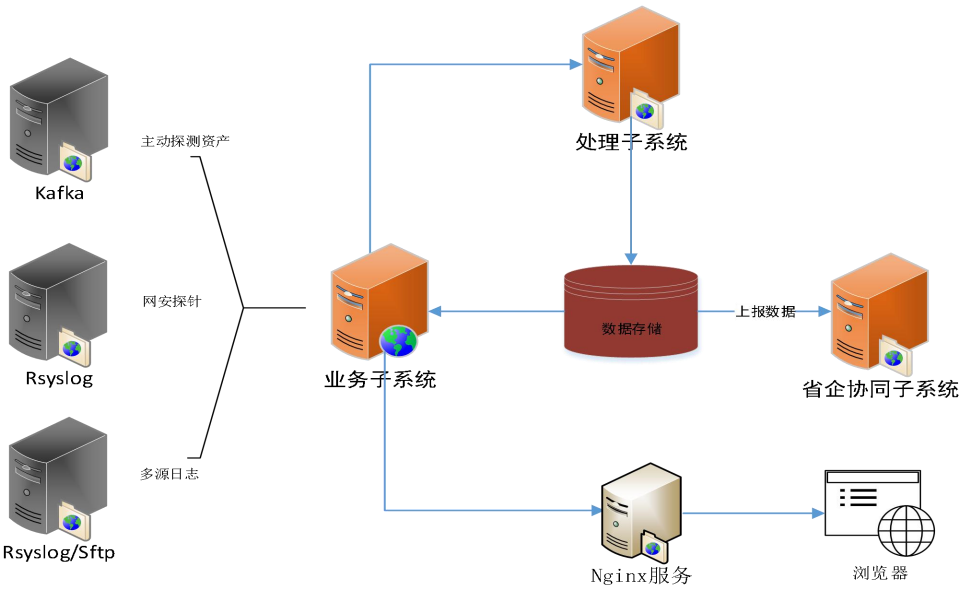

图 3-8　系统网络架构示意图

在化工集团车间及工厂部署主动探测及网络安全探针，以及对企业各类系统及日志的数据采集。整体平台构建统一大数据，实现对标准化数据的分析及处理、存储、分析呈现。

3. 具体应用场景和安全应用模式

（1）安全应用场景

方案方案后续对工业互联网企业各行各业均适用。

本次方案实用于工业企业的资产整体测绘、安全监测、威胁识别及溯源、态势感知呈现及省企对接服务。

（2）安全应用模式

方案的建成，极具推广价值，这个方案的安全应用模式，主要体现在以下几个方面发挥效果：

➢ 能够快速实施部署并达到既定效果，发挥试点区域先行示范的良好作用，为后续向全国工业互联网企业建设积累足够的建设经验，发挥试点区域现行示范的良好作用。

➢ 解决工业互联网企业痛点需求，如对监管部门要求理解不透彻，对省企接口规范了解不深入，难以满足监管部门的合规要求。

➢ 针对不同企业提供分类、分级差异化安全解决方案，开拓工业互联网服务客户市场，对分级分类工作提供全面保障，从企业安全全方位支撑工业互联网企业分级分类保障工作，建立实战化常态化安全技术手段，形成支持工业互联网安全发展合力。

4. 安全及可靠性

本方案将通过构建工业互联网企业全周期生命安全体系，从工业互联网企业互联网网络底层设计出发，采用多种先进的安全技术手段，为我国工业互联网的安全提供了有效的监测、预警、通报、协助处置能力。

该方案的实施，将会为工业互联网领域的发展提供有效的安全保障。具体包括：

（1）为工业互联网行业健康发展提供有效保护

我国是制造业大国，加快建设和发展工业互联网，推动互联网、大数据、人工智能和实体经济深度融合，发展先进制造业，支持传统产业优化升级，具有重要意义。通过本方案的研发，建设工业互联网安全态势监测与感知技术手段，有效应对网络安全攻击，形成与工业互联网发展相匹配的安全保障能力，为我国深化“互联网+先进制造业”战略的顺利推进和推广保驾护航。

