江苏中新赛克工业互联网
安全技术创新中心有限公司

共建工业互联网安全新生态

工业互联网企业

网络安全分类分级实施指导

国内工业互联网安全事件形势十分严峻

全国近两年发生的企业网络攻击事件，涉及汽车生产、智能制造、能源电力、烟草等多个行业，企业的办公网和生产网已成为最主要的攻击对象。企业**生产主机蓝屏、文件被加密、核心数据被盗取、遭遇挖矿病毒等事件时有发生。**黑客的**攻击手段愈加复杂，**数据泄露的规模、攻击的破坏效果都**呈现扩大趋势。**

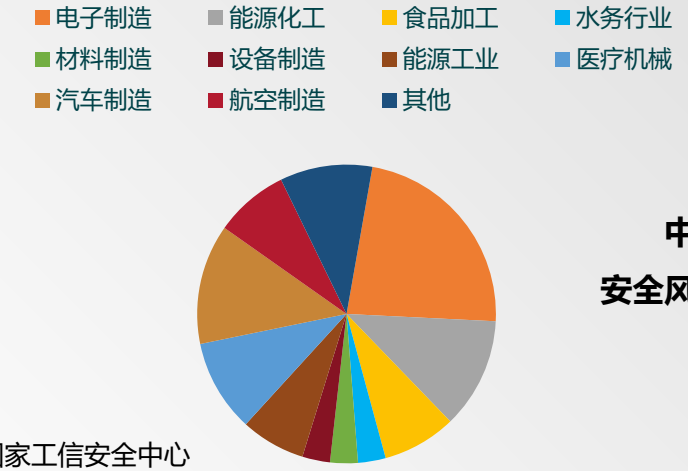
2022.5 电子制造巨头富士康某生产工厂遭受勒索软件攻击。

2022.2 我国互联网遭受境外网络攻击，百万台电脑沦为“肉鸡”

2022.6 滴滴被罚80.26亿，存在过度收集乘客信息等行为

滴滴出行
—滴滴一下 美好出行—

2022年，公开披露的工业领域安全事件共312起，其中工业领域勒索事件共89起，较2021年增长78%。



中国工业信息安全风险涉及行业分布

数据来源：国家工信安全中心

抽样研判的工业信息安全风险主要集中在智能**制造、交通、能源**等关键行业领域，其中风险数量排名前三的是：制造业23%，汽车制造13%、能源化工12%。

工业互联网安全体系化设计布局逐步完善

我国坚持发展和安全并重，高度重视工业互联网创新发展和网络安全工作，在工业互联网系列政策中同步强化安全设计和体系化布局，明确分类分级管理、技术保障、人才培育、供给创新等细化工作要求。

2017年11月 ■ **国务院出台《关于深化“互联网+先进制造业”发展工业互联网的指导意见》**：明确提出构建**网络、平台、安全**三大体系。

2018年6月 ■ **工业互联网专项工作组发布《工业互联网发展行动计划（2018-2020年）》**：提出网络、平台、**安全**相关行动目标与任务。

2019年7月 ■ **工信部等十部门联合印发《加强工业互联网安全工作的指导意见》**：明确7大任务和17项重点工作，布局建立**分类分级管理**等重点工作，构建体系化、多部门协同的**工业互联网安全工作格局**。

2020年12月 ■ **工业互联网专项工作组印发《工业互联网创新发展行动计划（2021-2023年）》**：提出**安全保障强化行动**，2023年，**工业互联网安全分类分级管理在全国实施推广**。

2021年1月 ■**工信部发布《关于开展工业互联网企业网络安全分类分级管理试点工作的通知》**：加强**工业互联网网络安全精细化管理**，提升工业互联网安全水平。

2021年12月 ■**工信部网络安全管理局指导下，工业互联网产业联盟、工业信息安全产业发展联盟、工业和信息化部商用密码应用推进标准工作组共同发布《工业互联网安全标准体系（2021年）》**：明确**工业互联网安全标准建设方向、任务和目标、确定工业互联网安全标准第一批研制计划**。

工业互联网安全标准体系加快完善

支撑制定发布《工业互联网安全标准体系（2021年）》，加大标准协调和推进力度，布局推动分类分级配套标准、关键领域及要素的安全标准规范研制，加快启动和推进第一批32项标准研制计划。

支撑制定发布《工业互联网安全标准体系（2021年）》

1.研制安全标准体系：以分类分级管理为基础，加快企业及关键要素分类分级防护、安全管理、安全应用服务等标准研制，**细化16个领域、76个标准方向。**

完善分类分级管理配套规范，开展定级规则、安全评估、能力评价等标准研制应用

2.牵头分类分级国标立项研制：经标协组织研讨、立项审议、意见征求，一致评审通过，**已上报国标委立项通过并完成公示。**

3.牵头开展7项安全行业标准立项研制：覆盖平台、标识**定级规则、安全评估、产品能力评价以及企业防护能力评价等**，健全分类分级管理配套标准和实操规范。


国家标准化管理委员会文件

国标委发〔2021〕41号

国家标准化管理委员会关于下达2021年第四批推荐性国家标准计划及相关标准外文版计划的通知

全国标准信息公共服务平台

开展关键领域标准布局研制，推动分类分级安全标准在重点行业领域落地

4.分类分级重点行业标准研制：联合**轻工、钢铁**等行业协会，推动**《轻工行业工业互联网企业网络安全分类分级防护要求》《钢铁行业工业互联网企业网络安全分类分级防护要求》**等多个行业标准立项研制；

5.关键领域标准研制：围绕**关键要素、安全上云、5G+工业互联网安全**等领域，在ccsa启动**9项**标准立项研制。

工业互联网企业网络安全分类分级管理落地深耕

2021年，工信部组织开展工业互联网企业网络安全分类分级管理试点工作，15省份、200余家工业互联网企业完成分类分级管理工作，我国工业互联网安全管理进入实践深耕阶段；2022年江苏省130多家企业完成分类分级工作。

明确安全监管职责，完善管理服务能力

- **行业范围**：主要涉及**原材料工业、装备工业、消费品工业**和**电子信息制造业**等重点行业领域。
- **管理范围**：

企业：主要包括联网工业企业、平台企业、标识解析企业**三类**工业互联网企业类型。

- **防护范围**：保障工业互联网**相关设备、控制、网络、平台、应用、数据**等的**网络安全**。
- **职责范围**：

地方工信主管部门和地方通信主管部门联合，分别指导本行政区域内联网工业企业和平台企业、标识解析企业开展网络安全分类分级工作。

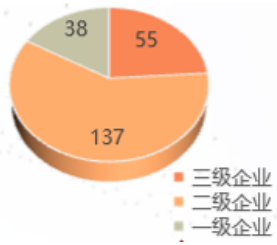
试点工作顺利完成成效显著

分类分级管理政策发挥引领作用

- 试行**《工业互联网企业网络安全分类分级管理指南》**及系列标准规范，分类分级管理工作思路得到落地应用。
- 验证了工业互联网企业网络安全分类分级管理设计的科学性、可操作性，为**全面摸清底数，了解风险状况**奠定工作基础。

初步形成重点企业清单

- 指导试点企业系统梳理数字化、网络化、智能化应用程度，围绕钢铁、石化、装备、汽车等行业差异化属性及网络安全风险影响等要素开展科学定级。



2023 年工业互联网企业网络安全分类分级工作启动

2023年9月21日，省工业和信息化厅、省通信管理局联合印发《关于开展2023年工业互联网企业网络安全分类分级管理工作的通知》，正式启动2023 年工业互联网企业网络安全分类分级管理工作。

