1.1 案例九：面向工业互联网领域的集约化安全运营解决方案——全面可靠的系统化解决方案

1.1.1 方案概述

中国移动通信集团有限公司信息安全管理与运行中心（以下简称“中国移动信安中心”）在安徽开展试点，联合中国移动通信集团安徽有限公司打造面向工业互联网安全纵深防御的安全运营解决方案，面向工业互联网、能源、电力等垂直行业开展集约化安全运营服务，可从整体上提升工业互联网系统内的安全保障能力，切实保障国家工业互联网安全。在新时期、新形势下，保障航空、纺织、家电、矿山、港口等国民经济重点领域网络安全，有助于提升行业内应对愈加复杂的网络安全形势，促进集约化安全运营中心模式的发展，加快我国集约化安全运营中心建设，抵御国内国外不断增强的网络攻击态势，保证工业互联网领域内企业的业务稳定，为国家网络安全保驾护航。

1. 方案背景

（1）网络安全形势日益严峻

当前，我国工业互联网领域的网络安全形势异常严峻，复杂的网络空间政治战、舆论战、信息战和技术战日趋激烈、公开化。政府网站及金融、能源、电力、通信、交通等领域关键信息基础设施已经成为网络攻击的重点目标。

全球领先安全厂商 Check Point《网络攻击趋势：2022 年年中报告》，全球网络攻击激增 42%，勒索软件成为头号威胁。国际知名公司 NETSCOUT《威胁情报报告》，2022 年上半年，全球共发生 6,019,888 起 DDoS 攻击。CNCERT《2022 年互联网安全报告》，我国境内直接暴露在互联网上的工控设备和系统存在高危漏洞隐患占比

仍然较高。20%的能源、轨道交通等关键信息基础设施生产管理系统存在高危安全漏洞。CNVD 平台全年新增收录通用软硬件漏洞数量创历史新高，达 20,704 个，同比增长 279%，近五年来新增收录漏洞数量呈显著增长态势，年均增长率为 176%。综上所述，全球网络安全形势日益严峻，安全风险不断提高。

（2）网络安全工作要求不断提高

习近平总书记在全国网络安全和信息化工作会议上提出：没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。

从小安全到大安全、从安全风险检测到安全手段建设、从监控防守到攻防实战，从网络安全到数据安全、从关基到车/物联网。国家和行业对工业互联网领域的网络安全要求在不断提高、范围在不断拓展、管控在不断增强。对网络安全从业人员的要求也在不断加深，不仅仅要做到防的住，还要攻得出。

（3）网络安全工作亟需调整

随着网络安全形势日益严峻和内外部对网络安全工作要求不断提高，网络安全的工作范围也在不断扩大。传统的“信息孤岛”、“各自为战”的工作模式，安全风险监控与风险处理协同欠佳，无法实现全生命周期管理和处置。传统工业互联网的网络安全运营模式碎片化严重，服务方式和流程标准不一，造成安全防护机制臃肿，应急响应不够及时。以上问题导致防护力度保障不高、安全事件频出等诸多问题存在。在一些工业互联网企业内，许多已经建设好的安全防护资源处于边缘化的境地，这样的结果是：基础通信设施安全岌岌可危，直

接威胁国家安全，广大人民群众利益也难以得到保障，改变迫在眉睫！

2. 方案简介

本方案为进一步提升工业互联网领域的安全应急响应、安全运营能力，致力打造集约化安全运营中心，开展工业互联网企业集中的安全应急响应与运营工作。从流程优化、手段完善、人员培养等方面入手，重点提升企业网络安全技术能力和实战能力。

3. 方案目标

（1）网络安全运营的统筹

统筹和加强工业互联网企业暴露面资产的安全风险管理，建立多级联动应急保障与响应体系。

（2）数智化发展的护航

推进工业互联网企业的安全防护从分散、点状向集中、体系化转变，组织开展网络条线基础设施安全防护。

（3）安全能力的创新

构建部署企业上下多级的实战化防护能力，实现防护能力随“算网”而动，研究推动多种新兴技术比如：零信任、SOAR、内生安全等尽快落地。

构建常态化安全集中运营能力，实现重要网络安全事件的集中监测、集中运营、集中处置；统筹安全保障，建立多级联动应急保障体系；在实战攻防、手段建设和安全赋能方面积极探索创新，为企业的数智化发展护航。

1.1.2 方案实施概况

中国移动信安中心围绕“机制、能力、队伍、管理、底线”，从三方面构建集中高效的网络安全运营机制，从三方面提升智能敏捷的安全技术能力，培育一支攻守兼备的实战化专家队伍。强化全企业集

中安全运营，强化极限风险系统应对、深化分类协同运营机制、提升标准化引领与科技创新实力、打造统一安全服务产品、提高攻防一体实战对抗能力，统筹安全保障，形成多级联动的安全对抗能力。

1. 方案总体架构和主要内容

（1）整体框架设计

中国移动信安中心以多年安全领域沉淀为基础，通过统一标准体系、统一技术平台、统一安全防护、统一风险监控、统一运维监管、集中人才培养，多措并举，融合安全资源、统一支撑服务，建立安全可信的集约化安全运营平台，具有较强的创新性和示范性，为全国工业互联网集约化安全运营中心的建立贡献“安徽方案”。

