ISC 2019 第七届互联网安全大会

模型和算法在自动化攻击模拟中的应用

董靖

思睿嘉得创始人

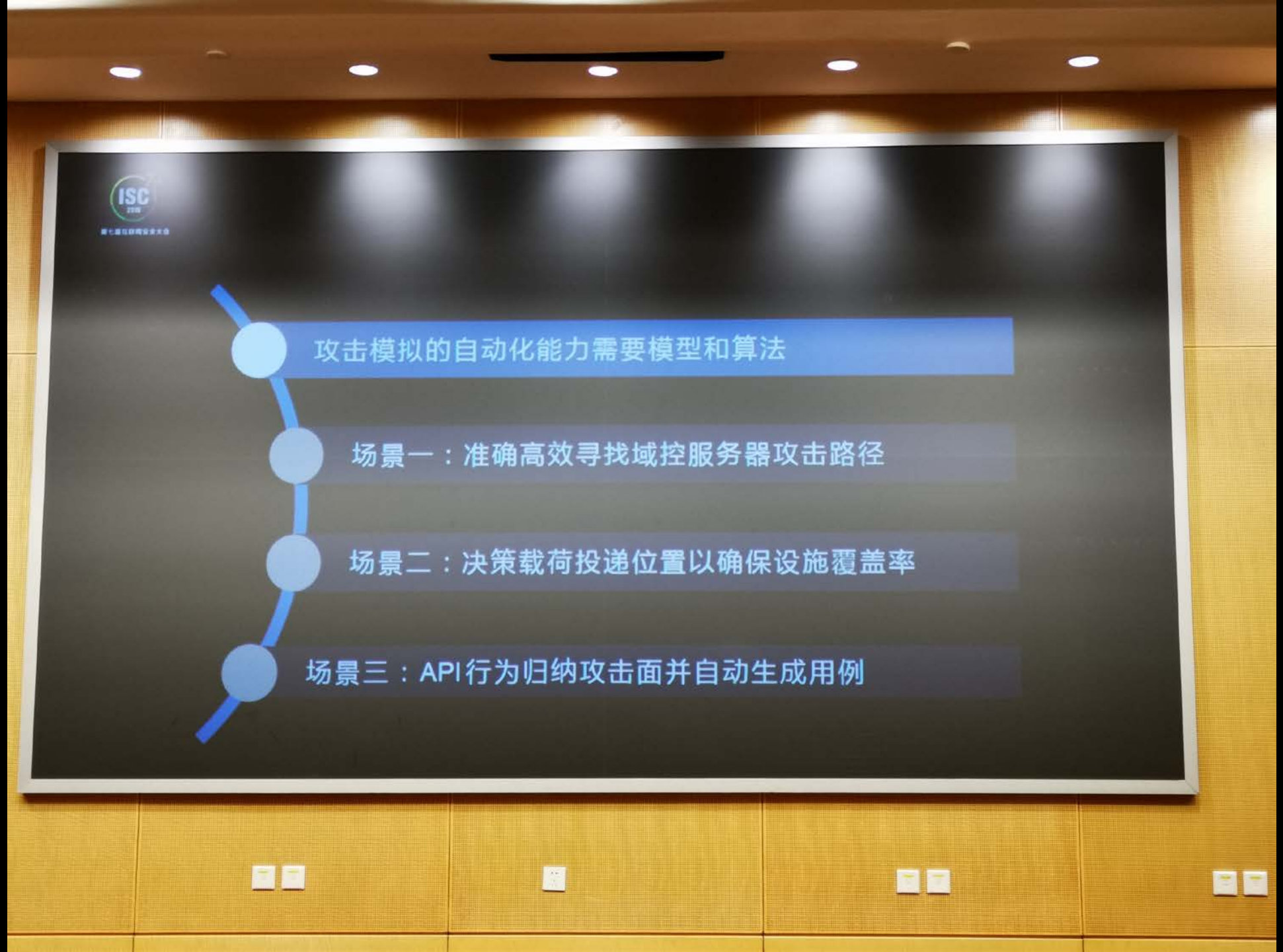
小鹅助理

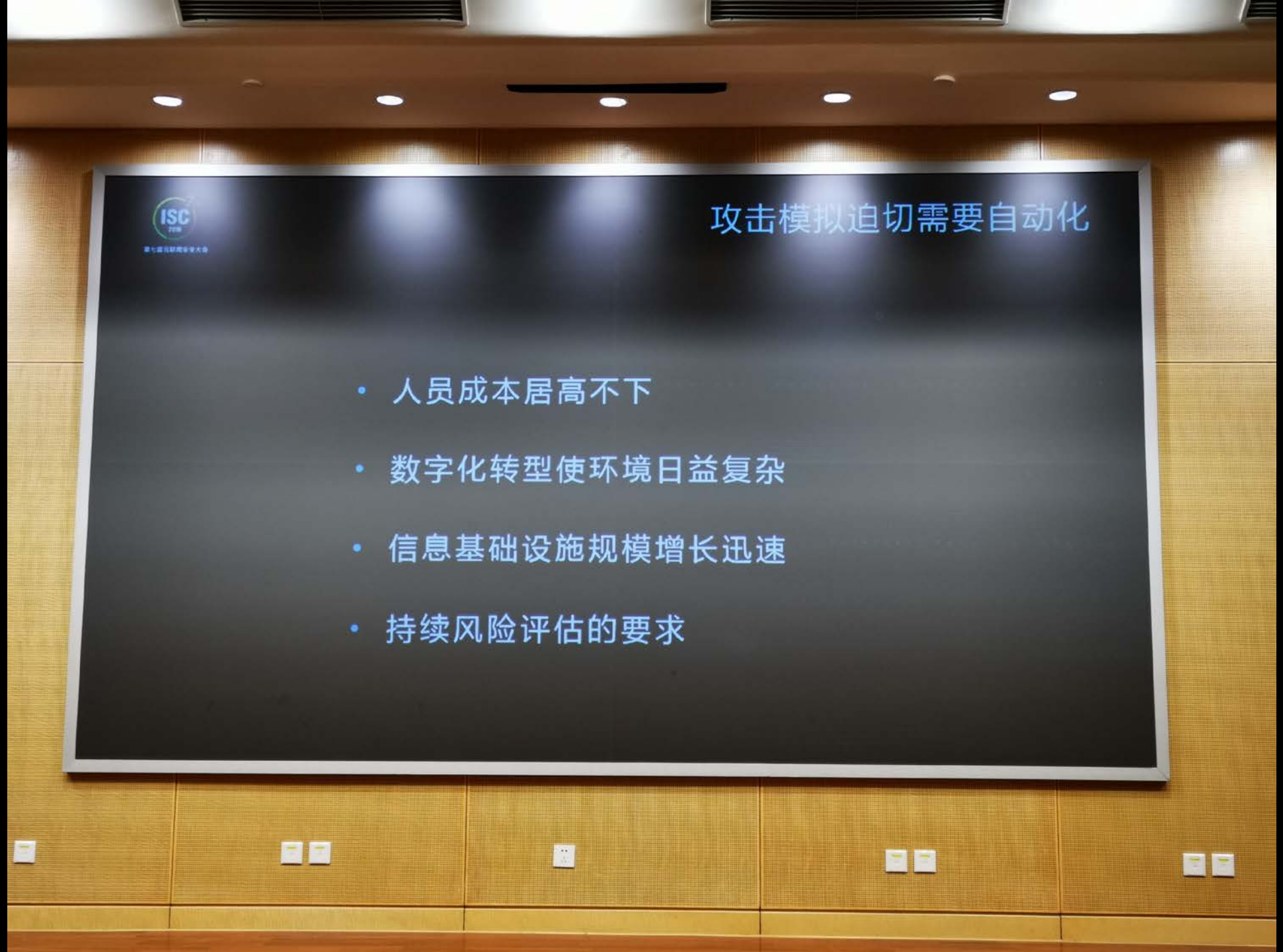
扫码添加小鹅助理，与数万科技圈人士

