保障工业企业生产安全
助力“十四五”新建设

威努特 WINICSSEC | 专注工控 捍卫安全

2022北京网络安全大会

2022 BEIJING CYBER SECURITY CONFERENCE

全球网络安全 倾听北京声音

保障工业企业生产安全 助力“十四五”新建设

郭洋

目录
CONTENTS

1 工业企业的安全形势
2 工业企业面临的核心安全问题
3 工业企业网络安全解决之道探讨

— 01 —

工业企业的安全形势

数字化转型：IT&OT深度融合

国内新技术的应用使得原来封闭的工业控制系统网络越来越“开放”，在工业互联网、两化融合、制造业生产控制网络不可避免会遭遇更多的网络威胁：

- 工业控制系统走向对外开放；
- 工业控制系统走向内部互联。

工 业 互 联 网

普度模型

工业控制系统的攻击威胁持续加剧

生产网络威胁

国家工信安全中心完成全国工业控制系统威胁诱捕网络部署工程（2021年）

数量统计

全年捕获境外105个国家和地区对我国实施的扫描探测、信息读取等恶意行为超过**600万次**。

时间分布

2021年，境外对我攻击主要集中在**5-7月**，其中7月达到峰值，攻击数量140余万次，占全年攻击总数的23%，达到年均值2.8倍。

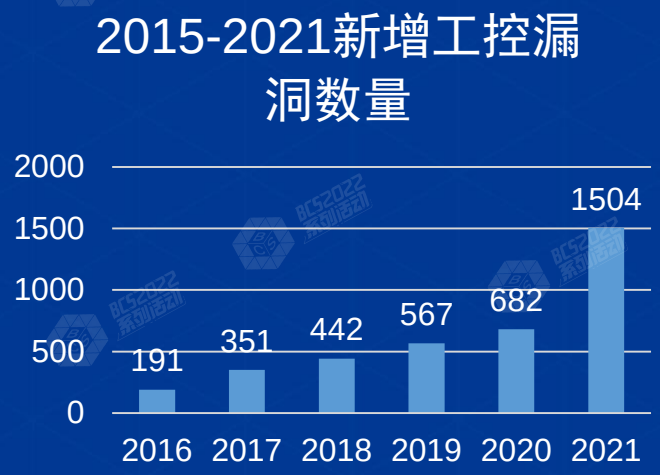
协议分析

从协议类型看，针对**EtherNet/IP、IEC104、S7comm**等工控协议发起的攻击次数位列前三，其中**EtherNet/IP**攻击占比最高，达37%。