整体运营机制如图所示：

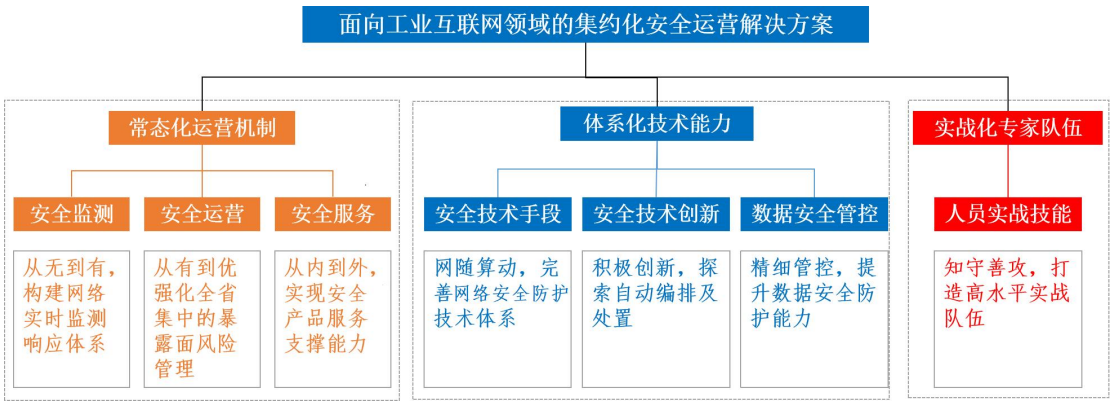

图 9-1　集约化安全中心运营解决方案

➢ 内部运作：

中国移动信安中心打造的集约化安全运营中心，面向工业互联网端到端，对内统一负责企业内各部门的全部安全工作，并积极落实基础安全运维、数据安全管控、安全手段运营、安全攻防团队的建设等工作，落实国家和工业互联网领域的工作要求，构建常态化安全集中运营能力。总体发展下面两方面的内容。

强化基础安全运营：具备安全资产、安全威胁管控能力，重点强化安全资产梳理、暴露面收紧等工作。实现安全事件全流程调度、快

速处置和闭环管理，开展安全系统运维、漏洞扫描、合规审计和态势分析等基础运营工作。

强化手段能力建设：落实构建集约化安全运营中心网络安全防护能力的改造落地，构建多级的实战化防护能力，实现防护能力随“算网”而动。夯实安全漏洞、安全事件等基础性安全防护处置，研究推动各种安全新技术尽快落地。

➢ 外部协同：

对标工信部远程检测要求，对新发现的软硬件漏洞进行处置，建立企业上下多级联动应急保障与响应体系。

打造面向工业互联网企业暴露面资产风险的集中发现、及时预警与跟踪闭环机制。实现重要网络安全事件的集中监测、集中运营、集中处置。

2. 网络、平台或安全互联架构

（1）打造企业集约化安全运营中心解决方案

没有规矩，不成方圆。中国移动信安中心致力打造一个全面、有效、快速反应的集约化安全运营中心。通过中国移动通信集团整体规划，在企业安全应急响应、安全运营能力两方面上建设打造安全运营中心，开展企业集中的安全应急响应与运营工作。从流程优化、手段完善、人员培养等方面入手，重点提升网络安全技术能力和实战能力。

图 9-2　总体网络安全运行体系

（2）梳理整合企业安全系统总体工作

知己知彼，百战不殆。面向工业互联网领域，深入挖掘、梳理并整合企业内安全系统的所有工作，纳入集约化安全运营中心，做到规范流程、统一编排、集中处理。对上落实上级单位考核要求，大力积极推进企业安全运维系统的落成。在建设集约化安全运营中心时，根据企业内安全工作需求，针对性的建设安全管控、日志留存等重要安全运维系统，整合梳理网络攻击、安全防护等方面 9 类 53 项工作。在工业互联网领域内真正打造出一个内外兼修的高效集约化安全运营中心工作体系。

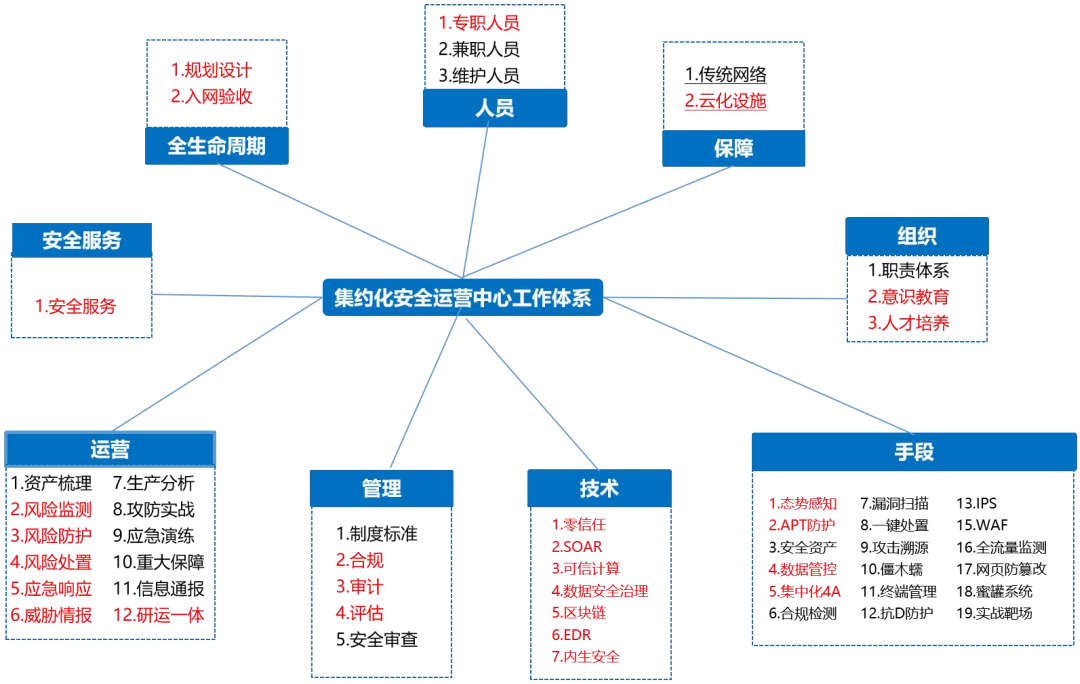

图 9-3　集约化安全运营中心工作体系

（3）加强安全资产管理

千里之堤，毁于蚁穴。面对愈发严重的网络攻击态势，即使只有一个安全资产的遗漏都会迅速打碎企业努力构建的防护罩。通过多举措夯实安全资产管理，一是已知资产的收集、梳理、上报，二是未知资产的扫描、对比、发现，尽力实现全条线安全资产全覆盖。