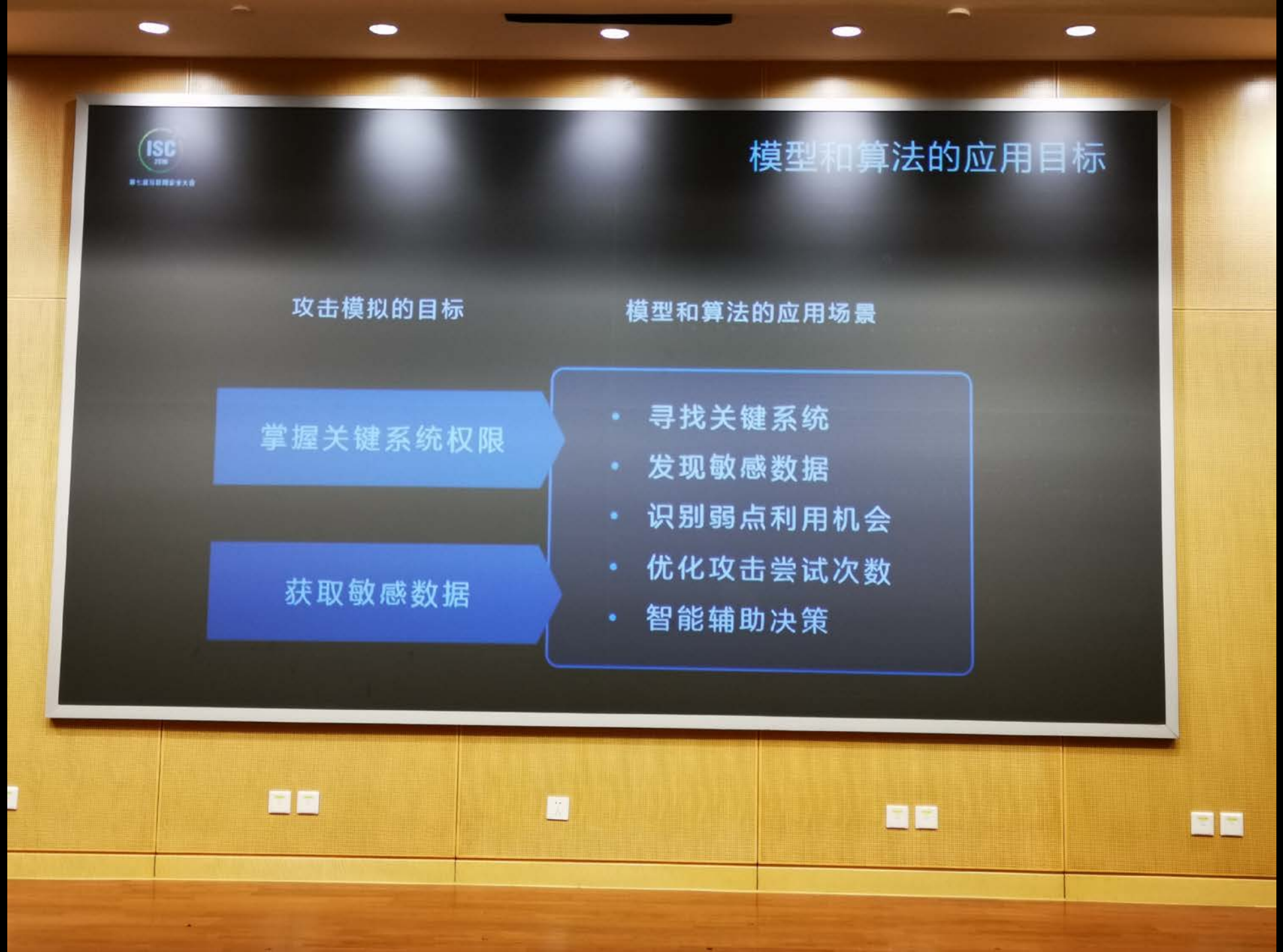
分享重量级活动PPT、干货培训课程、高端会议免费

门票


ISC
模型和算法在自动化攻击模拟中的应用
董靖
思睿嘉得

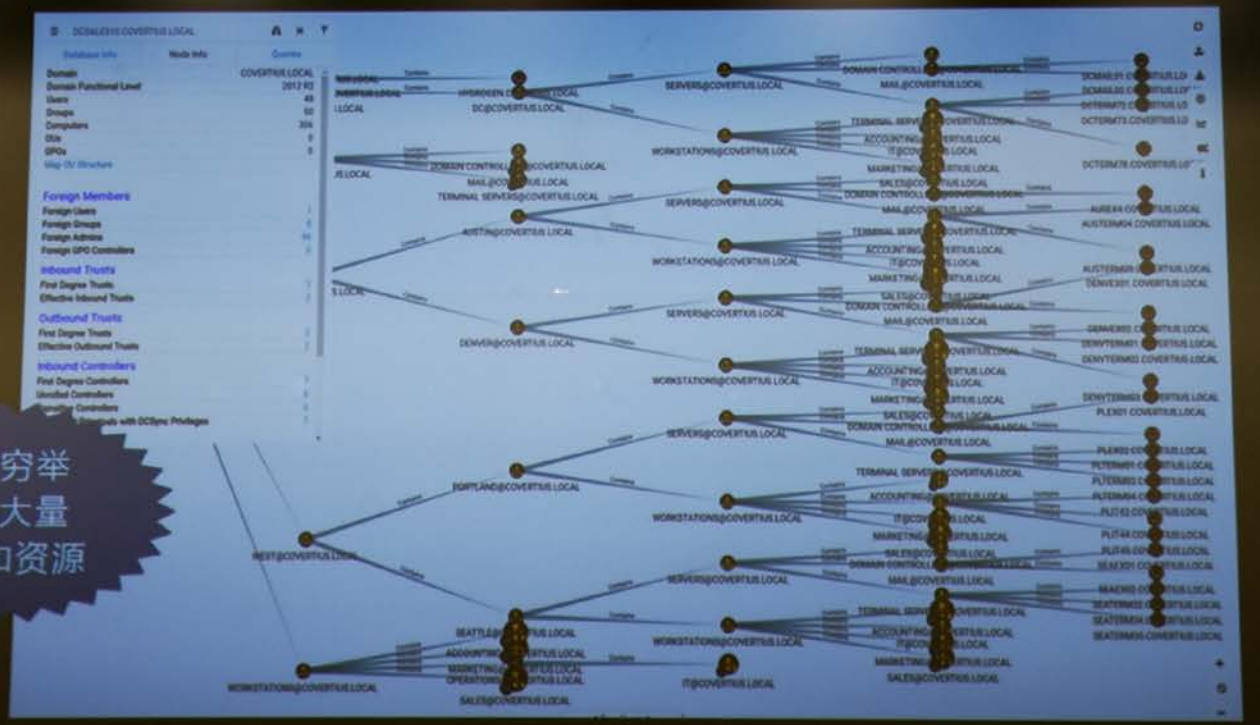

