IT/OT融合的安全挑战与应对

陶耀东

工业控制系统安全国家联合实验室主任
360工业安全业务线 负责人

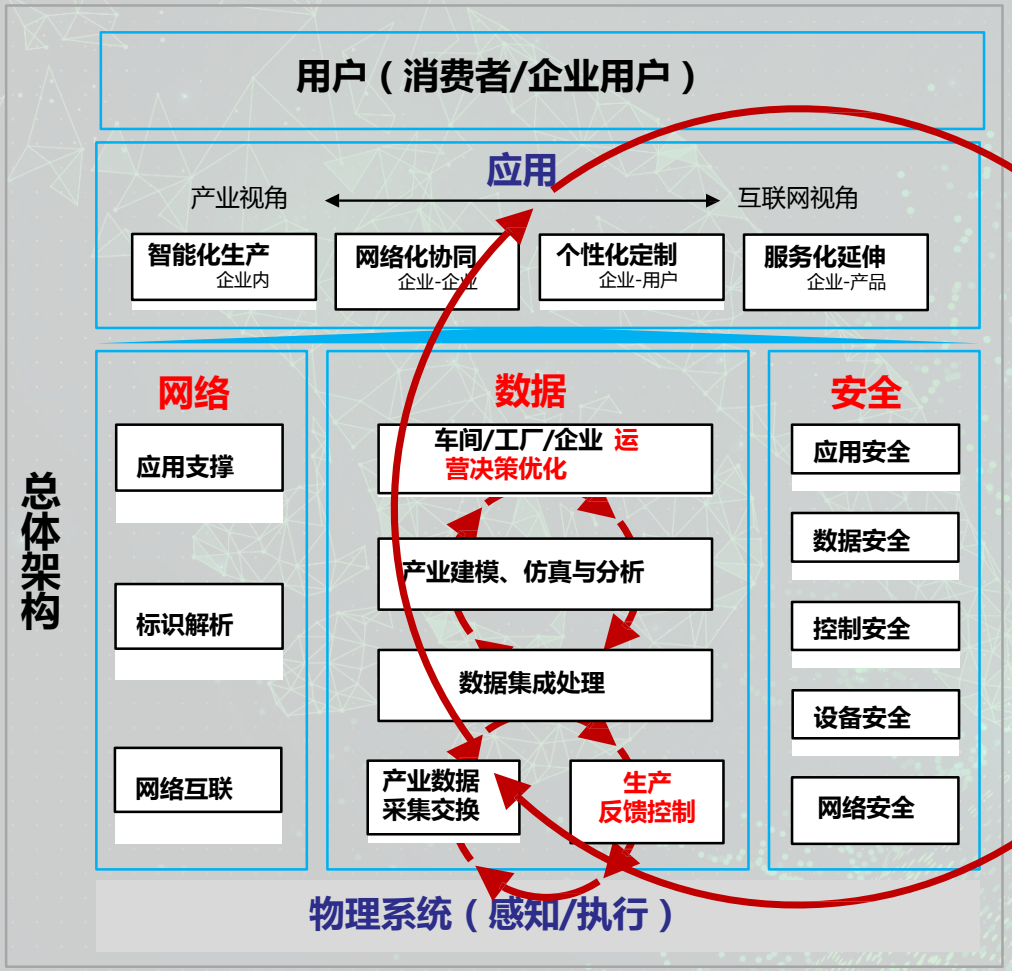
目录

工业互联网 IT/OT 融合的驱动力？

效率 盈利

我国工业互联网总体架构

三大智能化闭环：智能生产控制、智能运营决策优化、消费需求与生产制造精确对接



数据：本质是数据智能在工业 中的全周期应 集成处理-建模分析-决策与 控制 ，形成优化闭环，驱动工 业智能化。

数据是核心

网络：本质是实现数据智能的 网络基础，包 应用支撑三大体系。

网络是基础

安全：本质是工业/产业互联网 各个领域和环 络安全、控制安全、网络安 全、应用安全等。

安全是前提

中国的工业互联网= 工业物联网（OT）+ 工业关联的消费性互联网（IT）

IT/OT融合的驱动力

有效的管理和保护工作的“物”，当应用他们产生的传感器数据进行分析和盈利时，

需要前所未有**IT和OT组织合作获得竞争优势**

- 简化操作获得更大的生产率

  Greater productivity with streamlined operations

- 提高安全性与预测性维护以避免危险的环境中

  Improved safety with predictive maintenance to avoid dangerous environments

- 提高经营决策精度和速度

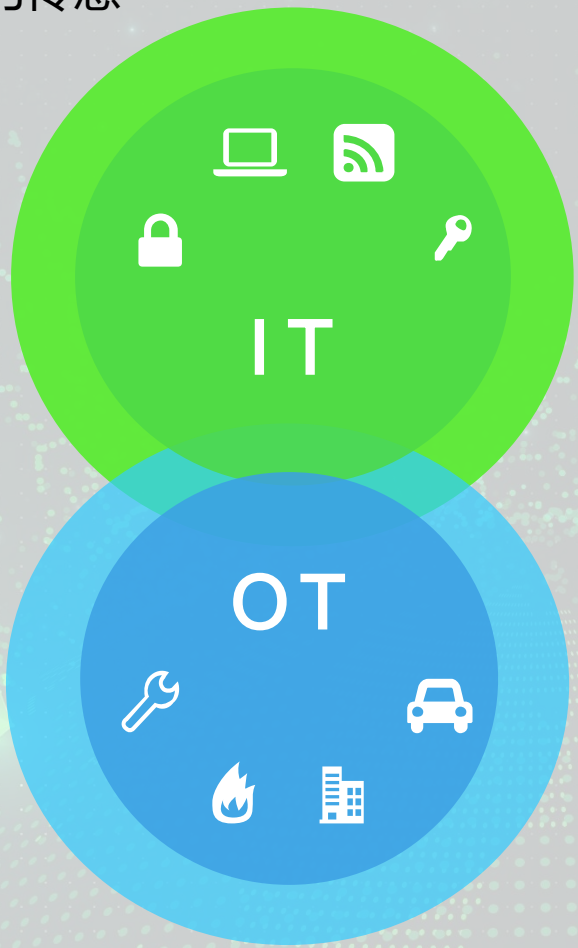
  Increased accuracy and speed in operational decisions

