赛姆科技
SAM TECHNOLOGY

数字化转型的安全思考

演讲人：闫维玮
TEL：13570544916

可信·安全·通畅

系统管理大师 ▪ 专注数据安全

一、现有信息安全解决方案的盲区

赛姆科技 SAM TECHNOLOGY

智慧城市的软肋：网络攻击威胁公共安全

作者：nana 星期二, 十月 11, 2016 0

技术分析师对“智慧”城市的概念存在分歧。一方面，支持者认为，通过创建“智慧”系统运营公共交通、垃圾处理、交通管控和供水系统，城市可以提升市政服务的效率。随着全球人口持续增长，这种增强的生产率将会帮助大都市更好地容纳更多人口。

2021年针对关键制造业漏洞的攻击事件激增

2021-07-15 19:57 • 稿源：cnbeta

新的研究表明，在2021年上半年，关键制造业的漏洞增加了148%，基于勒索软件的全套服务（RaaS）驱动了大部分攻击数量的增幅。 Nozomi Networks的报告发现ICS-CERT的漏洞也增加了44%。制造业是最容易受到影响的行业，而能源行业也被证明是脆弱的。

游离于主流信息安全技术视野之外的各类基础设施设备系统的安全

一、现有信息安全解决方案的盲区

广东：成功破获首例非法入侵“常规摄像头”黑客案件 500多组

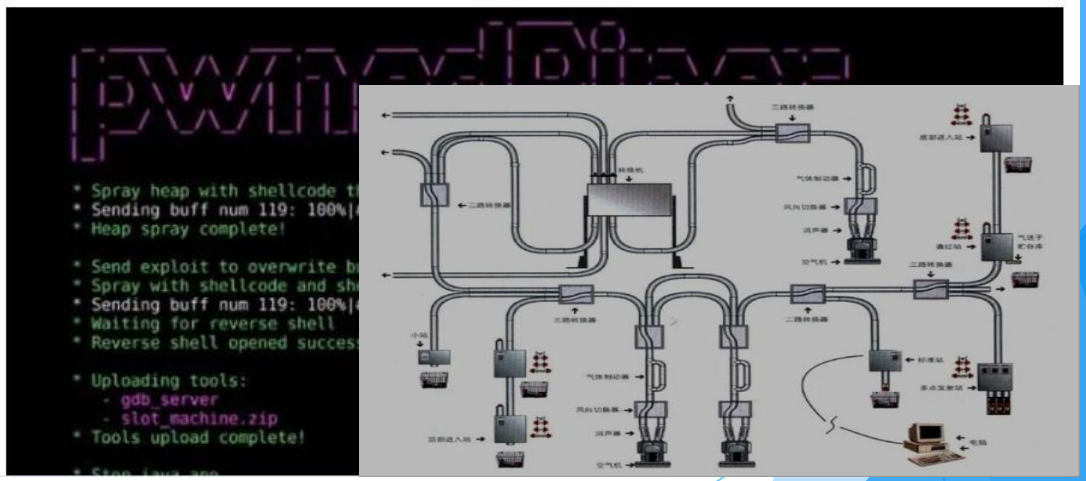
GRT直播广东

广东：成功破获首例非法入侵“常规摄像头”黑客案件 500多组摄像头被入侵 涉换衣间、卧室

全球数千家医院受严重漏洞影响，敏感运输系统可被劫持

医疗卫生 · 互联网安全内参 · 2021-08-03

研究员发现，全球数千家医院广泛使用的医院气动管道输送系统，存在一系列严重漏洞，可被劫持完全接管系统。气动管道输送系统负责在医院内部安全运输血液、药物和测试样本等高度敏感的物品。



