工业互联网安全与实践

李鸿培

2017.5.11

议题

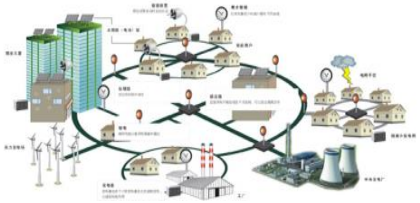
360 互联网安全中心

- 安全威胁
- 安全理念
- 安全实践

万物互联时代——网络连接无处不在

360 互联网安全中心

智慧城市



智能电网

智能家居

万物互联

车联网

智能工厂&制造

联网的可穿戴设备

工业互联网——信息化与工业化融合的基础

360 互联网安全中心

工业互联网

是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是提升工业系统智能化能力的关键信息基础设施。

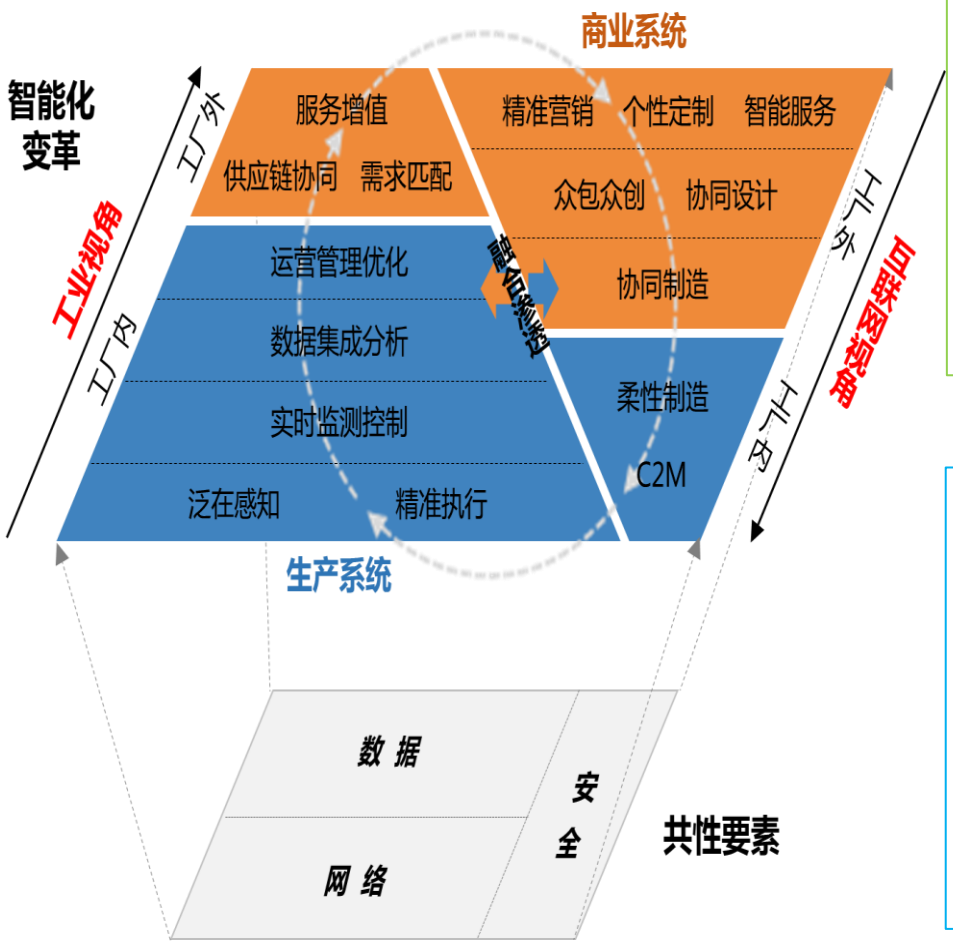
工业互联网

工业 4.0

互联网+

Internet + IoT + Cloud + BigData => Cyber-Physical-System（CPS）

工业互联网的两个视角、三大要素



- **工业视角**

  企业内生产系统的信息化进步，促进外部商业活动的优化

- **互联网视角**

