

# 黑客游乐场—云技术带来的教育变革

永信至诚 张凯

# 自我介绍

- 大四时分析导致蓝屏的局域网病毒，开启了我的信息安全之路。
- 毕业后在启明星辰ADLab、中国移动研究院、中国电力科学研究所和永信至诚从事信息安全研究和开发工作近14年，算是安全行业的一名老兵了。
- 2013年，组建i春秋学院和e春秋信息安全实验室团队，专注于信息安全人才实践和竞赛平台的研发和运营。

微博

<http://weibo.com/9x2u>



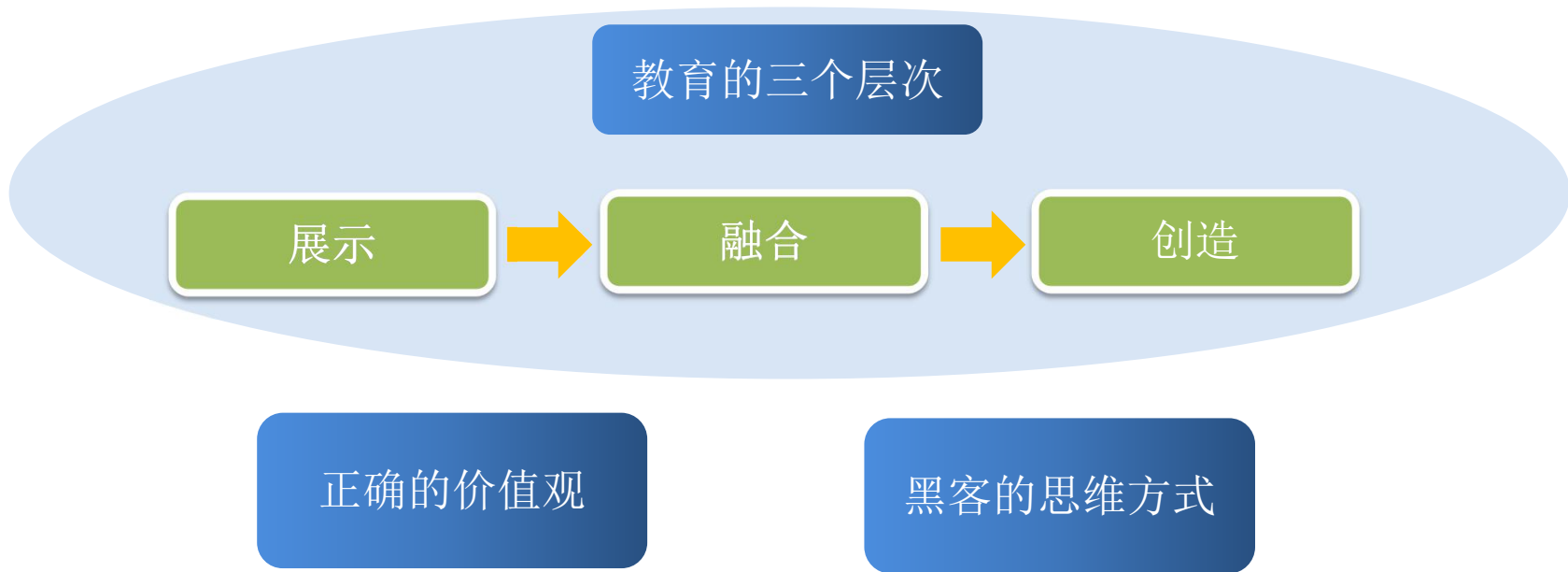
微信

wx\_9x2u



# 安全和教育的演变

# 教育的变革



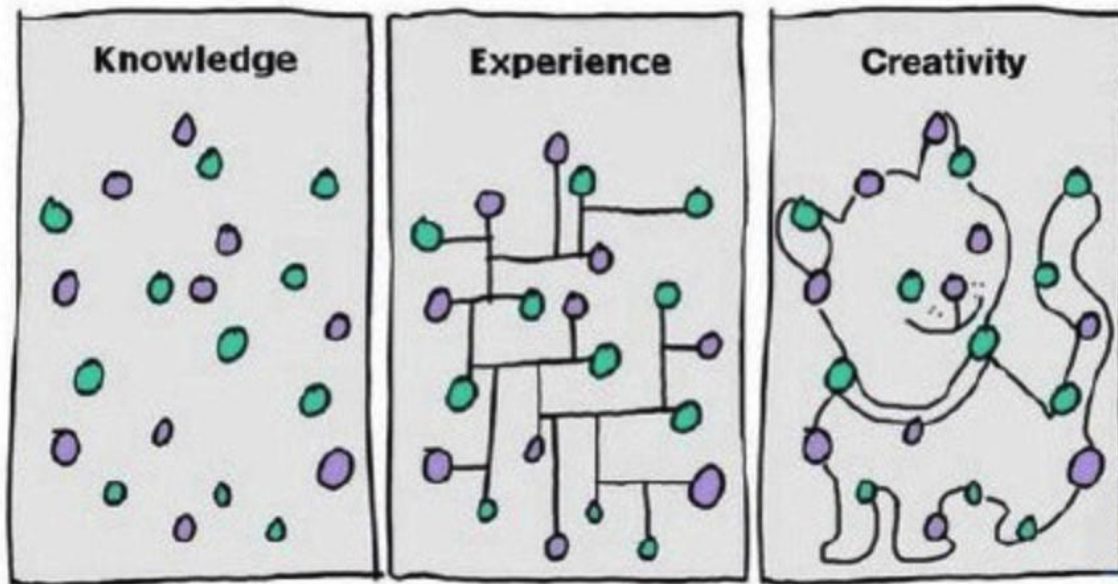
- 教育的目标不仅是传授知识，更重要的是培养正确的价值观和思维方式

HOW?

知识

经验

创造力



Knowledge

Experience

Creativity

21天效应

10000小时定律

“实践”

# 安全在演进



安全已经成为 **“生存技能”**

# 攻击手段日新月异，必须“持续学习”



- APT ( Advanced Persistent Threat ) – 高级持续威胁

- 攻击来源变化：从个人到有组织犯罪，到网络战
- 攻击目的变化：从炫技到经济、政治利益
- 攻击方法变化：从单一粗糙技术到成体系的精细平台
- 规模：大流量、大范围

# 安全认识的变革

- 过去几十年，企业制定了各种方案、购买了大量的产品，构筑了坚固的堡垒和防线



“以人为本”

“动态防御”

“全员提升”



# 人是安全体系中最重要但最薄弱的环节



- 信息安全对抗是信息不对称性的对抗。
- 防御是被动的，而渗透是主动的。
- 大多数的渗透并未被感知。

安全意识

+

安全应用

+

安全技能

人才困局

# 信安人才的困局



- 困境
  - 实用型安全人才严重缺乏，攻防经验不足
  - 对新技术和新工具掌握能力差距巨大
  - 业务敏感性高，难以在实际业务环境培训人才
  - 业务系统复杂，无法有效评估、验证测试
- 需求
  - 加强安全意识，加强技术能力
  - 利用高仿真实验环境，持续培养人员的实战能力
  - 加入安全社区，不断最新技能，学习最新技术

“纸上谈兵”

“盲人摸象”

# 安全人才缺口有多大？



- 截止2014年底，我国重要行业信息系统和信息基础设施需要各类网络空间安全人才70万，预计到2020年，需要各类网络空间安全人才约**140**万人，而目前我国高等学校每年培养的信息安全相关人才不足1.5万人，远远不能满足网络空间安全的需要。

