1.1 案例十二：工业企业安全纵深防御新范式——为能源企业打造平战结合的安全综合能力管控平台

1.1.1 方案概述

浙能集团网络安全综合能力管控平台方案通过汇聚接入现有安全能力，面向浙能集团及下属单位实现网络安全脆弱性集中检测、安全策略集中分析、安全要求集中下发、安全能力集中调度、安全威胁集中通报、安全事件集中处置、安全风险集中可视，提升企业安全运营及应急响应能力，打造集团级纵深防御网络安全体系，积极应对网络安全新形势下的新变化、新威胁、新挑战。

1.方案背景

随着工业互联网发展进程加快，浙能集团 IT 与 OT 网络融合加速，互联互通需求日益增多，安全边界日益模糊，网络边界防护压力与日俱增。另一方面，随着数字化转型的不断深入，信息系统的资产数量、技术架构、应用场景等方面发生了巨大的变化，传统以策略和产品防护的理念已无法适应业务云化动态防护要求。

在面对严峻复杂的网络安全形势下，浙能集团当前存在安全工具孤立建设、安全能力难以复用、安全运营联动不足、能力难以服务化输出等问题，安全防护体系建设面临巨大挑战。亟需通过梳理沉淀现有安全能力，适当补充新的安全能力，通过能力拉通、编排及服务化输出，赋能集团与厂区安全防护，提升网络安全应急响应及防护效率，抵御复杂网络威胁，保障信息系统安全运行。

2.方案简介

方案建成的网络安全综合能力管控平台以信息系统资产为基础，以安全能力管控为核心，实现安全合规集中检测、安全策略集中审计、安全风

险集中通报、安全事件集中处置、安全能力集中调度，赋能厂区网络安全建设，实现企业降本增效，提升安全防护效率，打造集团级纵深防御体系。

3.方案目标

安全综合能力管控平台方案基于 IPDRR 模型实现浙能集团现有工具统一纳管与安全能力接入，并通过能力编排与调度，构建日常安全运营及重大活动保障场景的安全服务，赋能集团和下属单位，助力企业安全建设降本增效，提升安全防护效率。

从安全管理角度看，依托平台能力，集团侧可摸清下属工业企业网络安全现状，明确安全责任、落实上级单位安全考核，安全策略的统一下发；下属工业企业可依托平台提供的开展安全自主服务，实现安全作业常态化执行、安全预警闭环管理，安全策略高效执行，为浙能集团产业高质量发展提供强有力的安全支撑。

1.1.2 方案实施概况

1. 方案总体架构和主要内容

安全综合能力管控平台采用集团集中部署，用户分权分域模式建设，支持微服务架构，通过集团侧安全工具的集中纳管、安全能力的分类调用，以 IPDRR 模型为指引构建安全能力中心，为浙能集团及下属单位安全运营人员提供安全服务。建设安全合规中心、安全监测中心、安全防护中心、应急响应中心，依托浙能集团数据中台安全数据实现安全驾驶舱，在满足安全监管要求的同时，具备网络安全中台演进能力，为浙能集团安全建设降本增效，解决浙能集团安全设备管理建设，安全运营缺乏协同等问题。