  外部互联网商业模式的变革，倒逼企业内生产组织及制造模式的智能化升级

- **网络是基础**

  工业系统的互联、互通及互交换

- **数据是核心**

  企业运营、生产管理及商业活动优化，工业智能化的核心驱动

- **安全是保障**

  保障网络、数据在工业中应用的安全

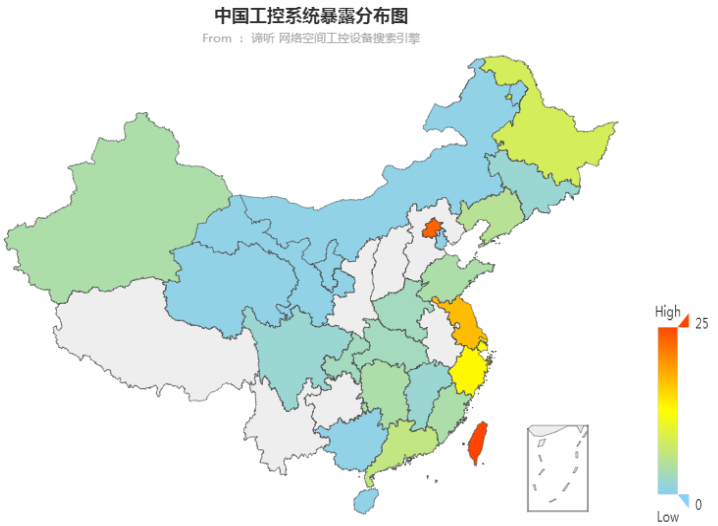
互联导致工业设备暴露在互联网上，引入新威胁

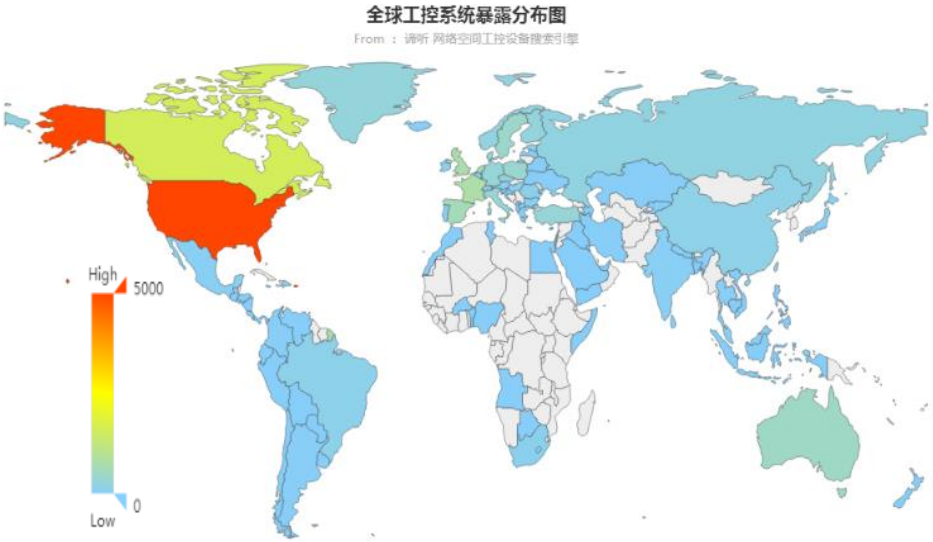
360 互联网安全中心

连入互联网的工业设备 越来越多……

工业设备自身的脆弱性问题

来自网络的信息安全威胁日益严重

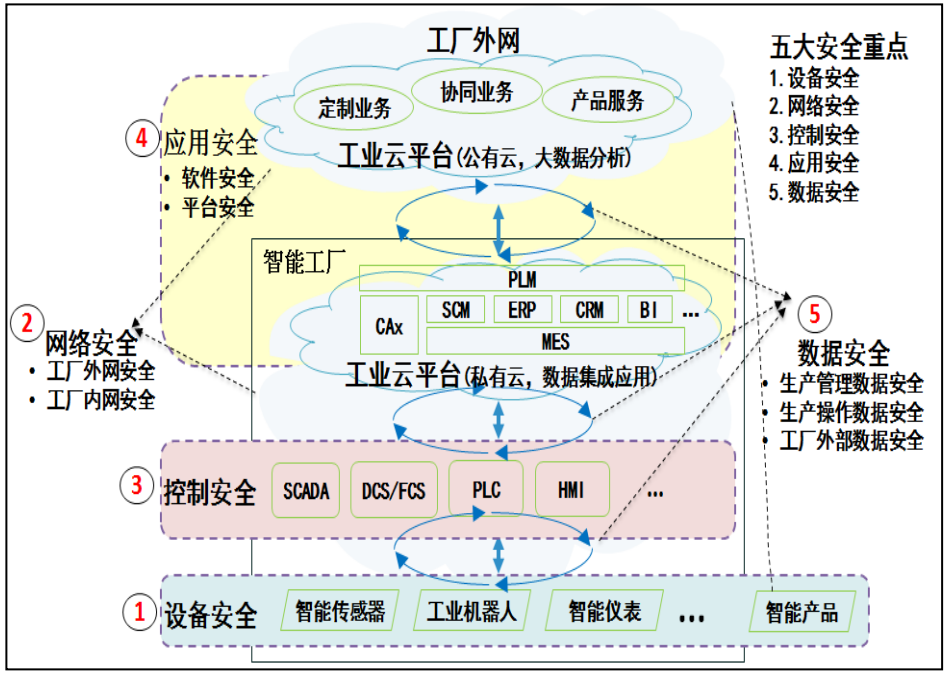




来源: AII 工业互联网安全态势报告,2016

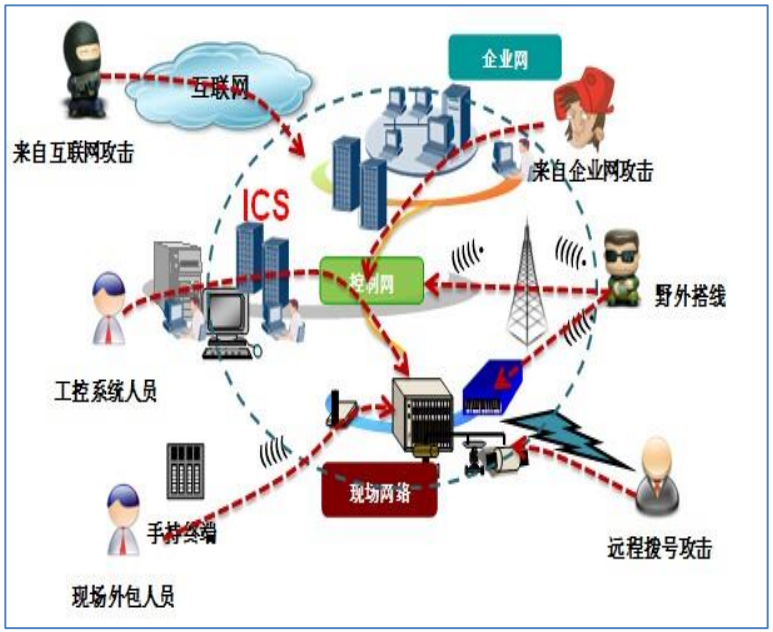
互联导致的潜在攻击威胁

360 互联网安全中心



工业互联网所面临的安全问题(AII)

智能工厂所面临的潜在攻击/威胁



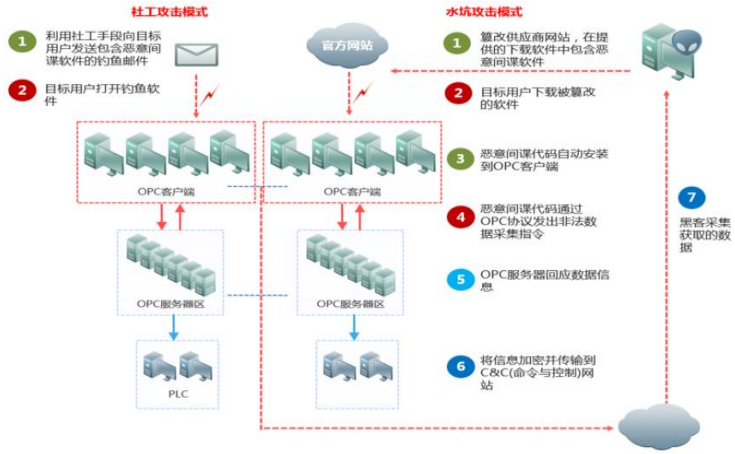