游离于主流信息安全技术视野之外的各类基础设施设备系统的安全

1、智慧城市需要安全防护吗？

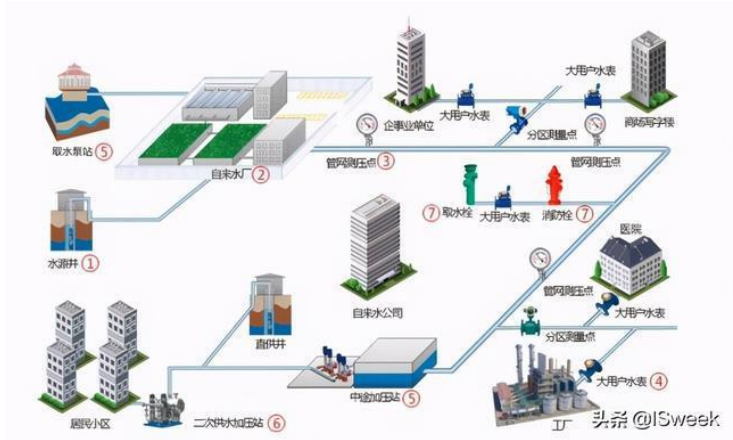
智慧城市

智慧交通

安防摄像头

抓拍摄像头

智慧供电



智慧供水

智能信号灯

2、联网医疗设备有安全风险吗？

赛姆科技 SAM TECHNOLOGY

高端影像设备，如CT、核磁共振等

安全风险

- **远程运维和更新升级联网风险：**设备联外网提高了风险等级，有关部门提出要求，不能解决进口设备安全问题就停止该设备的进口；
- **无安全解决方案**，多数不支持第三方提供的安全软件；
- 易被**内网安全威胁**干扰正常工作；
- 原厂工程师现场**维护费用极高**，**效率极低**，停用医院**损失大。**

3、数字化工业设备需要防护吗？

赛姆科技 SAM TECHNOLOGY

工控机、机器人设备、产线台机、智能显示终端

安全风险

- **设备价值高厂家直接维护**，用户不能擅自更改后台操作系统，即使允许也风险极高，可能导致设备停运；
- 多数不支持第三方提供的安全软件；
- 原厂工程师现场**维护费用极高，效率极低。**

4、终端、亚终端设备需要安全防护吗？

闸机

自助机

摄像头

智慧灯杆

- ✓ **领导用电脑**
- ✓ **设计师用电脑**
- ✓ **财务部用电脑**
- ✓ **低版本终端**

特点：

- ✓ **低版本**操作系统
- ✓ **嵌入式**操作系统
- ✓ **不支持**第三方提供的安全软件
- ✓ 防护级别不够
- ✓ 亚终端设备
- ✓ 户外暴露
- ✓ 无人值守

