



中小企业如何做好工业互联网安全防护

陶耀东 研究员
奇安信集团 副总工程师
工业控制系统安全国家联合实验室

目录

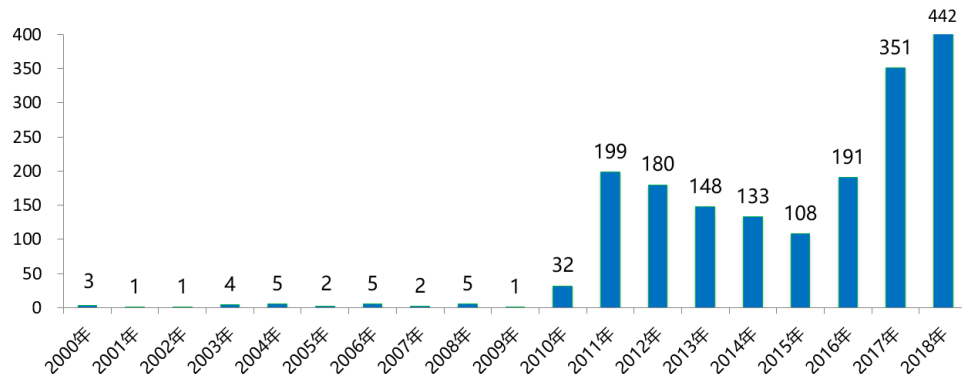
工业互联网安全现状与趋势

中小企业面临的工业互联网安全挑战

怎样的防护方案对中小企业更适用吗？

中小企业工业互联网安全防护建议

CNVD历年收录工控系统漏洞数量分布

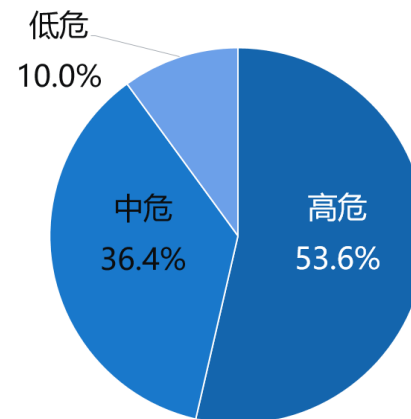


工业控制系统安全国家地方联合工程实验室

- 基于CVE、NVD、CNVD、CNNVD漏洞平台收录的工控漏洞为基础，2018全年，高危漏洞数量占比最高，**达到53.6%**

- 基于CNVD漏洞平台收录的漏洞为基础，2018年全年，新增工控漏洞达到442个，**创历史新高**
- 工业互联网安全风险突出，安全态势严峻

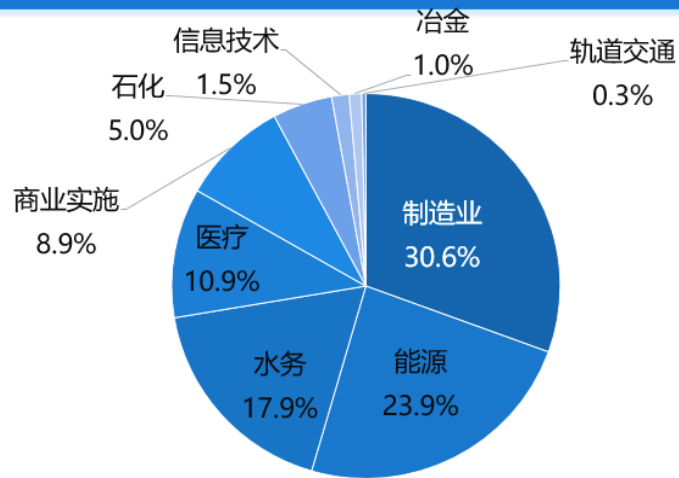
2018工控系统新增漏洞危险等级分布



工业控制系统安全国家地方联合工程实验室

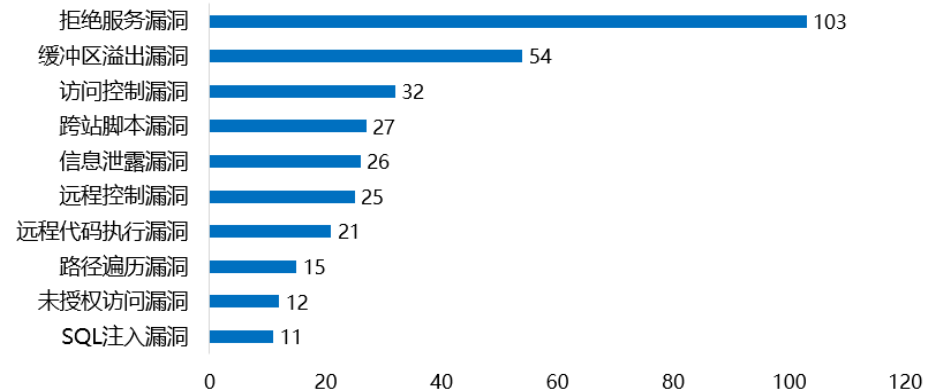
- 漏洞攻击类型多样化特征明显，**技术类型** **多达30种以上**
- 无论攻击者无论利用何种漏洞造成生产厂区的异常运行，均会造成严重的安全问题

工控新增漏洞行业分布



工业控制系统安全国家地方联合工程实验室

工控系统新增漏洞类型分布 (Top10)

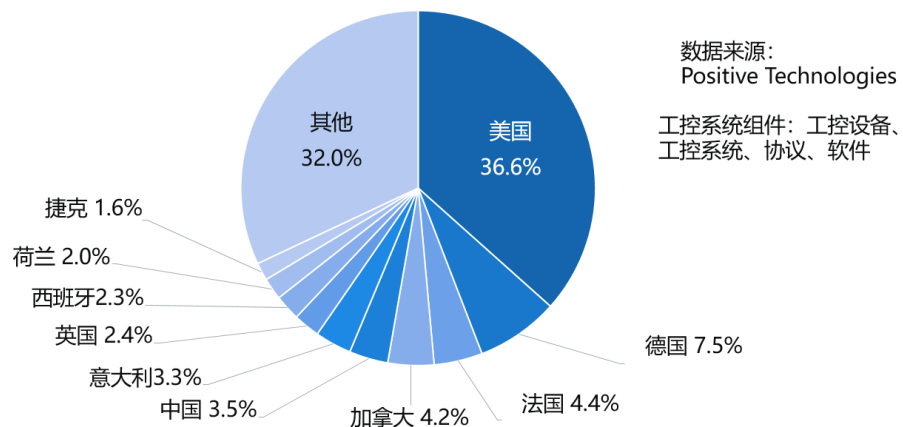


工业控制系统安全国家地方联合工程实验室

- 漏洞涉及行业广泛，以制造业、能源行业为主
- 制造业占比最高，**高达30.6%**，能源行业涉及的相关漏洞占比**高达23.9%**

工业系统互联网暴露数量增多，攻击面增大

世界各国工控系统组件联网暴露数量及比例分布

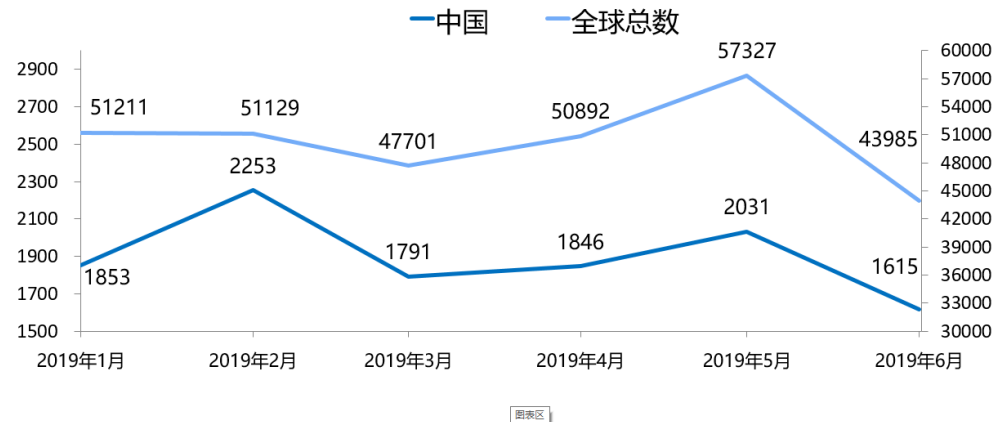


工业控制系统安全国家地方联合工程实验室

- 全球工控系统联网暴露组件**总数量约为17.6万个**，暴露数量增加明显
- 中国工控系统暴露数量为6223，占比**3.5%**，**排名全球第五**

- 以奇安信工业互联网安全大数据分析平台——哈勃平台统计，工控设备暴露数量**基本处于稳定状态**
- 工控设备: PLC、DCS、SCADA等设备

暴露在互联网上的工控设备数量变化情况



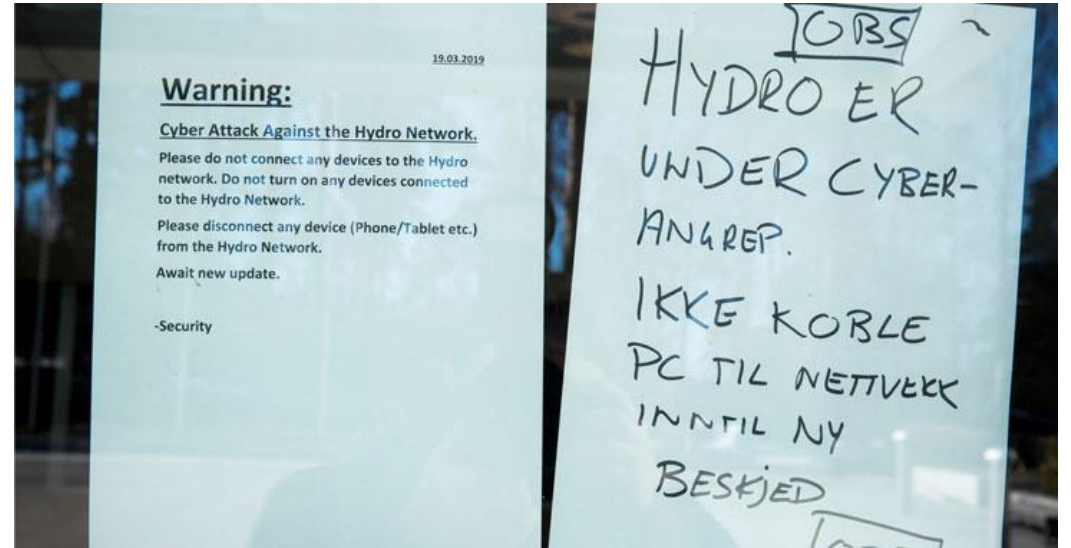
工控设备: PLC、DCS、SCADA等设备

工业控制系统安全国家地方联合工程实验室

大型企业停产，损失越来越大：海德鲁&驱动人生



- 8月3日周五，台积电新机台安装引入疑似永恒之蓝勒索病毒
- 数分钟内大规模攻击导致3个工厂停产，工业主机蓝屏重启
- 损失惨重，**3天损失近2亿美元**、毛利降1%
- 8月6日下午召开记者会：应对完毕。