智能工厂内及工厂间的IT与OT系统的互联，将使智能工厂的生产控制系统面临更多的安全威胁

互联导致黑客组织的针对性攻击威胁(APT)

360 互联网安全中心

IT & OT的打通， 工业相关安全事件日益频繁：Stuxnet、duqu、Havex、blackengergy……

2010 ,震网，伊朗核电站 ,8000台离心机损坏



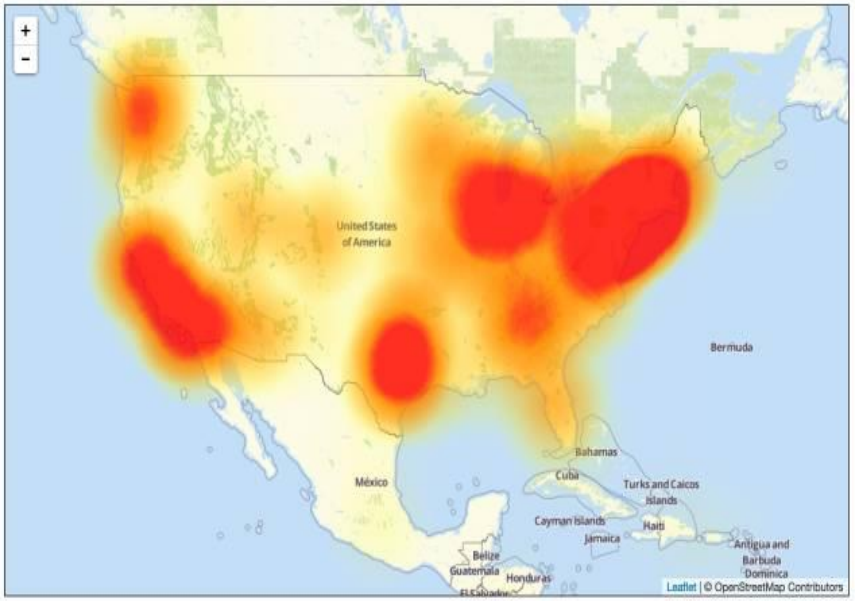
Havex——2014年利用供应商软件网站的“水坑攻击”
影响欧美1000多家能源企业（供应链安全）

2012.5,火焰Flame 攻击中东大量电脑

2015.12,乌克兰，10万户大停电

互联导致黑客利用物联设备的攻击威胁(OT→IT)

- 2016年10月21日,美国最主要的DNS服务商Dyn遭遇大规模 DDoS 攻击，
- 导致 Twitter、Spotify、Netflix、AirBnb、CNN、华尔街日报等数百家网站无法访问。媒体将此次攻击称作是“史上最严重 DDoS 攻击”，
- 值得注意的是，此次网络攻击中，黑客利用了大量的物联网设备。