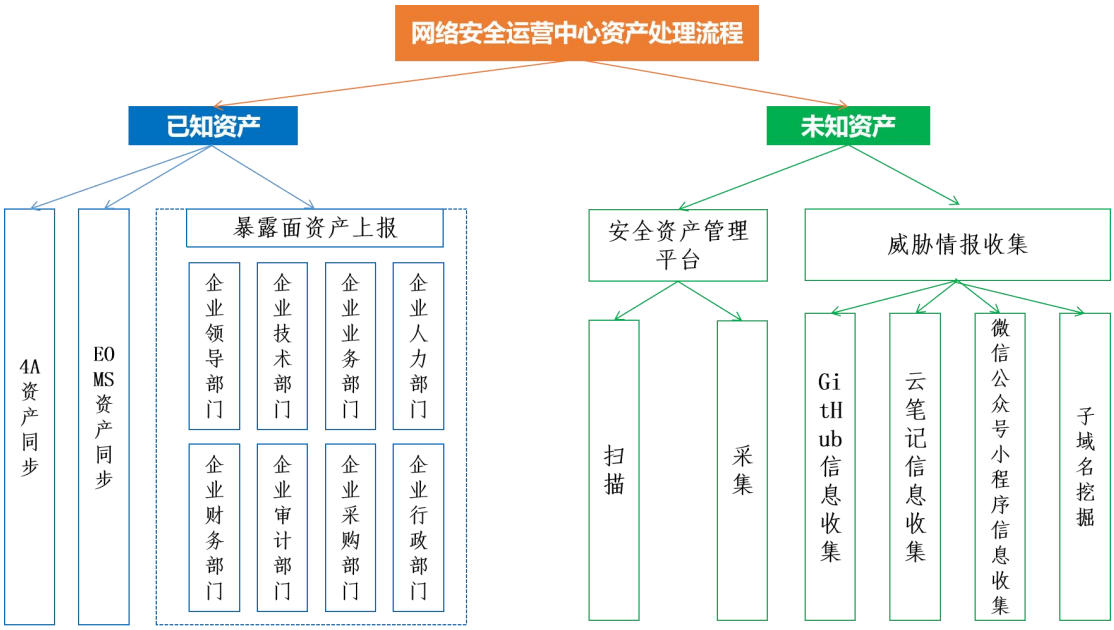

图 9-4　安全资产管理

3.具体应用场景和安全应用模式

（1）建立实时监测响应体系

聚焦快、准、清，开展实时安全监测，实现统一调度，安全事件从分散、点状监测到建立体系化的实时监测体系，推动千万级攻击从按天级“粗”分析到分钟级“精”处理能力。

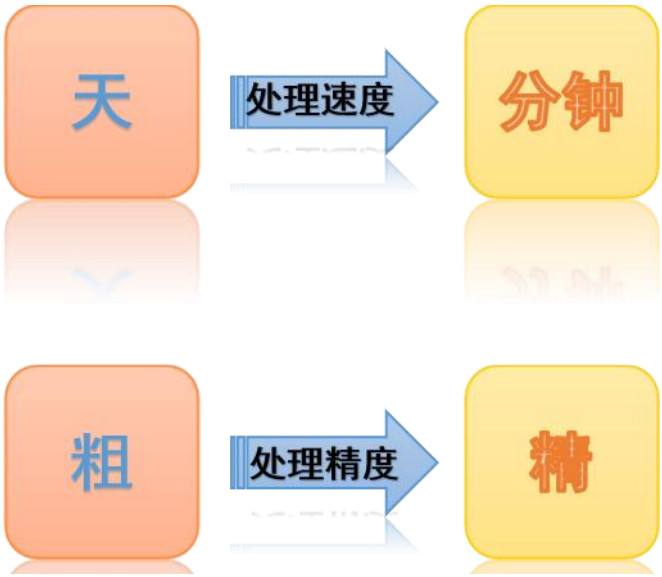

图 9-5　实时监测响应体系

（2）强化全企业集中的暴露面风险管理

强化全企业集中管控、集中运营，实现安全运营从“分散的事后分析”到“集中的常态化实时处置”转变。

面向互联网暴露面资产，开展资产的统筹管理与报备更新，资产归属部门负网络安全主体责任，网络安全运营中心集中开展扫描渗透与预警跟踪，上级主管部门负责监督考核。各部门协作，严格落实网络安全相关工作要求。

