
# 工业互联网安全战略落地与推进建议

陶耀东　　360企业安全集团 副总工程师

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018　Beijing · China

# 目录

# 工业互联网 IT/OT 融合的安全挑战？

## SECURITY CHALLENGES FOR IT/OT INTEGRATION

# 工业互联网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

  Improved safety with predictive maintenance to avoid dangerous environments

- 提高经营决策精度和速度

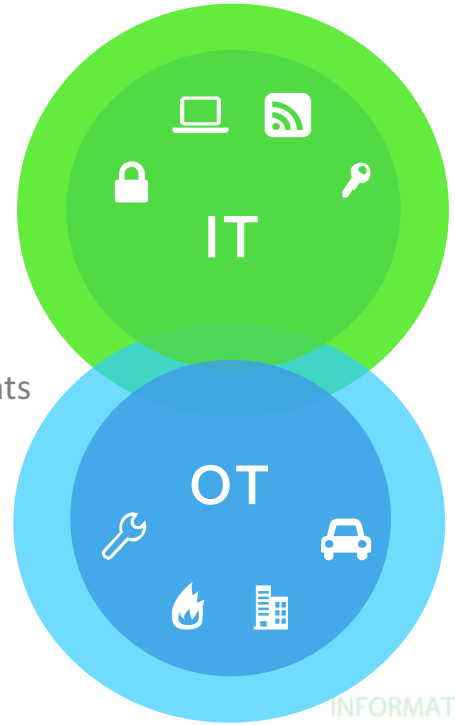
  Increased accuracy and speed in operational decisions

- 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



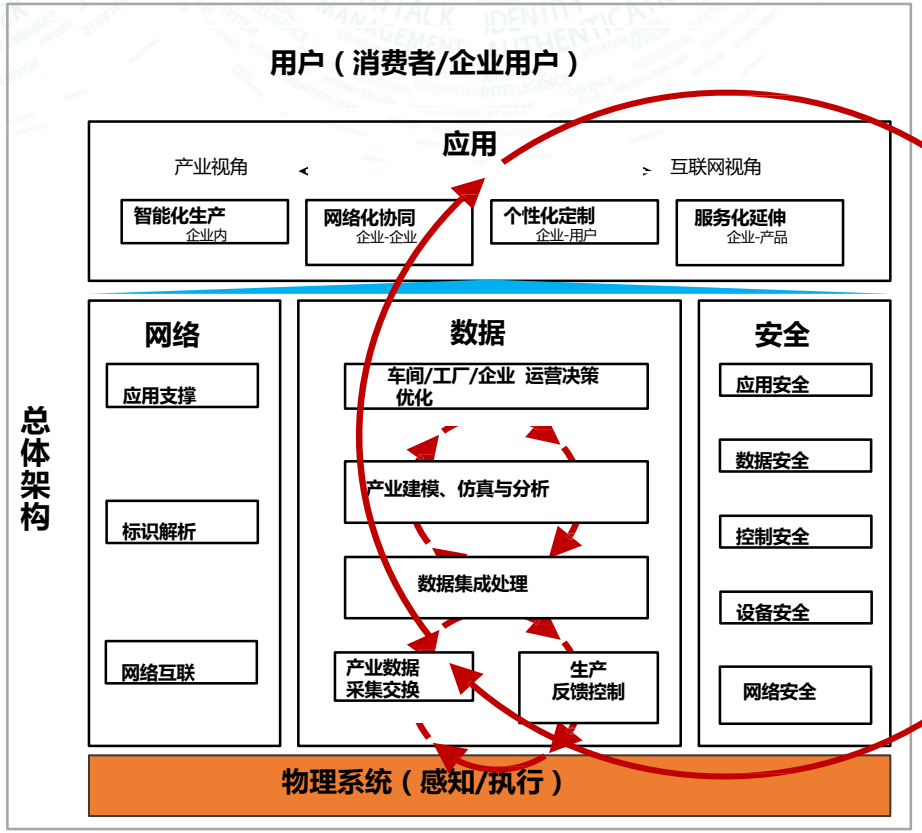

企业在管理方面采用的手段、技术、制度、流程、文档等对信息流管理的统称

监视、控制和保护改变物理环境的系统

**工业互联网= 工业物联网（OT）+ 工业关联的消费性互联网（IT）**

# 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




**智慧应用层安全威胁**

- WEB、ERP、CRM、业务软件
- 网站被黑
- 接入应用存在后门
- 僵尸网络攻击
- 木马攻击
- 蠕虫攻击
- 病毒攻击
- ……

**网络通信层安全威胁**

- 物理攻击
- 网关节点捕获
- 普通节点捕获
- 传输截获、窃听
- 传输篡改、伪造
- DoS攻击
- 重放攻击
- 完整性攻击
- Sinkhole黑洞攻击
- Wormholes虫洞攻击
- HelloFlood攻击
- Wannacry勒索
- ……

**数据及工业云安全威胁**

- 丢失、泄露、篡改
- 商业数据、用户数据泄露
- 跳板入侵、内部入侵、多租户风险
- ……

**控制层安全威胁**

- 控制器漏洞
- 控制协议漏洞
- 控制软件漏洞
- 配置错误
- 身份鉴别弱/缺失
- 凭证管理不足
- ……

**设备层安全威胁**

- 感知设备被攻击（仪表、传感）
- 执行设备被攻击（泵、阀..）
- ……

**表现：攻击入口多、防御剖面大！　　后果：带来物理伤害、威胁生命！　　原因：缺乏现代威胁理解和安全架构**

# IT环境与OT环境 安全功能差异

| 安全功能 | IT | OT |
| --- | --- | --- |
| 防病毒和移动代码 | 很常见，轻松部署和更新。用户可以控制定制可以是基于资产或基于企业的 | **内存的限制**要求可能会影响ICS;<br>只能通过售后解决方案保护传统系统;<br>通常需要“排除”文件夹以避免程序隔离关键文件 |
| 补丁管理 | 容易定义; 企业范围内实施;可以远程和自动化 | 成功的安装补丁程序需要长时间验证;<br>定制性OEM产品难打补丁； 可能影响ICS功能；<br>资产所有者需要明确定义可接受的风险 |
| 技术生命周期 | 2～3年；大量供应商；无处不在的升级 | 10～20年；通常是单个供应商； |
| 资产分类 | 常用，每年执行一次；结果驱动支出 | 必需时执行；资产可见性低；资产价值与适当对策没有联系 |
| 事件响应和取证 | 易于开发和部署；有明确监管规定；采用嵌入技术 | 侧重于系统恢复活动；取证程序不成熟；需要良好的IT/ICS关系 |
| 物理和环境安全 | 范围可以从差（系统）到优秀（关键的IT系统） | 通常对关键区域非常有用；现场设施的成熟度各不相同 |
| 安全系统开发 | 整个开发过程的一部分 | 长久以来，不是整个开发过程的一部分；供应商走向成熟，但比IT慢；核心ICS解决方案在安全性方面困难重重 |
| 安全合规 | 取决于部门的监管监督 | 根据部门（而不是所有部门）的具体监管指导 |

**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1：8.3 台积电勒索停产事件

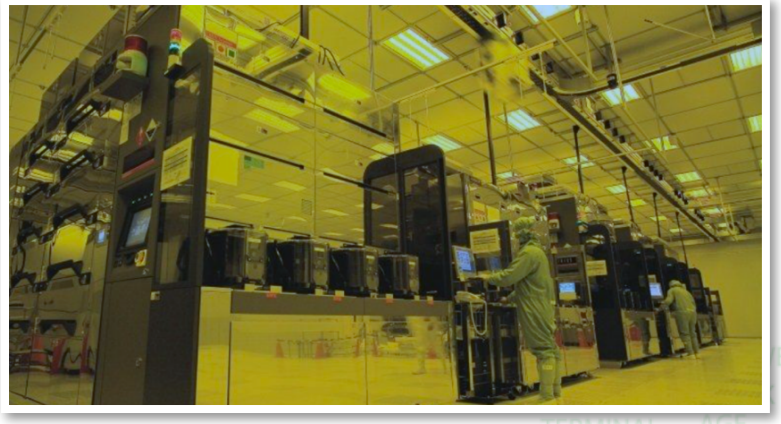
（网络安全+控制安全）

**IT/OT状态**

- 台湾三工厂直接IT、Ot融合互联，全球多工厂
- IT和OT网络融合
- 严格网络安全管控和U盘管控
- 大量机台·接入网络，标准SOP
- 与台湾以外工厂防火墙连接