标红的为无法访问的区域

360网络安全研究院分析报告: 《关于 dyn / twitter 受攻击情况的说明和 mirai 僵尸网络的回顾》

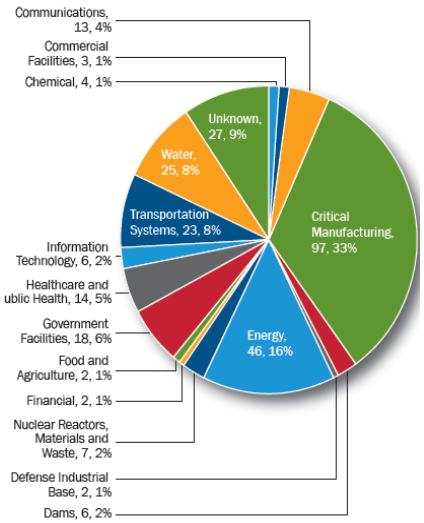
分析表明：以maria为代表的基于IoT的僵尸网络参与了该次攻击： syn flood 和 dns flood

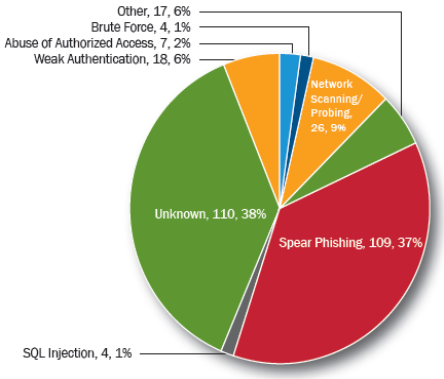
maria的控制对象分析后认为是光猫、网络摄像头和网关路由器

互联的威胁:2015工业安全事件+APT攻击

360 互联网安全中心

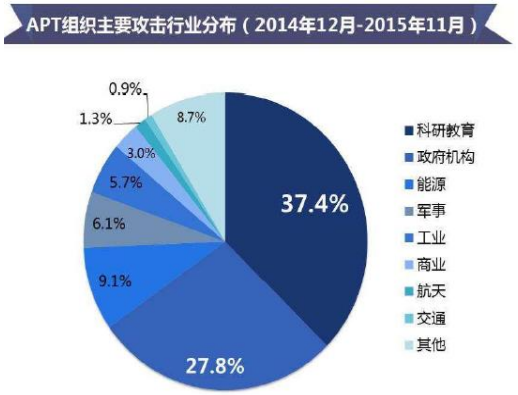
ICS-CERT 2015: Incident Response Statistics，
Incidents：**295 total**





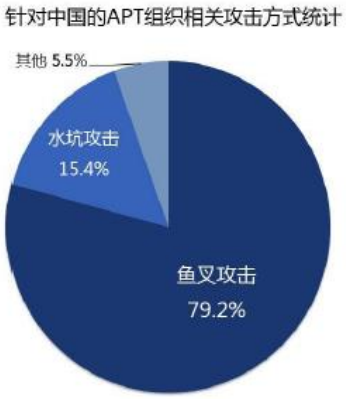
- **关键制造（33%）**与能源（16%）行业的安全事件约占一半
- **鱼叉式攻击**是主要的攻击方式(特定目标攻击)

备注：部分事件（38%）因证据不足，无法判断其攻击方式



据**奇虎360的2015年APT研究报告**，可知：

- **能源、工业系统也是APT组织的重要攻击目标**
- **鱼叉攻击与水坑攻击**是主要攻击方式
- 目的：**长期窃取敏感数据**



2016年工业互联网的10大安全事件(AII)

360 互联网安全中心

2月	海康威视部分设备被境外IP 控制, 存严重安全隐患
3月	美国Kemuri 水务公司安全事件
3月	黑客组织“洋葱狗”潜伏 3 年终曝光(针对能源\交通行业)
4月	德国核电站检测出恶意程序并被迫关闭
6月	“食尸鬼行动”事件(针对工业领域企业,范围遍及全球的黑客攻击事件)
8月	伊朗多个重要石化工厂发现恶意软件攻击
10月	北美地区Dyn 公司遭遇最大DDoS 攻击事件(利用物联网设备的攻击)
11月	《中华人民共和国网络安全法》出台
11月	旧金山Muni 地铁站被黑，售票系统停运
12月	乌克兰电力系统的自动控制系统遭受黑客攻击

来源: AII, 中国工业互联网安全态势报告,2016

议题

360 互联网安全中心

- 安全威胁
- 安全理念
- 安全实践

互联导致工业系统安全理念的转变

360 互联网安全中心

工业系统安全的”互联网+”