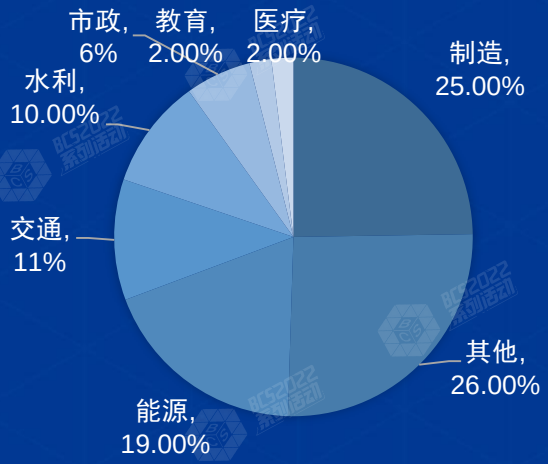
数据来源：国家工信安全中心

工控系统安全漏洞持续增多并呈现多样化

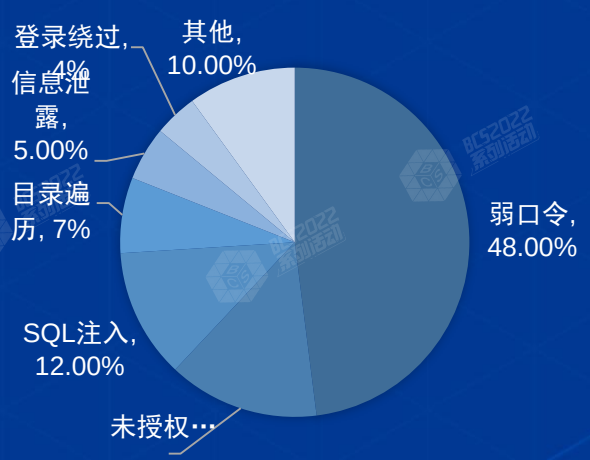
工控系统漏洞持续增长



新增漏洞行业分布广



安全漏洞类型多样



- **2021年**，CICSVD新收录工业信息安全漏洞**1504**个；
- **漏洞类型**：缓冲区错误漏洞数量最多，达到333个，占比**22%**；
- 抽样研判的工业信息安全风险主要集中在**智能制造、能源、交通**等关键行业；其中**制造业**安全风险数量较上一年增长**86%**。

数据来源：国家工信安全中心

新勒索病毒不断涌现，旧勒索病毒不断演变进化

- 2017年5月，全球爆发大规模勒索软件感染事件，我国大量行业企业内网遭受大规模感染。针对工控系统，勒索病毒与恶意软件的传播方式是相似的。勒索软件在工业网络的攻击行为主要以邮件、程序木马、网页挂马的形式进行传播，该病毒性质恶劣，危害大，一旦感染将给用户带来无法估量的损失。近年来出现多个新型勒索软件将攻击目标精准定位于工业控制系统。
- 威努特在2017年勒索病毒刚刚爆发时，就在西气东输项目上的现场成功拦截勒索病毒。

- 新型勒索软件能终止关键工业控制系统进程；FireEye公司报告显示，2020年已经有千余个工控系统软件进程被列入勒索软件终止进程的“黑名单”。

1. 《 2022 SonicWall Cyber Threat Report 》- SonicWall
2. 《勒索病毒安全防护手册 》-中国信通院

网络安全问题将进入集中爆发期

- 资产识别、渗透等网络攻击行为更加专业化；
- 具有国家组织背景的黑客组织对工业控制系统发起攻击。

网络攻击供应链日趋成熟

对手变化、手段升级		
对手	散兵游勇	组织化、规模化
目标	个人主机、离散系统	关键信息基础设施
手段	扫描、探测、猜解	0day漏洞、APT攻击、网络战
动机	技术炫耀、个人好奇窥探隐私、经济利益	有预谋、有计划，与政治、经济、社会、军事密切相关

智改数转导致脆弱性被无限放大

- 智能化改造、数字化转型推动工业互联网快速发展，但在发展的同时也将工业企业和其生产系统的安全脆弱性被无限放大，例如现场大量采用的WIN7，WINXP等微软已经停止更新补丁的系统；
- 存量市场进行安全改造已经进入快车道。

勒索病毒直接威胁企业命脉

- 2021年，勒索攻击呈现手段复杂化、工具专业化、分工精细化等特征，仍为工业领域头号威胁；
- 从行业领域来看，电子制造行业遭受勒索攻击最多，占比达20%，食品加工和能源化工行业并列第二，占比均为16%。

数字货币市场的“繁荣”，直接带来了勒索软件、“挖矿”木马的增长势头。为了寻求更多的“挖矿工具”，提高“挖矿”能力，网络攻击者将会综合利用多种网络攻击手段，包括安全漏洞、恶意邮件、网页挂马、应用仿冒等，对目标实施网络攻击，且攻击方式会越来越复杂和难以发现。

顶层设计逐步完善，工控安全已然成为刚需

2017年6月1日《中华人民共和国网络安全法正式施行》

工信部：
工业控制系统信息安全行动计划（2018-2020年）；
工业互联网发展行动计划（2018-2020年）

公安部：
等保2.0体系化标准发布，代替原有等保标准，新标准对原有通用要求进行优化，同时也针对云计算、移动互联、物联网、工控系统等列入标准范围，标准与2019年12月1日开始实施，网络安全等级保护制度正式进入2.0时代。