——教育部教指委秘书长 封化民

- 到2017年，全球信息安全人才缺口达**475**万。

# 信息安全从业人员“钱”景如何？



- 未来的一年，首席安全官 (CSO) 的薪酬范围是 14.025 万美元到 22.250 万美元之间。这代表着平均 7.0% 的涨幅，是整个薪酬调查中第 4 高的。CSO 薪酬增长在 2016 年将比其他 IT 高管要高得多。

# 哪类人才更紧缺？

表 1 各单位信息安全专业人才缺口 TOP5

序列	政府机关	科研院所	国有企业	私营企业	外资企业	合资企业
TOP1	运营与维护类 (32.09%)	技术开发类 (26.47%)	运营维护类 (28.16%)	技术开发类 (30.22%)	技术开发类 (30.22%)	技术开发类 (40.00%)
TOP2	保护与防御类 (27.61%)	保护防御类 (20.59%)	保护防御类 (22.74%)	运营维护类 (17.58%)	保护防御类 (21.43%)	研究分析类 (30.00%)
TOP3	管理类 (17.16%)	运营维护类 (13.73%)	管理类 (21.66%)	保护防御类 (16.48%)	网络攻防类 (14.29%)	运营维护类 (15.00%)
TOP4	技术开发类 (16.42%)	研究分析类 (13.73%)	技术开发类 (21.30%)	管理类 (11.54%)	运营维护类 (10.71%)	风险评估与测试类 (15.00%)
TOP5	风险评估与测试类 (8.96%)	风险评估与测试类 (11.76%)	技术支持类 (15.88%)	技术支持类/研究分析类 (8.79%)	研究分析类/管理类 (10.71%)	监督审计类 (5.00%)

- 超七成受访者认为组织内信息安全专业人才不足
- “技术开发类”、“运营维护类”、“保护防御类”信息安全专业人才是我国各行业主要短缺的信息安全专业人才类型

\* 数据来源：中国信息安全测评中心《2014-2015年度我国信息安全从业人员现状调查》

# 黑客游乐场

# 科技发展导致了知识传递方式的变革



甲骨文—》文字—》书籍—》图书馆—》互联网

师父—》私塾—》学校—》在线教育

找不到知识



找不到好知识

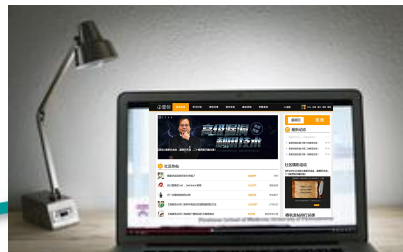
获取知识不再是问题，而获取知识的方式，解决如何理解知识、消化知识，把知识转变为解决问题的能力，这才是未来教育所需要关注的主要问题。