**攻击过程**

- 8月3日周五，新机台安装引入病毒
- 数分钟内wannacry大规模攻击3个工厂停产，机器蓝屏重启损失严重，受影响机器超万台
- 8月6日下午召开记者会：应对完毕，损失：近2亿美元、毛利降1%



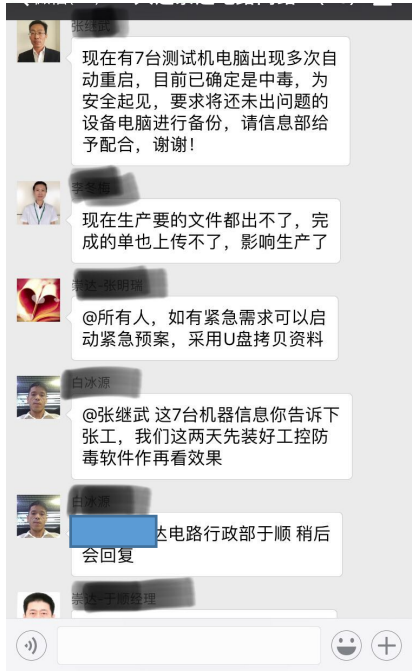
**解决**

- 建立防呆机制（人和技术协同）
- 推动网络安全保险

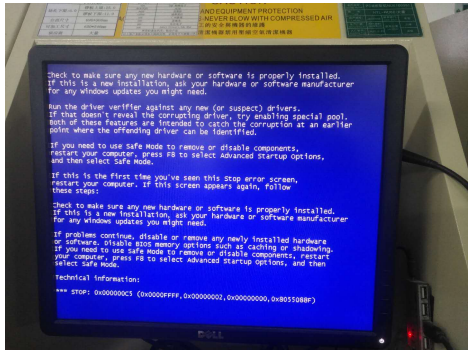
近一年：航空界的波音公司、汽車界的雷 諾、日產與本田、 貨運界的 **Maersk**、物流業的 **FedEx**，均遭受到了勒索病毒的攻击损失巨大？

# 案例2：某电路板企业（控制安全）

**2018年4月3日**接到客户的**应急需求**：**东北某电路板企业**有200台左右工控机，50台已被Wanncry感染出现反复蓝屏或重启现象，严重影响正常生产，大量订单积压








**进行安全服务应急响应后，部署工业安全产品，进行安全防护**

# 案例3：某装备企业上千台工程机械“失联”（设备安全）

## 事件背景

2016年6月底，某装备巨头向长沙县公安局报案。 山东、江苏、山东、福建、内蒙、辽宁、新疆、广州、 杭州等地陆续有数十台机械失联，导致技术研发和售后服务大受影响，更有大量客户恶意拖欠该公司 货款，失联泵车价值高达数千万元


## 攻击过程

内鬼张某把ECC系统中的锁机模块删除后，重新制作成刷机镜像。就像破解后的windows系统一样，只要把这个镜 像刷入泵机，就能实现解锁，使其“失踪” ，每台收取1-2万；


**启示：**

1. **工业互联网带来商业模式的创新**
2. **安全问题也随之而来**
3. **工业互联网平台也为安全带来了解决方案**

**未来将采用工业互联网、数字双胞胎，云制造，数字供应链等的超数字化工厂，安全问题可能产生可怕的后果!**

In the future, Ultra-digital factories such as the Industrial Internet, Digital Twins, Cloud Manufacturing, Digital Supply Chains, etc. will be adopted. Security problems may have disastrous consequences.