江苏省工业和信息化厅
江苏省通信管理局 文件

苏工信信发〔2023〕406 号

省工业和信息化厅 省通信管理局
关于开展 2023 年工业互联网企业网络安全
分类分级管理工作的通知

各设区市工信局，各有关单位：

为贯彻落实《江苏省关于加强工业互联网安全工作的实施意见》《江苏省“十四五”工业信息安全保障体系建设规划》《江苏省制造业智能化改造和数字化转型三年行动计划（2022—2024年）》等文件精神，持续推进我省工业互联网安全分类分级管理体系建设，进一步提升工业互联网企业网络安全防护水平，现决

明确工作目标

■ **完成新增网络安全分类分级管理企业不少于60家**

2023 年全省新增不少于 60 家以上工业互联网企业纳入分类分级管理，组织 50 家以上企业完成安全防护整改，遂选一批分类分级管理优秀企业和典型案例。

明确组织方式

■ **组织单位：**

省级工信主管部门联合通信管理局共同组织实施

■ **支撑机构：**

中国信通院等部属单位

工作目的

以强化企业网络安全管理和防护能力为目标，**以评促建、以评促管、以评促改、以评促防**，增强企业网络安全意识，推动企业落实**网络安全主体责任**，提高**网络安全基础水平和防护能力**，预防和减少网络安全事件，保障企业安全平稳运行，**推动企业建立自主定级、对标防护、风险评估、安全建设的安全工作闭环。**

■ 落实安全责任，探索安全机制

- ✓ 工业互联网处于快速发展过程中，其中应用服务APP、人工智能、云平台等技术应用更新较快，通过开展安全评估工作，探索形成“以评促建、以评促管、以评促改、以评促防”的网络安全工作长效机制。
- ✓ 推动企业建立自主定级、对标防护、风险评估、安全建设的安全工作闭环。

■ 推动企业安全建设工作

- ✓ 安全检测评估是企业安全建设的起点和基础
- ✓ 安全检测评估是加强网络安全保障体系建设的关键环节
- ✓ 重视安全检测评估是规划建设安全体系的基本依据

- ✓ **发现风险和威胁**
- ✓ **加强整改和建设**
- ✓ **强化合规和能力提升**
- ✓ **保障重点战略实施和企业长远发展**

目标对象

定级对象

工信部主管行业范围内的工业互联网企业：

三类企业

联网工业企业：
主要是指将新一代信息通信技术与工业系统深度融合，推动企业网络化、智能化升级，实现智能控制、运营优化和生产组织方式的变革，主要涉及原材料工业、装备工业、消费品工业和电子信息制造业等行业；

平台企业：
主要指面向工业企业提供云服务等资源协作、信息服务及应用（工业APP）服务等的企业；

标识解析企业：
主要指从事工业互联网标识注册服务、解析服务及其运行维护的机构。

等级划分

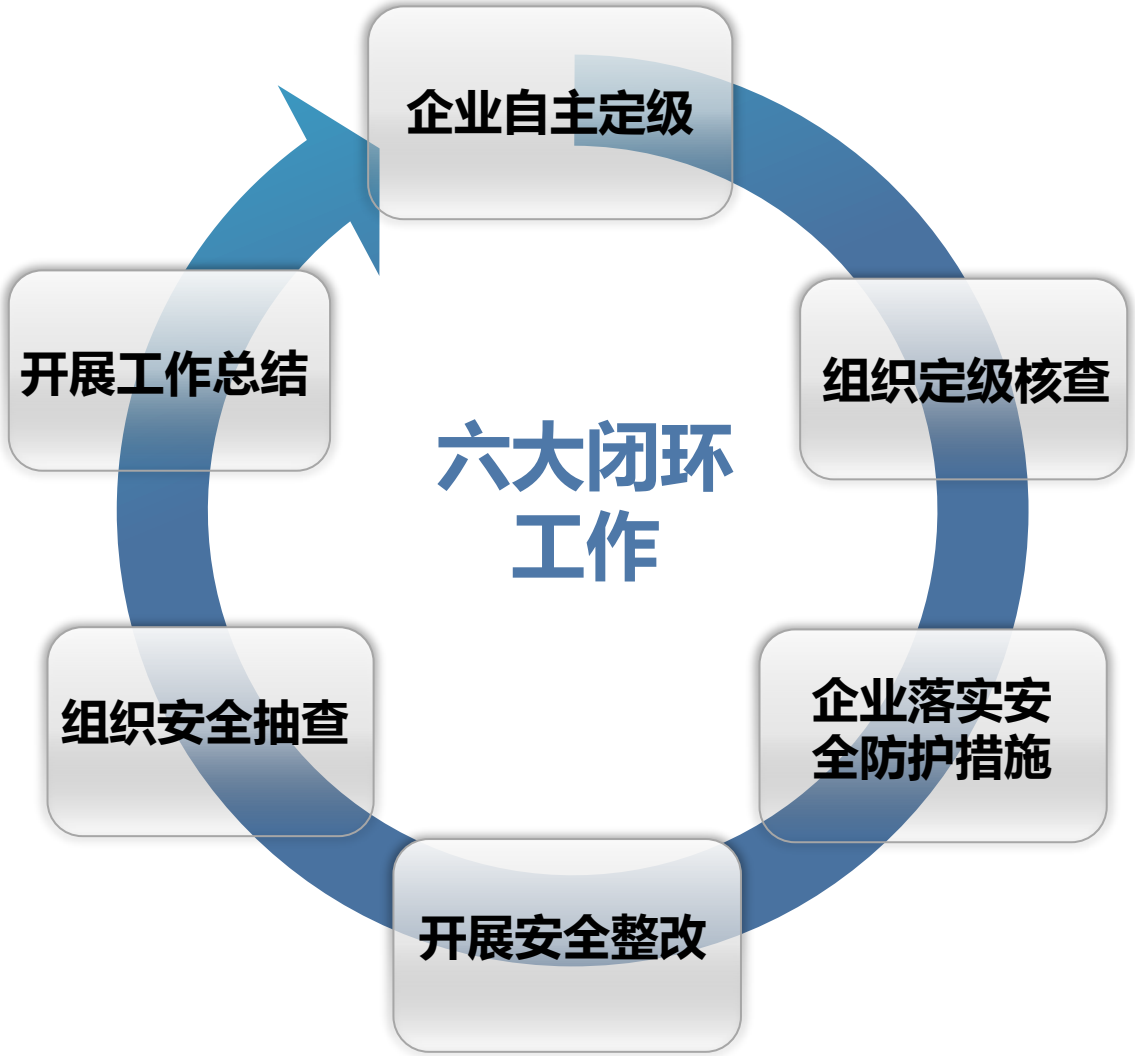
采用计分方式，将企业网络安全等级由高到低划分为三级、二级、一级：

三级企业：
评分大于等于80分

二级企业：
评分大于等于60分，小于80分

一级企业：
评分小于60分

工作流程



关键时间节点

2023年11月20日

■ 企业于 10 月30 日前完成管理平台注册及基础信息填报工作，**开展自主定级**，于11月 20 日前将自主定级报告上传管理平台。

2023年12月20日

■ 各设区市工信局组织第三方专业机构开展**定级核查**，于12 月20日前在管理平台完成属地企业网络安全定级结果审核确认。

2023年12月底

■企业自行或委托第三方专业机构开展标准**自主安全评估**，形成评估报告并上传至管理平台。

■年底前，省工业和信息化厅联合省通信管理局组织第三方专业机构开展**企业安全抽查，**并要求企业完成整改。

2024年1月底

■各设区市工信局督促企业**落实防护规范**，并于1月底前将安全防护落实情况上传至管理平台。

2024年1月30日

■各设区市工信局结合开展分类分级**工作总结**，推荐一批典型企业及优秀案例，于 1 月30 日前报送省工业和信息化厅。

各环节主要工作内容—自主定级，依据定级方法

试点企业根据《工业互联网企业网络安全分类分级评定规则》中提供的定级方法开展自主定级，完成各**定级要素评分**，确定**企业级别**，完成**定级报告**并提交主管部门。

定级方法

联网工业企业

- 企业所属行业网络安全影响程度（20分）（**三类、二类、一类行业**）
- 企业规模（20分）（**大型、中型、小微**）
- 企业应用工业互联网的程度（30分）（**高、较高、较低**）
- 企业发生网络安全事件影响程度（30分）（**重大影响、较大影响、一般影响**）

平台企业

- 企业平台服务行业网安影响程度（20分）（**服务三类、二类、一类行业**）
- 平台业务范围（20分）（**覆盖行业数量，大、中、小范围**）
- 平台业务规模（30分）（**大、中、小规模**）
- 企业发生网络安全事件影响程度（30分）（**重大影响、较大影响、一般影响**）

标识解析企业

- 建设运营**国家顶级节点**的为三级;
- 建设运营**二级节点、公共递归节点**的为二级;
- 建设运营**企业节点**的为一级
- 建设运营不同级别节点的，**依据较高级别确定**.

