奇安信
新一代网络安全领军者

中小企业如何做好工业互联网安全防护

工业控制系统安全国家地方联合工程实验室
奇安信集团 工业互联网事业部

2019-09-01

目录

工业互联网安全现状与趋势

中小企业面临的工业互联网安全挑战

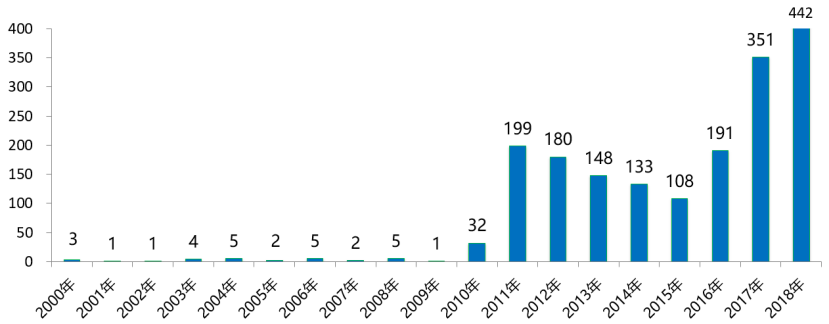
怎样的防护方案对中小企业更适用

中小企业工业互联网安全防护建议

安全漏洞数量快速增长，且高危漏洞呈高发态势

奇安信 新一代网络安全领军者

CNVD历年收录工控系统漏洞数量分布

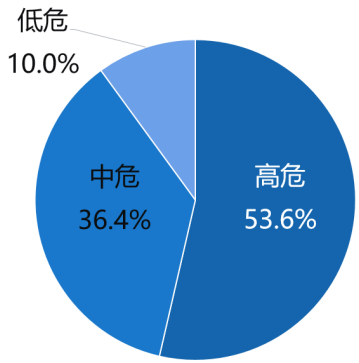


工业控制系统安全国家地方联合工程实验室

- CNVD漏洞平台2018年新增工控漏洞达到442个，创历史新高
- 工业互联网安全风险突出，安全态势严峻

- CVE、NVD、CNVD、CNNVD漏洞平台2018年收录的工控漏洞中，高危漏洞数量占比最高，达到53.6%

2018工控系统新增漏洞危险等级分布



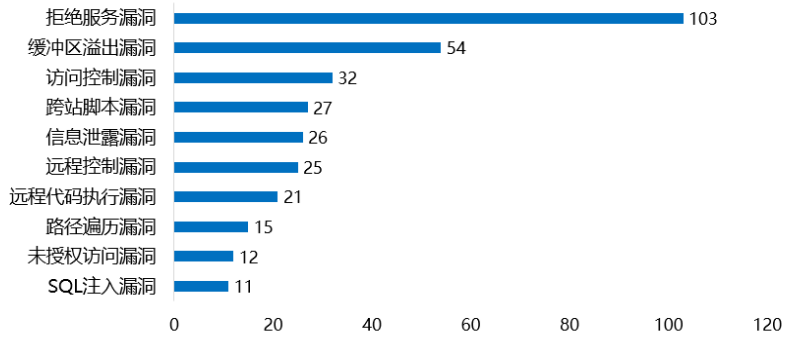
工业控制系统安全国家地方联合工程实验室

攻击手段多样化明显，目标以制造业、能源行业为主

奇安信 新一代网络安全领军者

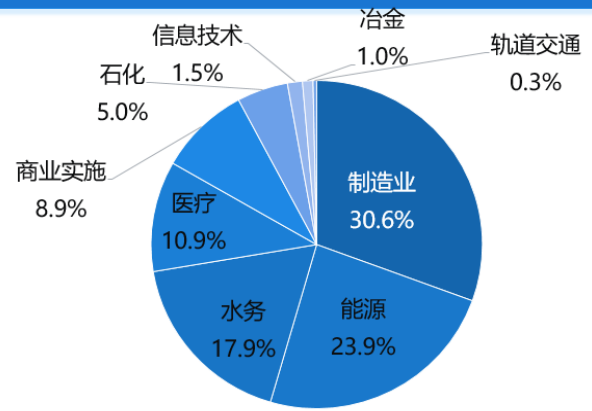
- 漏洞攻击类型多样化特征明显，技术类型多达30种以上
- 攻击者无论利用何种漏洞造成生产厂区的异常运行，均会造成严重的后果