- 减少所需人力成本

  Cost savings with lesser manpower required

- 提高客户需求的响应速度和服务能力

  Increasing responsiveness and service capabilities of customer requirements



Gartner

我国工业互联网的特点：两大视角

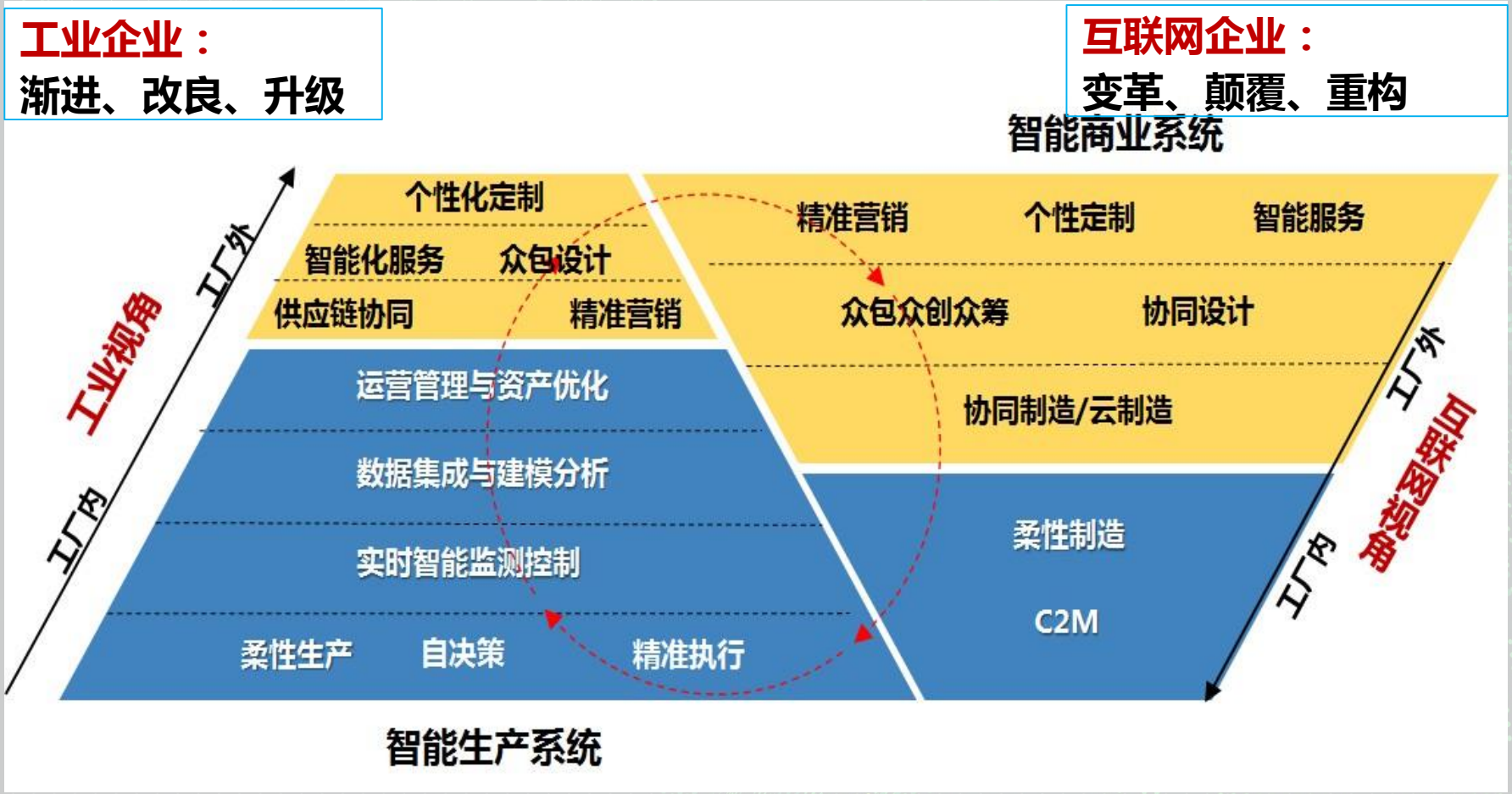
2大视角：

—工业企业：由内及外，渐进、改良、升级，生产系统的智能化

—互联网企业：由外及内，变革、颠覆、重构，商业系统的智能化

工业企业：
渐进、改良、升级

互联网企业：
变革、颠覆、重构



工业互联网 IT/OT 融合的方向？

效率 盈利

IT/OT融合的发展趋势

到2020年底，物联网的全球经济影响将达到2兆美元，其中有超过210亿个联网的“物联网”

- IT和OT分离管理的情况将会打破
- 基于以太网的尽力交付模型将不再适用
- 开始考虑时间敏感网络（TSN）自底向上打通
- 数字孪生

IT / OT一体化实现更直接控制和更完整监控，更容易地分析来自世界任何地方复杂系统的数据

IT/OT 融合带来的安全挑战？

效率 盈利

IT / OT安全收敛，对齐，整合

Mission任务

可靠性Reliability

安全Safety

物理变化的数据
Data for Physical Changes

Security安保

Privacy隐私

商业决策的数据
Data for Business Decisions

http://www.istockphoto.com/photo/two-engineers-discussing-a-building-project-gm483851688-70891017?st=2ffbd09

IT/OT融合的安全挑战

IT/OT融合后带来的安全挑战

- 工业互联网增加更多端点，也带来了更大的攻击面
- IIoT growth in complexity increases the “attack surface” in industrial settings, such as ICS, SCADA, manufacturing, smart grids, oil and gas, utilities, and transportation.
- 与IT相比，IIoT系统安全问题，可以造成物理伤害，生命和社会损失
- IIoT systems have different attack vectors and threats associated with them, as compared with their IT counterparts, which can cause physical harm, loss of life and major societal disruption.
- 安全态势和资产可视性不足，无效的安全对策及合规性和互操作性减缓了在IOT中的使用安全措施
- Lack of security posture and asset visibility, ineffective security countermeasures, and compliance and interoperability issues are key concerns slowing security adoption in IIoT.
- 许多旧的工业协议都是专有的，未考虑到现代威胁和安全架构，带来互操作性和安全挑战
- Many older industrial protocols are proprietary and are not designed with modern-day threats and secure architectures in mind, creating both interoperability and security challenges

Gartner G00317591 “Pragmatic Strategies to Improve Industrial IoT Security”

IT/OT系统主要差异

分类	IT系统	OT系统
可用性需求	可重启、热切换	高可用（不能重启）、计划性中断、重要系统冗余
管理需求	保密性、完整性、有效性、隐私	人身安全、有效性、完整性、保密性、隐私
体系安全焦点	IT资产及信息、中央服务器更重要	边缘设备与中央设备一样重要
未预期的后果	安全解决方案围绕典型的IT系统进行设计	安全工具必须先测试以确保不会影响ICS的正常运作
时间紧迫的交互	交互时效可有弹性 可实施严格限制的访问控制	实时性、紧急响应 访问控制不能妨碍必要人机交互
系统操作	典型的操作系统、自动部署、持续升级	专有的操作系统，无安全功能、软件变更须验证
资源限制	近3-5年主流硬件，有性能冗余	按需设计，可能10-20年前设备，刚好够用
通信	标准通信协议、有线、无线	专有标准、异构、难互操作

IT/OT融合后带来的进一步挑战

- OT大量采用IT设备和技术，IT安全风险随之而来，并将成为主要威胁
- IT和OT安全常常由两个不同团队管理，带来管理效率和 有效性的挑战

案例1：KWC水厂SCADA受到攻击

IT/OT状态

- IBM AS/400小型机系统成为SCADA平台
- 系统通直接连接到多个网络中，包括：地区税务（向外）、流量控制应用程序、几百个PLC、安置客户的相关计费信息等

攻击发现

- 为期60天的评估期间，专家们发现了四个可疑的对外连接
- 可以被用来窃取其中的250万条记录，包括客户数据和付款信息
- 通过访问AS/400系统，攻击可完全控制水流和用于净化水的化学物质