多重属性企业

同时具有联网工业企业、平台企业、标识解析企业中**两种及以上属性**的企业，按照**业务活动涉及的不同属性分别定级。**

各环节主要工作内容—自主定级，提交定级报告

企业根据《工业互联网企业网络安全分类分级定级报告》模板撰写定级报告，模板中概括了企业在级别评定中需要综合考虑的指标要素，同时也为政府核查企业网络安全情况提供基本参考。

定级报告模板

01 企业基本情况

概述企业工业互联网相关业务规模范围、服务对象及类型，安全管理情况，安全技术建设情况。

02 各定级要素描述及分值确定

联网工业企业、平台企业、标识解析企业具体定级的参考要素说明及各要素对应的评分情况

03 企业网络安全等级确定

综合考虑各定级要素分数，并结合指南评定规则，确定企业网络安全等级。

提交定级报告

企业类型	定级要素得分				总分	安全等级
联网工业企业						
平台企业						
标识解析企业	（节点级别）					

自主定级-实施案例分析

以某联网工业企业为例，依据定级规则开展自主定级流程如下：

梳理企业基本情况

✓ **基本情况：**某钢铁行业联网工业企业主干网已覆盖各分子公司以及钢铁板块全部办公和生产区域，建立了完整的信息化五层架构体系，工序级数采控制站，可接入工业控制系统、仪表及传感器，设备产线数字化率达到65%，生产工艺自动化配置达95%以上。

✓ **网络安全情况：**企业建设了集中化安全监测平台，该平台可发现整个工业企业中安全的趋势和态势，从多种事件和具有上下文信息的安全日志中收集和分析安全事件。可实现安全保障的关口前移，防患于未然。

自主定级-实施案例分析

依据定级规则对四个定级要素分别评分：

定级要素一评分　企业所在行业网络安全影响程度（20分）

✓ 企业所在行业：钢铁行业 ➡ 三类行业 ➡ 得分：18分

根据企业所在行业网络安全风险程度，将企业所在行业网络安全影响程度由高到低可划分为三类行业、二类行业和一类行业（见附录）。	
企业属于三类行业	≥18
企业属于二类行业	15分-18分
企业属于一类行业	≤15分

工业互联网行业网络安全影响程度分类目录

序号	行业名称	行业门类及代码
三类行业		
1	石化化工	石油、煤炭及其他燃料加工业 化学原料和化学制品制造业（除日用化学品制造）
2	钢铁	黑色金属冶炼和压延加工业
3	有色	有色金属冶炼和压延加工业
4	轨道交通装备	铁路运输设备制造 城市轨道交通设备制造
5	船舶及海洋工程装备	船舶及相关装置制造
6	航空航天装备	航空、航天器及设备制造

自主定级-实施案例分析

依据定级规则对四个定级要素分别评分：

定级要素二评分　企业规模（20分）

根据工业企业从业人员数量、营业收入（或营业收入指标）、资产总额多少，可将企业分为大型企业、中型企业、小微企业（国家统计局《统计上大中小微企业划分标准（2017）》）。	
大型企业：从业人员＞1000人；营业收入＞40000万元	≥18分
中型企业：300人≤从业人员≤000人；2000万元≤营业收入≤40000万元	15分-18分
小微企业：从业人员＜300人；营业收入＜2000万元	≤15分

- ✓ 企业从业人员：2000人
- ✓ 企业营业收入：80000万元

大型企业

得分：18分

自主定级-实施案例分析

依据定级规则对四个定级要素分别评分：

定级要素三评分　企业应用工业互联网的程度（30分）

根据企业工业化和信息化融合程度、互联互通程度、综合集成程度、数据分析利用程度等，判定企业应用工业互联网的程度为高、较高、较低（参考《工业企业信息化和工业化融合评估规范》（GB/T 23020-2013）；《工业互联网成熟度评估》）。

程度高	≥25分
程度较高	15分-25分
程度较低	≤15分

✓ **企业信息化建设及联网设备、系统情况：**企业围绕生产制造执行、能源管控等信息化建设，在各生产片区构建了昆钢全网的基础网络，共铺设光缆1270公里，建立工序级数采控制站59个(数采控制站：数据信号及控制信号双向传输)，离散数采站308个，接入工业控制系统698套，接入仪表及传感器85973套。公司主干网目前已覆盖各分子公司以及钢铁板块全部办公和生产区域，主干网带宽1G，与互联网接口带宽4G，拥有IBM 3850等各型号服务器111套，存储容量可达500T。

企业应用工业互联网程度高

得分：27分

自主定级-实施案例分析

依据定级规则对四个定级要素分别评分：

定级要素四评分 企业一旦发生工业互联网网络安全事件的影响程度（30分）

企业根据自身情况，判定一旦发生重大工业互联网网络安全事件后，对国家安全、社会秩序、经济运行、公众利益、人身安全及企业自身运行的影响程度，分为重大影响、较大影响、一般影响。	
重大影响：严重影响企业自身运行、造成特别重大人员伤亡，会对社会秩序、经济运行和公众利益造成严重损害，或对国家安全造成严重损害。	≥25分
较大影响：影响企业自身运行、造成重大人员伤亡，或对社会秩序、经济运行和公众利益造成较大损害，或对国家安全造成轻微损害。	20分-25分
一般影响：影响企业自身运行，造成轻微人员伤害，或对社会秩序、经济运行和公众利益造成轻微损害，不损害国家安全。	≤20分

- ✓ **企业一旦发生重大工业互联网网络安全事件后，对哪些客体造成侵害或影响及影响程度：**
- ✓ 本企业联网生产片区网络连接工业控制系统和仪表传感器等设备，一旦发生重大工业互联网网络安全事件后，会严重影响企业自身运行，可能会对社会秩序、经济运行等造成严重损害。

重大影响

得分：25分

自主定级-实施案例分析

依据等级划分规则，确定企业安全等级：

安全等级确定

序号	企业名称	各定级要素得分				企业得分	企业级别
		企业所在行业网络安全影响程度（满分20分）	企业规模（满分20分）	企业应用工业互联网的程度（满分30分）	企业一旦发生工业互联网网络安全事件的影响程度（满分30分）		
1	某钢铁有限公司	18	18	27	25	88	三级企业

企业开展分类分级核查需准备的材料

工业企业

- 营业执照复印件
- 对外的公开财报
- 企业人员名录
- 详细网络拓扑架构
- 企业资产台账（包含资产名称、资产类型、所在网络区域、IP地址等）
- 自动化投入与信息化投入资金预算证明材料
- 安全管理制度文档（如有）
- 风险评估报告（如有）
- 安全培训资料文档（如有）

平台企业

- 营业执照复印件
- 对外的公开财报
- 企业人员名录
- 详细网络拓扑架构
- 企业资产台账（包含资产名称、资产类型、所在网络区域、IP地址等）
- 平台服务行业类型、行业数量、接入用户数、接入设备数等证明材料
- 安全管理制度文档（如有）
- 风险评估报告（如有）
- 安全培训资料文档