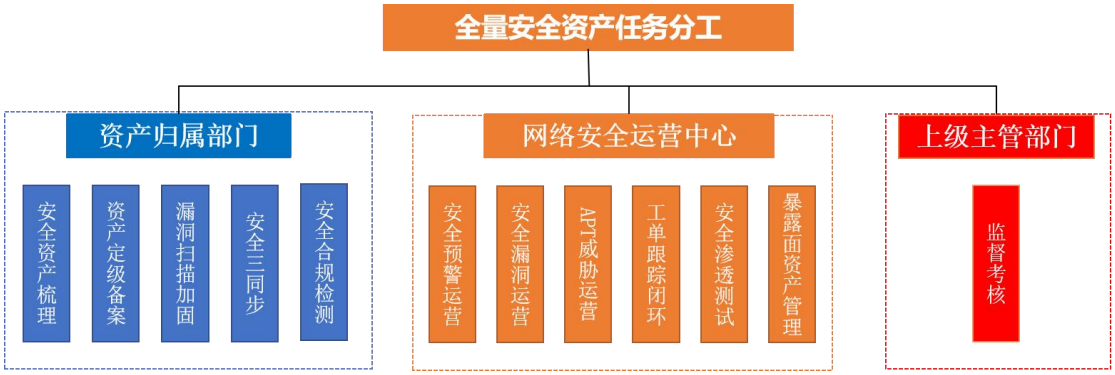

图 9-6　暴露面风险分工管理

（3）实现安全产品服务支撑能力

构建集中化智能服务平台，引入高效的资源整合和编排能力，实现企业各网络节点的一体化、灵活调度。

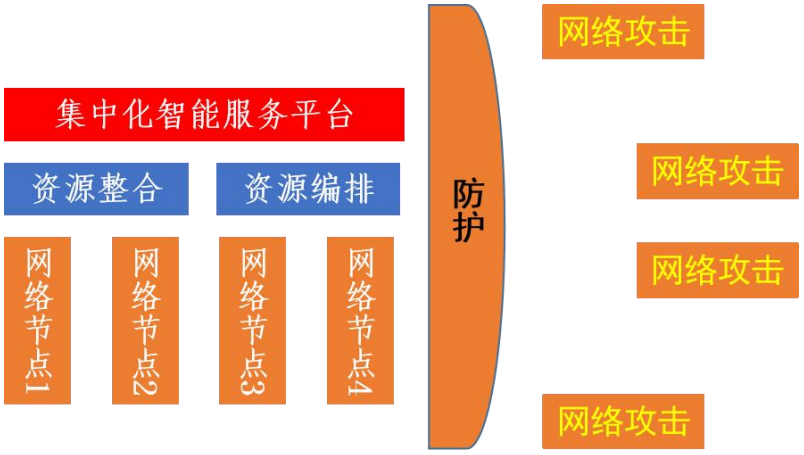

图 9-7　安全产品服务支撑能力

以集中化安全服务面向各类网络攻击事件，以稳定的安全防护打造工业互联网企业的安全防护壁垒。

（4）完善网络安全防护技术体系

工业互联网体系中，网络体系是基础，平台体系是核心，安全体系是保障，数据是核心的核心。

中国移动通信集团安徽有限公司以网络为基础，从安全防护平台和设备上构建企业安全防护壁垒，全面覆盖网络设备、关键业务，强化公网暴露面的集中分析、研判和一键处置能力。实现防护能力的灵活性，做好对企业内赋能各部门、对外服务各类客户、对上落实国家

行业监管要求。

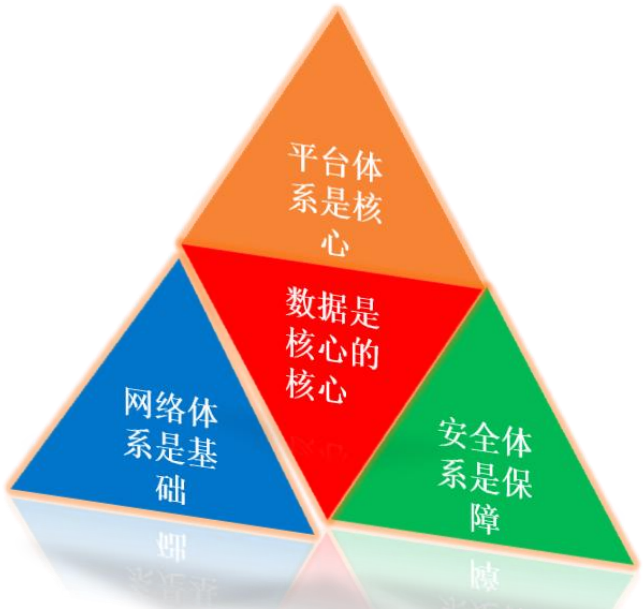

图 9-8　工业互联网体系要求

（5）探索自动编排及处置

为了减轻流程化的工作任务，大力推进 AI 能力落地，基于网络安全态势感知能力开发实现安全能力自动编排，支撑实现海量告警压减 80%和超过 70%的安全事件自动处置，降低人员重复性劳动，避免人为操作失误，保障在网络规模不断扩大、安全告警数量激增情况下，安全监测分析人员不大幅增加。

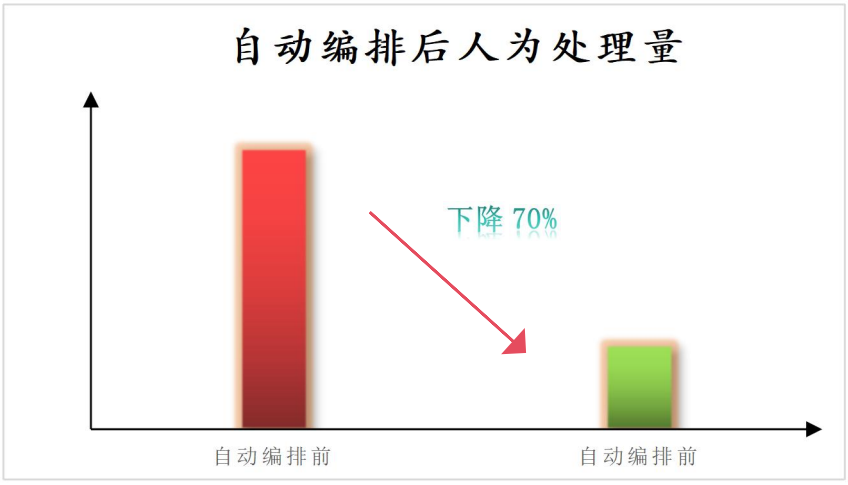

图 9-9 自动编排及处置降低工作量

（6）精细管控，提升数据安全防护能力

面向全企业网络资产，围绕“规范化操作、自动化审计、流程化处理”目标，开展精细化安全管理。以网络安全管控平台为抓手，实现安全接入、身份验证、金库管控、日志审计等管控能力，落实数据全生命周期管理。

