1.1 案例八：某省工业互联网安全综合服务平台——打造省、市级工业互联网安全公共服务生态体系

1.1.1 方案概述

今年，工信部印发组织开展2022年工业互联网安全深度行活动，旨在全国范围内深入实施工业互联网企业网络安全分类分级管理工作，要求各地工信厅、通信管理局联合第三方专业机构制定实施方案5月30日前报送工信部，并在11月底前开展本地深度行活动。

针对深度行活动提到的“分类分级管理”内容，湖南省工信厅搭建了省级湖南省工业互联网安全综合服务平台，安恒全程主导并参与平台建设。2022年5月20日，在湖南省工信厅和省通管局联合举办“工业互联网安全深度行活动”中平台正式发布，预示整个湖南省的分类分级管理工作将在该平台的支撑下进行深度推广，为工业企业用户提供服务。

1. 方案背景

（1）工业互联网是数字经济高质量发展的国家战略

工业互联网以数字化、网络化、智能化为本质特征的第四次工业革命正在兴起。作为新一代信息技术与制造业深度融合的产物，通过对人、机、物的全面互联，构建起全要素、全产业链、全价值链全面连接的新型生产制造的新型生产制造和服务体系，是数字化转型的实现路径，是实现新旧动能转换的关键力量。为抢抓新一轮科技革命和产业变革的重大历史机遇，世界主要国家和地区加强制造业数字化转型和工业互联网战略布局，全球领先企业积极行动，产业发展新格局正孕育形成。

2019年10月18日，习近平总书记向“2019工业互联网全球峰

会”发来贺信。习近平指出，“当前，全球新一轮科技革命和产业革命加速发展，工业互联网技术不断突破，为各国经济创新发展注入了新动能，也为促进全球产业融合发展提供了新机遇。中国高度重视工业互联网创新发展，愿同国际社会一道，持续提升工业互联网创新能力，推动工业化与信息化在更广范围、更深程度、更高水平上实现融合发展”。 同时，习近平强调，“深入实施工业互联网创新发展战略，系统推进工业互联网基础设施和数据资源管理体系建设，发挥数据的基础资源作用和创新引擎作用，加快形成以创新为主要引领和支撑的数字经济”。习近平关于工业互联网的系列指示体现了对工业互联网发展的高度重视，彰显了推进工业互联网发展的紧迫性和重要性。

（2）工业互联网安全是其发展的重要保障

工业互联网包括网络、平台、安全三大体系。其中，网络体系是基础，工业互联网将连接对象延伸到工业全系统、全产业链、全价值链，可实现人、物品、机器、车间、企业等全要素，以及设计、研发、生产、管理、服务等各环节的泛在深度互联。平台体系是核心，工业互联网平台作为工业智能化发展的核心载体，实现海量异构数据汇聚与建模分析、工业制造能力标准化与服务化、工业经验知识软件化与模块化，以及各类创新应用开发与运行，支撑生产智能决策、业务模式创新、资源优化配置和产业生态培训。安全体系是保障，建设满足工业需求的安全技术体系和管理体系，增强设备、网络、控制、应用和数据的安全保障能力，识别和抵御安全威胁，化解各种安全风险，构建工业智能化发展的安全可信环境。

（3）工业互联网安全在转型过程中面临的挑战

随着工业互联网的发展，IT 与 OT 不断融合，使原有的工厂内外网络边界变的模糊，由于产业模式的创新发展，工厂内外的信息传递

更加频繁，这将使黑客更容易入侵到工厂内网络，攻陷生产设备和系统，对生产造成巨大损失。工业控制系统信息安全目前面临着信息安全与工控系统自身安全融合的要求。目前工业互联网安全产品还处于产品阶段的 1.0 版本的时代，与目前 IT 信息安全和 IT 系统的适配程度相比还有比较大的差距。工业控制系统安全产品是与业务应用相关度比较高的产品。目前的工业互联网安全产品体现在与业务的融合度不够，在深度检测与业务相关的攻击行为的时候往往乏力，缺乏创新性的安全检测思路，防护思路往往缺乏真正有效的方法。另一方面，随着工业领域中的一些新的应用，如工业云、工业大数据等的普及，工业控制的业态也必将发生一些变化。而信息安全技术与新的业态融合时，必然需要与业务进行融合。而目前工控信息安全技术的融合还没有完全展开，需要在技术方向和应用上有所突破。

2. 方案简介

（1）需求分析

政策驱动需求：政策文件的下发，为各地方区域级工业信息安全监管部门具有明确的监管工作指导意义，分别从如何对企业分类分级，如何做好分类分级的安全防护，以及如何做好相关安全监测预警工作给出了较为明确的工作行动目标。

业务驱动需求：形成监测预警、信息通报、协同应急处置的闭环管理机制；形成工业企业分类分级安全监管闭环管理机制；形成面向工业企业提供安全服务的生态体系。

（2）解决方案

方案将工业互联网安全“监测预警与协同应急管理”、“工业互联网企业安全合规管理”和“工业互联网安全支撑综合服务”三大业务应用融为一体，以“工业互联网安全公共服务”为核心能力，为工业

互联网安全监管部门和工业企业提供“双向赋能”。打造省、市工业互联网安全公共服务生态体系，逐步形成集约化工业互联网安全运营服务中心。

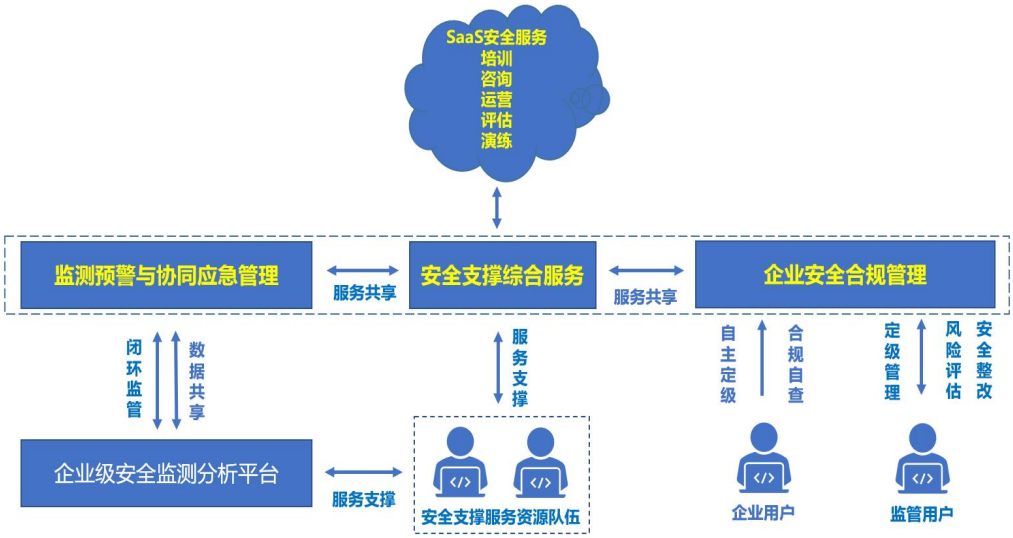


图 8-1　集约化工业互联网安全运营服务中心

3. 方案目标

（1）提升、完善全省工业互联网威胁感知能力

工业互联网数字化转型过程中，业务应用场景也越来越多，因此相应的网络安全监测手段也需要进行补充和技术提升。本次建设需要提升全省工业互联网企业安全整体态势感知、分析能力，实时掌握更多、更全面的各类工业互联网场景下的安全动态，在发生工业互联网安全事件时，也无法进行精准预警。为实时掌握全省工业互联网安全情况及动态，在发生安全隐患时可以进行快速、精准预警，需依托大数据技术建立全省工业互联网安全感知分析能力，实现精准匹配、重点分析，并提供多个维度可视化的大数据分析结果，为研判、决策工业互联网安全保障工作提供有效支撑，提升对关键目标的管控、风险识别的水平。

（2）建立省级工业互联网安全应急响应协同指挥体系

根据《湖南省工业控制系统信息安全事件应急预案》的相关要求，

为积极落实责任要求，形成安全事件闭环管理机制，加快建立省工业互联网安全协同协作机制，需要结合实际需要对全省工业企业建立监测、预警、防范协同管理机制，建立相应的技术平台，实现省工信厅、地市工信局、工业企业、技术支撑单位级其他监管单位等在工业互联网安全安全层面上的协作、互通，进一步完善监测预警、信息通报、应急处置等相关机制的建设。

（3）建立工业领域网络安全分类分级合规管理机制

以《网络安全分类分级》为依据，完善工业企业网络安全合规管理机制，打造精细化、差异化的科学管理方式。形成面向工业互联网联网工业企业、工业互联网平台企业、标识解析企业等三类工业互联网企业开展网络安全分类分级管理工作，参照行业重要性、企业规模、安全风险程度等因素，将企业网络安全等级由高到低划分为三级、二级、一级，并针对不同类型、不同级别的企业提出差异化安全防护要求。

组建工业互联安全评测机构和专家队伍，提供专业化工业互联网安全风险评估工具，开展对工业企业的现场安全检查和信息调查。针对工业企业进行定期及不定期的巡视检查，通过建立全省工业互联网安全检查机制，借助线上监测加线下检查形成监管合力，摸底全省工业互联网安全状况。

（4）建立工业企业与省平台监测数据安全共享能力

依据《工业互联网企业网络安全分类分级管理指南》要求，三级工业企业需要在企业建设安全监测分析平台，并将在企业内监测的数据信息上报给省级平台。因此，需要实现工业企业安全监测分析平台与省湖南省工业互联网安全综合服务平台的安全认证与数据传输共享服务，以保证两平台间数据传输共享的安全性。

（5）建立工业互联网安全公共服务能力

一是加强对省工业信息安全公共服务能力，通过对工业企业资产梳理、安全隐患监测、安全事件分析研判、应急响应支持、安全态势感知服务、安全运营服务等，提高全省工业企业提供网络安全公共服务的能力。

二是针对信息安全意识、安全技能、热点安全事件定期组织安全培训，辐射全省，对各级工信单位、重点工业企业进行网络安全业务培训，形成常态化工控信息安全人才队伍建设与培养机制，增强各级各部门网络安全意识和防护水平。

（6）建立跨平台数据采集和共享机制

目前省工信厅、通管局等相关单位均对各自负责监管领域建设监测、存储系统，同时工信部已建设国家级工业互联网安全监测与态势感知平台，但尚未建设各级信息互通、共享的数据交换平台，数据无法连通，工作难以互动。为解决这一问题，需建立共享数据机制，互通有无，信息共享，同时保证数据的安全性。

1.1.2 方案实施概况

1.总体设计原则和策略

（1）设计原则

厉行节约原则：在平台建设过程中，要尽量利用现有的信息系统、网络基础设施、安全监控数据等，综合考虑对已有资源的共享和利用，避免重复建设和浪费。

标准规划原则：在方案设计和设备选型方面遵循国家以及行业内的相关标准，严格按照有关程序组织方案建设，并且建设标准符合国家及行业提出的接口规范和技术架构。

重点保护原则：根据工业互联网系统的重要程度、业务特点，实

现不同强度的安全保护，集中资源优先保护重点工业控制系统。

技术先进原则：平台设计立足先进技术，采用先进的系统结构、开放的体系架构，使系统在一个周期内保持技术领先水平，具备长足的发展能力，以适应未来网络技术和安全技术的发展和系统使用的科学性。

（2）设计策略

平台建设坚持三个策略：

“全”。即全源化采集，在现有数据采集来源的基础上扩大数据采集范围和采集数据类型，确保平台数据来源的全面性。

“优”。即整合优势产品，平台选用的产品是从众多安全厂商中优中选优，确保平台的先进性，并整合各安全设备管理能力，如等流量监测引擎、威胁感知引擎、工具箱等设备可实现与平台业务系统的无缝对接。

“实”。即实战化应用，平台设计涵盖监测、态势、通报、处置、情报、应急指挥、攻防演练等功能，最大程度实现工作业务需求，形成工控安全态势监管业务闭环，最大限度服务于实战。

2.平台逻辑架构设计

湖南省工业互联网安全综合服务平台是为省监管部门提供工业安全数据采集、大数据研判分析、实时监测、通报预警、响应处置、应急指挥等，以及提供工业企业分类分级管理和综合安全服务一体化的服务平台。

平台总体架构设计遵照“分层解耦、异构兼容”的原则，分为安全引擎层、安全中台层和安全应用层三个层次，各层级以及模块之间的功能设计具有相对的独立性，从而使得整个系统具有较高的扩展性。安全引擎层作为平台的基础能力层，安全中台实现数据的采集处理、

挖掘分析和提供统一的数据服务，构建数据驱动业务体系。安全应用层通过建设满足用户的各类业务应用，协助监管部门开展工业互联网安全的保卫工作。

平台总体架构如下图所示：

图 8-2　湖南省工业互联网安全综合服务平台架构设计

（1）可视化安全态势感知层

平台为监管人员、企业人员和安全支撑机构人员提供不同岗位视角的可视化安全态势感知大屏，满足不同角色需求，提供综合态势、预警态势、隐患态势、事件态势、分类分级态势、攻击者溯源态势、资产威胁溯源态势和网络星空态势。

（2）业务应用层

平台基于微服务架构，结合用户实际需求，分别为各级用户实现各类应用服务能力，平台由可视化安全态势感知、监测预警与协同应急、安全合规管理和综合安全服务，打造完整生态，将各级监管部门、安全支撑机构、安全专家等人员联合起来，一同来治理工业互联网安全问题。

（3）安全中台层

安全中台层包括安全数据中台、安全业务中台和安全能力中台组成，为上层业务应用提供安全数据服务、业务流程管理和安全能力服务。

（4）安全引擎层

基础安全能力层为平台运行和其他单位提供必要的基础安全能力和数据来源，包括网络资产测绘引擎、威胁检测识别引擎、网络攻击诱捕引擎、网络防御引擎、威胁情报管理引擎、云端安全监测引擎、网站安全监测引擎和安全检查引擎等。

3.平台技术路线

（1）分布式存储技术

分布式存储技术作为态势感知系统最为重要与基础的支撑技术。分布式存储技术能够实现结构化及半结构化数据的统一存储，兼容传统的关系型数据库以及 SQL 访问模型，同时支持对海量数据的在线实时流式处理框架和离线分布式计算框架。分布式数据库面向时序数据和小文件数据存储进行深度优化，支持第三方存储引擎和传统关系型数据库的无缝接入；支持海量混合数据的统一存储管理和在线离线一体化查询；支持可插拔安全算法模块和主流分布式计算框架；支持跨库、跨源、异构数据库之间的跨库访问和关联查询，解决了多系统交互时对海量混合数据统一管控的问题；支持多源异构混搭数据间基于规则导向的高可靠近实时数据同步。主要功能包括：

● 大数据采集存储和分析处理。满足采集海量数据储存需要，如流量信息、设备状态、链路状态等，满足大规模结构化流式数据的并发能力、吞吐量、低时延的高要求。

● 分层架构、模块化设计、多场景支持。采用模块化的设计思路，在数据访问层、数据路由层和数据存储层都提供多种高内聚、低耦合

的模块，通过这些模块的灵活搭配，分布式数据库表现出不同的技术特征，从而能够适应不同的业务场景。

● 在线检索和离线分析一体化。通过配置，分布式数据库可同时支持高速数据写入，在线交互访问、实时查询以及高并发大数据集查询在内的各种访问方式，适应在线检索和离线分析等不同业务场景。

