360 企业安全

安全第一 就用360

工业互联网产业联盟
Alliance of Industrial Internet

工业互联新时代
人是安全的核心

陶耀东

AII安全组执行主席

360工业控制系统安全国家联合实验室 主任

创新引领 融通发展

2018 工业互联网峰会

INDUSTRIAL INTERNET SUMMIT 2018

目录

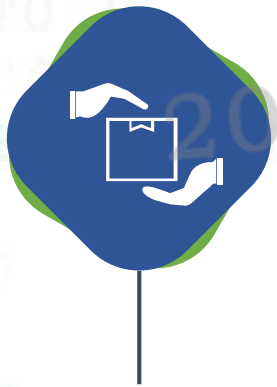
2018工业互联网峰会

一、互联网+先进制造 中国发展新动力

互联网、人工智能、先进制造构建融合系统，各国给予高度重视，先后提出相应发展战略

2006

《美国竞争力计划》将互联网与先进制造融合列为重要的研究项目，CPS概念正式提出



2012

美国发布“先进制造业国家战略计划”，将网络与先进制造融合放在了未来工业发展的战略层面

2013

德国政府在汉诺威工业博览会上正式推出“工业4.0”战略，其技术核心是制造业的网络化、智能化

2014

美国发布“AMP2.0”，指出优先发展制造业中的先进传感技术、控制技术，虚拟化、信息化和数字制造以及先进材料制造

2015

中国政府正式发布“中国制造2025”战略，力争跻身制造强国行列，其中互联网+先进制造技术占据着举足轻重的位置

互联网 + 先进制造 构成工业互联的信息物理系统（CPS）

一、互联网+先进制造 中国发展新动力

我国将发展“工业互联网”作为“制造强国”和“网络强国”建设的关键支撑

2015年3月9日，工信部下发了《2015年智能制造试点示范专项行动实施方案》

- 2015年启动**超过30个**智能制造试点示范项目
- 2017年扩大范围，在全国推广有效的经验和模式。

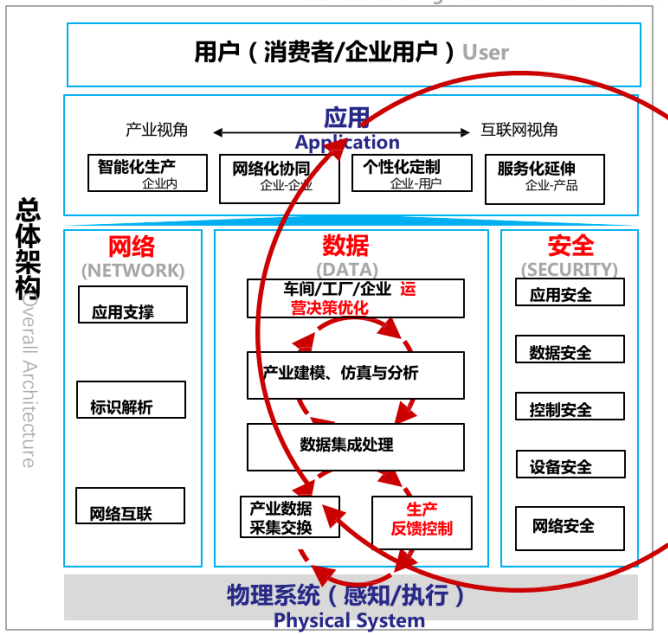
2015年5月8日，国务院印发了《中国制造2025》

- 推进五大工程：制造业创新中心、智能制造工程、工业强基工程、绿色制造工程、高端制造装备工程
- 十大领域：**新一代信息技术**、高档数控机床与机器人、航空航天装备、海洋工程装备及高技术船舶、先进轨道交通设备、节能与新能源汽车、电力装备、农机装备、新材料、生物医药及高性能医疗器械

2017年11月27日，国务院印发《深化“互联网+先进制造业”发展工业互联网的指导意见》

- 四大应用模式：**智能化生产、网络化协同、个性化定制、服务化延伸**
- 打造3体系：网络体系、平台体系、**安全体系**
- 推进2应用：大型企业集成创新和中小企业应用普及两类应用
- 构筑3支撑：产业、生态、国际化
- 提出了7项主要任务 ：基础设施升级工程、平台建设及推广工程、标准研制及试验验证工程、关键技术产业化工程、集成创新应用工程、区域创新示范建设工程、**安全保障能力提升工程**

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
3 Intelligent Closed Loops: Intelligent production control, Intelligent operational decision optimization, Accurate docking between consumer demand and manufacturing



数据(DATA)：**本质是数据智能在工业中的全周期应用**，包括“采集交 换-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。

网络(NETWORK)：**本质是实现数据智能的 网络基础**，包括网络互联、标识 解析、应用支撑三大体系。

安全(SECURITY)：**本质是工业/产业互联网 各个领域和环节的安全保障**，包括设备安全、控制安全、网络安 全、应用安全等。

二、新动力下 网络安全进入大安全时代

360企业安全 安全第一 就用360

“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”