攻击模拟的自动化能力需要模型和算法
场景一：准确高效寻找域控服务器攻击路径
场景二：决策载荷投递位置以确保设施覆盖率
场景三：API行为归纳攻击面并自动生成用例

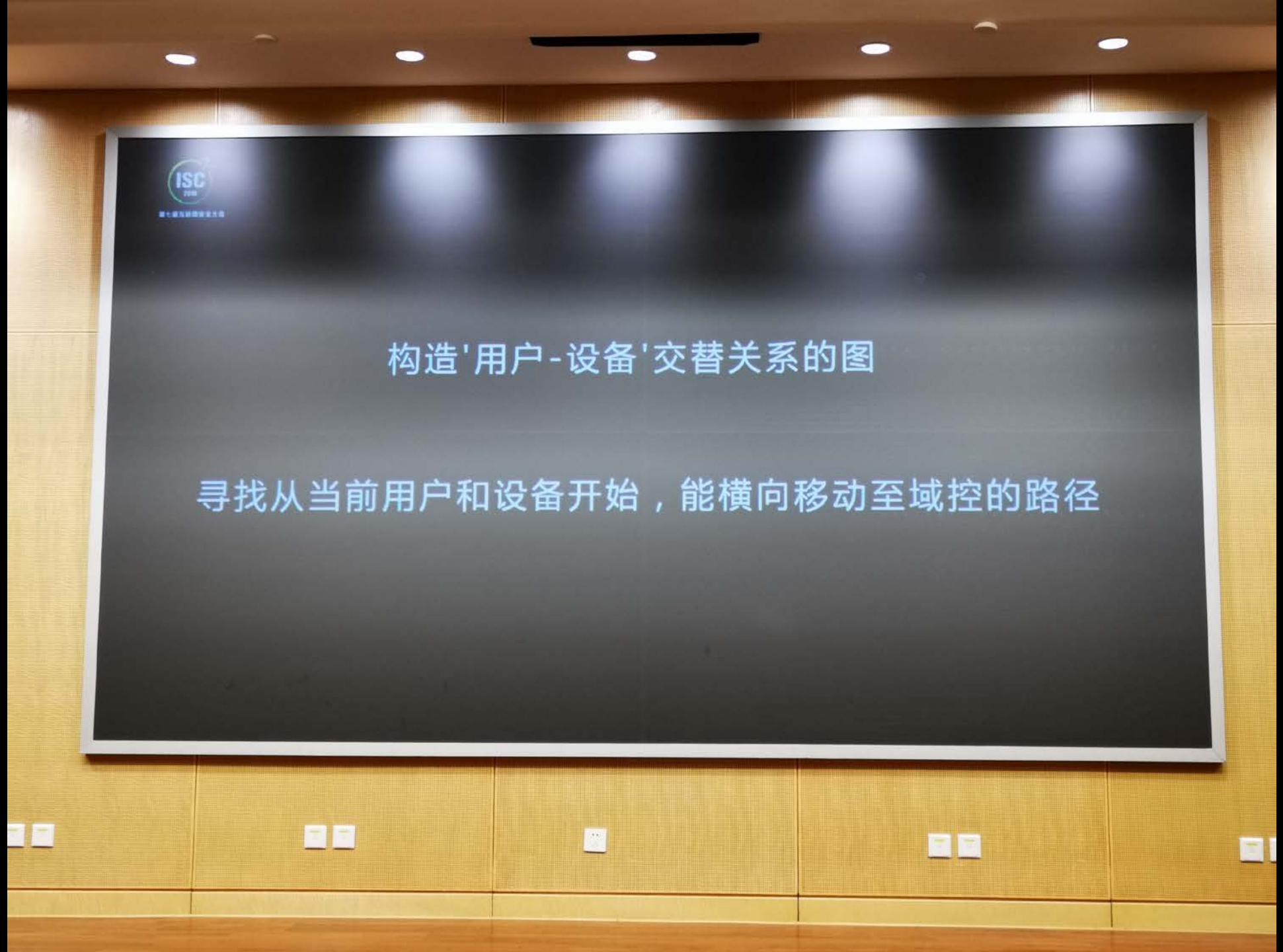

ISC
攻击模拟迫切需要自动化
人员成本居高不下
数字化转型使环境日益复杂