● 混合数据支持。分布式数据库支持与传统关系型数据库Oracle、MySQL等联合访问。业务系统可以把部分表建在Oracle或MySQL上，把部分表建在分布式数据库上，然后透明地访问这些表，包括在这些表之间进行join、union等操作。

● 跨域、多数据中心支持。分布式数据库在保证数据一致性的前提下支持多数据中心或多数据集群之间近实时的跨域数据同步复制，实现系统的跨域多中心部署模式。总体处理性能，数据读写、扫描等，随集群规模扩展线性增长。

● 分布式存储形式主要基于通用/定制化的X86服务器提供存储，可提供对象、文件和块存储，具备低成本、灵活扩容、高并发访问等优势，通过软件保障性能和可靠性。可作为资源池的分级存储手段，满足中低端存储、数据归档备份、大数据存储等需求。采用X86服务器和分布式块存储软件技术的Server-SAN在I/O能力、部署速度和扩展性方面已验证优于传统块存储技术（例如FC-SAN/IP-SAN）。

分布式存储技术用于系统架构的大数据组件当中，使系统能够实现高效的数据采集和检索能力。

（2）多源异构数据融合技术

大数据分析的根本是数据，针对高价值数据的分析往往事半功倍。然而测评领域大数据分析在数据方面所面对的现实问题总结下来主要分为以下三种形态：

来源多：包含服务数据、基础数据资源、数据交换获得的私有数据资源、以及互联网采集的数据资源，这些数据随着业务的变化而变化。

组成乱：数据资源包含结构化数据，如 MySQL、Oracle 等等；半结构化数据：XML、CSV 等等；以及非结构化数据。数据结构乱、形式不一。

质量碎：数据往往以孤岛或碎片化的形式存在、缺少关联、语义不明确甚至缺失。

面对上述问题，就需要一种能够处理、整合多源异构等复杂形态的数据归一化模型，将不同形态、杂乱无章的数据整合成统一的样式形态。同时，能够基于该数据整合模型，以“人”、“事”、“物”等数据分析为主体、实现数据的大串联、大融合，将原来孤立的“点”数据、“面”数据、“条”数据融合成为一定空间、时间范围内的“块”数据，做到价值的萃取，形成业务可用的大数据。

多源异构的数据融合技术运用在系统的数据治理融合层，通过体系化的数据治理方法论结合基于模型驱动的数据治理技术用以提升数据质量，便于数据分析建模的建立。

（3）全文检索技术

全文检索技术是态势感知系统的核心基础功能，其基础要求是根据搜索条件快速、准确的匹配命中数据对象，为安全分析人员提供高效准确的分析工具，以便能更加快速的发现安全风险。因为大数据系统往往采用分布式存储技术，所以全文检索技术的选择必须能够支持主流的分布式存储系统。同时，分布式并行计算系统的支持也是在技术路线选择中必须考虑的因素，需能够做到对并行计算框架的无缝对接。由于测评系统的大数据分析功能对数据搜索准度、实时性与多样

性的要求，这就要求检索技术需支持基于关键词，数值范围，日期范围等各种复杂的搜索功能。

全文检索技术采用倒排索引的结构达到快速全文检索的目的，倒排检索是实现“单词”-“文档矩阵”的一种具体存储形式，通过倒排索引可以更加快速的获取包含这个单词的文档列表，倒排索引主要由两个部分组成“单词词典”和“倒排文件”，具体结构如下图：

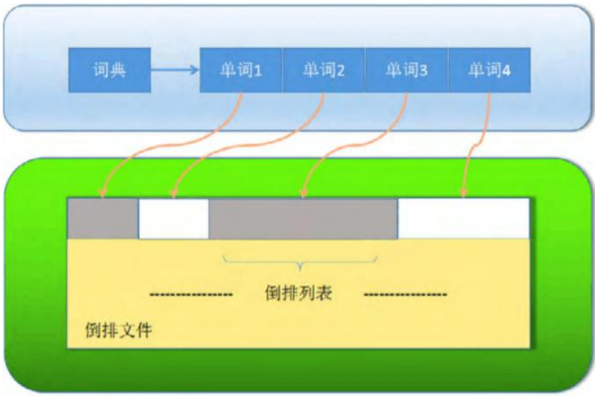


图 8-3　全文检索技术架构图

全文检索技术运用在安全监测中，主要用于对监测数据的检索查询，通过查询安全分析人员能够实现对安全事件的细致分析，并将有效数据运用于模型建立当中。

（4）关联分析可视化技术

数据关联分析即线索扩线，是一个从有限的数据线索向未知数据进行挖掘探索的过程。选用关联分析可视化技术主要因为是：数据分析人员需要在各类数据库中反复比对、查询、线索串联。运用可视化关联分析技术能够以图形化界面、流畅交互操作等形式将枯燥的数据分析变得生动，能够在很大程度上提高数据分析员的工作效率。在可视化技术选择上，能够突出数据关联关系的特征，便于分析人员理解。同时，数据统计等可视化辅助功能能够帮助分析员理解数据含义，提高工作效率。

通过数据清洗、要素提取融合，系统实现多要素多维度的关联分

析，从工控异常行为、工控恶意操作、僵尸网络、木马、蠕虫、勒索软件、漏洞攻击、WEB 攻击、DDOS 攻击、恶意通联关系、恶意样本、恶意通信、恶意邮件、恶意域名、APT 攻击等安全事件入手，运用关联分析技术完成态势可视化展现，构建由微观到宏观的态势分析，形成安全攻击态势变化的能力。

关联分析可视化技术用于系统的数据分析层，主要作用是将多源异构数据通过关联分析模型串联起来，找到各类数据源之间的关系，并通过可视化技术进行最终呈现。

（5）溯源分析可视化技术

在处理和分析互联网事件时往往需要从海量的数据里查找有用的线索，这不但是存储、索引、计算技术的挑战，具体分析工作也面临着困难：呈现在列表式表格中的大量数据，难以发现数据的模式、趋势和关联关系等分析重要要点。可视化就是用来解决这些问题的最佳方案。

目前已知的对人类认知最有效的方式就是通过视觉感知，相比其他的交流呈现方式，使用数据可视化来交流具有很多的优势，包括：

数据可视化能快速的进行复杂信息的交流：可视化在最小化数据细节特征损耗的同时，可以在数秒钟快速呈现上百万个点信息，非常适合与统计信息呈现。具体到本方案，对本地威胁态势全局信息的展示就非常适合采用可视化的方法，可以快速的掌握趋势、热点等重要信息，对从全局把握网络安全态势有着不可替代的作用。

数据可视化能识别潜在模式：一些模式特征通过统计学方法或者扫描数据的方式难以发现，却可能通过可视化方法被揭示出来。而当在可视化展示数据的时候，存在于单个变量中的模式或者多个变量之间的关联关系就可以呈现出来。数据可视化的这个特点特别有利于在

网络事件调查过程中使用，通过一点线索，利用可视化分析方法，可以发现、呈现出更多和它有关联的其它信息点，达到拓线，进而溯源事件的目的。

溯源分析可视化技术用于数据分析层，是态势感知系统的一类重要分析技术，主要用于对安全事件的追溯，通过溯源可视化分析方法帮助管理人员准确发现攻击背后的真正意图。

（6）威胁情报生成技术

威胁情报的生成是一个复杂的过程，需要具备多种能力才有可能完成，一般可以分为如下图这样的八步：

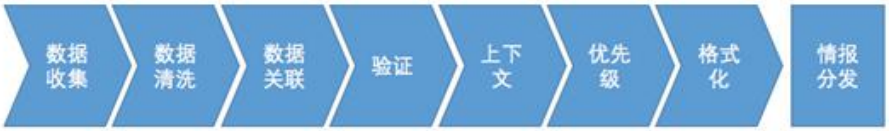


图 8-4　威胁情况流程图

➢ 数据收集：这是关键的一步，决定了产生的情报是否能最全面的覆盖威胁，因此往往需要聚集多种不同来源的情报数据（包括但不限于样本数据、黑客团伙相关数据、DNS 相关数据、WHOIS 相关数据、僵尸网络相关数据等），以保证情报质量。

➢ 数据清洗：将以上数据根据后续加工的需要进行整理、去除不可信数据、将关键数据结构化等过程。

➢ 数据关联：数据关联是数据验证的前提条件，通过数据关联梳理不同类型数据间的关系，如样本、样本不同方式的检测分析结果、样本的网络行为、域名注册者、域名指向的 IP、IP 上面的其它域名等。

➢ 验证：通过建立了关联关系的数据，再利用机器学习的方式（有可能结合部分的人工分析）对情报的准确性进行验证，并赋予相应的

可信度指标。这也是决定情报质量关键的一步。

➢ 上下文：包括如攻击类型、样本家族、攻击团伙、攻击目地、传播渠道、具体危害等报警响应需要的内容。

➢ 优先级：根据攻击目的、具体危害等信息，确定报警优先等级信息；

➢ 格式化:根据分发的要求,将情报以特定的格式输出,如:STIX、openIOC、JSON、xml 等，非 MRTI 类型的情报还可能以 PDF、word 等类型提供。

➢ 情报分发：根据不同类型情报的用途，可以推送给安全产品、打包供下载、或者邮件发送。

威胁情报生成技术使用在数据治理融合层和数据分析层,在数据治理融合层主要解决情报信息的收集、格式化、清洗及情报分发等问题，在数据分析层实现情报信息的验证和关联分析。

（7）总体数据库设计

平台数据库设计基于海量数据采集、处理、存储及分析挖掘需要，主要包括原始库、主题库、资源库、知识库和业务库等。

■ 原始库

原始库数据为前端部署的威胁检测识别引擎采集的流量数据,数据结构分为结构化数据、半结构化数据和非结构化数据。数据类型主要包括应用会话识别数据、应用会话流量数据、网络传输流量数据、应用层流量数据、用户登陆行为数据、流量审计数据和风险告警数据等。

■ 主题库

主题库是融合各类原始数据、资源数据长期积累形成的多维数据的公共集合，具有数据规模量大，且频繁更新等特点。支持通过实时

计算和离线分析计算对数据执行查询、分析、映射、检索等操作，支持实现海量数据规模下检索的秒级响应。数据类型主要包括单位画像数据、系统画像数据、IP 画像数据、失陷主机数据、黑客组织数据、重大漏洞数据、僵尸网站数据和非常规端口开放数据等。

■ 资源库

资源库是存储各类数据资源建立的关键要素以及要素之间关联关系的公共数据集合，包括单位数据、资产数据、流量日志数据、隐患数据、告警数据、安全事件数据和其他外部数据等。

■ 知识库

知识库是指信息安全专业领域或与信息安全专业领域相关的特征知识数据和规则方法集合。一般通过管理手段、工作积累、第三方提供、机器学习等方式获取。数据类型包括恶意 IP 数据、恶意域名数据、告警规则数据、重大漏洞等。

■ 业务库

业务库记录业务过程，为上层业务系统提供数据支撑。数据为结构化类型且数据规模不大，常用的应用场景是查询和关联。主要包括通报预警业务数据、应急指挥业务数据和管理评价业务数据等。

（8）协同监管体系

平台纵向实现与工业企业、国家平台的数据贯通和业务协同，横向实现与各行业主管部门以及社会上从事网络安全工作的企业单位的数据的数据共享交换和工作业务协同，并借助安全厂家的威胁情报数据能力，提升全省网络安全监管能力。为此需要提供自动化的数据接口、制定相关数据和接口标准规范，以实现数据的传输交换。

数据传输类型

传输的数据类型主要包括：

✓安全事件类数据；

✓安全隐患类数据；

✓网络资产类数据；

✓业务处理类数据。

数据传输接口

查询及业务类的数据支持 HTTP 协议传输；

原始数据的交换共享支持 kafka 和 syslog 等方式进行大流量网络传输；

若有特定的传输需求，支持通过协商的方式进行其他协议或组件进行数据传输。

数据共享交换

平台纵向实现与工业企业和国家平台的数据共享，横向实现与行业主管单位的数据共享，并通过全面采集接入全省网络安全监管数据和第三方安全厂商威胁情报数据，形成平台数据存储中心。

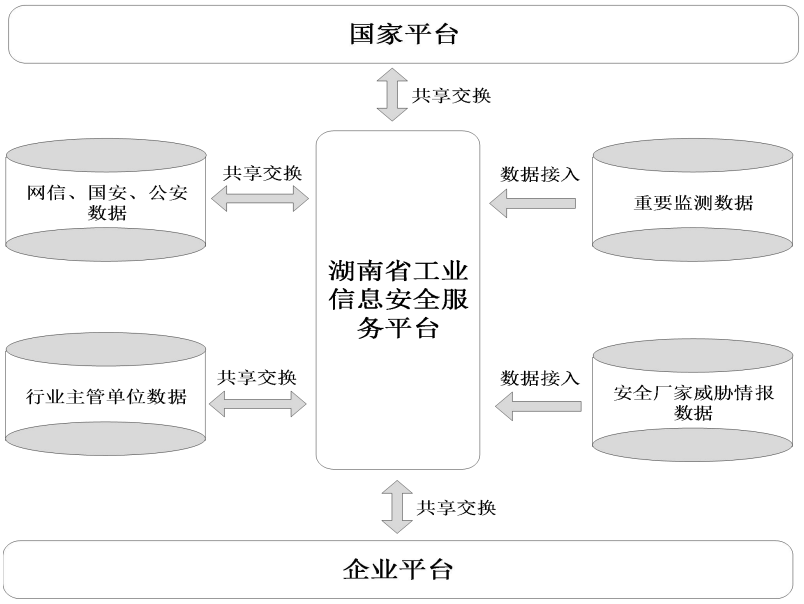


图 8-5　数据共享交换图

4. 平台建设内容

湖南省工业信息安全公共服务平台是为湖南省工信厅工业信息

安全监管部门提供工业安全数据采集、大数据研判分析、安全监测、通报预警、响应处置、应急指挥等，以及提供工业企业安全合规管理和综合安全支撑服务一体化的服务平台。

（1）平台数据采集方案

- **工业企业数据采集**

多源异构日志数据采集

对主流安全设备、网络设备、主机、数据库、中间件、应用系统和虚拟化系统等设备异构日志进行全面采集，实现资产日志数据统一管理。同时为满足日志数据共享需求，提供收集日志转发，当原始日志设备无法设置多个日志服务器时，可通过本系统进行日志转发将日志转发到其他日志存储设备。

异构日志数据采集覆盖 Syslog、SNMP、OPSec、XML、FTP 及本地文件等多种协议，对安全对象属性、运行状态、安全事件、评估与检测等异构数据进行采集，针对不同类型数据能够自动适配协议。同时为提升采集性能，降低数据冗余噪音，可自定义配置日志过滤功能，对采集的重复日志进行自动聚合归并，减少日志量。