——2014习近平中央网信领导小组第一次会议讲话提出网络强国战略愿景

“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。

——2016年4月19讲话习近平在网信工作座谈会讲话

2018工业互联网峰会

现在的网络攻击，与过去完全不同。现在一个病毒就可以造成几十亿美元的经济损失，全球网络安全已经进入**大安全时代**

- 大安全时代，物联网、车联网、工业互联网、关键信息基础设施 成为攻击目标
- 大安全时代，网络犯罪和网络恐怖主义的潘多拉盒子已被打开
- 大安全时代，网络安全产业与军工产业合并，军民融合成为必然
- 大安全时代，**网络安全出现了六种新常态**

新常态1：漏洞军火化，军火民用化

新常态2：网络攻击产业化，网络犯罪集团化

新常态3：应急响应小时化

新常态4：“重保”常态化

新常态5：“等保”法制化

新常态6：态势感知自动化

2018工业互联网峰会

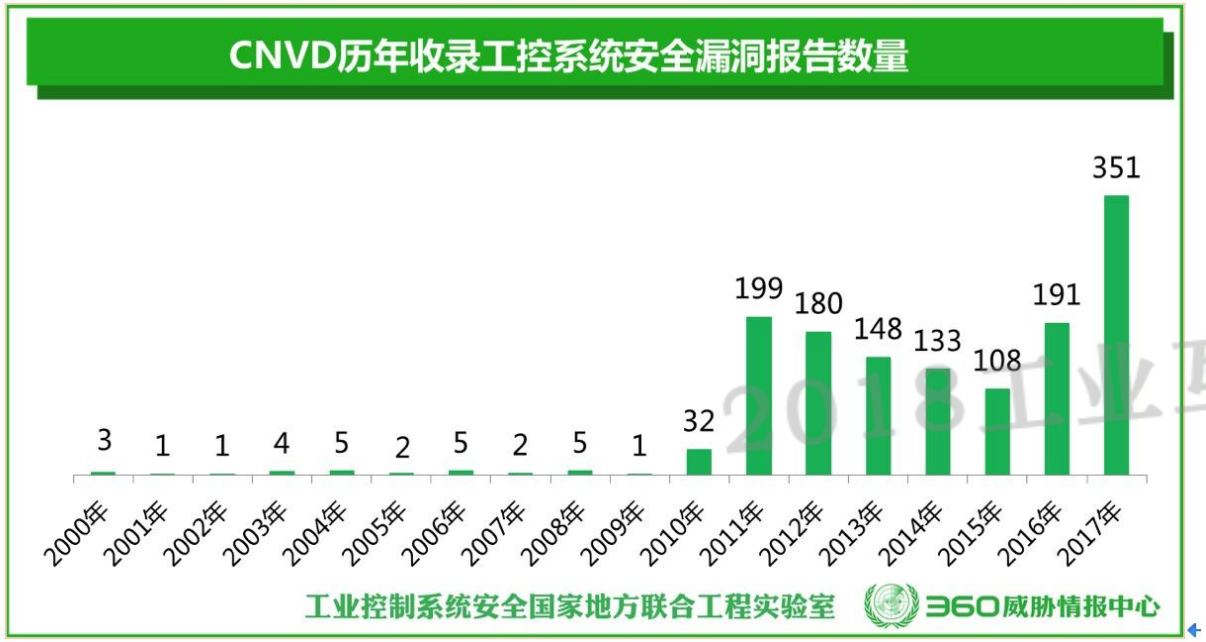
三、大安全时代工业互联网安全“四个假设”

