ISC 2019 第七届互联网安全大会

信息安全竞争趋势下的AI应用

王雨晨

工业互联网产业联盟安全组副主席

小鹅助理

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费

门票


ISC
信息安全竞争趋势下的AI应用
工业互联网产业联盟安全组副主席 王雨晨


ISC
目录
安全威胁发展趋势
安全危机原因分析
业界思考
解决方案与关键技术

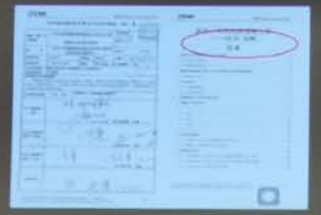

ISC
目录
安全威胁
安全危机
业界思考
解决方案
ISC
2019
第七届互联网安全大会
INTERNET SECURITY CONFERENCE 2019

威胁发展趋势：安全攻击事件背后的利益驱动

- 国家级攻击
- 有组织攻击
- 黑客攻击
- 灰色产业链
- ……

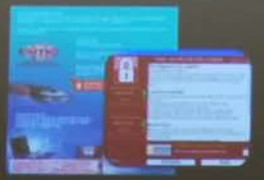
2010年伊朗震网

伊朗核计划被迫推迟2年，相当于一次外科手术打击！



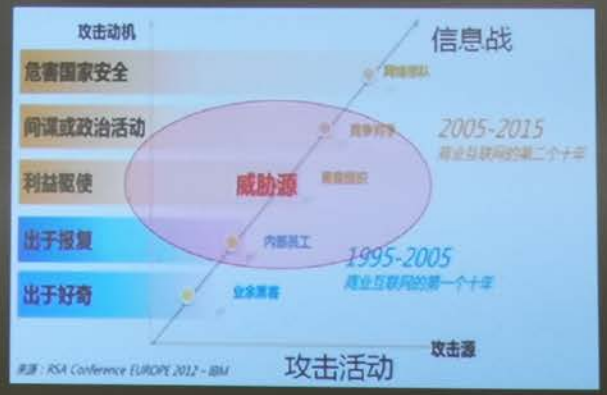
2016年：美国商务部制裁中兴

价值14亿美元！



2018年：台积电遭遇变种蠕虫

每小时损失约270万$；



- 攻击活动成为服务于利益的工具（个人、组织、经济、政治…）
- 系统所面临的风险强度，只由系统的价值决定，而与系统是否具备良好的防护无关；

原因及后果：全球对抗升级，网络安全形势严峻

"如果你控制了石油，你就控制住了所有国家；如果你控制了粮食，你就控制住了所有的人；如果你控制了货币，你就控制住了整个世界。"
——美国前国务卿 亨利·基辛格

人民网 people.cn 人民网 >> 国际

加紧备战 美国欲将全球拖入网络战争

史往生

2019年06月14日05:20 来源：人民网－人民日报

网络战成为大国博弈的重要手段

- 10年前，美国国家安全局（NSA）就开展了代号为"**狙击巨人**"的入侵行动，对华为总部网络实施了长达7年的攻击和监控；2013年，**明镜周刊披露NSA入侵华为网络设备;2019年美国接口5G安全问题制裁华为；**
- 未来大国间科技竞争是常态，网络战也会是长期和常态：允许相关部门对俄罗斯与伊朗发动网络攻击！
- 网络攻击的背后是黑客组织甚至是网络部队，网络战从网络空间向经济、社会、国防、外交等全域交织渗透。

加强网络战应对刻不容缓

- 转变防御思想，建立"敌人在内"的防御前提；
- 加快建立国家级的网络空间安全防护系统；
- 常态化、制度化开展现网攻防演练。

- 适用范围扩大：从政府主导投资的系统变为关键信息基础设施；
- 从自主定级变成第三方评定；
- 从强调产品能力，变成强调端到端的系统能力；
- 增加了"可信计算"——对抗NSA攻击的唯一有效手段！

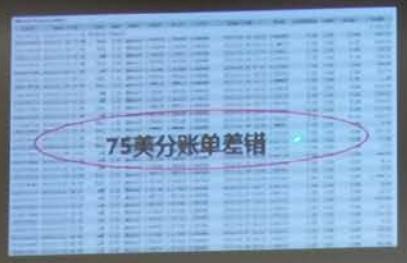
网络安全不仅仅影响到Cyber层面，而且已经实际影响到日常经济；

419讲话：没有网络安全就没有国家安全

网络安全是整体的而不是割裂的；是动态的而不是静态的，依靠几个安全设备和安全软件想永保安全的想法不合时宜...

