ISC 2016

2016 中国互联网安全大会 China Internet Security Conference

协同联动 共建安全+命运共同体

《安全通论》----网络空间安全教育的理论与实践

杨义先

教授、长江学者、国家杰青
北京邮电大学信息安全中心主任
灾备技术国家工程实验室主任

目录

网络空间安全的基础理论

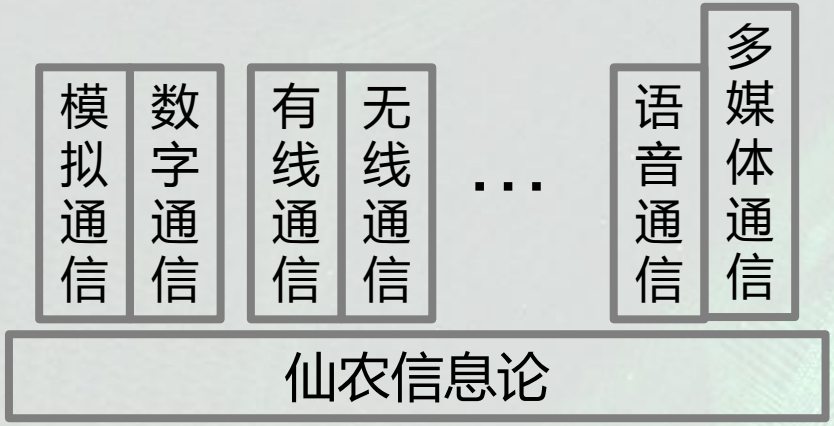
新型网络安全观的树立

学生工程实践能力的培养

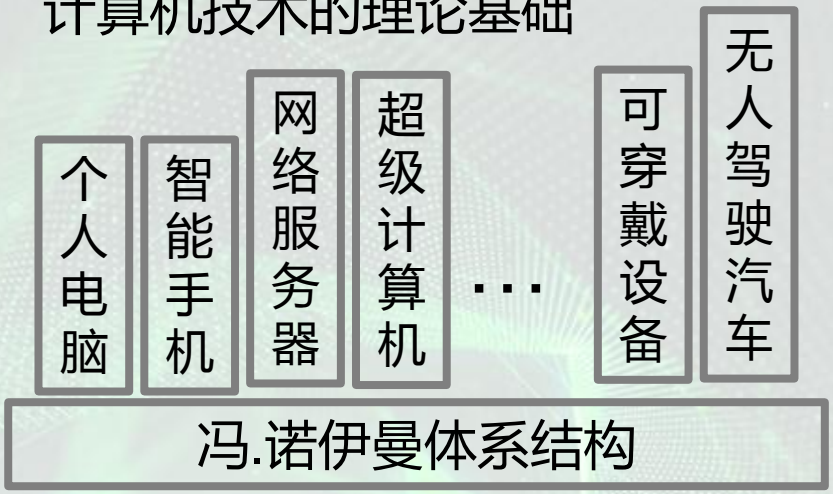
网络空间安全的基础理论

能否建立一个统一的安全基础理论体系

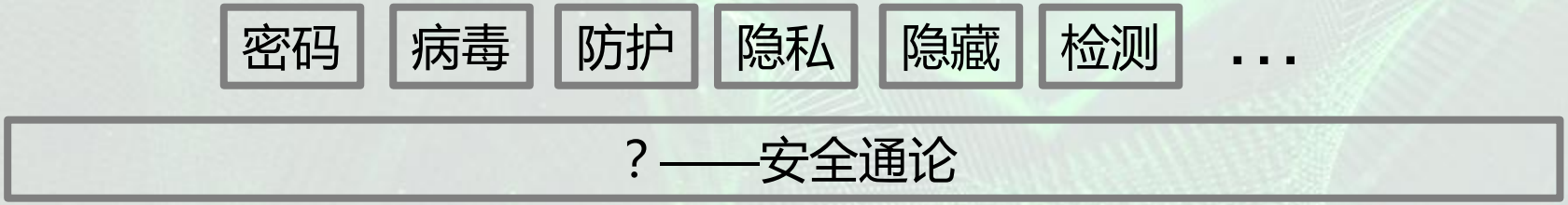
仙农的信息论是所有现代通信技术的理论基础



冯·诺伊曼体系结构是所有现代计算机技术的理论基础



然而，安全技术，实践先于理论。是否能够建立一个统一的基础理论体，将网络空间安全问题的各个分支统一起来。



网络安全基础理论体系建设的意义

- 提升学生学习的系统性
- 指导高校的学科建设规划
- 有效应对安全问题的多样性、复杂性，以及层出不穷的新威胁
- 使学生能够更好的学习和接受新技术、新方法、新产品