- 3月19日 全球最大铝制造商 Norsk Hydro 欧美多工厂遭“大规模的网络攻击”，工厂运营模式改为“可以使用的”手动
- LockerGoga勒索软件是本次感染的源头，可加密扩展名的文件：doc, dot, wbk...
- 全球现货市场铝价上涨超1%下,股价下跌近3%

工业互联网安全事件层出不穷，整体形式严峻

2018年2月，台湾台达电子公司修复了公司两款**工业自动化产品**中的**多个漏洞**，包括可导致远程代码执行问题的缺陷。

2018年4月，研究人员在某些**西门子继电保护设备**中找到多个潜在的严重漏洞，它们可导致变电站和其它供电设施易遭黑客攻击。

2018年4月，工业安全公司 Applied Risk 在新加坡工控网络安全会议上披露影响多家主要供应商安全控制器的**DoS 漏洞**，可能对设备和人员造成物理伤害。

2018年6月，德国安全公司 ERNW 的研究人员发现，瑞士工业技术公司 ABB 的**门禁通信系统**中存在多个严重漏洞。

2018年7月，西门子通知消费者称，公司的某些 **SIPROTEC** 中继保护设备的 **EN100** 通信模块中存在多个漏洞，导致其易受 DoS 攻击。

2018年8月，两家公司研究人员在艾默生 **DeltaV DCS** 工作站中发现了多个严重和高危漏洞，攻击者在目标网络中横向移动并可能控制其它 DeltaV 工作站。

2018年4月，德国纳图**医疗设备**曝光**多个漏洞**，可导致设备遭远程攻击。该厂商已发布固件更新予以修复。

2018年4月，罗克韦尔自动化通知客户称其**工业路由器**易遭远程攻击，原因是所使用的思科 IOS 软件中存在多个漏洞。

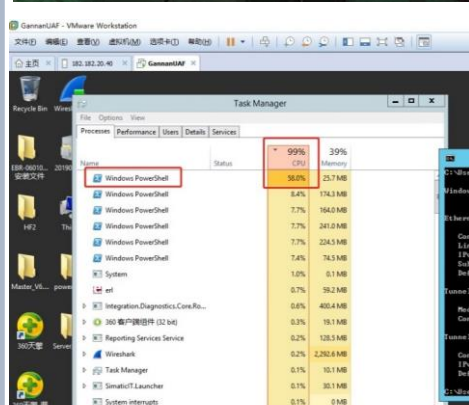
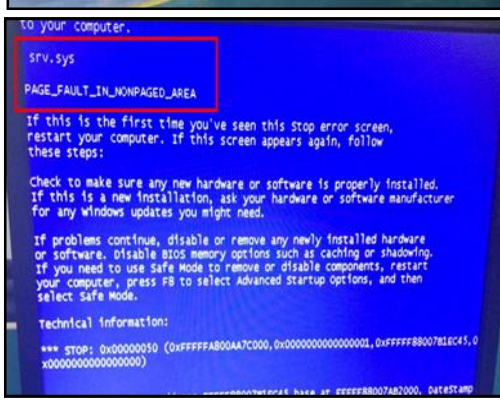
2018年5月，施耐德电气**开发工具**爆严重漏洞：可远程代码执行。

2018年6月，日本横河电机有限公司为 STARDOM 控制器发布固件更新，解决可**被远程用于控制设备**的一个严重漏洞。

2018年7月，西门子指出，**SICLOCK 中央工厂时钟系统**共受六个漏洞的影响，可致使设备宕机、命令执行以及重启。

国内工业企业频繁遭到“永恒之蓝” & “挖矿”攻击

近两年奇安信应急响应过的工业企业网络攻击事件，涉及：汽车生产、智能制造、能源电力、烟草等行业，**工业主机成为最主要的攻击对象。几十余家企业，大多数都导致了工业主机蓝屏，文件加密，生产停工**



某汽车模具厂，停产

某冷轧钢板厂，停产

某炼钢厂，停产

某关键IC厂，停产

某奶粉企业，停产

2017.05

2018.07

2018.10

2019.01

2019.04

安全事件：某智能制造企业遭网络攻击停产

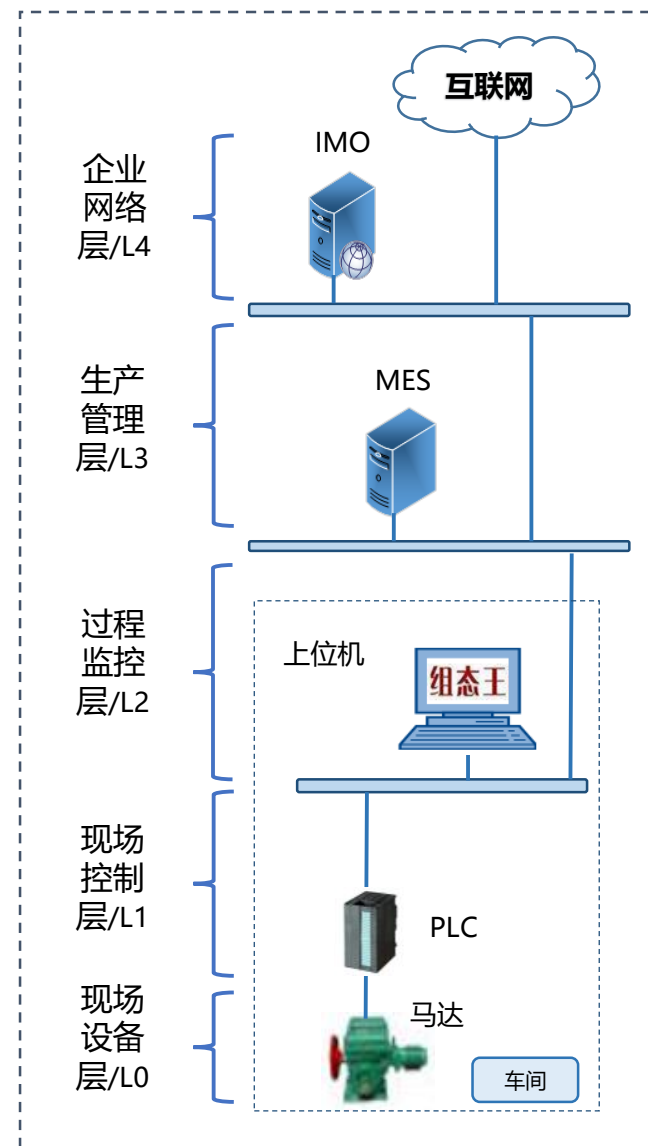
事件过程

2018年9月，某大型智能制造企业遭勒索病毒攻击，数十台工业主机蓝屏重启，多条生产线停产，损失严重。

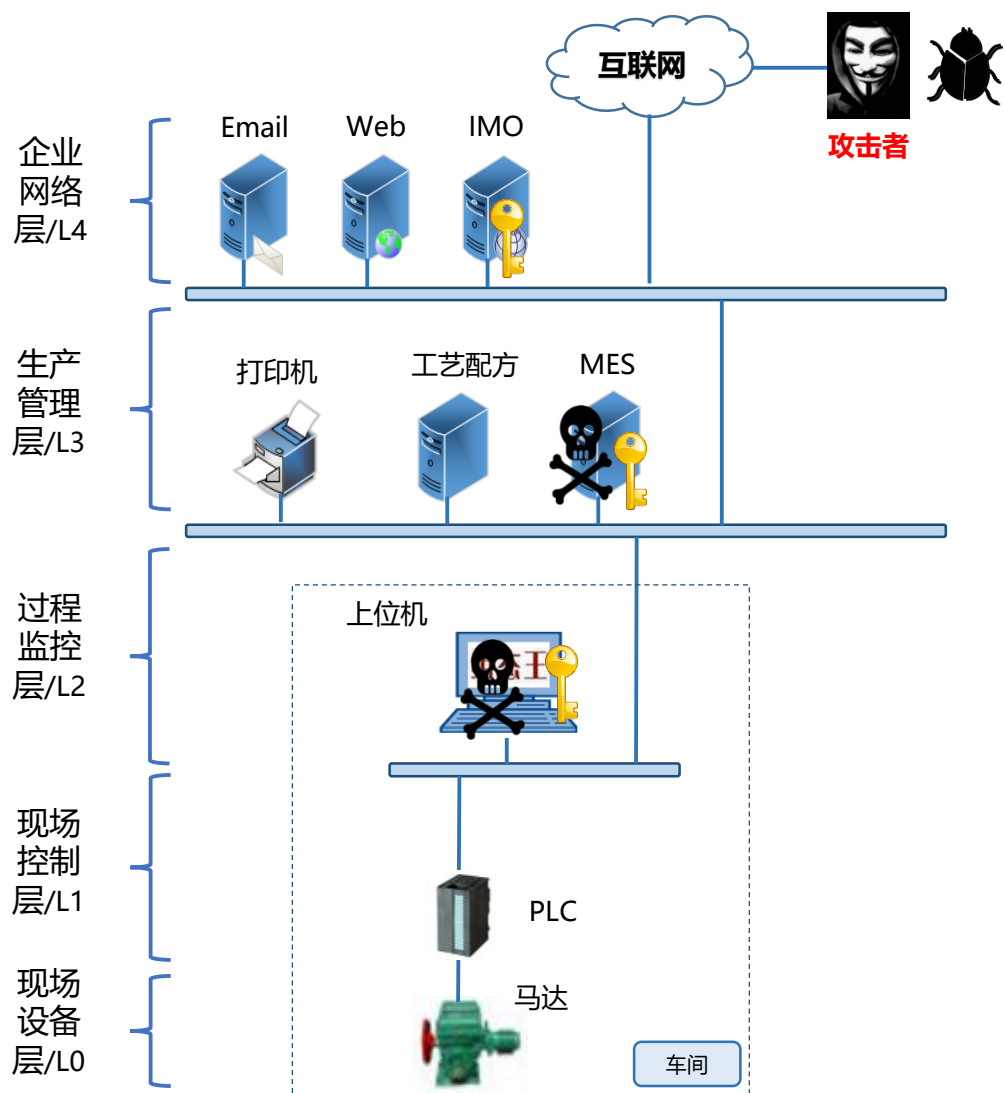
奇安信工业安全提供紧急安服响应，帮助快速恢复生产。通过对现场网络安全风险评估，发现多个安全漏洞。