全流量数据采集

对网络流量数据进行采集，并将捕获的通信数据转换为数据分组报文格式递交给上层组件，作为上层特征检测引擎分析处理的原始数据。通过双向流量检测对网络流量行为进行判定（例如数据报文恶意特征匹配、资源使用情况、使用者的访问行为等），识别病毒、木马、敏感信息等异常行为。

- **威胁情报数据采集**

提供云端采集、接口采集、本地累计以及本地导入共 4 种方式进行威胁情报采集和累计。

云端采集

提供针对外界的威胁情报采集、展示和利用功能。

接口同步

支持动态采集开源威胁情报，也可以采集第三方商用威胁情报，至少提供一家商业威胁情报厂家接口；

提供丰富的云端采集更新接口，支持安恒自身威胁情报库、第三方商用威胁情报库以及开源的威胁情报库，网络威胁情报包含恶意IP、URL、Domain、Email等。

本地威胁情报积累设计

支持将本地发现的安全事件和恶意IP、域名、文件、钓鱼网站、E-MAIL等事件转化为威胁情报。

本地导入

支持通过本地离线包导入情报，支持通过使用离线威胁情报数据包更新情报数据。

- **网络空间扫描探测数据采集**

采用云端网络空间资产探测雷达对全省网络资产进行侦测以及漏洞扫描和分析趋势分析，快速识别全省以公网IP接入互联网的物联网设备、工控设备、应用系统、网络设备的存活情况、开放端口、组件等信息。通过对互联网资产、邮箱资产、监控设备资产、工控设备资产等各类资产进行探测，识别其指纹信息、漏洞信息以及可能受攻击情况，摸清全省资产底数，为监测、预警、溯源等提供基础数据支撑。

- **现场检查数据采集**

现场检查数据是通过工业控制系统安全检查工具箱对企业进行安全检查过程中所采集的数据，主要包括企业安全合规自查数据、资

产漏洞、流量分析、配置核查、恶意代码等检查数据。

采用离线采集方式，将工业控制系统安全检查工具箱的检查数据导出后，再通过工业企业分类分级模块的进行数据导入，以完成采集动作。

➢ **第三方平台数据采集**

鉴于本地监测存在单点监测的局限性和高级威胁监测的不足，平台将接入第三方威胁情报数据，按一定的时间规则推送到本地平台大数据中心，并利用大数据平台机器学习能力，结合互联网上活跃的数百亿样本以及样本的行为进行实时追踪分析以及事前预测。

➢ **数据采集管理**

采集部署

数据采集引擎实现个性化数据采集，支持配置不同采集策略，如动态配置采集周期，清洗过滤策略等。采集部署支持如下功能：

- 支持分布式多节点部署；
- 支持多采集节点存活、健康状态监控，发现节点异常后，及时告警；
- 支持对采集节点进行性能监控，保证采集性能与数据量匹配，防止数据丢失；
- 支持对采集策略进行管理，包括采集频率、采集协议、采集目标、过滤策略等；
- 支持流量数据镜像采集，支持在多个机房交换机上复制镜像，分布式部署分光器和 DPI 进行采集，并将多余接口关闭；
- 支持主机终端数据采集，支持数据库审计分析数据采集；
- 支持数据汇聚，综合考虑专网传输性能的基础上，满足将多个机房采集到的数据传输汇聚。

采集协议和频率管理

适配各种采集数据源，需要支持多种采集协议，以实现对各类数据的采集，包括不限于安全对象属性、运行状态、安全事件、评估与检测等数据。为实现对包括安全对象的属性、运行状态、安全事件、评估与检测等数据的采集，针对不同类型的数据以及对应的适配协议

（2）平台安全中台建设方案

安全中台层包括安全数据中台、安全能力中台和安全业务中台。

- **安全数据中台设计**

安全数据中台实现对所有监管数据、威胁情报库数据的整合、归档、应用以及对上层提供数据服务能力；包括安全大数据中心和安全大数据分析引擎两部分。其中，安全大数据中心主要提供数据集成、数据管理、数据目录等功能，通过统一的数据接口为上层提供数据服务。安全大数据分析包括实时分析、离线分析，为上层提供统一的安全大数据分析能力。

架构设计

安全数据中台的总体目标是建设一个完善的信息资源共享服务技术体系，建立信息共享的标准和规范，为平台上层业务应用提供统一、开放、标准、完整的信息资源服务；全面开展内外部数据归集、整合、重新组织、共享等工作，建立完整的信息共享资源目录和信息资源服务能力；提供统一的大数据处理服务能力，提升信息资源服务能力，解决平台对海量数据的深度挖掘、分析、应用的迫切需求。大数据服务平台是基于平台建设，以服务应用为根本目标，建立信息资源服务能力和大数据处理能力，实现数据集成、数据整理、数据共享、数据分析等数据处理及服务能力。

功能架构

安全数据中台遵从数据安全和数据标准的规范，并按照数据采集、数据处理、数据治理、数据资产、数据服务和数据运维几个方面进行有机结合。全方位打造集“采集”、“融合”、“服务”于一体的数据服务平台。

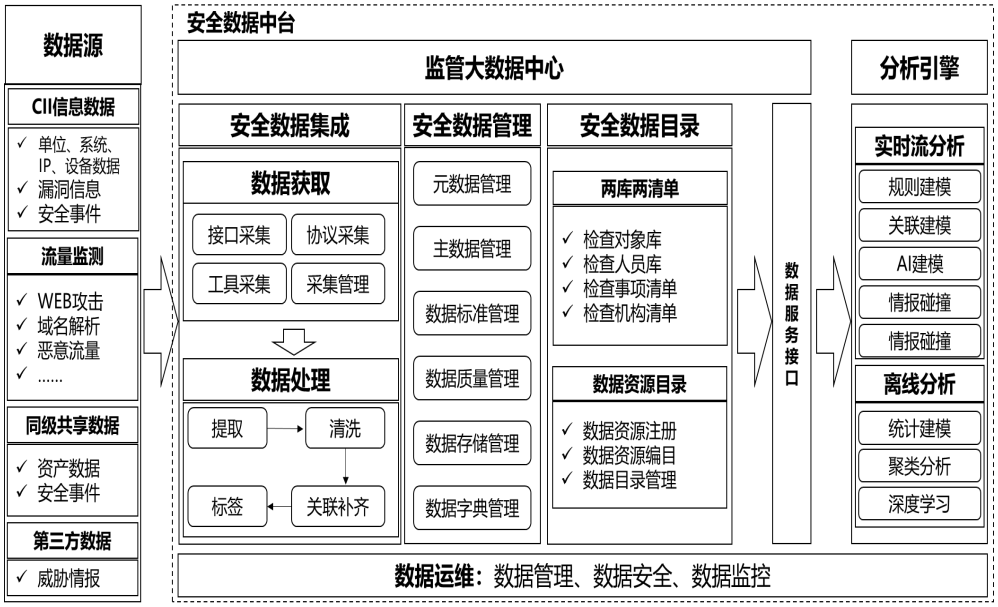


图 8-6　安全数据中台功能架构图

技术架构

大数据中心是大数据存储和计算的基础，对外提供统一的各类型数据存储、计算、分析等能力，可满足多源异构海量数据存储、查询、计算。

数据采集包括实时采集、自定义接口采集和离线采集，支持各类数据源数据

接入，如日志数据、流量还原数据、syslog 数据及用户自定义数据等。

数据预处理实现数据消息缓存和 ETL。

数据存储实现外部数据保存至大数据服务平台。数据存储需支持结构化数据、

半结构化数据、非结构化数据等多种数据类型。数据存储中包含

两大主要部分，非结构化存储系统、半/结构化存储系统。

安全大数据分析引擎实现安全数据中台的计算功能。数据计算能够对所有已保存的数据进行计算，并且提供相应的计算调用接口，能够满足外部分析系统的调用。数据计算中包含实时流分析和离线分析两部分。

运维管理包括大数据管理系统和大数据交互系统，支持数据平台的所有组件集中安装、部署。支持对数据平台各个组件的配置管理、动态调整配置实时生效。

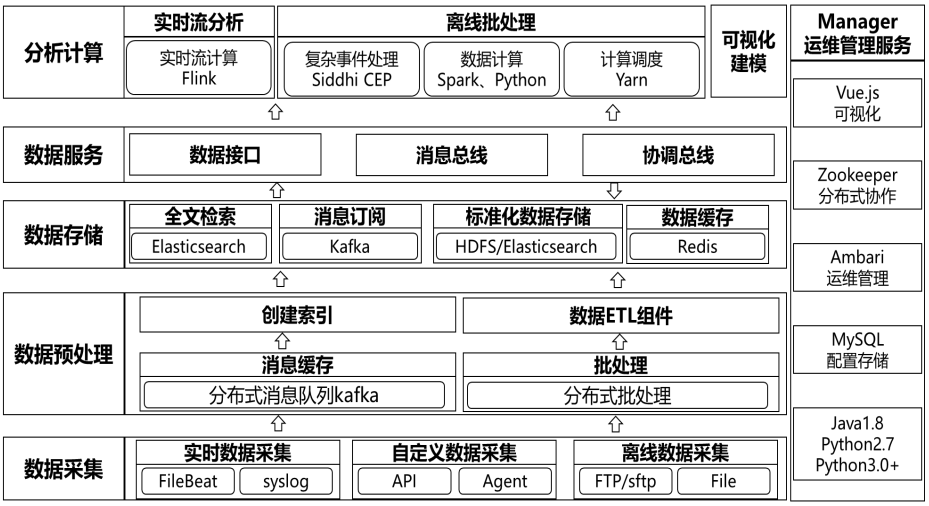


图 8-7　安全数据中台技术架构图

➢ 安全业务中台设计

构建工作流引擎，快速有效的支撑不断出现、迭代、优化的安全管理业务流程：一是可以通过引擎完成业务流程的节点编排，支持用户完成通报、预警、通知、检查等业务流程的构建；二是通过引擎对参与到业务流程的用户权限进行合理的配置，包括审核权、回退权、处置权、办结权等，需能通过引擎合理的进行赋权，且支持用户级的权限变更和删除；三是通过引擎将流程与资源库、业务库中的相关表单进行关联，并通过引擎支撑业务流程中挂载业务、处置表单的自定义，完成业务数据和流程的动态结合，真正将流程与业务紧密捆绑。

工作流引擎

随着工信安全业务的快速发展，通报、预警、检查等业务流程越来越精细化、人性化，其相关的流程、表单也不断在进行迭代优化，因此在这种快速发展的环境下，需要有一套工作流引擎高效、人性化地支撑变化的业务。

需要构建工作流引擎，快速有效的支撑不断出现、迭代、优化的安全管理业务流程，满足以下三方面：一是可以通过引擎完成业务流程的节点编排，支持用户完成通报、预警、通知、检查等业务流程的构建；二是通过引擎对参与到业务流程的用户权限进行合理的配置，包括审核权、回退权、处置权、办结权等，需能通过引擎合理的进行赋权，且支持用户级的权限变更和删除；三是通过引擎将流程与资源库、业务库中的相关表单进行关联，并通过引擎支撑业务流程中挂载业务、处置表单的自定义，完成业务数据和流程的动态结合，真正将流程与业务紧密捆绑实现用户的管理需求。

自动化办公引擎

工信安全管理业务中涉及到安全专家、安全管理员、安全审核员、安全联络员等众多角色和人员，这些角色需要参与到不同流程的不同环节中，为了提升业务流程的处置时效性，需要实现业务的多端发起、多端触达和汇聚呈现，需求通过相应引擎使得业务多端自动流转贯通。

需要构建自动化办公引擎，实现业务的多端通信、汇聚，满足以下两方面：一是通过引擎将 PC 端和移动端发起的业务自动的向另一端实时同步，满足用户随时通过移动端发起、办理相应业务的需求；二是需求通过引擎从平台所有业务模块中获取当前用户待办事宜，提供给 PC 端或者移动端的门户页面，支持客户在一个页面中就能完整的了解当前待办事务，提升处置效率。

值班排班调度引擎

工信在应急活动保障期间和重大事件应急处置中需要快速的传达信息到相应的值班专家、安全管理员处，因此需要制定相应的值班排班表，并根据排班表进行高效的人员调度。

需要构建值班排班调度引擎，实现以下功能：一是通过引擎，支持用户在相应重保活动或应急处置保障期间，对安全专家等角色的值班工作进行排班，且自动化的通知到相关人员；二是通过引擎，自动向相应业务流程发布排班信息，使得值班期间相应业务可自动派单值值班人员；三是支持通过引擎调度短信网关、移动端应用通知等通知通道，将值班安排、业务流程等第一时间送达相应的用户处；四是支持引擎将平台用户登录、操作情况与值班表自动进行匹配、关联，定期生成值班分析报告，供用户进行后续工作考评和优化。

绩效管理引擎

工信安管工作由众多角色、厂商参与支撑，旨在推进了辖区内被监管单位提升网络安全工作质量。为了对平台人员/厂商的支撑绩效进行科学合理的评价，同时也对辖区内被监管单位的网络安全工作效果进行评估，需要绩效管理引擎进行自动化的初始绩效输出。

绩效管理引擎需要实现以下功能：一是通过引擎，可以对平台内已有的资源库、业务库中的相应指标项进行提取，支持用户结合实际绩效考核方案对指标进行自由的遴选、组合，进而生成符合工作实际场景的绩效评价表和评价方案；二是确定评价表和评价方案后，通过引擎周期性或按指令对全平台相应数据进行采集、统计、核算，并自动统分，输出相应的绩效报告；三是支持客户对平台外的数据进行录入后作为绩效考核项，进而更加全面、科学的给出绩效报告。

- **安全能力中台设计**

安全能力中台包括安全能力中心和安全能力管理，可将各种安全能力服务化，形成安全服务目录，实现安全资源的灵活调度，从而对基础安全能力进行统一管理。安全能力中心约定系统建设的安全能力目录，包括安全检测能力、智能安全分析能力以及态势感知能力。安全能力管理约定系统建设的安全能力调度和实用能力，例如能力编排、能力调度、策略管理以及场景管理功能。

架构设计

安全能力中台包括安全能力中心和安全能力管理。

安全能力中心约定本次建设的安全能力目录，包括安全检测能力、智能安全分析能力以及态势感知能力。

安全能力管理约定了建设的安全能力调度和实用能力，包括能力编排、能力调度、策略管理以及场景管理功能。

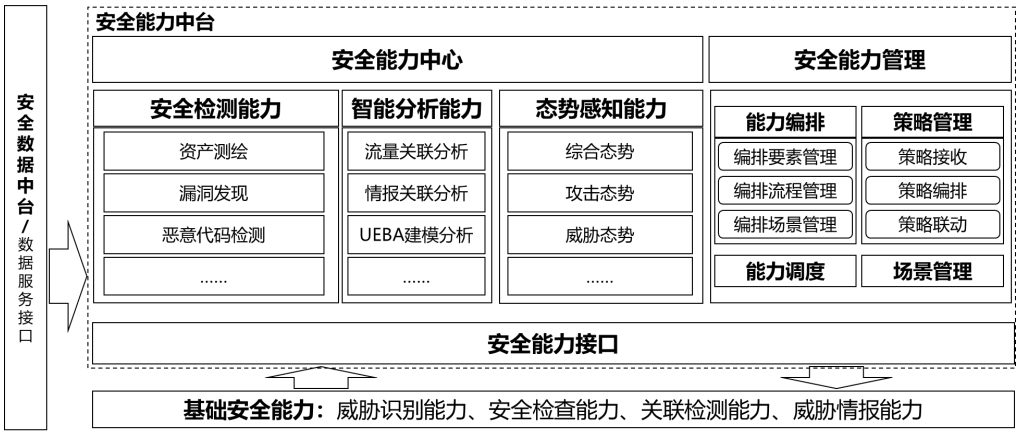


图 8-8　安全能力中台功能架构图

安全检测能力

安全检测能力主要包括基础安全能力中的威胁识别能力、关联检测能力接入和统一管理。主要依赖安全基础安全能力中的资产发现识别、漏洞扫描和深度流量威胁检测等产品来实现多维安全检测能力。