案例2：乌克兰停电（Industroyer/Crashoverride)

攻击过程

- 2016年12月17日影响了乌克兰的变电站
- 黑客使用Industroyer无限循环打开关闭的断路器，使断路器持续打开、关闭，这可能会触发保护，并导致变电站断电，并组织HMI上发出的关闭命令
- **攻击发现**
- Industroyer是模块化恶意程序
- 利用的四种工业协议：IEC 60870-5-101/5-104、IEC 61850、OPC DA
- 还可用于对美国的基础设施硬件发动攻势
- 清理器模块擦除关键性注册表项并覆盖相关文件，导致系统无法启动提升恢复难度

案例3：一些公网上工业应用站点

IT-OT融合后的安全如何应对？

效率 盈利

滑动标尺模型（Sliding Scale）

依赖

进化

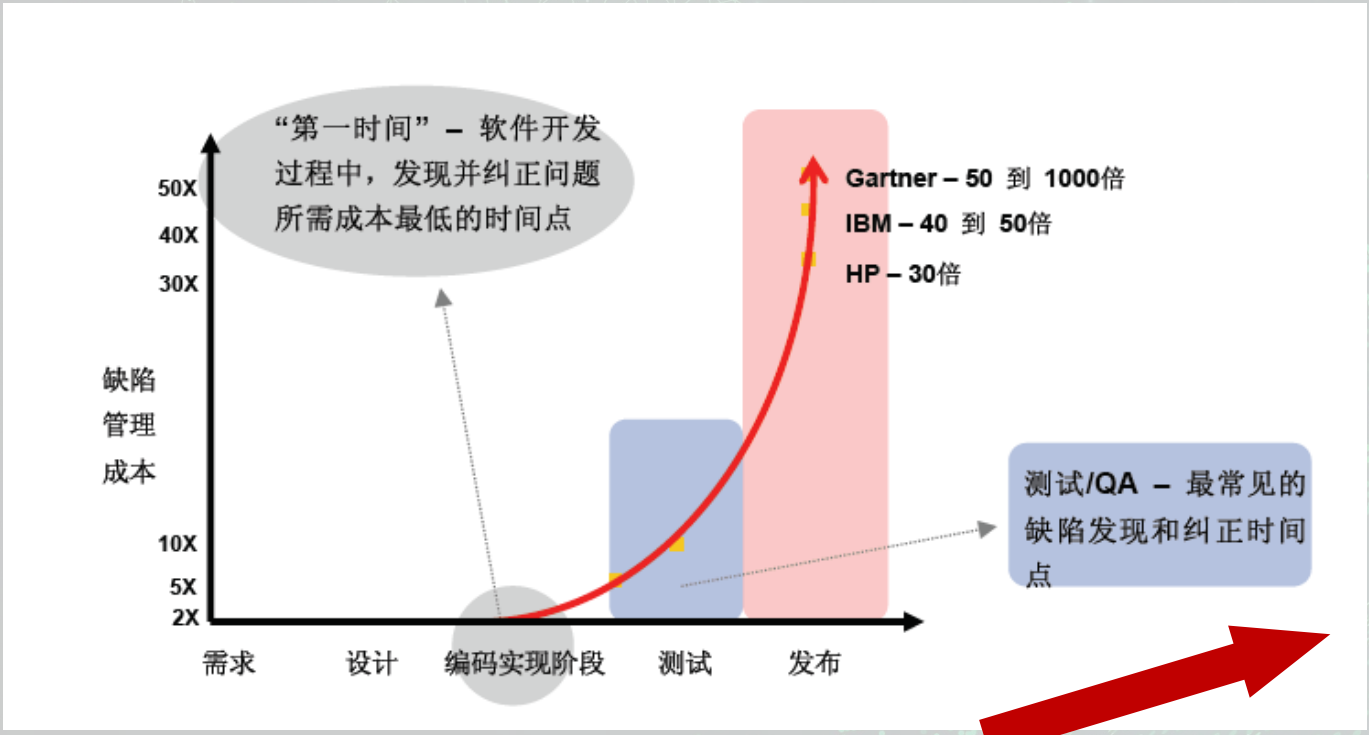
架构安全	被动防御	积极防御	威胁情报	进攻反制
强身健体	纵深防御	检测响应	掌握敌情	先发制人
ARCHITECTURE	PASSIVE DEFENSE	ACTIVE DEFENSE	INTELLIGENCE	OFFENSE
在系统规划、建设、运维的过程中充分考虑安全防护的建设	在无人员介入的情况下，附加在架构安全之上，可提供持续的威胁防护及威胁洞察力的系统	强调人员的参与，对所防御范围内的威胁进行持续的监控，学习经验和应用知识的过程	收集数据，将数据转化为有价值的信息，并将信息生产加工	对抗攻击者的法律反制措施、自卫反击行动

IT/OT一体化架构安全

规划和建设阶段，建立与组织机构实际需求相适应的架构安全体系，可以使其他类别的措施变得更有效且成本更低

- IT和OT功能安全与信息安全一体化规划
- 开发结构化的补丁管理和验证程序
- 使用网络分段的方法隔离关键系统
- 进行管理认证和访问控制
- 实施主机加固和白名单，只允许部分软件运行
- 遵循最佳实践的远程访问
- 选择合适的供应商和组件