标识解析企业

- 营业执照复印件
- 对外的公开财报
- 企业人员名录
- 详细网络拓扑架构
- 企业资产台账（包含资产名称、资产类型、所在网络区域、IP地址等）
- 标识解析用户量及业务量
- 安全管理制度文档（如有）
- 风险评估报告（如有）
- 安全培训资料文档

评估范围

评估内容主要从安全管理和安全技术两个层面进行。

安全管理评估

安全管理评估主要以访谈、查阅资料的方式进行。

安全管理类	安全管理子类
安全策略和管理制度	包含管理制度、安全策略、制度制修订等子类
安全管理机构和人员	包含岗位人员设置、授权审批、沟通合作、教育和培训等子类
安全建设管理	包含安全方案设计、产品采购和使用、软件开发、工程实施、供应商选择等子类
安全运维管理	包含环境管理、资产管理、安全审计、恶意代码防护、配置管理、安全事件和应急处置等子类
物理和环境安全	包含物理位置选择、物理访问控制、防盗窃和防破坏、温湿度控制、电磁防护等。

安全技术评估

三类企业的安全技术检查范围与内容有所不同，具体如下表：

企业类型	安全技术检查范围
联网工业企业	主要包括**工业企业应用工业互联网过程中所涉及的各类系统和数据**。涵盖企业业务应用系统，如ERP、MES等系统；工业控制系统，如SCADA、DCS、HMI等；现场控制设备,如PLC、RTU等；其他工业互联网相关设备，如数据采集网关、网络摄像头等。
工业互联网平台企业	**主要为工业互联网平台的各层级对象**，包括接入层（边缘接入设备、边缘计算环境等）、基础设施层（服务器操作系统、虚拟化组件、数据库、网络和安全设备等）、平台层（工业PaaS、微服务组件、资源管理平台、服务接口API等）、应用层（订阅的SAAS web应用、工业移动APP等）以及数据安全。
标识解析企业	主要包括**标识基础设施**（云计算资源管理平台、服务器操作系统、数据库、网络和安全设备等）、**网络安全**（网络结构、网络安全防护措施等）、**应用安全**（主要为标识应用）以及**数据安全**。

评估内容

安全评估内容包括对**三类企业**的**法律法规落实、安全管理**及**安全防护技术手段落实情况**以及**安全漏洞隐患情况**等。

选择评估指标

**按照企业级别选择相应的评估指标*

- 三级企业 → **增强级**
- 一、二级企业 → **基本级**
- 未定级企业 → 充分评估其可能存在的网络安全风险，根据实际情况结合相关规范要求进行评估

安全检查评估

安全管理评估内容

- ✓ 检查企业安全管理策略、安全机构设置、人员配备、安全责任落实情况、应急机制建立、安全建设管理和安全运维管理等方面的标准符合性情况
- ✓ 机房和中控室等现场物理环境的安全

安全技术评估内容

- ✓ 检查企业工控系统、工业互联网平台、标识解析等系统涉及的主机、网络、应用、数据等的安全基线配置情况及标准符合性情况
- ✓ 利用漏洞扫描和渗透测试等方法，发现系统可能存在的漏洞等网络安全隐患

◆ **针对实时性和可用性要求较高的DCS、PLC等工控系统**，安全漏洞隐患主要借助专用的工业互联网安全评估评测工具进行无损漏洞探测，并结合可控的人工渗透方式。同时利用被动流量分析等手段，发现病毒、木马等影响工业网络安全的恶意代码。

风险评估企业需配合事项

为做好评估实施和保障工作，需要企业指派专人统筹协调，做好工作安排、协调相关事项和问题，确保评估工作有序开展。

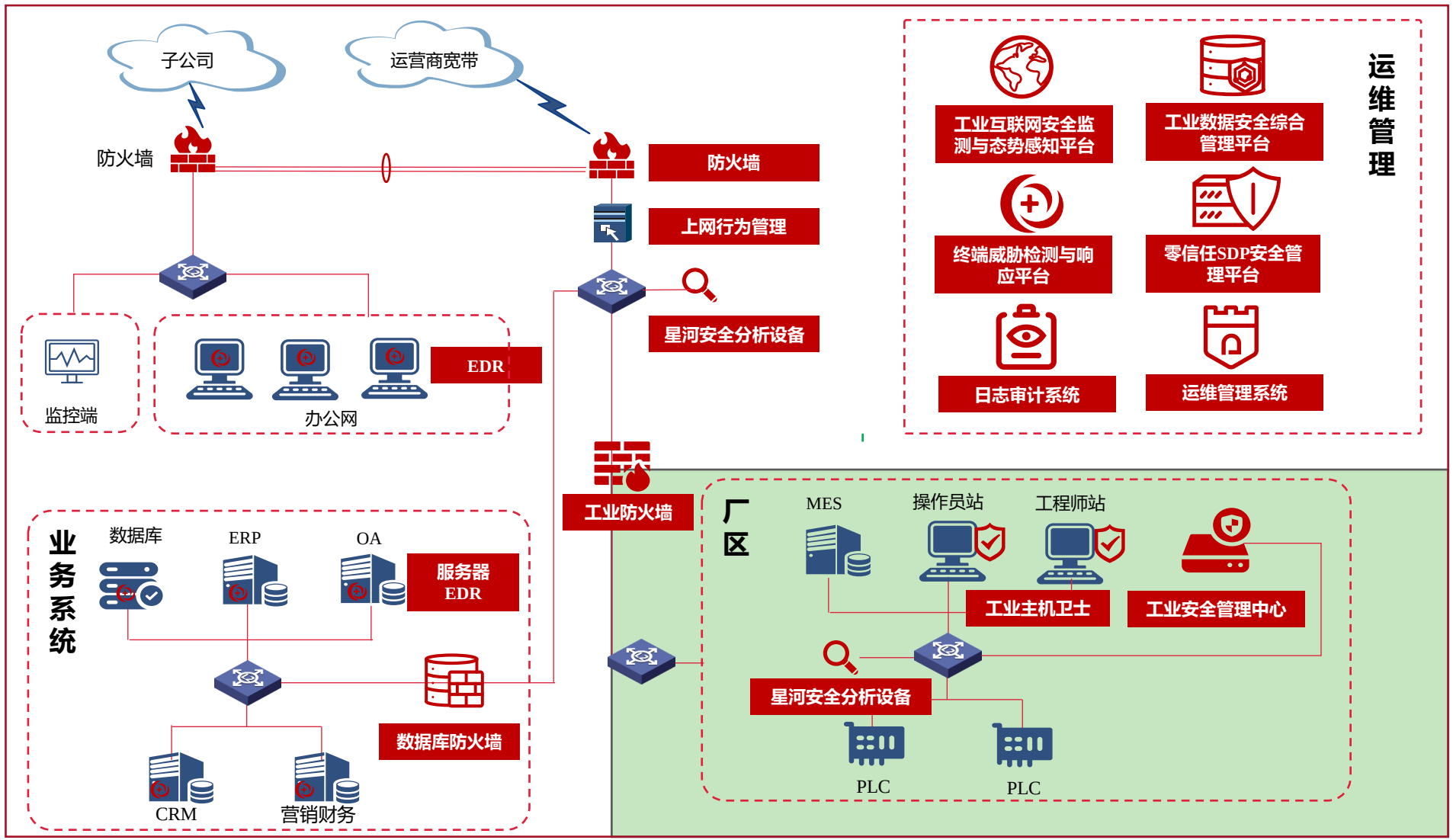
人员对接和配合

1. 企业指派**1名评估工作总体对接人**，需熟悉相关被测系统及对应的对接人员，确保做好调研沟通、组织协调和进度质量控制等工作。
2. 现场评估时，需相关单位、场站或系统的**安全管理员、系统开发和部署人员、安全运维**等人员参与。
3. 需相关参与评估人员尽可能提供相关材料或反馈回复相关情况，后期将直接体现进评估报告中。