- *物理空间*
- *可信的人*
- *可控环境*
- *规范操作*
- *……*

- *网络空间+物理空间*
- *存在不可信的人/主体*
- *存在不可控环境*
- *存在非授权违规操作*
- *……*

重点解决：工控系统的**业务连续性 + 误操作**

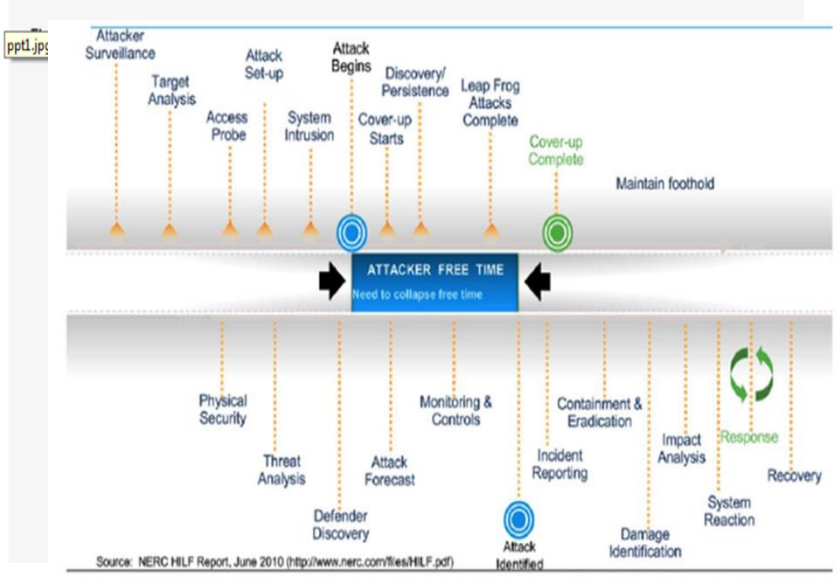
重点解决：**系统的脆弱性、系统的非授权访问**及**恶意破坏行为**

互联导致工业系统安全理念的转变:攻防安全

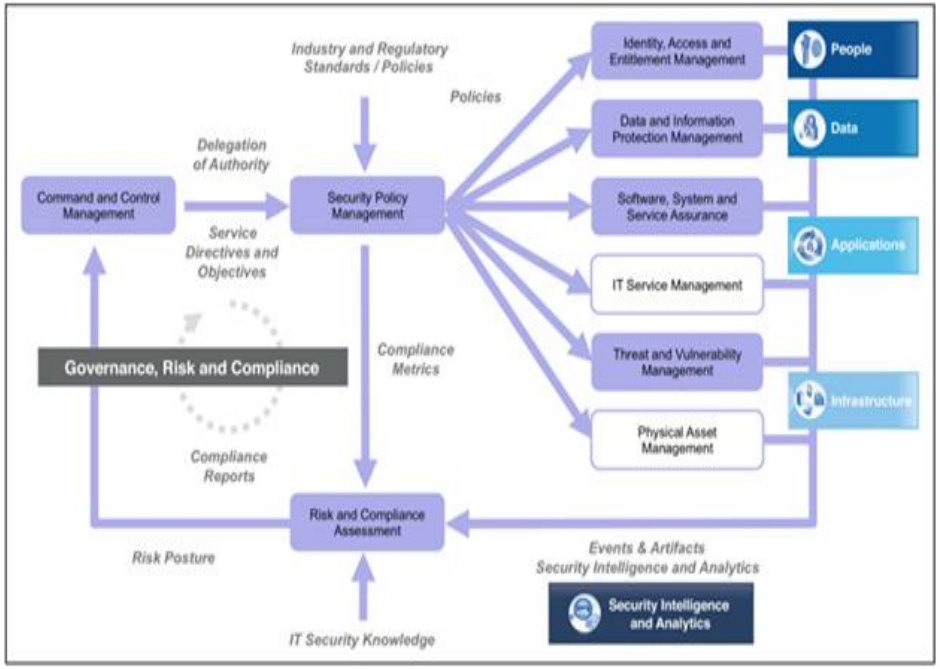
360 互联网安全中心

从攻防对抗的角度，系统总会被攻破　>>>仅部署传统的安全防护机制是不够的

- 针对系统缺陷的攻防，**攻方占尽先机**
- 防御成功的关键将在于：
  - **如何及时洞察系统中的安全缺陷，并尽早主动弥补？**
  - **如何尽早发现攻击行为并及时处置？**
    缩小系统被自由攻击的时间窗口



- 面对当今主流的定向攻击，任何单一化的检测、防护措施均不能达到理想效果
  - 通过**多安全机制的协同检测**，构建**体系化的安全防护**成为必然
  - 基于威胁情报的安全协同（安全控制闭环运营）