工信部：
《加强工业互联网安全工作的指导意见》
《工业互联网企业网络安全分类分级指南（试行）》
《工业互联网综合标准化体系建设指南》

《信息安全技术 关键信息基础设施网络安全保护基本要求》（报批稿）【2019.11.5】
《信息安全技术 关键信息基础设施安全保障指标体系》
《信息安全技术 关键信息基础设施安全控制措施》(征求意见稿)【2019.4.12】
《信息安全技术 关键信息基础设施安全检查评估指南》
《信息安全技术 基于信息流的关键信息基础设施边界确定方法》【2019.4.21】
《关键信息基础设[illegible]护条例》

公安部：
《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》

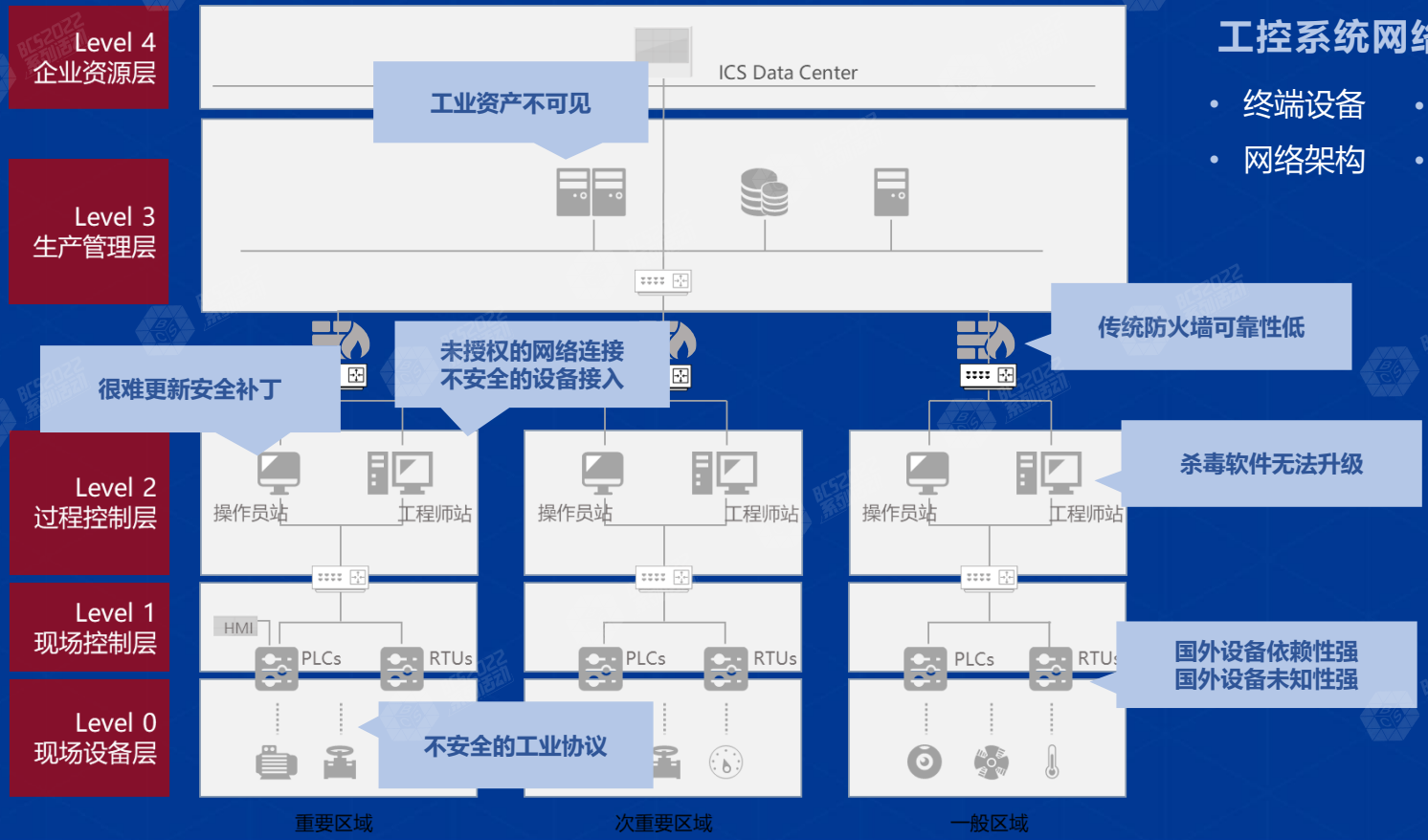
2021年9月1日正式起施行《中华人民共和国数据安全法》

工信部：
《工业互联网创新发展行动计划（2021-2023年）》

— 02 —

工业企业面临的核心安全问题

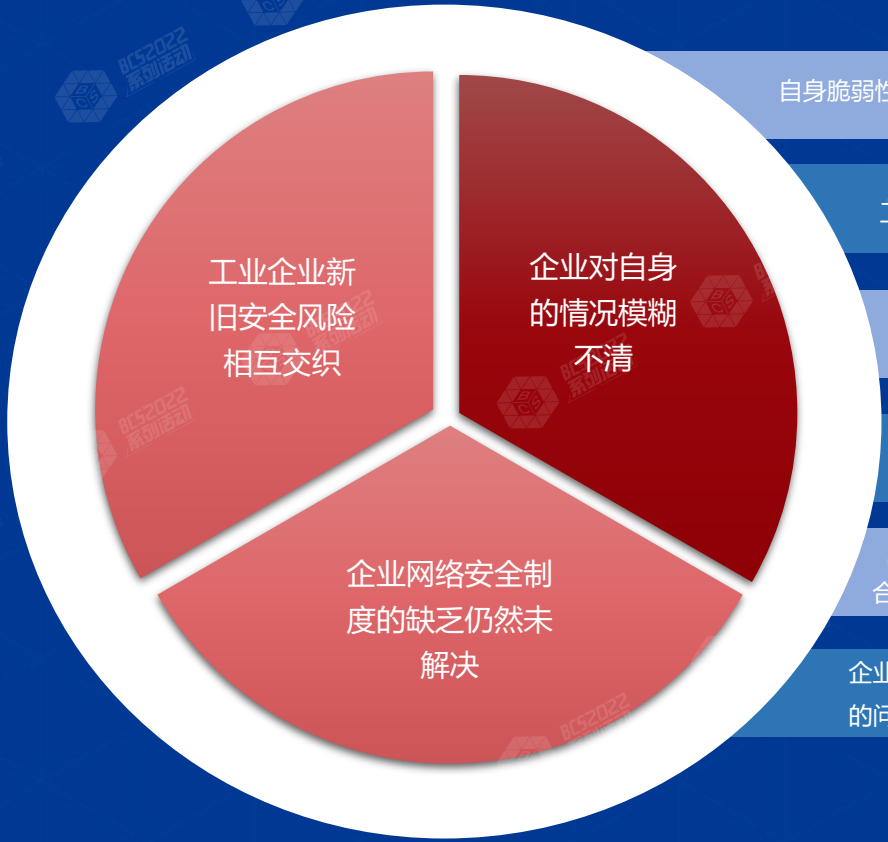
工业控制系统存在的网络安全隐患



工控系统网络安全隐患

- 终端设备
- 安全技术
- 网络架构
- 安全管理