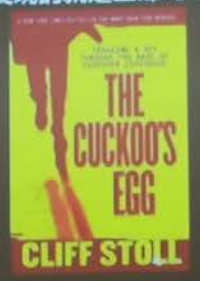
网络攻防的本质：是一种“系统性”的“对抗”

- 网络安全的历史沿革



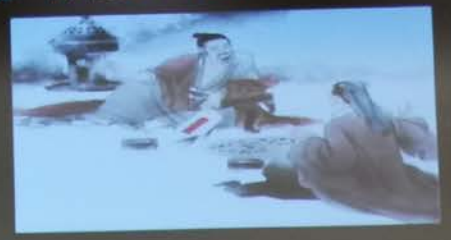
1980年代：LBL Clifford Stoll

发现的就是全部吗？



网络攻击是人与人之间的对抗！

- 网络安全是一种能力对抗…

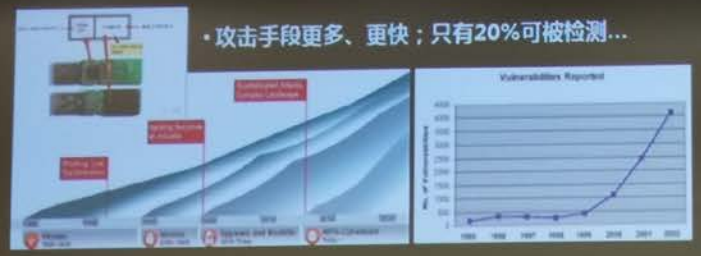


- 系统性：系统不是部件的堆叠；无法拆分比较

没有绝对的安全：威胁无穷而防御成本有限

——安全现状：能力和资源都不占优势的攻击者，可对具有全面优势的组织造成重大破坏...

•无法防御你所看不到的...

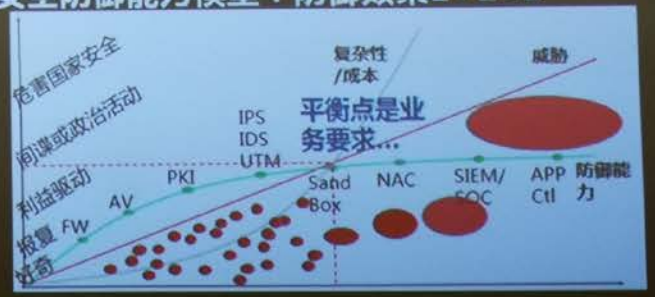


•二十年信息攻防间的成本变化

•APT攻击能力模型：攻击效果1+1>2

2015年乌克兰电网遭受APT攻击

•安全防御能力模型：防御效果1+1<2



对抗方法论决定了，当前安全防御一定无法成功

- 信息对抗的方法论：现代信息对抗理论源自美国90年代信息战，都基于包以德（OODA）对抗方法论
  - 通过Observe（观察）、Orient（调整）、Decide（决策）和Act（行动）实施对抗，谁更快谁占据优势——即：发现即摧毁！