信息基础设施规模增长迅速
持续风险评估的要求

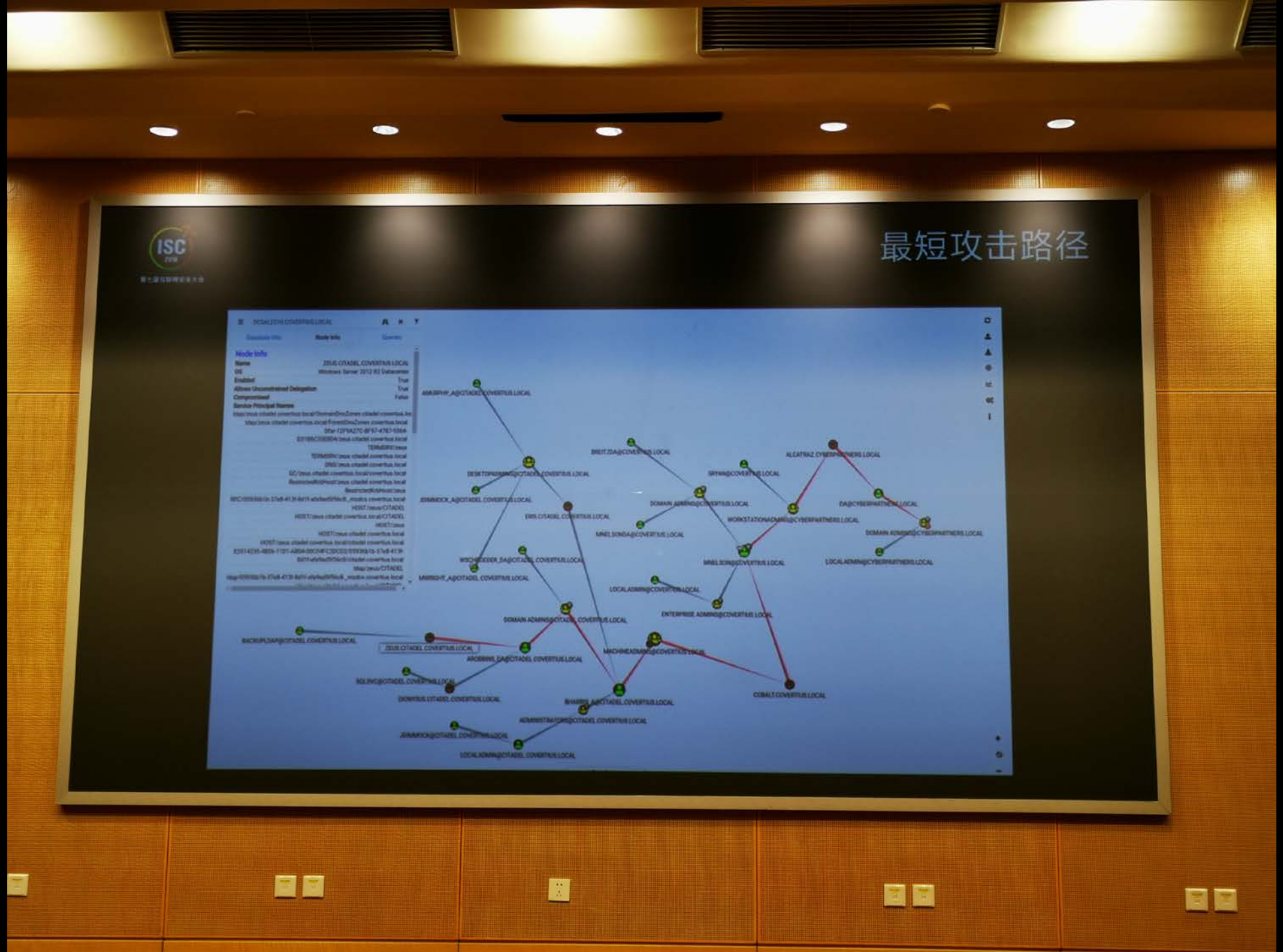

ISC
模型和算法的应用目标
攻击模拟的目标
模型和算法的应用场景
掌握关键系统权限
获取敏感数据
寻找关键系统
发现敏感数据
识别弱点利用机会
优化攻击尝试次数
智能辅助决策