通过对各种安全基础安全能力的封装和编排，终端、边界等实体防护对象提供安全检测服务，快速发现已知和未知的安全威胁。安全

检测能力能够通过安全能力管理对安全检测能力管理、数据分析、规则管理、安全基础资源管理实现自动化编排和协同联动。

安全检测能力结合大数据相关技术和智能算法，从资产角度出发，重点关注资产管理，提供基线核查配置，并结合多种角度维度分析攻击，全局化地安全态势感知能力，智能感知攻击中的安全事件，为用户信息系统安全识别、威胁检测和安全业务管理提数据支撑。

智能安全分析能力

智能安全分析能力主要包括流量关联分析、情报碰撞分析、攻击画像和原始日志检索。

态势感知能力

态势感知能力主要在全局监测数据、检测数据、智能分析数据等多维数据的综合态势分析之上，形成综合态势、攻击态势、威胁态势、预警态势等多种态势感知能力。

风险隐患调查能力

隐患调查功能是安全监测的核心功能，实现独立的安全事件采集、分析和集中管理功能。主要提供如下功能：

安全设备告警事件管理。为用户提供集中的安全设备告警事件管理功能，支持事件分析和处置及误报标记；

风险隐患统计。提供以资产维度和攻击链维度的安全事件统计功能，支持根据资产和攻击链进行事件检索和攻击影响范围分析；

风险隐患溯源。提供安全事件一键溯源和关联攻击链功能，可关联威胁情报、安全告警、安全原始数据上下文等信息，极大的方便安全事件调查和分析；

资产管理调查。提供以资产为维度的安全威胁调查，以攻击链的方式展示资产受攻击的过程和正处于的被攻击状态；提供的调查维度

包括资产间访问关系、行为画像、服务/请求的端口以及弱点等信息；

攻击知识图谱调查。提供通过全流量数据生产的企业网络安全攻击知识图谱，为用户提供单个资产为视角出发的攻击知识图谱和全网络的攻击图谱，支持图谱的向下钻取和关系扩展， 图谱信息包括攻击链阶段、协议、端口等信息。

安全能力管理

基于构建的能力体系，通过剧本编排，对分析、响应处置过程中各种复杂的分析流程和处理平台进行整合，形成自动化的能力集成，实现从静态事件响应到动态工作流跟踪的转变，提升整体的协调及决策能力。

剧本以原始数据或安全事件作为输入，结合统计分析以及统计模型、情报模型、关联模型进行分析，并实现追踪溯源、联动阻断等响应动作，最终上报监控单位并通知管理员。具体流程如下图所示：

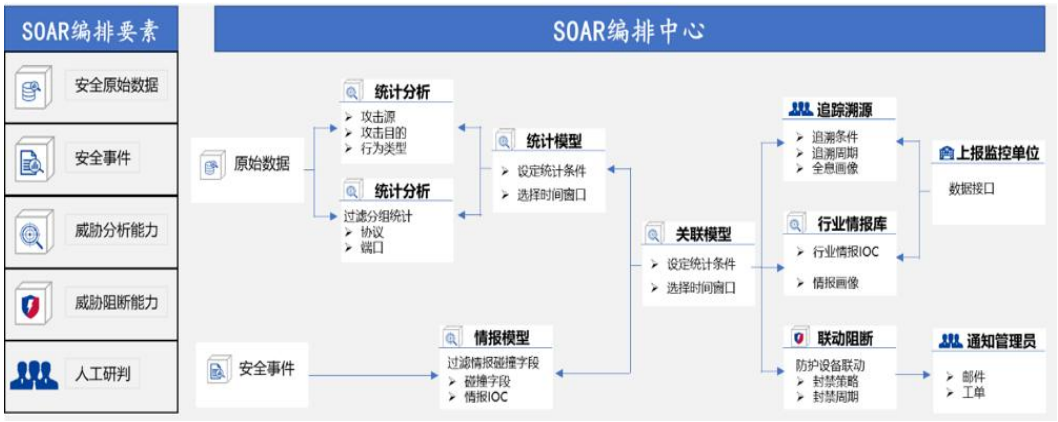


图 7　能力编排流程图

（3）平台业务应用建设方案

平台基于微服务架构，结合用户实际需求，分别为各级用户实现各类应用服务能力，平台由于三个业务应用模块构成，分别是工业互联网安全监测预警与协同应急业务应用、安全支撑综合服务业务应用和企业合规管理业务应用，打造完整生态，将企业、安全厂商、监管机构联合起来，一同来治理工业互联网安全问题。

➢ 监测预警与协同应急

监测预警与协同应急为工业互联网企业监管部门提供一套具备工业互联网企业安全数据采集、数据处理、存储、分析，以及对安全事件实时监测、通报、预警、处置的一体化解决方案。主要业务应用包括实时监测、态势感知、分析研判、通报预警、威胁情报、应急指挥等，全面提高工业互联网网络安全监测、预警与应急响应水平。

实时监测

实时监测针对工控系统、工控设备、服务系统、网络设备、终端、物联网设备等在线网络资产的资产分布、漏洞和指纹信息进行扫描探测和统一管理，摸清区域资产底数。及时发现各类网络攻击、风险隐患、安全事件以及网络资产。实时临测主要包括验证中心、成果中心、搜索中心和监测任务中心。

图 8-9　实时监测界面

分析研判

分析研判利用大数据关联分析技术，结合机器学习算法，自动对流量、情报、攻击等数据进行分析；分析研判提供对平台汇总的各类监测服务威胁信息的专家核验功能。并为威胁分析人员提供包括情报关联分析和模型算法分析功能。为平台业务人员提供各类统计分析能

力和模型，可实现基于平台威胁告警信息和统计分析模型生成的预警信息，为湖南省网络安全预警业务提供基础能力，主要包括模型中心、追踪溯源、可视化中心、报告中心和知识库。

图 8-10　分析研判界面

威胁情报

威胁情报是一种基于证据的知识，包含了上下文、机制、指示标记、启示和可行的建议。威胁情报描述了现存的或者是即将出现针对网络资产的威胁，并可以用于通知主体针对相关威胁或危险采取某种响应。高级威胁尤其 APT 攻击手法隐蔽，危害巨大，主要针对掌握有重要数据和信息的特定人群，攻击一经发生就会导致国家重要价值资产的泄密流失，而且后续定位、追查、定性都会遇到技术难度。高级威胁情报可以对 APT 攻击事件的定位、发现、定性、溯源提供良好的支撑，可以强化安全保障部门对各个重点保护企业的监控力度和防护强度。

图 8-11　威胁情报界面

通报预警

通报预警提供对安全事件、风险进行及时预警、通报和处置的功能。当监测到工业控制系统存在重大风险隐患，或产生重大安全事件时，通过平台进行通报，被通报的工业企业按期反馈处置结果。平台需具备多种通报方式，包括钉钉、短信和邮件等。在发生严重情况时，可立即通过短信、钉钉等方式进行通报；当系统监测到轻微安全隐患时，可进行预警提醒或限期整改，被通报单位须及时反馈处置结果。

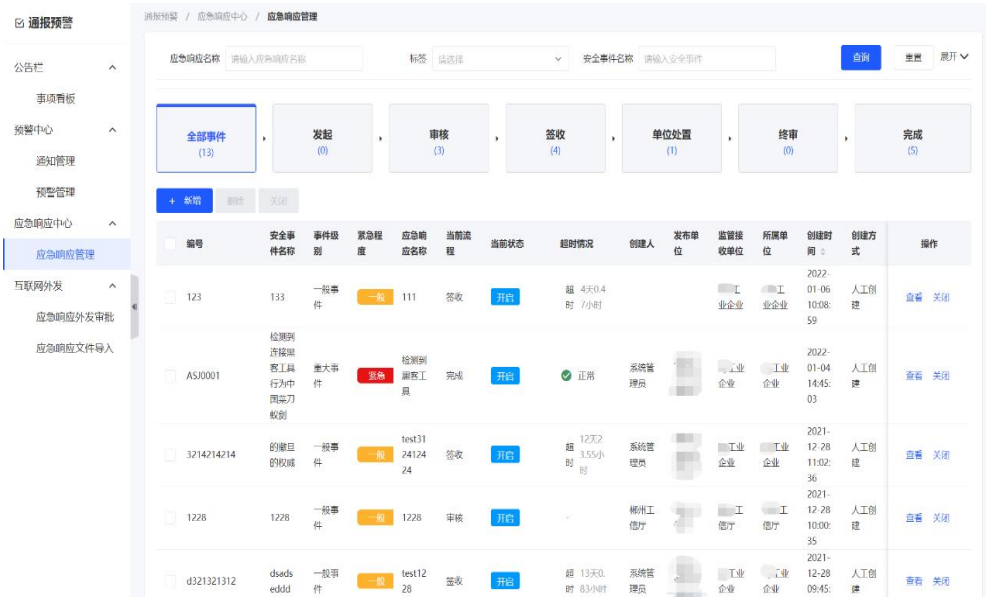


图 8-12　通报预警界面

应急指挥

应急指挥基于挂图作战理念，基于 GIS 系统的可视化特性，同业

务系统进行数据对接，通过直观图形化点击拖拽等方式支撑各级单位、人员的活动监控和应急指挥两个应用场景。其中活动监控是通过可视化技术直观展示活动的实时情况，包含：当前活动的进度，活动的资源、活动的威胁情况、活动的值守情况、活动的各项业务开展情况等信息。应急指挥将活动要素在地图上展示，在发生突发事件时，支持指挥中心“挂图作战”，依据地图展示的资源来对事件的处置。

图 8-13　应急指挥界面

态势感知

态势感知中心提供网络安全威胁可视化的入口，基于平台获取的各类监测数据及日常业务流转产生的业务数据，以网络安全事件与威胁风险监测为驱动，对网络空间安全相关信息进行汇聚融合，从不同视角感知网络安全态势。

态势感知系统以单位数据、资产数据、网络安全事件与威胁风险监测为驱动，基于多维态势可视化技术，对网络空间安全相关信息进行汇聚融合，从不同视角出发感知网络安全态势。

图 8-14　态势感知界面

➢ **工业企业安全合规管理**

工业企业安全合规管理，首先可以服务于参与分类分级工作的主管部门、工业互联网企业和工业互联网安全评估机构等用户，功能覆盖工业互联网企业分类分级工作的全部环节，提供企业定级管理、合规自查、风险评估、安全整改和档案管理等相关功能。其次可满足工业互联网企业网络安全分类分级工作信息化管理要求，将各参与方的工作纳入规范流程中，并做到工作留痕，推进相关工作的规范化、常态化、便捷化。

定级管理

根据《管理指南》要求，工业互联网企业需要开展自主定级工作，主管部门需要定期对工业互联网企业开展抽查，指导企业准确定级，为主管部门更好指导企业准确定级，分类分级业务应用提供定级核查功能，主管部门可对工业互联网企业提交的自主定级信息进核查，并将核查情况反馈给工业互联网企业。同时，针对已定级的企业提供定级清单管理及统计分析功能，主管部门可掌握管辖范围内工业互联网企业定级情况。

图 8-15　定级管理概况界面

安全合规自查

监管部门定期对企业开展合规自查工作，便于落实与自身安全级别相适应的防护措施。提供符合性管理和企业安全自评估功能。

图 8-16　企业合规自查界面

符合性评估任务管理

符合性评估任务管理为监管部门提供对工业企业的在线评估工作，评估内容主要依据《工业互联网企业数据安全防护规范》、《工业互联网平台企业安全防护规范》和《工业互联网标识解析企业安全防护规范》开展对企业的符合性评估工作。

监管部门通过从基础库调用符合性评估模板建立评估任务，可从企业定级清单中先择要评估的对象，根据不同的企业类型和级别对企业进行在线下发评估任务，可选择评估任务的跟踪人，包括监管部门、安全支撑单位；能够对评估任务的保存、下发和删除，以及任务的状态跟踪；能够对符估的任务设置限时完成评估的时间；能够对企业名称、任务跟踪人等进行查询。

企业用户接收到任评任务后，按时间要求进行评估，评估后可自动生成评估报告并提供下载功能，该报告也同时会展示给监管部门提供查看与下载。

安全自评估

安全自评估是提供给企业进行自我评估的方法，自我评估的结果不会上传给监管部门用户，目的是让企业能够通过自评估发现自身存在的问题，做好提前整改的工作。

安全自评估为企业提供自评估模板，企业可根据自身企业类型和等级选择评估模板进行自查，同时提供自评估的进度状态、结果和报告查看与下载功能。

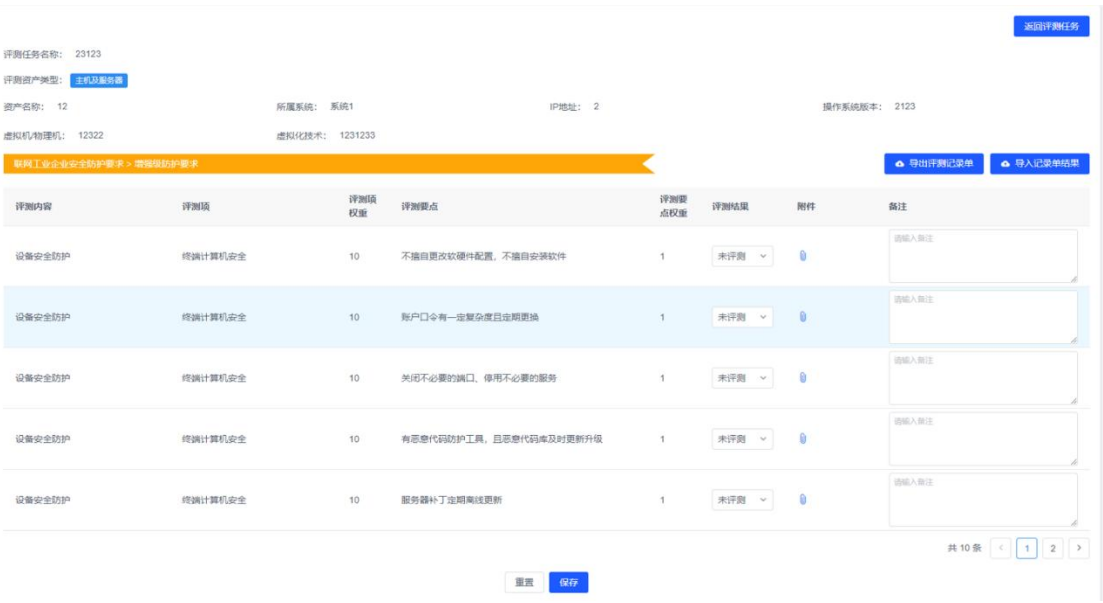


图 8-17　安全自评估界面

风险评估

工业企业应基于工业互联网安全相关标准，定期开展评估评测工作，便于落实与自身安全级别相适应的防护措施。分类分级业务应用提供对企业的安全估计管理，安全评估用于监管部门开展对企业的风险评估与情况上报上给主管部门。