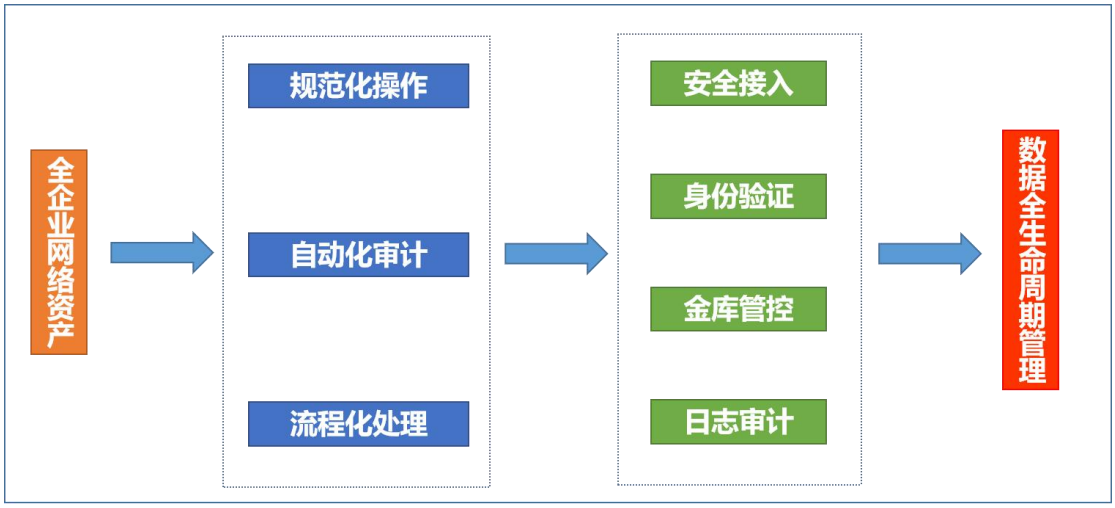

图 9-10　数据全生命周期管理

（7）知守善攻，打造高水平实战队伍

集约化安全运营中心需要一支知守善攻的安全保障团队。中国移动通信集团安徽有限公司认真规划安全保障团队的建设计划，通过创建团队、提升能力、全面支撑三个阶段，稳步提升人员的综合实力，并成立专门面向竞赛的种子队，针对性的培养行业顶尖的网络安全人才，打造一支高水平安全攻防技术队伍，积极参加企业内外专项行动及重大活动的网络安全保障工作，覆盖全公司的网络安全各领域。

图 9-11　安全保障团队培养体系

4. 安全及可靠性

集约化安全运营中心是中国移动通信集团安徽有限公司面向工业互联网领域倾力打造的安全，可靠的安全运营解决方案。在建立网络安全运营中心时，推进建设网络安全运维系统的建设工作，统合开展多个平台总计 9 类 53 项网络运维工作，依托全方面的安全运维工具对安全工作进行系统性的梳理和解决。在运维平台建设的同时，对网络安全工作人员进行重新划分，细化人员培养路径，降低传统网络安全工作模式所造成的疏忽和错误。不断完善重大活动期间网络安全的保障能力，建成分钟级应急响应能力。在完善集约化网络安全运营中心时也为工业互联网企业带来全方位、安全、可靠的集约化安全运营解决方案。

（1）全方位、安全、可靠的网络安全运营中心建设

细分终端、网元、业务、出口，统筹构建网络安全“集中+分布”协同防护能力。依托网络安全感知平台，提升网络安全集中监控水平。针对重保场景，健全网络安全风险检测与处置能力。

检测型设备：系统/Web 漏扫、防火墙、防病毒、IPS、堡垒机、WAF、抗 D、VPN、网页防篡改、网站安全监测、蜜罐等。

关键网元/业务/出口安全能力概览										
网络	DPI/僵木蠕	抗DDOS	IPS	全流量	WAF	网页防篡改	漏扫	域名防护	防病毒	一键封堵
1	√	√	√		√	√	√	√		√
2	√	√				√	√	√		√
3	√		√			√	√	√		
4			√	√	√	√	√	√	√	
5	√	√	√	√	√	√	√	√		√
6	√	√	√	√		√	√	√	√	√
7	√	√	√	√	√	√	√	√	√	√
8	√	√	√	√		√	√	√	√	√
9				√			√			
10							√		√	
11							√		√	

图 9-12　全面的风险管控机制

（2）全面、敬业、专业的安全保障团队

中国移动通信集团安徽有限公司积极探索网络安全队伍培养新模式，组建面向网络安全保障的联合团队——“徽盾”网络安全团队。常态化开展攻防实训与实战，已经成为保卫企业的中坚力量。

集约化安全运营中心的保障团队不仅要做好团队的工作计划安排，稳步推进各项工作：重大活动保障、应急演练、技能培训、竞赛组织等，也要承担安全运营中心内各类常态化、临时性安全防护任务。中国移动通信集团安徽有限公司开发的集约化安全运营中心采取依托安全攻防平台的形式，落实常态化竞赛培训，并取得了突出成绩。一方面，此项举措锻炼了安全保障团队的技术能力，另一方面也对外营造了集约化安全运营中心的专业形象，为企业荣誉添砖加瓦。

图 9-13　优秀安全保障团队

（3）系统化、分钟级的重大活动网络安全保障

中国移动通信集团安徽有限公司的集约化安全运营中心通过整合资源，协调分工，在重大活动期间，成立网络安全领导小组办公室统筹组织，协调企业内“徽盾”网络安全团队专家优势资源，组建专家队伍参与保障活动。

为保证重保行动顺利开展，统筹工作组下设事件协调组、事件监控组、事件处置组和应急响应组分别开展工作。

图 9-14　重大活动网络安全统筹

在面对网络攻击时，积极应对“侵”、“扰”、“窃”，深化 IPDRR 动态防护理念在现网攻防实战中落地，突出强化保障中响应速度快的能力，提升网络和数据安全端到端安全防护水平。