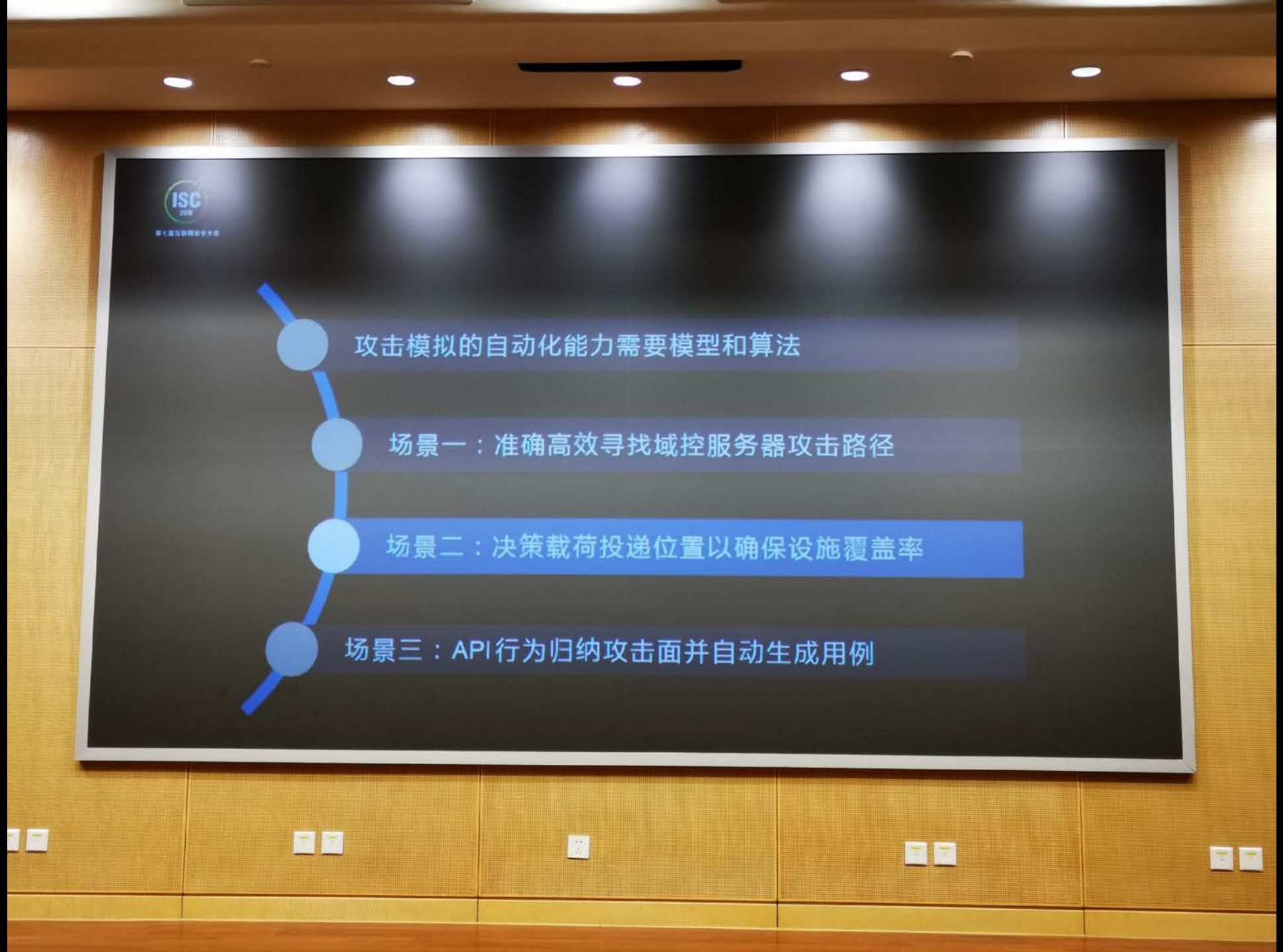

真实场景需求
针对微软AD域环境的横向移动手法
User A
PC X
User B
PC Y
Admin
Domain Controller

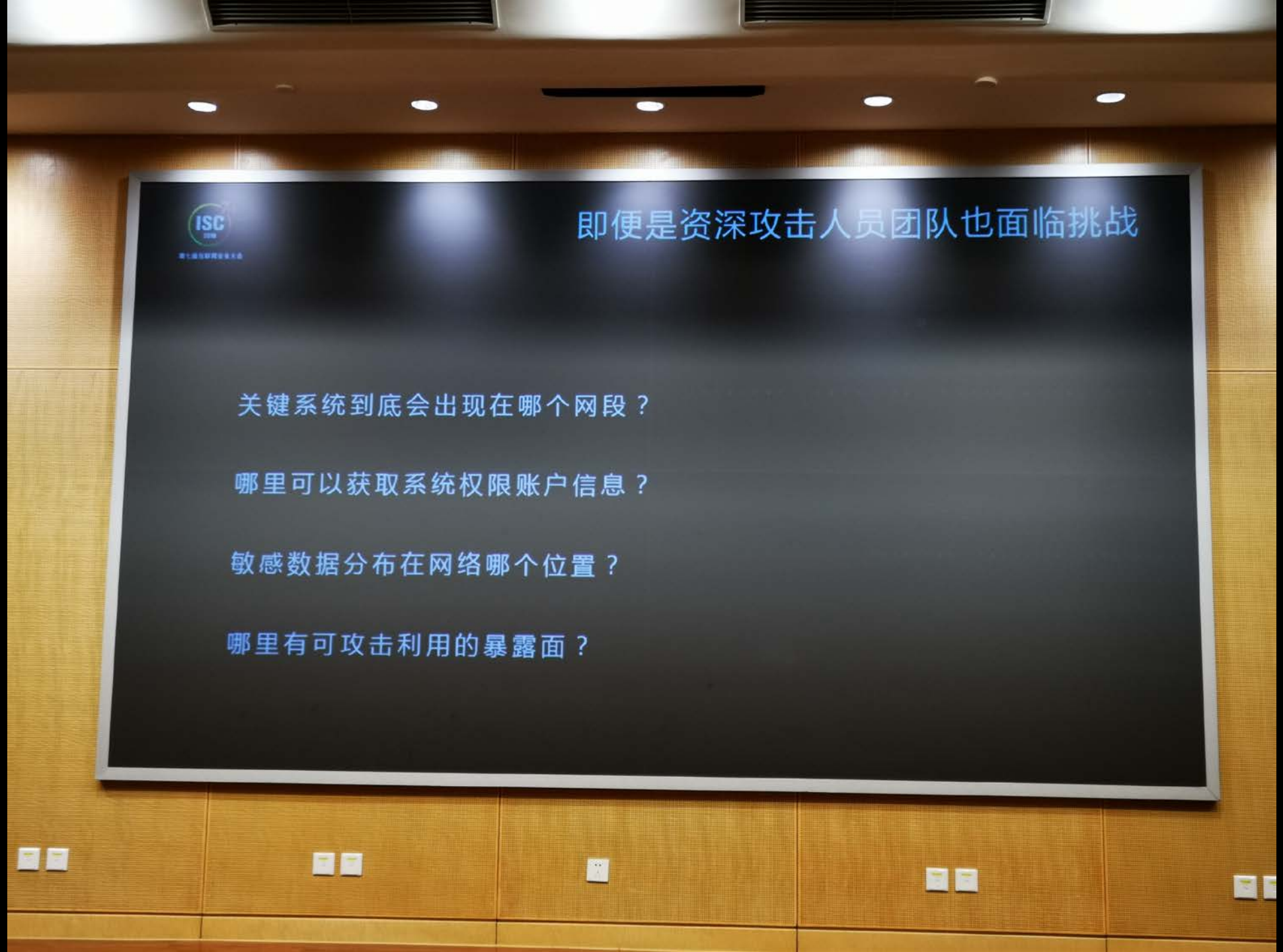
复杂的域、账号、和设备的关系




构造'用户-设备'交替关系的图
寻找从当前用户和设备开始，能横向移动至域控的路径


最短攻击路径
Node Info
Name
OS
Enabled
Allows Unconstrained Delegation
Compromised
Service Principal Names
ZEUS.CITADEL.COVERTIUS.LOCAL
Windows Server 2012 R2 Datacenter
True
True
False
ZEUS.CITADEL.COVERTIUS.LOCAL
BRETT.DA@COVERTIUS.LOCAL
ALCATRAZ.CYBERPARTNERS.LOCAL
SRYAN@COVERTIUS.LOCAL
DOMAIN ADMINS@CITADEL.COVERTIUS.LOCAL
DA@CYBERPARTNERS.LOCAL
WORKSTATIONADMINS@CYBERPARTNERS.LOCAL
DOMAIN ADMINS@CYBERPARTNERS.LOCAL