在技术方案设计上充分考虑风险识别、安全检测、安全防护、安全响应、安全恢复 5 个阶段能力的管控，通过 API 等接口实现对接，总体框架图如下所示：

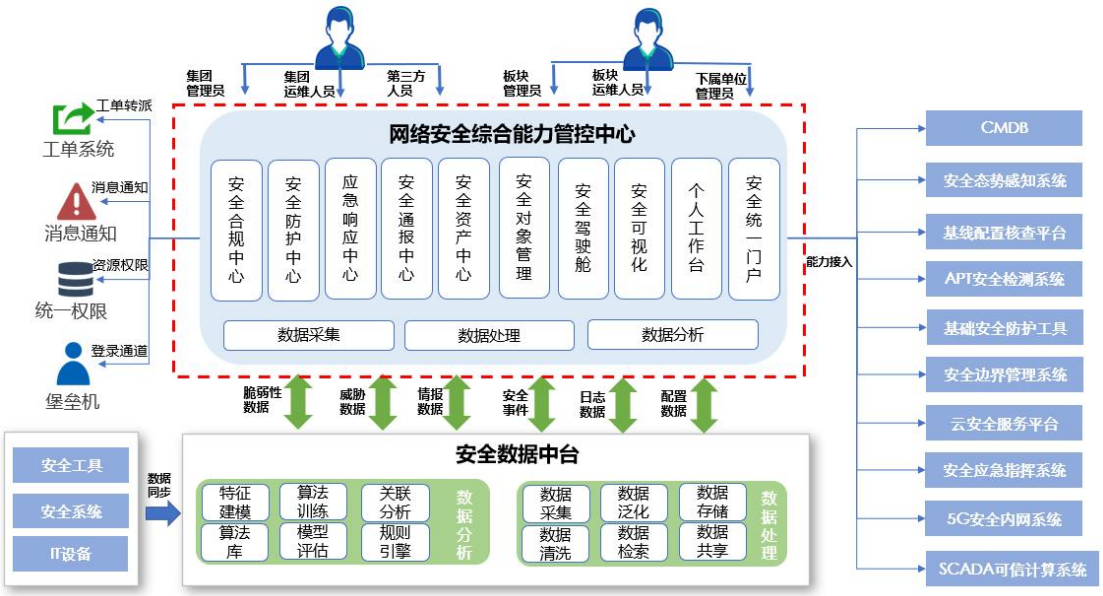

图 12-1　安全综合能力管控平台总体框架图

（1）系统架构设计

平台系统架构设计主要分为四部分，包括安全工具层、能力管控层、安全服务层、外部系统层。应急指挥、基线核查、安全边界作为工具能力接入安全能力管控系统，分别部署至浙能集团总部两个数据中心。在技术方案设计上充分考虑风险识别、安全检测、安全防护、安全响应、安全恢复 5 个阶段能力的管控，通过 API 接口实现基线配置核查系统、安全边界防护系统、安全应急指挥系统、哨兵云、防火墙、堡垒机等安全能力接入，面向集团、板块、下属单位提供安全服务统一入口，与现有安全数据中台实现数据同步及共享实现安全驾驶舱，并通过接口与浙能集团信息运维管理平台、统一消息系统、统一认证系统等外部系统对接，在满足安全监管要求的同时，具备网络安全中台演进能力。

