网络安全创新大会
Cyber Security Innovation Summit

网络攻防靶场的技术经验分享

张锦章 360实网攻防中心 总经理

网络安全问题面临的四大变化

网络安全问题面临的四大变化

对手变了 | 对象变了 | 手段变了 | 假设变了

什么是实网攻防演习

什么是实网攻防演习

实网攻防演习是有组织、有目的通过对实际环境**开展网络攻击**，以达到**通过实战**分析目标安全风险，检验**目标综合防御能力的目的**。

明确目标系统，不限制攻击路径，以

提权 | 控制业务 | 获取数据

为最终目的

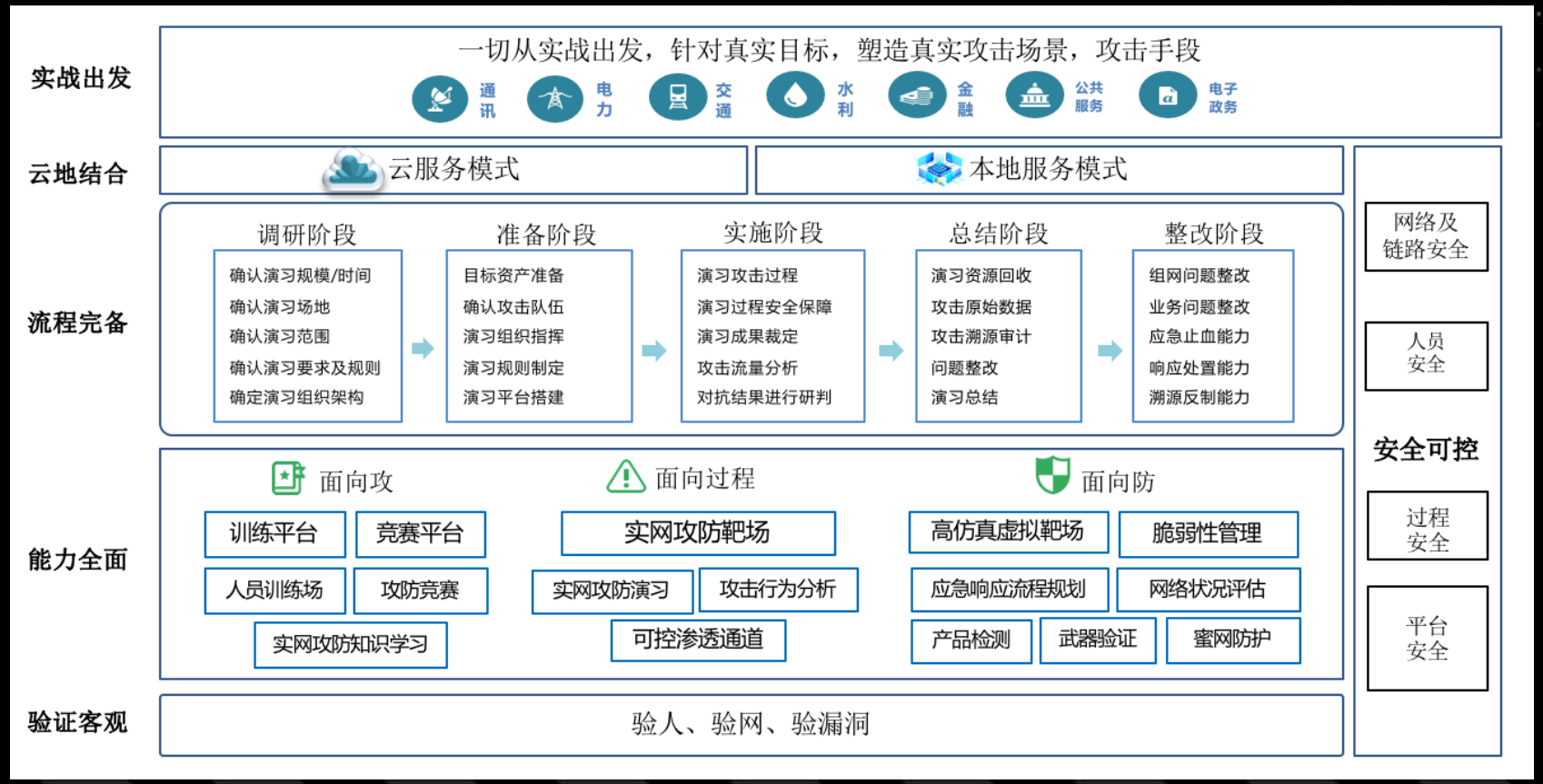
实网攻防的关键要素

实网攻防的关键要素

实战出发 | 云地结合 | 流程完备

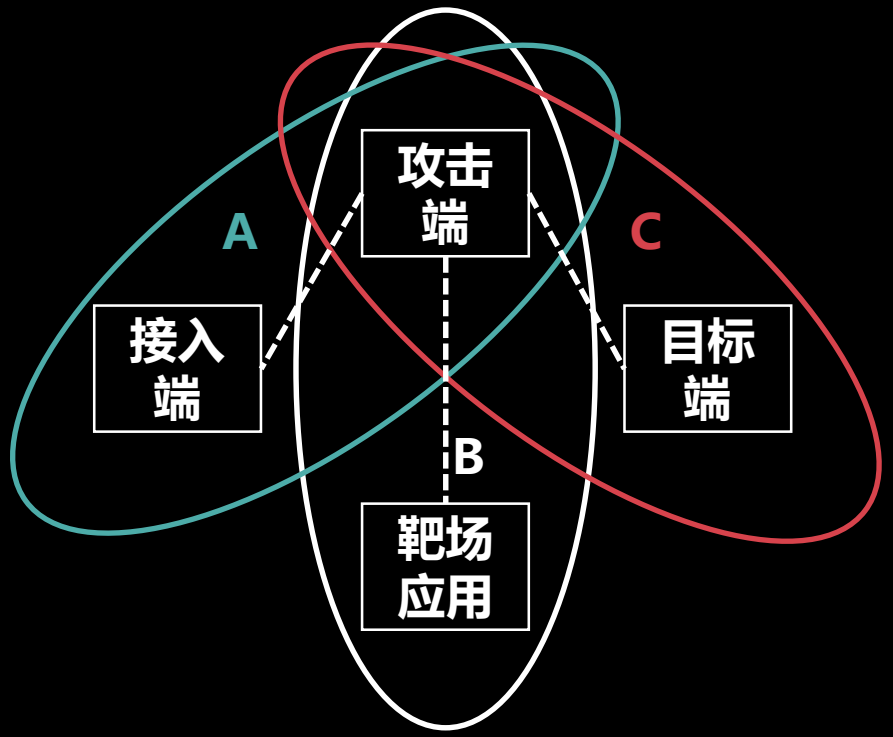
能力全面 | 验证客观 | 安全可控

实网攻防的关键要素


实战出发
一切从实战出发，针对真实目标，塑造真实攻击场景，攻击手段
通讯
电力
交通
水利
金融
公共服务
电子政务
云地结合
云服务模式
本地服务模式
流程完备
调研阶段
确认演习规模/时间
确认演习场地
确认演习范围
确认演习要求及规则
确定演习组织架构
准备阶段
目标资产准备
确认攻击队伍
演习组织指挥
演习规则制定
演习平台搭建
实施阶段
演习攻击过程
演习过程安全保障
演习成果裁定
攻击流量分析
对抗结果进行研判
总结阶段
演习资源回收
攻击原始数据
攻击溯源审计
问题整改
演习总结
整改阶段
组网问题整改
业务问题整改
应急止血能力
响应处置能力
溯源反制能力
能力全面
面向攻
训练平台
竞赛平台
人员训练场
攻防竞赛
实网攻防知识学习
面向过程
实网攻防靶场
实网攻防演习
攻击行为分析
可控渗透通道
面向防
高仿真虚拟靶场
脆弱性管理
应急响应流程规划
网络状况评估
产品检测
武器验证
蜜网防护
验证客观
验人、验网、验漏洞
网络及链路安全
人员安全
安全可控
过程安全
平台安全