工业企业面临的核心安全问题



自身脆弱性还未解决，工业现场WIN XP,WIN 7的存量很多，漏洞仍然是我们面对的最主要脆弱性

工业互联网开放化、平台化，互联网仍然是工控系统的最大威胁来源

新基建下数字化转型，新技术的应用伴生问题，5G,大数据，云计算等

虽然有明确的制度要求，但企业内部仍然缺失管理抓手和支撑力量，而且责任不清，对内部的管控不足是普遍现象

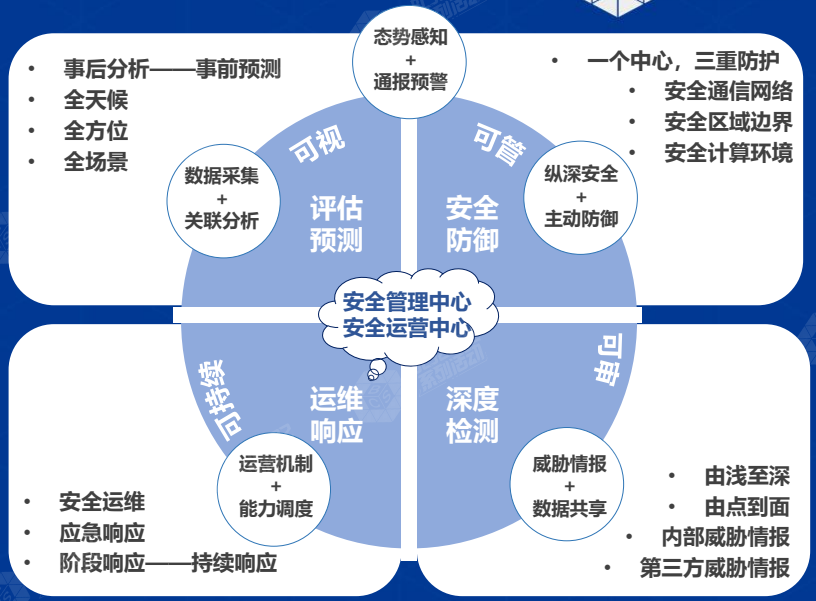
有针对性的工业企业网络安全制度建设比较滞后，主要工业企业网络安全防护基本是以合规为主，管理制度也相对简单，缺乏针对性