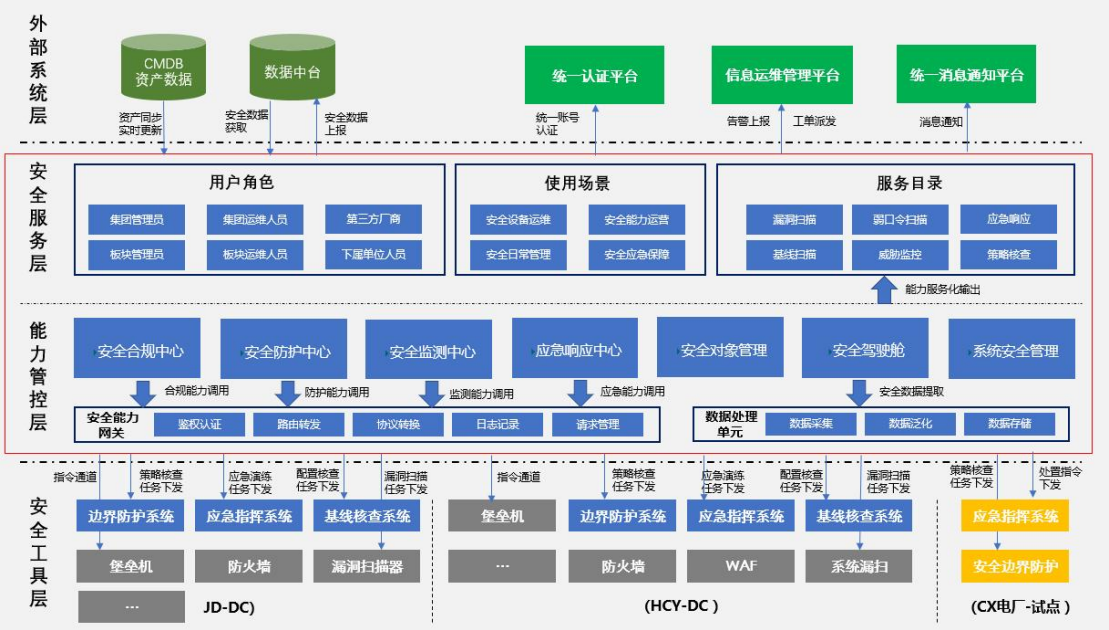

图 12-2　安全综合能力管控平台架构图

本期方案总体架构分为四层，自下而上分别为安全工具层、能力管控层、安全服务层、外部系统层

➢ 安全工具层：

安全工具层主要是指分布在浙能集团大楼以及海创园数据中心以及电厂的安全设备与系统，安全工具包括本期新建及存量设备。

➢ 能力管控层：

能力管控层主要包括安全能力网关、数据处理单元、安全能力中心，以及能力管控所需的安全对象管理及系统安全管理。依托数据处理单元抽取工具任务运行数据及数据中台威胁数据构建安全驾驶舱。安全能力网关实现工具接口接入，同时北向创建 API 接口供能力中心调用。

➢ 安全服务层：

安全服务层基于安全能力中心能力，形成面向浙能集团及下属单位安全管理员、安全运维人员提供漏洞扫描、基线合规扫描、弱口令扫描、应急处置、防护策略审计、安全威胁监测等服务，可在安全设备运维、安全能力运营、安全日常管理、安全应急保障等场景下发挥作用。