网络安全基础理论体系的一些要点

- 不安全熵
- 攻击容量、防御容量
- 安全经络图
- 图论、信息论、系统论、博弈论

网络安全的基础理论体系（安全通论），将是多种基础理论与实践科学相互融合的产物

ISC 2016 中国互联网安全大会

360互联网安全中心

新型网络安全观的树立

从正确的理论到正确的观念

- 网络安全教学，往往重技术，轻观念，或者说不知道什么是正确的观念。
- 正确的安全观念是正确的使用技术，以及做出正确决策的重要前提。
- 正确的安全观念，应当出自科学的安全基础理论，并在实践中接受检验。

从二态安全观到三态安全观

传统二态安全观

你死+我活，零和博弈

后果：敌我双方不惜耗费大量的人力、物力和财力，长期斗争，但却没有最后的赢家

新型三态安全观

水涨+船高+纳什均衡

信息弱国信息战策略应该以追求“纳什均衡状态”为主要目标！

从局部安全观到系统安全观

追求局部绝对安全，对吗？

判断某种网络安全保障措施是否正确的唯一标准，是“它将引起系统的不安全熵向哪个方向发展”

最笨的做法

以局部的不安全熵的减小，激发全局不安全熵的大幅度增加

以暂时的不安全熵的减小，激发长期不安全熵的大幅度增加

以封闭性不安全熵的减小，激发开放性不安全熵的大幅增加

为追求绝对安全，却激发了系统不安全熵的大幅度增加

为追求孤立的安全，却激发了共同的不安全熵的大幅度增加

攻防的极限页可以度量

如果黑客经过n次攻击，获得了S次成功，那么，一定有S≤nC。这里C是“攻击信道” 的信道容量