360企业安全 安全第一 就用360

假设一	• 一定有未被发现的漏洞
假设二	• 一定有已发现但仍未修补的漏洞
假设三	• 系统已经被渗透
假设四	• 内部人员不可靠

2018工业互联网峰会

假设1：系统一定有未被发现的漏洞



摘自：360《IT/OT一体化的工业信息安全态势报告（2017）》

2017年，360向微软、谷歌等五大厂商提交漏洞519个，全球**致谢次数最多**

360研究：程序员每写**1000行**代码，会出现**一个**漏洞

现　状：ICS系统由程序员写的，安全知识**更**薄弱！

缺陷是天生的，漏洞是不可避免的，被攻击是必然的

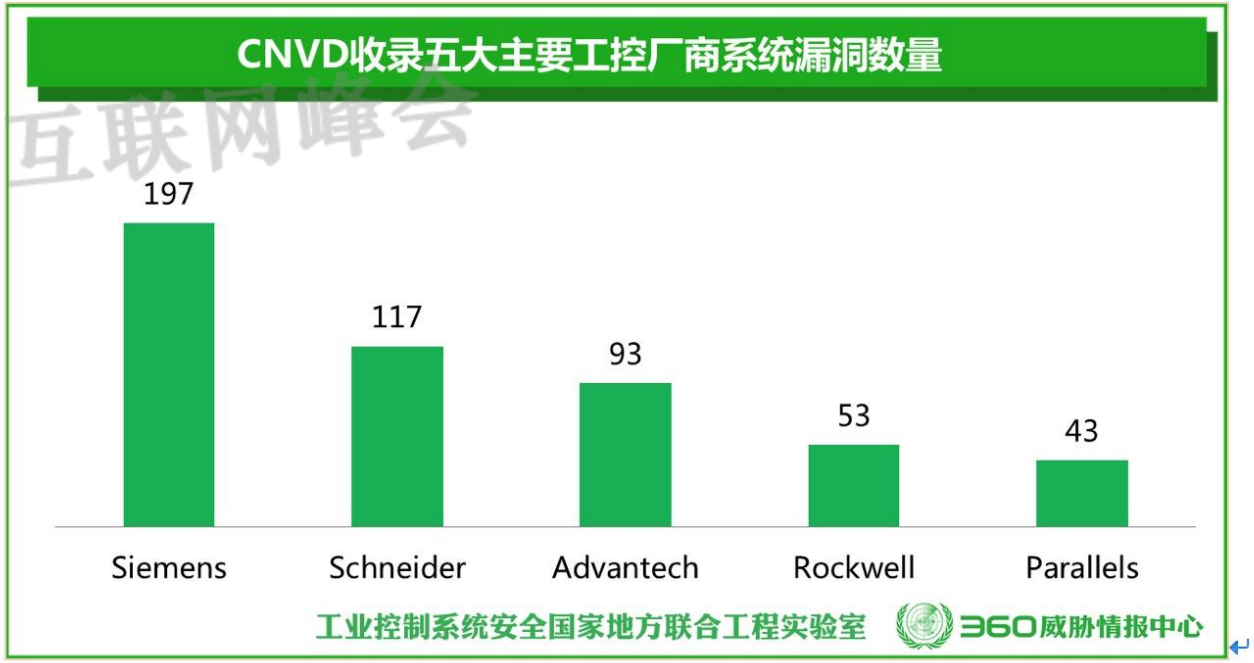
2018工业互联网峰会

假设2：一定有已发现但仍未修补的漏洞

360企业安全 安全第一 就用360

每次提交的漏洞，不一定会立刻得到修补

- 微软知道但还没修补的漏洞还有很多，具体有多少没人知道
- 企业IT网络：管理好的企业，每个月会自动打补丁，修补漏洞
- 企业OT网络：**没有**补丁、**不会**打补丁，**不能**打补丁