外部系统层：

外部系统层是指安全管控平台需要对接的第三方平台，主要包括 CMDB、数据中台、统一认证平台、信息运维管理平台、统一消息通知平台。

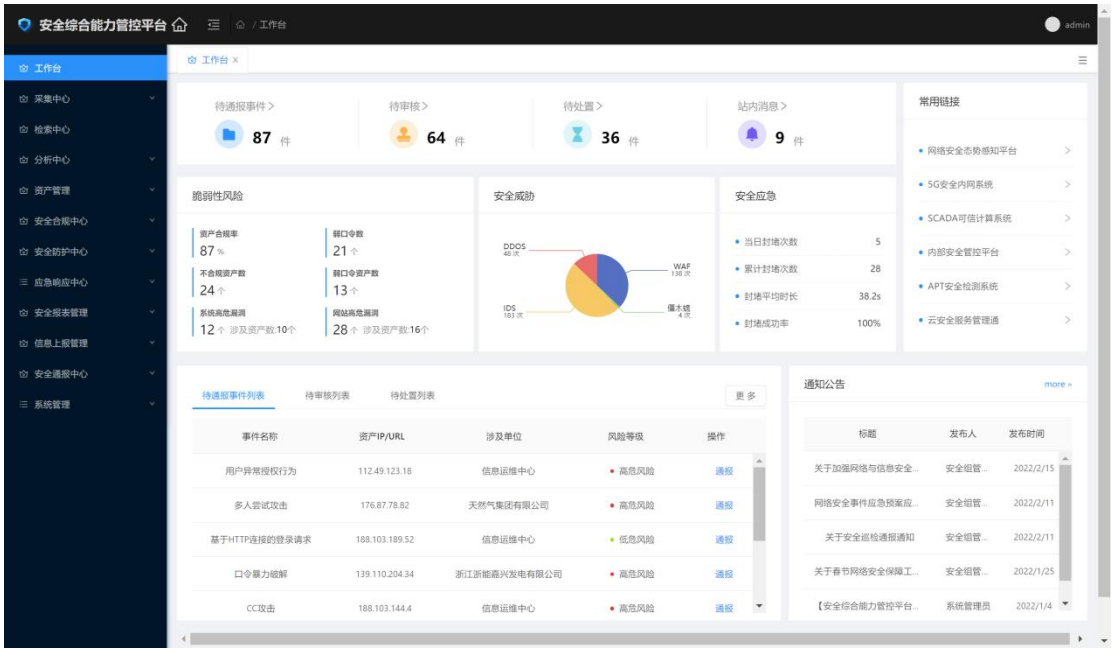

图 12-3　平台功能图——个人工作台

图 12-4　平台功能图——安全驾驶舱

2. 网络、平台或安全互联架构

网络安全综合能力管控平台支持集中式、分布式或混合模式部署方式，

集中式部署时，分支机构可根据权限实现对本单位所辖资产及安全风险的管理。分布式部署时，支持三级平台级联，通过级联实现统一处置、检测、通报。

方案部署地点位于浙能集团数据中心，后续通过部署处置节点方式与管控大区、工控大区对接，实现集团统一管控，具体如下图。

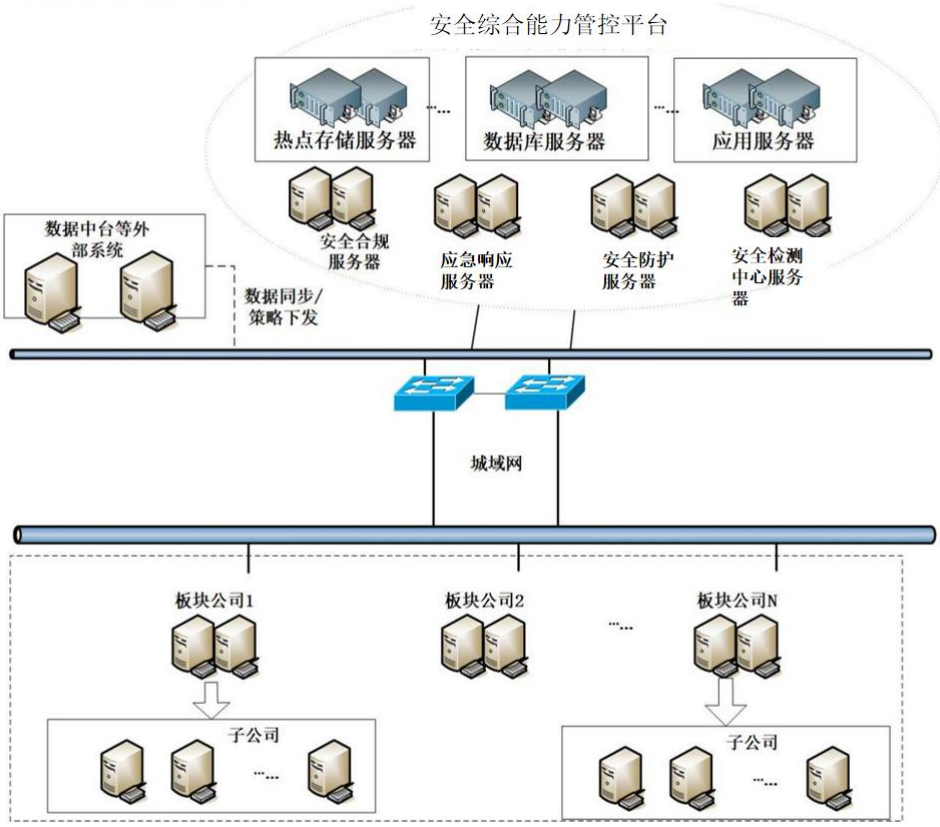

图 12-5　安全综合能力管控平台部署示意图

3. 安全及可靠性

在集团统一的网络与信息安全管理要求下，系统相关的物理安全、网络结构安全、设备安全、系统安全、应用安全、数据安全等满足等级保护三级要求，建立有效的安全机制，实现应用的安全访问控制，同时保障数据在采集、传输、存储、访问中的安全性。传输过程中采用必要的国产商业加密算法对数据进行加密，并完成国产操作系统的兼容性测试。

4. 具体应用场景和安全应用模式

（1）应用场景

安全综合能力管控平台建设后，面向安全日常运营、重大活动保障等场景提供安全合规检查、安全应急处置、安全策略审计、安全事件处理等安全服务入口。

日常运营：在日常安全运营期间，系统可提供安全设备合规扫描、弱口令扫描，支持对新入网设备进行合规基准检查，针对不符合要求的策略项进行整改筛查；提供系统漏洞扫描、网站漏洞扫描等服务，针对集团内部资产进行定期漏洞扫描，并对中高危漏洞进行整改核查；提供防火墙策略审计服务，针对防火墙设备的策略进行在线/离线采集，通过多维分析算法进行策略解析，输出审计报表，针对不合规策略问题项进行处理；提供安全事件通报预警服务，可对安全事件的上报、审核、通报、处置流程进行管理记录，及时对安全事件进行响应处置；提供安全应急处置入口，针对日常发现的需要进行封堵操作 IP 地址进行一键封堵。