# AII联盟Q3全会工业企业调研（100+）

**自我判断（乐观了？）：**

1、 行业内对自己单位的网络安全水平都有较高的认可

2、 超过一半的企业认为自己公司不会遭受攻击

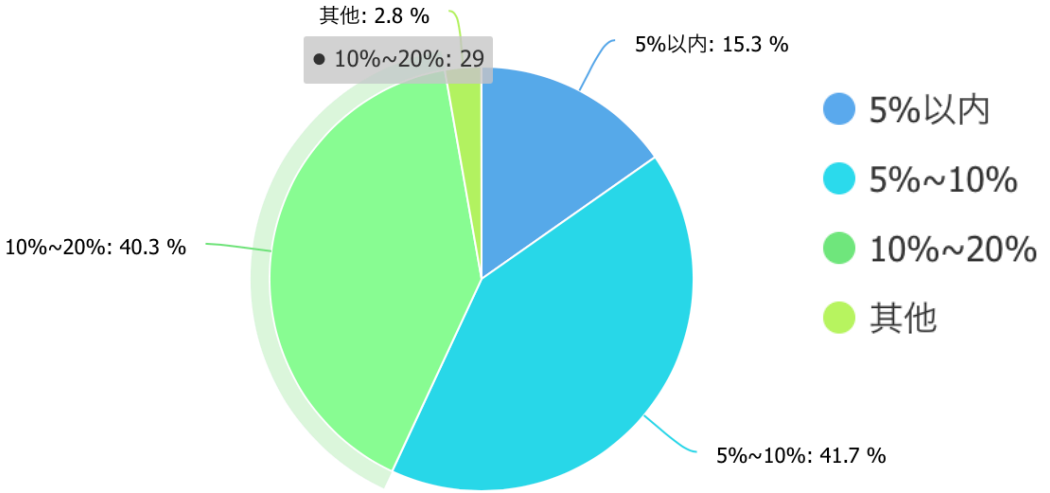
**趋势：**

1、国家政策的推动有利于工业互联网网络安全的实施

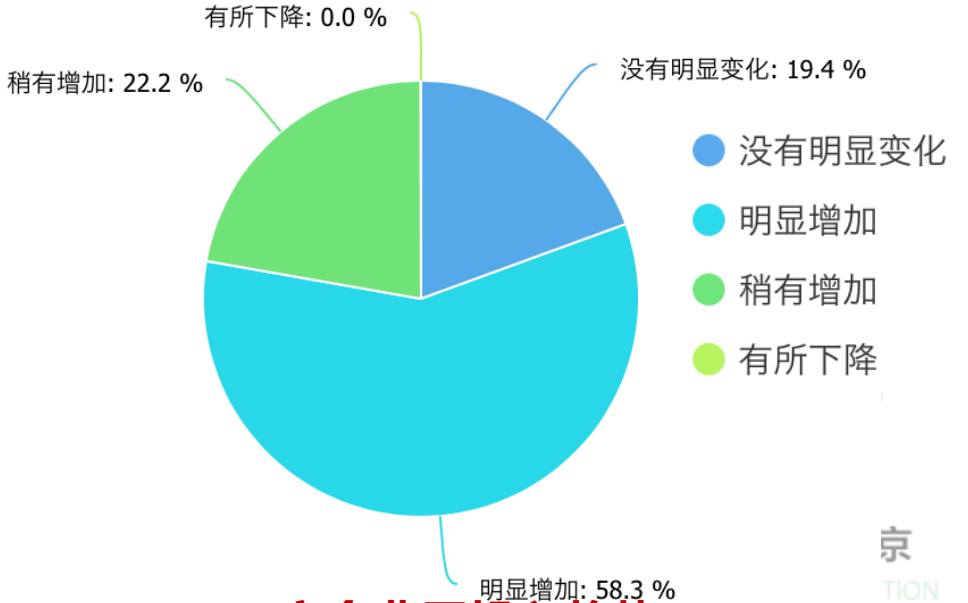
2、80%企业认为安全投入应占工业互联网投入的5%-20%

3. 超76.4%认为高层领导决策决定公司的网络安全重视程度

4、工业网络安全最大挑战是安全人才匮乏




**安全建设费占工业互联网投入的比例**

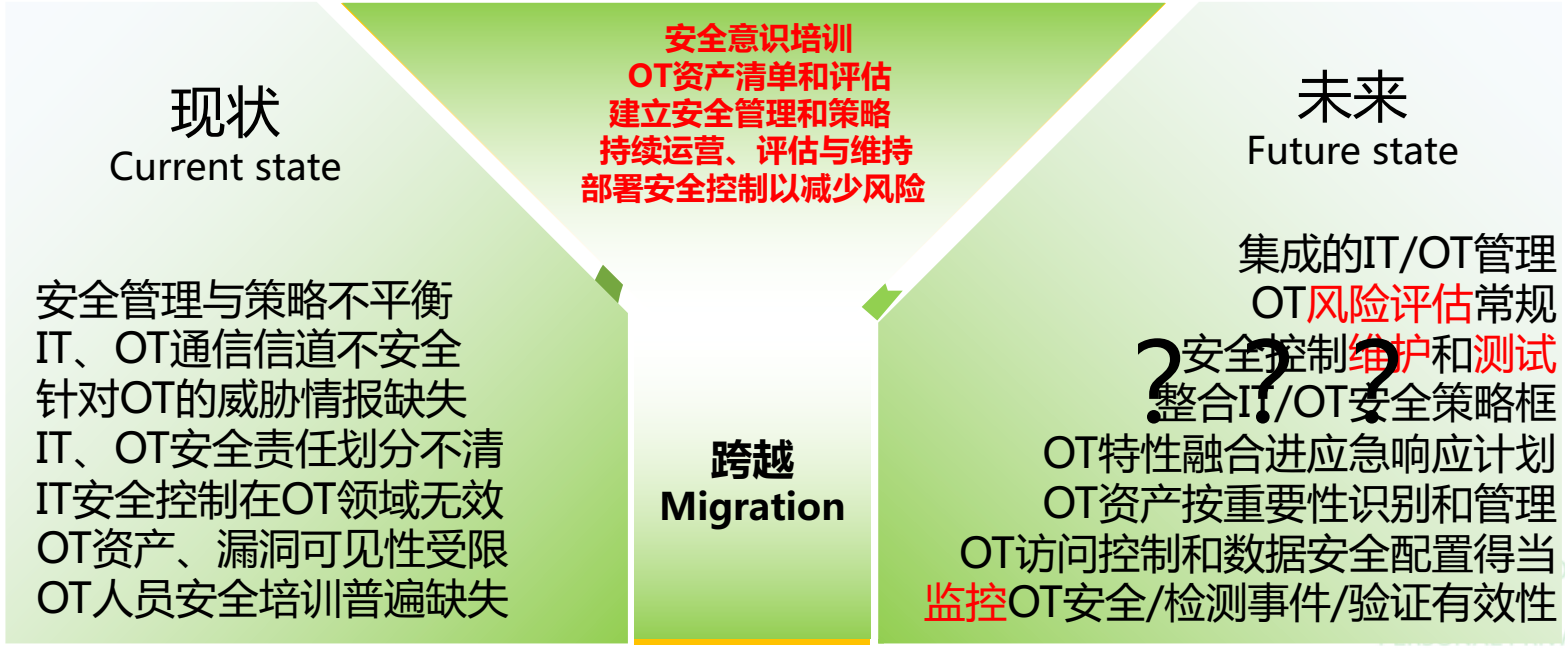



**安全费用投入趋势**

ZERO TRUST SECURITY

# IT/OT一体化安全现状-GAP（鸿沟）

安全和风险管理者应该在充分了解安全现状的基础上，规划与设想企业安全生产的未来安全图景，并在两者之间寻找企业目前缺失的安全管理和控制手段，然后对症下药，找到过度至未来安全图景的方法。