监管部门通过下发安全评估任务，实现对各企业的安全评估工作，安全评估是通过评估对使用的安全评估工具开展对企业的评估工作，当完成评估工作后，可将评估数据上传至平台，监管部门查看报告，如果报告查看不满足安全要求，则要求企业限期整改，同时支持对企业整改工作的跟踪工作。

图 8-18　风险评估界面

安全整改

工业企业根据监管部门安全检查和评估工作过程中发现的重大安全隐患，开展网络安全整改工作，并将安全整改情况报送给主管部门，安全整改报送内容包括整改名称、整改企业、整改依据、整改内容、整改建议和限期整改信息。

主管部门查看各企业报送的网络安全整改信息，了解存在网络安全隐患的企业安全整改工作落实情况并及时跟踪整改进度。

图 8-19　安全整改界面

档案管理

企业档案针对终端、监控、工控、在线业务系统等在线网络资产的资产分布、漏洞和指纹信息进行统一管理，摸清企业资产底数，形成统一的资产立体化监管，形成更加细化的信息系统资产数据：按所属行业、机关横向分类；按所属地域、行政归属横向分类；按工业互联网企业类型、等级纵向分级；按信息系统重要、敏感程度纵向分级；按信息系统脆弱程度、可用程度纵向分级。

以资产管理为核心，以资产数据为基础，与隐患、事件、攻击、情报、单位信息等数据进行深度分析，支撑考核评价、信息共享、安全专项、数据安全监管、APP 监测等核心业务，共同构建指挥驾驶舱。

图 8-20　档案管理界面

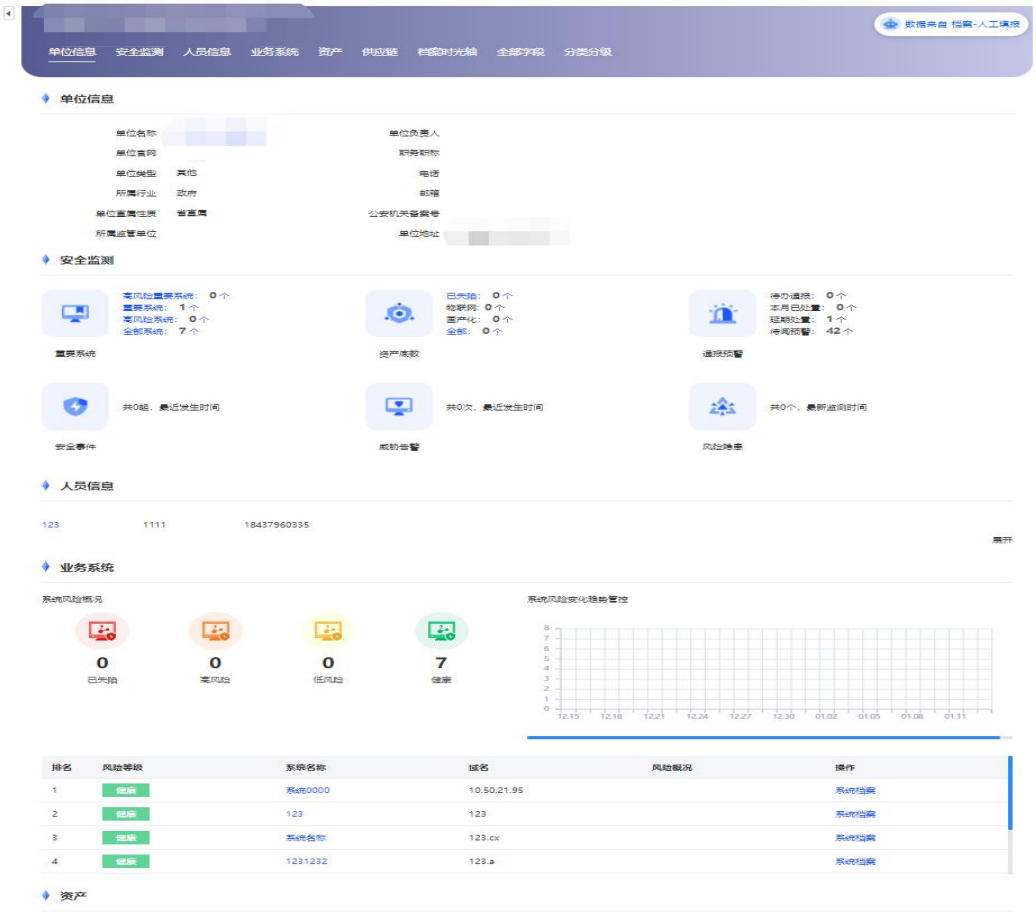


图 8-21　企业安全画像界面

➢ **安全支撑综合服务**

安全支撑综合服务是湖南省工业信息安全公共服务平台的门户，是为工业企业、监管机构、安全厂商提供统一安全服务，主要包括培训服务、检测服务、监控服务、工业云安全服务、工业 APP 安全服务、安全运营服务、安全咨询服务和安全保险服务，同时将监测与态势感知各业应模块、工业企业分类分级各应用模块作为统一的服务入口，提升日常运营效率。

图 8-22　安全支撑综合服务界面

5. 配套管理机制

多级协同安全预警与应急响应管理机制是根据《湖南省工业控制系统信息安全事件应急预案》的相关要求、流程进行设计。提供对安全事件、风险进行及时预警、通报和应急处置的功能。当监测到工业企业存在重大风险隐患，或产生重大安全事件时，通过平台进行通报，被通报的工业企业按期反馈处置结果。平台需具备多种通报方式，包括钉钉、短信和邮件等。在发生严重情况时，可立即通过短信、钉钉等方式进行通报；当系统监测到轻微安全隐患时，可进行预警提醒或限期整改，被通报单位须及时反馈处置结果。