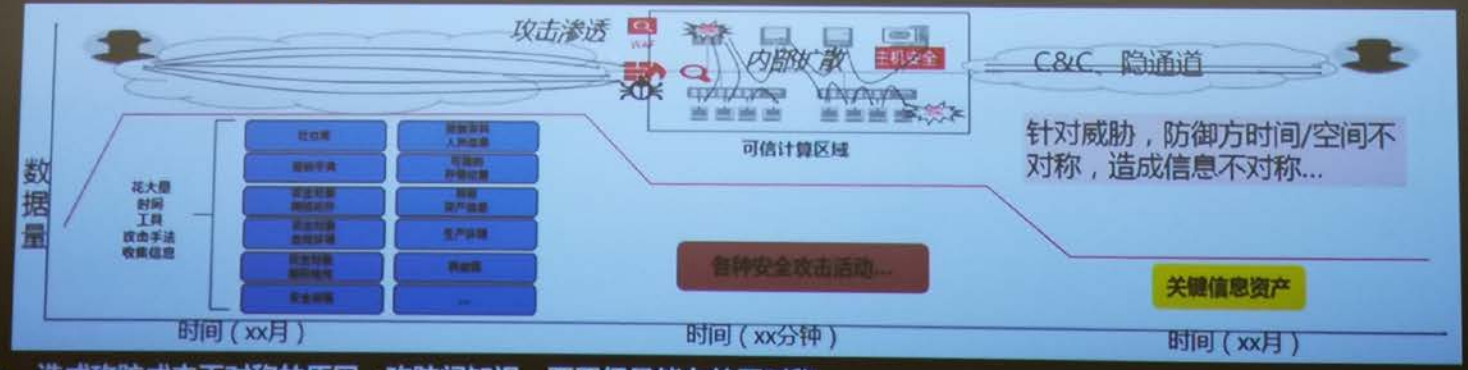



- 攻击链（洛克希德•马丁）：围绕漏洞的“发现即摧毁”；
- 因为攻防间信息的不对称，造成成本的不对称！

Reconnaissance 情报收集 → Weaponization 工具准备 → Delivery 载荷投递 → Exploitation 漏洞利用 → Installation 释放载荷 → Command and Control (C2) 建立通道 → Actions on Objectives 目标达成

攻击还未发生/计划　　攻击正在发生/执行　　攻击已经发生/破坏

- 防御环：发现威胁（攻击/脆弱性）消除威胁；



- 造成攻防成本不对称的原因：攻防间知识，而不仅是能力的不对称...

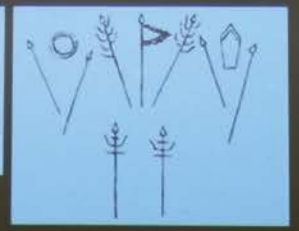
启发：与其对抗攻击，不如建立易守难攻的环境

- 安全防御思路：建立安全体系，降低防御成本，提升攻击成本！

两千年前的《孙子兵法》揭示了对抗的艺术...

- 上兵伐谋，其次伐交，其次伐攻...
- 是故百战百胜，非善之善者也；不战而屈人之兵，善之善者也
- 能而示之不能，用而示之不用，近而示之远，远而示之近...