MNELSON@COVERTIUS.LOCAL
MNELSON@CITADEL.COVERTIUS.LOCAL
LOCALADMIN@CYBERPARTNERS.LOCAL
LOCALADMIN@COVERTIUS.LOCAL
ENTERPRISE ADMINS@COVERTIUS.LOCAL
DOMAIN ADMINS@CITADEL.COVERTIUS.LOCAL
ZEUS.CITADEL.COVERTIUS.LOCAL
MACHINEADMINS@COVERTIUS.LOCAL
COBALT.COVERTIUS.LOCAL
ADMINISTRATORS@CITADEL.COVERTIUS.LOCAL
LOCALADMIN@CITADEL.COVERTIUS.LOCAL


攻击模拟的自动化能力需要模型和算法
场景一：准确高效寻找域控服务器攻击路径
场景二：决策载荷投递位置以确保设施覆盖率
场景三：API行为归纳攻击面并自动生成用例

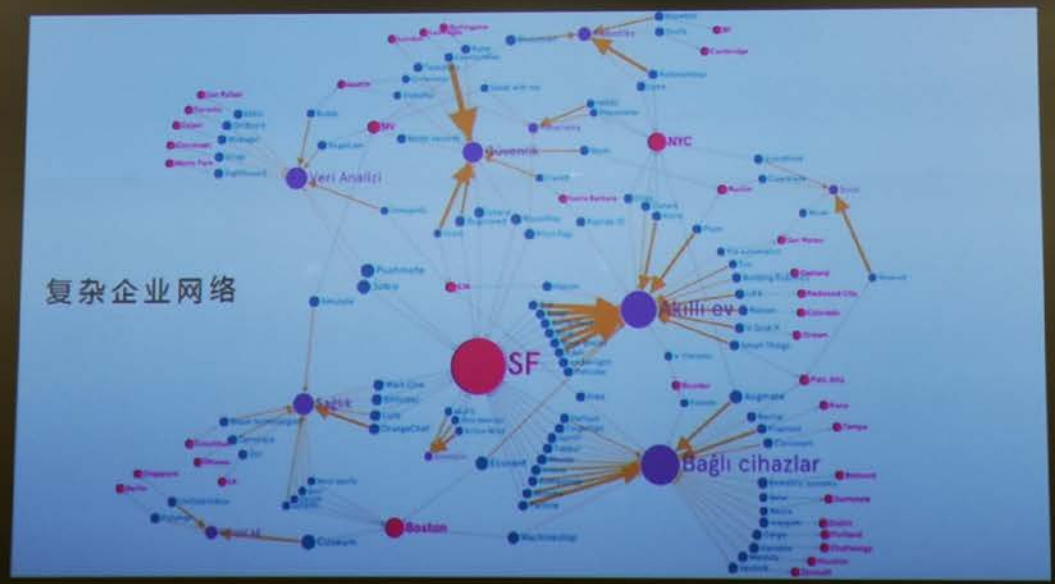

ISC
即便是资深攻击人员团队也面临挑战
关键系统到底会出现在哪个网段？
哪里可以获取系统权限账户信息？
敏感数据分布在网络哪个位置？
哪里有可攻击利用的暴露面？


即便是资深攻击人员团队也面临挑战
关键系统到底会出现在哪个网段？
哪里可以获取系统权限账户信息？
敏感数据分布在网络哪个位置？
哪里有可攻击利用的暴露面？
覆盖率是发现
弱点利用机会
的先决条件