安全风险：

- ✓ 摄像头非法接入
- ✓ 摄像头入侵
- ✓ 摄像头假冒
- ✓ 视频篡改
- ✓ 视频数据窃取
- ✓ 摄像头刷机
- ✓ 口令暴力破解

5、已过等保测评，就没有安全漏洞了吗？

赛姆科技 SAM TECHNOLOGY

等保要求以主流安全防护手段为主 → **主流安全防护手段难以覆盖的地方**

等保测评

- **核心系统**通过**三级**等保测评，**非核心系统**通过**二级**等保测评
- 部分单位坚持**每年复审**，复审结果均为**合格**

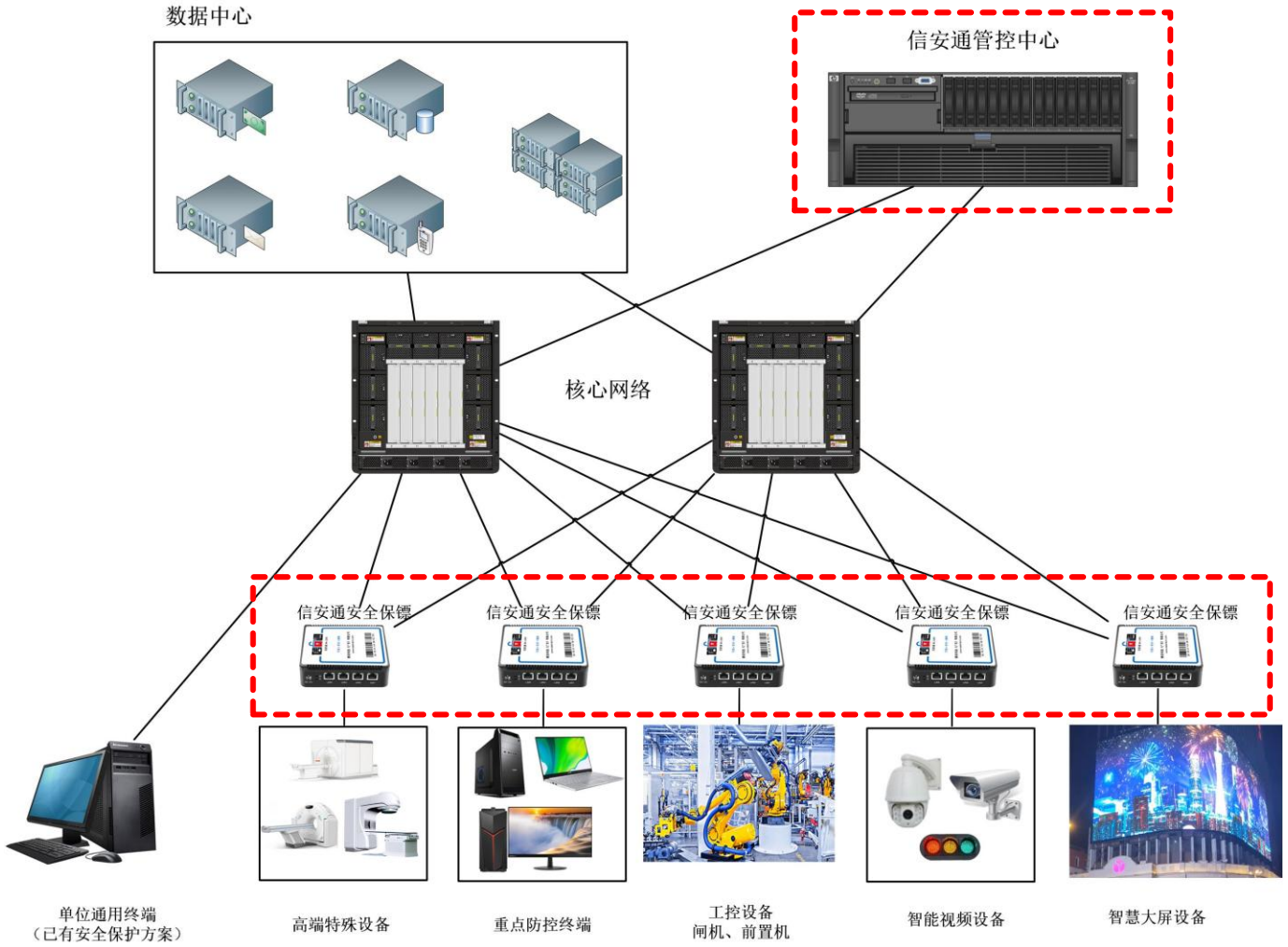
安全建设

- **边界设备齐全：**防火墙、网闸、上网行为管理、WAF等
- **具备检测类设备**：入侵检测、态势感知、日志审计
- **终端安全防护到位**：终端杀毒、准入控制
- 单位具备安全制度和流程
- 人员具有一定的安全意识和安全事件处理经验

安全漏洞

- **性能不足以部署杀毒软件**等安全管控软件的终端设备
- **各种物联网设备**：摄像头、闸机等
- **各种行业特殊设备**：工控设备、医疗仪器、自助柜员机
- **难以侦测**到违规的**WIFI热点**
- 其它各类难以安装、部署常规安全管控软件的设备

二、信安通解决方案——系统架构



信安通分布式防火墙：

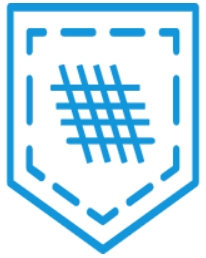
- 高性能、高稳定性的**软硬架构**
- 硬件级解决方案，**提供适用于百兆/千兆/万兆网络的多款型号**
- 自带**硬件Bypass和软件Bypass**
- 即插即用，统一管控
- 无状态，零感知
- **可适配多种应用场景**