# i 春秋全新的在线学习生态链



在线学习



分享观点



在线实验



成为讲师



参加竞赛



完成挑战 (实验)

# i 春秋的人才培养之道

培养黑客思维

不知攻，焉知防？

自由、创新、突破

实践为主

理论与实践相结合

构建高度仿真的攻防目标场景，实验场景化

内容为王

用最优秀的人才去培养未来更优秀的人才

# i 春秋的核心要素

- 丰富且“与时俱进”的课程和实验
- 竞赛对抗的趣味挑战题目

课程体系

仿真场景

- “模拟实战”仿真
- 典型企业、网站等环境，从数据到服务

- 有大牛潜伏的社区
- 定期线下沙龙，构建学习型社区

用户社区

云端集群

- 多集群、多链路
- 基于场景服务的私有云
- 千人并发实验

# 数读



# 云端实验

# 游乐场怎能没有玩具？

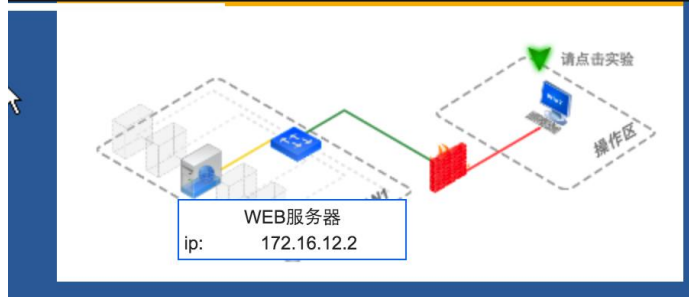
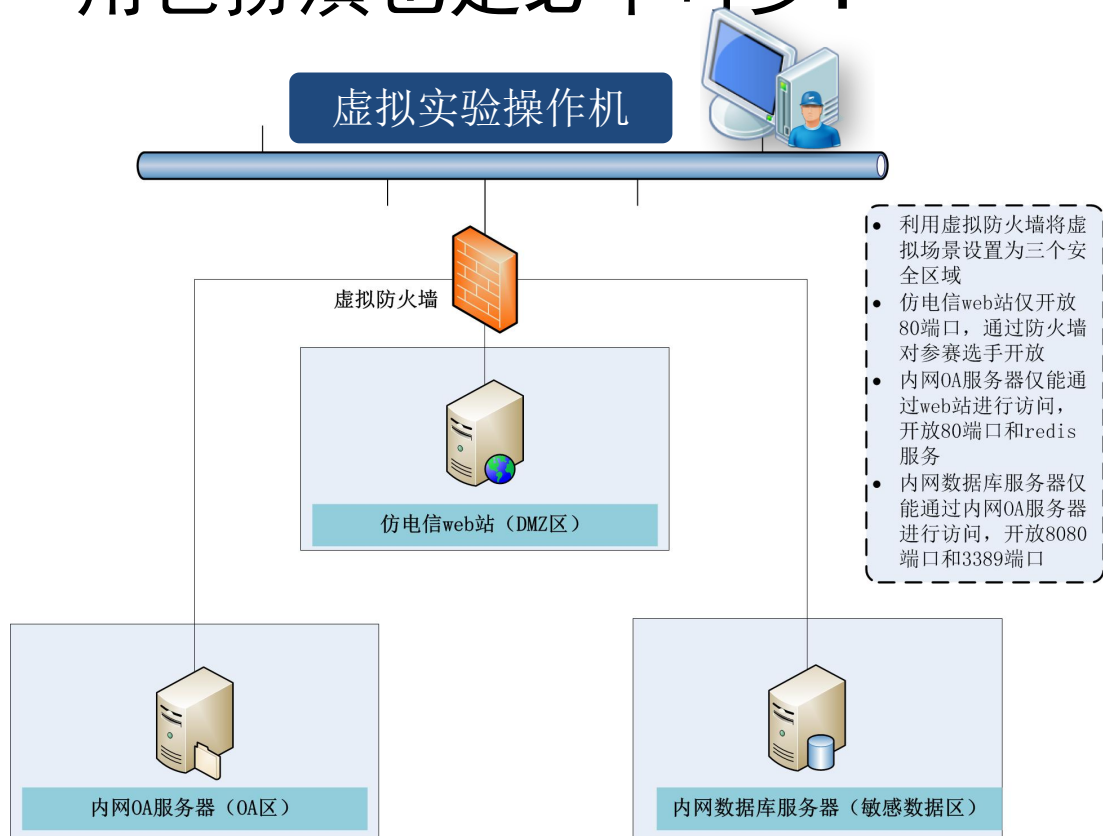