为什么“鸳鸯阵”可以获得冷兵器时代最悬殊的战损比？

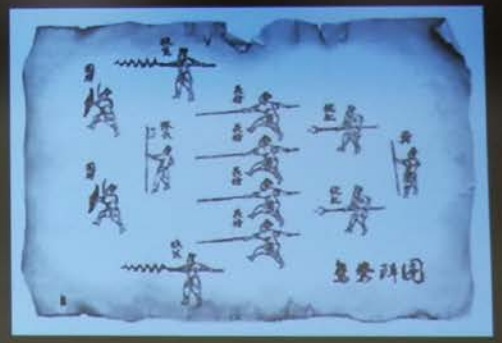


花街之战：336比3

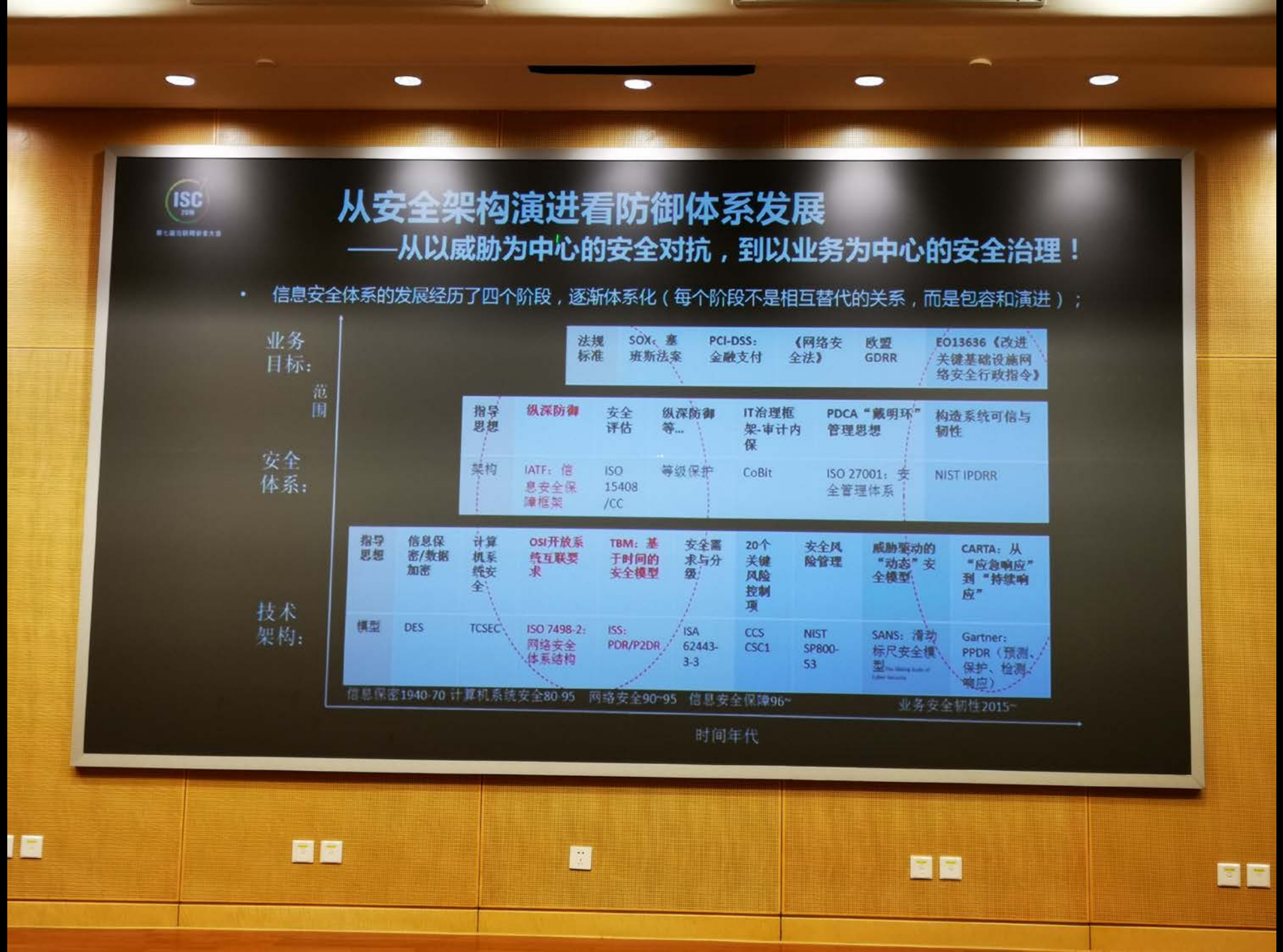
——安全的目标不是消灭威胁，而是保障业务！

——陷入对抗，已经输了一半！

—— 建立能使攻防成本保持平衡的信息治理体系，比击败每一个威胁更为重要！



局部的不对称，不等于系统间的不对称！


从安全架构演进看防御体系发展
——从以威胁为中心的安全对抗，到以业务为中心的安全治理！
• 信息安全体系的发展经历了四个阶段，逐渐体系化（每个阶段不是相互替代的关系，而是包容和演进）；
业务目标：
范围
安全体系：
技术架构：
法规标准
SOX：塞班斯法案
PCI-DSS：金融支付
《网络安全法》
欧盟GDRR
EO13636《改进关键基础设施网络安全行政指令》
指导思想
纵深防御
安全评估
纵深防御等...
IT治理框架-审计内保
PDCA“戴明环”管理思想
构造系统可信与韧性
架构
IATF：信息安全保障框架
ISO 15408/CC
等级保护
CoBit
ISO 27001：安全管理体系
NIST IPDRR
指导思想
信息保密/数据加密
计算机系统安全
OSI开放系统互联要求
TBM：基于时间的安全模型
安全需求与分级
20个关键风险控制项
安全风险管理
威胁驱动的“动态”安全模型
CARTA：从“应急响应”到“持续响应”
模型
DES
TCSEC
ISO 7498-2：网络安全体系结构
ISS：PDR/P2DR
ISA 62443-3-3
CCS CSC1
NIST SP800-53
SANS：滑动标尺安全模型
Gartner：PPDR（预测、保护、检测、响应）
信息保密1940-70 计算机系统安全80-95 网络安全90~95 信息安全保障96~
业务安全韧性2015~
时间年代