工控系统新增漏洞类型分布（Top10）



工业控制系统安全国家地方联合工程实验室

工控新增漏洞行业分布



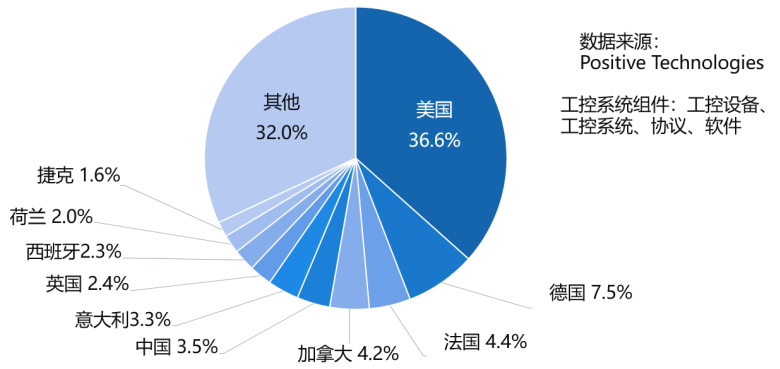
工业控制系统安全国家地方联合工程实验室

- 漏洞涉及行业广泛，以制造业、能源行业为主
- 制造业占比最高，高达30.6%，能源行业涉及的相关漏洞占比高达23.9%

工业系统互联网暴露设备数量增多，攻击面增大

奇安信 新一代网络安全领军者

世界各国工控系统组件联网暴露数量及比例分布

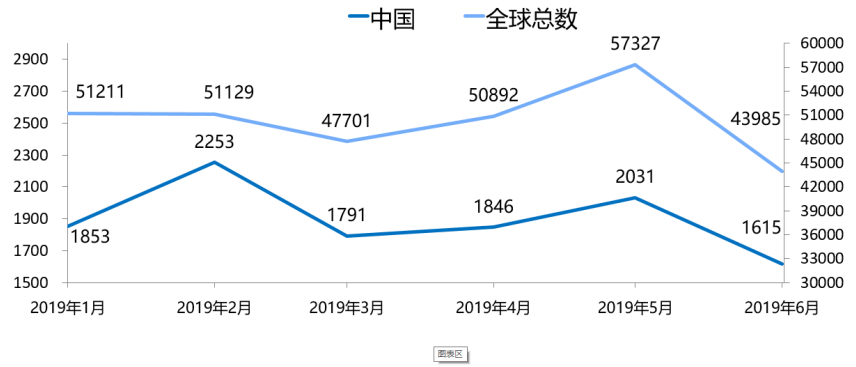


工业控制系统安全国家地方联合工程实验室

- 全球工控系统联网暴露组件总数量约为17.6万个，暴露数量增加明显
- 中国工控系统暴露数量为6223，占比3.5%，排名全球第五

- 以奇安信工业互联网安全大数据分析平台——哈勃平台统计，工控设备暴露数量基本处于稳定状态
- 工控设备：PLC、DCS、SCADA等设备

暴露在互联网上的工控设备数量变化情况

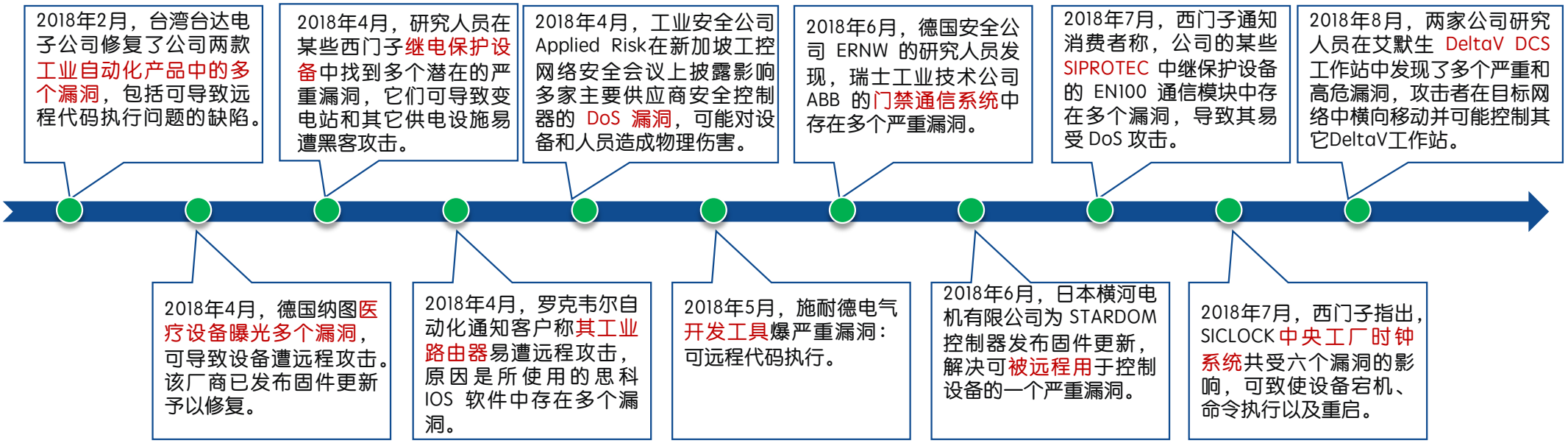


工控设备：PLC、DCS、SCADA等设备

工业控制系统安全国家地方联合工程实验室

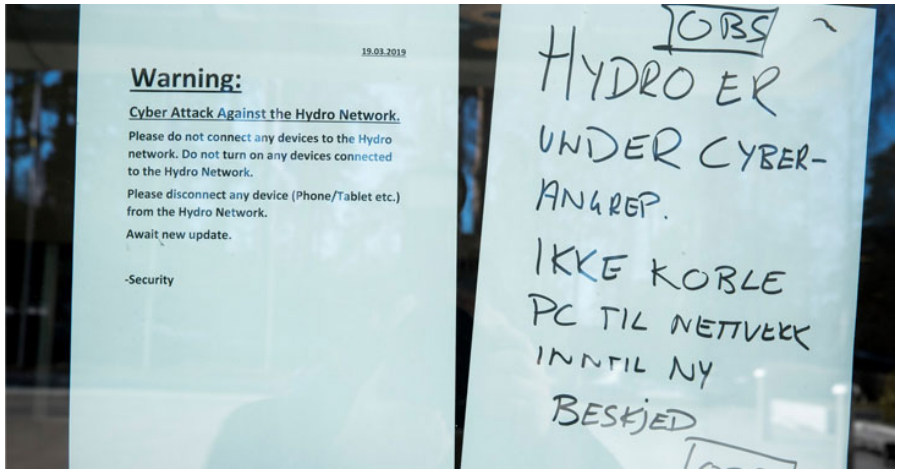
工业互联网安全事件层出不穷，整体形式严峻

奇安信 新一代网络安全领军者



大型企业停产，损失越来越大：海德鲁&驱动人生

奇安信
新一代网络安全领军者



- 8月3日，台积电因为安装新机台引入疑似“永恒之蓝”勒索病毒
- 数分钟内大规模攻击导致3个工厂停产，工业主机蓝屏重启
- 损失惨重：3天损失近2亿美元、毛利降1%
- 8月6日下午召开记者会：应对完毕。

- 3月19日 全球最大铝制造商 Norsk Hydro 欧美多工厂遭“大规模的网络攻击”，工厂操作模式改为手动模式
- LockerGoga勒索软件是本次感染的源头，可加密扩展名的文件：doc, dot, wbk...
- 全球现货市场铝价上涨超1%下,股价下跌近3%

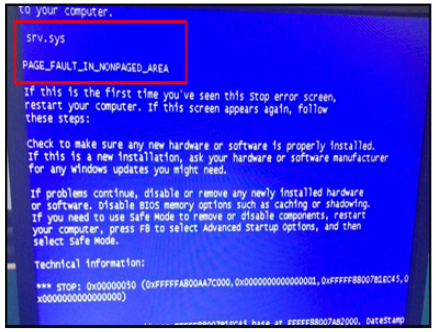
国内工业企业频繁遭到“永恒之蓝”&“挖矿”攻击

奇安信
新一代网络安全领军者

近两年奇安信应急响应过的工业企业网络攻击事件，涉及:汽车生产、智能制造、能源电力、烟草等行业， **工业主机成为最主要的攻击对象。涉及几十家企业，大多数都导致了工业主机蓝屏，文件加密，生产停工**