互联导致工业系统安全理念的转变

360 互联网安全中心

纵深防御 提高攻击成本

- 多点防御、联合防御
- 传统安全手段 + 新型防御手段
- 产业界合作联合防御

主动挖掘漏洞 与自我保护

- 投入资源主动挖掘系统漏洞
- 与白帽子及漏洞举报平台合作
- 漏洞利用的检测与保护

数据安全

- 数据是新的保护核心
- 保护生产、管理与控制相关的各种敏感数据

假设被攻破

- 做最坏打算，被攻击者成功突破后，如何发现已被突破，如何将攻击者清除出去

工业互联网的安全保障体系

360 互联网安全中心

安全管理体系

人员管理规范行为

安全标准合规遵从

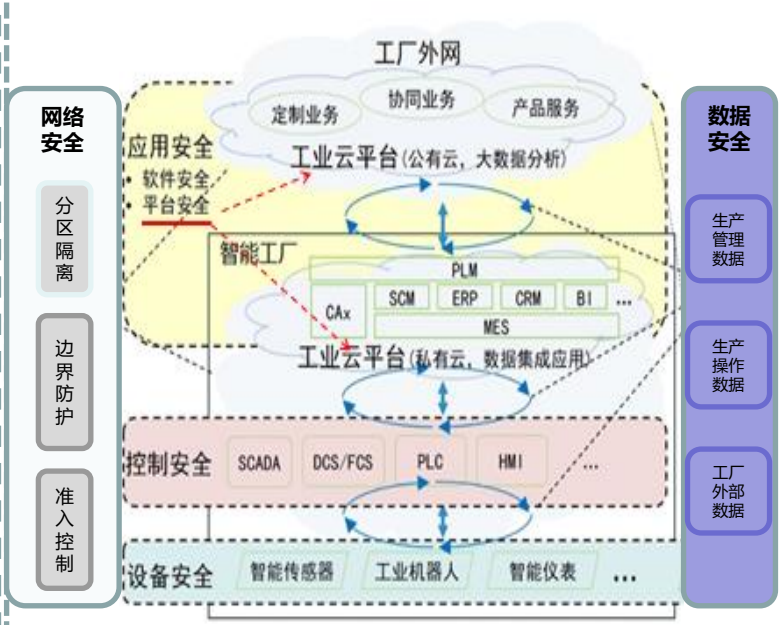
安全设备管理控制

安全策略管理执行

安全风险有效管控

监测预警体系

安全监测 | 安全预警 | 安全态势 | 威胁情报



纵深安全防护体系（来源：AII）

工业互联网安全体系功能框架

安全服务体系

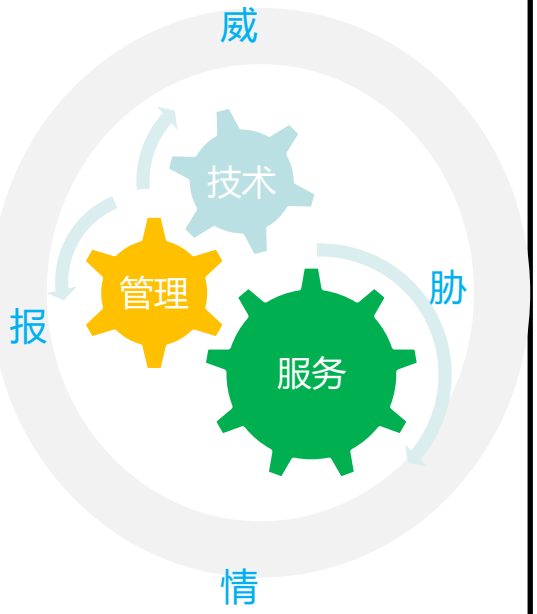
系统上线风险评估

测评认证

应急响应

威胁情报共享服务

教育培训



数据驱动、安全协同

数据驱动的动态安全模型

工业互联网安全保障体系

KasperSky：工业网络空间安全保障体系

360 互联网安全中心

KASPERSKY INDUSTRIAL CYBER SECURITY

Services

- Knowledge
  - Cyber Security Trainings
  - Intelligence reporting
  - Industrial Simulations
- Expert services
  - Security Assessment
  - Solution Implementation
  - Solution Maintenance
  - Incident Response

Centralized management

- Software provisioning
- Reporting
- Single Management Console
- Policy Management

Integrity Control

- Application startup Control
- Device Control
- Network Integrity Control
- PLC Integrity Check
- Process Integrity Control

Intrusion Prevention/Detection

- Network Attack Blocker
- Firewall
- Automatic Exploit Prevention
- IDS

Vulnerability Assessment

- Vulnerability Scan

Anti-Malware

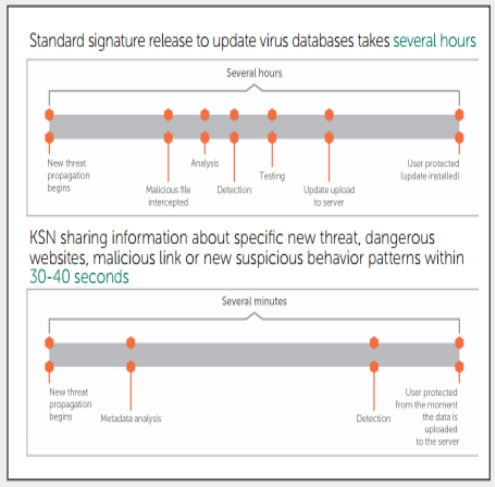
- Signature based detection
- Proactive based detection
- KPSN
- Malware actions rollback

Forensic

- Safe Event logging
- Data analysis

Interoperability

- SIEM
- HMI
- Syslog
- Network Management System
- Mail



Reducing threat reaction times with KSN: Real time, Proactive, Global view.