在实验室仿真客户环境，还原攻击过程。

设备	用途	系统配置	存在漏洞
IMO	OA服务器	CentOS	任意命令执行漏洞
MES	生产管理服务器	Win7 64位	“永恒之蓝”漏洞
上位机	控制PLC	WinXP SP3, 组态王, 双网卡配置	远程堆溢出漏洞
PLC	控制器	西门子300	拒绝服务漏洞



工控安全事件回顾（某智能制造企业受到攻击而停产）



1. 攻陷IMO服务器

攻击者利用办公网IMO服务器的**任意执行漏洞**，发起攻击获得服务器权限。

2. 攻陷MES服务器

搜索内网发现MES主机，利用MES存在的**“永恒之蓝”漏洞**，获取权限；将勒索病毒样本上传至MES主机运行，病毒在内网中蔓延传播。

3. 攻陷上位机

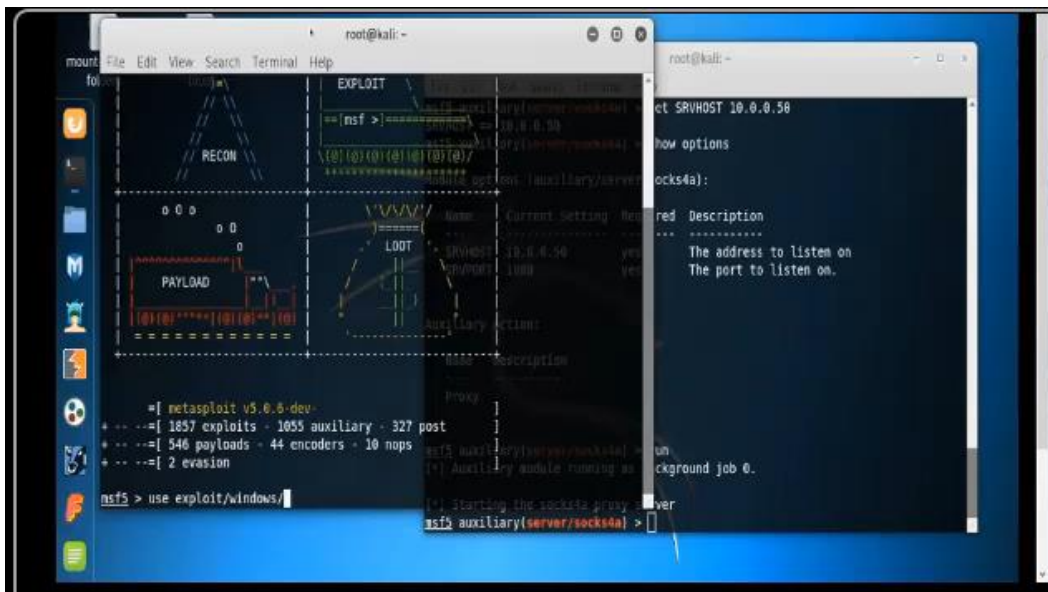
搜索内网发现双网卡配置的XPSP3上位机，利用上位机组态软件的**远程堆溢出漏洞**，获取上位机权限。

4. 攻击PLC

继续搜索发现西门子300控制器，向上位机投递PLC攻击软件，程序运行后向PLC发送特制**Crash漏洞**攻击报文，致使PLC进入Defeat状态，其控制的马达（生产线）停转。

攻击过程实验室复现

```
root@kali:~# msf5 > use exploit/windows/socks4a
msf5 exploit/windows/socks4a >
msf5 exploit/windows/socks4a > set SRVHOST 10.0.0.58
SRVHOST => 10.0.0.58
msf5 exploit/windows/socks4a > show options
[*] Auxiliary module running as background job 0.
msf5 exploit/windows/socks4a > run
[*] Starting the socks4a proxy server
msf5 auxiliary(server/socks4a) >
```



目录

工业互联网安全现状与趋势

中小企业面临的工业互联网安全挑战

怎样的防护方案对中小企业更适用吗？

中小企业工业互联网安全防护建议

《关于印发中小企业划型标准规定的通知》

(二) 工业。从业人员1000人以下或营业收入40000万元以下的为中小微型企业。

其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；

从业人员20人及以上，且营业收入300万元及以上的为小型企业；

从业人员20人以下或营业收入300万元以下的为微型企业。

年收入在5000万美元至10亿美元之间的组织。

Gartner.

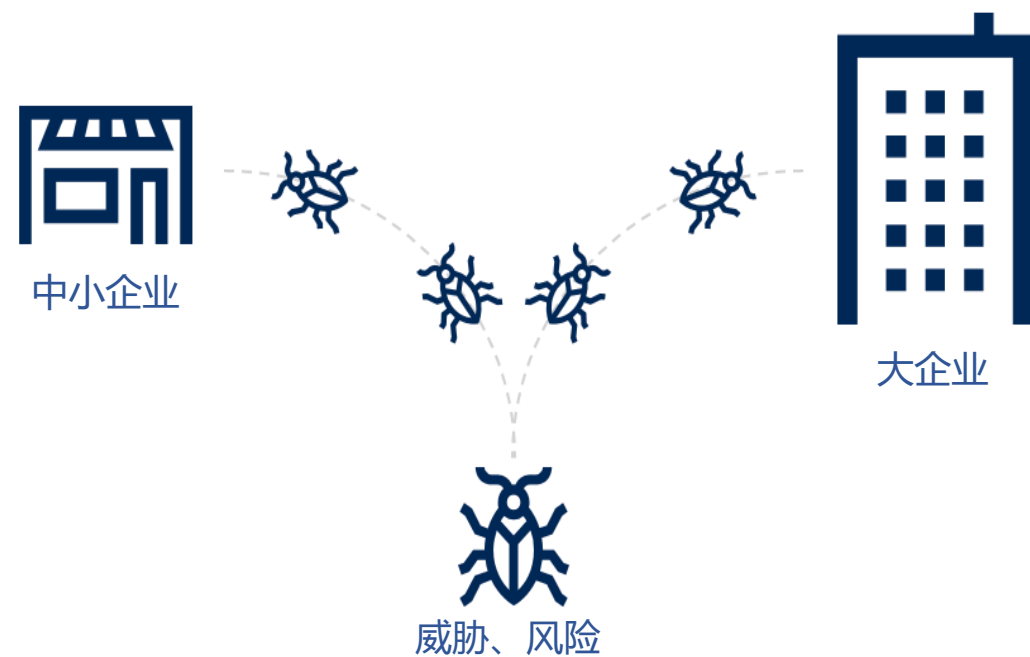
广义的中小企业：

有一定生产规模和网络化基础，在行业排名中处在中上水平的工业企业。

中小企业而外的安全挑战

- 有限的安全控制、人员分配、预算和流程使中小型企业面临安全问题
- 无专门的OT安全团队，IT人员难以处理工业安全事件和策略实施
- 人才稀缺，难于跟大公司竞争相同网络安全人才

中小企业面临和大公司相同的威胁



CIMT2019 上500家工业企业调研

工业互联网安全现状调查

为了深入了解国内工业企业网络工业互联网安全建设现状，特展开本次展开此次针对工业互联网的调研活动。

1. 您所在单位的行业是:

- A、政府机构/事业单位 B、科研机构 C、制造业 D、市政/交通 E、通信/网络
F、石油石化/化工 G、能源电力 H、水务 I、医疗 J、其他
G、汽车 建筑 (设施) 自动化
H、水泥和玻璃
I、化学, 电子和电气
J、电力
K、机械
L、采矿和金属
M、石油和天然气
N、精炼

O、半导体石油石化/化工 G、能源电力 H、市政/交通 I、通信/网络 J、其他 远程联网调试设备经常蓝屏、重启

2. 贵单位是否组织过网络安全意识培训?

- A、有 B、没有 C、不了解

3. 您听说过以下哪些有关工业互联网的安全事件? ()

A、伊朗核电站震网病毒事件 B、委内瑞拉遭受网络攻击大规模停电事件 C、挪威铝业公司 Norsk Hydro 遭受勒索软件攻击工业

4. 您认为贵单位工业网络遭遇攻击的可能性:

- A、很大可能 B、基本不会 C、完全不会

5. 您认为网络病毒是否可以攻击到您单位车间的工业设备?

- A、能 B、不能 C、不了解

6. 如果车间的设备上遭遇网络病毒攻击, 您认为会对设备产生哪些影响?

- A、不能运转 B、产品质量受损 C、浪费生产材料 D、没影响

7. 贵单位生产车间的工业设备是否可以插入U盘?

- A、可以 B、不可以 C、不了解

5.1 对U盘是否有管理规范 (如果回答可以)

A, 没有任何规定, 任意U盘都可以 B有, 只能使用公司U盘, 但不需要任何杀毒 C, 有, 只能使用公司U盘, 使用前需要杀毒

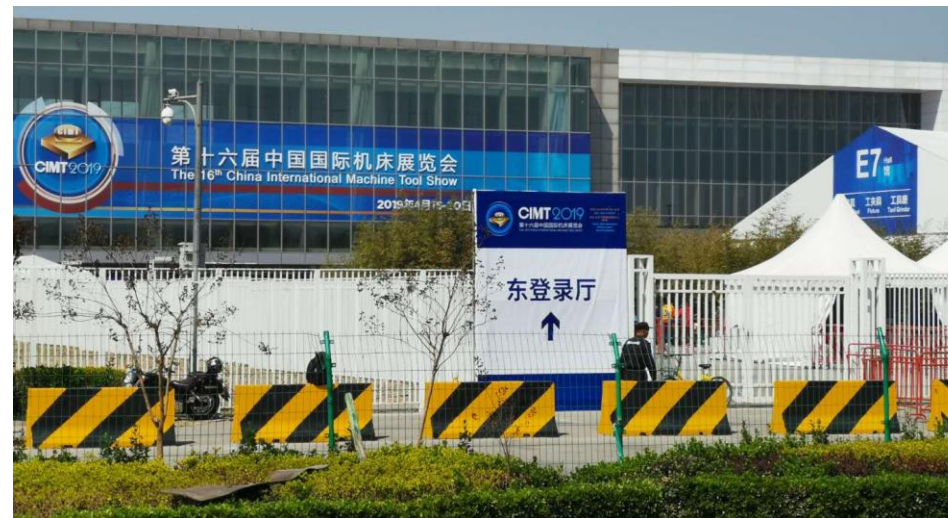
8. 贵单位生产车间中的工业设备能否联网?