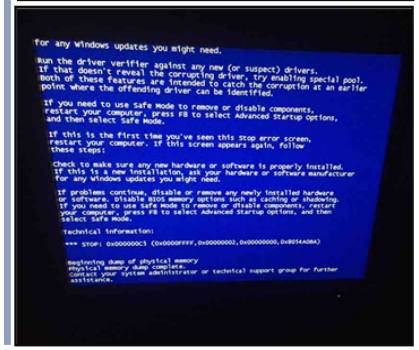
某汽车模具厂，停产

2017.05



某冷轧钢板厂，停产

2018.07

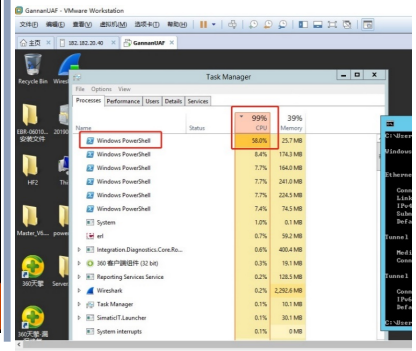


某炼钢厂，停产

2018.10

某关键IC厂，停产

2019.01



某奶粉企业，停产

2019.04

安全事件：某智能制造企业遭网络攻击停产

奇安信 新一代网络安全领军者

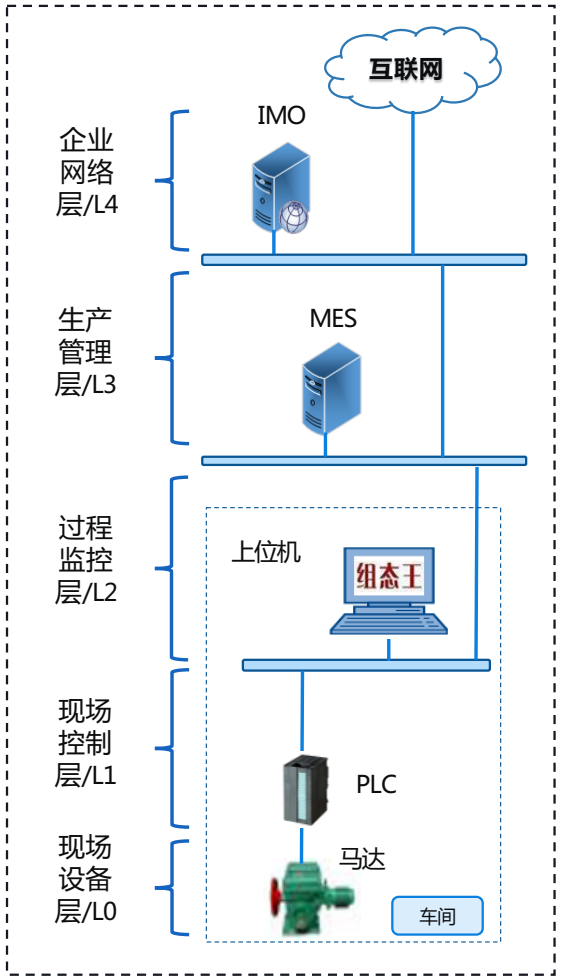
事件过程

2018年9月，某大型智能制造企业遭勒索病毒攻击，数十台工业主机蓝屏重启，多条生产线停产，损失严重。

奇安信工业安全提供紧急安服响应，帮助快速恢复生产。通过对现场网络安全风险评估，发现多个安全漏洞。

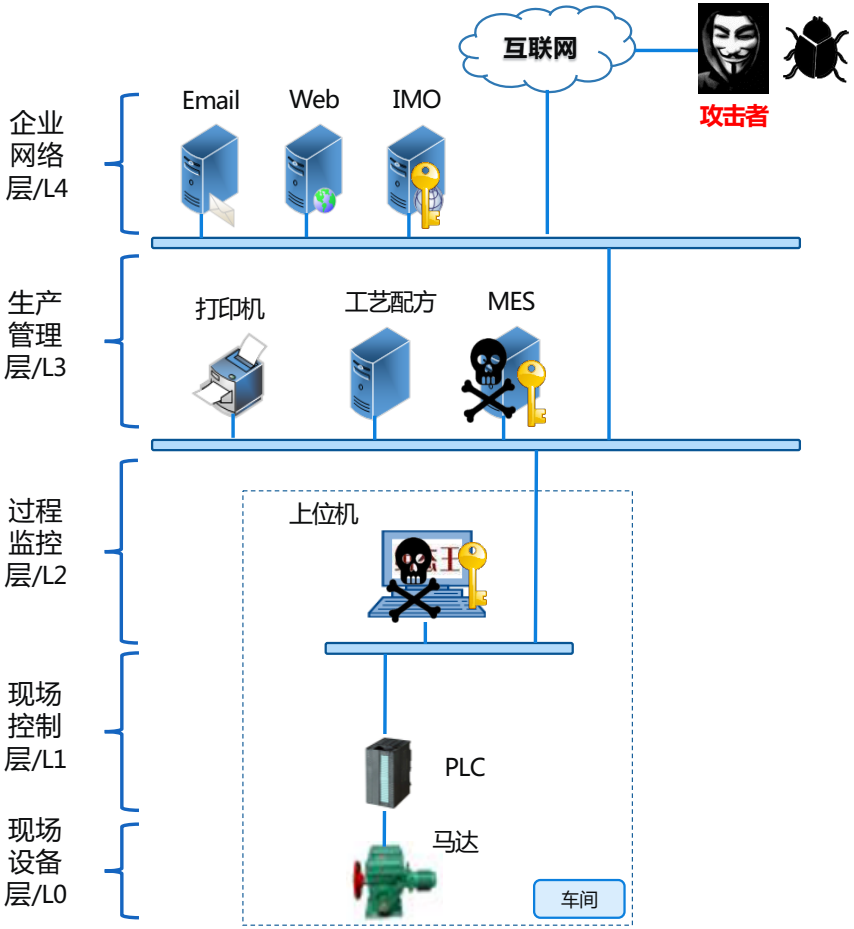
在实验室仿真客户环境，还原攻击过程。

设备	用途	系统配置	存在漏洞
IMO	OA服务器	CentOS	任意命令执行漏洞
MES	生产管理服务器	Win7 64位	“永恒之蓝”漏洞
上位机	控制PLC	WinXP SP3，组态王，双网卡配置	远程堆溢出漏洞
PLC	控制器	西门子300	拒绝服务漏洞



工控安全事件回顾（某智能制造企业受到攻击而停产）

奇安信 新一代网络安全领军者



1. 攻陷IMO服务器

攻击者利用办公网IMO服务器的任意执行漏洞，发起攻击获得服务器权限。

2. 攻陷MES服务器

搜索内网发现MES主机，利用MES存在的“永恒之蓝”漏洞，获取权限；将勒索病毒样本上传至MES主机运行，病毒在内网中蔓延传播。

3、攻陷上位机

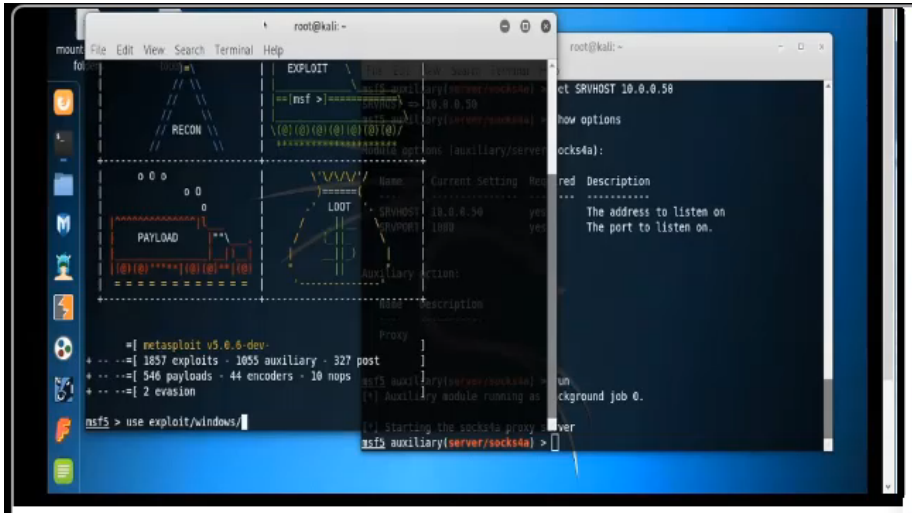
搜索内网发现双网卡配置的XPSP3上位机，利用上位机组态软件的远程堆溢出漏洞，获取上位机权限。

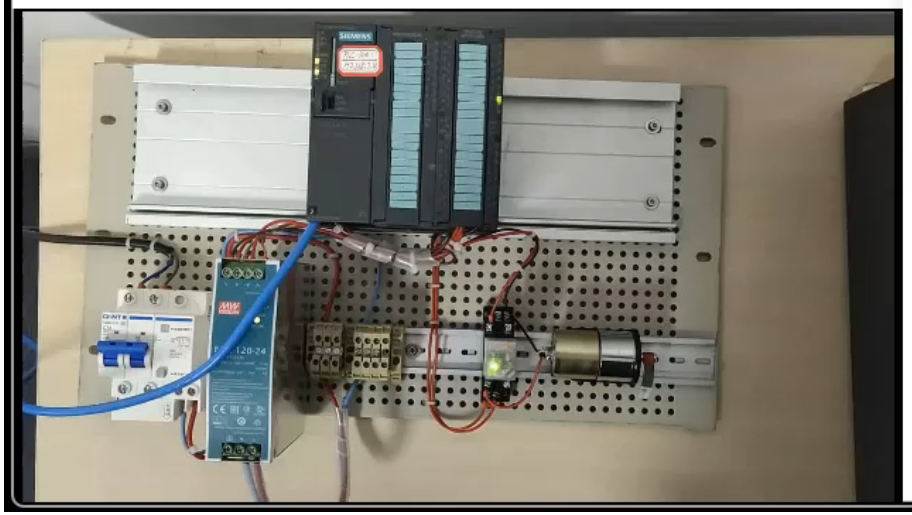
4、攻击PLC

继续搜索发现西门子300控制器，向上位机投递PLC攻击软件，程序运行后向PLC发送特制Crash漏洞攻击报文，致使PLC进入Defeat状态，其控制的马达（生产线）停转。