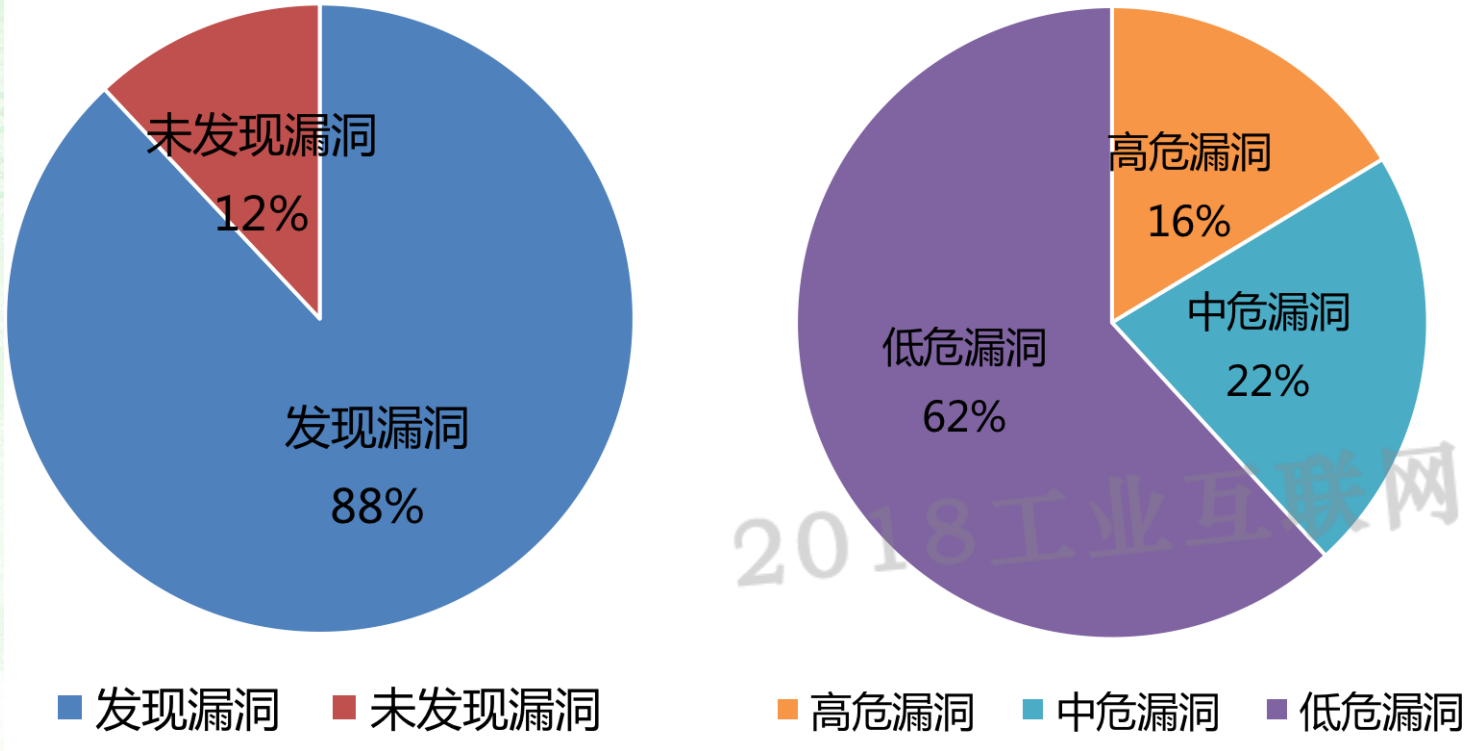


摘自：360《IT/OT一体化的工业信息安全态势报告（2017）》

2018工业互联网峰会

假设2：一定有已发现但仍未修补的漏洞

360企业安全 安全第一 就用360



2018工业互联网峰会

排名靠前的漏洞类型如下：

- ✓ 敏感信息泄露漏洞（SVN目录、网站目录）
- ✓ SQL注入漏洞
- ✓ 跨站脚本攻击漏洞

- 联盟工业企业越多的地区，漏洞越多
- 安全工作不是某家企业做的不好，而是一个整体水平不高，普遍缺乏安全意识和安全防护能力。

假设3：系统已经被渗透

360企业安全 安全第一 就用360

隔离网一度被认为是安全的

→ 恶意威胁的复杂性和多样性显著变化

→ 攻击入侵的路径不再局限于互联网攻击

2018工业互联网峰会

2011年震网病毒事件

伊朗核设施是物理隔离、高防护的网络 → 攻击者用USB介质为跳板，成功绕过安全产品的检测 → 利用Windows和西门子系统漏洞，成功入侵离心机的控制系统

2017年工业相关事件

勒索软件爆发： 石油、医院、云平台、智能制造……；重点企业，**工业网络中大量病毒**

假设4：内部人员不可靠

360企业安全 安全第一 就用360

1. **无泄密动机：**把核心资料存在云盘或U盘，没有将资料及时销毁/被钓鱼邮件、恶意软件利用

2. **有泄密动机：**有意识有计划地破坏、盗取内部数据/主动利用内部管理漏洞或技术漏洞，进行踩点、试探、入侵、窃取等

2018工业互联网峰会

四、工业互联 数据驱动安全

- 外部数据
- 本地数据

- 数据挖掘
- 机器学习
- 专家经验
- 关联分析

- 高级威胁
- 内部威胁
- 业务风险

数据驱动安全，建立基于大数据的联动防御系统

2018工业互联网峰会

四、工业互联 数据驱动安全

1、大数据引擎，是工业互联网安全产品的大脑

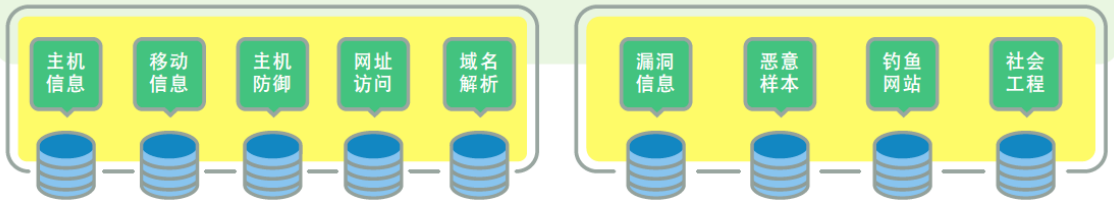
全球文件样本库	最全的样本行为库	最大的存活网址库	全球域名信息库
每天新增样本 900万	总日志数 18.9万亿条	每天查询 200亿条	90亿 DNS 解析记录
总样本数 145亿+	每天新增 380亿条	每天处理 100亿条	每天新增记录 100万条