业务应用软件的供应链安全



最大的风险来自这里

缺陷检测
检测编写的代码是否存在常见的安全缺陷

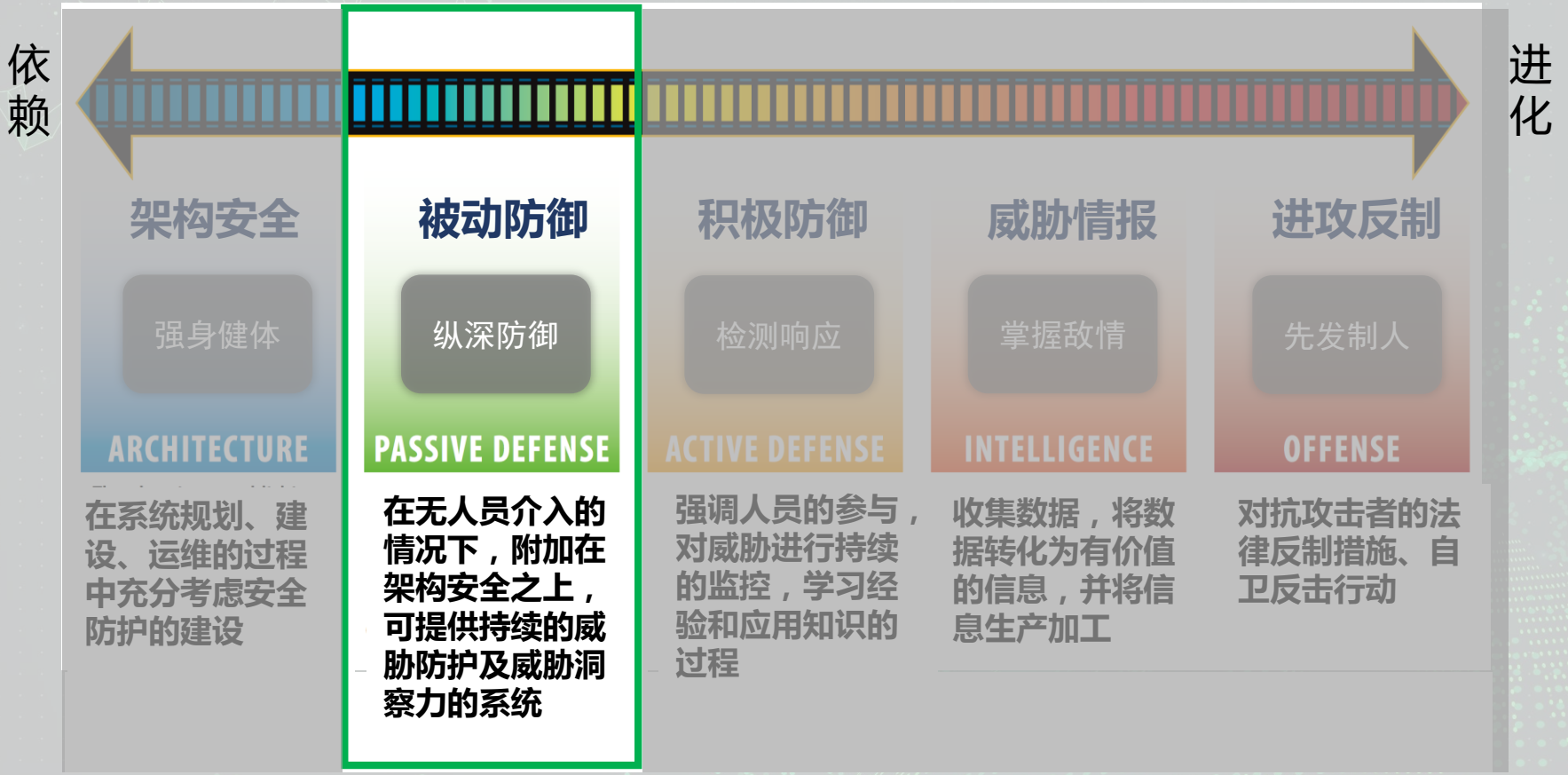
合规检测
检测代码的编写是否遵循了安全编程标准

溯源检测
检测开发中是否使用了不安全的第三方组件

供应链的选择

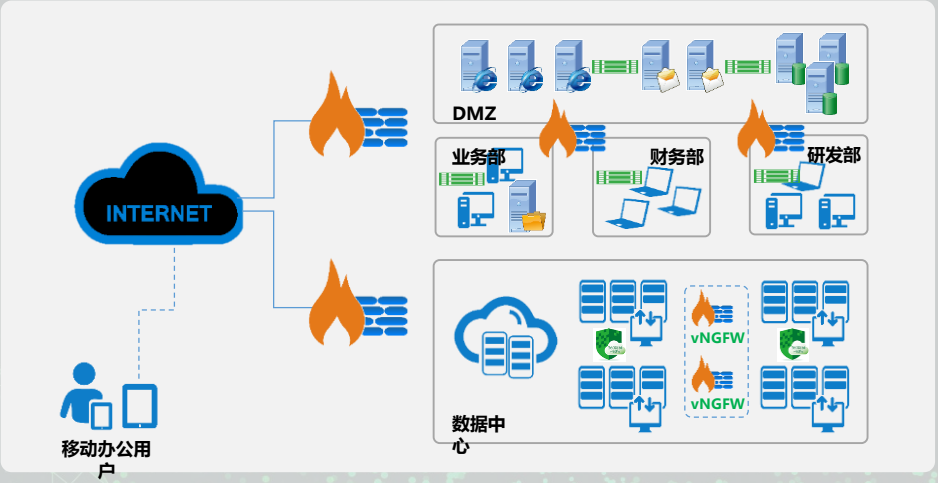
- 规划供应链暴露情况 Map the chain to understand exposures
- 识别风险的切入点 Identify risk entry points
- 列举的风险 Address the risks
- 协调与供应商和合作伙伴的合作（Coordinate and collaborate with suppliers and partners）