环境准备和对接

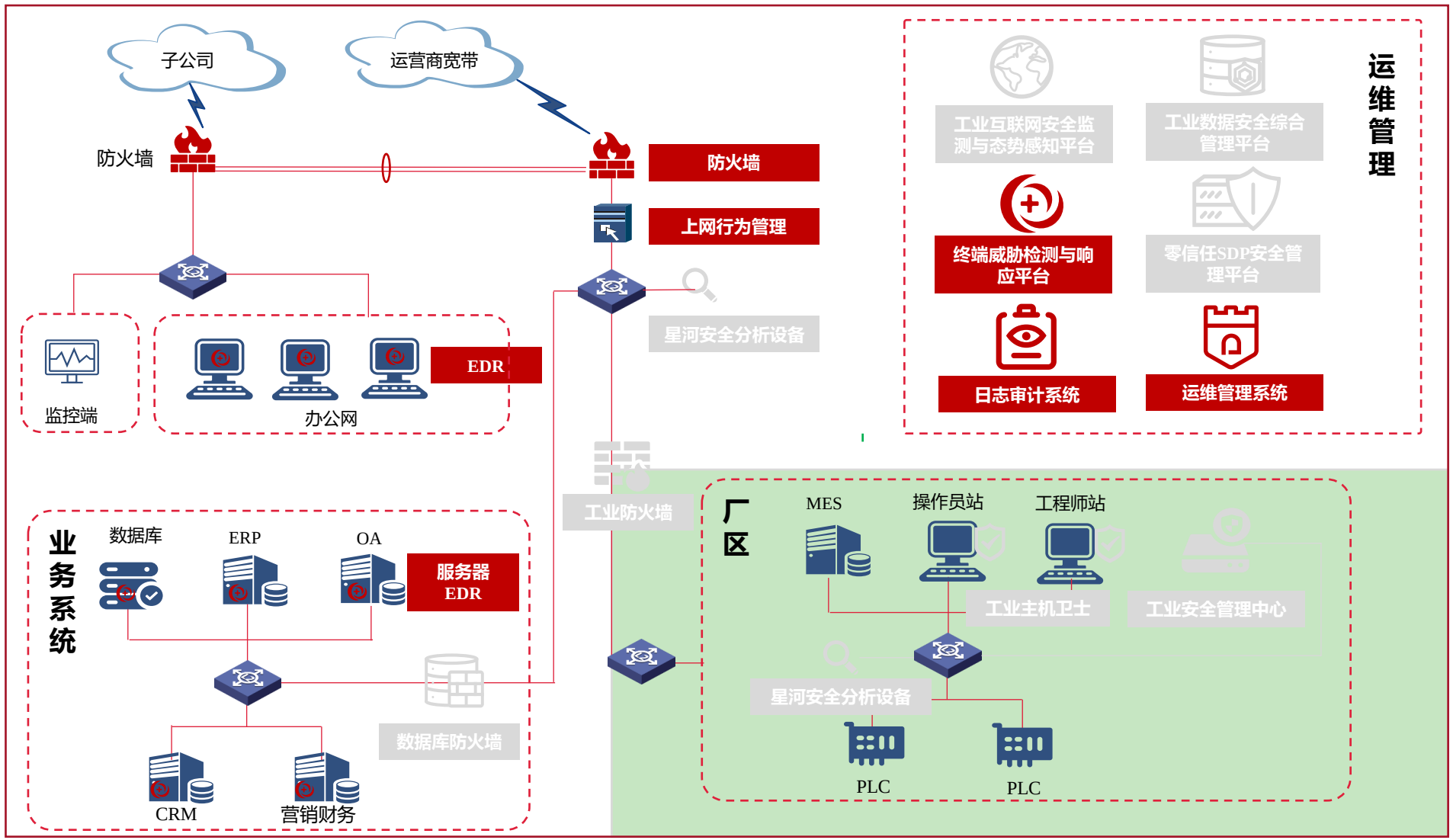
1. 提供一定的专用办公场地；
2. 提供互联网及企业内网接入环境。
3. 企业梳理实施团队开展评估所需遵守的**审批程序，针对评估内容是否有不可协调事项（如被测应用系统无法提供测试账号，被测系统评估需领导审批）**，反馈评估工作需审批和协调事项。

工业互联网企业网络安全分类分级典型建设方案



- 建立基本安全保障能力
- 构建企业级安全大脑
- 形成围绕数据全生命周期的安全能力
- 建立主机安全加固与病毒防御能力
- 建立基于零信任的身份控制机制
- 构建场景化的工控网络安全防护能力

建立基本安全保障能力——满足等保2.0要求



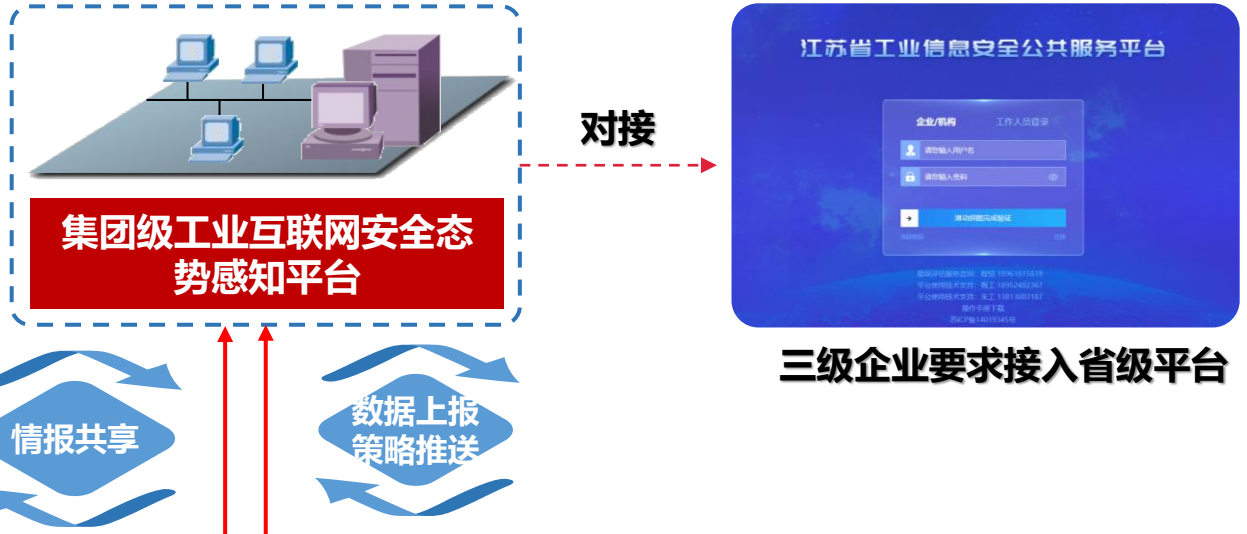
- 建立基本安全保障能力
- 构建企业级安全大脑
- 形成围绕数据全生命周期的安全能力
- 建立主机安全加固与病毒防御能力
- 建立基于零信任的身份控制机制
- 构建场景化的工控网络安全防护能力