普通公有云IaaS为“租户”提供空白虚拟机，就像“**毛坯房**”，用户可根据自己需要进行服务和应用的“装修”



i春秋根据教学需要，为学员搭建好各种“**主题套房**”模版，工具、漏洞、服务俱全，几十秒钟即可拥有，还可反复申请

# 角色扮演也是必不可少!



# 实验场景的分类

- 单机场景——所有实验在同一台虚拟机内完成，即是攻击机，又是防御机

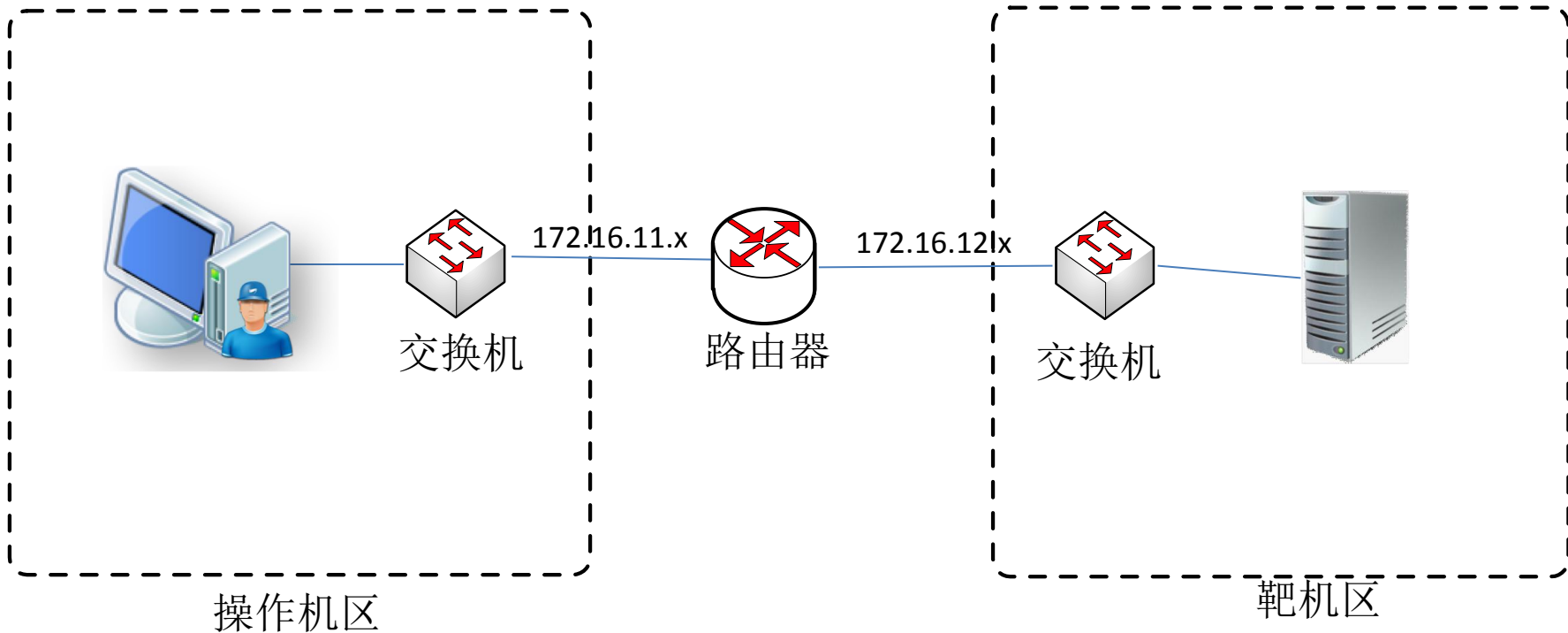