攻击过程实验室复现

奇安信
新一代网络安全领军者





目录

中小企业的定义

奇安信
新一代网络安全领军者

《关于印发中小企业划型标准规定的通知》

（二）工业。从业人员1000人以下或营业收入40000万元以下的为中小微型企业。

其中，**从业人员300人及以上，且营业收入2000万元**及以上的为中型企业；

从业人员20人及以上，且营业收入300万元及以上的为小型企业；

从业人员20人以下或营业收入300万元以下的为微型企业。

年收入在5000万美元至10亿美元之间的组织。

Gartner

广义的中小企业：

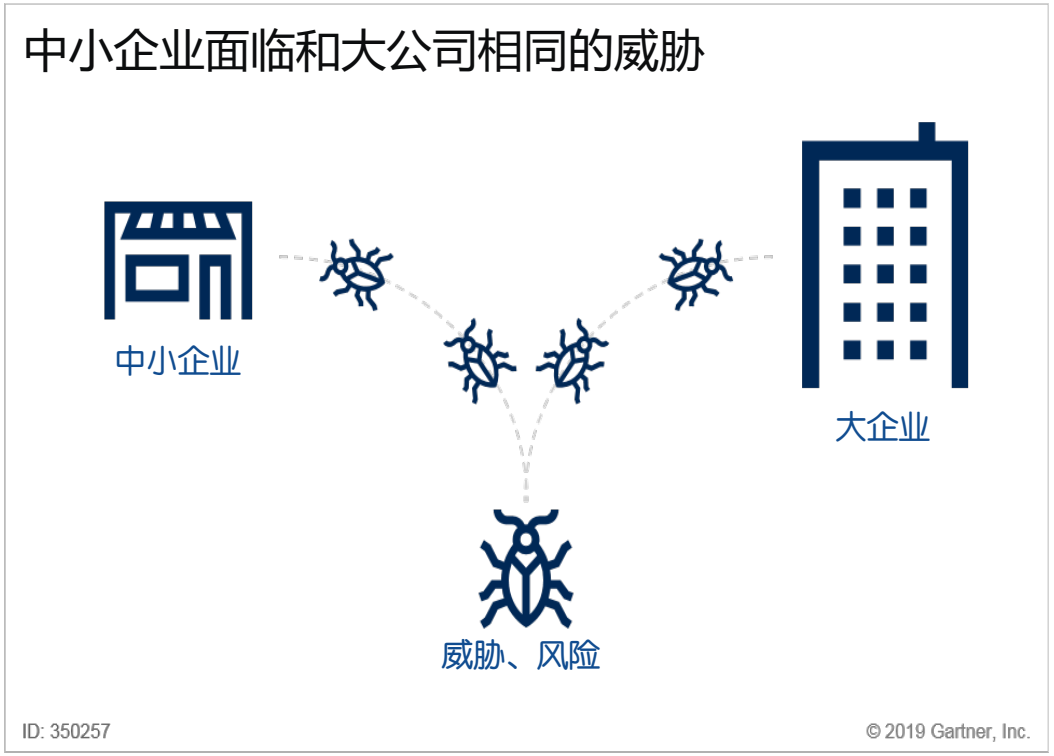
有一定生产规模和网络化基础，在行业排名中处在中上水平的工业企业。

中小企业面临的安全挑战

奇安信
新一代网络安全领军者

中小企业而外的安全挑战

- 有限的安全控制、人员分配、预算和流程使中小型企业面临安全问题
- 无专门的OT安全团队，IT人员难以处理工业安全事件和策略实施
- 人才稀缺，难于跟大公司竞争相同网络安全人才



CIMT2019 上500家工业企业调研

奇安信
新一代网络安全领军者

工业互联网安全现状调查

为了深入了解国内工业企业网络工业互联网安全建设现状，特展开本次展开此次针对工业互联网的调研活动。

1. 您所在单位的**行业**是：

A、政府机构/事业单位　B、科研机构　C、制造业　D、市政/交通　E、通信/网络
F、石油石化/化工　G、能源电力　H、水务　I、医疗　J、其他

G、汽车　建筑（设施）自动化
H、水泥和玻璃
I、化学，电子和电气
J、电力
K、机械
L、采矿和金属
M、石油和天然气
N、精炼
O、半导体石油石化/化工　G、能源电力　H、市政/交通　I、通信/网络　J、其他 远程联网调试设备经常蓝屏、重启

2. 贵单位是否组织过**网络安全意识培训**？
A、有　B、没有　C、不了解

3. 您听说过以下哪些有关工业互联网的**安全事件**？（）
A、伊朗核电站震网病毒事件 B、委内瑞拉遭受网络攻击大规模停电事件　C、挪威铝业公司 Norsk Hydro 遭受勒索软件攻击工业

4. 您认为贵单位**工业网络遭遇攻击**的可能性：
A、很大可能　B、基本不会　C、完全不会

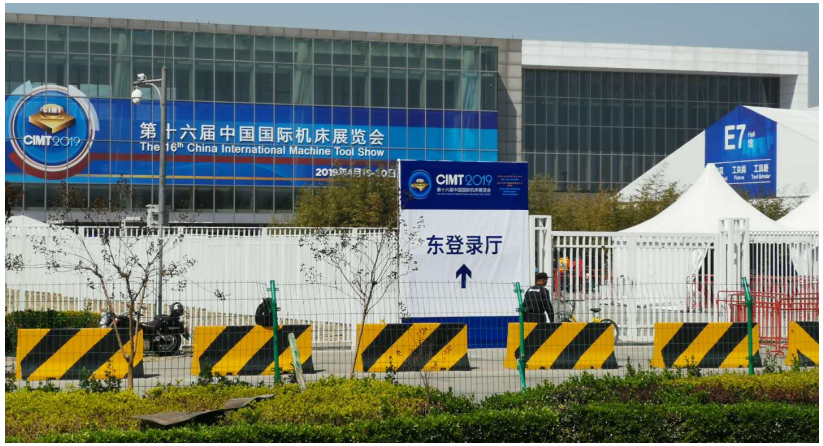
5. 您认为网络病毒是否可以**攻击到您单位车间的工业设备**？
A、能　B、不能　C、不了解

6. 如果车间的设备上遭遇网络病毒攻击，您认为会**对设备产生哪些影响**？
A、不能运转　B、产品质量受损　C、浪费生产材料　D、没影响

7. 贵单位生产车间的工业设备是否可以**插入 U 盘**？
A、可以　B、不可以　C、不了解
5.1 对 U 盘是否有管理规范（如果回答可以）
A，没有任何规定，任意 U 盘都可以 B有，只能使用公司 U 盘，但不需要任何杀毒 C，有，只能使用公司 U 盘，使用前需要杀毒

8. 贵单位生产车间中的工业设备能否联网？
A、能　B、不能　C、不了解
7.1 可以连上哪些网络？（选择能）
A、只能连接工业网络　B、　工业网络和普通办公网络都可以连接