二、信安通解决方案八大功能

赛姆科技 SAM TECHNOLOGY

访问控制

- 基于黑白名单
- 细粒度访问控制
- 实现点对点防护

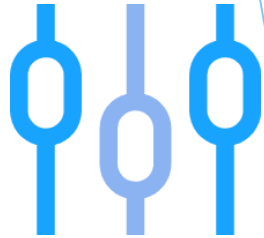


虚拟补丁

- 内置常见漏洞的补丁
- 基于行为特征的防范
- 可自定义开发

弱口令检测

- 基于流量的分析
- 使用常用的弱口令库
- 识别应用弱口令



文件管控

- 可识别exe文件
- 可控制传输的文件类型
- 可实现文件转发控制

二、信安通解决方案八大功能

赛姆科技 SAM TECHNOLOGY

ARP防护

- 自动发现ARP攻击
- 实现主动防御
- 被保护设备获得免疫攻击能力

IP/MAC绑定

- 建立IP和MAC策略表
- 阻止违反策略的访问
- 可以实现黑白名单

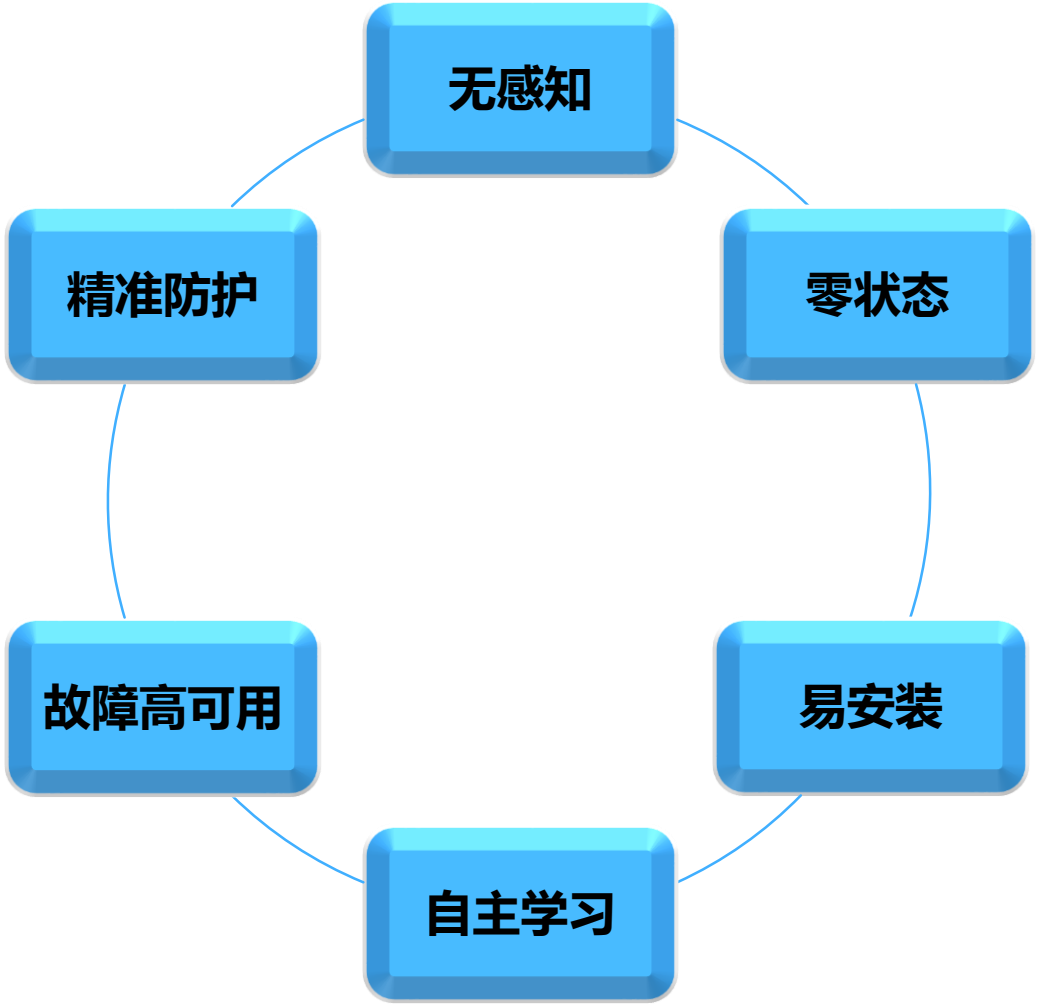
Flood防护

- 针对SYN/TCP/UDP/ICMP等常用协议
- 可调整泛洪阈值
- 自动防护自动阻断

大流量预警

- 针对网络流量可设置阈值
- 超过阈值自动报警

三、信安通解决方案六大特点



三、信安通解决方案——产品型号

赛姆科技
SAM TECHNOLOGY

SA-100
适用于百兆或以下网络

SA-1000
适用于千兆或以下网络

SA-10000
适用于万兆或以下网络

四、信安通安全防护效果

赛姆科技 SAM TECHNOLOGY

- 通过点对点的访问控制+IP/MAC绑定功能，**阻止99.999%**的**非法访问**；
- 通过文件识别，实现业务数据流的正常放通，**非业务数据流的有效管控**；
- 通过弱口令检测功能，能及时发现终端应用的**潜在安全风险**；
- 通过虚拟补丁的安全防护能力，有效**提升**管控设备自身安全**防御能力**；
- 对内网的ARP、泛洪攻击具有**免疫能力；**