反过来，如果红客经过N次防卫，获得了R次成功，那么，一定有R≤ND。这里D是“防御信道”的信道容量

如果C<D，那么黑客输；如果C>D，那么红客输；如果C=D，那么，红黑实力相当。

学生工程实践能力的培养

加强工程实践能力培养（北邮的做法）

1. 信息安全实验教学平台
2. 网络安全攻防实训平台
3. 网络安全演练竞技平台

信息安全实验教学平台-功能概述

信息安全实验教学平台-功能概述

实验中心功能

虚拟调度

采用业界最流行的开源虚拟化技术，实现虚拟机按需定义、创建、暂停、关闭、删除、克隆、迁移、Web调用展现

虚拟Windows、Linux、bt5等主流操作系统

虚拟路由交换、FW、IDS等网络及安全设备

安全实验

支持密码学、网络攻防、系统安全等安全实验，具有详细实验目的、描述、步骤、环境等

拓扑构建

简单拖拽实现网络环境搭建
Flex实现动态展现效果

监控中心功能

网络数据监控

攻击流量抓取

攻击数据还原

攻击行为呈现

性能监控

支持虚拟机CPU、硬盘、内存等性能监测

屏幕监控

攻击屏幕监视

支持录屏及攻击回放

资源中心功能

课程体系

北邮等重点高校权威课程体系支撑

课程具有可伸缩性按需组合呈现

实验体系

配套课程体系设置

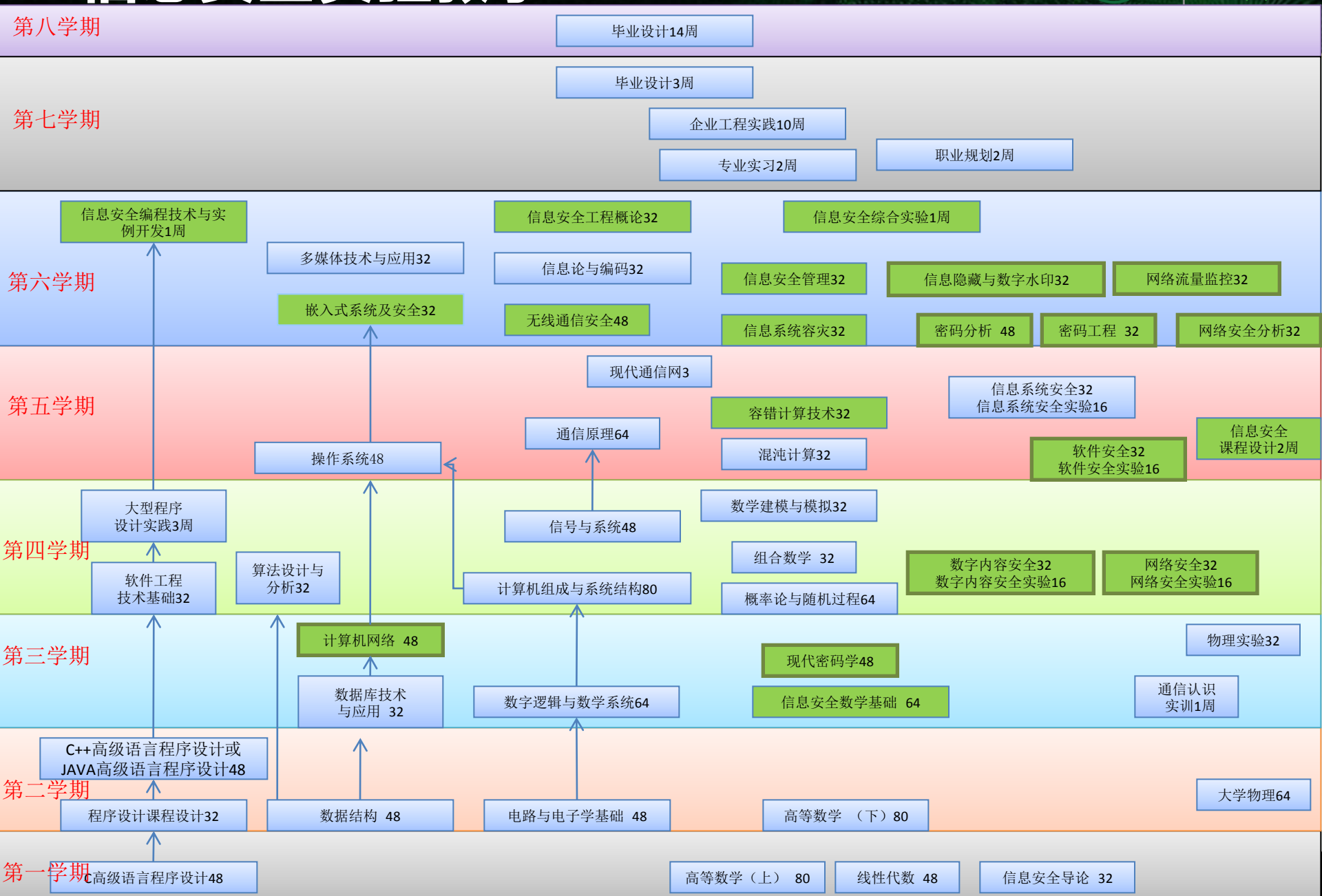
支持自编辑可拓展

虚拟场景

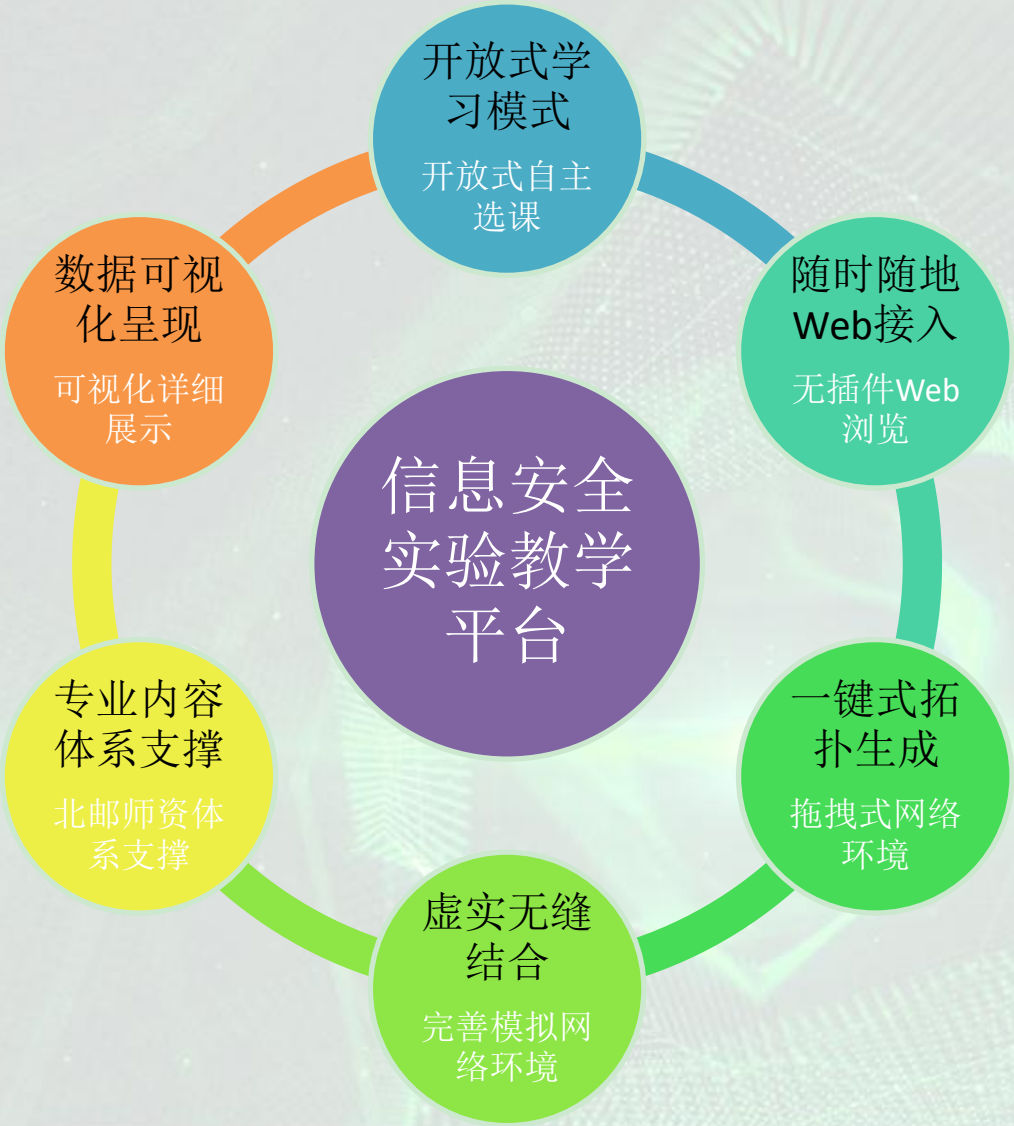