9. 您办公电脑是否可以和车间设备（上位机）进行**联网，传输文件**？



CIMT2019 中国国际机床展集中企业调研

企业调研结果分析

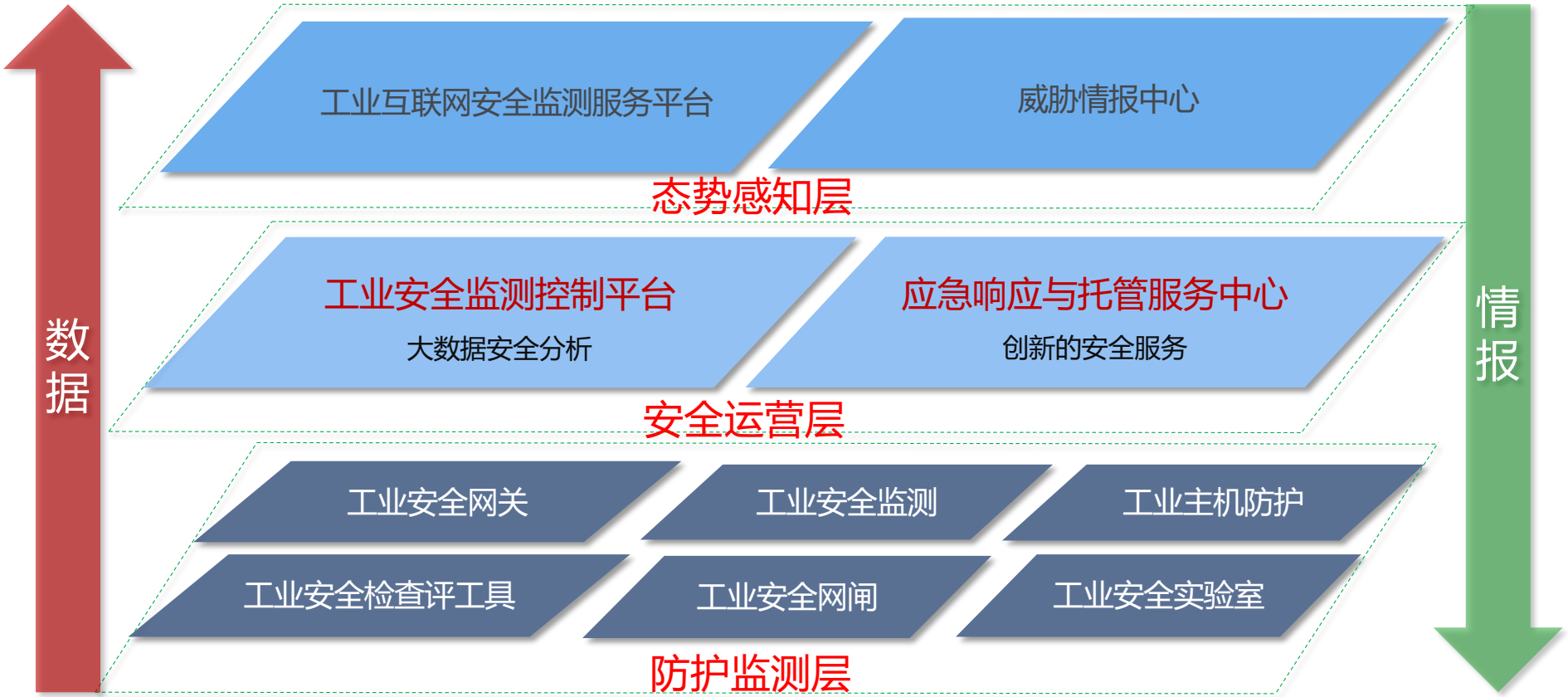
奇安信
新一代网络安全领军者

- 超过50%企业生产联网——工业互联网发展潜力大
- 超过50%的出现蓝屏重启（勒索）——安全事件频发、损失大
- 网络事件37%找安全厂商，36.4%找工控厂商——产业协同必要

目录

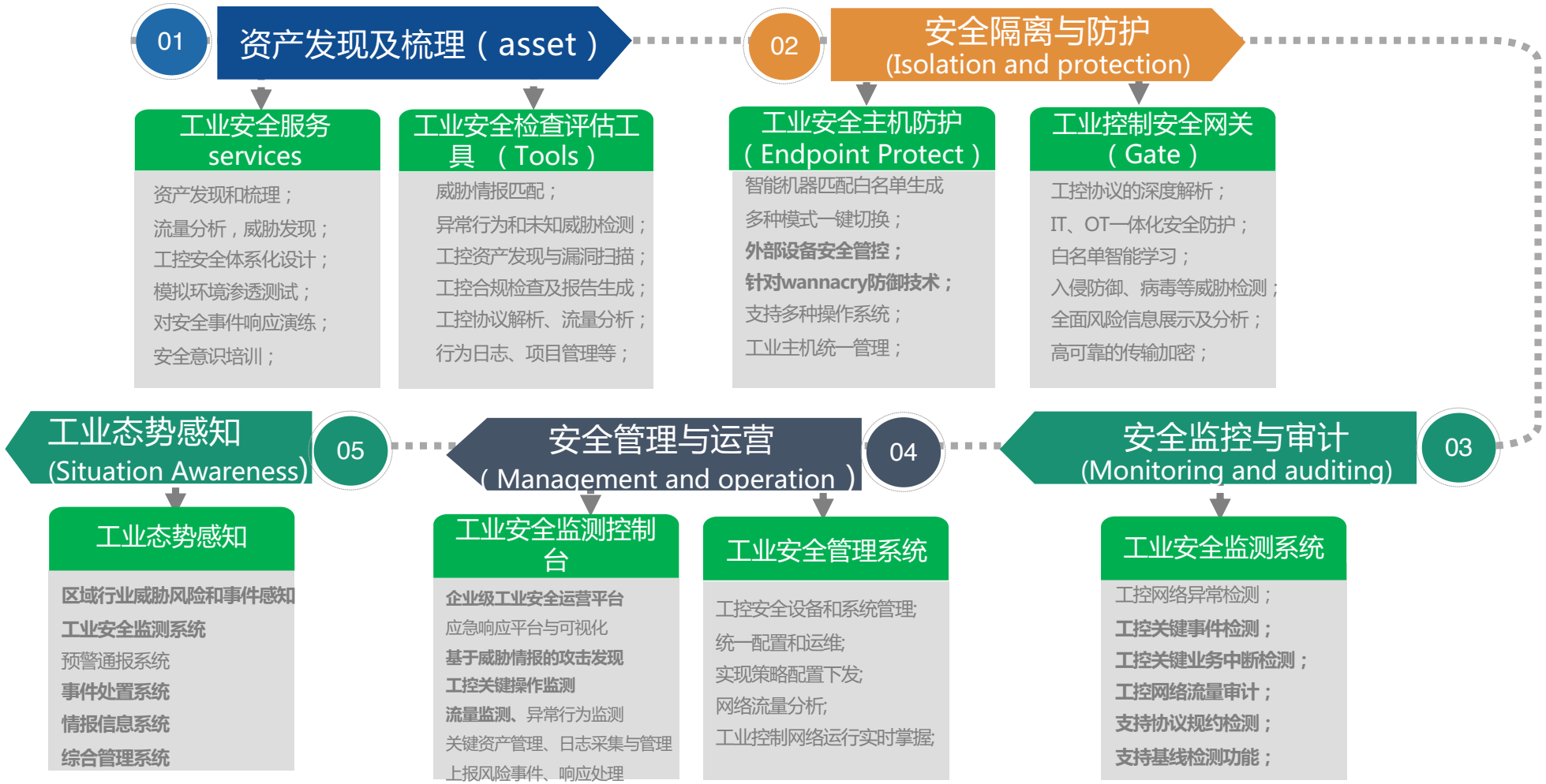
数据驱动安全理念，协同联动防护体系

奇安信
新一代网络安全领军者



工业互联网安全防护整体思路

奇安信 新一代网络安全领军者



新等保2.0 发布为指明了方向！ 成本呢？

奇安信 新一代网络安全领军者

工业行业代表——电力
《电力监控系统安全防护总体方案》

《信息安全技术 网络安全等级保护基本要求》

等保1.0

安全分区
网络专用
横向隔离
纵向加密
综合防护

- ✓ 入侵检测
- ✓ 主机与网络设备加固
- ✓ 应用安全控制
- ✓ 安全审计
- ✓ 专用安全产品的管理
- ✓ 备份与容灾
- ✓ 恶意代码防范
- ✓ 设备选型及漏洞整改