总体应急处置流程为《湖南省工业控制系统信息安全事件应急预案》中的“监测预警和应急处置流程图”，具体流程详见下图所示：

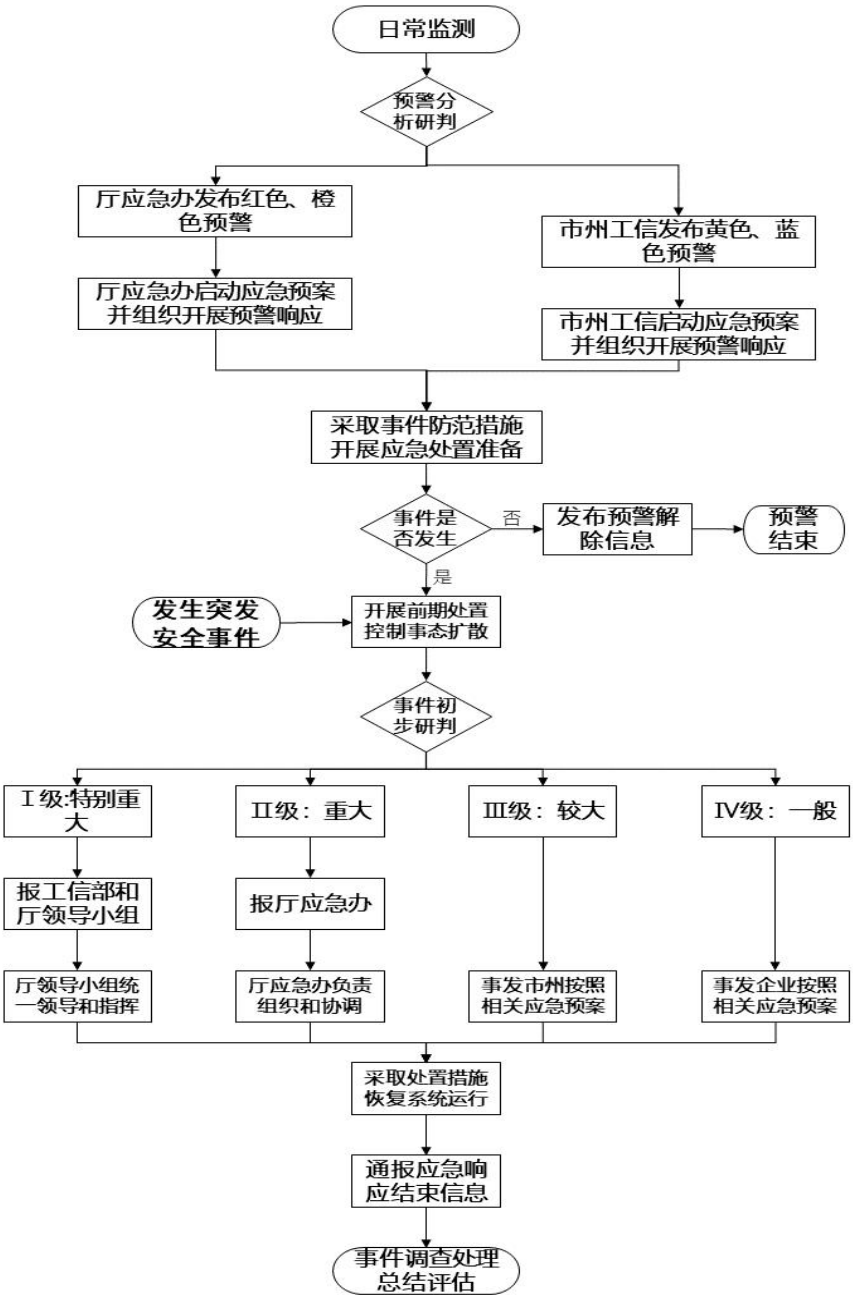


图 8-23　监测预警和应急处置流程图

同时，还根据总体流程，制定了监测预警流程与应急处置响应流程。

如下图所示：

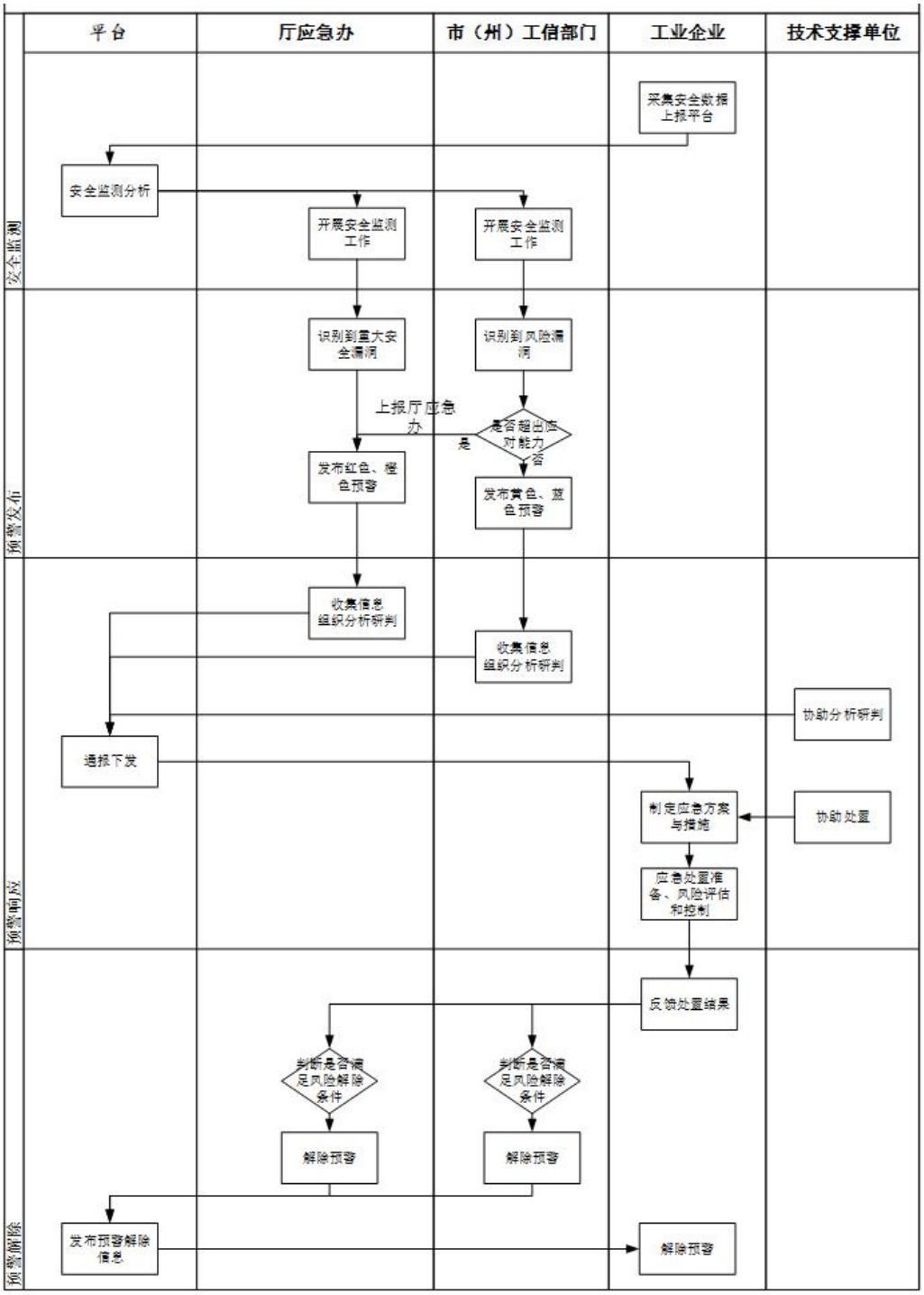


图 8-24　监测预警流程图

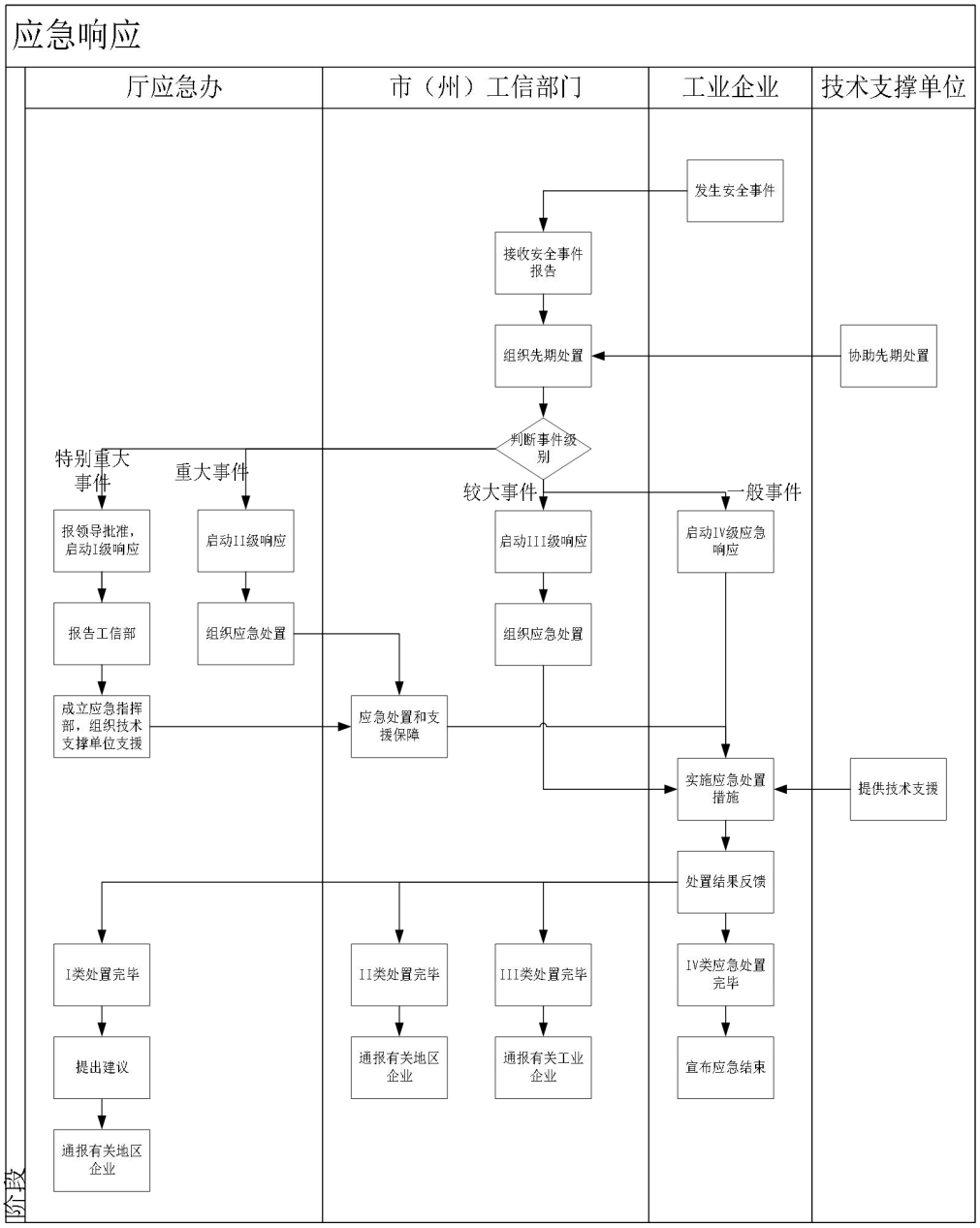


图 8-25　应急响应处置流程图

6.技术升级与动态更新方案

本方案充分考虑未来技术发展，整体平台才有用分层解耦的方式设计，使用模块化、集群化编程思想，整体平台天然具备功能模块扩展能力和系统架构扩展能力，提供了完善的技术升级和动态更新解决方案。

（1）功能模块化扩展

采用 Storm 集群进行实时流数据分析计算，提供方便的可扩展处理能力；采用 Spark 进行高性能的离线处理，利用 Spark 的底层框架作为其执行基础。基于模块动态扩展技术，平台将每个计算、分析功能作为一个功能模块，可以实现模块级别的扩展，比如需要增加一些新的安全分析检测功能，只需将新开发功能按照一定规则和接口动态的纳入到分析计算引擎中，就可以动态的实现分析功能的扩展。

- **实时分析插件模块化技术**

目前主流的传统大数据平台提供 Hadoop 架构对大规模数据的计算进行分解，然后交由众多的计算节点分别完成，再统一汇总计算结果。Hadoop 架构通常的使用方式为批量收集输入数据,批量计算，然后批量吐出计算结果。然而在安全大数据分析的应用场景下，通常对告警的实时性要求较高，需要对海量的原始数据进行实时流式处理和持续处理，Hadoop 架构难以处理实时性要求较高的业务。针对这一难题，安恒采用运行拓扑(topology)的 strom 架构，极大的降低了安全事件的告警延迟。

Storm 集群提供控制节点(master node)和工作节点(worker node)。控制节点上面运行一个叫 Nimbus 后台程序，负责在集群里面分发代码，分配计算任务和监控状态。每一个工作节点上面运行一个 Supervisor 的进程，监听分配给它那台机器的工作，根据需要启动/关闭工作进程 worker，多个工作进程 worker 组成拓扑(topology)。数据流交互如图所示。

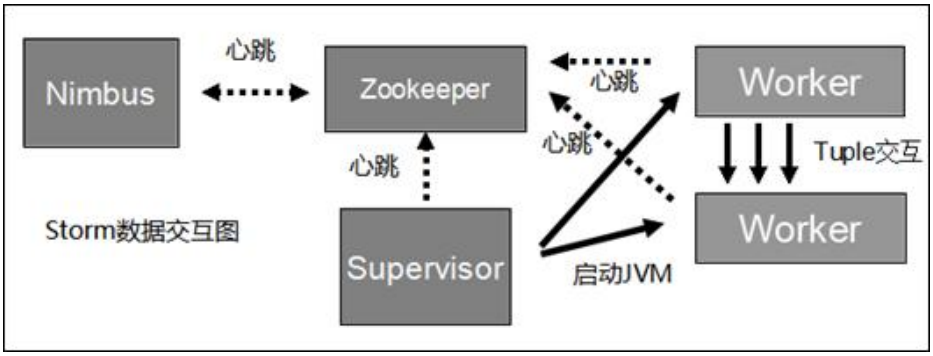


图 8-26　数据交互示意图

工作进程 worker 中每一个 spout/bolt（数据处理单元）的线程称为一个 task（任务），使用 Spout/Bolt 编程模型来对消息进行流式处理。Spout 组件是消息生产者，支持从多种异构数据源读取数据，并发射消息流，Bolt 组件负责接收 Spout 组件发射的信息流，并完成具体的处理逻辑。在复杂的业务逻辑中可以串联多个 Bolt 组件，在每个 Bolt 组件中编写各自不同的功能，从而实现整体的处理逻辑，只需将不同的实时分析数据处理任务按照一定的规则和接口纳入和封装到 Bolt 组件中，就可以动态的实现实时分析功能的模块扩展。

➢ **离线批处理分析模块化技术**

目前在离线数据批处理应用中，主流使用的是基于 Hadoop 架构的 MapReduce 分布式计算框架，在安全事件溯源分析应用场景中，需要关联多维、多源的数据，如日志、流量、漏洞数据以及威胁情报，甚至其他检测模型的分析结果等数据，计算和处理逻辑比较复杂，MapReduce 的 copy 阶段要求每个计算节点从其它所有计算节点上抽取其所需的计算结果，copy 操作需要占用大量的网络带宽，十分耗时，从而造成 Reduce 任务整体计算速度较慢。

在实践过程中使用自主研发的任务调度系统取代 MapReduce 框架，使用 ElasticSearch 集群存储需要进行离线分析的数据，解决 MapReduce 的 copy 阶段的占用大量的网络资源的问题。如图所示，

每个 Job 中含有 1 个或多个 Stage，Stage 一般在获取外部数据和 shuffle 之前产生），然后以 Stage（或者称为 TaskSet）提交给 Task Scheduler，Task Scheduler 负责将 Task 分配到相应的 Worker，最后提交执行，从而从而实现整体的处理逻辑。当有新的离线分析和数据批处理的需求是时，只需将不同的离线批处理分析数据的任务按照一定的规则和接口纳入和封装到 TaskSet 中，然后就可以动态的实现批处理功能的模块扩展。

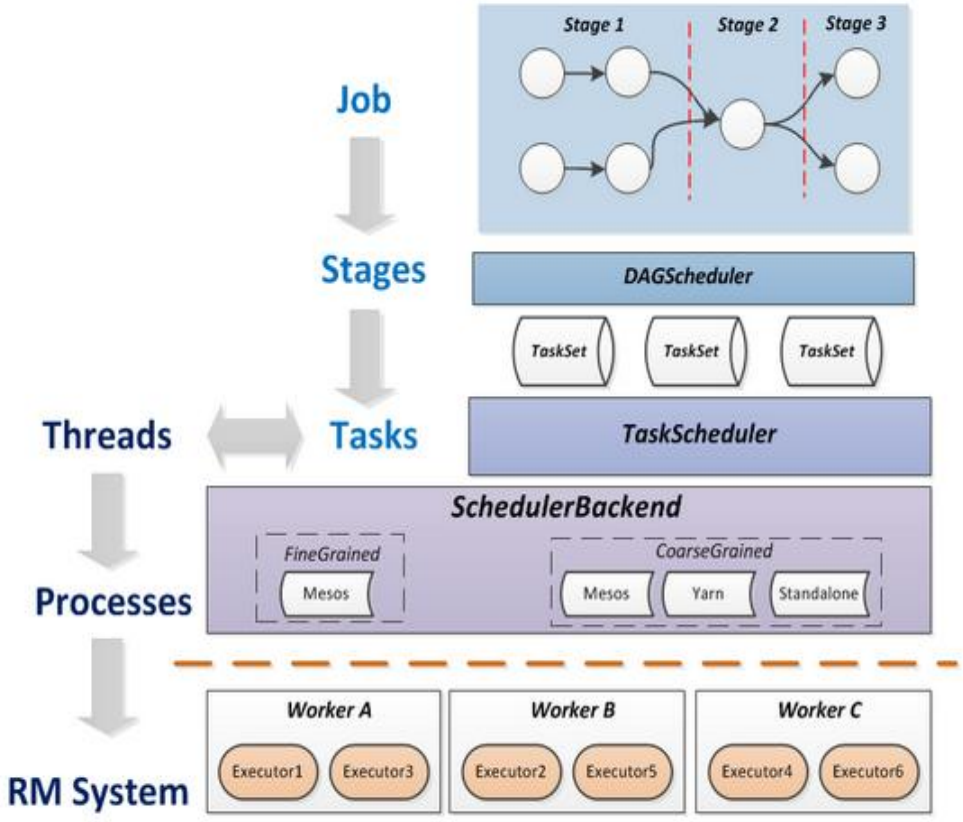


图 8-27　任务调度系统架构示意图

（2）系统架构扩展

系统间通讯的透明化。系统通过采用分布式系统，利于系统的简便易行的分布式部署，同时实现对开发人员的通讯透明，简化了定制开发的难度，确保了系统的可扩展性。

- 系统间模块的耦合性低

通过使用面向消息的中间件作为应用架构的主干有效降低系统间各模块的耦合性，模块直接的接口通用化，能方便的实现各模块接口的重用，便于分块开发、调试和除错。

实现系统的热部署能力。系统可以在运行状态中加入新的组件或者卸除已有组件（非核心组件），整个过程都不影响系统的运行。系统的各重要模块可以运行在不同的进程中，有效的隔离错误。

➢ **灵活的分布式部署**

系统的各模块不仅可以分布在不同的进程中，同时可以透明分布在不同的主机中，以通过分布式计算提供系统的处理能力。无需额外开发，部署成本低。能适应复杂环境下的部署。

当服务器的某中状态崩溃时，状态能够被透明的复制到其它服务器，并支持集成部署到其他的大数据平台。

本系统支持模块集群。横向扩展的系统确保了系统运行的高效性。服务提供和调用的无关性，系统中关联规则、过滤器等都可以资源方式被调用，极大提高的系统的分析能力和数据查询展现效率。

1.1.3 下一步实施计划

为落实工信部印发的《工业互联网企业网络安全分类分级管理指南（试行）》要求，平台以工业互联网企业网络安全分类分级管理为核心，平台在完成建设后，需要湖南省内各地市/州工信局，协同市/州网络安全支撑单位，对工业企业开展工业企业分类分级活动，形成企业清单，以便开展精细化、差异化的安全管理，做到有目标、有计划、有行动的目的，为更好地运用平台，依据平台提供的各类服务能力，安排了如下步骤。

1. 平台发布

完成平台实施搭建，满足三级等保要求；

完成平台对外的域名申请和备案，可以通过互联网侧访问平台；

组织工业企业、各地市/州工信局和安全支撑单位进行平台使用的培训；

平台试运行，组织试点企业、地市工信局和安全支撑单位进行小范围试点；

对外发布通知，平台正式发布。

2.企业分类分级

湖南省厅领域组织湖南省各地市/州工信局依托平台公共服务能力，开始对外公外征集遴选工业企业参与分类分级活动，对参与活动的工业企业开展自主定级和定级审核活动，通过审核的企业最终形成定级清单。

3.企业自评估

根据企业定级清单，平台为联网企业、平台企业和标识解析企业提供在线安全自评估，自评估内容根据平台的不同类和安全级别进行有针对性的评估，同时，平台可委托安全支撑单位协助企业完成安全自评估，企业评估完成后，最终自动生成评估报告，让湖南省厅领域及各地市/州工信局管理人员及时掌握当前企业清单中的合规状况。

4.应急演练

根据《工业互联网企业网络安全分类分级安全管理指南（试行）》要求，三级企业每年必须完成一次应急演练，及时上报预急预案。

省厅领导组织各地市州管理人员依托平台 SaaS 化攻防演练平台和协同应急模块，开展三级企业的应急演练，及时汇总企业演练情况，总结演练结果，给出合理化的安全防护建议。

5.安全整改

工业企业在完成安全评估与应急演练后，通过经验总结，发现自

身安全防护问题，企业结合自身安全现状，输出安全整改方案，并提交所属辖区工信局进行审核，工信局可委托安全支撑机构进行技术审核，以确定该整改方案的技术合理性，待审核通过后，企业可根据方案内容开展整改建设工作。支持对整改建设企业的审核状态进行统计分析。

6.验收检查

工业企业完成整改建设后，向所属辖区工信局提交整改落实情况报告，工信局审核通过后提交省级监管单位进行复审，省级监管单位可依据实际情况委托安全专家对整改内容进行技术复审，同时支持对验收检查审核状态进行统计分析。

安全专家可通过工控安全检查工具箱开展对企业的现场检查，并输出报告，同时可将安全检查数据内容作为输入对企业进行专业化的风险评估工作，以便掌握企业安全整改后的真实防护情况。在企业通过安全专家的复审后，省级监管单位可发布验收成果，对于整改效果好的企业进行鼓励。

7.重点企业监测

在完成以上六大步聚后，省厅及各地市州主管部门可清晰地掌握辖区范围内工业企业的类别、安全等级、合规现状、整改情况，能够有效针别哪些企业需要重点监测。

对于要重点监测的企业，部署监测设备，以便能够实时掌握安全现状，及时协同地方工信局和安全支撑单位共同帮助企业完成安全监测预警工作，形成闭环管理能力。

8.完善服务能力

依据湖南省内当前现状，组建各地工信局管理人员和安全支撑机构，完善当前平台安全支撑服务资源，以便进一步提升省内工业企业

的安全监测预警、安全防护与响应处置能力。

本方案计划今年要完成前六大步骤，形成全省范围内的定级清单，并针对这些企业开展安全评估、应急演练、安全整改和验收检查等工作，掌握清单中工业企业的安全合规现状，为开展后续对重点企业开展监测预警与协同应急奠定基础。