建立企业级安全大脑——安全可视可知可控

◆工厂侧部署星河安全分析设备进行工业流量预处理后上送工业安全管理中心分析研判；

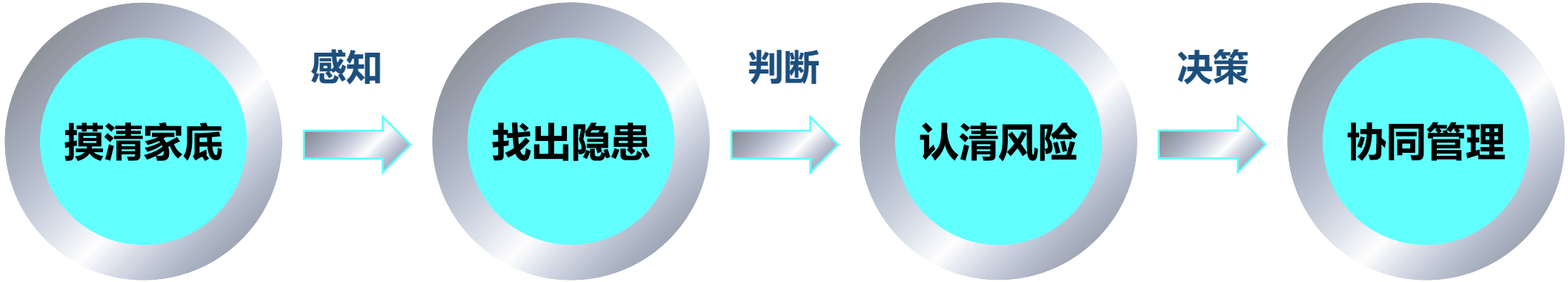
◆集团侧部署工业互联网安全监测与态势感知平台对接各个工厂安全管理中心的数据进行集团级的态势感知和分析；

◆对于第三方的探针设备，我们提供工业数据安全接入认证设备进行对接处理，之后再接入我司的工业互联网安全监测与态势感知平台



建立企业级安全大脑——安全可视可知可控

威胁处置



- 资产自动感知
- 拓扑自动绘制

- 资产脆弱性分析
- 资产威胁关联

- 异常监测告警
- 威胁事件分析
- 攻击行为还原

- 日志统一审计
- 事件协同处置

安全运营

- 安全报告生成
- 合规自评

- 资产脆弱性情况
- 内外部威胁分析

- 安全咨询、风险评估
- 应急响应、结果汇报

建立企业级安全大脑——安全可视可知可控

内部网络威胁一张图

外部网络威胁一张图

数据资产一张图

资产脆弱性评估一张图

外联流量一张图

数据资产理得清、安全威胁管得好

© SINOVATIO Corporation. All rights reserved.

形成围绕工业数据全生命周期的安全能力

数据分类分级	敏感数据地图	数据库脆弱性评估	API安全监测	数据流转行为画像	数据安全事件监测
跨境数据安全检查	数据扫描任务	数据分类分级	数据复核	数据安全策略配置	数据安全态势感知

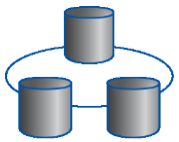
SALAXY 星河
数据安全管理平台

安全策略下发 联防联控

数据采集	数据传输	数据存储	数据分析	数据共享	数据防泄漏	数据删除
数据源认证	传输加密	分类分级	数据脱敏	数据脱敏	终端防泄漏	精准删除
数据收集 合规检测	敏感数据加密	数据加密	多方安全计算	安全审核	网络防泄漏	匿名化
		数据组件安全	联邦学习	API安全	邮件防泄漏	数据销毁