安全通信网络
安全区域边界
安全计算环境
安全管理中心

安全通用要求扩展要求

工业控制系统安全扩展要求

安全物理环境
安全通信网络
安全区域边界
安全计算环境

等保2.0 一个中心 三重防护

物理与环境安全

- 视频监控
- 漏水检测
- 精密空调
- 静电地板
- UPS备用电源
- 防雷击系统
- 门禁系统
- 电磁屏蔽

网络与通信安全

- 边界隔离
- 入侵防范
- 安全审计
- 链路冗余
- 访问控制
- 恶意代码防范
- 可信验证

设备与计算安全

- 身份验证
- 访问控制
- 安全审计
- 入侵防范
- 恶意代码防范
- 可信验证

应用和数据安全

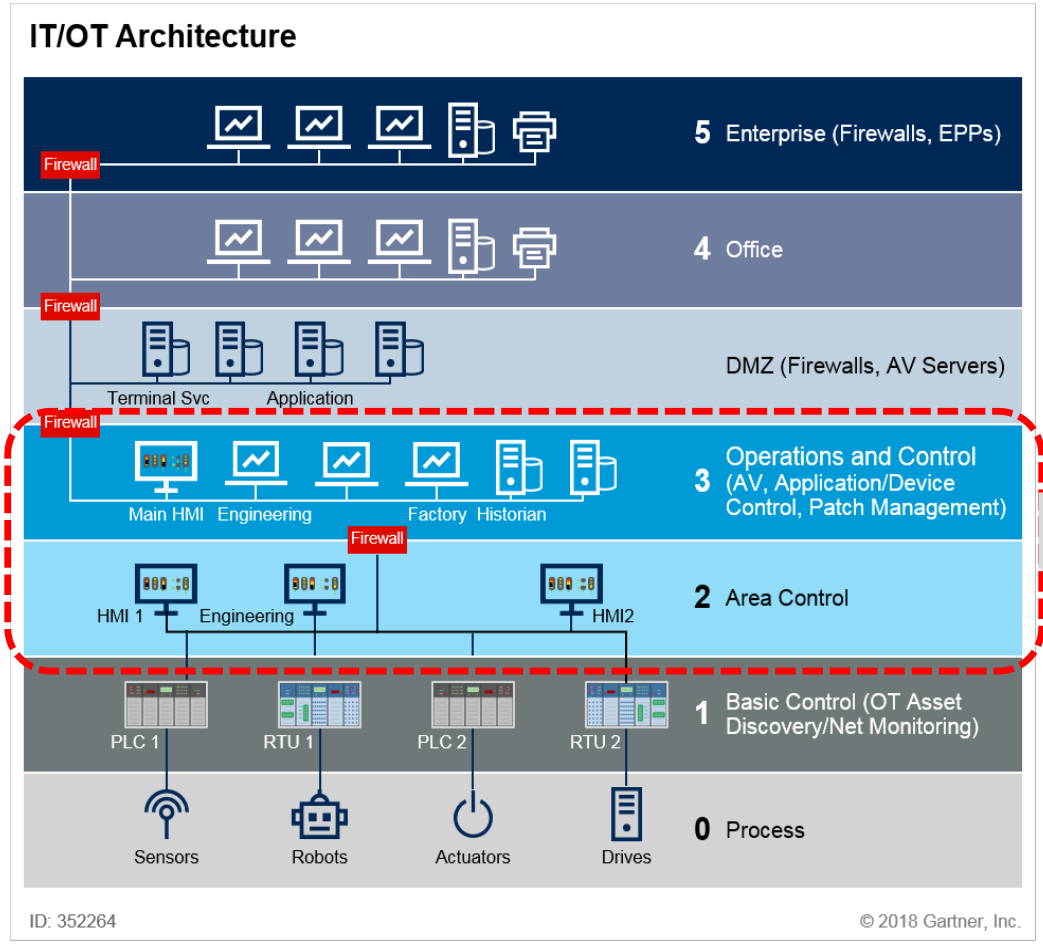
- 数据完整性
- 数据保密性
- 数据备份恢复
- 剩余信息保护
- 个人信息保护

安全管理中心

目录

工业主机是CPS的“大门”

奇安信
新一代网络安全领军者

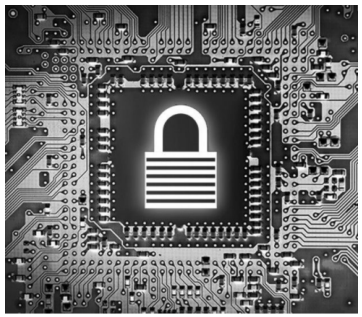


工业主机安全管理痛点

奇安信
新一代网络安全领军者

补丁打不上
漏洞百出

- 担心影响生产不想打
- 主机不联网无法升级
- 系统老旧无补丁可打



病毒杀不完
带病运行

- 硬件配置太低装不上杀毒软件
- 无法升级杀毒软件病毒库老旧
- 担心误杀工业软件，干脆不装

资产查不清
暗藏隐患

- 工业主机家底不清楚
- 资产配置分布不可视
- 整体安全隐患不了解

应用程序白名单&关卡式病毒拦截

奇安信
新一代网络安全领军者

“永恒之蓝”超前防御，防蓝屏

一键设置白名单，无需升级

网络防护，主机中毒后防止扩散

入口拦截 | 运行拦截 | 扩散拦截

U盘管控，防止非授权外设引入病毒

注册 → 授权 → 审计

三种模式一键切换，保障生产连续性

关闭 → 告警 → 防护

日志审计，溯源攻击主机和恶意程序

白名单漏洞防御日志 → IP 端口 应用程序 → 溯源 主机 恶意 软件

工业主机集中管理，降低运维成本

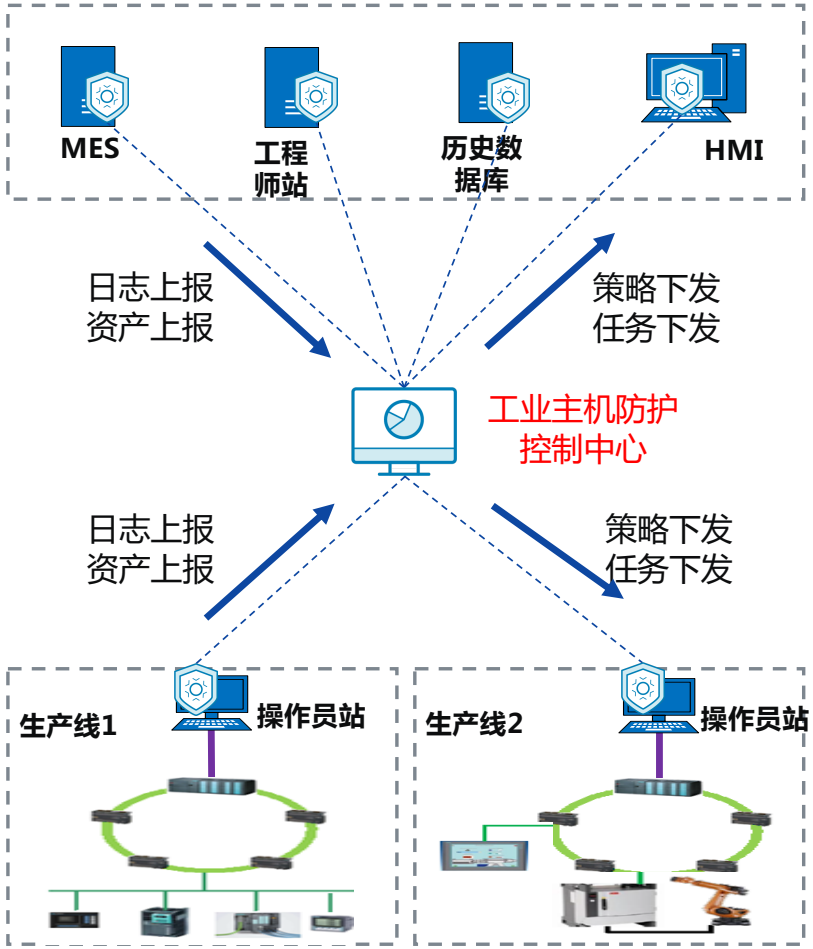
奇安信
新一代网络安全领军者

集中管理

- 配置策略下发
- 日志汇总分析
- 资产汇总分析
- 主机风险展示

灵活配置

- 灵活部署模块
- 灵活设置权限
- 灵活配置页面
- 灵活扫描时间



工业网络安全管理缺少“抓手”