- A、能 B、不能 C、不了解

7.1 可以连上哪些网络? (选择能)

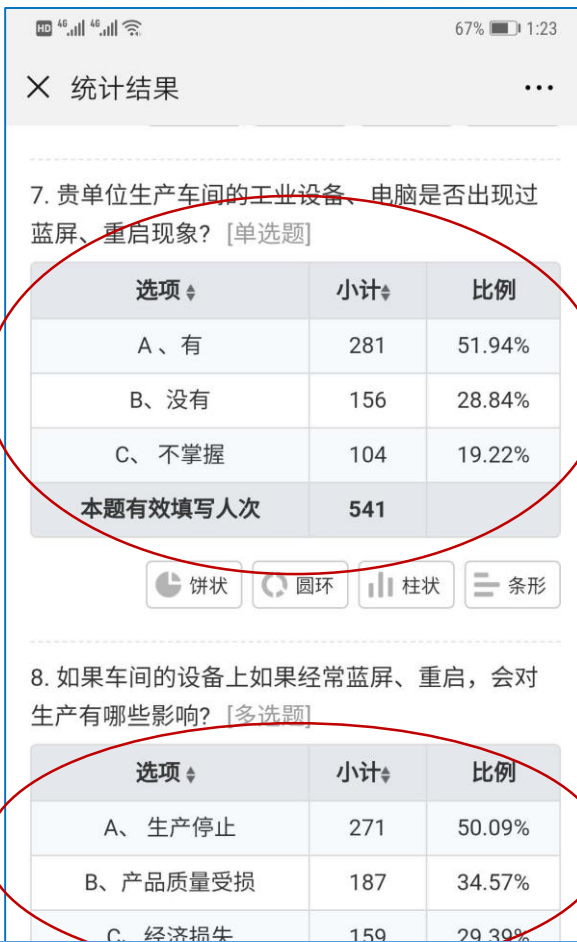
- A、只能连接工业网络 B、工业网络和普通办公网络都可以连接

9. 您办公电脑是否可以和车间设备 (上位机) 进行联网, 传输文件?



CIMT2019 中国国际机床展集中企业调研

企业调研结果分析



- 超过50%企业生产联网——工业互联网发展潜力大
- 超过50%的出现蓝屏重启（勒索）——安全事件频发、损失大
- 网络事件37%找安全厂商，36.4%找工控厂商——产业协同必要

案例一：某家具制造企业出现蓝屏、重启现象

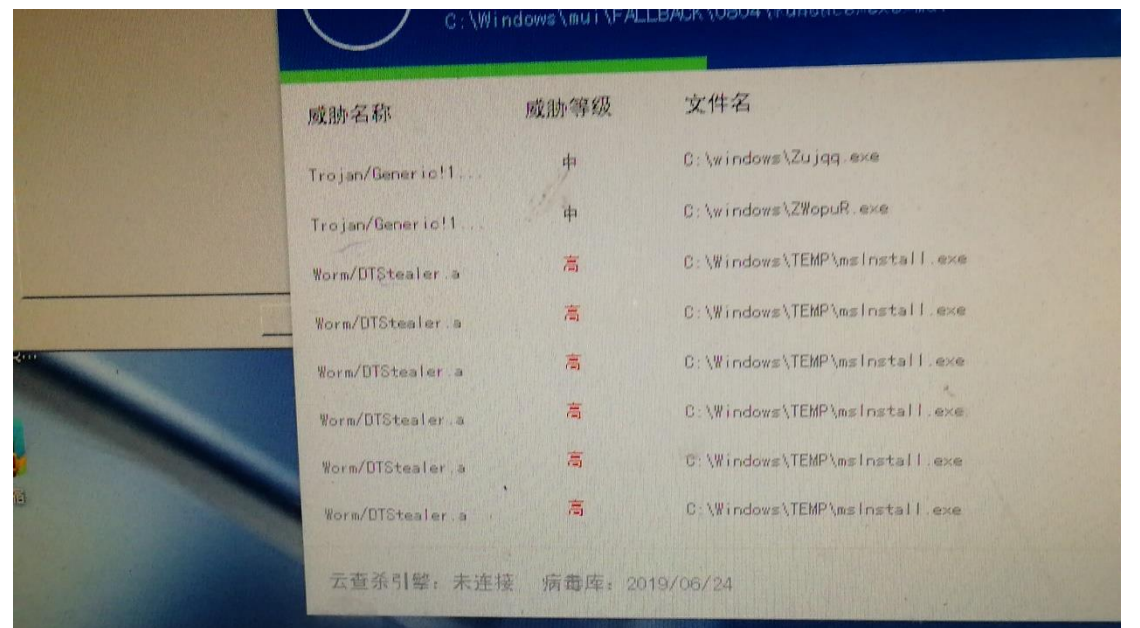
2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

工厂投资1.2亿元，拥有2.5万平方米数字化定制工厂，致力于**德国品质板式家具的研发与生产**。2019年5月27日，车间板件加工主机出现CPU使用率达100%现象，占用CPU最高的进程为powershell.exe；同时，同时有其他板件加工主机出现系统重启后，**工控软件无法正常运行的现象**。对问题进行全面了解后，6月24日应急人员出发前往现场协助问题处置。

事件分析：

整个厂区的网络结构较简单，**车间近20台主机与办公网主机路由可达**，且均能上外网，最大的特点为网络**未进行分区域规划**（划分办公网与生产网）网络中无基本的安全防护设备。另外，车间的**主机密码存在相似、未满足密码复杂度要求**的现象。

当前生产网络中存在各类病毒：DTLMiner、驱动人生病毒，可推测DTLMiner病毒为外部攻击、渗透进入。



案例二：某IC生产企业出现蓝屏、重启现象

2019年2月，该制造企业将机台设备集体进行上线，卧式炉、厚度检测仪、四探针测试仪、铜区等多个车间的机台主机以及MES客户端都不同程度的遭受蠕虫病毒攻击，出现蓝屏、重启现象。

事件分析：

操作站上抓取挖矿病毒样本、勒索蠕虫变种样本，病毒可被检测，后端进行样本分析，在现场处于MES网络的主机上，同时发现“永恒之蓝”蠕虫变种和挖矿病毒。

扫描完成！共发现 2 个需要处理的危险项

扫描时间：00:00:25 扫描类型：自定义扫描 扫描项目：2个 暂不处理 一键处理

发现 2 个危险项

- 建议隔离 Win32/Trojan.Multi.daf 木马 立即处理
D:\工作\应急响应\中车\样本01\xp\AppDiagnostics\svchost.exe
- 建议隔离 Win32/Trojan.Multi.daf 木马 立即处理
D:\工作\应急响应\中车\样本01\xp\AppDiagnostics\spoolsv.exe

46 engines detected this file

SHA-256 ce4573d7a13df05dd8b84b6ea5acca119a28d070d976a8cfc97f5c6ec1224818
File name TrustedHost.exe
File size 1.43 MB
Last analysis 2019-02-19 02:01:10 UTC

46 / 66

Detection	Details	Relations	Behavior	Community	
Acronis	suspicious			Ad-Aware	Generic.Application.CoinMiner.1.0E40...
AhnLab-V3	Trojan/Win64.Miner.R213290			Antiy-AVL	GrayWare/Win32.Unwaders
Arcabit	Generic.Application.CoinMiner.1.0E40...			Avast	Win32:CryptoMiner-L [Trj]
AVG	Win32:CryptoMiner-L [Trj]			BitDefender	Generic.Application.CoinMiner.1.0E40...
CAT-QuickHeal	Trojan.IGENERIC			ClamAV	Multios.Coinminer.Miner-6781728-2
Comodo	Malware@#1ulu51rad746p			CrowdStrike Falcon	malicious_confidence_100% (D)
Cybereason	malicious.6a2110			Cylance	Unsafe