（2）构建工业互联网安全监管技术体系

工业互联网作是产业互联网新业态，建设企业级工业互联网平台，有利于增强企业安全防护能力，为行业主管部门的安全技术保障提供支撑，为行业主管部门政策制定、安全监管、事中处置、事后溯源提供强有力协同共荣。

5. 其他亮点

（1）灵活的接入安全设备

方案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、工控监测审计、工控主机卫士等，同时支持第三方设备接入，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。

（2）领先的安全检测能力

支持安全合规检测、异常攻击检测、非法外联检测、设备运行状态检测、内网异常访问检测、非法程序启动检测、APT 攻击检测、恶意加密流量检测等。

（3）全面的安全分析技术

方案支持汇总各类安全数据，运用关联分析、用户画像、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，识别漏报及误报行为，提升安全运维工作效率，形成实时监测、动态感知的整体安全分析能力。

（4）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、业务等多个维度建立资产库，对网内资产进行实时安全监控，呈现网络安全风险、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

（5）完善的政企联动体系

快速实现省企对接，实现企业安全信息上报和省级平台威胁情报接收，并及时掌握对接效果，构建完善的省企联动、联防联控的安全防御体系。

（6）多维度安全态势感知

从资产的脆弱性、威胁和攻击等多个视角全面分析工业网络系统安全态势。通过人工智能和大屏可视化技术，直观呈现全网拓扑视图、告警趋势、实时告警等工业安全态势。

1.1.3 下一步实施计划

随着 5G+工业互联网的发展，势必带来如下安全问题：

■ 网络安全边界模糊

■ IT 与 OT 技术的融合，从专有硬件设备变成了通用服务器和云；

■ 专享组网模式将 UPF 和 MEC 从 CT/IT 信任域下沉到非信任域，业务通过切片进行逻辑隔离；

■ 部分用户数据仍会出公网，端到端安全边界防护受限。

■ 信令风暴风险

核心网下沉在企业后，信任域发生变化。 对 UPF 的 N4 接口以及 BBU 进行 N1/N2 接口的信令风暴监测，避免对云化核心网形成信令 DDoS 攻击

■ 物联终端接入协议复杂

新型物联网终端接入协议较为复杂，并且面临着代码漏洞，逻辑缺陷。攻击者可利用木马或者 APT 等方式入侵。

■ 网络安全风险

网络仍会通过 N6 接口访问互联网，会收到来自互联网的网络安全攻击来自于利用物联终端漏洞的攻击。

■ PLC 工控数据传输安全

PLC 通过 5G 将相关数据回传至管理平台，需要对 PLC 信令数据进行校验，防篡改。

因此，后续我们将于接下来解决 5G+工业互联网安全问题，如下

图所示：

图 3-9　5G+工业互联网安全

1.1.4　方案创新点和实施效果

1. 方案先进性及创新点

（1）方案创新性

➢ 企业安全能力建设

建设工业互联网完整基础资产库：工业互联网资产是其安全监测和预警的基础。本方案通过备案数据、主动探测、流量分析、特征识别等多种机制，形成覆盖全国各省的工业互联网资产库。

构建工业互联网特色安全知识库：构建最全面最权威的工业特征和安全知识库，提升安全管理能力。基于工控专用协议的盲识别与逆向解析技术工控设备深度信息扫描技术：通过工控漏洞互联网深度扫描技术，结合 CNVD 工控漏洞库，对目标区域的工控接入互联网设备进行深度扫描，从而实现攻击威胁和风险隐患识别预警，有效提升工业互联网资产发现能力。

大数据、云计算、人工智能关联分析技术：关联分析是对暗含攻击行为的安全事件序列建立关联规则。工业互联网网络安全公共服务

平台可对网络攻击事件等建立关联。

➢ 建立多方联动安全管理和预警机制

通过建立工信部、省、企业等多方联动监测和预警机制，实现安全威胁数据共享、知识库共享、应急能力共享的全方位联动响应。

（2）方案先进性

➢ 贴近实战为目标，服务企业工业互联网安全

通过建设面向工业互联网企业的企业安全综合防护系统及态势感知，打造完整生态，将工业互联网企业、工业设备制造商、安全厂商、工创中心、监管机构联合起来，一同治理工业互联网安全问题。在技术层面重点突破工业互联网安全诊断评估、安全预警、安全加固等相关核心技术。