企业对自身的工业控制系统的情况不清楚，对网络结构不了解，对资产情况不了解，对存在的问题不了解

—03—

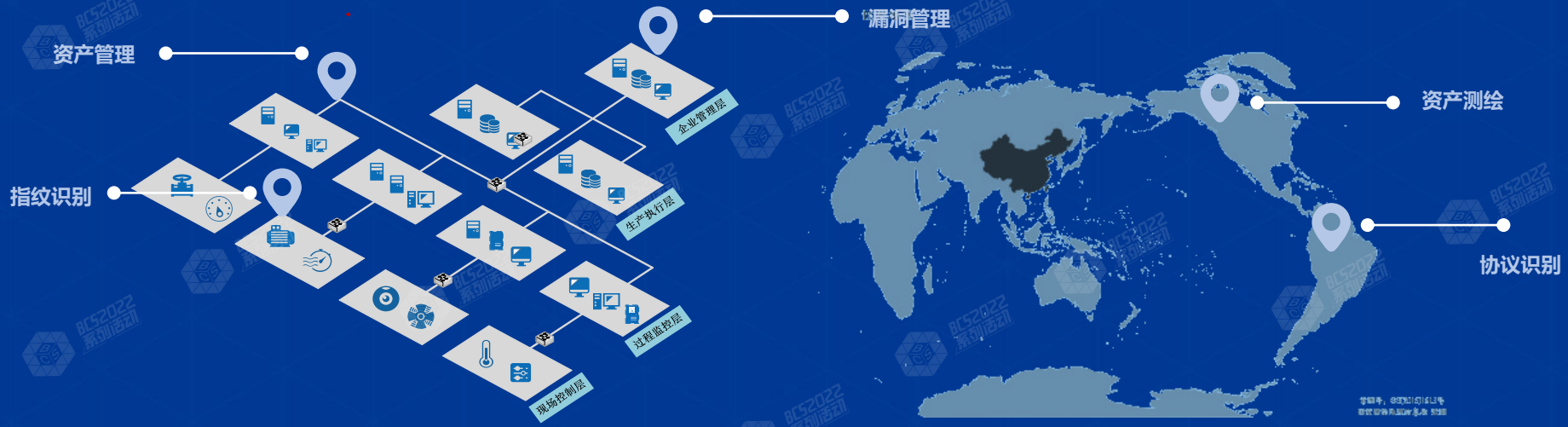
工业企业网络安全解决之道探讨

基于“白名单”技术构建“1246”网络安全防护体系



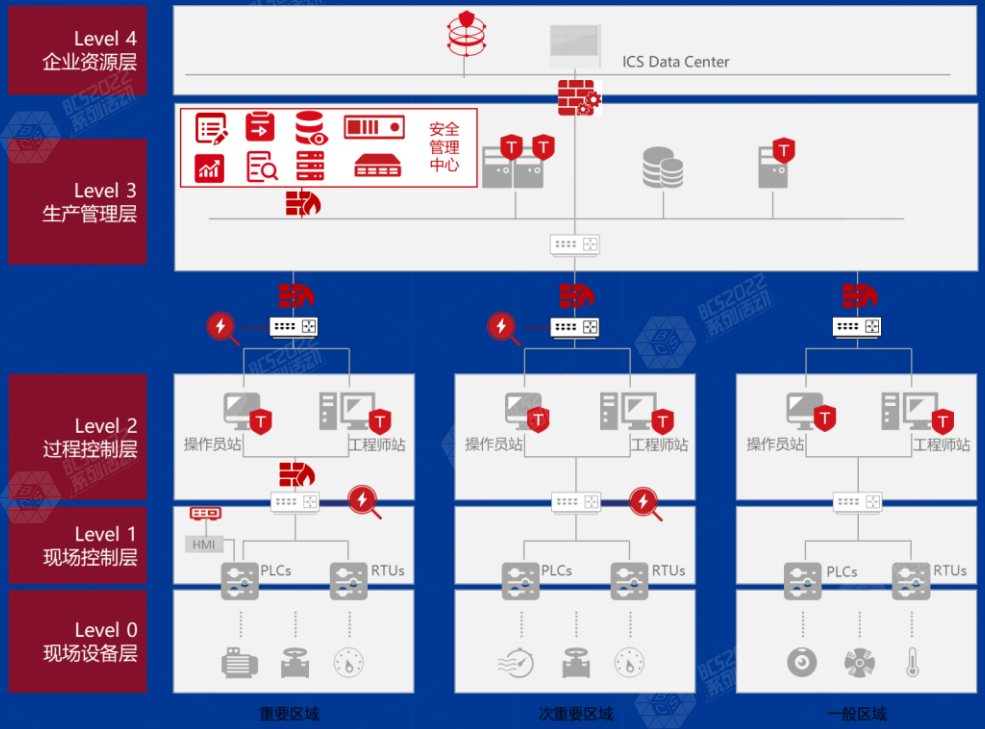
- 以管理风险为核心目标
- 以国内“两个要求”体系合规、国际“技术体系”接轨为两个视角
- 形成可防御、可检测、可响应、可预测的全生命周期的四大体系
- 孵化出动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控的安全能力