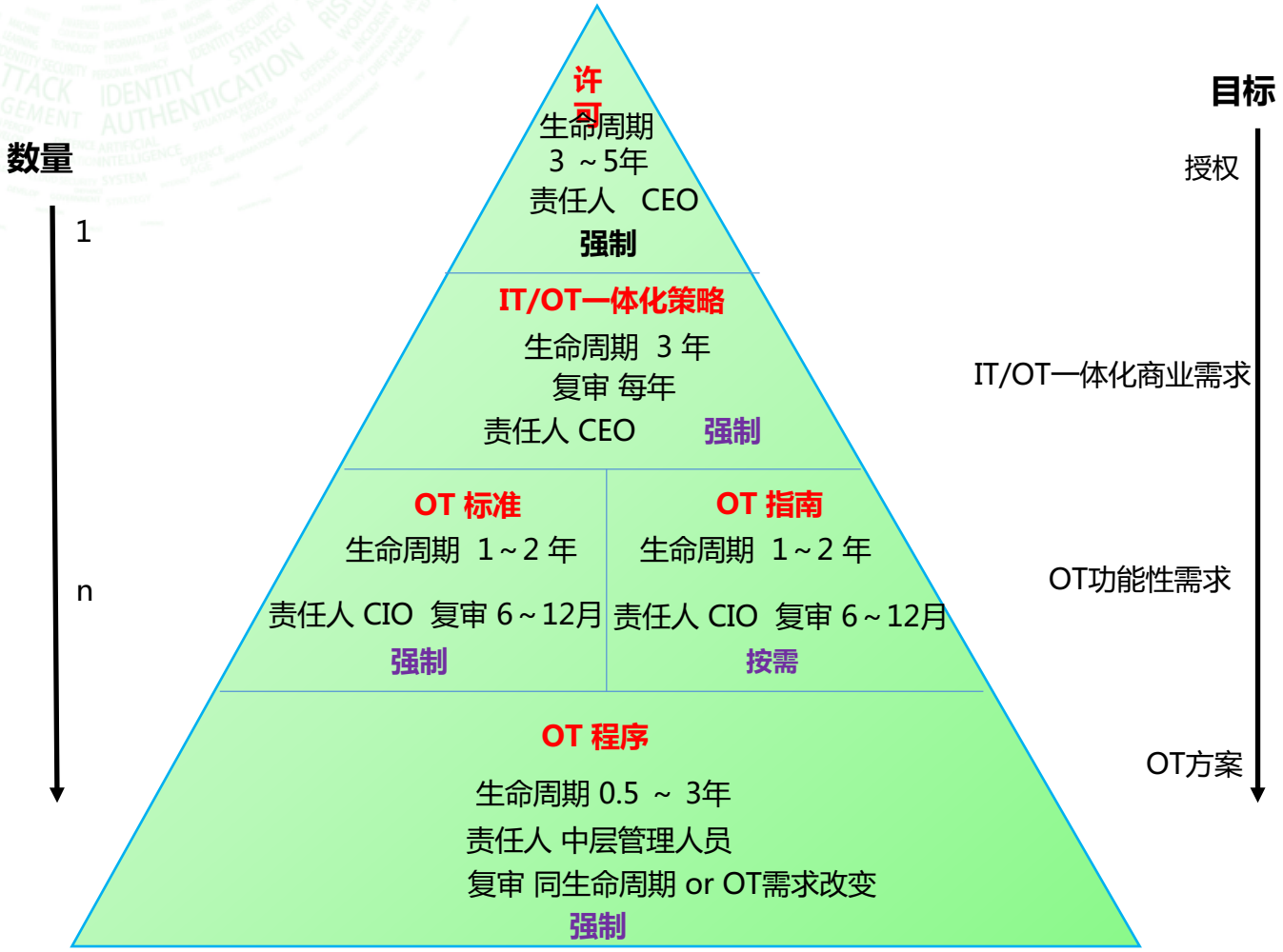

安全战略路线图

# 工业互联网的安全如何应对？

## HOW TO PROTECT INDUSTRIAL INTERNET SECURITY

ZERO TRUST SECURITY

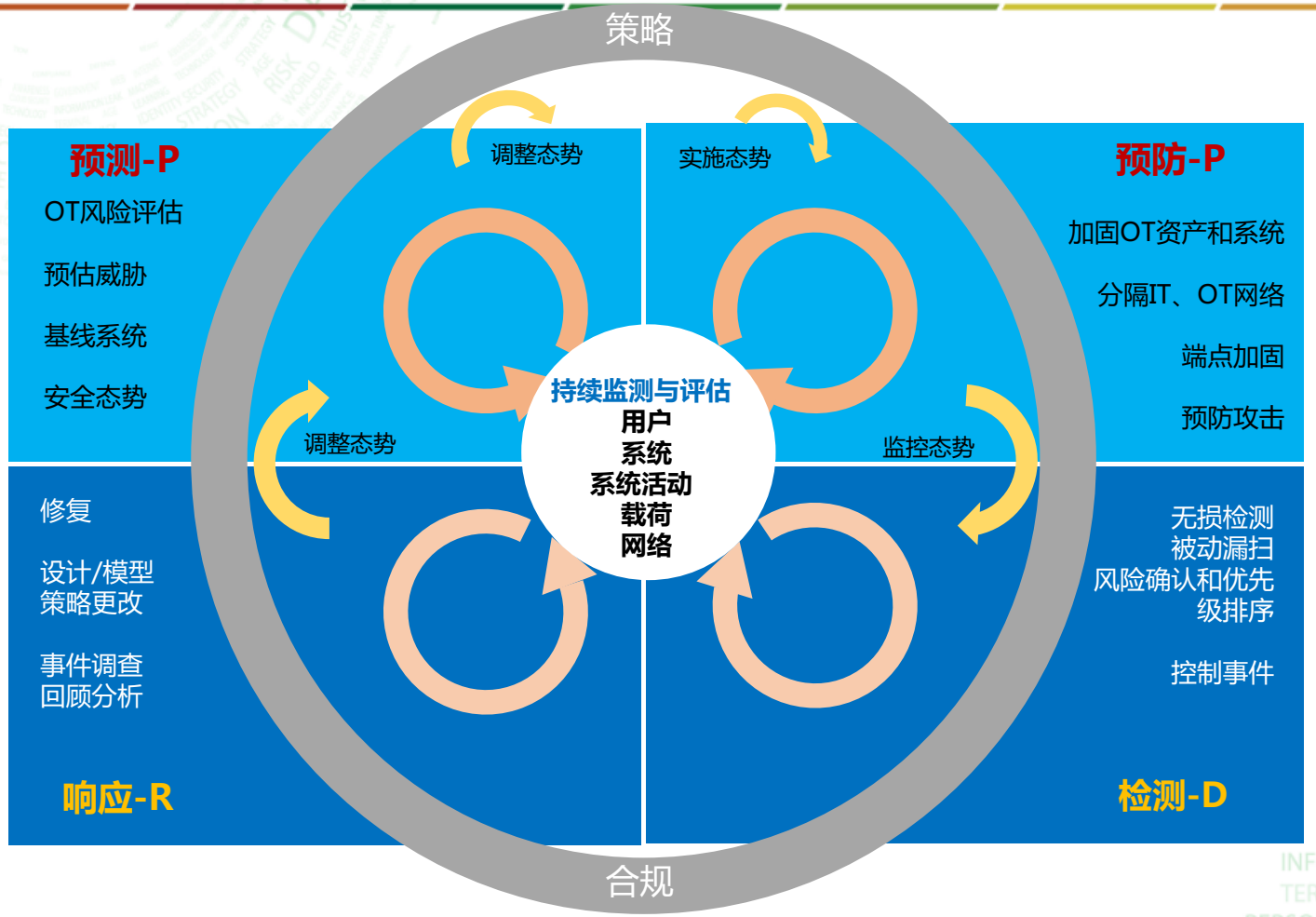
# IT/OT一体化安全发展路线




IT/OT一体化安全策略框架（Gartner）

**集成的IT和OT安全性是一个业务问题**

# IT/OT一体化的自适应防护架构

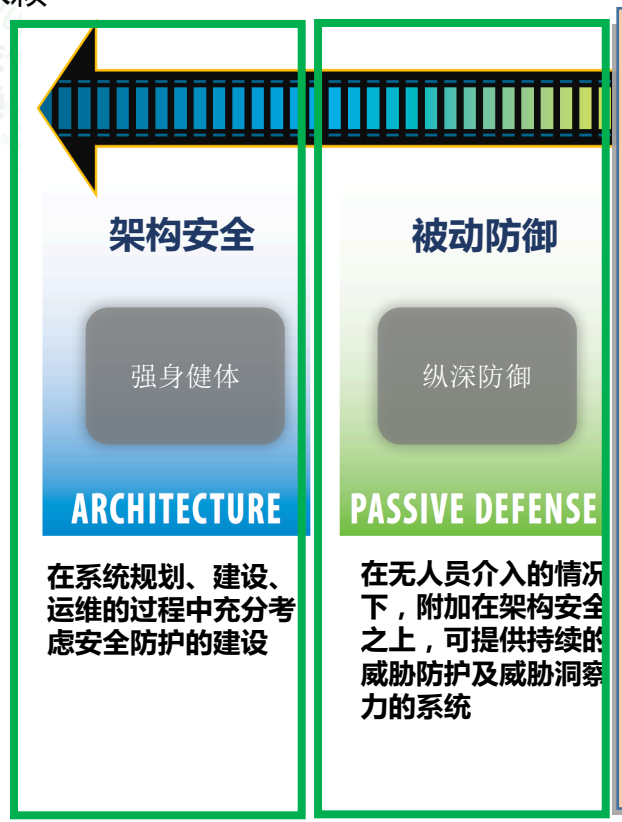


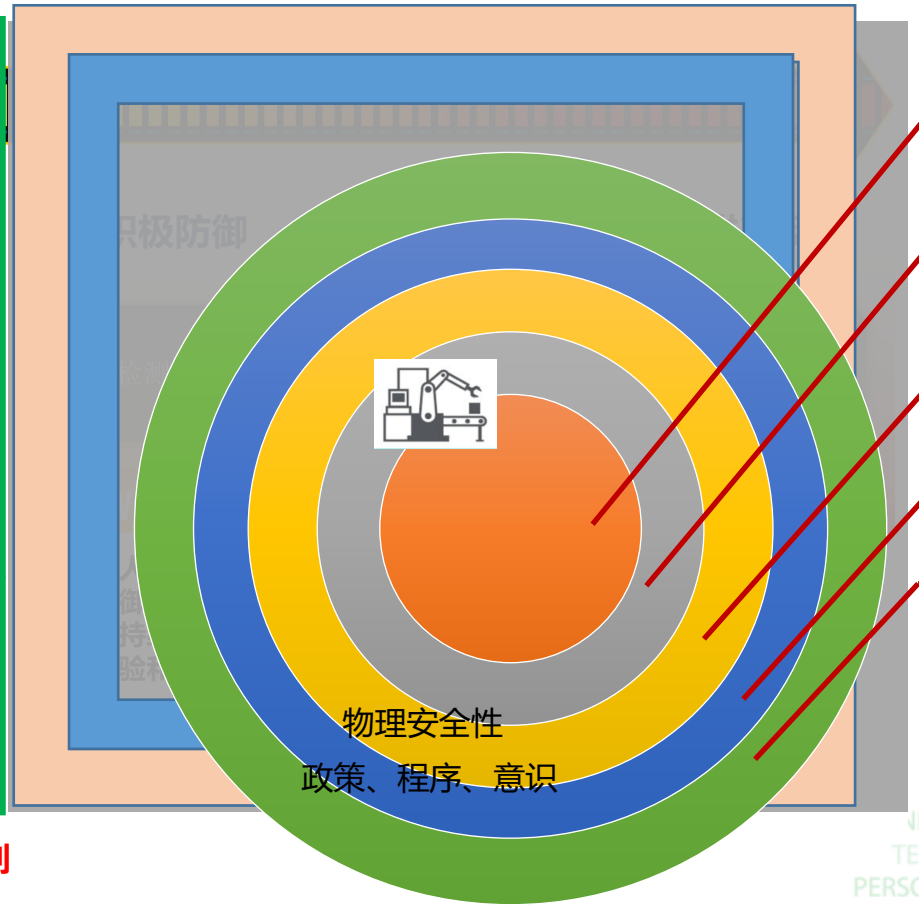