奇安信
新一代网络安全领军者

恐惧源于未知，看见才能安全

资产状况

资产数量不清楚
资产类型不清楚
资产分布不清楚

安全威胁

谁有隐患不知道
谁被攻击不知道
攻击后果不知道

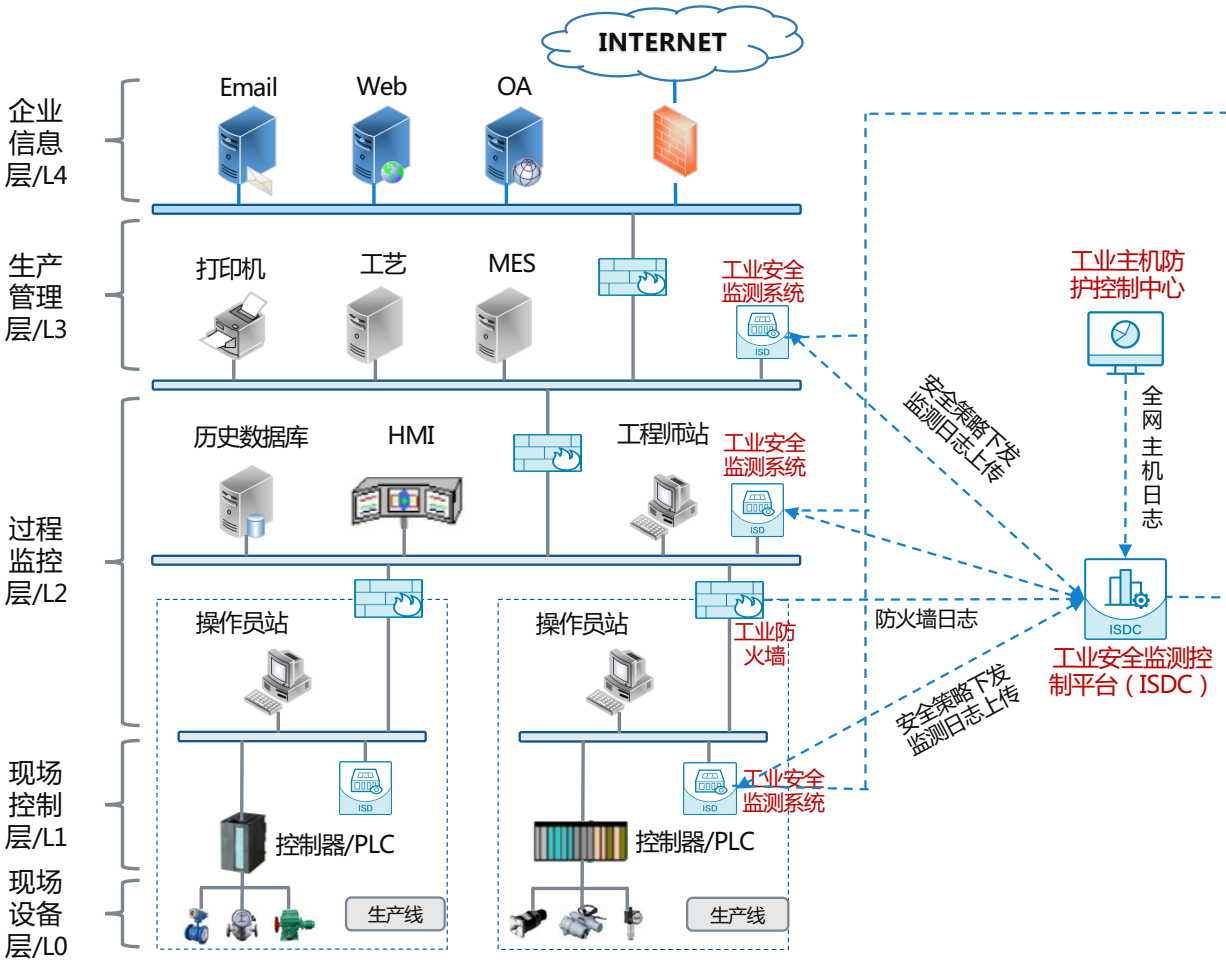
生产故障

设备断线难定位
设备停机难定位
违规外联难定位

看清、看透、看全工业生产中的威胁，是保障工业安全的基础和前提

工业安全监测系统

奇安信
新一代网络安全领军者



安全监测系统 ISD（硬件）

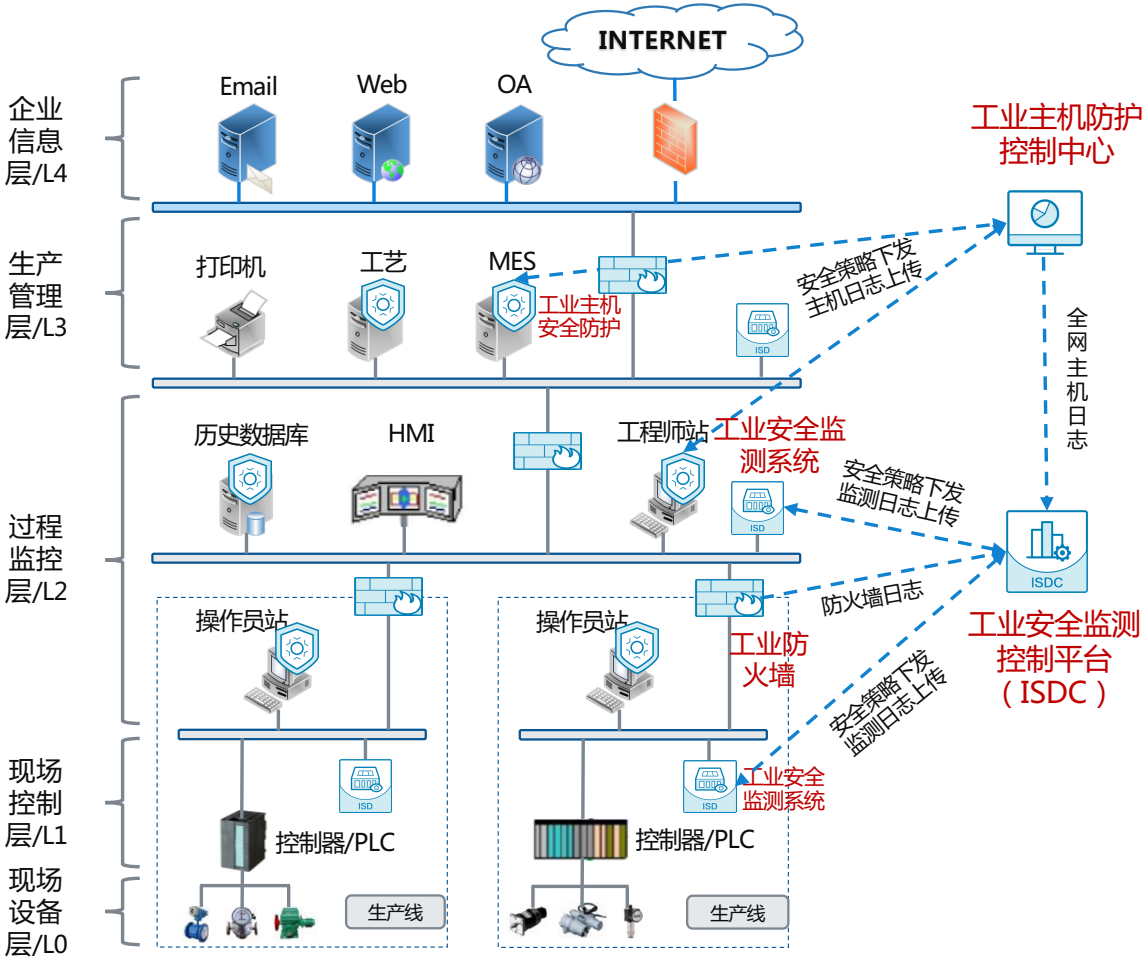
- 旁路监听网络流量
- 自动发现工业资产
- 自动发现资产漏洞
- 实时监测业务操作
- 实时检测网络攻击
- 实时检测病毒传播

安全监测控制平台 ISDC（软件）

- 汇集安全检测数据
- 汇集主机安全数据
- 全局安全风险评分
- 大屏实时态势展示
- 安全事件应急处置
- 统一安全运维管理

生产网络“三板斧”解决90%工业安全问题

奇安信
新一代网络安全领军者



【主机防护】工业主机安全防护系统

- 软件形态，安装在工业主机，防病毒攻击
- 白名单管控，兼容老旧软硬件系统
- 入口、运行、扩散三重关卡病毒拦截
- 永恒之蓝专防，无需打补丁、关端口

【网络分区】工业防火墙/交换机

- 隔离不同网络，防止跨网攻击
- 专有硬件适应工业生产环境
- 工业协议及子协议深度识别
- 网络、应用、规约指令、规约数据四重防护

【安全监测】工业安全监测系统

- 旁路部署，监听网络流量
- 自动发现资产，监测非法设备接入
- 检测工控漏洞，识别工控安全风险
- 监测设备异常操作，保障连续生产
- 风险集中分析，大屏展示安全态势