数据来源 全球 6亿 PC 安全客户端，8亿 移动端安全客户端；360 浏览器、搜索终端等。

数据来源 互联网基础设施 DNS，猎网、补天等各类举报与相应平台，以及 100+ 第三方 数据源。

大数据服务器规模超过 60000台，总存储数据接近 1.3EB 每天新增超过 1.5PB。

每天各种数据计算任务 10万个，每天处理数据量 10PB。



- 威胁情报中心
- 安全服务与响应中心
- 工业安全运营中心
- 工业互联网监测防御
- 工业互联网平台防御
- 端点、网络保护

360工业互联网安全能力平台与产品

富士康

FOXCONN®

Invictus®
硬软整合智能存储

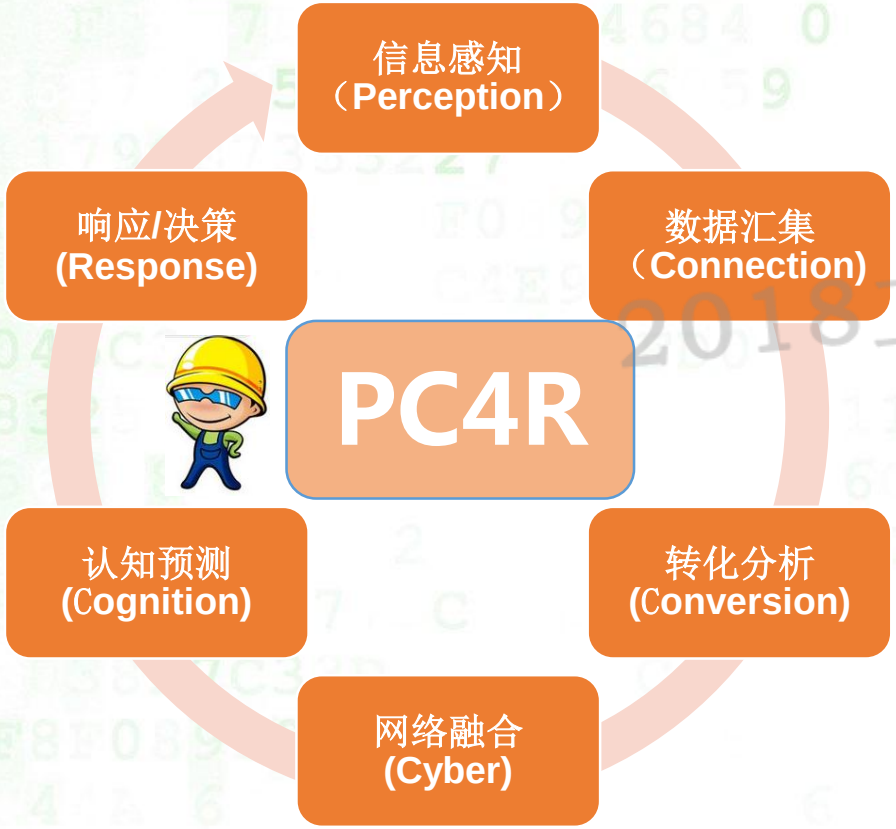
Utah®
工控设备中央控制系统

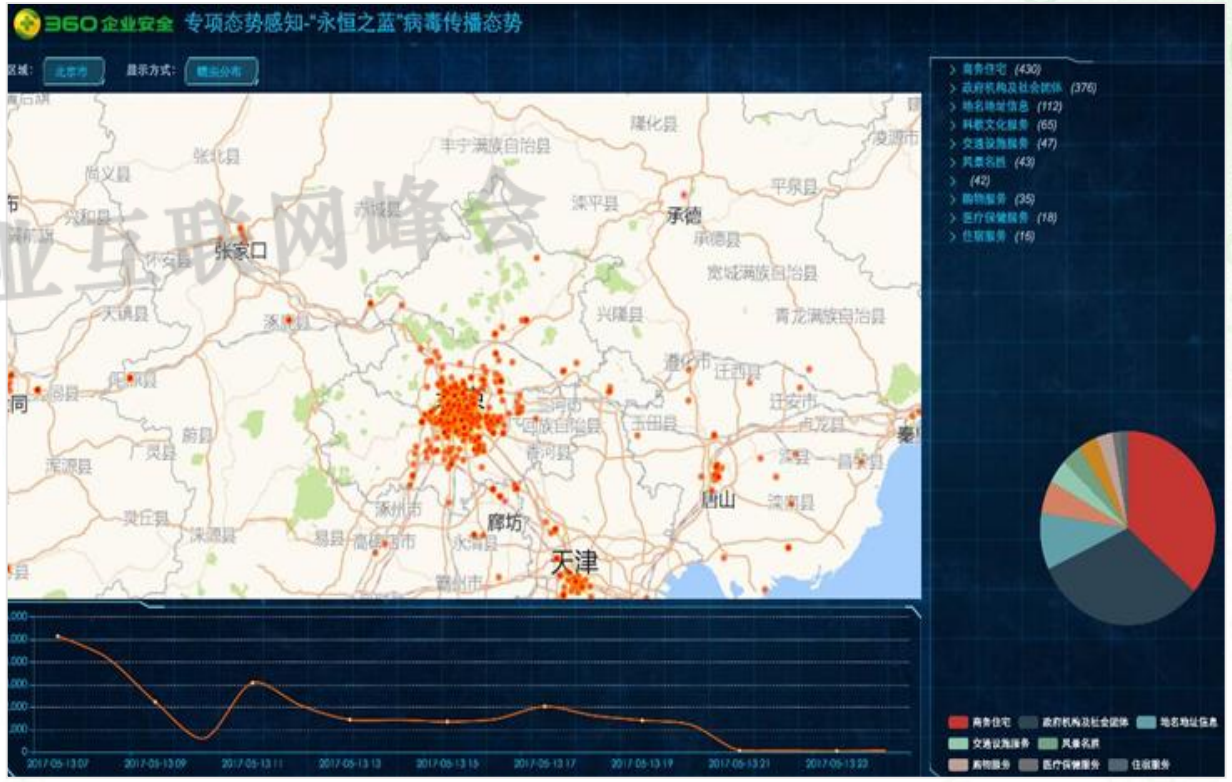
Comanche®
虚拟桌面管理

海尔海安盾平台

四、工业互联 数据驱动安全

2、IT-OT融合的网络行为大数据分析，“秒级”检测网络攻击





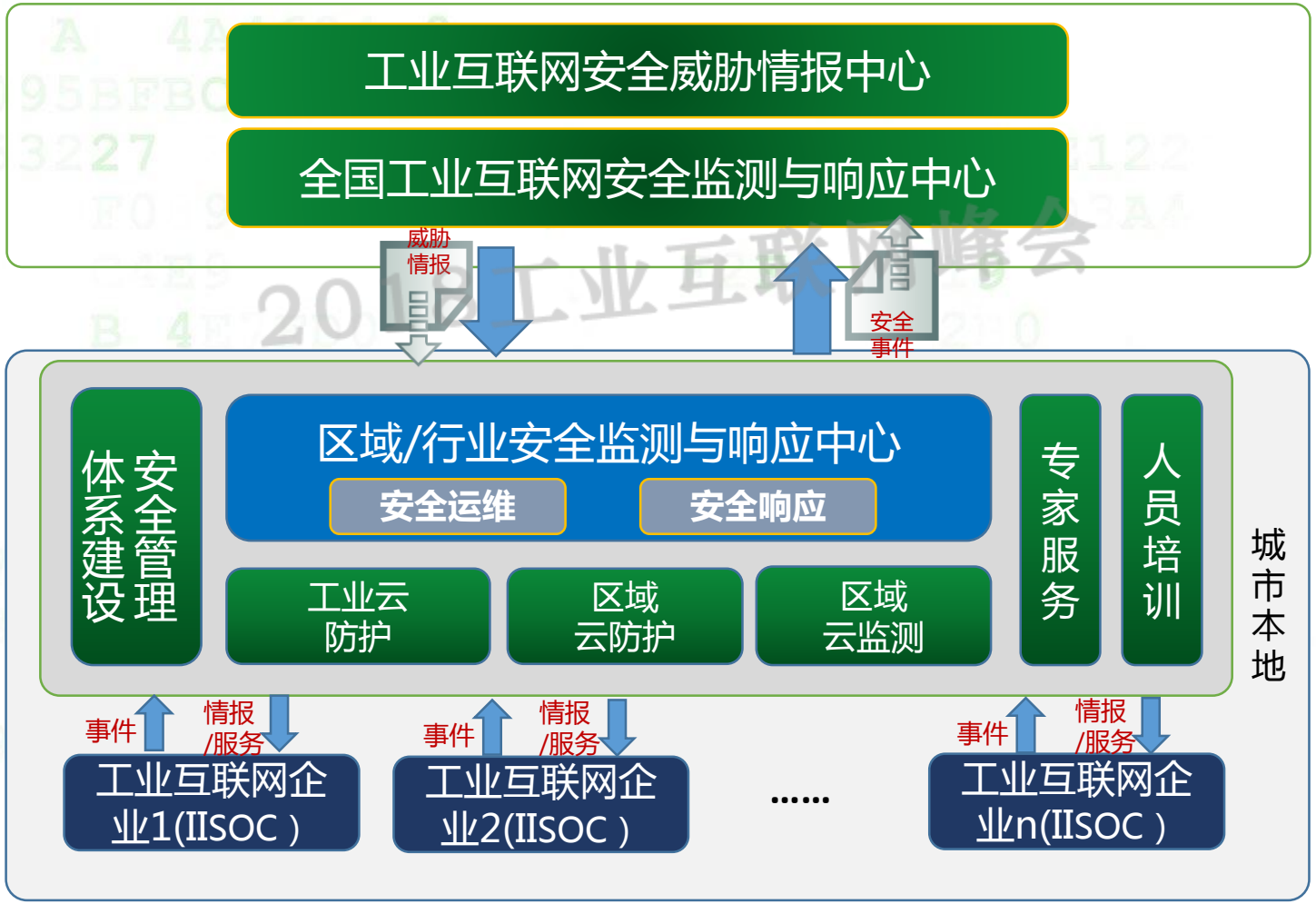
工业互联网自适应防护模型-PC4R

“以空间换时间”：掌握数据越多→检测信息越全→发现攻击速度越快