Gartner IT-OT自适应安全架构

# 安全的滑动演进（Sliding Scale）

依赖

进化

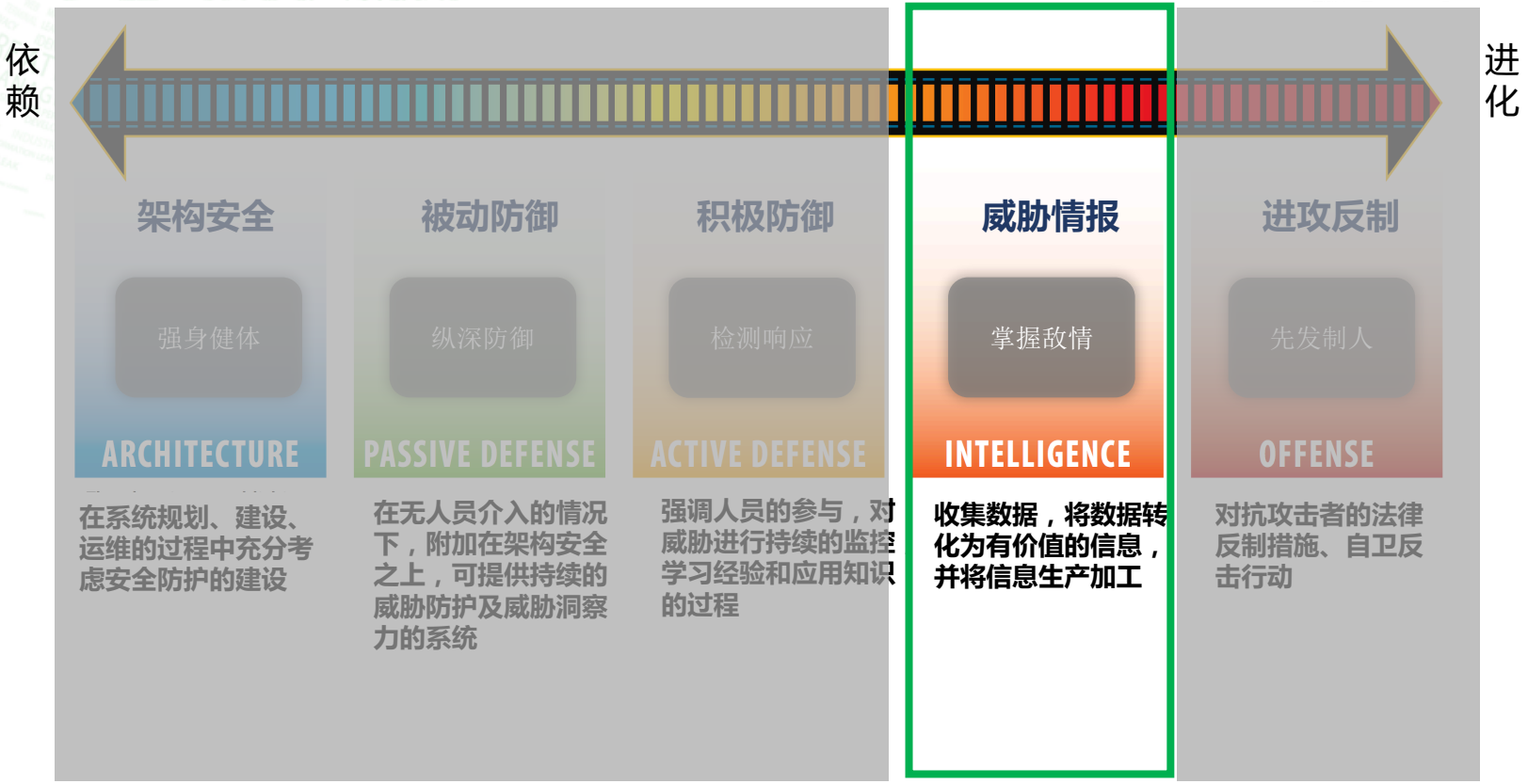



- 嵌入式设备加固
- **选择合适的供应商和组件**
- **进行管理认证和访问控制**
- 协议与[illegible]
- **遵循最佳实践的远程访问**
- **开发结构化的补丁管理和验证程序**
- 应用与资产加固
- **使用网络分段的方法隔离关键系统**
- 网络分段
- 周边防御

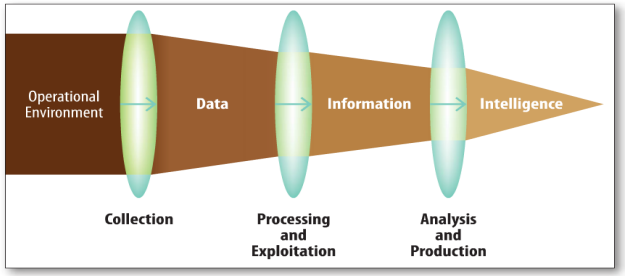
- **IT和OT功能安全与信息安全一体化规划**
- **（投入产出最高）**