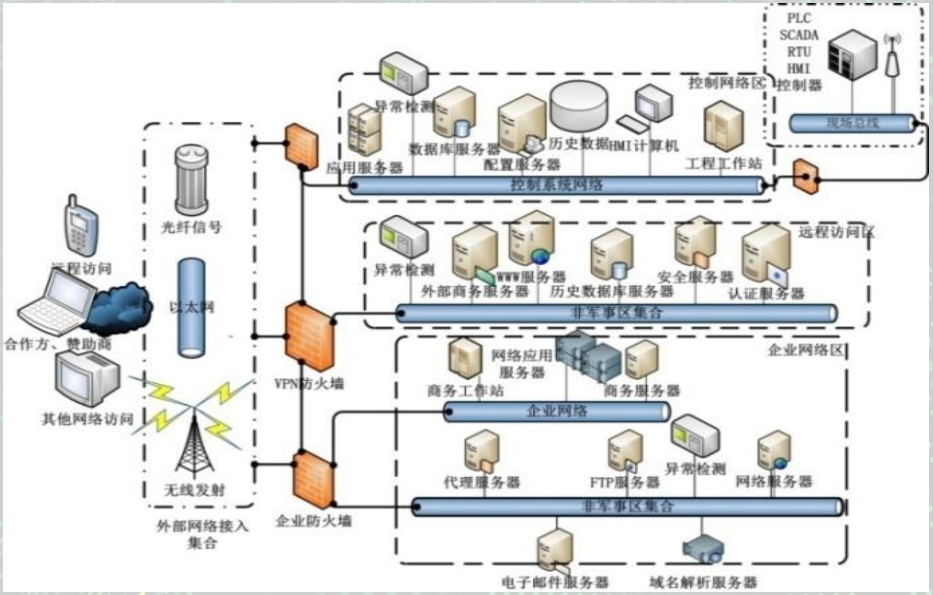
滑动标尺模型（Sliding Scale）



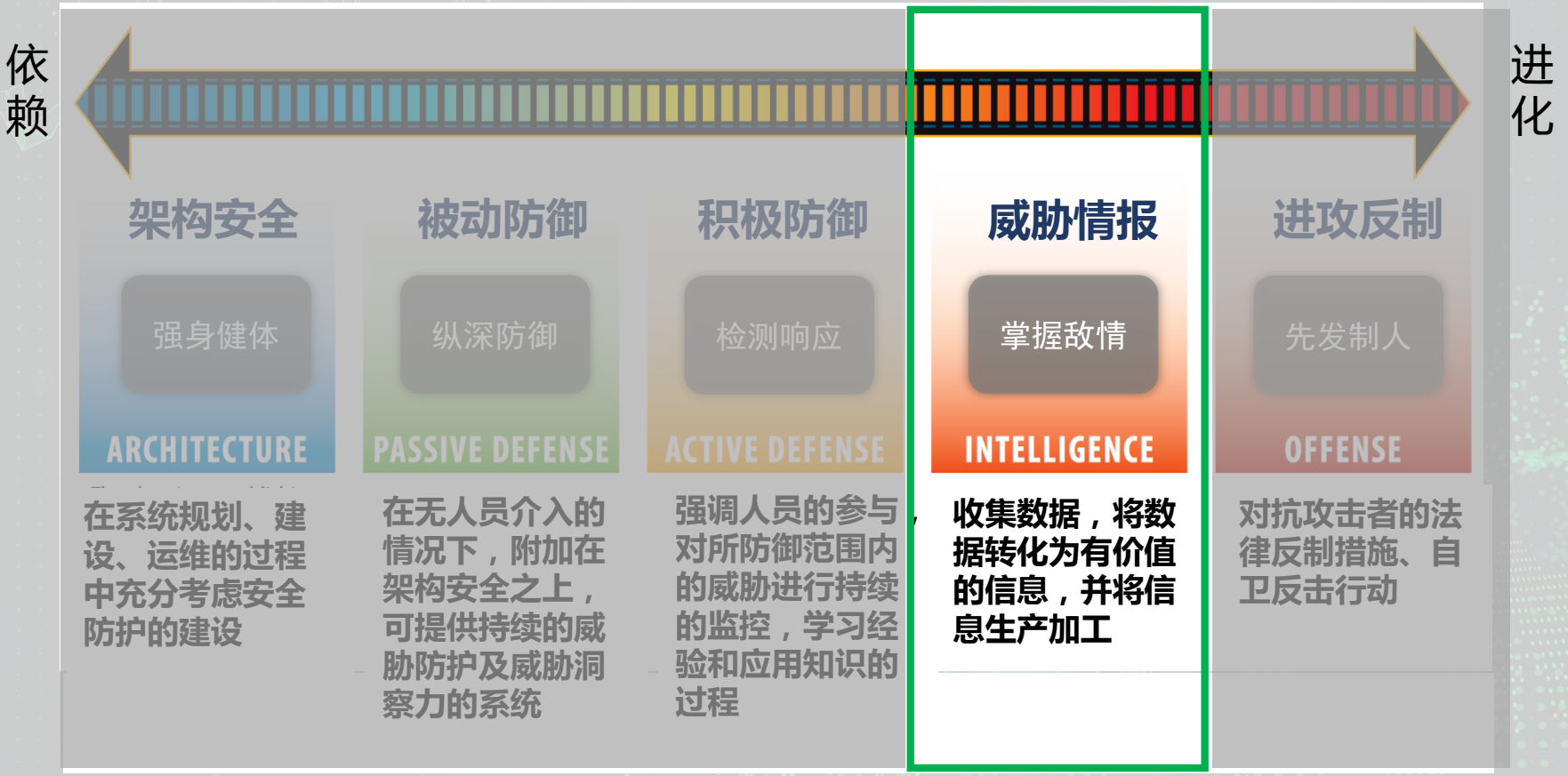
纵深防御：“零信任网络”下的“巷战塔防”

1. 终端防御（杀毒、审计、白名单等）
2. 纵深防御
   - 安全分区、网络专用
   - 横向隔离、纵向认证
   - 审计、蜜罐等
3. 边界防御
   - 工业防火墙、网闸等
4. 安全远程访问（VPN等）
5. 漏洞和补丁管理
   - 漏洞扫描
   - 部分补丁



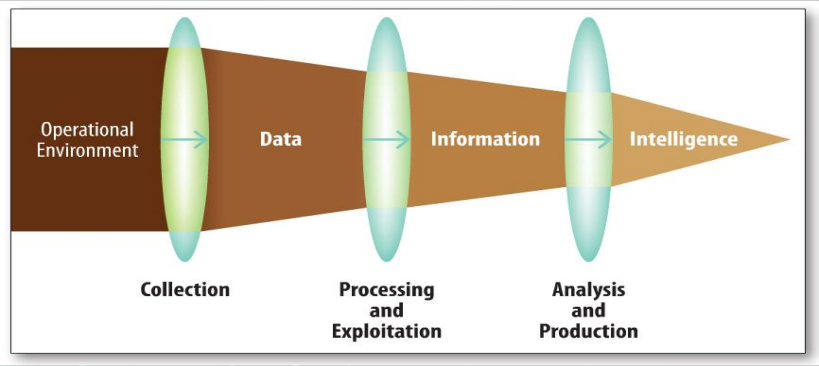


滑动标尺模型（Sliding Scale）



威胁情报的生产

- 程度如何？（指标）
- 现象如何？（表象）
- 后果怎样？（影响）
- 如何补救？（方案）
- 谁攻击的？（源头）
- 目标是谁？（目标）
- 为啥攻击？（动机）
- 手段如何？（工具）



恶意样本行为库
- 总日志**18.9万亿**条
- 每天新增**380亿**

域名解析库
- **90亿**DNS解析记录
- **13年**whois信息

存活网址库
- 每天处理**100亿条**
- 钓鱼数网站**1.4亿**/天

中文漏洞库
- 总漏洞超过**47万**
- 每天新增**500个**

恶意代码样本库
- 总样本**145亿+**
- 每天新增**900万**

安全大数据

第三方数据源
100+

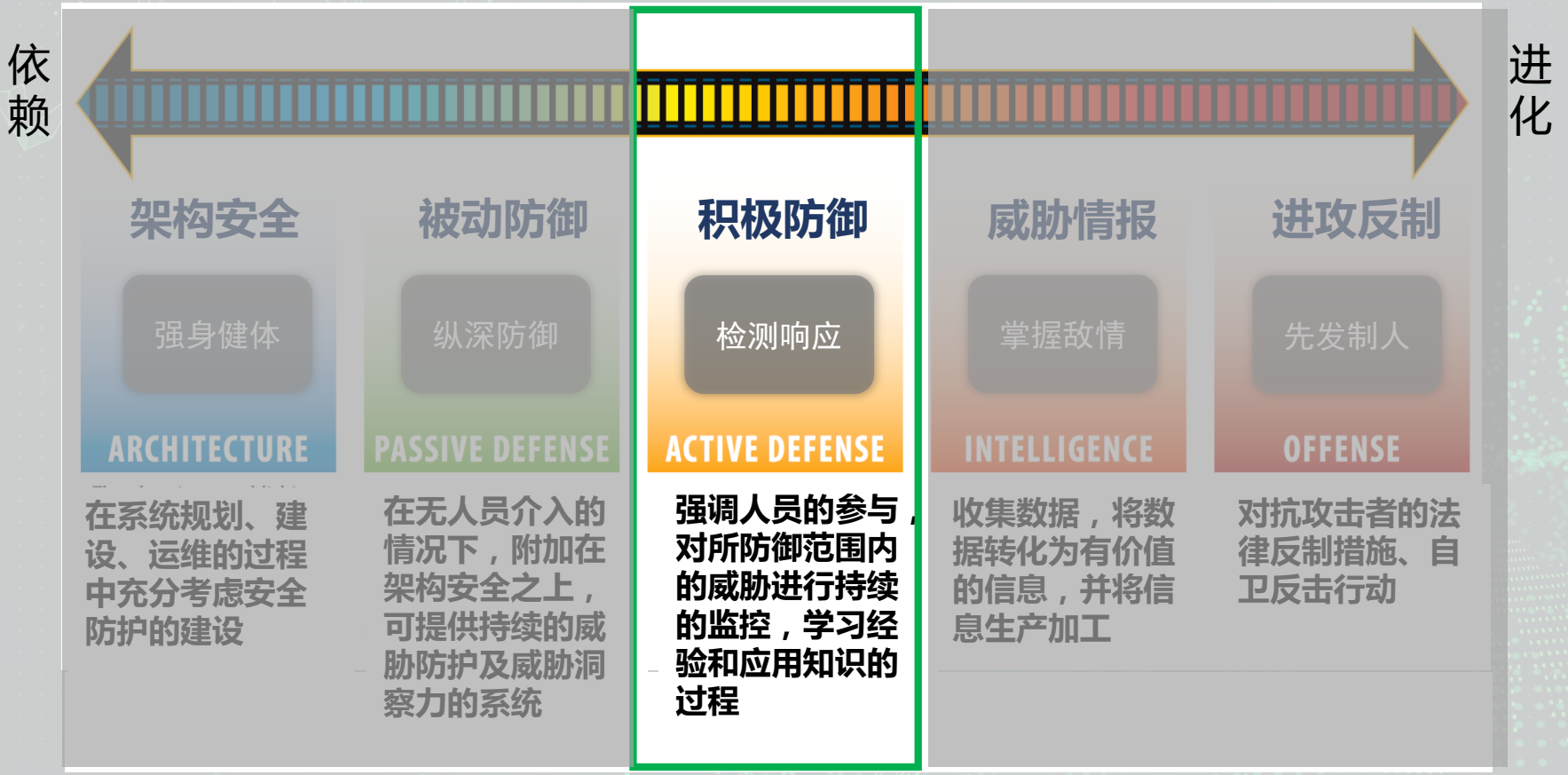
机器学习
大数据分析
- 服务器超**20万**台
- GPU并行计算平台
- **1TB**数据/秒处理能力