➢ 政策优势与整合能力相结合推动工业互联网安全研究

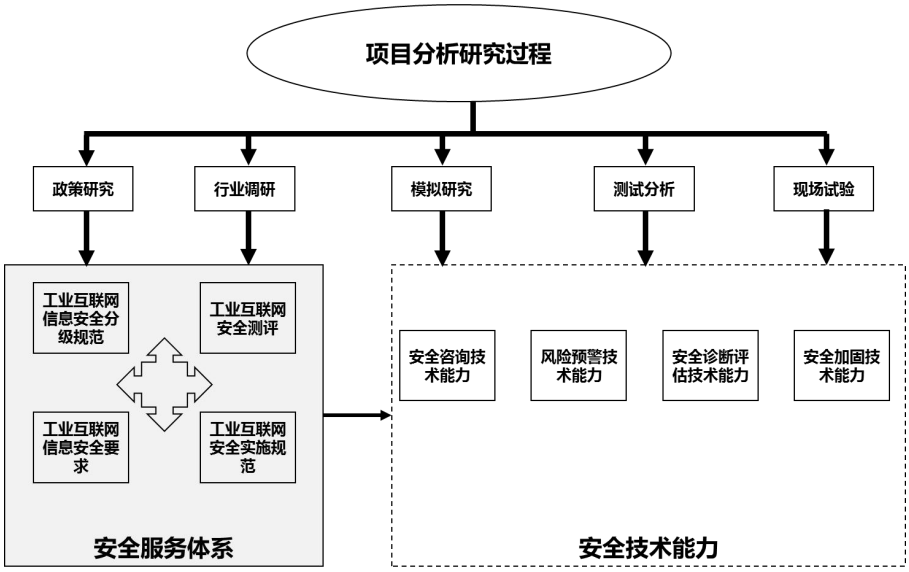

图 3-10　分析研究过程

➢ 开展关键技术方案研究

安全规范的落地：根据工业互联网信息安全分级规范、信息安全要求、安全实施规范和安全测评的规范，结合北京亚鸿世纪科技发展有限公司多年的安全行业经验，形成工业行业安全管理规范知识库进

行落地，为工业互联网企业提供技术标准、安全规划、安全咨询服务和安全培训服务。

关键技术能力的提升：通过攻防演练与仿真技术、工业互联网资产信息探测技术、工业互联网未知威胁监测技术等技术提升工业互联网企业行业风险预警、安全诊断平台、安全加固的能力。

➢ 全闭环安全能力覆盖为企业提供“云管边端业”多维安全防护服务

工业互联网进行全过程安全事件监测、事件溯源和处置，是保障工业互联网安全稳定运行的关键。本方案以流量覆盖检测为基础，数据安全能力相结合，从安全事件杀伤链的多个维度，实现安全串并分析能力建设，实现对工业互联网的安全监测、事件的追溯定位，安全问题及风险的封堵处置全流程实现安全事件的闭环管理服务。

2. 实施效果

通过方案的实施，解决了工业互联网企业防护手段集中于 IT 域，OT 域检测防护手段缺失的问题；利用未知威胁深度检测分析技术解决了传统安全基于规则，难以防御未知威胁的问题；利用自动化数据清洗及归类模块，解决了企业 IT 设备众多，各自为政的数据孤岛无法产生价值的问题；构建统一数据中心，解决工业互联网企业海量数据研判分析效率低，响应时间长的问题，同时为态势感知呈现提供数据支撑，解决企业安全现状不可见，无法掌握全局安全态势；与省平台对接，满足分类分级等合规要求。具体实施效果数据如下：

（1）通过多源异构数据汇聚技术和安全数据关联分析体系，实现 18 个省，21 个工厂，56 类设备，累计汇聚 2 千万条安全数据，实现安全数据的统一汇聚和关联分析，以及各厂区安全威胁实时检测。

（2）基于 100+工业协议深度解析能力，通过在指定厂区部署工

业安全监测与审计系统，接入和分析生产网的工业协议（S7，MODBUS等）流量，实现工业协议的深度解析和工控威胁检测能力。在实际运行中，发现：工控异常报文、高危指令执行、非法设备访问等工控威胁合计1600余次，帮助企业及时响应和处置生产网威胁，保障生产安全、业务连续性。