ISC

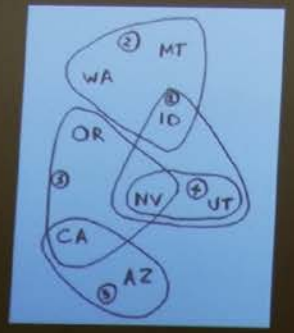
真实场景需求

如何确保攻击测试充分覆盖？

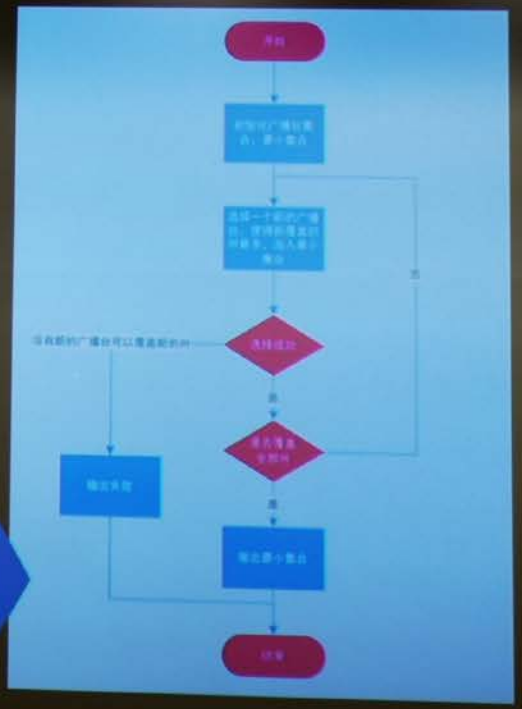


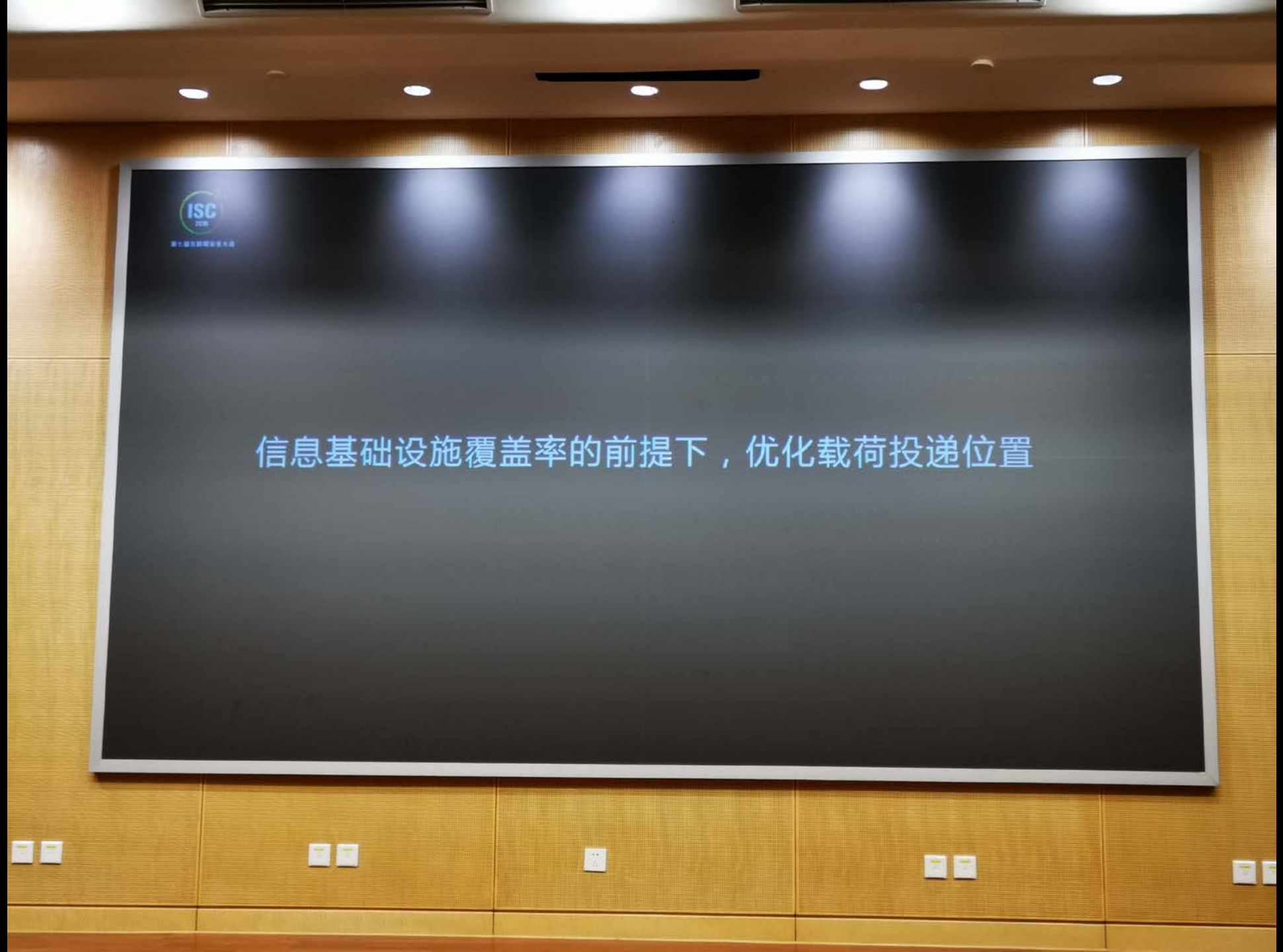
集合覆盖问题

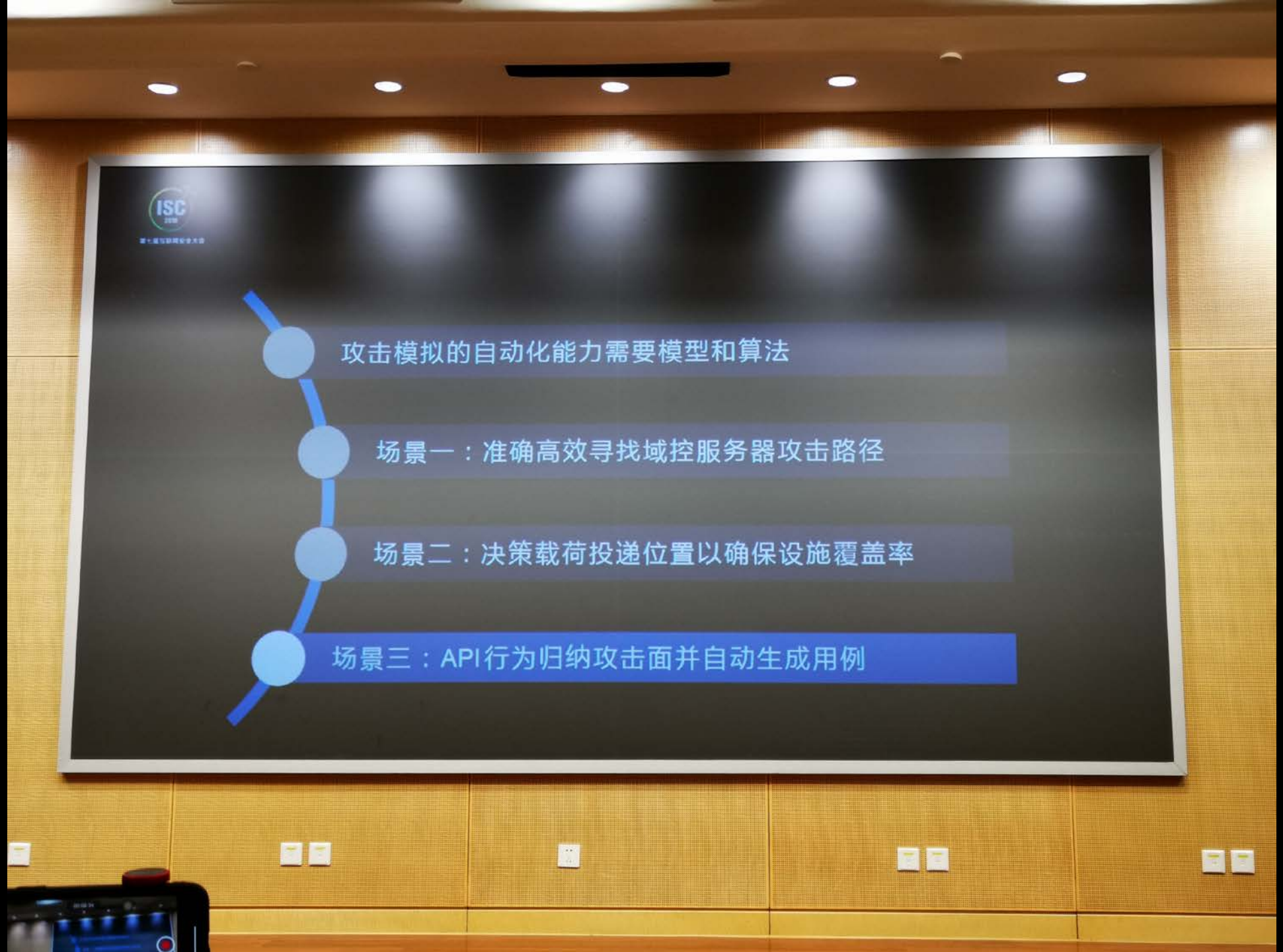
一个电视节目计划在美国全国上映。每个电视台覆盖范围都不同，还可能有重复覆盖的区域。选出覆盖全美50个州的最小电视台集合。