含有丰富的虚拟标靶场景库

支持场景库加载创建

信息安全实验教学


第八学期
毕业设计14周
第七学期
毕业设计3周
企业工程实践10周
专业实习2周
职业规划2周
第六学期
信息安全编程技术与实例开发1周
多媒体技术与应用32
嵌入式系统及安全32
信息安全工程概论32
信息论与编码32
无线通信安全48
信息安全综合实验1周
信息安全管理32
信息隐藏与数字水印32
网络流量监控32
信息系统容灾32
密码分析 48
密码工程 32
网络安全分析32
第五学期
现代通信网3
操作系统48
通信原理64
容错计算技术32
混沌计算32
信息系统安全32
信息系统安全实验16
软件安全32
软件安全实验16
信息安全课程设计2周
第四学期
大型程序设计实践3周
软件工程技术基础32
算法设计与分析32
信号与系统48
计算机组成与系统结构80
数学建模与模拟32
组合数学 32
概率论与随机过程64
数字内容安全32
数字内容安全实验16
网络安全32
网络安全实验16
第三学期
计算机网络 48
数据库技术与应用 32
数字逻辑与数学系统64
现代密码学48
信息安全数学基础 64
物理实验32
通信认识实训1周
第二学期
C++高级语言程序设计或JAVA高级语言程序设计48
程序设计课程设计32
数据结构 48
电路与电子学基础 48
高等数学 （下）80
大学物理64
第一学期
C高级语言程序设计48
高等数学（上） 80
线性代数 48
信息安全导论 32