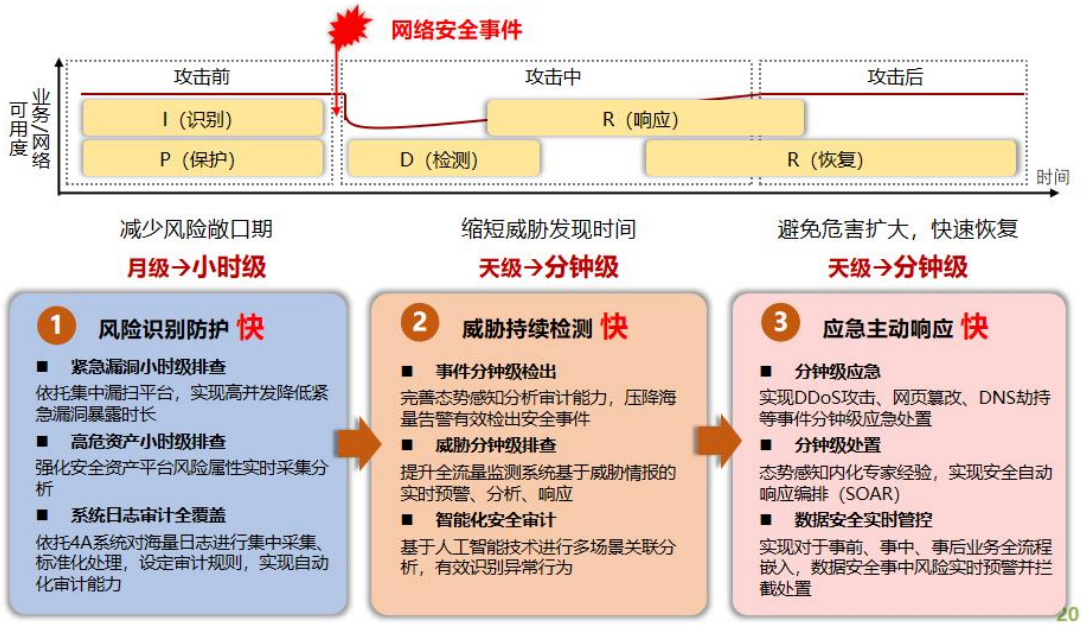

图 9-15　分钟级应急响应

5. 其他亮点

中国移动通信集团安徽有限公司面向工业互联网领域打造的集约化安全运营解决方案，主要从三个方面为企业打造安全防护壁垒。一是梳理网络安全条线的工作，面向全企业互联网暴露面资产开展风险的集中发现、及时预警与跟踪闭环，实现重要网络安全事件的全企业集中监测、集中运营、集中处置，建立多级联动应急保障与响应体系。二是全方位的网络安全防护，梳理了网络攻击、安全防护方面 9 类 53 项工作。通过对标分析，推进安全防护从分散、点状向集中、体系化转变。组织开展网络条线基础设施安全防护，加强手段建设，强化攻防能力。三是组织结构的优化，打破传统网络安全人员的防卫性工作模式，细化分工，研究更加专业，系统，高效的集约化安全运营中心人才培养体系，培养各方面的网络安全人才，建立一个攻防兼备的安全保障团队。

1.1.3　下一步实施计划

1. 算力网络安全探索实践

当前，随着新一轮科技革命和产业变革的深入发展，算力已成为信息社会的核心生产力，将直接影响数字经济的发展速度，直接决定社会智能的发展高度。网络作为连接用户、数据、服务的主动脉，与算力结合日益紧密，融合共生已成趋势。算力网络的不断发展，带来新的安全威胁，需要相应的安全保障措施。中国移动通信集团安徽有限公司集约化安全运营中心积极开展算力网络安全技术探索，推进相关工作落地。

图 9-16　算力网络安全防护

2. 5G 专网安全服务标准化推进

面向 5G 端到端，提升安全风险告警、IP 溯源、快速处置能力。面向 5G 垂直行业客户，积极推进安全服务产品化，形成服务标准化流程、输出安全服务能力清单，提升集约化安全运营中心对新业务的保障能力，目前已实现多个方案落地试点。

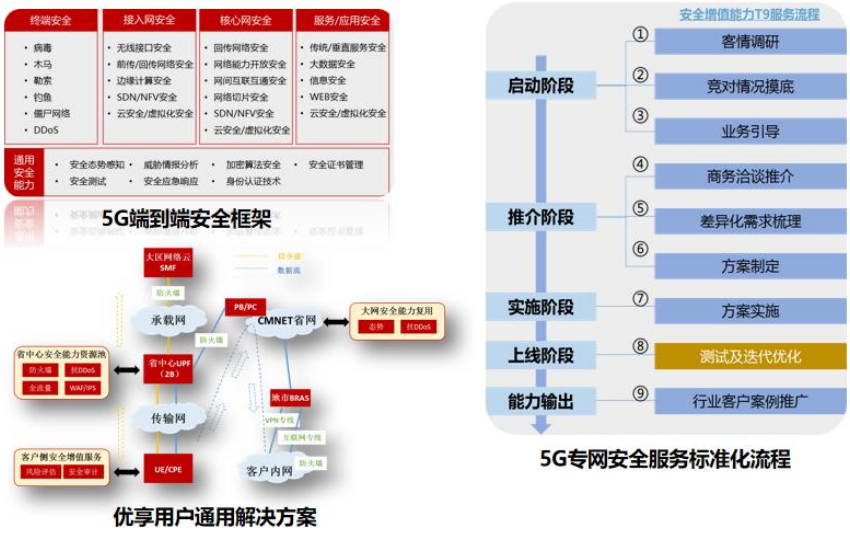

图 9-17　5G 专网安全服务标准化

3. 5G 应用安全创新示范中心筹备

5G 网络引入网络功能虚拟化、网络切片、边缘计算、网络能力开放等关键技术，一定程度上带来了新的安全威胁和风险，对集约化网络安全运营中心的数据保护、安全防护和运营部署等方面提出了更高要求。

定位及方向：面向重点行业 5G 应用发展中的安全需求，旨在打造 5G 安全产品、设计 5G 安全端到端解决方案、输出 5G 安全服务、开展 5G 安全人才培养，形成标准化、可复制、易推广的 5G 应用安全