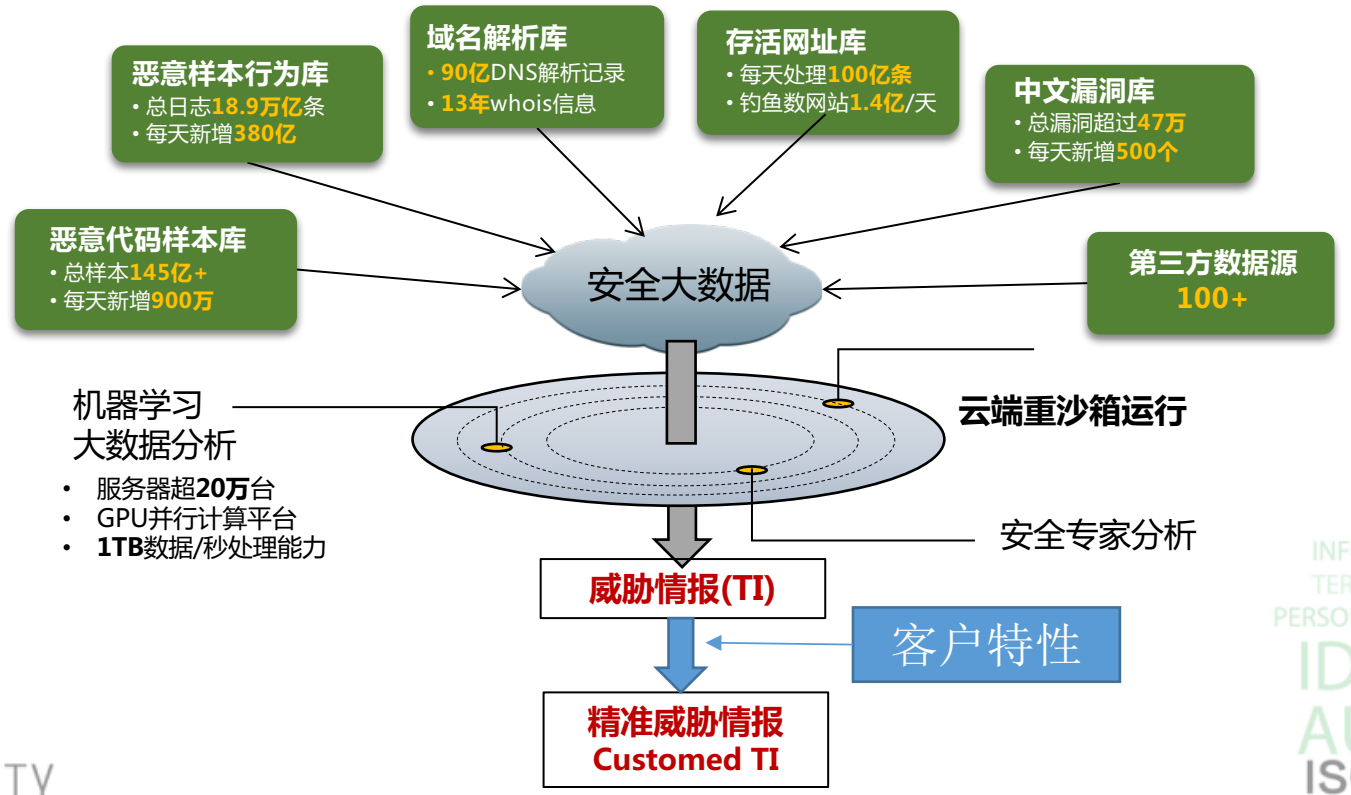
# 安全的滑动演进（Sliding Scale）



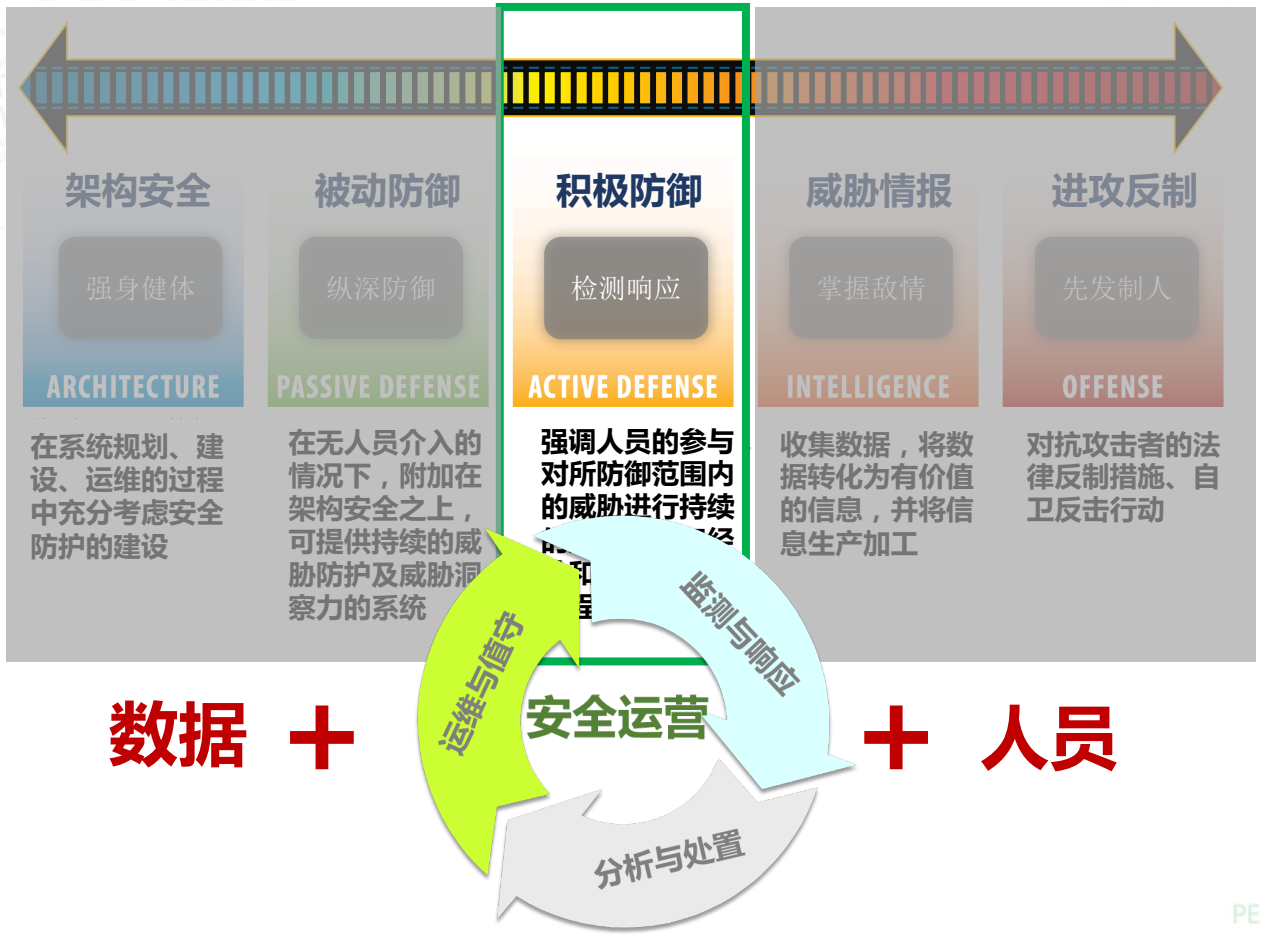
# 威胁情报的生产

- 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）



# 安全的滑动演进（Sliding Scale）

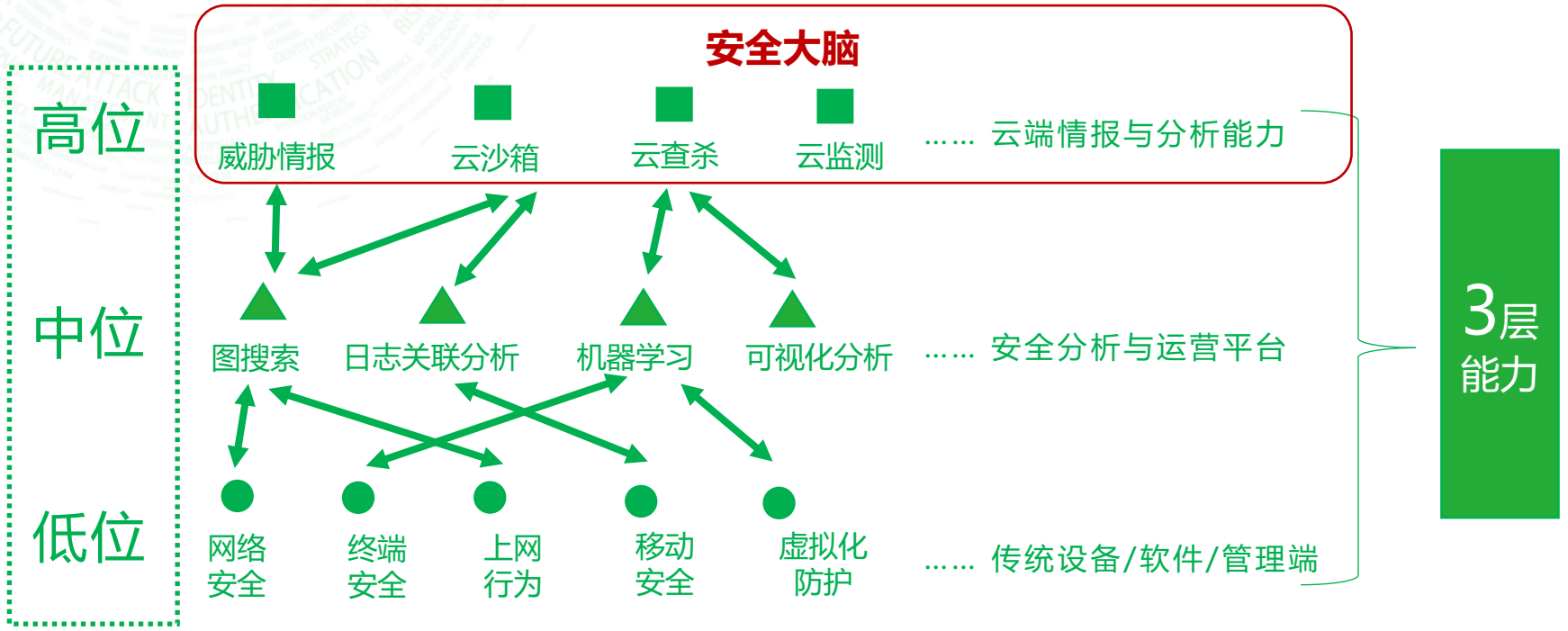


# 360在IT/OT协同防护的安全实践
## SECURITY PRACTICE

ZERO TRUST SECURITY

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

# 数据驱动的三层安全能力构建




**低位能力(Field)**

- 数据的生产和采集
- 数据的广度和深度

**中位能力(Middle)**

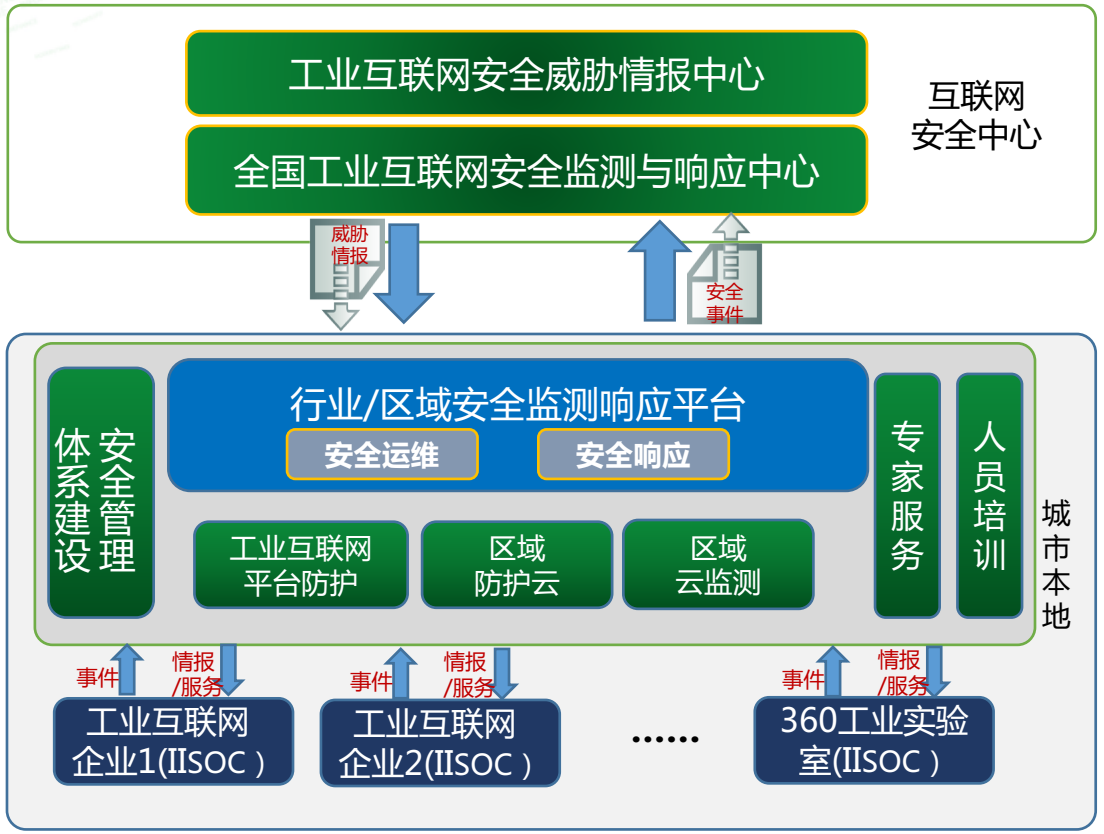
- 数据的建模与分析
- 数据的治理与质量

**高位能力(High)**

- 威胁情报
- 云端安全大数据

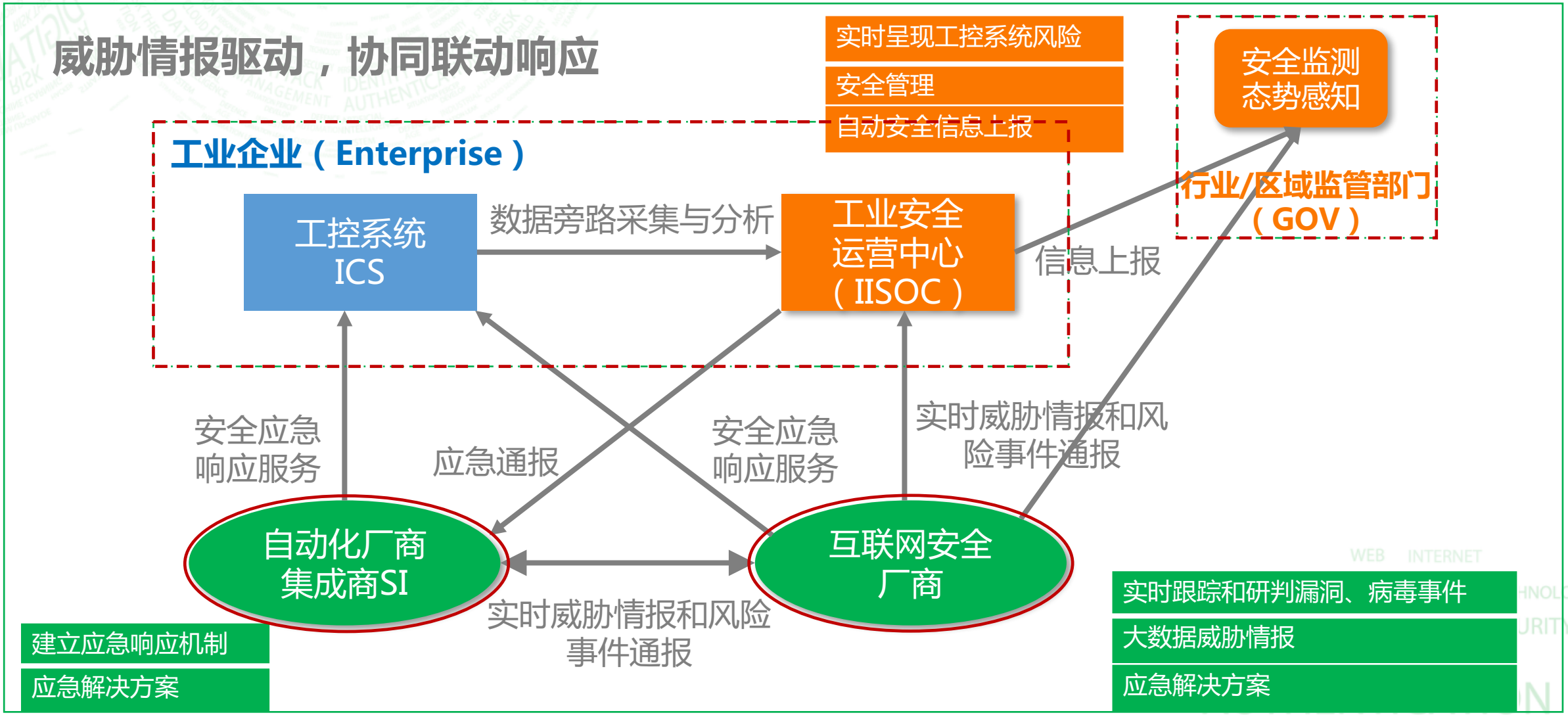
# 防御技术路线：多级安全服务体系

**目 标** **协同防御：构建工业互联网企业安全共同体**




安全服务

# 协同联动：建立工控安全应急响应协同机制



# 工业互联网安全工作思路

## 01 资产发现及梳理（asset）

### 工业安全服务 services

资产发现和梳理；
流量分析，威胁发现；