基于威胁情报的快速响应

安全技术

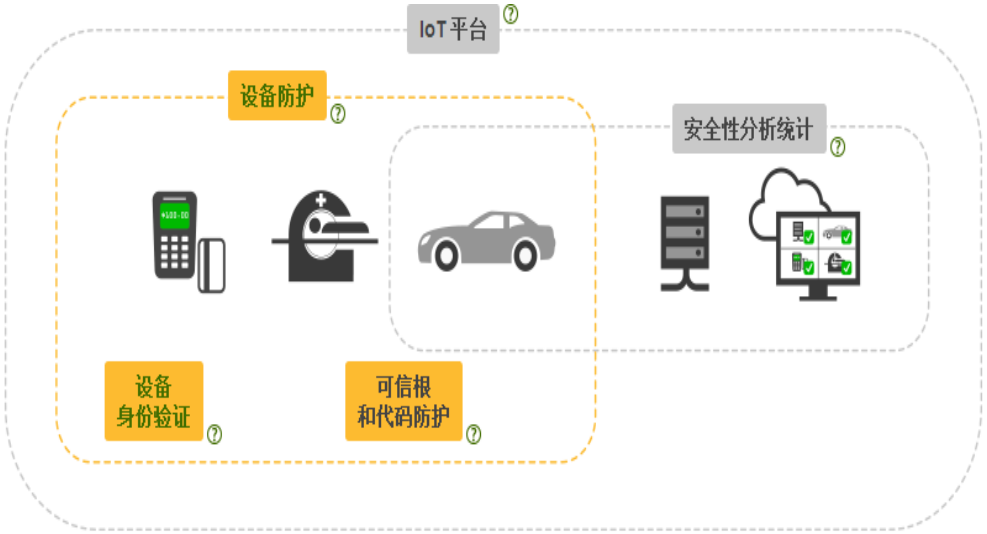
+

安全服务

+

威胁情报

Symantec：IoT的安全防护



IoT安全

强调设备防护、加密、身份验证、密钥管理以及代码签名功能

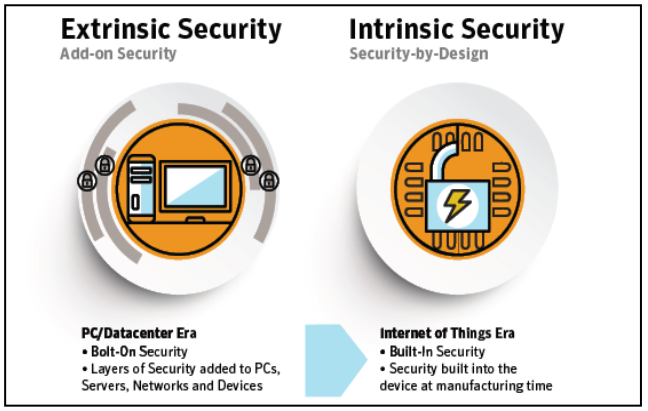
① **设备安全防护**，锁定 IoT 设备，防止攻击者损害设备

② 用设备身份证书对 IoT **设备身份验证**，对通过 IoT 系统和网络进行传输的**数据加密**

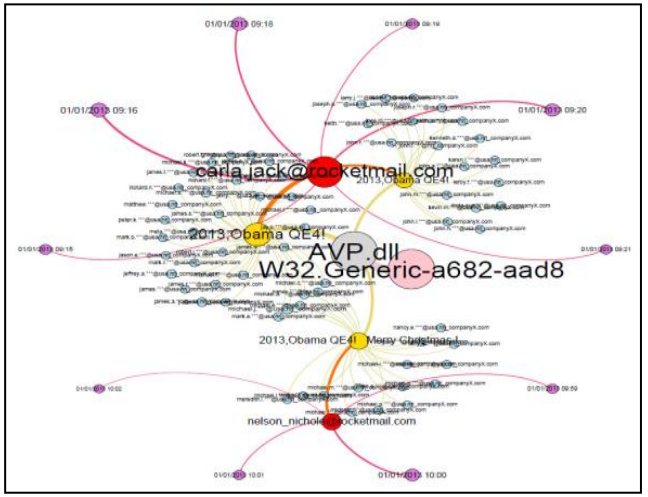
③ **可信根和代码防护**，检验 IoT 设备上运行的所有代码都已相应授权给对应设备，并由强可信根提供**代码完整性保护**

④ **安全性分析统计**，主动检测IoT网络上存在的异常攻击行为

⑤ **IoT 平台**，远程更新和配置设备及数据分享



强调IOT设备制造时内置安全



威胁可视化分析

基于Symantec全球智能网络监控数据、智能分析处理安全事件

议题

360 互联网安全中心

- 安全威胁
- 安全理念
- 安全实践

安全实践：威胁看的见，APT检测

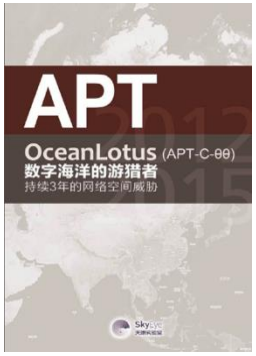
360 SkyEye

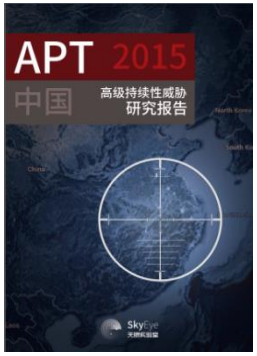
360 互联网安全中心

天眼ATP攻击检测防御系统

- 国内率先**运用大数据技术发现未知威胁**的厂商
- 360威胁情报中心已监测到各类APT攻击事件数万次
- 针对中国境内发动APT的境外组织29个，其中14个为360首先发现