解决方案的研发供给、试点示范和推广应用能力。

图 9-18　5G 应用安全创新示范中心

1.1.4　方案创新点和实施效果

1. 方案先进性及创新点

（1）创新点 1：创新资产安全风险发现方法

采用自动化扫描、人工渗透相结合方式，开展暴露面资产的发现、风险的检测，实现多种扫描器交叉扫描、不同人员交叉渗透，依托网络安全运维平台，派发预警工单、跟踪闭环。

图 9-19 资产安全风险发现体系

（2）创新点 2：创新全流量安全风险检测方法

提升集约化安全运营中心对新业务的保障能力，在企业重要数据出口处部署全流量安全检测系统，开展安全风险深度挖掘。对网络链路全流量采集存储、全数据分析，引入 AI 检测引擎，基于规则+行为

分析，为识别发现漏洞利用、高级木马通讯、APT 攻击、数据窃密等提供更有效的监测手段。

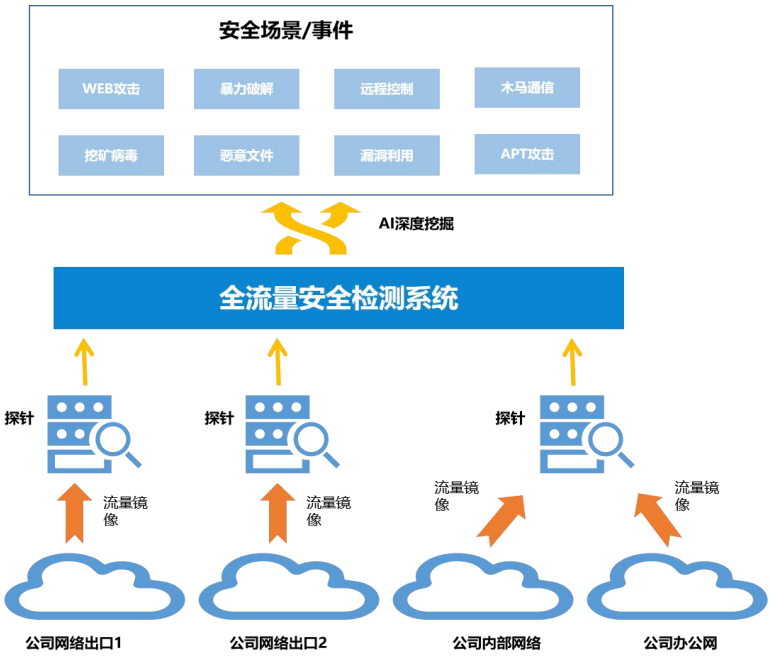

图 9-20　全流量安全风险检测方法

（3）创新点 3：创新网络数据安全管控方法

“以数据为中心，融合零信任理念，基于场景化的思路”进行设计，在对数据资产自动发现并分类分级的基础上，根据不同场景的安全需求和安全风险，统一制定安全策略并调配底层能力组件，实现数据全生命周期管理。

资产自动发现功能设计：

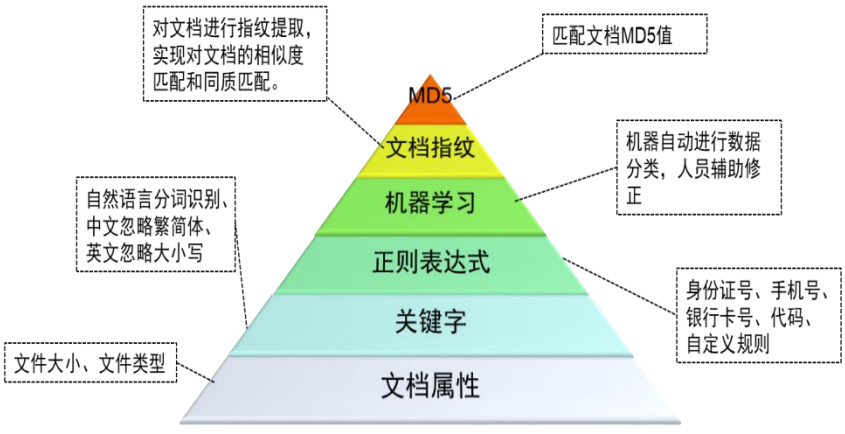

图 9-21　资产自动发现功能设计

敏感数据发现：

敏感数据自动扫描，自动识别不同资产上的敏感数据。支持识别数据库：MySQL、DB2、Oracle、SqlServer、SQLite、Sybase、Teradata、Greenplum、MongoDB、PostgreSQL 等。支持识别大数据平台：HDFS、Hive、HBASE。

数据脱敏处理流程：

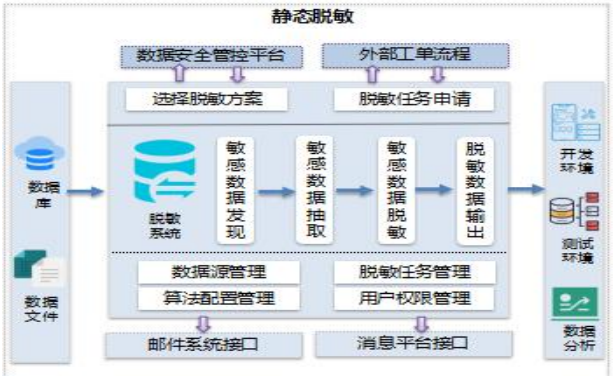

图 9-22　数据脱敏处理流程

数据防泄露：

终端数据防泄漏：对接入终端防泄漏进行策略管控和可视化审计视图展示。

网络数据防泄露：维护区到生产区之间的交换机中接入静态流量，管理监控维护人员的流量数据。

主机数据防泄漏：通过数据安全管控系统下发主机敏感数据发现策略，通过自定义路径遍历扫描，识别到敏感文件并进行分类分级展示。

2. 实施效果

（1）成效 1：提升了对安全事件的处理速度

集约化网络安全运营中心对安全系统，安全设备，安全事件的统一安全服务、集中管理运营维护、统一把控网络安全风险，减少了各部门人员之间的沟通成本，大大提升了对安全事件的处理速度。