云端重沙箱运行

安全专家分析

威胁情报

滑动标尺模型（Sliding Scale）



工业互联网自适应防护架构（PC4R）

信息感知
（Perception）

响应/决策
(Response)

数据汇集
（Connecti）

PC4R

认知预测
(Cognition)

转化分析
(Conversion)

网络融合
(Cyber)

人在回路的回溯、决策、部署、优化、响应，实现安全防护管理与控制（Management & Control）

感知工业现场（压力、摩擦、振动、温度、电流等）物理量数字化、资产

CNC/PLC、DNC、SCADA、MES、ERP工业数据跨层汇集建立（安全数据仓库）

人在回路对规律、异常、目标、态势、背景等完成认知，发现看不见威胁

机理、环境、群体、操作、威胁情报有机结合内容化（Content）和情景化（Context）

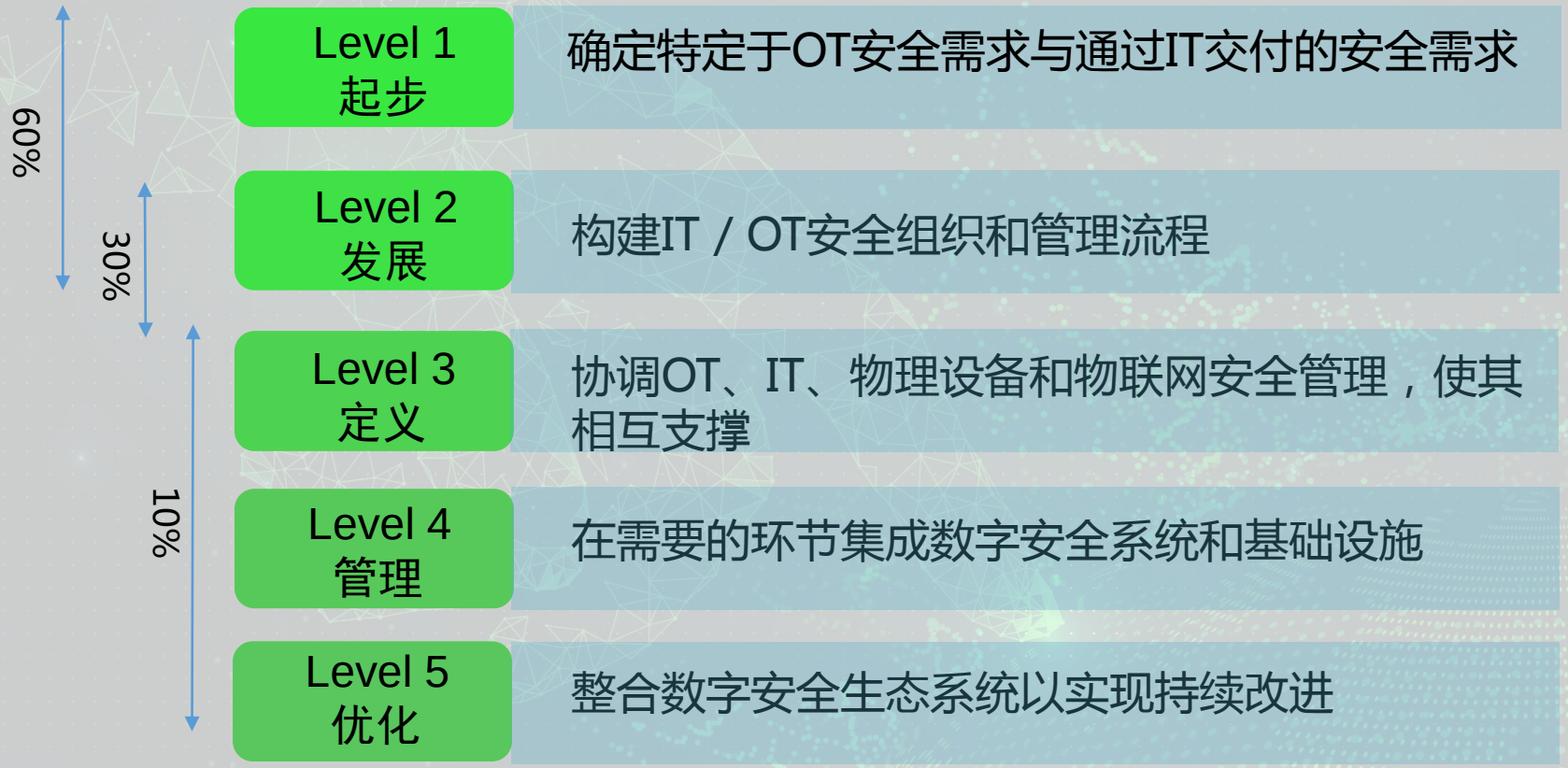
打通IT & OT
人在回路、数据驱动

IT/OT安全问题的管理应对

管理总体思路

1. 建立IT和OT统一的安全团队
2. 规划IIoT架构，进行IIoT资产清查
3. 使用并维护准确和良好的记录库，用于进行风险分析
4. 集中化跟踪用户配置和资产信息、建立所有工业控制系统的资产和配置数据库
5. 采购过程对供应商提安全需求
6. 通过安全运营中心进行管理，实现自动化和可扩展，减少人员需求
7. 采购一个支持异构系统、支持多供应商的网络安全工具
8. 利用深度包检测，监测协议和控制系统漏洞