海外实践：DHS/DOD安全韧性与NIST IPDRR

1. 2007年美国DHS发布“National Strategy for Homeland Security”白皮书，首次指出面对不确定性的挑战，需要保证国家基础设施的韧性。
2. 2010年美国NSS（国家安全战略）首次将**国家韧性**列为首要目标；
3. 2017年3月DHS发布**《网络韧性白皮书》**

国防部指令与行动计划：
- 2018年，**多域战**：THE U.S. ARMY CONCEPT FOR CYBERSPACE AND ELECTRONIC WARFAREOPERATIONS
- **落地NIST SP800等风险治理规范**

- **NIST IPDRR定义一组持续闭环，不断改进的标准流程，帮助组织实现风险管理，指导用户达到安全韧性目标！**

NIST

- **安全的角色：引导 业务实现风险管理！**

定义流程方法，使用SP800-53，ISO27001等标准的基线能力！

Identify	Protect	Detect	Respond	Recover
确定安全目标和管理策略 • 定义风险 • 明确风险 • 供应链管理	**根据业务模型，制定保护策略** • 定保护对象 • 定保护流程 • 定保护技术	**根据P阶段的策略，检测行为（而非攻击），识别事件** • 异常和事件 • 安全连续监控 • 检测流程	**针对检测结果按预定策略执行响应** • 响应规划、沟通 • 分析 • 缓解、提升	**管理层面，恢复业务，消除影响** • 恢复计划 • 提升 • 沟通
安全咨询规划服务	P，设定行为策略；D，检测违规行为；R，恢复安全策略，恢复业务			运维、管理服务

总结：安全韧性系统是指，系统在某些安全约定不存在（如：威胁无法被消灭、漏洞无法被修复、部分安全功能失效）时，继续保证达成业务安全目标（机密性、完整性、可用性）的能力！

如何构造系统化的安全风险治理体系？

- 安全系统的构成：静态安全能力的组合+动态的安全业务流程
- 安全系统的价值：通过系统化方法，降低安全保障成本，提升攻击成本（系统安全防御能力：1+1>2）

- 安全业务需求

- 安全业务目标：在威胁环境下，保证系统内所有实体行为可预期！
- 威胁：破坏安全目标的潜在原因！

- 安全模型：纵深防御+信任体系+动态安全自适应

- 不但要看到棋子，还要感知棋局...

APT攻击源

攻击链/纵深防御

纵深防御

- “棋子级别”的安全威胁对抗！

关联分析/协同防御

安全自适应

- “棋局级别”态势感知与业务恢复！

业务安全设计

信任模型

- “预设棋局”建立有利防御的业务环境！

- *指挥调度！*

安全自适应

- *保护好人！*

信任模型

- *消灭坏人！*

纵深防御

为什么AI是构造安全体系的必要技术？

- 安全体系要实现1+1>2；
- 关键在于安全知识的积累与有效应用：

1、漏洞必然被利用

3、安全的价值，在于成本

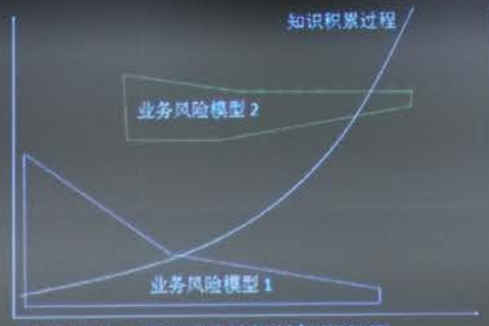
5、大数据改变了安全知识认知的方式

2、安全要提供知识与防护手段。

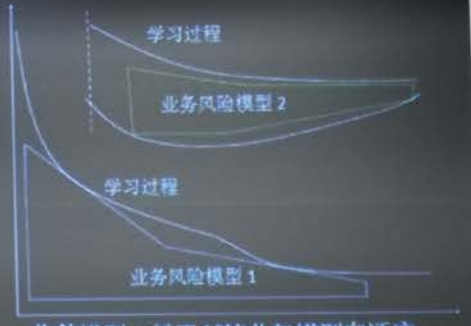
4、安全核心是构建安全知识系统。

6、未来（AI）...