工控安全体系化设计；
模拟环境渗透测试；
对安全事件响应演练；
安全意识培训；

### 工业安全检查评估工具 Tools

威胁情报匹配；
异常行为和未知威胁检测；
工控资产发现与漏洞扫描；
工控合规检查及报告生成；
工控协议解析、流量分析；
行为日志、项目管理等；

## 02 安全隔离与防护 (Isolation and protection)

### 工业控制安全网关（Gate）

工控协议的深度解析；
IT、OT一体化安全防护；
白名单智能学习；
入侵防御、病毒等威胁检测；
全面风险信息展示及分析；
高可靠的传输加密；

### 工业安全主机防护（Endpoint Protect）

智能机器匹配白名单生成
多种模式一键切换；
**外部设备安全管控；**
**针对wannacry防御技术；**
支持多种操作系统；
工业主机统一管理；

## 03 安全监控与审计 (Monitoring and auditing)

### 工业安全审计系统

工控网络异常检测；
**工控关键事件检测；**
**工控关键业务中断检测；**
**工控网络流量审计；**
**支持网络会话审计；**
**支持协议规约检测；**
**支持基线检测功能；**

## 04 安全管理与运营（Management and operation）

### 工业安全运营中心

**企业级工业安全运营平台**
应急响应平台与可视化
**基于威胁情报的攻击发现**
**工控关键操作监测**
**流量监测、**异常行为监测
关键资产管理、日志采集与管理
上报风险事件、响应处理

### 工业安全管理系统

工控安全设备和系统管理;
统一配置和运维;
实现策略配置下发;
网络流量分析;
工业控制网络运行实时掌握;