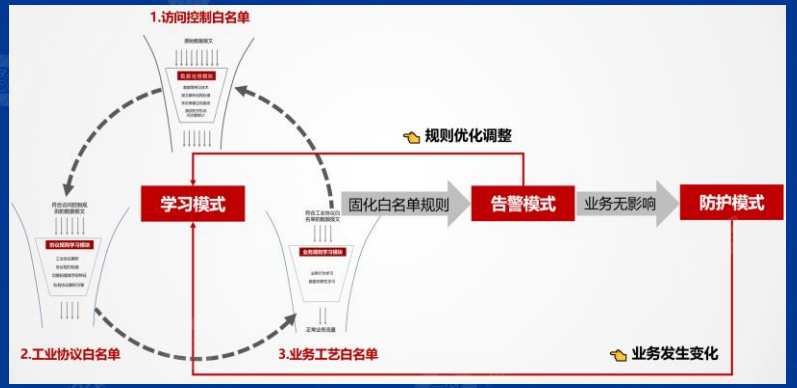
利用先进技术绘制工控网络资产地图实现资产可视



1. 无损快速扫描
2. 分布式部署
3. 工业协议识别
4. 工业资产指纹识别
5. 漏洞扫描与验证

利用白名单技术解决企业数字化转型过程中的安全问题





三重固化，渐进式防护规则自学习与优化

对象白名单

行为白名单

控制逻辑白名单

“四重锁定，两个中心”助力工业主机防勒索

应用锁定

- 锁定工业主机应用程序的运行
- 只有白名单的程序才可以运行
- 避免恶意代码、非法程序的运行

外设锁定

- 锁定外接输入设备的使用
- 提供安全的文件摆渡
- 避免引入恶意程序

安全管理中心

- 集中管理主机资产
- 集中下发安全配置策略
- 集中收集安全策略告警

两个中心，四重锁定

系统锁定

- 锁定工业主机运行环境和资源
- 符合基线策略的环境和资源允许访问
- 阻止注入、溢出等攻击

网络锁定

- 锁定工业主机的网络环境
- 只允许与特定服务器进行通信
- 控制恶意代码的传播、扩散

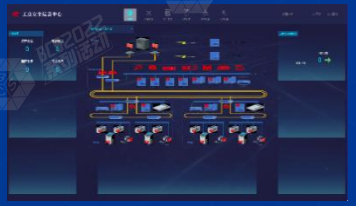
安全监测中心

- 集中监测主机资源状态
- 集中监测操作行为事件
- 集中监测关键事件告警

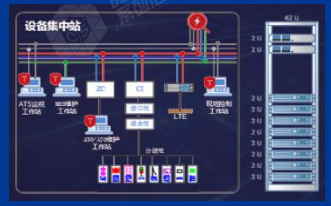
利用态势感知支撑工控网络安全主动防御体系落地

- **是一套态势感知解决方案**
  - ✓ 包含一系列设备装置作为网络的触角探针
  - ✓ 对汇集、整理的海量信息进行大数据分析
  - ✓ 充分利用可视化技术对安全态势进行展示
- **更是一个组织**，由机器与专家联合组成，面向工业控制系统网络安全关键问题建立的分析展示中心、通报预警中心、指挥调度中心

基于全景的态势感知

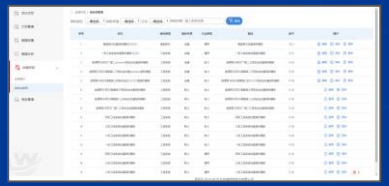


某地铁线信号控制系统



信号系统设备集中站

基于业务的安全展示



基于合规的安全可视化

未来工业安全战场的制胜关键取决于态势感知能力的建设。在于是否能够快速获取外部的攻击威胁情报，更重要的是能否实时动态地掌握自身的情况，并结合两者及时做出最恰当的决策与响