重保/护网：在提供重保模式安全驾驶舱，可针对重保护网期间产生的安全事件进行动态呈现，展示安全风险变化情况；提供应急处置入口，针对护网期间需要进行封堵的大批量 IP 地址进行极速封堵操作，快速完成攻击阻断。

（2）安全应用模式

系统可通过 SaaS 服务、本地建设等模式为工业企业提供安全应用。以应急响应场景为例，提供集团-板块-下属单位三级联动应急处置，通过对接各单位/板块公司的边界防火墙实现处置策略的下发。通过 HTTP 接口实现多级平台联动，集团一级平台收到上级单位处置指令后可下发处置工单至二级平台，二级平台可选择自动处置或者人工审核是否进行处置，并将处置结果上报至集团的一级平台。二级平台可自主下发处置工单至三级平

台，三级平台接收处置工单后可选择处置方式并将结果反馈至二级平台。

5. 其他亮点

（1）安全资产集中纳管，为资产安全风险定位提供追踪溯源基础

安全资产管理模块对浙能集团及下属单位资产信息进行管理，包含对主机、数据库、中间件、网络设备等 IT 资产以及网站资产的管理，为安全基线检测、漏扫检测、防火墙策略核查、安全监测通报等安全能力提供资产库信息，为安全驾驶舱、安全事件风险定位提供追踪溯源依据。

（2）安全风险集中可视，可全局掌握集团网络安全风险运行情况

将获取到的威胁数据、脆弱性数据与资产数据进行关联，形成网络安全决策依据，构建安全驾驶舱，从日常模式、巡检模式、护网模式多维度展现安全工作的重点关注指标，反映网络运行及安全状态，将安全风险形象、直观地呈现给安全决策者和管理人员，方便安全运营管理者全局掌握浙能集团网络安全风险及运行情况，为安全工作提供决策支撑。

（3）安全策略集中下发，实现防火墙安全防护策略精细化管理

面向浙能集团数据中心以及下属单位提供防火墙策略核查能力及处置能力，防火墙自动化审计功能可对存量策略进行分析检索并给出审计报告，大幅提升防火墙策略审计效率；应急处置能力可针对 IP 地址、域名、URL 等进行快速封堵处置，通过上下级联动的方式，实现“一点下发，全局防控”提升安全应急响应效率。

（4）安全能力集中调度，实现浙能集团安全能力调度编排共享

通过安全综合能力管控平台统一纳管基线合规、资产检索、漏洞扫描、弱口令扫描、策略审计、态势感知、应急处置等能力，并通过安全编排与智能调度有效支撑浙能集团及下属单位常态化安全运营工作开展，集约化地将人、技术、流程深度融合，实现安全能力与服务的集中输出。

1.1.3　下一步实施计划

计划 1：在浙能集团下属板块及单位推广，实现安全能力全面应用

方案后续计划在浙能集团下属板块及单位进行分阶段推广。目前已在电力板块及下属长兴电厂、镇海电厂，燃气股份，科工服务多个单位应用，后续计划在集团下属煤炭运输、石油、可再生能源等多个行业板块推广应用，提供应急处置、策略审计、合规检查、威胁监测、漏洞扫描等安全能力，实现安全能力服务化输出。

计划 2：在金融、电力、水利等行业推广，实现安全能力行业赋能

方案后续计划在金融、电力、水利等行业开展推广，安全综合管控平台提供的标准化安全事件研判与处置流程、沉淀安全策略知识库，自建的应急处置、策略审计、合规检查、威胁监测、漏洞扫描等安全能力可复制推广应用于各关键信息基础设施领域，实现安全能力行业赋能。

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：基于异构策略库模型实现安全应急响应智能编排

在构建安全综合能力管控平台过程中引入 playbook 原子化设计理念，将事件捕捉、特征识别、策略封堵、策略恢复、策略验证等脚本封装成原子能力并进行智能编排，三层异构模型，可支持基于特征规则的策略识别，也可支持基于行为模型（阈值、基线）的策略加载，同步引入大数据算法完成安全事件处置规则的自学习能力，进而提高策略库的准确性和完整性。