实验区域



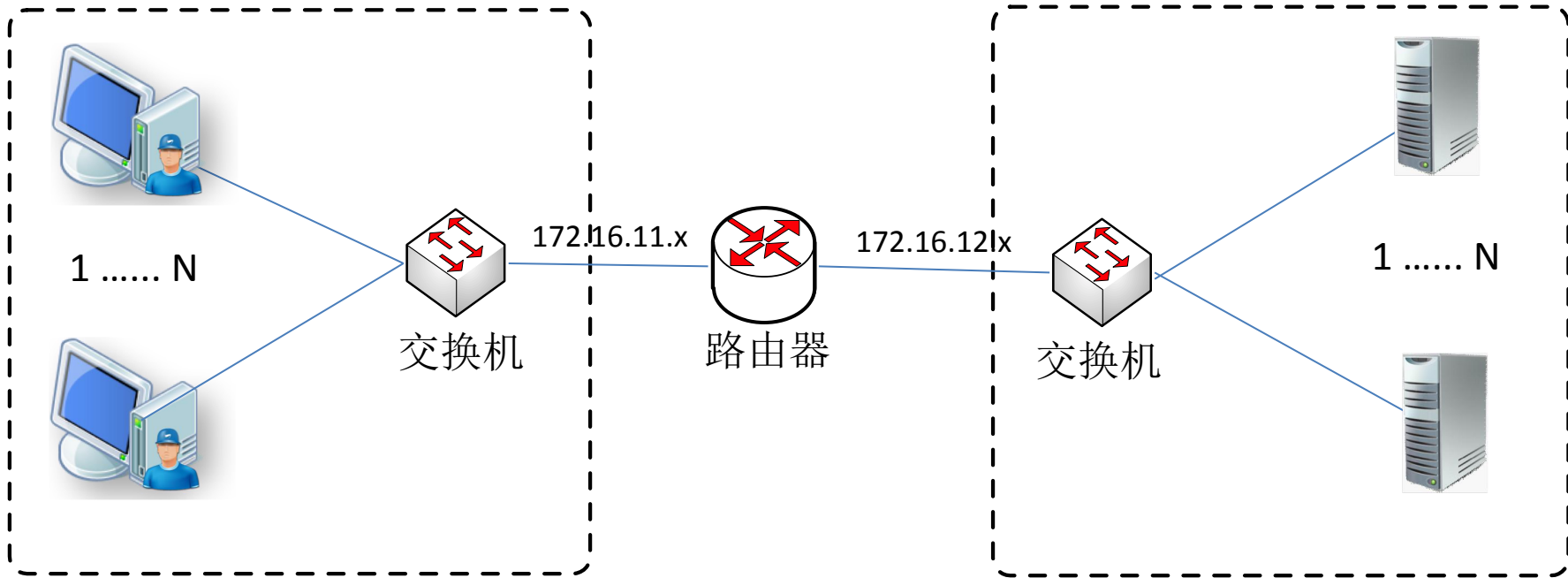
# 实验场景的分类

- 双机场景



# 实验场景的分类

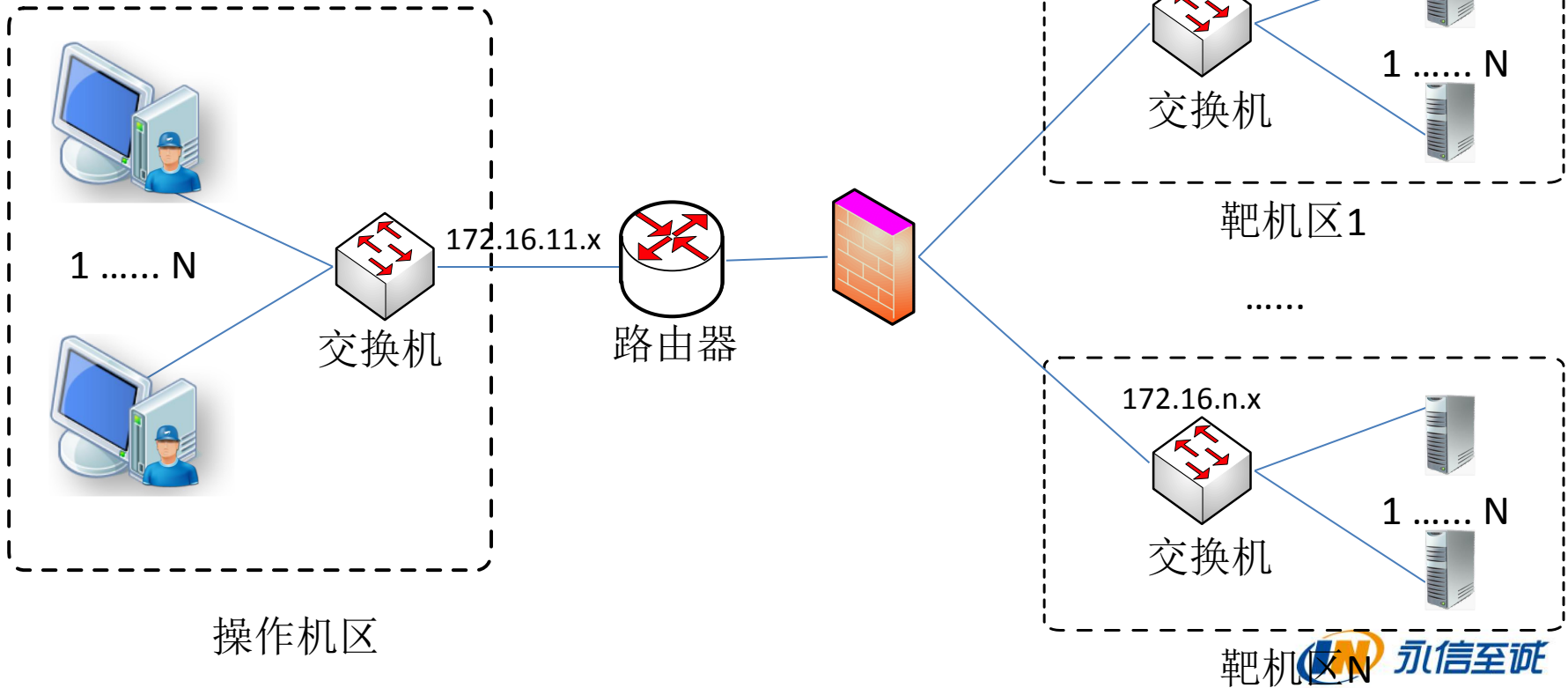
- 双网场景



操作机区

# 实验场景的分类

- 复杂靶机场景

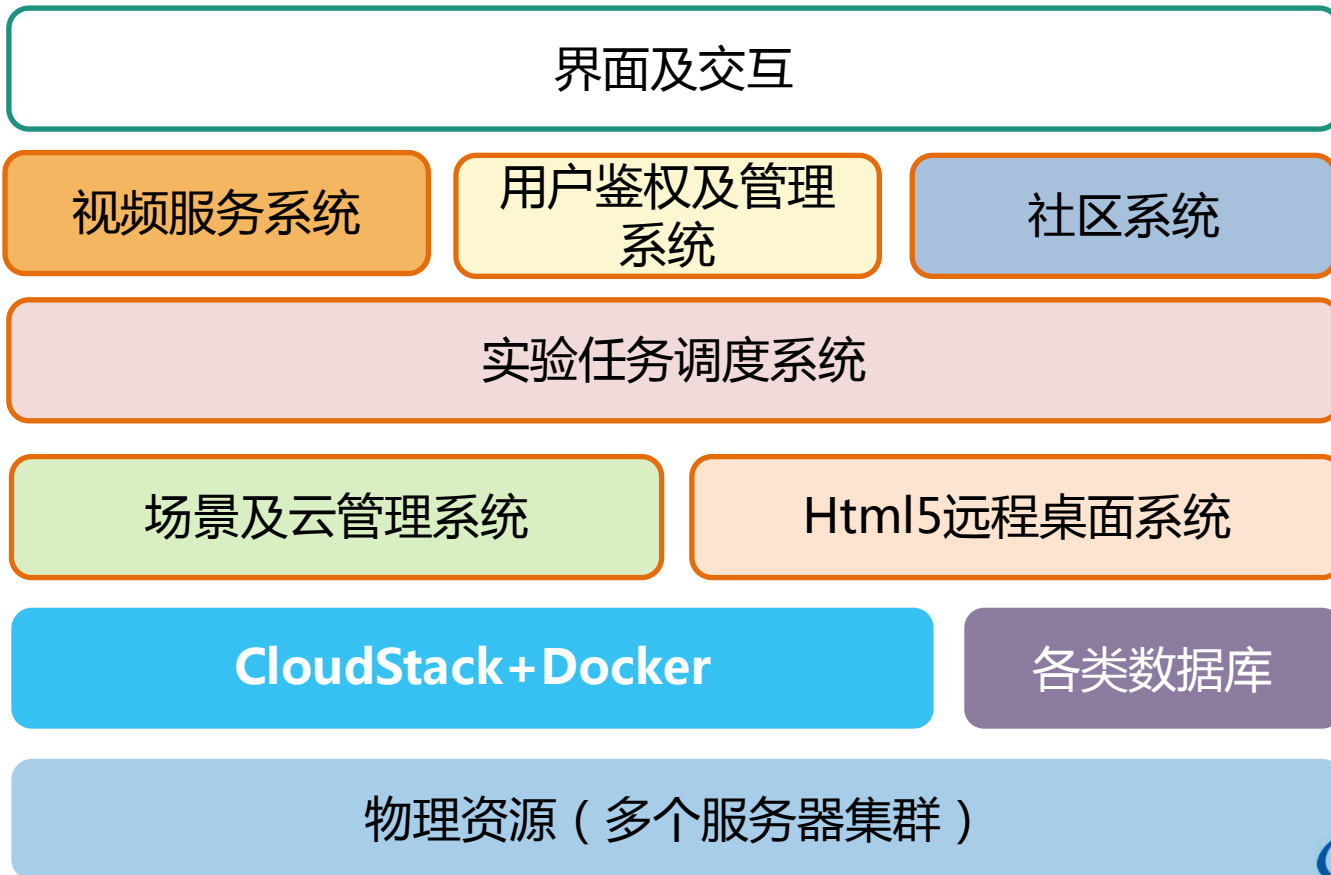