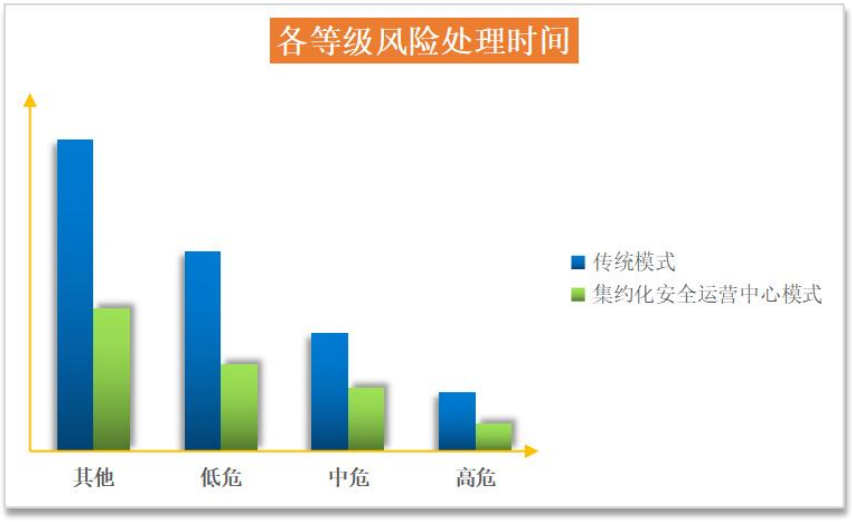

图 9-23　风险闭环时间减少

（2）成效 2：减少了网络安全人员的工作量

集约化网络安全运营中心通过对各类安全运维系统的建设，研发 AI 能力，提高自动编排及处置能力，减少网络运维人员对常见安全事件的处理量。

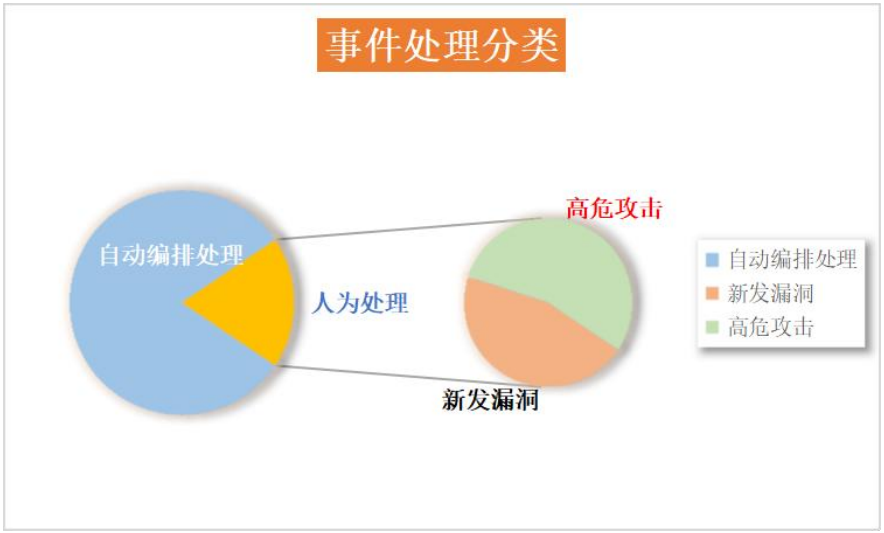

图 9-24　安全事件处理情况

1.1.5　单位基本信息

1、中国移动通信集团有限公司信息安全管理与运行中心

本方案由中国移动通信集团有限公司信息安全管理与运行中心牵头。2011 年 11 月，中国移动通信集团有限公司信息安全管理与运行中心成立（以下简称“信安中心”），具备“管理+生产”双重职能，

负责归口信息安全管理与不良信息治理，开展不良信息集中治理与信息安全集中运营。2018 年 8 月，集团成立中国移动网络安全领导小组，领导小组办公室设在我中心，负责集团网络安全相关工作统筹和协调。信安中心深入学习贯彻习近平总书记关于网信工作的重要指示精神，以建设网络强国为己任，工作范围覆盖终端安全、网络安全、应用安全、业务安全、内容安全等多领域，形成了全国“一盘棋”的工作格局，相关工作整体能力与水平始终保持行业领先。近年来，信安中心在开展网络安全重保、防范打击电信诈骗、组织网络安全攻防竞赛、开展网络安全研发等方面卓有成效。在工业互联网方面，特别成立了专门的研发中心，开展工业互联网业务及工业互联网安全防护解决方案的研制和推广。

2、中国移动通信集团安徽有限公司

中国移动通信集团安徽有限公司下辖 16 个市分公司、64 个县（市）分公司及 1 个全资子公司，拥有各类员工 16700 余人。公司以满意服务为宗旨，以创无限通信世界，做信息社会栋梁为使命，全面实施服务与业务领先战略，努力为安徽经济的腾飞服务。中国移动安徽公司自成立以来，运营收入平均增速达 20%，成为区域主导通信运营企业。2002 年上市以来，累计上缴中央和地方税收达 119 亿元。移动通信网络已全面覆盖全省各市、县、乡、村。中国移动安徽公司大力推进行业应用，助推政府和企业信息化建设。公司一直致力于以移动信息化助推当地经济社会发展。企业发展不忘回报，积极开展教育扶贫、捐资助学，支持农村教育、科技和文化事业发展。公司近年的发展得到了社会各界充分肯定，先后获得“全国五一劳动奖状”、“中央企业先进集体”、“全国履行社会责任贡献突出奖”、“全国通信行业用户满意企业”、国家级“诚信维权单位”、“全国优秀外商投资企业”、“全

国内部审计先进单位”、“全省外商投资经济效益先进企业、经济效益最好企业”、“全省模范劳动关系和谐企业”等荣誉称号。