（2）创新点 2：基于场景化 AI 算法实现安全风险智能研判预警

基于传统的样本特征比对和正则匹配的检测方式面临极大的挑战，攻击者一旦绕过或直接使用非特征库中的攻击载荷，传统的检测防护模式将不再生效。通过引入基于 AI 的轻量级数据处理及分析框架，对安全数据进行采集、预处理、富化，并采用神经网络、NLP、KNN、SVN 等模型进行训练和分析，生成的结果匹配威胁情报后输出安全事件，根据置信度选择不同

的处置流程，可有效提升安全事件的智能分析与自动化处置水平。

（3）创新点 3：通过建立平战结合安全驾驶舱支撑安全管理决策

为全方位掌握浙能集团网络安全运行状况，理解安全能力运行数据背后规律，挖掘安全数据蕴含的风险信息，进而快速发现潜在的网络威胁，通过建立安全能力指标体系，建立日常模式、巡查模式、护网模式等场景下的安全驾驶舱，多维度分析数据联系，反映网络运行及安全状态，支持多维安全数据联动交互，将安全风险形象、直观地呈现给安全管理人员，为安全提供决策。

（4）创新点 4：依托微服务安全网关技术实现安全能力解耦集成

基于微服务能力网关技术，通过接口技术标准化，能力输出标准化、流程标准化，实现平台侧安全能力解耦与集成，依托编排引擎实现能力的的拉通与智能调度，实现安全能力增强互补，同时建立能力评估体系，在提高安全工具接入的同时，便于对安全采购部门能力选型提供依据。

（5）先进性说明

方案已服务浙能集团及下属单位共 12 家，在电力、天然气、科服多个板块推广应用，累计授权专利 8 项，并发表多篇论文。平台中的网络安全边界防护子系统及网络安全应急指挥子系统已完成龙芯处理器、中标麒麟的操作系统、华为鲲鹏服务器、信创云完成兼容互认证测试并获得多项认证证书，实现安全自主可控。

2. 实施效果

（1）依托安全事件工作台，实现安全事件闭环高效管理

通过建设安全事件工作台，以安全事件的发现、上报、分析、通报、处置的安全事件应急响应流程为导向，将日常及重保期间的线下工作流程全面转到线上，实现安全事件的闭环管理，上线运营后，日均处理安全事件百条，平台完整记录了安全事件的上报过程、处理过程、处置责任人、

处置时间等信息，实现安全事件闭环高效管理。

（2）依托安全研判知识库，大幅提升安全事件处理效率

安全专家可针对上报的安全事件，通过溯源取证、威胁情报、IP 资产归属查询等辅助手段，评估该安全事件的威胁情况，给出处置方案进行处置。同时，安全综合能力管控平台通过沉淀浙能集团一线专家研判规则形成分级分析算法，提供自动化研判手段，给出研判结果，辅助专家进行研判决策，对日常及护网期间产生的安全事件进行快速的分级分类处理，在大批量的安全事件中辅助分析团队进行快速研判与精准决策，提升响应效率与研判质量，平台上线运行后，人力效率提升约 30%，每次重保期间节省人力成本约 200 万。

（3）依托极速封堵模式，大幅提升安全应急处置能力

在浙能集团本部建立的统一封堵能力，兼容异构边界防护设备，针对深信服、天融信、绿盟等异构防火墙设备进行策略管控，通过地址集自动扩展方式实现大批量 IP 地址的快速处置，单日可完成 10 万以上 IP 的封堵操作，满足演练和突发安全事件时攻击 IP 的快速封堵。通过重保期间的极速处置模式，大幅度提升应急处置效率，封堵速度提升 10 倍以上。

（4）依托多级联动机制，实现集团一点监控，全局防御

面向浙能集团下属单位，通过安全综合能力管控平台可实现封堵指令集中下发，实现“一点发现、全局封堵”，大大提升重大活动保障期间的应急处置效率，通过多级联动机制为重保防护提供坚实保障，优化管控流程，减轻运维压力。依托平台提供的安全能力及自动化服务，2022 年在国家级护网演习中只人员数量大幅减少，并获得主管部门认可。