## 云端实验室的优势？

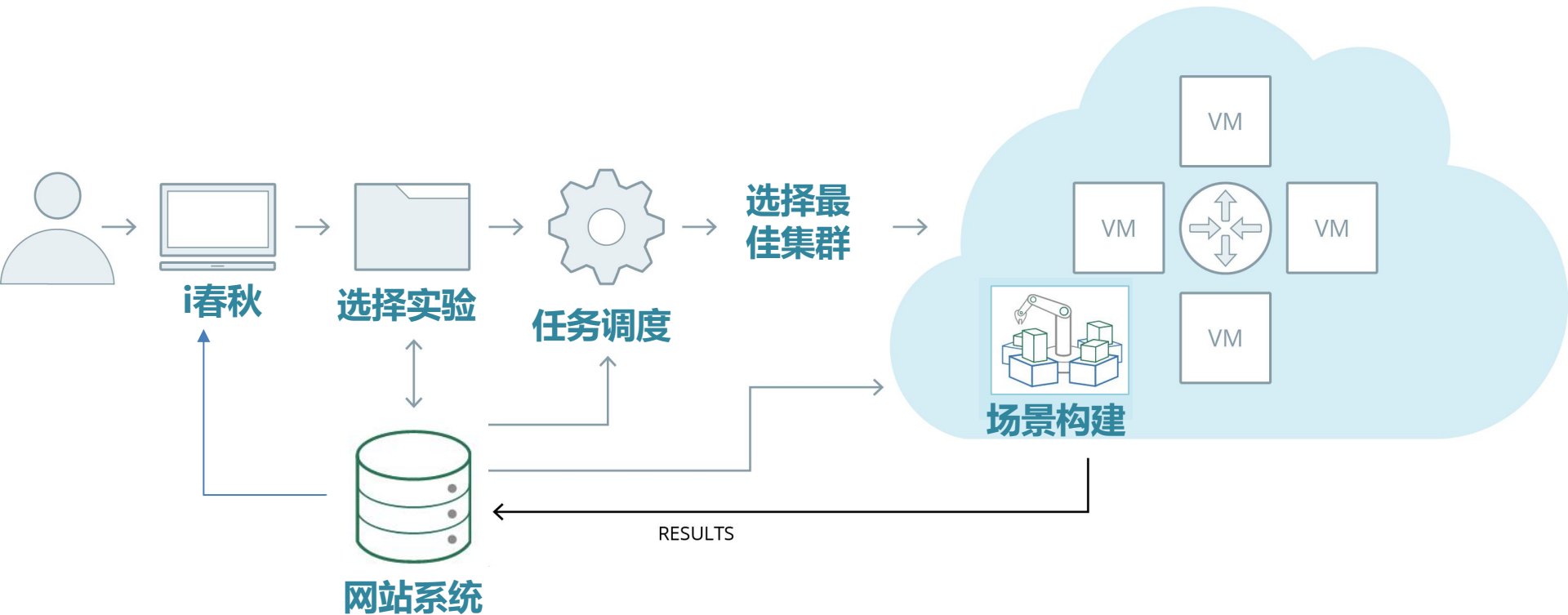
- 互联、共享
- 安全、可靠、无污染
- 精华内容、节约时间



# i 春秋技术架构



# 云端实验下发流程



# 虚拟操作桌面—高速模式

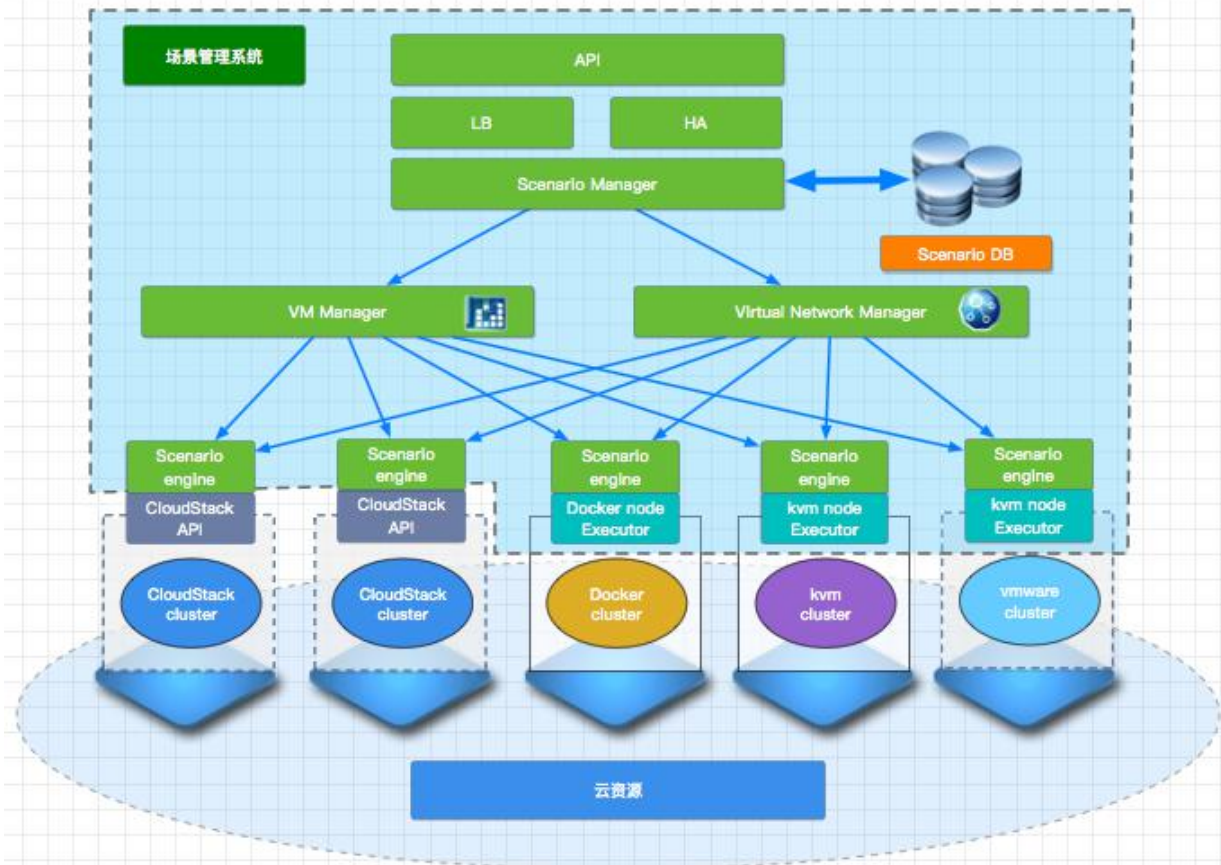


- 云平台通常会提供基于vnc或3389的远程操作桌面，用户可以使用客户端工具连接