## 05 工业态势感知 (Situation Awareness)

### 工业态势感知

**区域行业威胁风险和事件感知**
**工业安全监测系统**
预警通报系统
**事件处置系统**
**情报信息系统**
**综合管理系统**

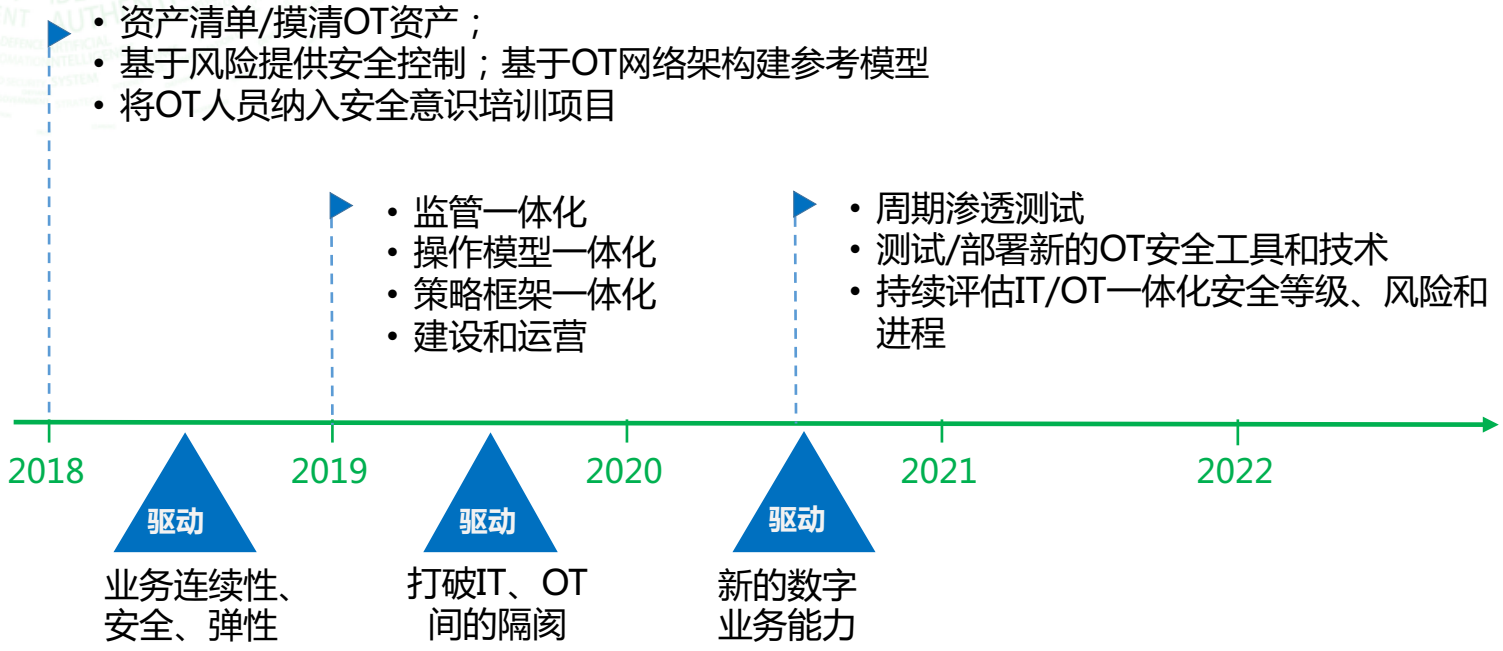
# 工业互联网安全战略推进建议

## PROPOSALS FOR PROMOTING INDUSTRIAL INTERNET SECURITY STRATEGY

ZERO TRUST SECURITY

# IT/OT一体化安全的战略推进时间表

安全治理是长期且复杂的过程，难以一蹴而就，需要循序渐进




## 战略路线图时间表

# 战略推进节拍-高优先级（意识、组织、评估、监测）

**近期**

- **安全意识培训**

  大多数安全事件是由于人为错误造成的。人仍然是网络安全环境中最脆弱的环节，IT如是，OT亦然。

- **形成一个统一的IT/OT安全治理机构**

  统一的IT / OT安全治理机构，由：管理层、IT团队、OT团队成员组成，在实现安全治理时提供最全面、代表企业最根本利益的解决方案。

- **OT资产管理**

  对OT资产进行充分管理，包括清点、分类、跟踪记录等。OT资产一般包括设备、过程、软件、网络资源、人员等。根据OT资产相对应的风险等级，制定安全应对方案。

- **对目标系统的安全评估**

  确定系统中存在的安全风险。包括：远程访问、VLAN不当使用、BYOD安全控制、第三方服务水平等

- **利用监测工具提高OT资产可见性**

  - 可以有效利用资产发现工具，对OT资产进行发现和管理，提高可见性和可控性。

# 战略推进节拍-中优先级（运营、流程、系统）

**中期**

- **继续将统一的IT/OT安全治理工作正式化**

  - OT安全功能范围的准确划分、选择合适的安全模型、什么技能至关重要、哪些技术需要更改

- **建立共同的IT/OT安全运营模式，建立联合角色、责任、流程和系统**

  - 确定了OT安全运营内容。资产和系统之间的互联和关系的复杂性和指数级增长，IT、OT和安全功能的纵向和横向集成和融合，网络威胁不断增长，需要更灵活和响应的运营模式。

- **修订现有安全策略框架**

  - 针对IT和OT的角色和责任定制安全策略或更新现有安全策略、保证宣贯和落地

- **OT网络及安全防护建设**

  网络分割、身份和访问控制管理、远程访问控制、无线网络安全控制等。OT网络中无线网络安全控制要一同部署，保障OT安全

- **使用工业防火墙、主机防护实施IT/OT网络安全控制**

  - OT系统中存在许多架构限制，选择合适的工业防火墙可有效解决工业网络分段和安全控制问题。选择合适的主机防护和工业主机防护，保护端点安全问题

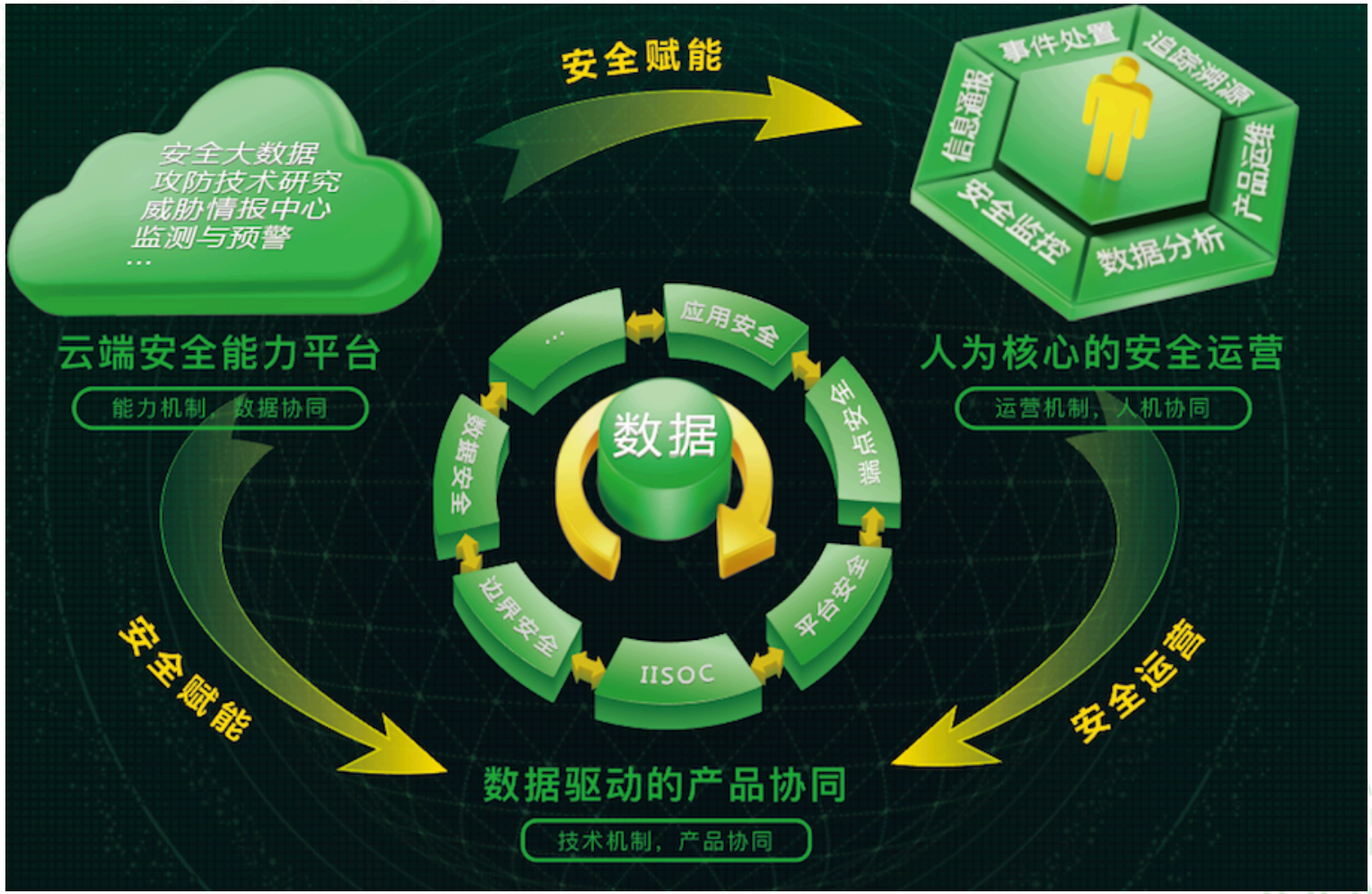
- **持续实施安全监测**

  开始并持续实施安全监测，例如实施配置管理、变更管理、定期审计等。

# 战略推进节拍-低优先级（持续运营、评估、改进）

**远期**

- **定期进行测试**
  定期进行外部渗透测试、漏洞扫描等安全测试工作。
- **应用新的OT安全工具和技术**
  - 发现、引入先进的IT、OT安全工具和技术，进行的概念验证、实现、测试、部署、维护
- 衡量和控制OT安全流程及其有效性
- 持续评估综合IT/OT安全级别
- 识别可能影响OT功能的基础设施和系统的潜在变化


安全赋能
安全大数据
攻防技术研究
威胁情报中心
监测与预警
…
事件处置
追踪溯源
产品运营
数据分析
安全监控
信息通报
云端安全能力平台
能力机制，数据协同
人为核心的安全运营
运营机制，人机协同
数据
应用安全
安全运营
平台安全
IISOC
边界安全
数据安全
…
安全赋能
安全运营
数据驱动的产品协同
技术机制，产品协同

# 谢 谢！