Gartner G00317591 “Pragmatic Strategies to Improve Industrial IoT Security”

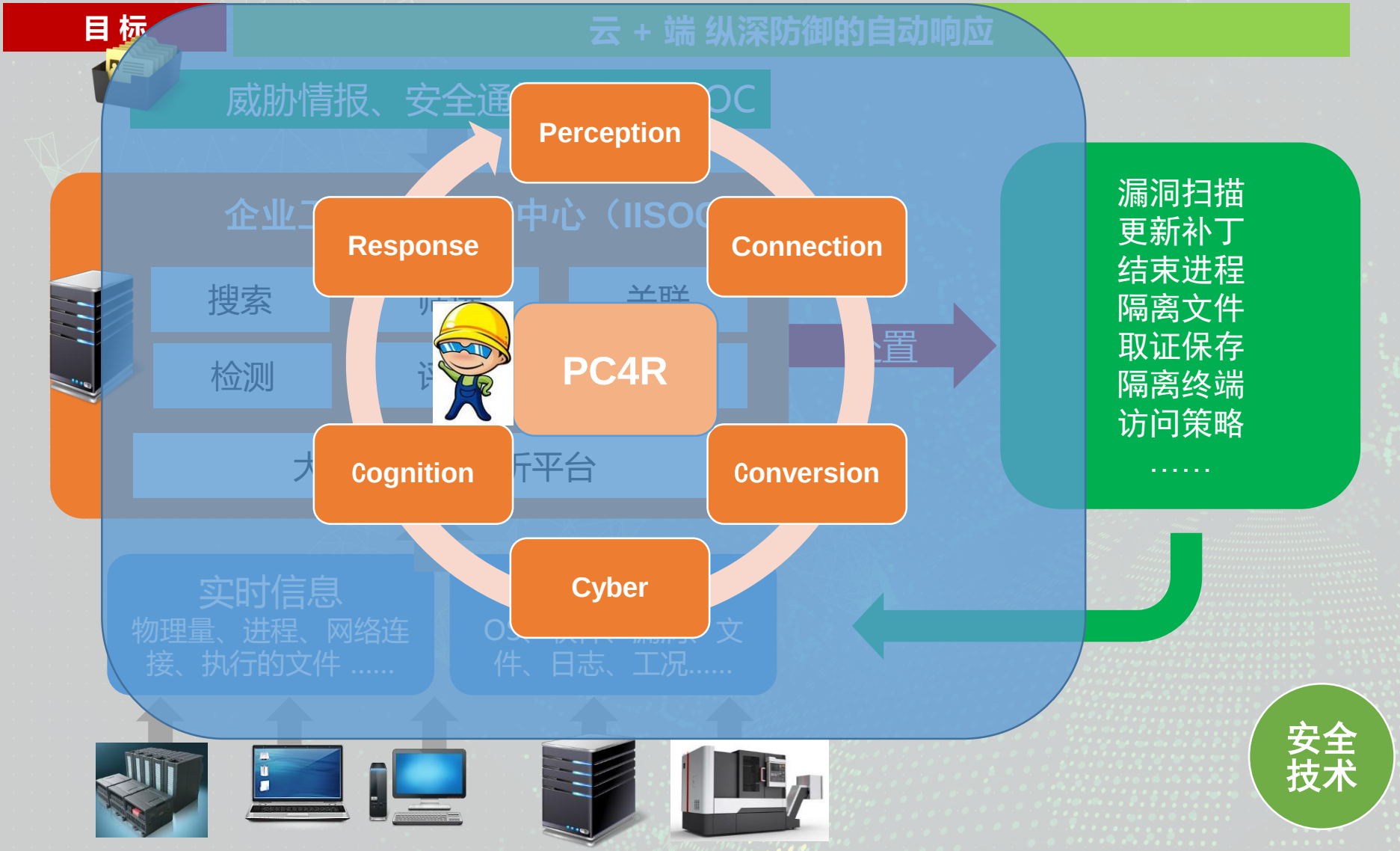

60%
30%
10%
Level 1
起步
确定特定于OT安全需求与通过IT交付的安全需求
Level 2
发展
构建IT / OT安全组织和管理流程
Level 3
定义
协调OT、IT、物理设备和物联网安全管理，使其相互支撑
Level 4
管理
在需要的环节集成数字安全系统和基础设施
Level 5
优化
整合数字安全生态系统以实现持续改进