信息安全实验教学平台-特色



信息安全实验教学平台-页面展示

实验管理

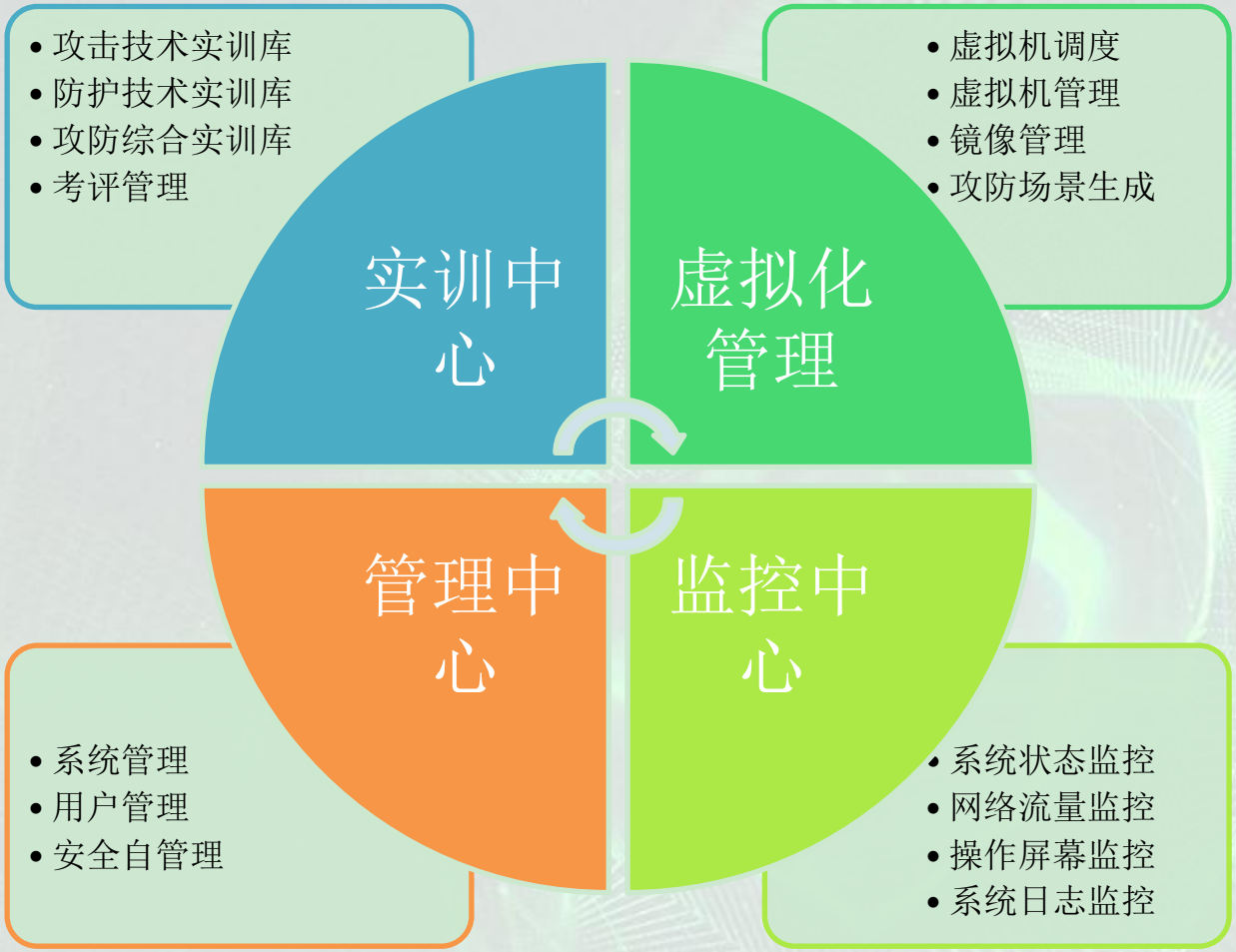
登陆

实验课程

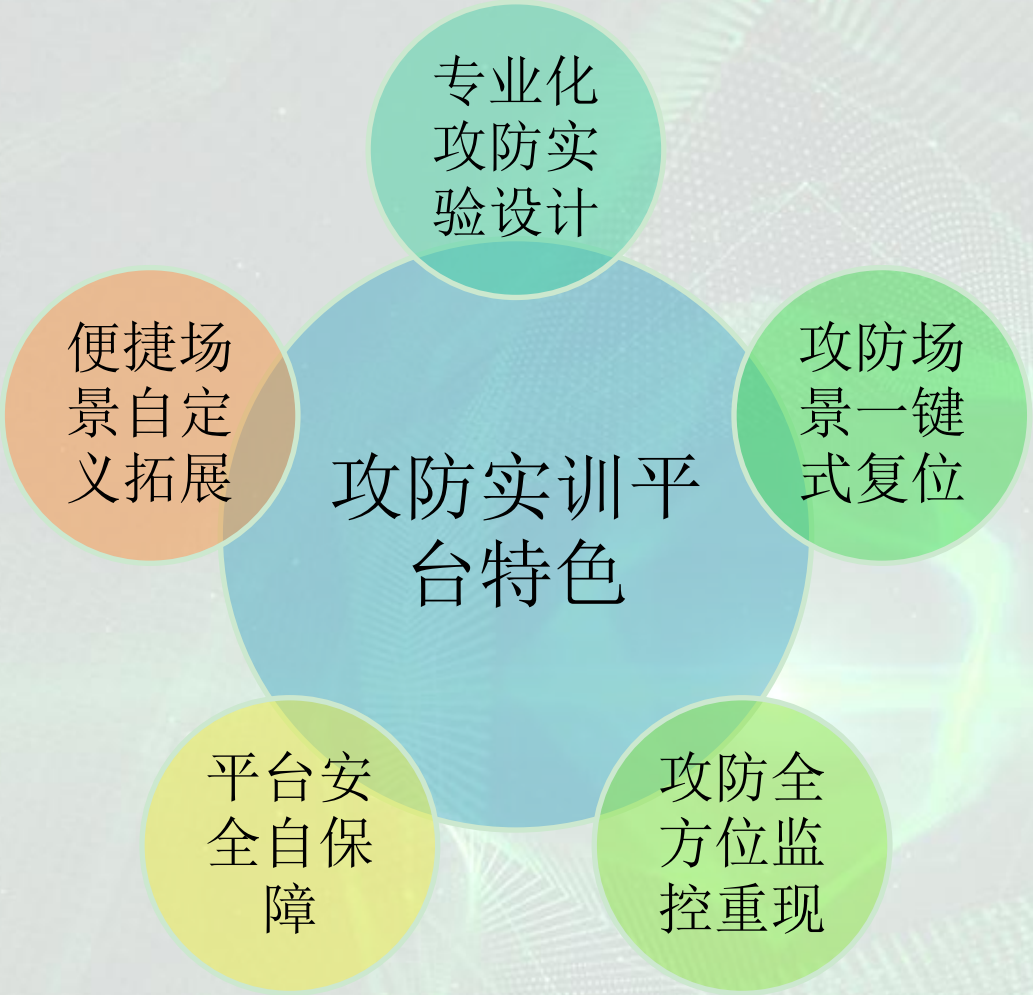
监控中心

用户管理

网络安全攻防实训平台-功能介绍



网络安全攻防实训平台-特色



网络安全攻防实训平台-页面展示

攻防实训

登陆

实验管理

用户管理

监控管理

网络安全演练竞技平台-功能介绍

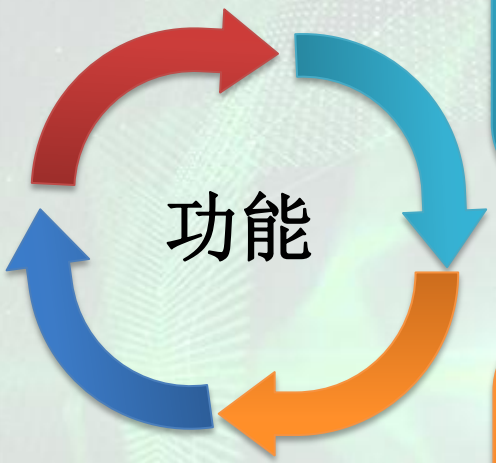
网络安全演练竞技平台