贪心算法




ISC
信息基础设施覆盖率的前提下，优化载荷投递位置

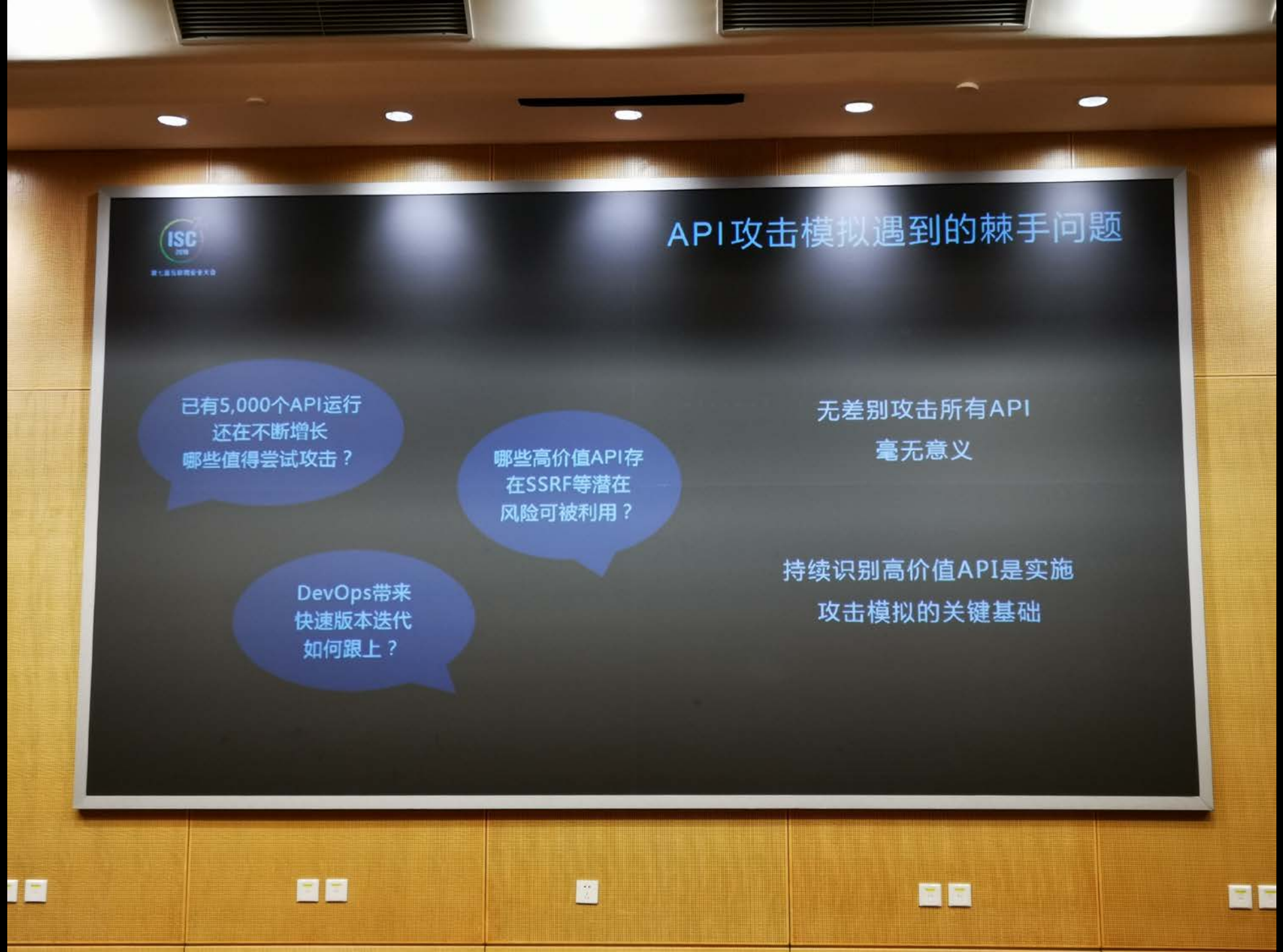

攻击模拟的自动化能力需要模型和算法
场景一：准确高效寻找域控服务器攻击路径
场景二：决策载荷投递位置以确保设施覆盖率
场景三：API行为归纳攻击面并自动生成用例


数字化转型带来新攻击面的产生
数据
中台
边缘
计算
API
微服务
供应链
数据交换
人工
智能


ISC
真实攻击案例
Pay
设计安全并被广泛使用的第三方API
https://cn-apple-pay-gateway-sh-pod3.apple.com/paymentSession
己方程序员错误可导致SSRF攻击泄露数据

真实攻击案例

供应链账号被滥用或盗取，非法下载大量数据


ISC
API攻击模拟遇到的棘手问题
已有5,000个API运行
还在不断增长
哪些值得尝试攻击？
哪些高价值API存
在SSRF等潜在
风险可被利用？
DevOps带来
快速版本迭代
如何跟上？
无差别攻击所有API
毫无意义
持续识别高价值API是实施
攻击模拟的关键基础

根据机器学习行为基线模型设计攻击方案

真实用户场景：从业务系统下载关键数据表单

恶意员工甲（某周六）

恶意员工乙（某周四）

针对每个API计算两条行为基线：同部门和个人

* 脱敏后的数据可视化，未包括API信息和用户信息

模拟登录地理位置改变和跳目标等隐蔽攻击行为

真实用户场景：供应商获取订单数据

用户访问API所在地快速位移

从不同API网关进行访问

* 脱敏后的数据可视化，未包括API信息和用户信息


ISC
cirrus gate
思睿嘉得

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