- 开发了专用的云桌面代理服务系统，根据实验操作学员的使用量动态调节资源，并将操作桌面嵌入了浏览器中，**只要有浏览器就能进行实验**
- 高速操作模式

# 幕后英雄—场景及云管理系统

- 为上层应用提供统一的api接口
- 向下支持多种虚拟化、容器和云管理系统
- 场景资源导入、注册和管理
- 任务的分发、调度、负载均衡以及实验场景的全生命周期管理
- 资源监控、报警及处理
- 集群间的同步和备份等





# 实践一场景构建流程

1、场景模板构建

2、攻防剧情设定

3、选择主机模板

4、网络拓扑构建

5、网络访问策略

分类

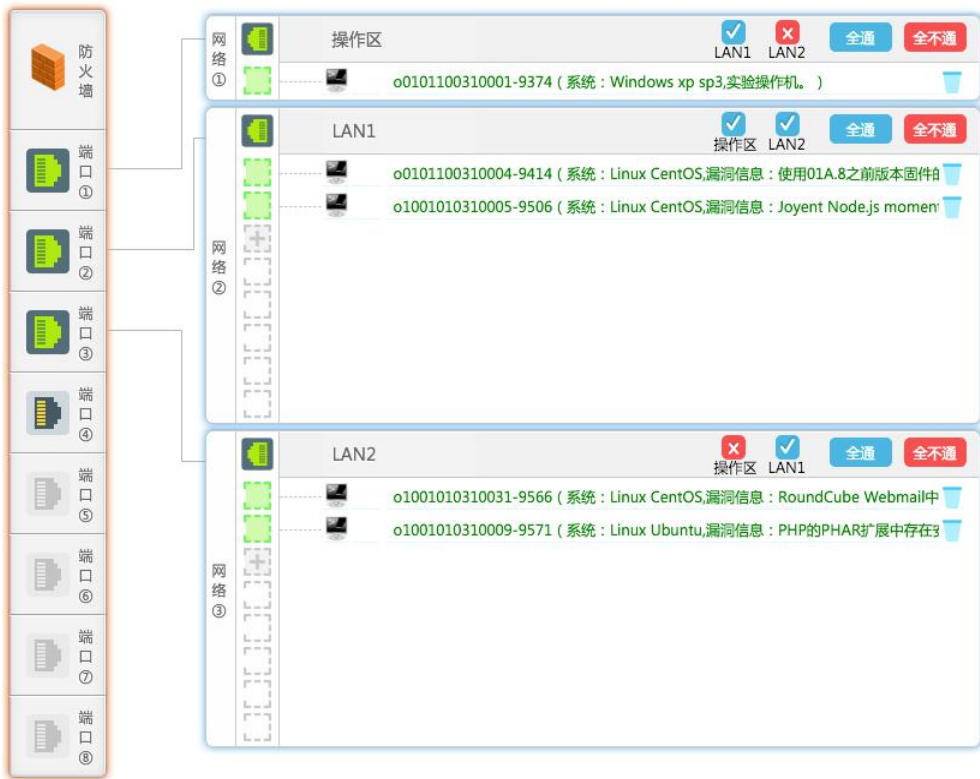
CTF实训管理

场景模板管理

- 虚拟机模板管理
- 场景制作

场景名称: 测试场景

场景描述: 3安全区剧本测试



# 小结

- 信息安全必将成为基本的生存技能
- 云计算使mooc和云端游乐场具备现实中应用的基础

虚拟化

+

MOOC

+

信息安全



培养信息时代的安全感

谢谢！