1.1.4 方案创新点和实施效果

1. 方案先进性及创新点

（1）集约化、数字化和服务化的公共服务技术创新

我国工业企业当前产业规模，技术实力参差不齐，尤其是在面对中小工业企业，这些企业的安全防护能力有限，有的在安全防护方面甚至处于“裸奔”状态，这些企业没有能力，也没有意识去解决其内部的安全隐患与风险问题。

建设省/市等区域级工业互联网安全综合服务平台，利用平台的“双向赋能”的服务特点，建立集约化安全支撑服务资源队伍，同时面向监管部门和企业用户提供“一站式”SaaS 化安全服务，帮助监管部门提高日常安全监测预警、研判分析能力，以及响应处置效率；帮助工业企业提高安全防护意识，显著提高安全防护水平。间接降低辖区内安全监管部门的管理成本。同时，利用平台制定对安全服务供应商和工业企业的考核规则，通过定期考核，使两者不断优化安全服务能力与安全防护能力，形成良好的生态体系。

图 8-28　省/市等区域级工业互联网安全综合服务平台“一站式”服务业务运行流程

（2）工业互联网场景的安全数据采集与融合分析技术创新

工业互联网场景具有网络结构复杂、业务系统和设备类型多的特点，因此需要具备可更多应用场景的安全数据采集能力，以及大数据智能分析能力。

数据采集能力：实现工业互联网全场景的数据采集能力，通过在设备、控制、网络、数据、平台、应用的安全数据采集，覆盖联网工业企业、工业互联网平台企业和标识解析企业在 5G、标识、平台、物联网、工控网、信息网、工业云、边缘计算等全场景应用。

大数据智能分析能力：将工业互联网场景下的 IT、OT、CT 和 DT 数据进行集中采集，对这些场景下的用户、系统、设备、网络和操作行为融合在一起进行分析，将各场景可能发生的安全现象进行总结分析，形成工业互联网专有的威胁分析模型，同时可根据用户实际业务场景自定义模型，更贴合用户业务，为安全生产提供稳定、可靠的威胁发现与分析能力。满足工业互联网安全在各场景的安全分析与追踪溯源能力。

（3）基于闭环安全管理机制的多级协同响应处置技术创新

近两年，工业和信息化部相继发布了《工业互联网创新发展行动计划 2021-2023》以及《工业互联网企业网络安全分类分级管理指南（试行）》，均强调了要建立健全工业互联网监测预警的闭环管理机制。

首先，当前工业信息安全监测预警技术体系并不完善，绝大部分只包含了安全监测和安全预警的能力，并没有包含通过研判分析进行调查取证，无法有效核实监测的安全事件或风险隐患的真实性，直接或间接造成在进行安全预警和信息通报的误报率。其次，当辖区内发生不同安全级别的事件后，监管部门也不能通过技术手段，开展省、市和企业级的应急响应与协同处置能力，导致相关信息不能同步，或延迟同步，提高了应急过程中最初的关键时间。最后，大部分监测预警技术体系并没有实现完善的闭环管理机制，并没有形成数字化安全闭环管理模式，发现相关事件或问题由谁负责，谁来跟踪，谁来决定该事件是否需要关闭，以及全部过程是否有操作行业记录进行跟踪。

基于以上的难点与问题，湖南省工业互联网安全综合服务平台的监测预警与协同响应业务应用以数字化安全服务底座为基础，具备了安全事件和风险隐患的实时发现能力，并提供了多种元数据的安全研判分析工具，为安全分析人员提供详细的调查取证工具，从而进行高效、精准备的安全预警与信息通报。当发现不同安全级别的事件或风险隐患时，可启动不同的响应流程，将省、市、工业企业和安全支撑机构开展联合协同响应，有效提高了应急响应与处置效率。

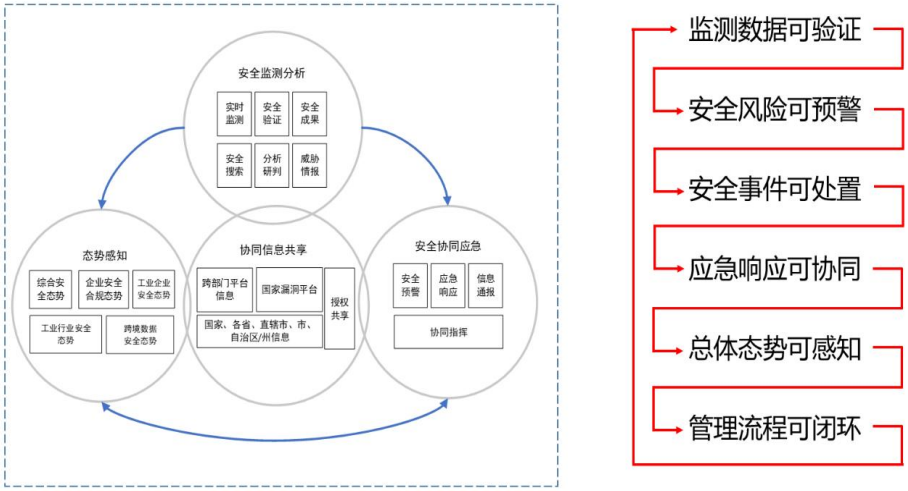


图 8-29　多级协同响应处置技术业务逻辑图

同时，应用中的协同指挥工具实现“挂图作战”的多级协同应急能力，可在重大安全事件或安全活动保障过程中组织省、市、工业企业和安全支撑机构的工作协同，也可以通过该应用组织各级单位进行安全应急演练，提升各级的协同作战能力，一旦发现相关事件，可立即采集相关行动，达到快速响应处置的目的。

图 8-30　协同指挥作战图

（4）数字化工业企业安全合规管理技术创新

2020 年 12 月，工业和信息化部印发了《关于工业互联网企业网络安全分类分级管理试点工作的通知》（以下简称《通知》），省/市等

区域级是15个省级部门开展分类分级的管理试点工作的其中之一，《通知》中要求省/市等区域级的16个工业企业单位参与本次管理试点工作。

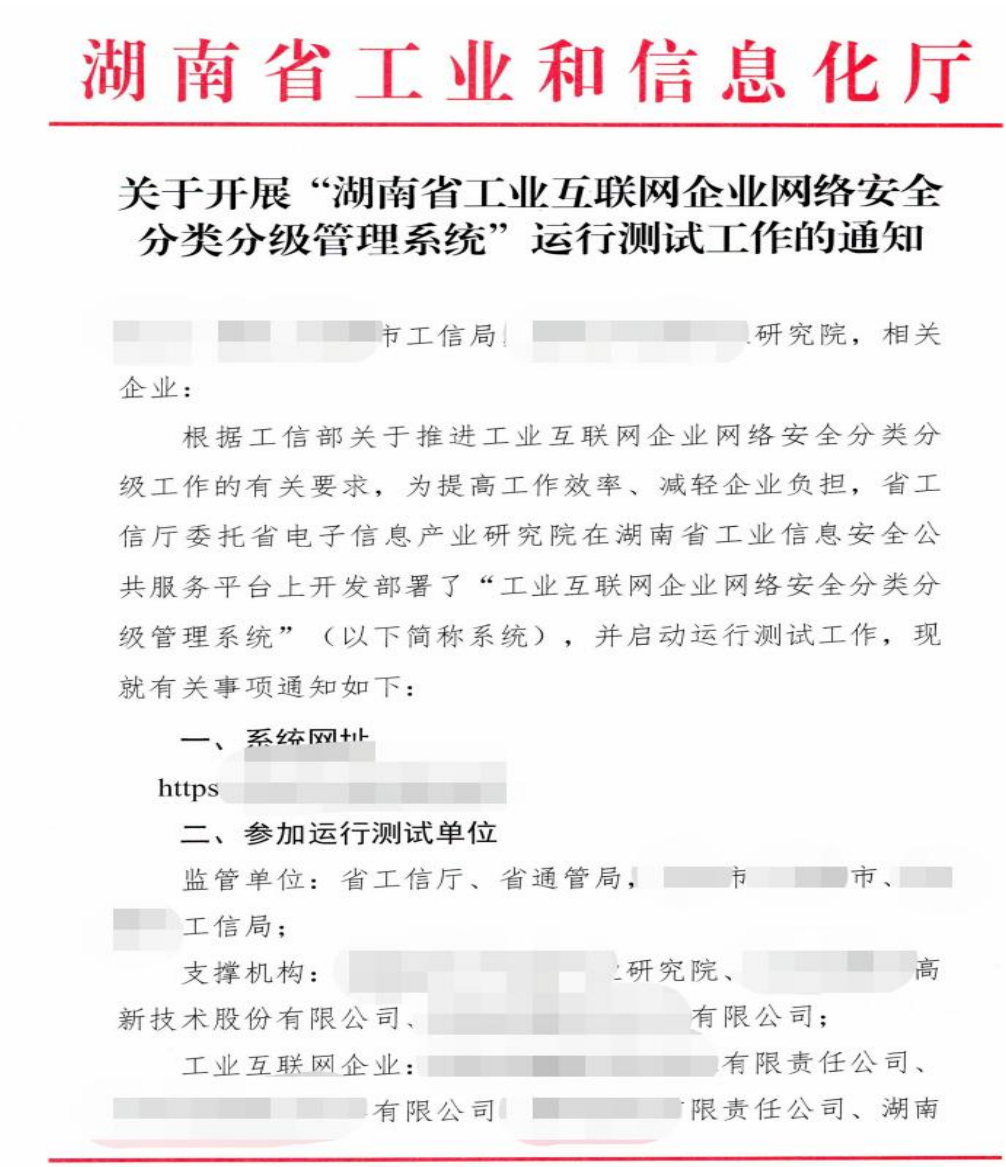
省/市等区域级厅面临的主要问题是，没有形成体系化、流程化、数字化的工业互联网企业网络安全分类分级的技术实现工具，虽然本次试点单位不多，但面对未来大量的工业企业将接入其中，将给监管部门用户带来更多的安全合规管理工作事项。

基于以上的难点与问题，湖南省工业互联网安全综合服务平台的工业企业安全合规管理业务应用，结合安全监管主管部门、工业企业主管部门和安全支撑机构三大用户角色，以及“定级管理、合规自查、风险评估、安全整改和档案管理”五大流程化管理应用，帮助监管部门实现了工业企业数字化、流程化的安全合规闭环管理机制，形成了对工业企业的精细化和差异化的安全合规管理模式。

2.实施效果

根据“下一步实施计划”章节，当前平台已完成前两个步聚，实施效果如下：

平台完成实施，确保达到等保三级防护水平，并发通知组织平台的试运行，见下图所示：



湖南省工业和信息化厅

关于开展“湖南省工业互联网企业网络安全分类分级管理系统”运行测试工作的通知

市工信局 研究院，相关企业：

根据工信部关于推进工业互联网企业网络安全分类分级工作的有关要求，为提高工作效率、减轻企业负担，省工信厅委托省电子信息产业研究院在湖南省工业信息安全公共服务平台上开发部署了“工业互联网企业网络安全分类分级管理系统”（以下简称系统），并启动运行测试工作，现就有关事项通知如下：

一、系统网址

https

二、参加运行测试单位

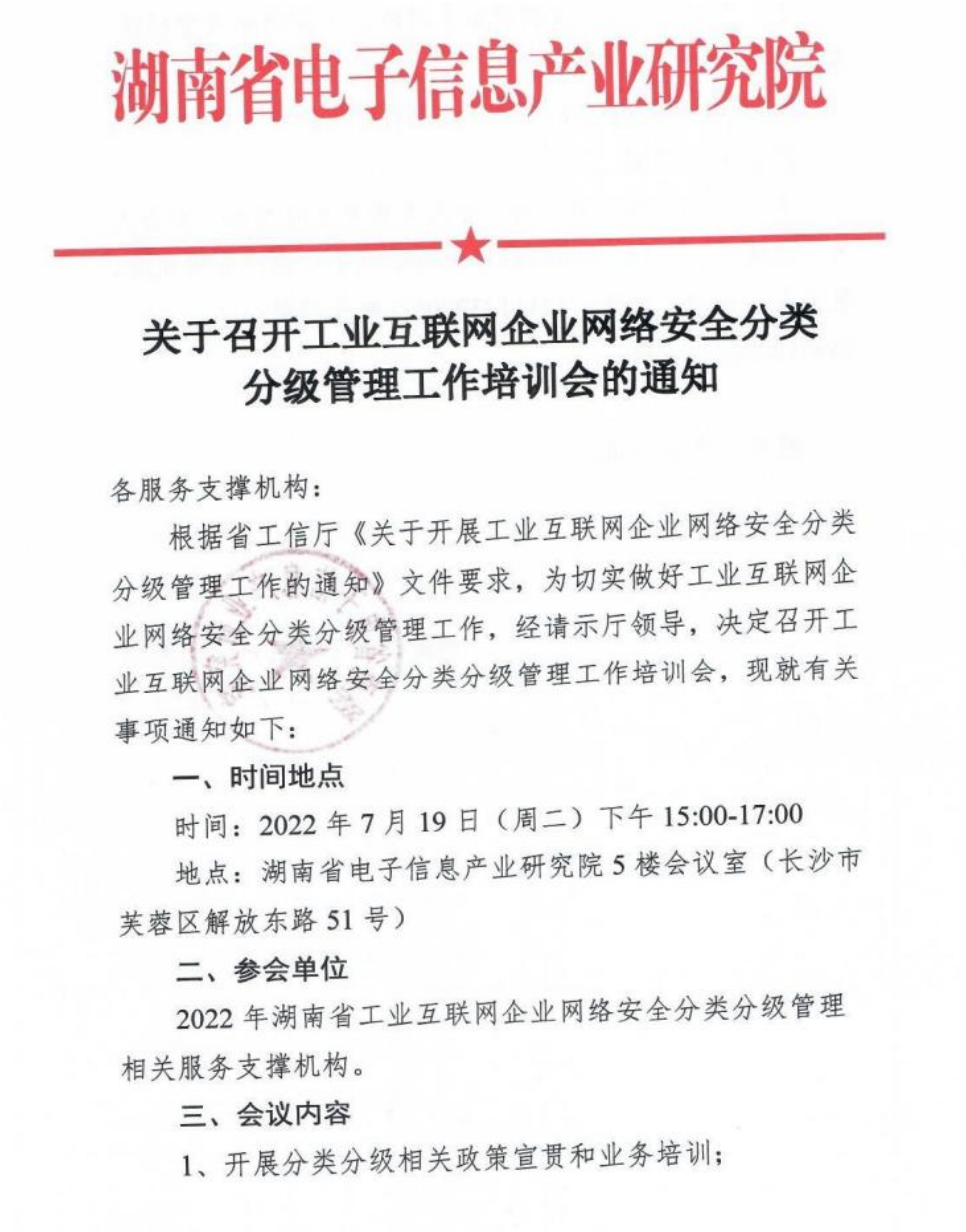
监管单位：省工信厅、省通管局， 市 市、 工信局；

支撑机构： 研究院、 高新技术股份有限公司、 有限公司；

工业互联网企业： 有限责任公司、 有限公司 限责任公司、湖南

图 8-31　平台试运行通知

湖南省电子信息产业研究院作为省级安全技术单位，组织开展平台使用的培训工作，见下图：



湖南省电子信息产业研究院

关于召开工业互联网企业网络安全分类分级管理工作培训会的通知

各服务支撑机构：

根据省工信厅《关于开展工业互联网企业网络安全分类分级管理工作的通知》文件要求，为切实做好工业互联网企业网络安全分类分级管理工作，经请示厅领导，决定召开工业互联网企业网络安全分类分级管理工作培训会，现就有关事项通知如下：