数据安全能力组件

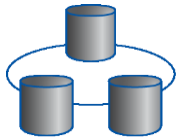
进不来



分级分类访问控制

- 敏感数据和非敏感数据等分级分类管理
- 访问控制精确颗粒度
- 登录安全审计

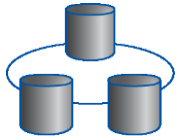
拿不走



权限控制职责分离访问隔离

- 最小权限原则，访问隔离原则
- 职责分离，防止合谋
- 流量安全审计

看不懂



数据加密数据脱敏

- 核心数据不出生产中心并全路径加密
- 出了生产中心必须映敏
- 操作和安全审计

建立主机安全加固与病毒防御能力

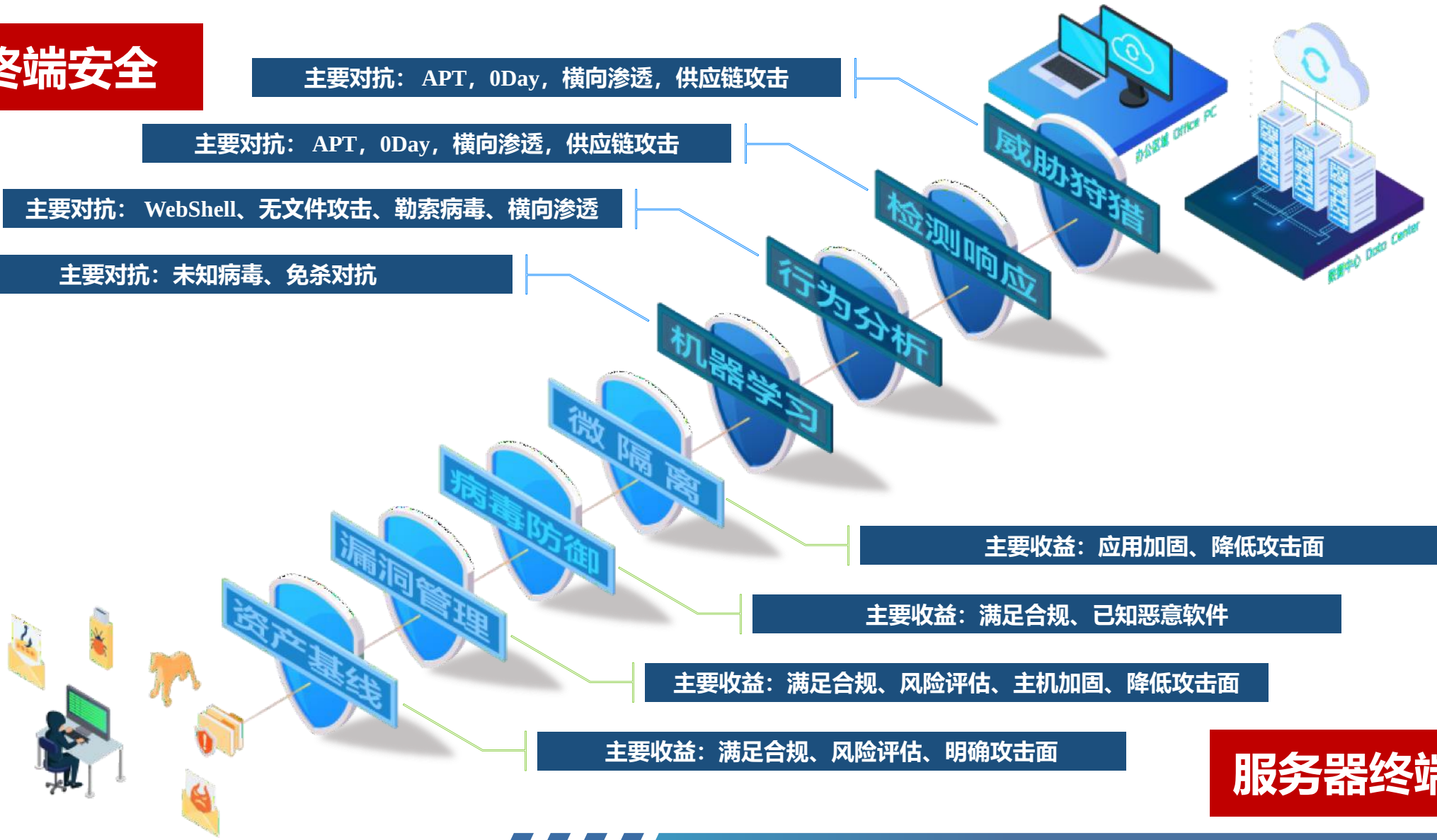
办公终端安全

主要对抗： APT，0Day，横向渗透，供应链攻击

主要对抗： APT，0Day，横向渗透，供应链攻击

主要对抗： WebShell、无文件攻击、勒索病毒、横向渗透

主要对抗：未知病毒、免杀对抗



主要收益：应用加固、降低攻击面

主要收益：满足合规、已知恶意软件

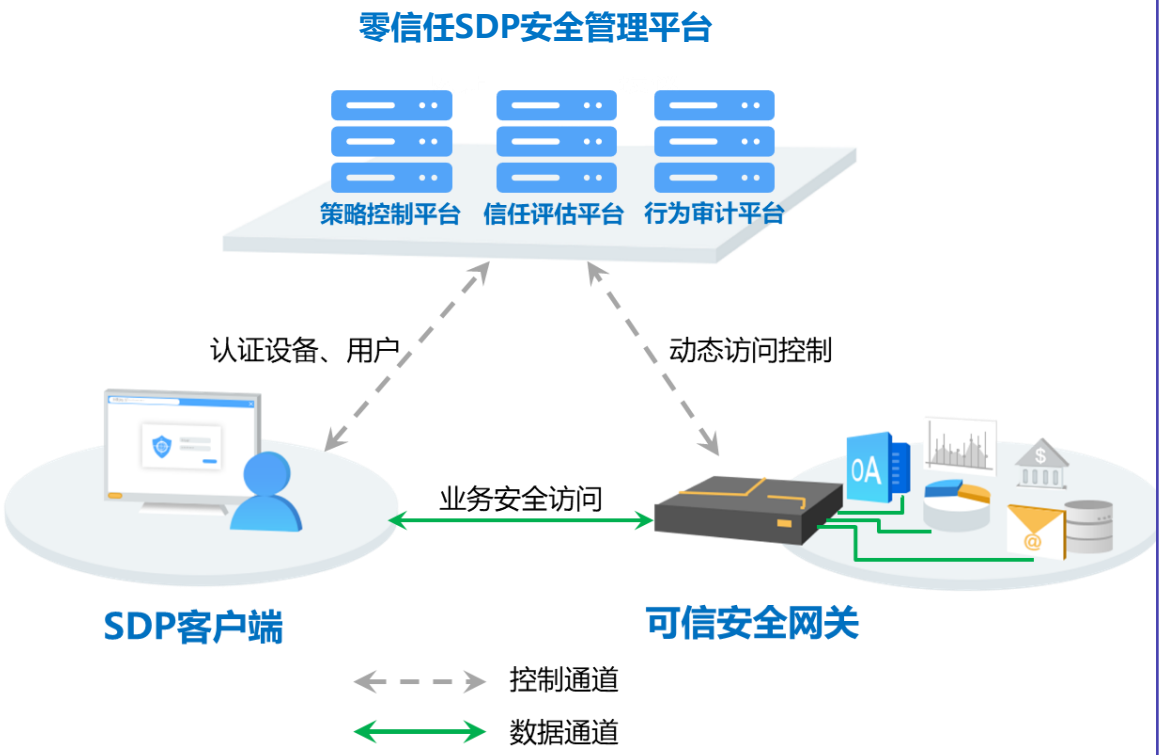
主要收益：满足合规、风险评估、主机加固、降低攻击面

主要收益：满足合规、风险评估、明确攻击面

服务器终端安全

建立基于零信任的身份控制机制

通过基于**零信任理念的SDP（软件定义边界）网络隐身技术**，使企业数据“隐身”于互联网之中，只对授权用户可见，让黑客无从发起攻击，从而有效保护企业的数据资产，为企业提供真正可靠的、一站式的“云网一体化安全防护”。



应用场景

采用零信任安全访问技术构建安全访问体系，针对企业不同的访问场景，实现面向应用系统的业务安全访问。

1. **针对企业用户移动办公/远程办公，**用户无需配置即可访问内网应用和云端应用， 使用更便捷；
2. **针对企业合作伙伴/分公司访问内网业务系统，**基于身份“按需授权”安全策略，合作伙伴只能访问完成工作必须的应用，不暴露其他内网资源；
3. **针对企业业务上云，**只有身份、设备验证合法的授权用户才能正常访问云上业务系统；
4. **针对企业内网安全加固，**为每个用户都基于身份做了“微分段”，即使某个用户被病毒“攻陷”，也只会影响到其权限范围内的应用，对其他应用没有影响。

构建场景化的工控网络安全防护能力

安全区域边界-边界防护

解决方案

在工程师站、操作员站与生产线的控制环网之间部署工业防火墙。

解决的问题

1）阻止来自外部系统攻击行为;

2）阻止不同系统之间的越权访问行为；

3）阻止病毒、蠕虫恶意软件扩散和入侵攻击保护控制系统安全运行;

4）阻止非授权设备的接入;

安全通讯网络-安全审计

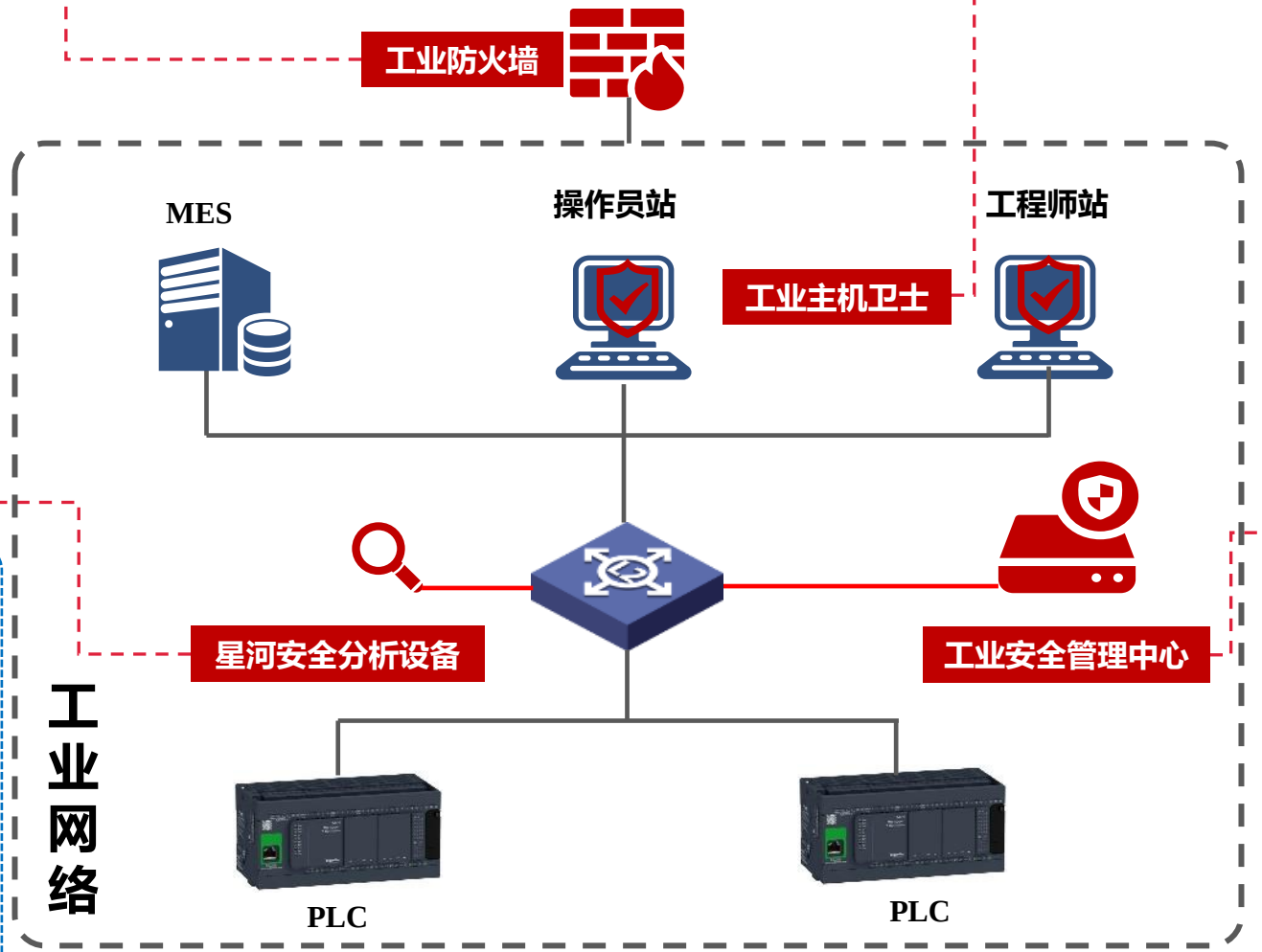
解决方案

在生产线各控制环网关键节点旁路部署星河安全分析设备。

解决的问题

1）实时监测工控网络中的恶意攻击、误操作、违规行为、非法设备接入以及蠕虫、病毒等恶意软件的传播，帮助客户及时采取应对措施·避免发生安全事故;