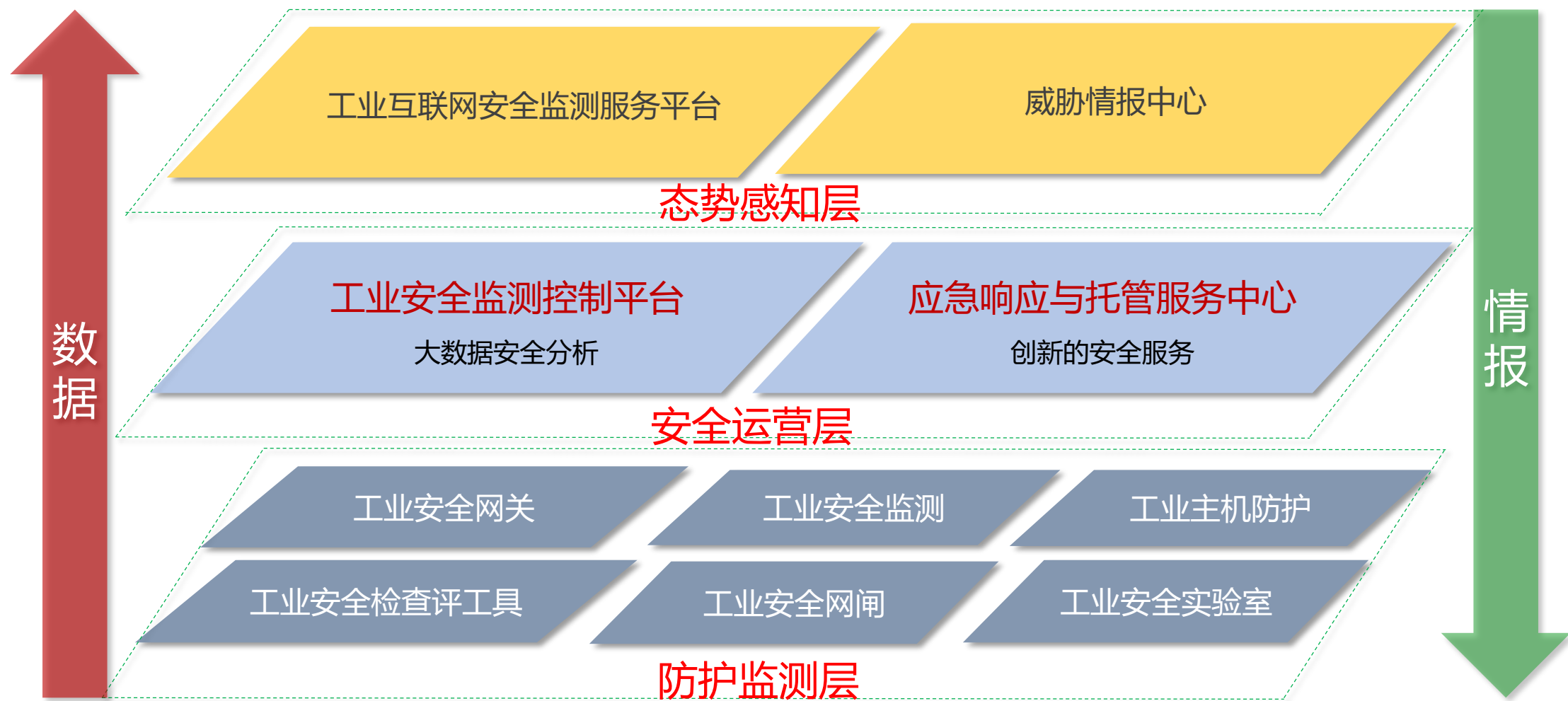
目录

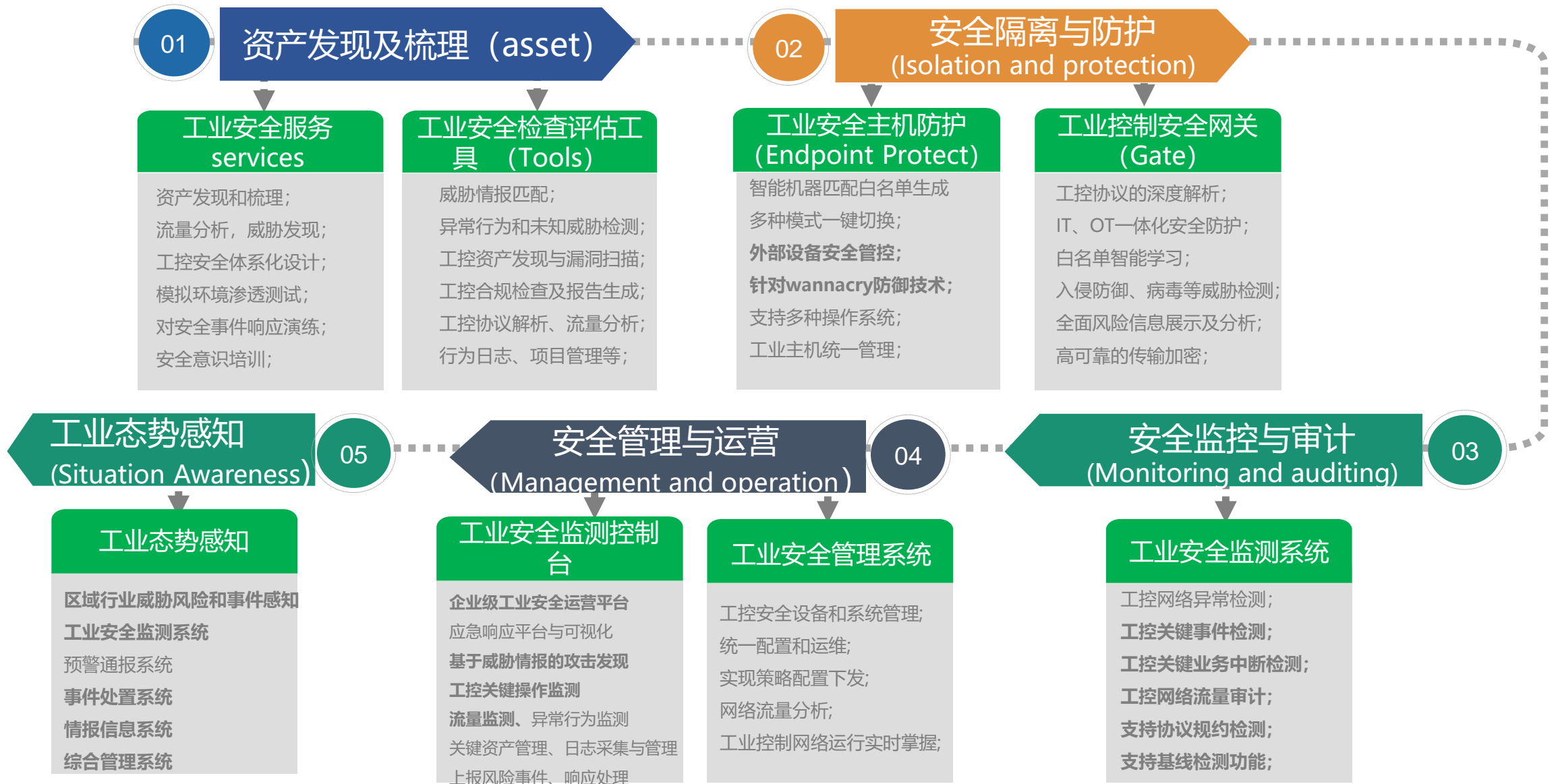
工业互联网安全现状与趋势

中小企业面临的工业互联网安全挑战

现有防护方案对中小企业适用吗？

中小企业工业互联网安全防护建议





- 由于大型企业，具有较强的实力和基础，应落实**高、中、低优先级**的战略路线
- 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



高优先级

- **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

- **持续实施安全监测**

开始并持续实施安全监测，例如：资产发现、实施配置管理、变更管理、定期审计等。

- **实施工业主机 (端点) 防护**

工业主机是连接信息世界、物理世界的门户，首先做好防护。

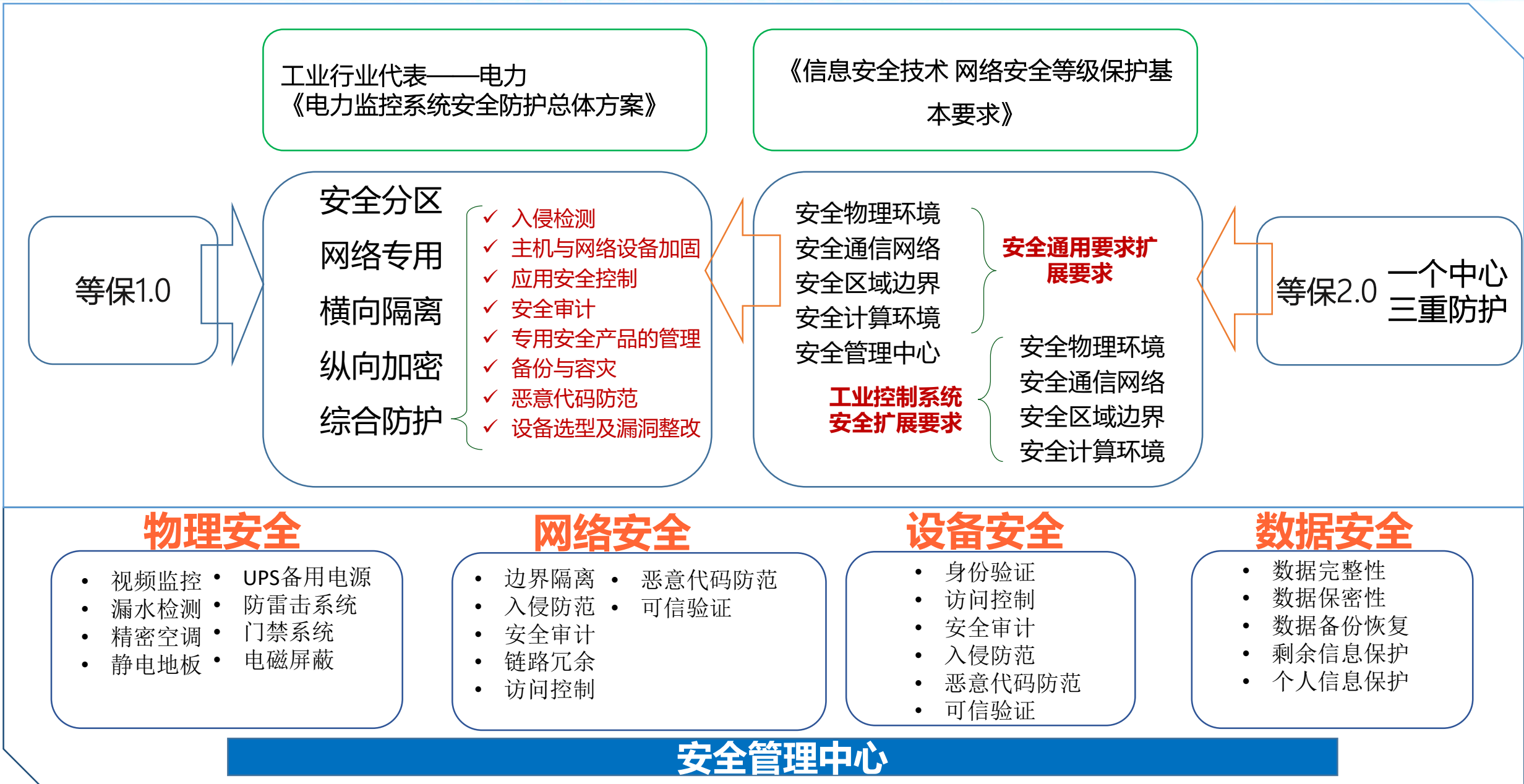
中优先级

- **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
- **提高OT安全流程的成熟度**
 - 如变更管理、配置管理、访问管理、事件管理等流程的成熟度。