一、时间地点

时间：2022 年 7 月 19 日（周二）下午 15:00-17:00

地点：湖南省电子信息产业研究院 5 楼会议室（长沙市芙蓉区解放东路 51 号）

二、参会单位

2022 年湖南省工业互联网企业网络安全分类分级管理相关服务支撑机构。

三、会议内容

1、开展分类分级相关政策宣贯和业务培训；

图 8-32　组织召开平台培训通知

经过对试点企业的测试，以及完成平台的培训工作后，由湖南省工信厅和省通管局联合举办的湖南工业互联网安全深度行活动中，正式发布了平台，见下图：

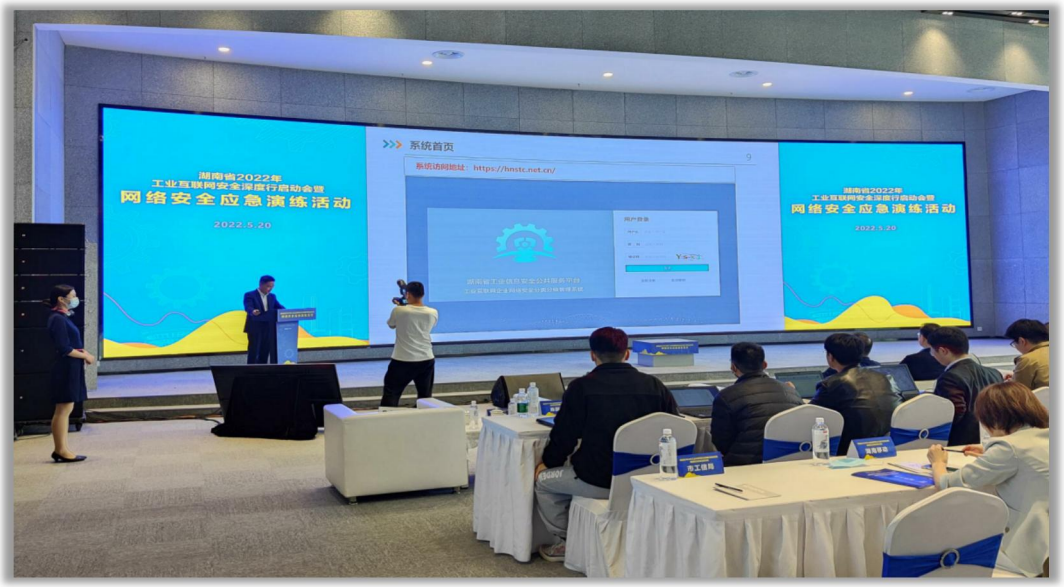


图 8-33　湖南省工业互联网安全深度行-平台发布现场图

在本次深度行活动中，为省内优秀工业领域网络和数据安全支撑机构颁发证书，如下图所示：

图 8-34　办法工业领域网络和数据安全支撑机构证书

湖南省工信厅在官网发布开展工业互联网企业网络安全分类分级管理工作的通知，征集省内各地方工业企业开展相关工作，见下图：

关于开展工业互联网企业网络安全分类分级管理工作的通知

湖南省工业和信息化厅 gxt.hunan.gov.cn　时间：2022年06月20日 16:05　【字体：大 中 小】

各市州工信局，有关单位：

为进一步加强工业互联网网络安全管理，提升工业互联网企业网络安全水平，根据工信部等十部委《加强工业互联网安全工作的指导意见》（工信部联网安〔2019〕168号）和《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）等文件精神，省工信厅、省通管局决定在全省范围内组织开展工业互联网企业网络安全分类分级管理工作（以下简称“分类分级工作”）。现就有关事项通知如下。

一、工作目标

打造“湖南省工业互联网企业网络安全分类分级管理服务平台”，在省内10个以上重点行业100家左右工业互联网企业实施分类分级，帮助解决1000个以上工业互联网安全问题。到2022年底，全省工业互联网企业安全责任意识全面增强，安全保障体系基本构建，安全从业人员大幅增长，安全管理水平和防护能力显著改善，安全事故发生率持续降低，网络安全产业快速发展。

全省工业互联网企业包括应用工业互联网企业（简称联网工业企业）、工业互联网平台企业（简称平台企业）和标识解析企业，均应实施分类分级。现结合各地工业互联网发展基础并参照省委考核办印发的《2022年度市州绩效考核实施细则》的通知（湘考办发〔2022〕3号）有关规定，将14个市州分为A、B、C三类。其中，A类地区为长沙市、衡阳市、株洲市、湘潭市、岳阳市、常德市、郴州市、娄底市8个市，B类地区为邵阳市、益阳市、永州市3个市，C类地区为张家界市、怀化市、湘西自治州3个市州。2022年各市州参加分类分级工作企业数量，A类地区不少于8家，其中长沙不少于25家；B类地区不少于5家；C类地区不少于3家。

二、职责分工

省级组织及监管单位：省工信厅和省通管局负责建立框架合作协议，全面领导和组织全省分类分级工作。

地区监管单位：市州工信局负责本行政区内分类分级工作，制订分类分级目录，指导督促工业互联网企业完成自主定级、安全评估、落实安全防护要求和参加应急演练，组织对工业互联网企业开展定级核查和安全评估检查。

工业互联网企业**（联网工业企业、平台企业、标识解析企业）**：履行工业互联网安全管理主体责任，按照有关规定开展自主定级、安全评估、安全整改、应急保障等工作，落实安全防护规范要求，保障工业互联网安全稳定运行。

支撑机构**（湖南省电子信息产业研究院及相关安全技术服务机构）**：湖南省电子信息产业研究院为分类分级工作支撑机构，在监管单位领导下，开展分类分级政策宣贯、业务培训，组织安全技术服务机构为工业互联网企业自主定级、安全评估、安全整改等工作提供义务技术指导，组织评估评测机构开展定级核查、评估检查和安全整改验收，研究制订分类分级标准规范和政策制度。

图 8-35　湖南省工信厅开展分类分解管理工作的通知

平台于 2022 年 10 月 22 日完成省内工业企业的定级工作，并对外公布，目前正处于安全自评估阶段，见下图：

关于公布2022年湖南省工业互联网网络安全分类分级管理企业名单的通知

湖南省工业和信息化厅 gxt.hunan.gov.cn　时间：2022年10月21日 10:37　【字体：大 中 小】

湘工信信软〔2022〕499号

各市州工信局：

根据省工信厅、省通管局《关于开展工业互联网企业网络安全分类分级管理工作的通知》和《湖南省工业和信息化厅关于印发<2022年真抓实干督查激励措施实施办法>的通知》（湘工信办〔2022〕220号）等文件精神，经企业申报、市州工信局推荐、省工信厅会同省通管局审核，明确123家企业纳入2022年湖南省工业互联网网络安全分类分级管理工作，现将名单予以公布。

各地要加强工作组织，督导工作进度，推动工作落实，确保11月底前完成各项工作任务。验收合格的企业数量将作为2022年真抓实干督查激励措施考核的依据。

附件：2022年湖南省工业互联网网络安全分类分级管理企业名单

湖南省工业和信息化厅

2022年10月20日

附件

2022年湖南省工业互联网网络安全

分类分级管理企业名单

形成工业企业定级清单，是对不同类型和安全级别的工业企业开展“精细化、差异化”安全管理措施。

平台可为各工业企业提供在线安全自评估服务，评估内容以《工

业互联网企业网络安全分类分级防护系列规范》和《湖南省工业互联网企业网络安全分类分级管理评估指标体系》为依据，为了保障企业能够顺利完成评估，平台提供委托安全支撑机构提供远程或现场评估服务，下图为在线安全评估图：

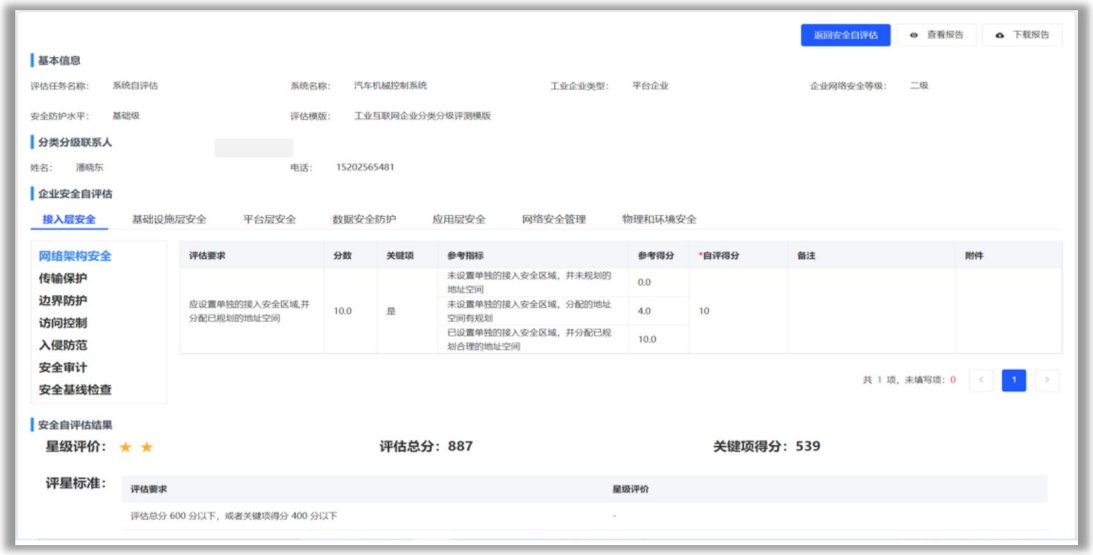


图 8-36 在线安全评估图

当完成在线安全评估，为了进一步掌握工业企业安全现状，现委托安全支撑机构技术人员对工业企业进行现场检查，通过工控安全检查工具箱，识别企业风险隐患，并生成安全检查分析报告上传至平台，地方主管部门根据情况对部分存在安全风险的企业开展安全整改工作，并督导其在限期时间内完成整改。安全整改提供流程化管理方式，如下图：

图 8-37　安全整改图

平台可对重点工业企业开展安全监测，实时掌握企业安全现状，提供一系列闭环管理工具，当发现相关问题时，需要实时发现问题-安全验证-通报预警，才可对相关事件进行发布，所有动作均提供流程化处理方式，全程留痕，实时如下图所示：

图 8-38　实时监测界面

图 8-39　分析研判界面

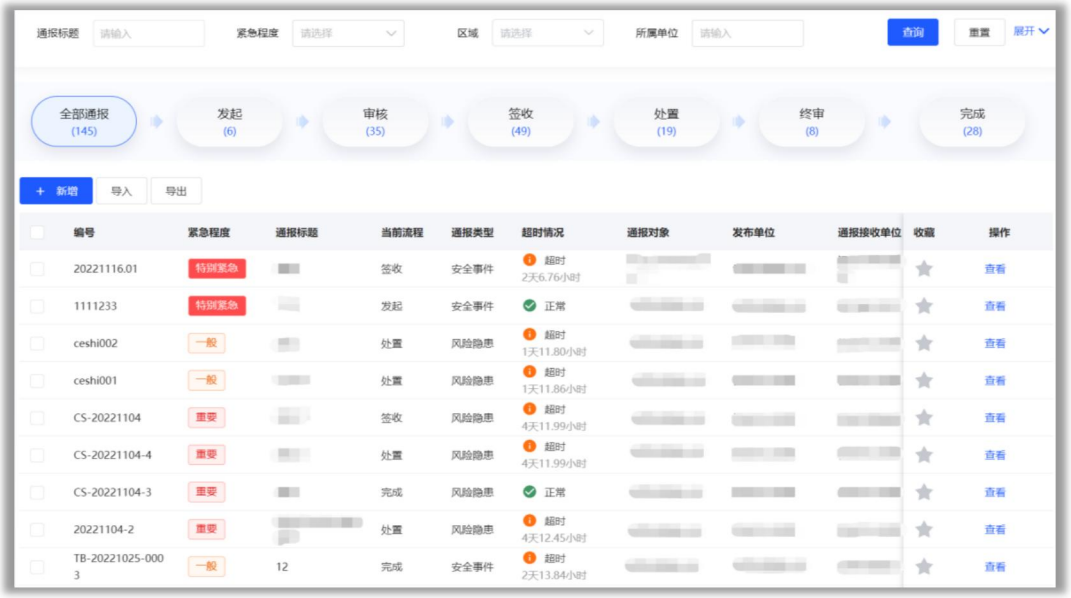


图 8-40　通报预警界面

当发生重大安全事件时，根据湖南省应急要求，需要由省级应急办协同地方人员一起进行响应急，需要组织事件发生地应急相关人员、安全支撑机构人员和行业领域安全专家共同解决问题，如下图所示：

图 8-41　协同应急指挥界面

平台为各级部门主管人员提供工业企业全息数字档案，将企业基本信息、资产信息、定级信息、安全评估信息、安全整改信息、风险隐患信息和安全事件等数据进行有效整理，以安全监管者为视角，提供卡片式，报告式的界面，让安全监管人员通过一张卡片，一页报告掌握工业企业的全面现状，为安全趋势预判提供有效数据支撑。下图为企业数字档案界面：

图 8-42　企业数字档案界面

1.1.5　单位基本信息

1.牵头单位基本信息

本次方案申报的牵头单位是**中国联合网络通信有限公司研究院**（简称中国联通研究院）。

中国联通研究院作为联通集团科技创新的主体，立足国家战略、公司战略和产业服务，成为公司战略决策的参谋者、公司技术发展的引领者、产业发展的助推者。内设一个综合支撑板块和智库研究、网络研究、应用技术研究三个技术研究板块，具备智库的专业咨询能力、网络技术的自主核心能力、前瞻技术的研究能力、技术与业务融合的应用能力。现有员工近700多人，平均年龄36岁，享受国务院政府特殊津贴专家10名、教授级高工26名、博士后9名、博士62名、硕士占比75%以上。

2.参与单位基本信息

本次方案申报的参与单位是**杭州安恒信息技术股份有限公司**（简称安恒信息）。

安恒信息主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务，制定了云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大市场战略。安恒信息凭借强大的研发实力和持续的产品创新，入选Gartner 《2020年中国ICT技术成熟度曲线》，成为中国云安全“标杆供应商”；AiLPHA大数据智能安全平台荣获2019“世界人工智能产业安全十大创新实践”；荣获首个全球工业互联网大奖——“湛卢奖”等。