- 威胁情报无法解决问题：积累数据量会随时间扩散，有效情报只占很小部分；
- AI算法：知识积累向风险模型收敛，自适应用户业务；



发散模型：基于威胁情报的知识积累

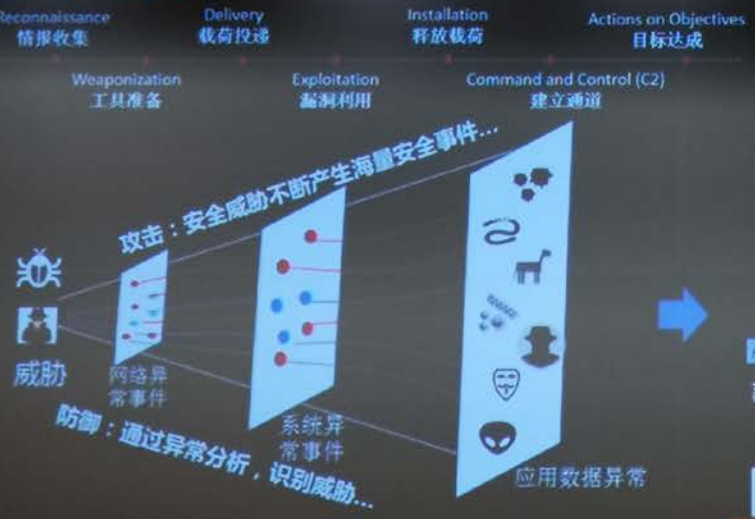


收敛模型：基于AI的业务模型自适应

- AI的价值并不是识别攻击或者攻击分类，而在于有效降低安全系统对安全知识的积累与高效使用成本。

功能要求：快速准确“预防、消减、处置”安全事故

· 安全攻击与防御模型



- **威胁**：ISO 27005：可能导致系统和组织的损害事故的潜在原因。
- **攻击**：试图收集、破坏、拒绝、降级或破坏信息系统资源或信息本身的任何恶意活动。（攻击活动相当于战斗，APT攻击相当于战役）
- **异常/恶意事件/事故**：攻击活动对系统的影响，攻击导致的后果。
- **风险**：出现损失、伤害或其他不利情况的可能性。

· 安全解决方案架构

- 当前能被看到的，是**异常事件**，而非**威胁本身**！
- **核心诉求：是从海量异常中定位威胁并自动化处置！**

基于AI的“纵深防御”：从特征检测→行为感知

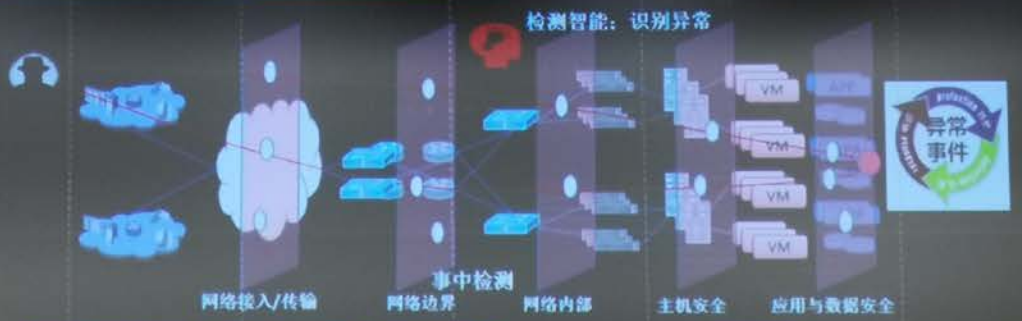
情报收集 | 工具准备 | 载荷投递 | 漏洞利用 | 释放载荷 | 建立通道 | 目标达成

攻击还未发生/计划 | 攻击正在发生/执行 | 纵深防御 | 攻击已经发生/破坏

安全木桶原理

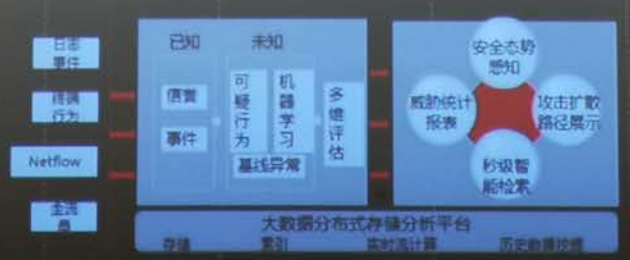
- 单点技术不可能100%有效；
- 系统本身会存在漏洞；
- 多层冗余，互为补充；
- P.D.R闭环，应急响应；