基于工业资产的安全保障运营

资产测绘

有什么？是什么？有哪些风险？

- 生产网络架构、工艺流程、控制设备
- 深度端口识别、工业协议、工业应用
- 高危端口、POC漏洞、版本漏洞

情报监测

发生了什么？哪些与我们有关？

- 定向的情报收集
- 与资产进行关联
- 与业务进行关联

持续监控

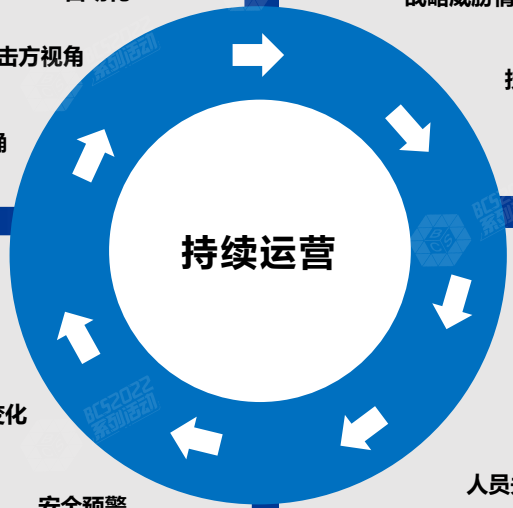
业务的变化？运营指标的变化？

- 人机结合
- 实时感知
- 闭环管理
- 数据驱动

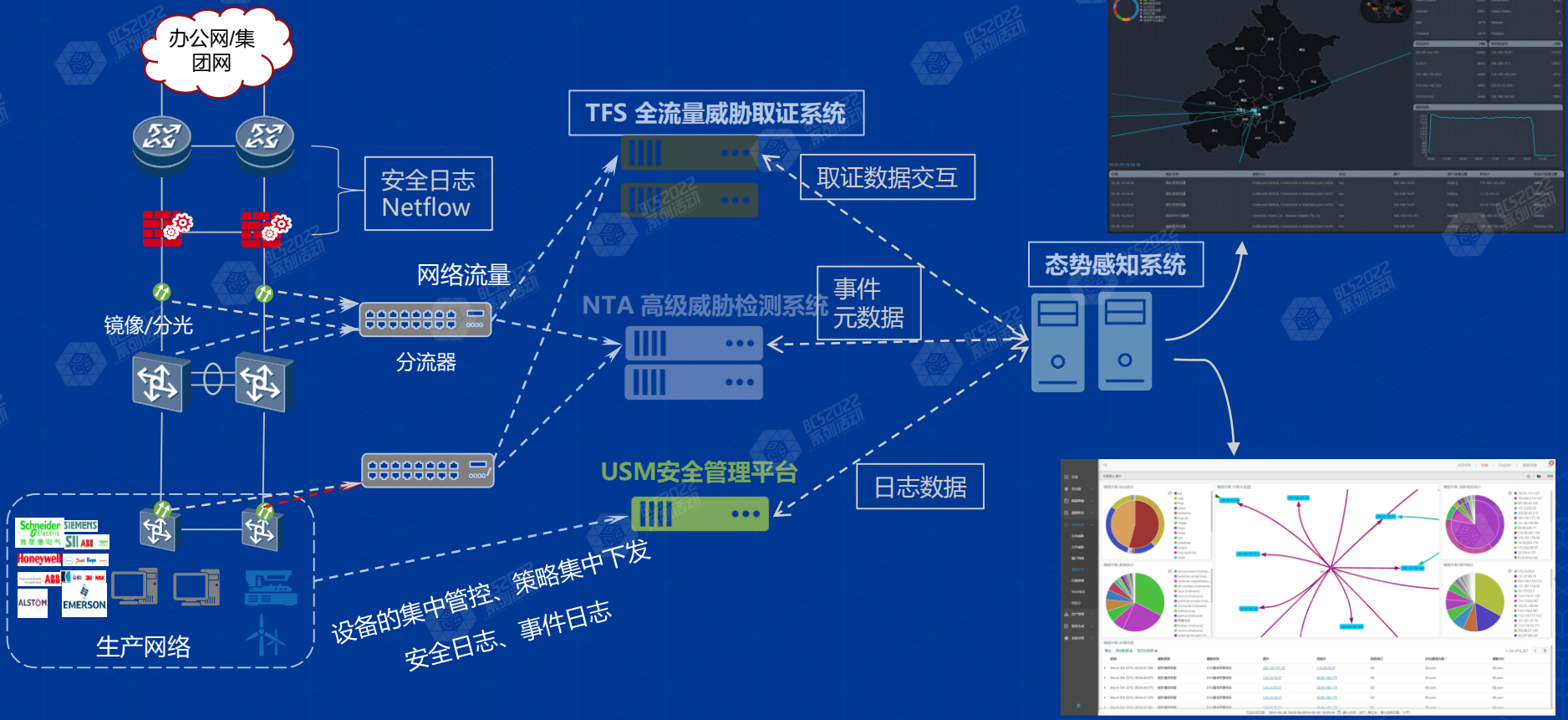
应急响应

业务的变化？运营指标的变化？

- 人机结合
- 实时感知
- 闭环管理
- 数据驱动



基于工业流量的预警态势感知



Thanks