- 可实现管控设备流量异常预警，及时发现**异常流量风险。**

五、产业意义

- **产业数字化** 过程中，企业以网络为支撑，通过IT技术为产业赋能，对传统生产模式进行升级、转型和信息化再造，通过信息化打通产业链的上下游。因此必然面临信息化的安全问题。

- **数字产业化** 是通过数字技术带来的产品和服务，如电子信息业、信息通信业、软件服务业、互联网业等，如智能网联汽车、超高清视频、大数据、区块链等，同样也面临信息化安全问题。

守护产业数字化和数字产业化过程的安全保镖！

五、产业意义

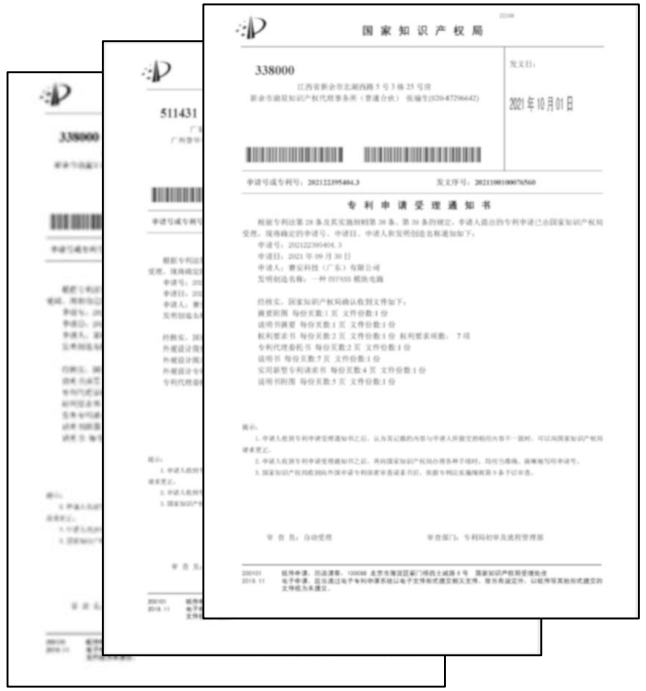
赛姆科技
SAM TECHNOLOGY

➢物联网

能够被独立寻址的普通物理对象通过互联网等网络实现物与物、物与人互联互通的泛在连接，以实现对物品的智能化识别、定位、跟踪、监控和管理的网络。

在万物互联中为“物”保驾护航！

六、信安通的专利和民参军认证



信安通专利受理证书

进入《2021年度广州市民参军技术与产品推荐目录》

销售许可证书

七、客户案例

某智能制造企业的MES产线台机运行多年，发现有多个安全漏洞，大批量感染病毒和木马，原有软件开发商无法提供安全技术支持。被感染的产线设备不仅影响了生产环境，还对外部网络发起攻击。

使用信安通一体化安全管控平台后，从源头上为产线台机提供了有效安全保护，实现了未感染设备不再被感染，已感染设备无法再攻击其他机器，产线业务很快恢复正常生产。

赛姆科技
SAM TECHNOLOGY

感谢您的关注

赛姆科技
微信公众号QR

赛姆商务

系统管理大师 · 专注数据安全

www.samgd.cn

电话：020-22123010 / 传真：转 616

7x24x365服务热线：400-889-3110

公司总部：广州市高新技术开发区科学城科研路3号自编A2栋203房

应急中心：广州市天河区珠江新城华夏路49号津滨腾越大厦南塔1503-1505