2）详实记录一切网络通信流量,包括网络连接、网络协议、网络会话、工控协议指令等，为安全事故调查取证提供技术支撑;



安全计算环境-主机防护

解决方案

在操作员站、工程师站等关键控制设备安装工控主机卫士。

解决的问题

1）对USB、网卡等外设进行白名单认证，仅允许白名单内的外设与主机连接，并对其进行读写、只读、不可访问细颗粒度控制。

2 ） 阻止非授权软件或进程的安装和运行，防止恶意代码攻击“0-day” 漏洞的利用 ;避免升级病毒库，变被动为主动； 防止操作员使用移动介质带入病毒在业务网中扩散

安全管理中心-安全感知

解决方案

在生产线控制网部署工业安全管理中心解决的问题。

解决的问题

1）资产管理：实现企业内资产发现、管理、安全监测以及可视化展示等。

2）风险监测：支持12大类，6万余种威胁检测以及上千种工控风险监测。

3）安全感知：实时掌握网络安全态势，及时掌握网络安全威胁、风险和隐患。

企业开展分类分级意义

满足分级分类合规需求，完成相关政府部门要求的试点建设工作

对平台的推广有重要的意义，可充分说明平台的安全性，有助于打消企业上平台的安全顾虑

建立一套完善的工业互联网安全管理与监测体系，有效保障企业网络与业务安全

定期的安全人员培训与省级平台的公共服务，为企业安全赋能

有效提升企业安全事件应急响应处理能力，降低安全事件造成的危害与经济损失；

后续工信部将为企业进行安全优秀示范企业等贯标贯名，提升公司知名度

可在申报工信部、工信厅等专项资金项目可占得先机

后续可能会有政府资金补贴，直接受益

往年中新赛克分类分级成果展示

分类分级工作部署启动会

现场核查

出具安全风险评估报告

- 工业互联网企业网络安全分类分级评估报告汇总-玄元科技.docx
- 工业互联网企业网络安全分类分级评估报告汇总-奥赛康药业.docx
- 工业互联网企业网络安全分类分级评估报告汇总-大全集团.docx
- 工业互联网企业网络安全分类分级评估报告汇总-海伦哲车辆.docx
- 工业互联网企业网络安全分类分级评估报告汇总-红太阳股份.docx
- 工业互联网企业网络安全分类分级评估报告汇总-济川药业.docx
- 工业互联网企业网络安全分类分级评估报告汇总-科远智慧.docx
- 工业互联网企业网络安全分类分级评估报告汇总-朗坤智慧.docx
- 工业互联网企业网络安全分类分级评估报告汇总-龙城精锻.docx
- 工业互联网企业网络安全分类分级评估报告汇总-擎天科技.docx
- 工业互联网企业网络安全分类分级评估报告汇总-盛虹石化.docx
- 工业互联网企业网络安全分类分级评估报告汇总-宿迁南钢.docx
- 工业互联网企业网络安全分类分级评估报告汇总-索普化工.docx
- 工业互联网企业网络安全分类分级评估报告汇总-沃得农机.docx
- 工业互联网企业网络安全分类分级评估报告汇总-洋河酒厂.docx
- 工业互联网企业网络安全分类分级评估报告汇总-中天互联.docx

出具安全整改方案

- 工业互联网企业网络安全分类分级整改方案_擎天科技.pdf
- 工业互联网企业网络安全分类分级整改方案_海伦哲.pdf
- 工业互联网企业网络安全分类分级整改方案_红太阳股份.pdf
- 工业互联网企业网络安全分类分级整改方案_索普化工.pdf
- 工业互联网企业网络安全分类分级整改方案_亲申车业.pdf
- 工业互联网企业网络安全分类分级整改方案_玄元科技.pdf
- 工业互联网企业网络安全分类分级整改方案_奥赛康药业.pdf
- 工业互联网企业网络安全分类分级整改方案_大全集团.pdf
- 工业互联网企业网络安全分类分级整改方案_济川药业.pdf
- 工业互联网企业网络安全分类分级整改方案_科远智慧.pdf
- 工业互联网企业网络安全分类分级整改方案_朗坤科技.pdf
- 工业互联网企业网络安全分类分级整改方案_龙城精锻.pdf
- 工业互联网企业网络安全分类分级整改方案_盛虹石化.pdf
- 工业互联网企业网络安全分类分级整改方案_宿迁南钢.pdf
- 工业互联网企业网络安全分类分级整改方案_沃得农机.pdf
- 工业互联网企业网络安全分类分级整改方案_洋河酒厂.pdf
- 工业互联网企业网络安全分类分级整改方案_中天互联.pdf
- 工业互联网企业网络安全分类分级整改方案_蒙光云.pdf

中新赛克分类分级项目案例——某石化集团

项目背景

该石化集团坚持炼化一体、高端石化全产业链均衡发展，是国家七大世界级石化产业基地中极具竞争力的支柱品牌。
在工业互联网企业网络安全分类分级试点项目中，该集团在中新赛克的指导下完成了企业工业互联网安全风险的摸排，并结合集团数字化转型战略，从顶层设计上融入安全建设规划，满足分类分级要求。

服务方案

- 通过零信任技术构建了企业级的身份安全与数据安全能力体系，保障业务访问与数据安全；
- 强化工业网络边界安全、工业主机安全、工控安全审计等能力，实现工控威胁“进不来、拿不走、跑不掉”！
- 建设企业安全管家，实现企业的网络安全、数据安全、工控安全、主机安全、应用安全的统一管理，完善持续化安全运营机制。

建设效果


7*24h代运维


定期健康体检


集中安全培训


安全应急演练

中新赛克分类分级项目案例——某电气设备制造商

项目背景

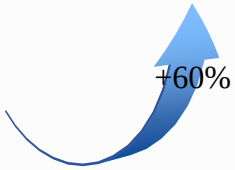
该公司是电气、新能源、轨道交通领域的领先制造商，主要研发生产中低压成套电器设备、智能元器件、轨道交通设备、新能源硅材料等。
该公司按照工业互联网企业网络安全分类分级（二级）要求，在中新赛克的指导下梳理了公司当前存在的资产不清、互联网业务暴露广、缺乏工控安全防护手段等安全问题，积极完成了安全整改工作。

服务方案

1. **摸清家底：**企业所辖所有厂区实体资产、数据资产进行梳理和分类分级；
2. **找出漏洞：**对资产存在的漏洞和隐患进行排查，并整理修复措施和方案；
3. **认清风险：**对企业办公网和生产网的安全威胁事件进行实时监测与预警；
4. **协同管理：**协同企业安全管理制度、安全防护手段迅速实现威胁的处置；
5. **态势分析：**构建企业数据安全、网络安全、工控安全统一态势分析平台；

建设效果

处置高危威胁
502例



提升运维效率
约**60%**

避免重复安全投入
约**30**万元

THANKS!