2018工业互联网峰会

四、工业互联 数据驱动安全

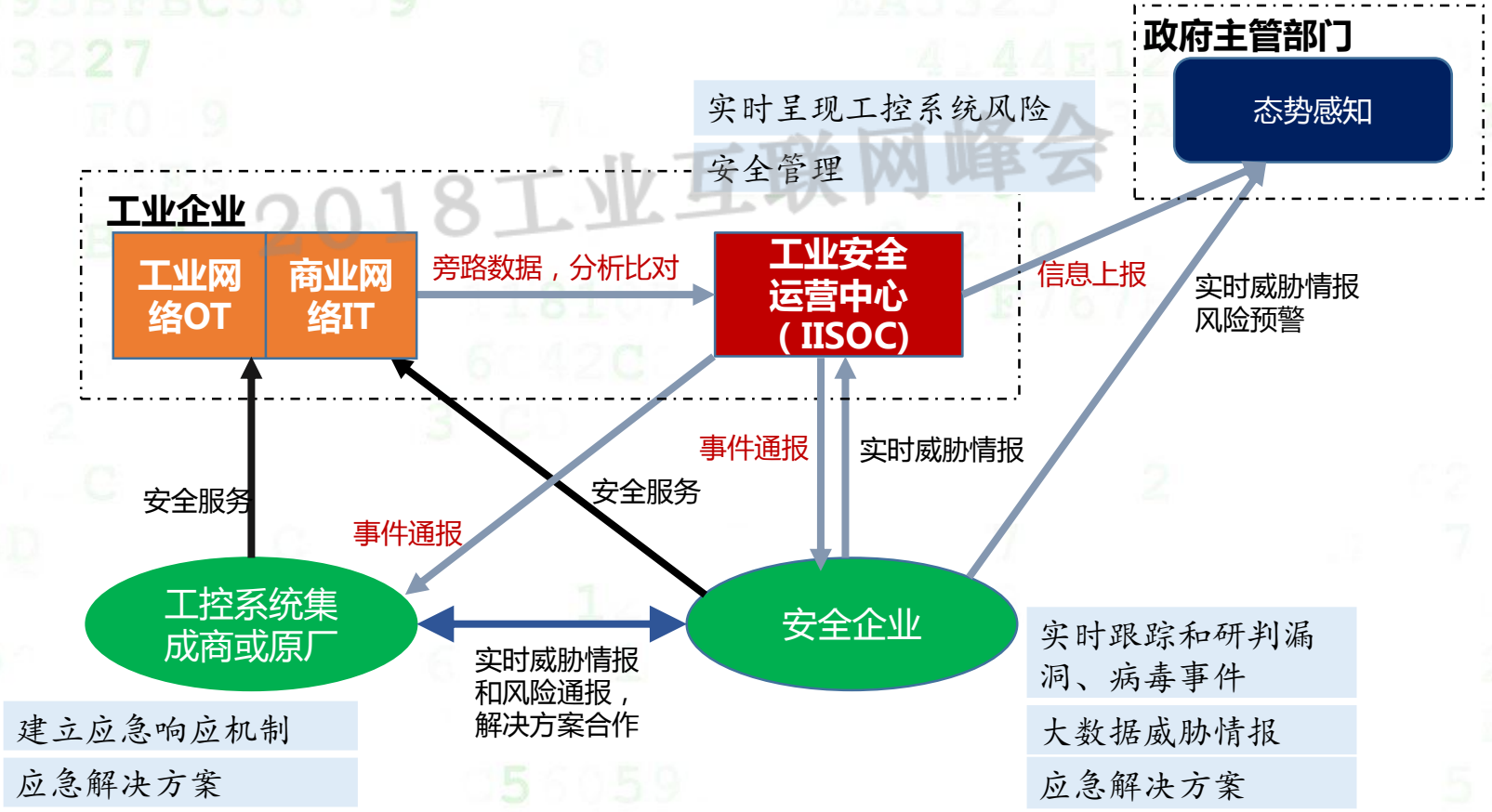
3、威胁情报大数据，全面提升产品的安全能力



四、工业互联 数据驱动安全

4、大数据的协同联动，让设备更聪明

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

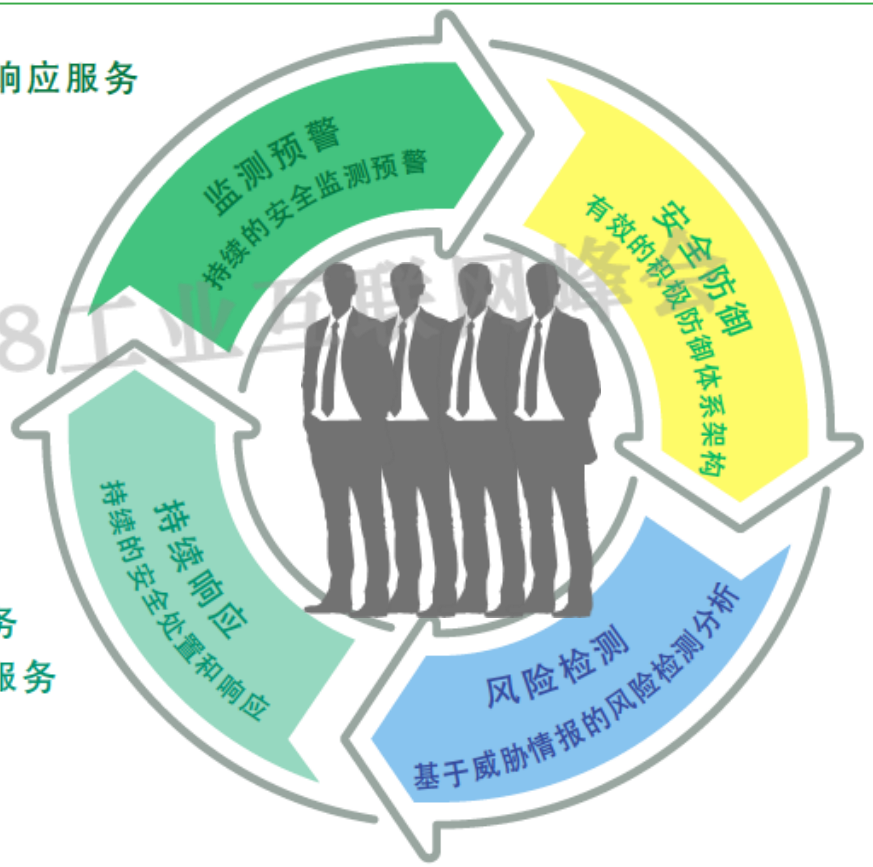


五、万物皆变 人是安全的核心

1、再聪明的机器，都无法替代人

360云端大数据安全能力平台

安全赋能
使人更“聪明”