- 异构价值：避免同源漏洞风险（熔断）
- 多层防御不等于多产品异构



第三代沙箱技术：基于行为的未知恶意代码检测

网络异常行为检测：C&C、隐蔽通道、加密流量检测



- AI能力要求
  - 全面的数据源；
  - 人工智能分析算法
  - 基于AI芯片的算力

基于意图识别的网络诱捕：从被动检测→主动防御

情报收集 | 工具准备 | 载荷投递 | 漏洞利用 | 释放载荷 | 建立通道 | 目标达成

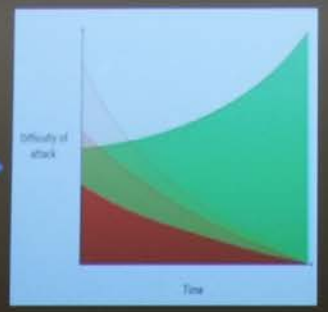
防御在攻击之前 | 攻击正在发生/执行 | 攻击已经发生/破坏

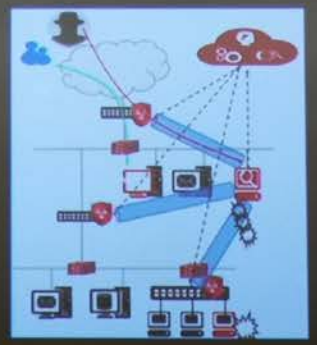
问题：防御滞后于攻击

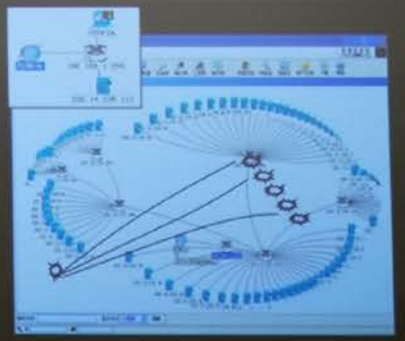
- 基于特征的检测（认识所有的狼）；
- 基于行为的检测（监控所有吃羊的行为）

对策：基于攻击意图的防御
（设置诱饵陷阱捕狼）

攻击者的优势：不确定的攻击活动VS确定的目标





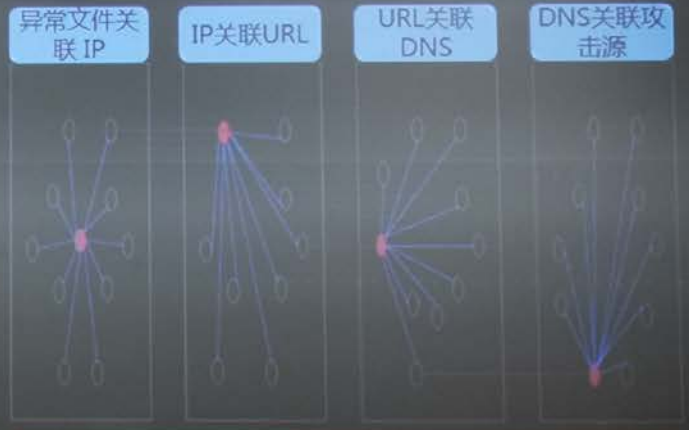


诱捕技术，诱使攻击者活动，在破坏发生前实现检测！提供虚假信息，增大攻击难度！

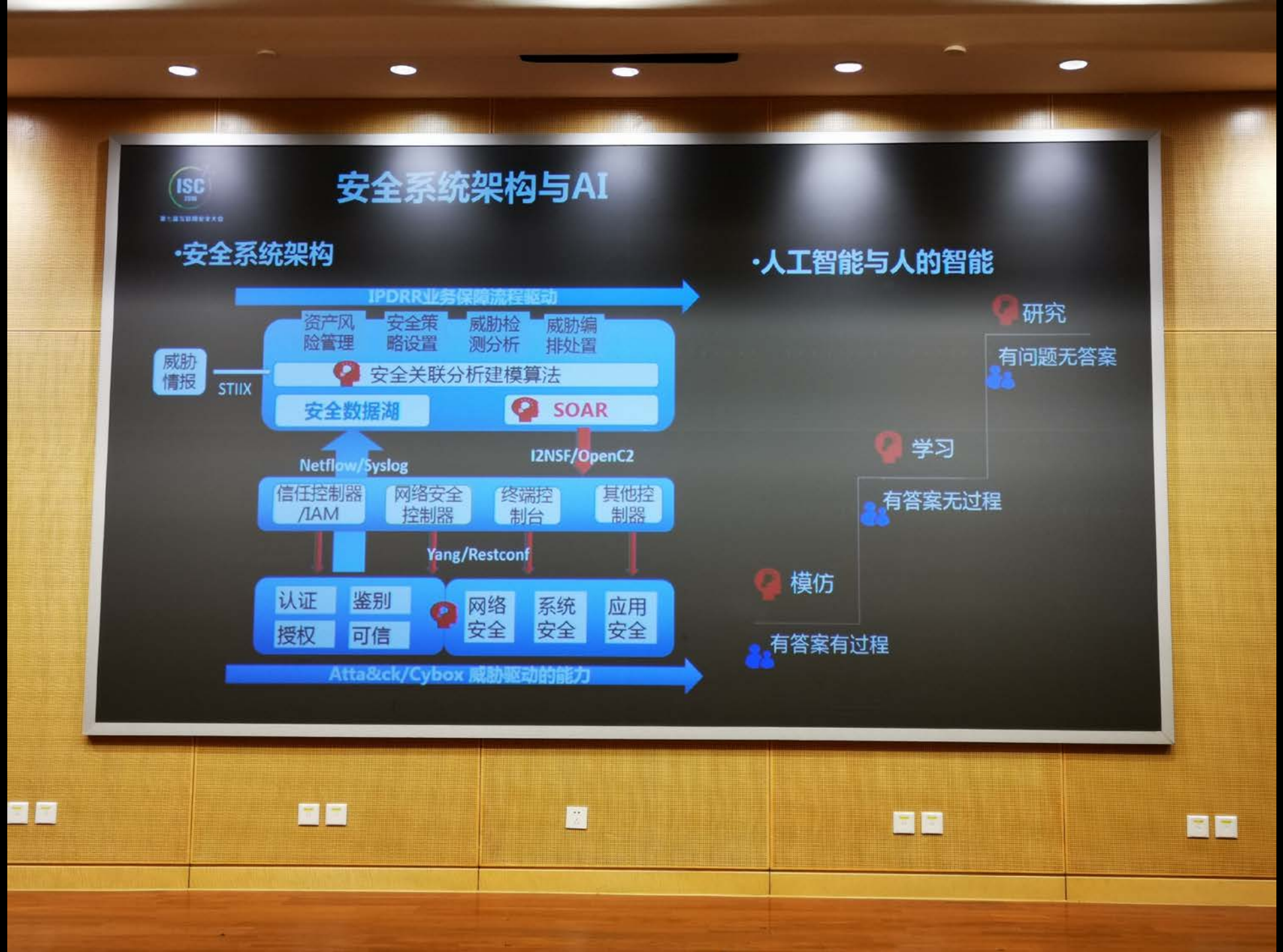
基于AI的威胁判定：从单点异常检测→协同威胁处置