竞技中心

个人挑战赛：五大类攻防方向，难度分级
夺旗争霸赛：多组学员抢先夺旗，占先可加固
分组对抗赛：红蓝军分别作为攻防方网络对抗

场景中心

快速拓扑：鼠标拖拽搭建攻防场景，赛程可记忆还原
虚机管理：攻防靶机分级管理、丰富的攻击及防御工具
题库管理：Web安全、协议分析、逆向等不同难度试题



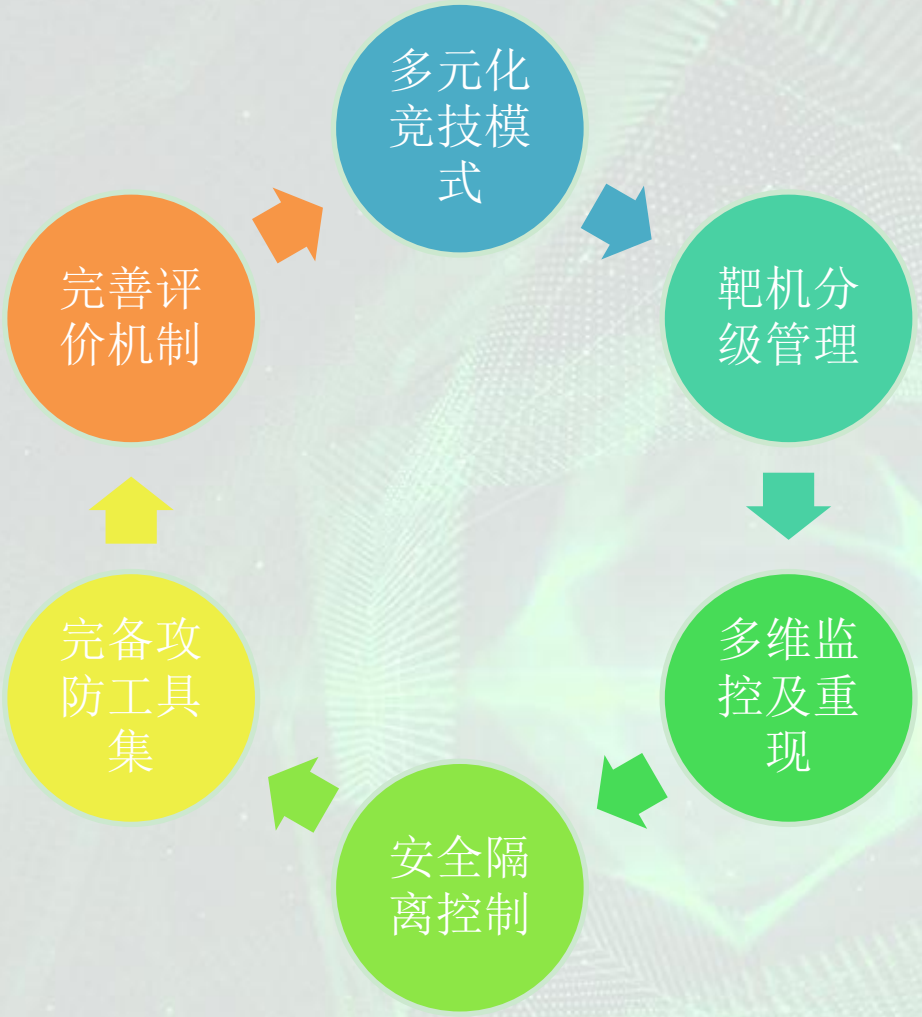
监控中心

数据流量监控
系统状态监控
操作屏幕监控
系统日志监控

管理中心

用户管理
系统管理
策略管理
安全自管理

网络安全演练竞技平台-特色



网络安全演练竞技平台-页面展示

夺旗争霸

登陆

个人挑战

分组对抗

靶机分级管理

应用与客户-应用场景

使用模式	行业应用	适用岗位
信息安全教学实验室建设	企业公司	安全专业教师
信息安全科研验证平台	高校	网络类教师
企业信息安全人力资源培训	金融行业	安全岗位人才
信息安全类攻防竞赛	军队	IT运维人员
网络攻防演练平台建设	能源行业	安全管理人员

应用与客户-典型用户

- 北京大学
- 北京邮电大学
- 中国传媒大学
- 重庆邮电大学
- 山东师范大学
- 河南警察学院
- 国家电网
- 总参三部
- 总参四部
- 360互联网安全实验室
- 国家网络与信息安全研究院
- 中国电信
- 等等

谢　谢