低优先级

- **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



目录

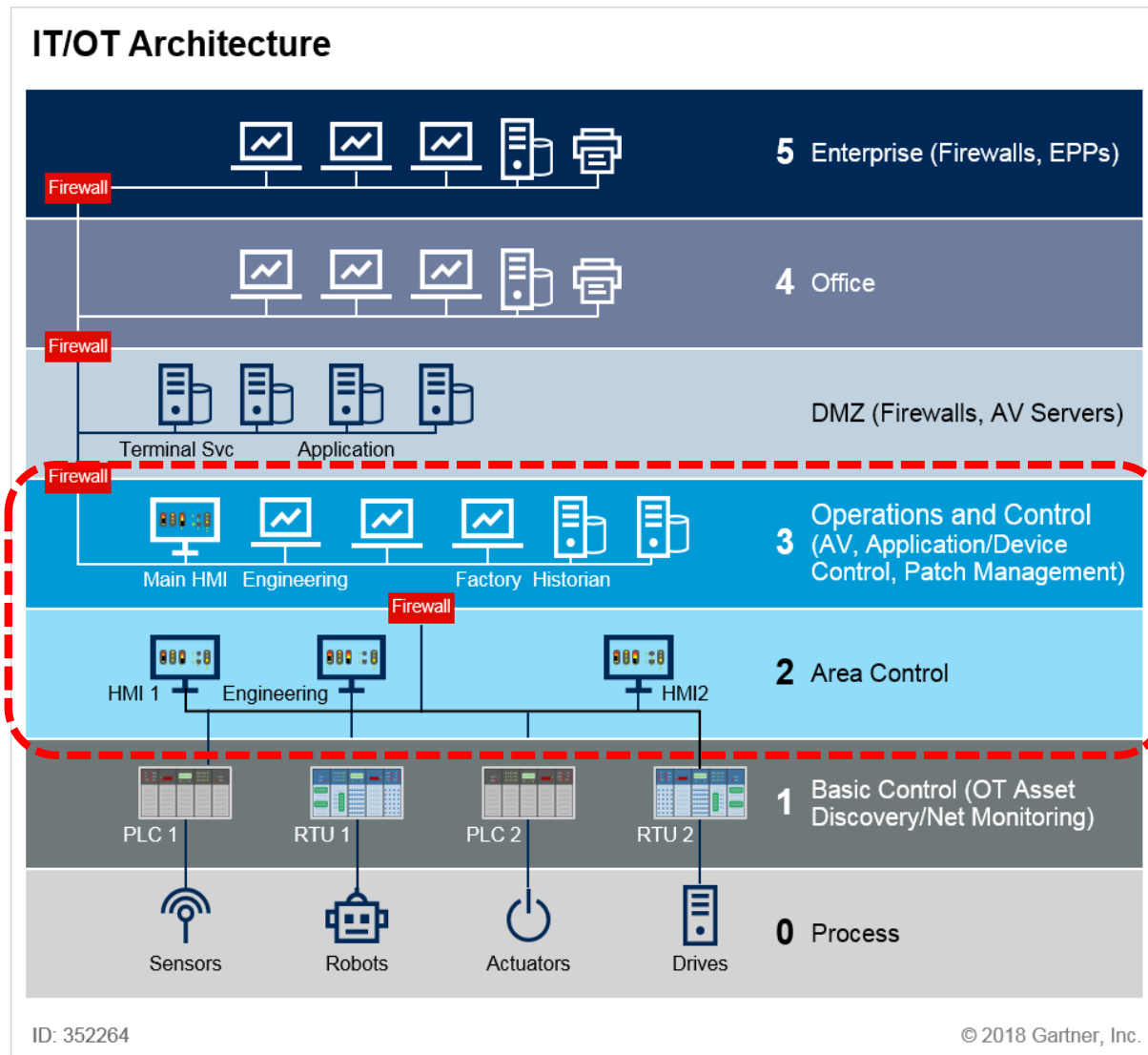
工业互联网安全现状与趋势

中小企业面临的工业互联网安全挑战

怎样的防护方案对中小企业更适用吗？

中小企业工业互联网安全防护建议

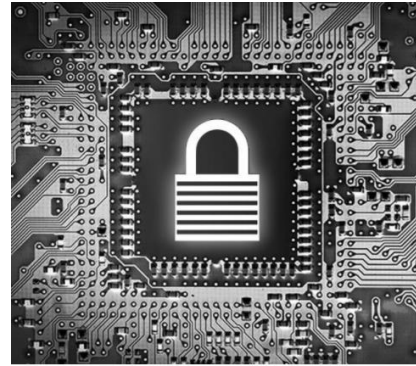
工业主机是CPS的“大门”