网络安全创新大会
Cyber Security Innovation Summit

面向攻防靶场的网络隔离技术



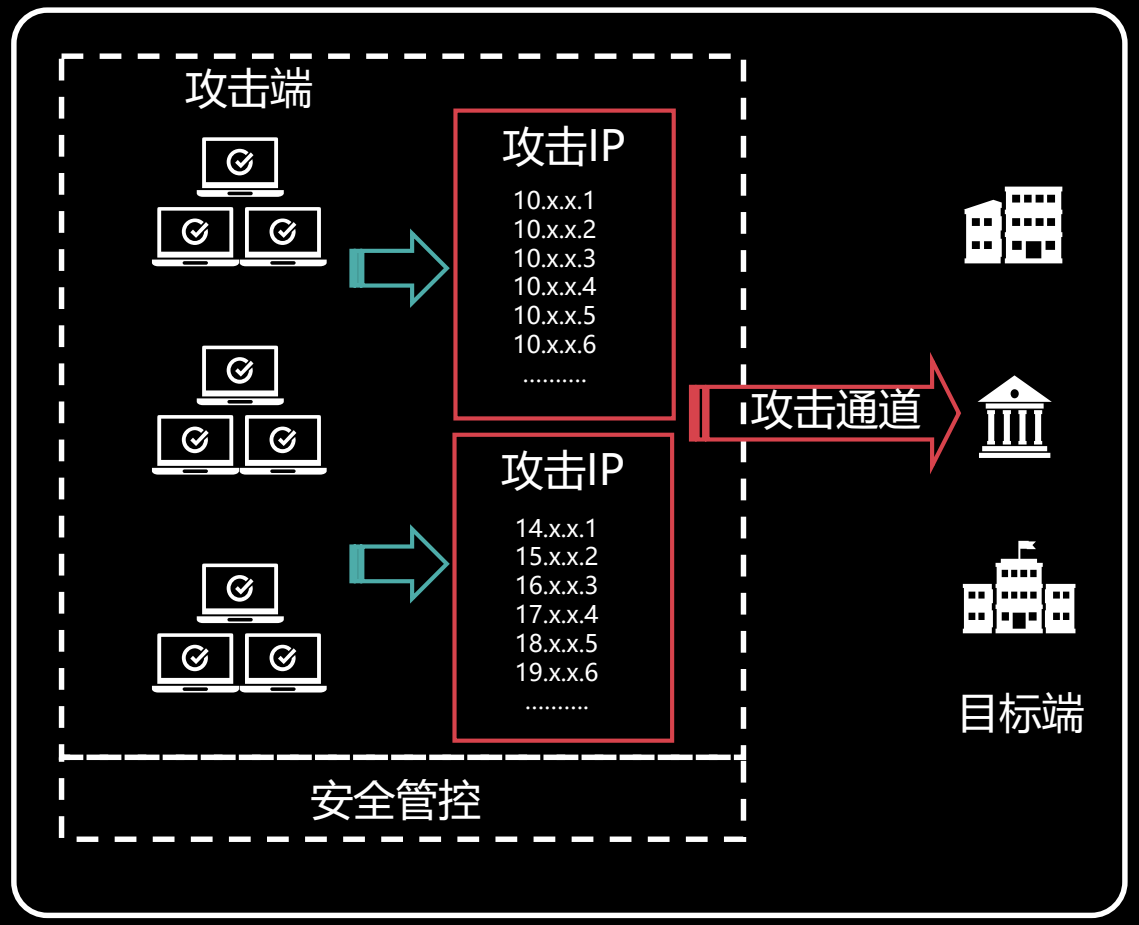
A.认证接入网络

B.内部应用网络

C.攻击专用网络

攻击IP地址伪装与切换技术

攻击IP地址伪装与切换技术



攻击IP伪装与实时扩充

攻击IP快速切换

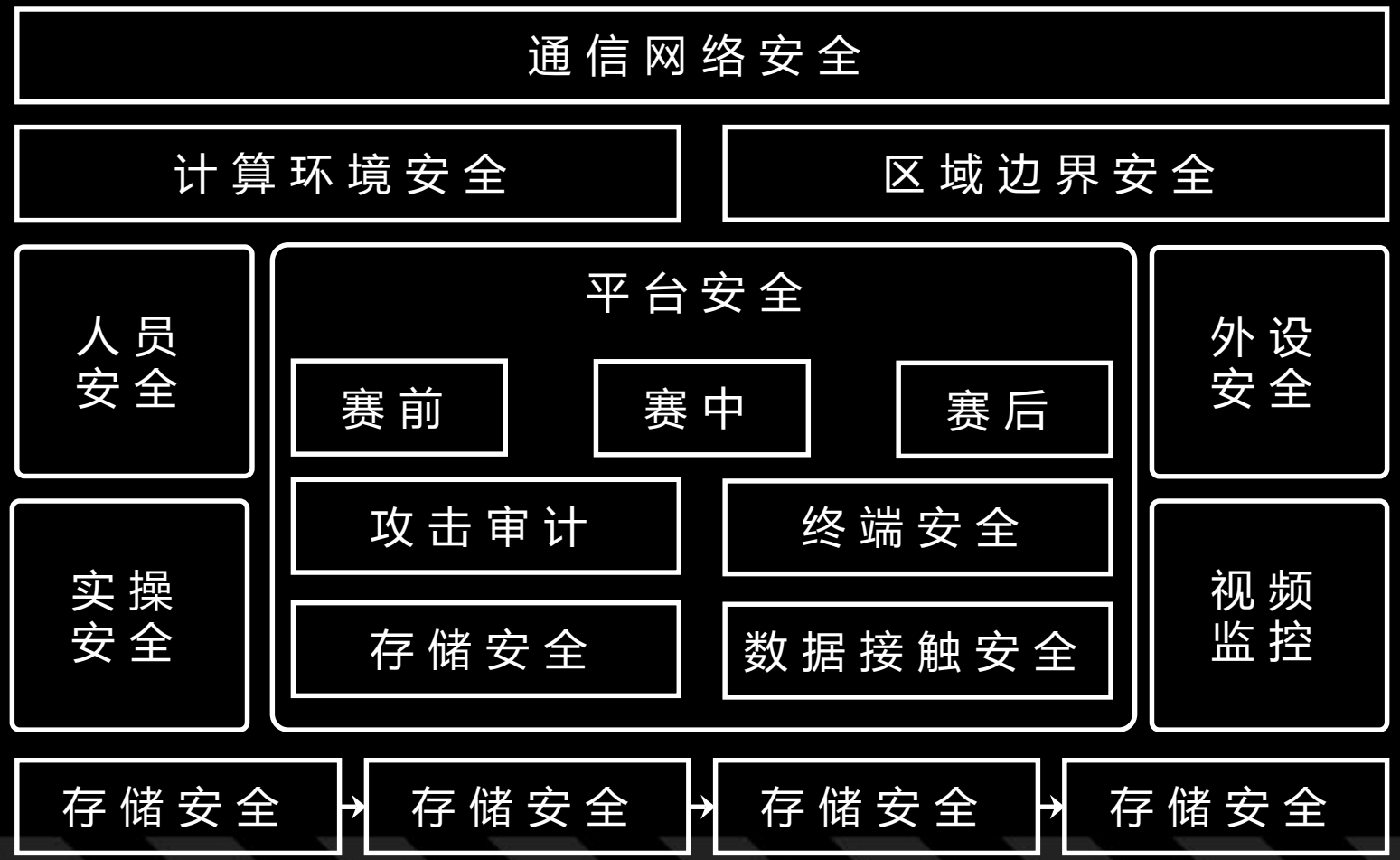
攻击IP安全管控

攻击IP溯源

靶场安全技术

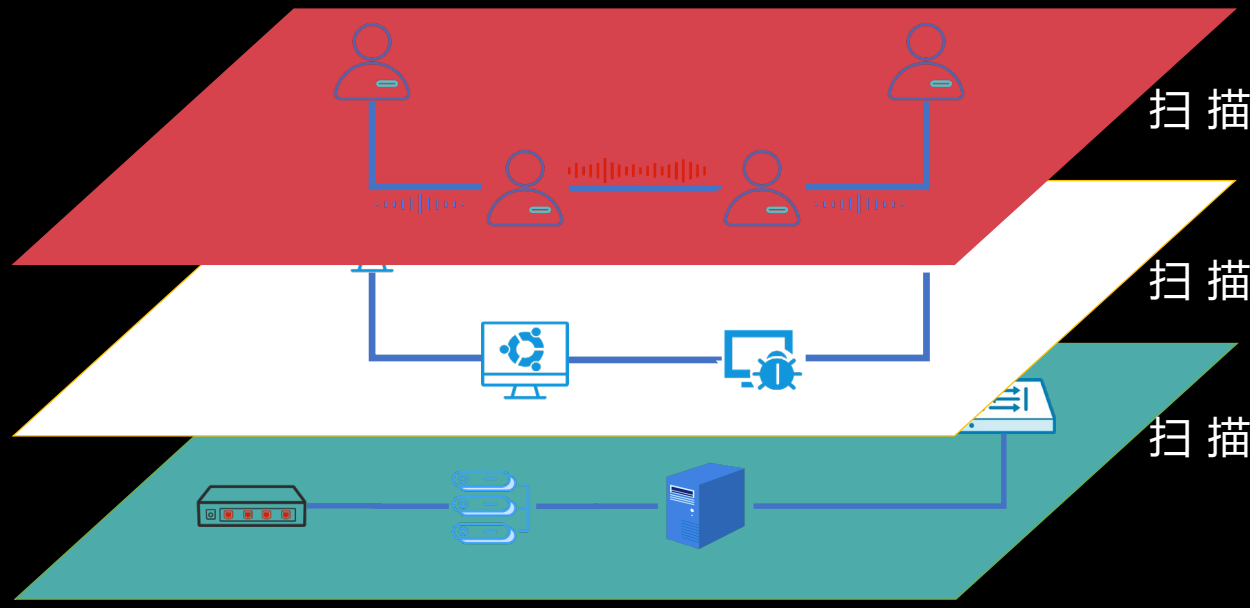
靶场安全技术

网络安全创新大会
Cyber Security Innovation Summit



如何解决仿真靶标滞后性与现实目标渐变性的矛盾？

如何解决仿真靶标滞后性与现实目标渐变性的矛盾?



扫描用户行为特性信息

扫描应用指纹信息

扫描实体设备指纹信息

流量采样及还原技术

如何解决仿真环境通用性与关键设施差异性的矛盾？

如何解决仿真环境通用性与关键设施差异性的矛盾?

网络安全创新大会
Cyber Security Innovation Summit

深层次虚实结合

深层次虚实结合，自动化配置与管理，与场景完美融合。

如何解决靶场架构固化性与现实威胁多样性的矛盾？

如何解决靶场架构固化性与现实威胁多样性的矛盾?

攻击行为模拟技术

如何解决靶场架构固化性与现实威胁多样性的矛盾?

用户行为模拟技术

实网攻防攻击技术趋势

信息收集 | 0day攻击 | 迂回、隐蔽 | 钓鱼、社工

防守基础应对要点

防守基础应对要点

边界防护

内网主机防护

信息泄露排查

应用系统加固

内部人员管理与培训

五重保障，让攻击者寸步难行

网络安全创新大会
Cyber Security Innovation Summit

THANKS