（3）基于大数据分析引擎和安全知识库，对接入的千万级安全数据进行关联分析，还原攻击者的攻击路径和攻击行为，关联出受影响或被控制的主机，帮助客户快速定位攻击源。在实际运行中，发现某主机7天内，对内网47台主机发起密码暴力破解攻击，达到14333次，通过进一步关联分析和攻击溯源，发现该主机遭受到外部攻击者漏洞利用攻击，可能已被控制，企业根据风险预警，对该主机进行了及时处置。

（4）帮助企业管理和运营人员，解决海量安全事件问题，基于已积累的300+条安全告警规则，达到业内领先水平。在系统实际运行中，安全管理和运营人员从每天面对10万条安全事件，降维到只需要聚焦处理1000条左右的安全告警，极大提升了安全管理和处理效率，让真正的安全威胁得到优先、及时和有效处理。

（5）从安全告警、资产漏洞、外部攻击、风险外联、横向渗透等多个视角，全面分析和展示企业整体安全状态，同时在实际运行中，通过分权分域管理和灵活的账号配置，各分厂可掌握自己的安全态势，而集团可掌握21个厂区安全态势。

（6）通过工业互联网协同联动一体机，在10个工作日内完成省企对接，满足分类分级合规要求。

1.1.5 单位基本信息

北京亚鸿世纪科技发展有限公司（简称“亚鸿世纪”）成立于2012

年，2017 年正式成为任子行网络技术股份有限公司的全资子公司，是一家专注于互联网空间数据治理、网络与信息安全及数据增值解决方案及服务的高科技公司。公司在北京和武汉设有分公司及研发基地中心，能够快速响应客户安全需求。目前研发中心技术人员达到 400 多人，其中 985、211 高校毕业人数达到 80%以上。

公司成立以来，协助工信部起草《IDC/ISP 信息安全管理系统技术要求》、《IDC/ISP 信息安全管理系统接口规范》、《域名信息安全管理系统技术要求及接口规范》、《数据核验技术要求及接口规范》等多项技术规范。公司目前已经承建了工信部全国统一资源协作管理系统、工信部全国域名信息安全管理系统、工信部互联网大数据管理子系统、设备运维子系统、全国 25 省通信管理局互联网网络与信息安全综合管理平台、19 省移动 IDC/ISP 信息安全管理系统、17 省联通 IDC/ISP 信息安全管理系统、14 省铁通 IDC/ISP 信息安全管理系统、5 省电信 IDC/ISP 信息安全管理系统。在 IDC/ISP 信息安全领域市场综合占有率达 80%以上，在互联网反欺诈安全市场占 50%以上。具备丰富的互联网信息安全和网络安全的实战经验以及相关安全能力。

围绕 5G+工业互联网安全建设方面：

■ 国家级

国家工业互联网安全态势感知与风险预警平台：建立国家、省级、企业级联动的工业互联网安全监管体系，实现重点行业、重点对象、重点风险的实时监测、动态感知、及时预警，支撑政府监管、服务企业防护。

工业互联网网络安全分类分级管理平台：自主定级、定级审核、现场评测、安全资源池建设，支撑分类分级政策落地。

工信部物联网基础安全接入监测平台：物联网资产摸底、宏观监

测、整体态势分析。

■ **省级**

工业互联网网络安全省平台：广东、湖南、河南、安徽、湖北、辽宁、贵州、新疆、黑龙江、海南、河北、四川、云南、内蒙、甘肃、上海、西藏、山西等 18 个省级工业互联网安全监测与态势感知平台。

工业互联网数据安全省平台：贵州、四川工业互联网数据安全监管平台试点。

■ **工业互联网企业级**

面向多个行业多个企业的 MEC 安全监测平台、边缘计算敏感数据保护技术系统、多业务场景数据脱敏技术工具、面向工业和通信业的网络及数据安全风险监测发现与预警平台、工业互联网网络安全公共服务平台、工控安全防护系列产品、企业安全服务等。