企业分布

360进行的安全实践

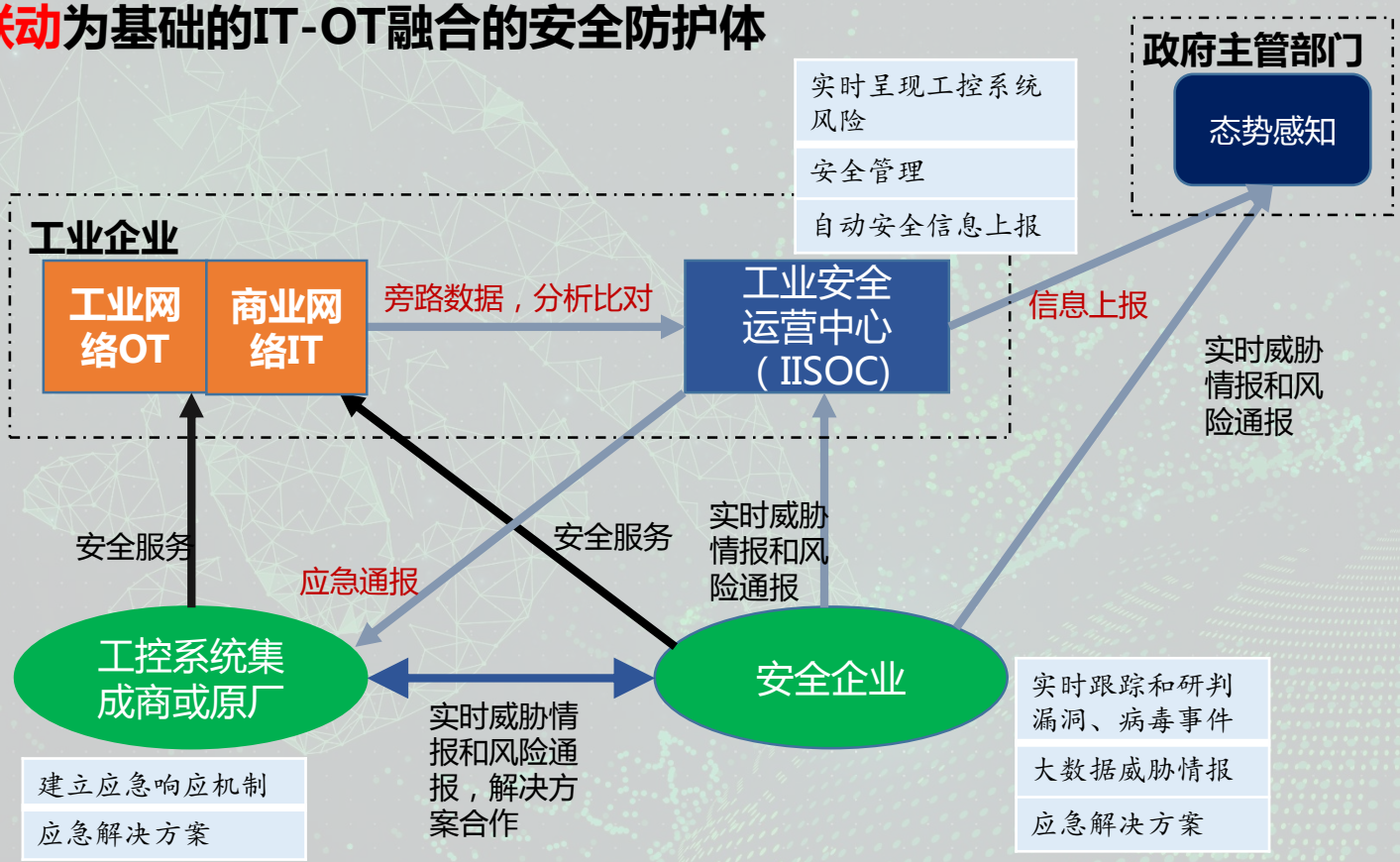
效率 盈利

防御技术路线：建立企业工业安全运营中心



工业安全运营中心（IISOC）

建立以安全运营为中心，以威胁情报为驱动，以协同联动为基础的IT-OT融合的安全防护体系



防御技术路线：构建工控系统安全白环境

目 标　基于大数据，构筑工业互联网系统“安全白环境”整体防护体系

收集数据

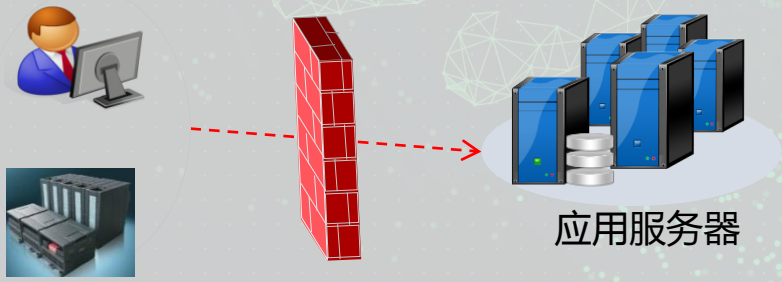
- 持续监控收集，实时探测，云端判断、取证、溯源、修复；
- 被动解决方案，不影响工控系统的“可用性”和“稳定性”
- 工控协议深度解析技术，具备高安全性，低时延影响；

构建白名单

云端+本地，获得“**可信网络白环境**”和“**工业互联网软件白名单**”

可信任的设备才能接入控制网络
可信任的信息才能在网络上传输
可信任的软件才允许被执行

安全技术



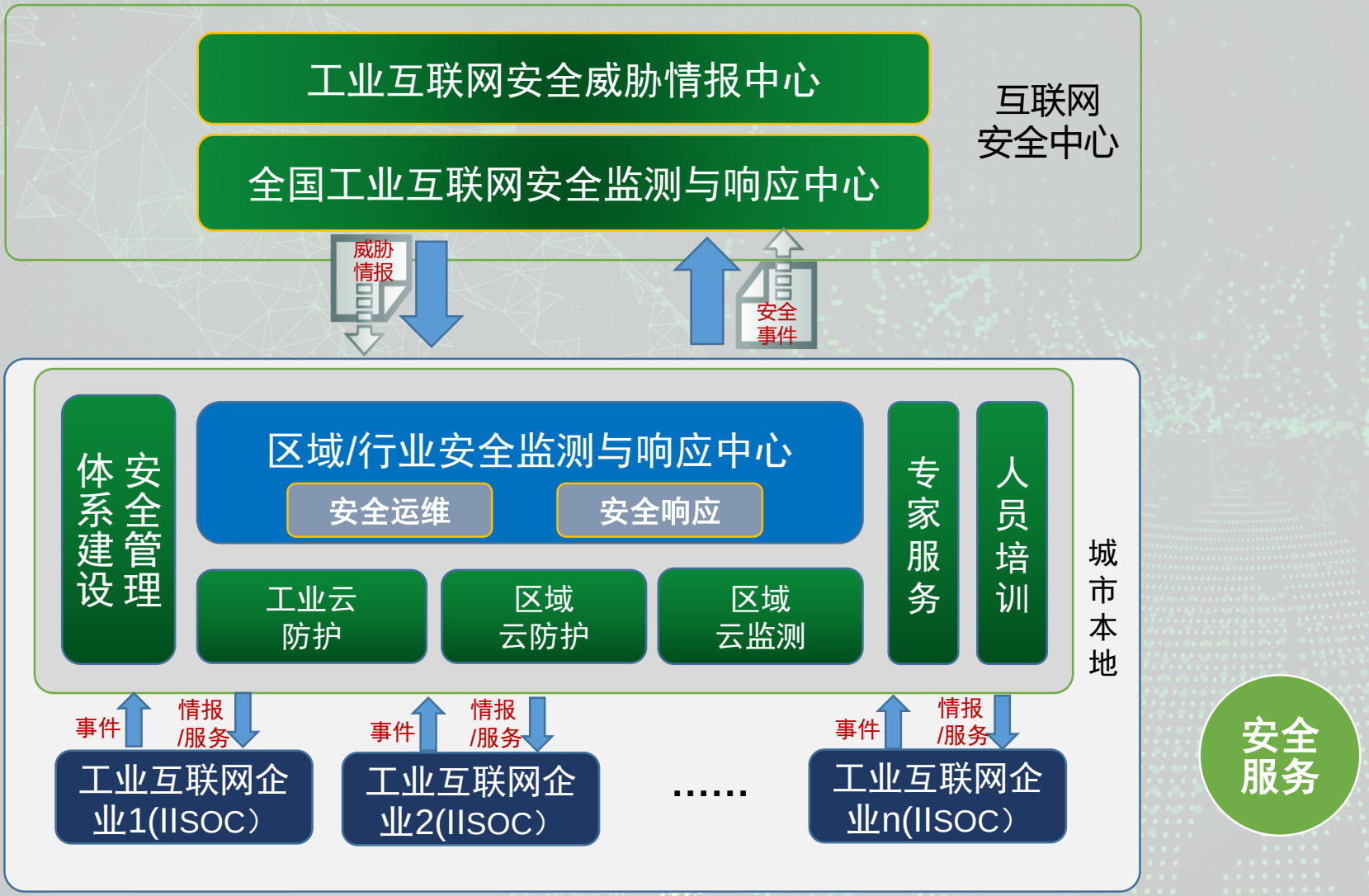
系统进程

应用进程

恶意进程

防御技术路线：多级安全服务体系

目 标 | **协同防御：构建工业互联网企业安全共同体**



具体案例1：永恒之蓝处理

专项态势感知——永恒之蓝传播态势监控：中国

数据驱动工业安全

谢　谢

中国互联网安全大会

360互联网安全中心