（5）提升企业安全基线，大幅减少工业企业安全合规问题

方案运行后，浙能集团及下属工业企业积极开展安全基线、弱口令、漏洞等常态化风险检查，并发现多处基线配置、弱口令、漏洞等安全风险，

通过整改，目前高危漏洞和弱口令已清零，基线配置合规率达到90%以上，集团侧在例行安全检查过程发现的安全风险大幅减低，有效提升企业安全基线。

（6）安全工具集中纳管，沉淀安全能力实现行业内外赋能

平台通过纳管集团本部安全设备，可实现安全工具的集中化运维，同时基于IPDRR模型形成安全能力中心，为集团本部及下属工业企业提供开箱即用的安全能力与服务，包含安全资产管理、安全风险检测、安全合规检测、安全应急响应、安全策略审计、安全事件通报等，后续平台安全能力及建设模式可复制推广至其他行业，实现行业赋能。

1.1.5 单位基本信息

浙能集团成立于2001年2月，总部位于中国杭州，主要从事电源建设、电力热力生产、石油煤炭天然气开发贸易流通、能源科技、能源服务和能源金融等业务，是浙江省委、省政府能源产业发展的主抓手、能源合作的主平台、能源供应的主渠道、能源安全保障的主力军、环境保护的主战场和能源科技创新的主引擎，为浙江经济社会持续健康发展提供了有力的能源供应保障。截至2022年底，浙能集团资产总额2991.8亿元，所有者权益1382.9亿元，控股管理发电装机容量3905.1万千瓦；全年实现营业收入1667.2亿元、利润总额60.2亿元。

近几年，浙能集团每年科研投入约为20亿元，其中信息化投入每年约4亿元，取得了一系列科技创新和数字产业化成果，拥有国家技术发明一等奖一项，省部级科技进步奖多项。浙能集团高度关注网络安全工作，统筹指导下属工业企业实践网络安全防护方案，其中“大型火电厂网络安全综合防护研究与实践”方案获2020年国有企业数字化转型优秀案例，“大型能源企业基于数据中台的态势感知平台”方案获2022年度浙江省数字化改革网络安全优秀案例。

浙江鹏信信息科技股份有限公司（以下简称：鹏信科技）是新三板挂牌的国家高新技术企业、国家级专精特新“小巨人”企业、浙江省网络安全行业创新型十强企业。公司专注于网络信息安全领域，公司具有中国信息安全测评中心、中国通信企业协会安全委员会、中国网络安全审查技术与认证中心多项安全资质。2019 年成为浙江省工业控制系统信息安全应急支撑单位，已通过 CMMI5 级软件成熟度国际认证，授权发明专利 30 余项，参与国家标准制订 7 项，行业标准制订 14 项；承担浙江省重点研发计划项 2 项、杭州市重大科技研发方案 1 项。获得工信部网络安全试点示范方案共 4 项。

鹏信科技公司产品已成功服务于全国 20 多省份，超过 1000 家企业，参与了多个省部级方案、工信部的工业互联网创新发展工程方案 3 个。公司自主研发的安全能力底座、安全一键应急平台、基线配置核查系统、安全漏洞管理平台、安全策略可视化分析、安全运营管理平台、安全态势感知平台等系列产品，为中大型企业提供网络安全运营全流程解决方案。

2. 结束语

“编制优秀试点示范推广案例集”是工信部 2022 年推动工业互联网加快发 展的工作方向之一。本报告从工业互联网安全的优秀实践层面，响应国家的决策 部署，着眼于新技术融合带来的安全问题以及固有的安全风险，汇编了业内优秀 安全解决方案，为工业企业提供安全建设参考。

本报告面向 5G+量子安全、新能源等新技术、新场景提供优秀安全实践，同时涵盖能源、汽车、地铁等重要行业的安全解决方案，以及安全服务综合平台、安全综合防护系统的建设方案，与往年案例汇编共同丰富工业企业安全最佳实践。

未来，工业互联网这一新兴基础设施建设将向更广范围、更深程度、更高水 平不断推进，助力经济发展新动能，推动产业升级。新基建中 5G 与工业互联网 的融合发展乘数效应显著，5G+工业互联网也将加档提速，渐行渐近。

安全，作为工业互联网建设的重要组成部分之一，将不断面临新的挑战，新 的安全解决方案也会不断诞生。唯有安全行业与工业行业互相协作，攻坚克难，深耕工业互联网安全，协同打造安全的工业互联网，才可共同促进工业互联网的 繁荣与发展。