情报收集 工具准备 载荷投递 漏洞利用 释放载荷 建立通道 目标达成

攻击日志与流量关联分析、协同处置



通过多因素关联，挖掘基于攻击链的APT攻击活动，完整展现APT攻击事件


安全系统架构与AI
·安全系统架构
IPDRR业务保障流程驱动
资产风险管理
安全策略设置
威胁检测分析
威胁编排处置
威胁情报
STIIX
安全关联分析建模算法
安全数据湖
SOAR
Netflow/Syslog
I2NSF/OpenC2
信任控制器/IAM
网络安全控制器
终端控制台
其他控制器
Yang/Restconf
认证
鉴别
授权
可信
网络安全
系统安全
应用安全
Atta&ck/Cybox 威胁驱动的能力
·人工智能与人的智能
研究
有问题无答案
学习
有答案无过程
模仿
有答案有过程

- 王雨晨，清华大学毕业，20余年安全领域从业经验。曾任多项国家级安全预研和型号项目负责人，设计实现了中国最早的网络入侵检测、防御性信息欺骗、计算机系统安全控制器等项目，成果曾被鉴定为“国际领先水平”。
- 曾获国家科技二等奖等多项奖励。
- 当前研究方向为信息安全、SDN与云安全、IPv6、5G Slice、工业互联网安全等。
- 拥有安全专利30余项，IEEE等专业论文多篇，在多个安全标准组织内任职。

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票