APT活动	境内感染量	首次发现时间	最近发现时间	影响省份数	影响行业	感染方式
APT-C-00	1047	2014/2/18	2015/5/22	30	政府、海洋、海事	鱼叉邮件、水坑
APT-C-01	235	2014/2/15	2015/4/5	28	政府	鱼叉邮件
APT-C-04	17	2014/4/3	2014/6/29	3	科研、教育	鱼叉邮件
APT-C-02	180	2014/8/1	2015/4/14	9	教育	鱼叉邮件
APT-C-03	5	2014/11/3	2014/12/15	2	非政府组织	鱼叉邮件
APT-C-05	12	2015/2/12	2015/3/24	3	政府	鱼叉邮件
APT-C-06	4	2015/2/24	2015/3/7	3	科研	鱼叉邮件
APT活动	境内感染量	首次发现时间	最近发现时间	影响省份数	影响行业	感染方式
Desert_Falcon	3	2014/4/30	2015/3/3	3	教育	鱼叉邮件、水坑
GDATA_TooHash	4	2014/6/1	2014/8/31	3	科研	鱼叉邮件
Darkhotel	334	2014/6/1	2015/3/19	29	教育、能源、电信	鱼叉邮件、网络层劫持
DarkSeoul	4	2014/6/5	2015/1/5	3	电信	鱼叉邮件
Epic Turla	14	2014/6/12	2015/3/21	6	科研、教育	鱼叉邮件
NGO_Attack	6	2014/6/18	2015/3/13	6	非政府组织	鱼叉邮件
Dragonfly	2	2014/7/15	2014/8/19	1	能源	鱼叉邮件、水坑
APT28	1	2014/8/7	2014/8/7	1	航空	鱼叉邮件
Anunak	383	2014/9/28	2015/3/26	26	金融、电信、政府、科研	鱼叉邮件
CARETO	1	2014/10/28	2014/10/28	1	政府	鱼叉邮件
XSLCmd_OSX	1	2014/10/30	2014/10/30	1	金融	鱼叉邮件
Waterbug	1	2014/12/31	2014/12/31	1	政府	鱼叉邮件、水坑
Snake	1	2015/2/15	2015/2/15	1	金融	U盘
Equation	1	2015/4/16	2015/4/16	1	军工	U盘





安全实践：系统脆弱，360补天

360 互联网安全中心

漏洞管理，防微杜渐

尽可能早地发现、修补工业系统及相关IT系统的漏洞，避免或降低企业因系统被攻击而造成的损失

补天漏洞响应平台

补天 漏洞响应平台

- 国内权威第三方漏洞收集、奖励平台
- 期望建立国内企业与网络安全专家的交流桥梁，最大程度地避免企业因系统漏洞而造成的损失，帮助企业提升企业网络信息安全防护能力
- 建立一个对各方都有益的企业安全生态系统

拥有国际顶级的系统漏洞研究能力

- 拥有中国一半以上的顶级安全专家，号称东半球最强的白帽子军团
- 拥有漏洞分析、网络攻防、网络安全研究等多个实验室
- 拥有协议与逆向分析、IOS安全、无线安全等8个安全团队

安全实践：智能硬件，物联安全

360 互联网安全中心

360UnicornTeam
无线、硬件安全

360 ADLAB

- 智能产品的安全研究
- 车联网的安全研究

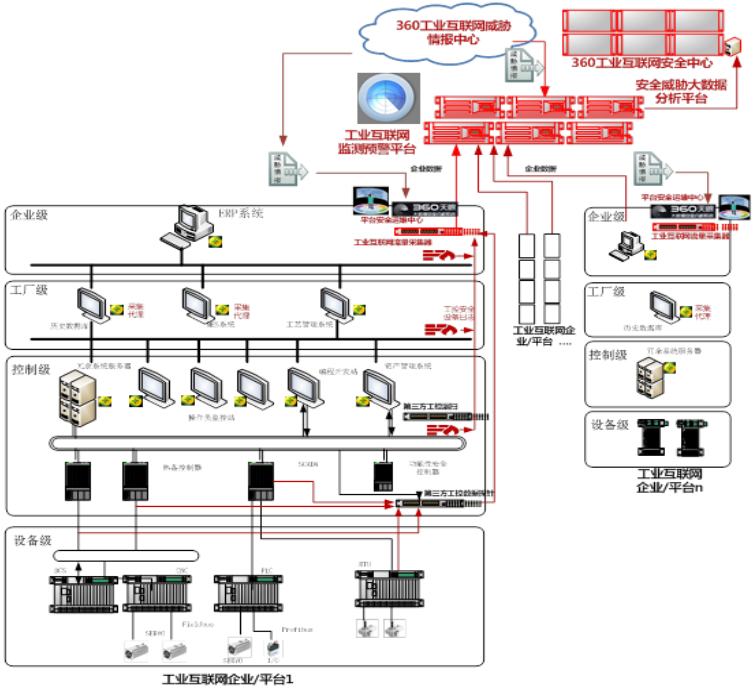
安全实践：工业互联网安全研究

360 互联网安全中心

1. 工业互联网安全实验室

2. 国家研究课题

- 2016年工业转型升级-数据驱动的工业互联网安全保障体系建设与应用示范
- 构建数据驱动+安全协同的工业互联网安全威胁监测预警平台



3. 研究报告

4. 国际会议+合作交流

谢 谢!

360互联网安全中心 | 安全第一 就用360

www.360.cn