工业安全产业安全生态：协同共治安全漏洞

奇安信
新一代网络安全领军者

45000+
已注册白帽子数量

5000+
已注册机构数量

30万+
已发现漏洞总数

2000万+
已发放奖金总额

网络安全产业

工控系统厂商
- 安全意识相对薄弱
- 安全开发能力不足
- 漏洞研究人才匮乏

+

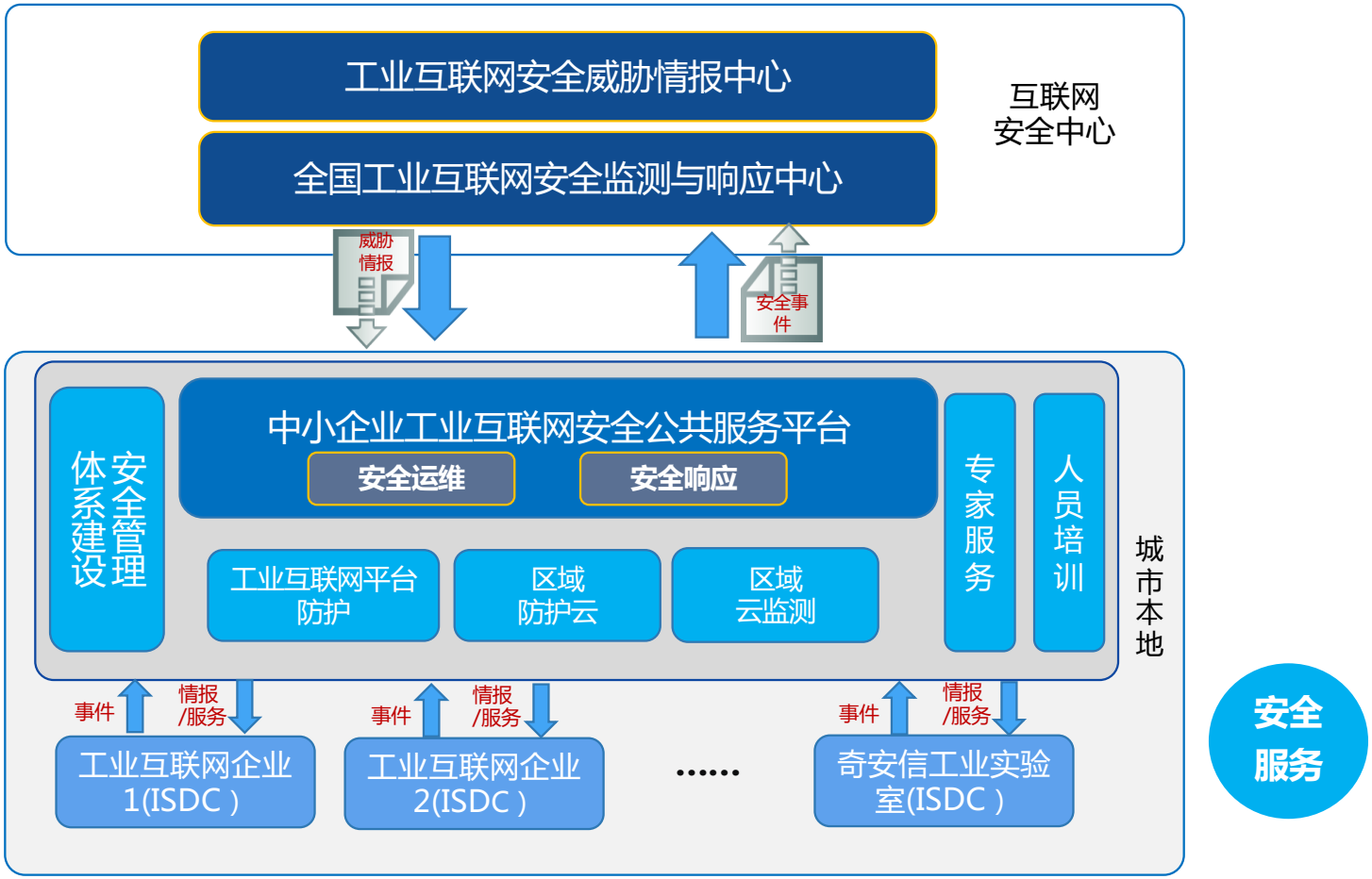
网络安全厂商
- 工控系统品类繁多
- 获取成本相对较高
- 工业领域认知有限

以用户知情为宗旨的
漏洞披露和协同治理机制

工业安全领域

政企联动——构建多级安全服务体系

奇安信
新一代网络安全领军者



中小企业战略防护重点

奇安信
新一代网络安全领军者

加强安全培训

- 领导者应在采购、运营和工程的执行层面建立安全意识，以确保在选择和采购新生产设备的过程中包含适当的安全要求。
- 每年进行一次安全培训；
- 将安全培训作为新员工入职培训的强制部分；
- 从意识——培训——教育三方面落实，关注安全，培养相关技能和能力，培养安全专家；

做好安全服务

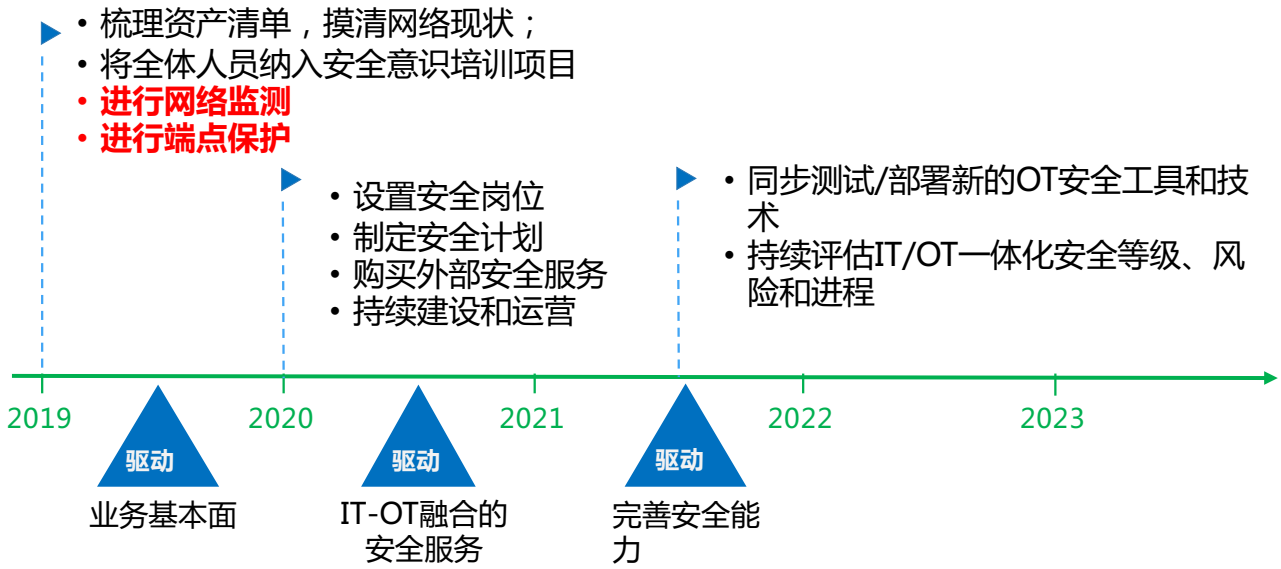
- 中小型企业资金紧张，无法按照普渡参考模型进行安全部署，要想做好安全建设应该与安全企业做好产业合作；
- 将网络安全的能力，将变成一种可定制的服务，工业互联网企业可以根据自己的威胁、成本、人才和运行阶段按需使用；

主机防护 + 安全监测 + 安全响应服务（找谁？） = 解决80%的网络安全问题

中小企业工业互联网安全战略推进时间表

奇安信 新一代网络安全领军者

- 由于中小企业，做好业务基本面抵御常见威胁，购买安全服务，降低安全支出
- 需要循序渐进，完善安全能力



奇安信
新一代网络安全领军者

让网络更安全，让世界更美好

感谢聆听

工业控制系统安全国家地方联合工程实验室

奇安信集团 工业互联网安全事业部