- 基于威胁情报的预警响应服务
- 态势感知服务
- 互联网资产发现服务
- 网站安全监测服务

- 重要时期安全保障服务
- 安全加固服务
- 等级保护合规服务
- 云安全保障服务
- 工控安全服务

- 安全事件应急响应服务
- 可持续安全运营保障服务

- 对抗式演习服务
- 全流量威胁分析服务
- Web 失陷检测服务
- 风险评估服务
- 代码检测服务
- 渗透测试服务

判断决策的事情，仍然需的人来完成

五、万物皆变 人是安全的核心

2、再聪明的人，离开机器也会束手无策

防御APT攻击需“双零”突破：零漏报、零误报

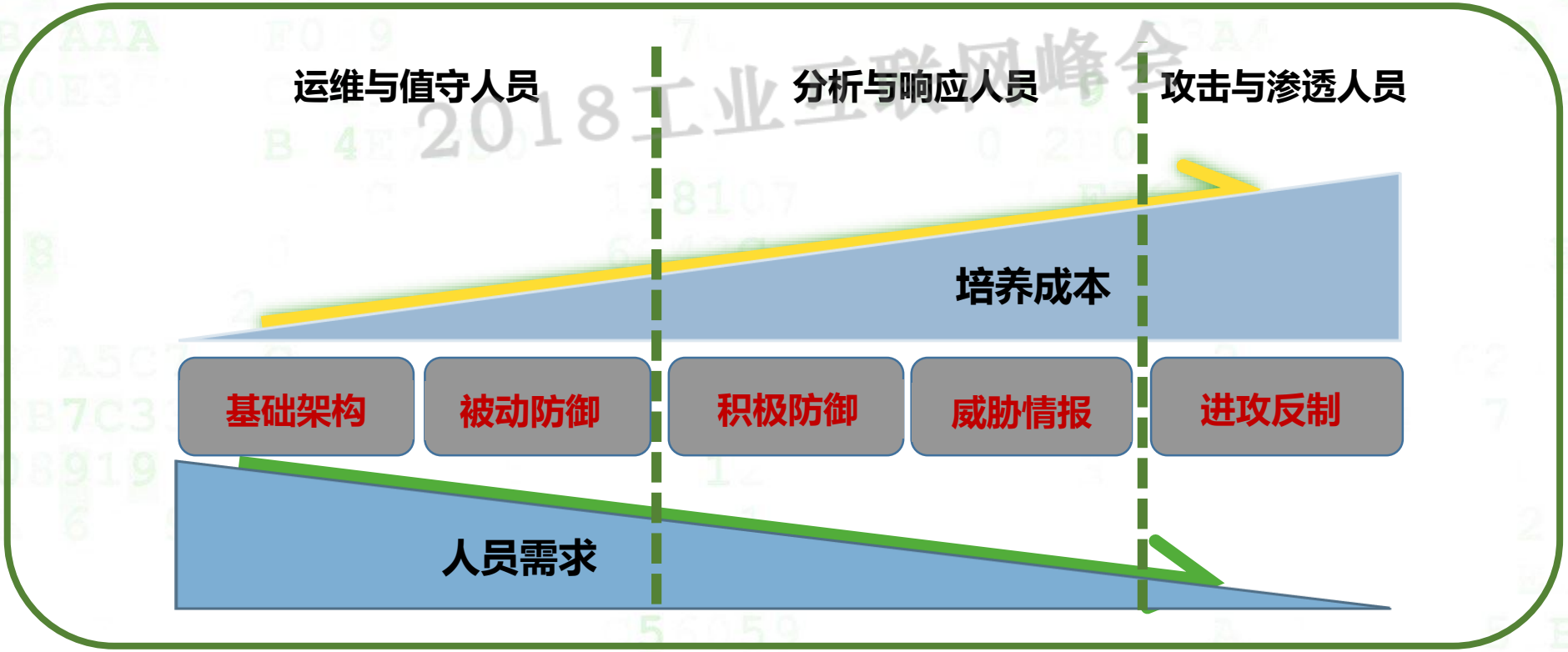
2018工业互联网峰会

- 网络攻击，99次失败，1次成功，等于成功
- 网络防御，99次成功，1次失败，等于失败

五、万物皆变 人是安全的核心

3、机器辅助运营，需要更多干“脏活、累活”的人

我国网络安全人才缺口达到70万，且以每年1.5万人的速度递增

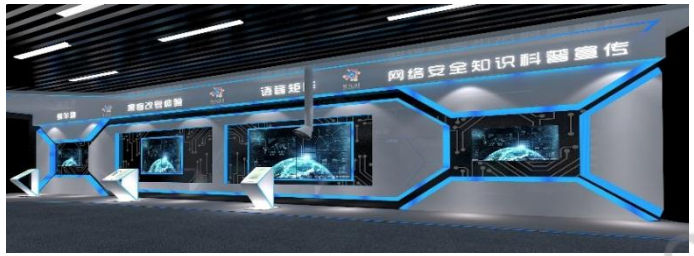


2018工业互联网峰会

五、万物皆变 人是安全的核心

4、培养多层次、多维度的网络安全人才，推动工业互联网发展

网络安全教育示范基地



社会公众

- 安全实训与竞技系统
- 安全运维人才培训班
- CISP/PTE 考核认证
- 安全训练营

从业人员

360网络空间安全学院

博士后科研工作站

- 国家级工程实验室
- 海量安全大数据
- 世界一流攻防技术研究
- 十一支安全研究团队

校企合作

2018工业互联网峰会

六、总结

数据驱动的工业互联网自适应安全体系

工业互联网产业联盟
Alliance of Industrial Internet

THANKS

2018 工业互联网峰会

360 企业安全

安全第一 就用360

陶耀东

AII 安全组执行主席

工业控制系统安全国家联合实验室 主任

《IT/OT一体化的工业信息安全态势报告（2017）》