补丁打不上
漏洞百出

- 担心**影响生产**不想打
- 主机**不联网**无法升级
- 系统**老旧**无补丁可打



病毒杀不完
带病运行

- 硬件**配置太低**装不上杀毒软件
- 无法升级杀毒软件病毒库老旧
- 担心**误杀**工业软件，干脆不装



资产查不清
暗藏隐患

- 工业主机**家底**不清楚
- 资产配置分布**不可视**
- 整体**安全隐患**不了解

“永恒之蓝”超前防御，防蓝屏



一键设置白名单, 无需升级



网络防护, 主机中毒后防止扩散



入口拦截

运行拦截

扩散拦截

U盘管控, 防止非授权外设引入病毒



三种模式一键切换, 保障生产连续性



日志审计, 溯源攻击主机和恶意程序

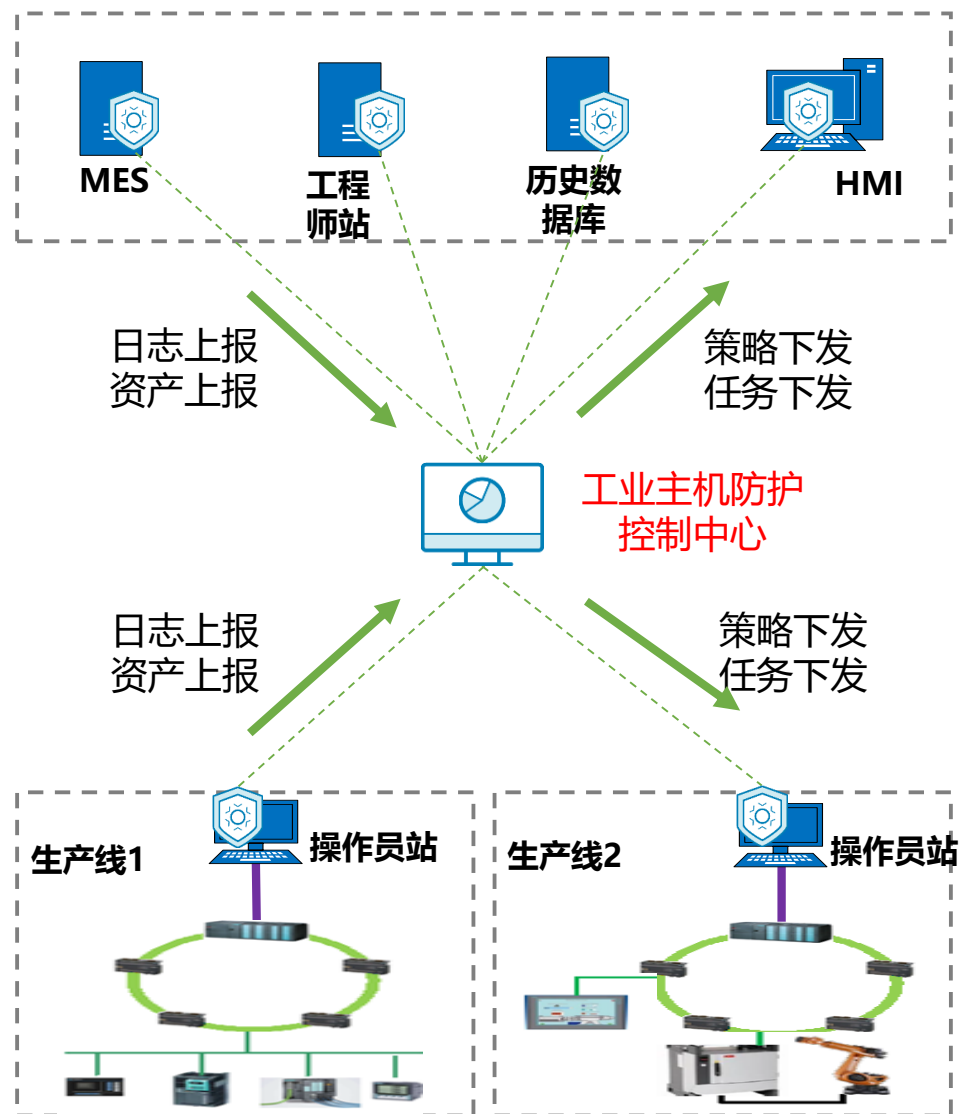


集中管理

- 配置策略下发
- 日志汇总分析
- 资产汇总分析
- 主机风险展示

灵活配置

- 灵活部署模块
- 灵活设置权限
- 灵活配置页面
- 灵活扫描时间



恐惧源于未知，看见才能安全



资产状况

资产数量不清楚
资产类型不清楚
资产分布不清楚



安全威胁

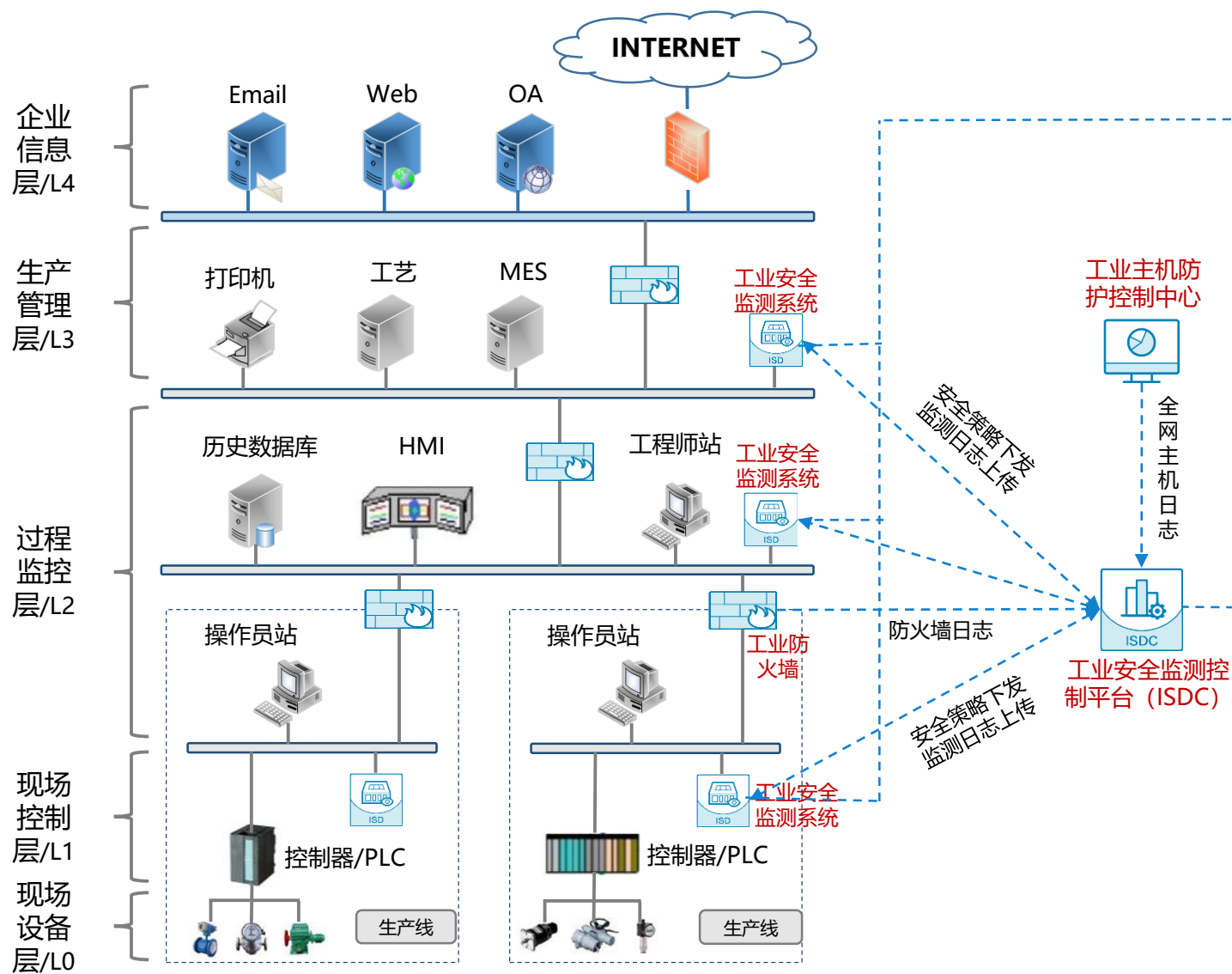
谁有隐患不知道
谁被攻击不知道
攻击后果不知道



生产故障

设备断线难定位
设备停机难定位
违规外联难定位

看清、看透、看全工业生产中的威胁，是保障工业安全的基础和前提

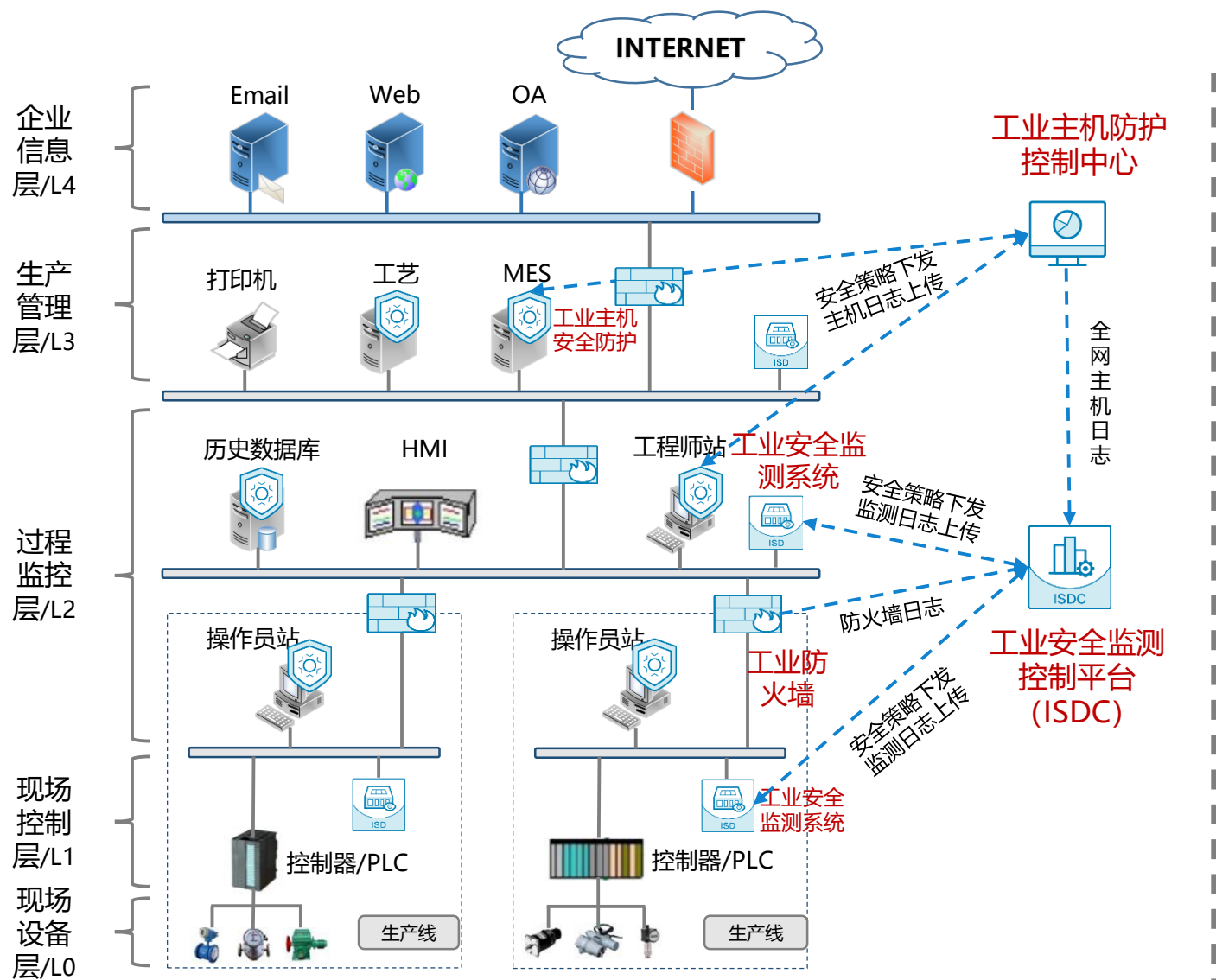


安全监测系统 ISD (硬件)

- 旁路监听网络流量
- 自动发现工业资产
- 自动发现资产漏洞
- 实时监测业务操作
- 实时检测网络攻击
- 实时检测病毒传播

安全监测控制平台 ISDC (软件)

- 汇集安全检测数据
- 汇集主机安全数据
- 全局安全风险评分
- 大屏实时态势展示
- 安全事件应急处置
- 统一安全运维管理



【主机防护】工业主机安全防护系统

- 软件形态，安装在工业主机，防病毒攻击
- 白名单管控，兼容老旧软硬件系统
- 入口、运行、扩散三重关卡病毒拦截
- 永恒之蓝专防，无需打补丁、关端口



【网络分区】工业防火墙/交换机

- 隔离不同网络，防止跨网攻击
- 专有硬件适应工业生产环境
- 工业协议及子协议深度识别
- 网络、应用、规约指令、规约数据四重防护



【安全监测】工业安全监测系统

- 旁路部署，监听网络流量
- 自动发现资产，监测非法设备接入
- 检测工控漏洞，识别工控安全风险
- 监测设备异常操作，保障连续生产
- 风险集中分析，大屏展示安全态势



45000+
已注册白帽子数量



5000+
已注册机构数量

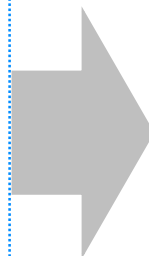


30万+
已发现漏洞总数



2000万+
已发放奖金总额

网络安全产业



工控
系统
厂商

- 安全意识相对薄弱
- 安全开发能力不足
- 漏洞研究人才匮乏



网络
安全
厂商

- 工控系统品类繁多
- 获取成本相对较高
- 工业领域认知有限

以用户知情为宗旨的
漏洞披露和协同治理机制

工业安全领域

漏洞验证-外部力量 白帽子与补天平台

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

https://admin.butian.net/Admin/Index/index.html#12/1129

欢迎您, zhangweifeng01 | 修改密码 | 修改资料 | 退出

后台首页

漏洞管理

漏洞管理

工控漏洞-初审

漏洞列表

工控漏洞-初审

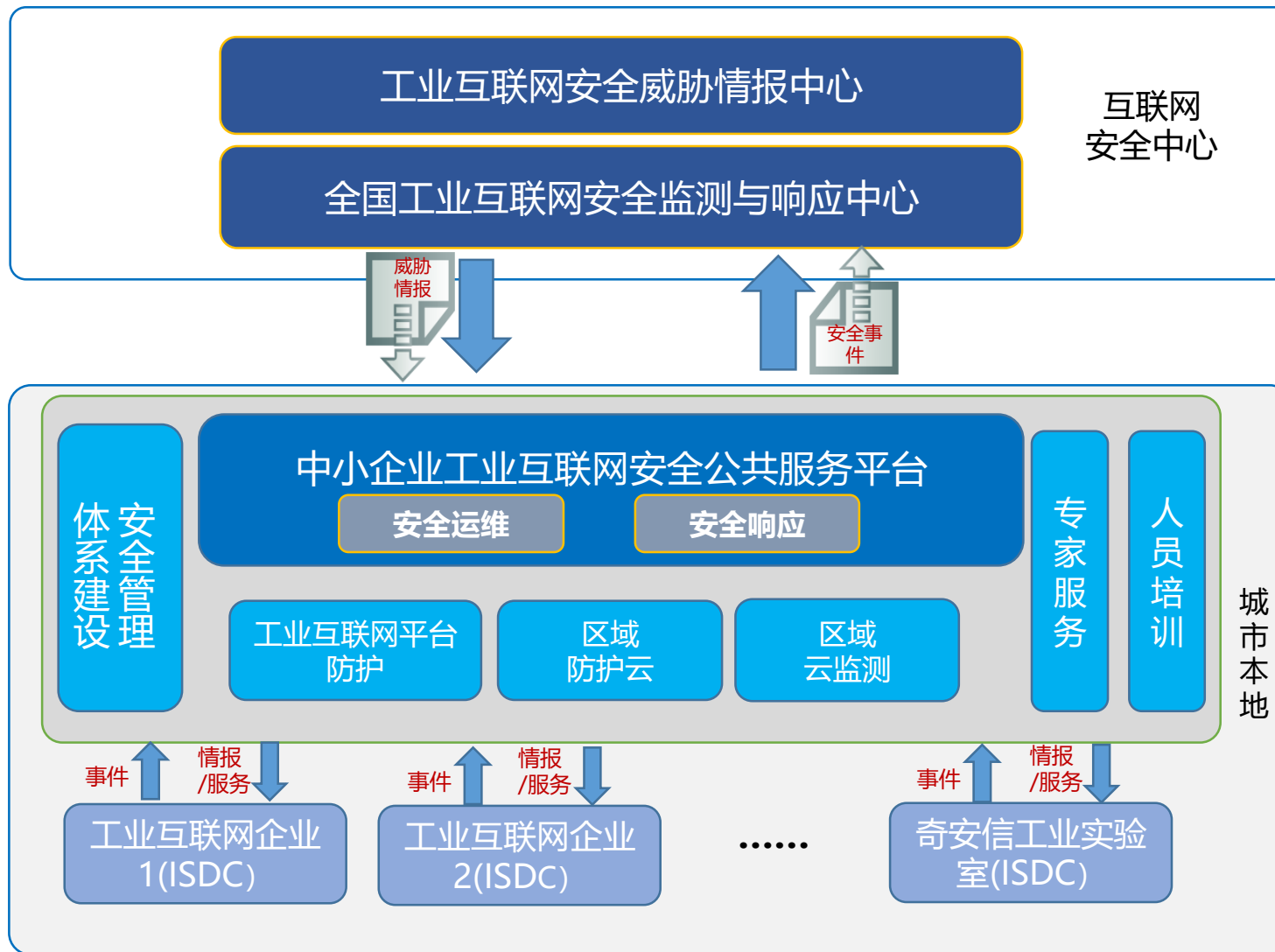
工控漏洞-复核

漏洞ID: 漏洞标题: 厂商名称: 漏洞内容: 白帽名称:

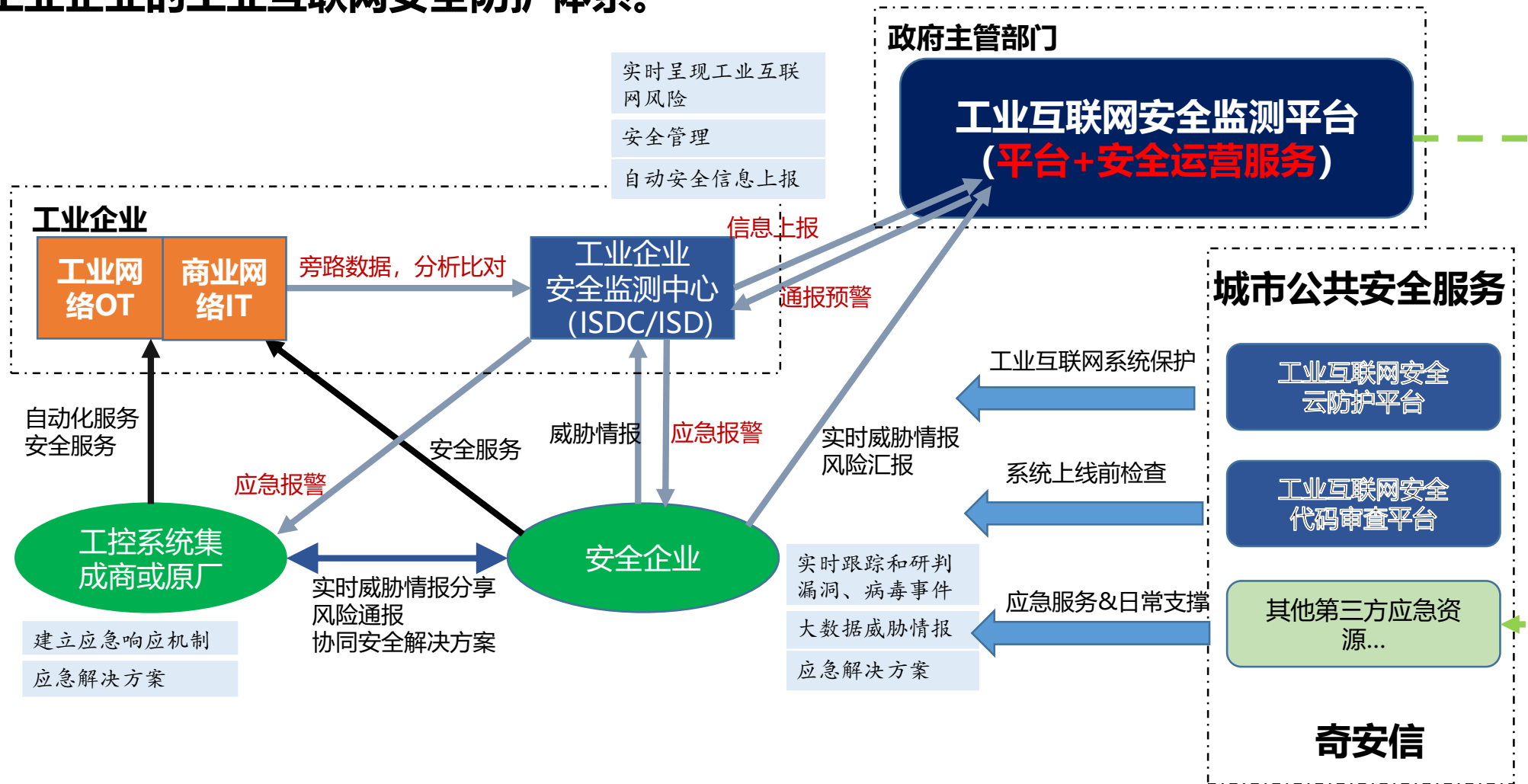
审核状态: 厂商状态: 每页: 条

漏洞已归属 (0) 未处理 (22) 暂不处理 (0) 显示更多条件 搜索

<input type="checkbox"/> 全选	漏洞标题	厂商	白帽奖金	估价	定价	等级	积分	白帽子	是否匿名	审核状态	厂商状态	财务状态	邮件状态	写入时间	更新时间	审核人员	操作
<input type="checkbox"/> 338021	研华Advantech WebAccess SCADA控制系统监控组态软件存在远程代码执行漏洞	研华科技				高危	1000	曲线人数	否	审核通过	等待确认	已支付	未发送	2019-04-14 23:06:59	2019-04-19 15:29:05	zhangweifeng01	编辑
<input type="checkbox"/> 338637	珠海方正某处未授权访问	珠海方正印刷电路板发展有限公司				低危	0	一般小小白	是	审核通过	等待确认	待支付	未发送	2019-04-18 18:24:33	2019-05-02 21:55:02	zhangzhao	编辑
<input type="checkbox"/> 338814	西门子s7协议异常导致设备宕机	西门子(中国)有限公司				高危	0	月落	是	审核不通过	默认	默认	未发送	2019-04-19 18:22:13	2019-05-02 21:55:02	zhangzhao	编辑
<input type="checkbox"/> 339417	GE Proficy Machine Edition任意文件删除漏洞	GE				低危	0	大佬666	是	审核通过	等待确认	待支付	未发送	2019-04-22 08:39:46	2019-05-06 14:55:01	zhangzhao	编辑
<input type="checkbox"/> 339676	施耐德SoMachine Logic Builder V4.3存在未授权访问漏洞	施耐德				中危	0	曲线人数	是	审核不通过	默认	默认	未发送	2019-04-23 01:09:21	2019-04-29 09:51:24	zhangzhao	编辑
<input type="checkbox"/> 339679	施耐德SoMachine Logic Builder V4.3存在认证保护限制绕过漏洞	施耐德				高危	0	曲线人数	是	默认	默认	默认	未发送	2019-04-23 01:36:41	2019-04-24 11:11:51	zhangweifeng01	编辑
<input type="checkbox"/> 340047	研华科技AdvantechWebAccess3.4.0存在文件夹删除漏洞	研华科技				低危	0	大佬666	是	审核通过	等待确认	待支付	未发送	2019-04-24 19:51:28	2019-05-06 14:55:01	zhangzhao	编辑
<input type="checkbox"/> 340898	北京力控ForceControl SCADA监控组态存在远程拒绝服务漏洞	北京力控				高危	0	曲线人数	是	审核不通过	默认	默认	未发送	2019-04-29 18:54:07	2019-05-14 15:55:01	chengwangzong	编辑
<input type="checkbox"/> 340947	北京力控ForceControl SCADA监控Web server服务存在缓冲区溢出漏洞	北京力控				高危	0	曲线人数	是	默认	默认	默认	未发送	2019-04-29 20:57:26	2019-04-29 20:57:26		编辑
<input type="checkbox"/> 340952	施耐德IWS v8.1 InduSoft Web Studio存在任意代码执行漏洞	施耐德				高危	0	曲线人数	是	默认	默认	默认	未发送	2019-04-29 21:15:15	2019-05-07 15:19:36	chengwangzong	编辑
<input type="checkbox"/> 340960	施耐德普池菲斯GP-Pro EX 4.08组态软件存在权限提升漏洞	施耐德	0	0	0	高危	0	曲线人数	是	默认	默认	默认	未发送	2019-04-29 21:43:19	2019-04-29 21:43:19		编辑



建立以**内外网监测**为基础，以**协同联动和信息共享**为驱动，以**安全运营**为中心，以**业务服务**为目标的面向工业企业的工业互联网安全防护体系。



加强安全培训

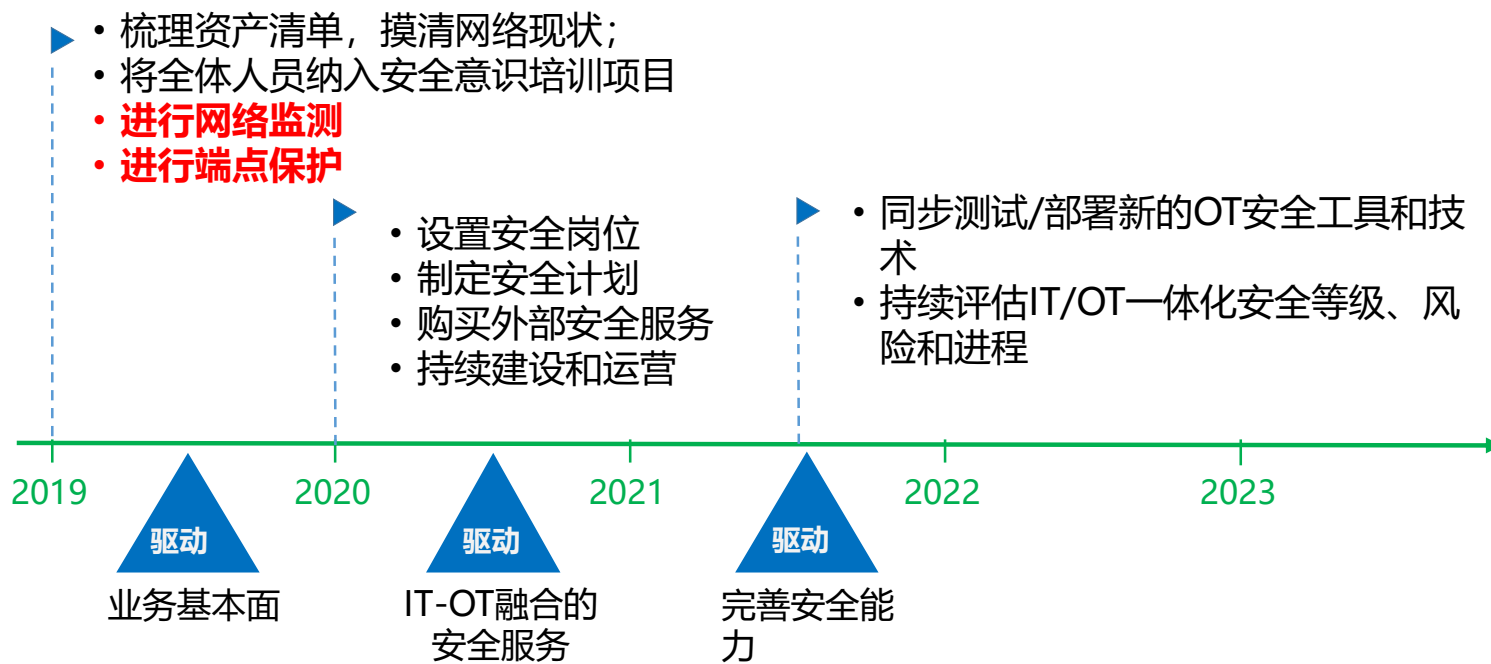
做好安全服务

- 领导者应在采购、运营和工程的执行层面建立安全意识，以确保在选择和采购新生产设备的过程中包含适当的安全要求。
- 每年进行一次安全培训；
- 将安全培训作为新员工入职培训的强制部分；
- 从意识——培训——教育三方面落实，关注安全，培养相关技能和能力，培养安全专家；

- 中小型企业资金紧张，无法按照普渡参考模型进行安全部署，要想做好安全建设应该与安全企业做好产业合作；
- 将网络安全的能力，将变成一种可定制的服务，工业互联网企业可以根据自己的威胁、成本、人才和运行阶段按需使用；


主机防护 + 安全监测 + 安全响应服务（找谁？） = 解决80%的网络安全问题

- 由于中小企业，**做好业务基本面抵御常见威胁，购买安全服务，降低安全支出**
- 需要循序渐进，完善安全能力



战略路线图时间表



The background features a dark blue color with a white grid pattern that forms a wave-like shape on the left side. The grid lines are thin and closely spaced, creating a mesh effect. The overall design is clean and modern, typical of a professional conference slide.

THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE