



# 面向实战运营的安全人才培养

张敬

安云科技CEO

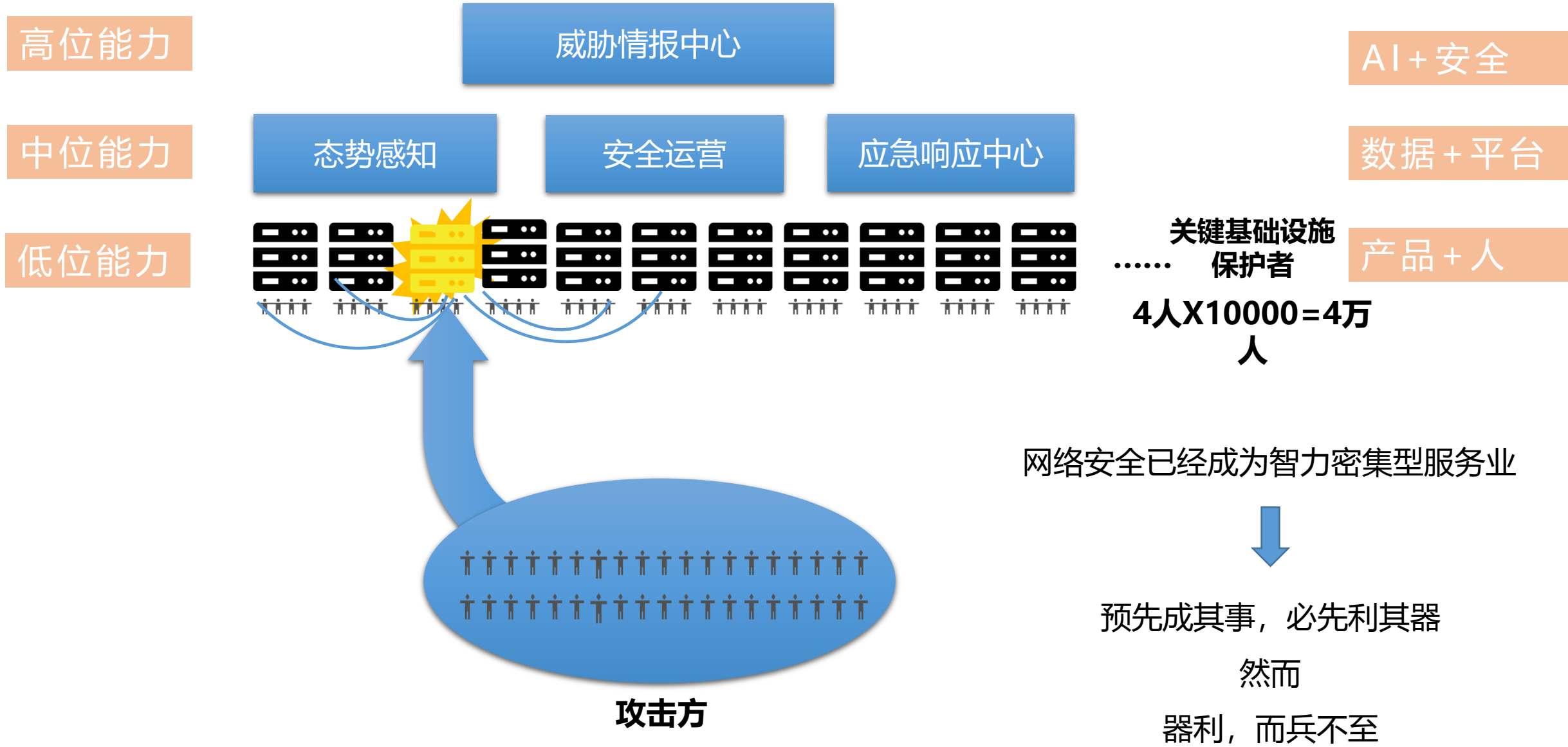
## 目录

### 实战安全运营人才需求

安全人才实训基地建设和培养方式

校企合作支撑网络空间安全专业建设

# 大数据时代的安全需要 “三位能力” 人才的协同







ARCHITECTURE  
**架构安全**

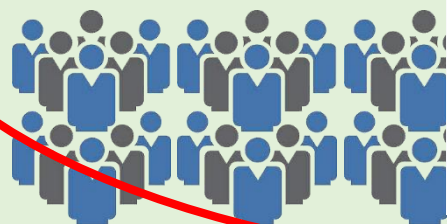
PA

OFFENSE  
**进攻反制**

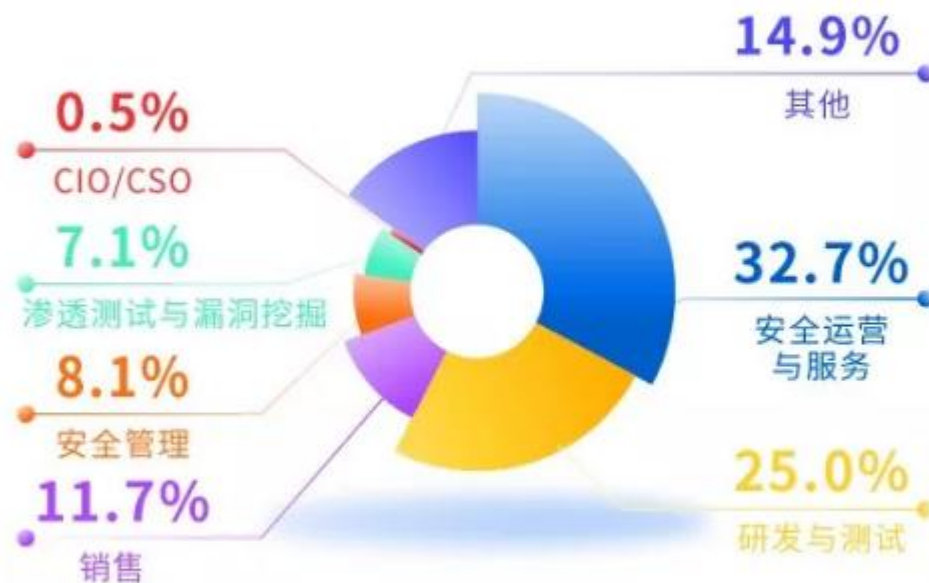
**安全**

## 运维与值守人员

- 需求量非常大
- 培养成本较低
- 适于学历教育培



政企机构网络安全人才的岗位类型分布



**人才**

## 攻击与渗透人员

需求量较少  
培养成本很高  
通过实战选拔为主



### 管理运维能力

#### 态势感知能力

- 一，低位能力
  - 态势感知和分析
- 二，中位能力
  - 破解和抑制宏观攻击
- 三，高位能力
  - 设计态势感知体系

#### 内网安全管理

- 一，低位能力
  - 安全监控和事件发现
- 二，中位能力
  - 应急响应能力
- 三，高位能力
  - 设计态势感知体系
  - 应急响应处置体系设计

#### 安全运维管理

- 一，低位能力
  - 执行安全巡检排查可疑事件
- 二，中位能力
  - 处理安全事件提交巡检报告
- 三，高位能力
  - 网络安全运维综合实践能力
  - 网络攻防综合实战能力

### 攻防能力

#### 漏洞挖掘能力

- 一，低位能力
  - 系统结构分析
  - 代码分析能力
- 二，中位能力
  - 漏洞发现能力
  - 协议弱点发现
- 三，高位能力
  - 漏洞利用设计

#### 渗透攻击能力

- 一，低位能力
  - 目标系统分析能力
  - 基础架构分析能力
- 二，中位能力
  - 系统攻击能力
  - 系统破坏能力
- 三，高位能力
  - 渗透过程设计
  - APT设计
  - 僵尸网络组建

### 安全工程能力

#### 系统安全建设能力

- 一，低位能力
  - 系统安全需求分析
- 二，中位能力
  - 系统层面的逆向攻击基本能力
- 三，高位能力
  - 安全架构设计
  - 搭建安全保障体系

#### 安全评估和测试

- 一，低位能力
  - 目标系统基础架构分析
  - 安全设备分析
- 二，中位能力
  - 系统层面的逆向攻击基本能力
- 三，高位能力
  - 系统安全风险评估
  - 系统安全测试
  - 进行设备和整体系统调试和验证

### 安全咨询能力

#### 安全体系咨询

- 一，低位能力
  - 务安全需求分析
- 二，中位能力
  - 体系层面的逆向攻击咨询能力
- 三，高位能力
  - 安全保障体系设计能力
  - 风险管理架构设计能力
  - 灾难恢复体系设计能力
  - 针对一个包含技术和管理的IT体系，解决其安全问题
  - 构建安全保障体系
  - 等保2.0
  - 网络安全法

### 产业综合治理能力

#### 政策制定

- 一，低位能力
  - 产业分析
  - 行业和安全领域态势分析
- 二，中位能力
  - 治理结构设计
  - 多干系方博弈体系设计和调整

#### 安全理念

- 三，高位能力
  - 共筑网络安全世界
  - 互联世界 安全第一
  - 数据驱动安全
  - 协同联动，共建安全+命运共同体
  - 人是安全的尺度
  - 安全从0开始

### 产品开发能力

- 一，低位能力：分析代码的安全性
- 二，中位能力：安全BUG发现，分析程序设计安全性
- 三，高位能力：安全代码构建，安全开发生命周期管理

### 安全编程能力

- 一，低位能力：能识别代码的安全性
- 二，中位能力：能发现问题，并提出有效的解决方案
- 三，高位能力：代码安全保障体系构建，安全开发生命周期管理



6000-8000元/月收入

## 专业知识

网络技术、计算机语言、协议分析  
应用软件、各类操作系统  
身份鉴别认证、密码学  
Web安全、移动安全、恶意代码  
大数据应用、虚拟化技术

## 工作常识

项目管理、工作汇报  
邮件会议注意事项、职业着装  
职业礼仪

## 专业技能

安全产品集成、产品策略优化  
风险评估、等级保护测评  
流量分析、日志分析、SOC运营  
安全应急处置、业务连续性保障  
渗透测试、安全配置加固

## 个人素质

领导力、团队管理  
协同、沟通、表达  
形象、气质  
学习能力、逻辑分析





## 目录

实战安全运营人才需求

# 安全人才实训基地建设和培养方式

校企合作支撑网络空间安全专业建设





## 教师与实践脱节

- 新知识欠缺
- 缺少实践
- 跟不上行业趋势



## 教材与实践脱节

- 知识体系不系统
- 人才培养针对性不强
- 实验内容不配套



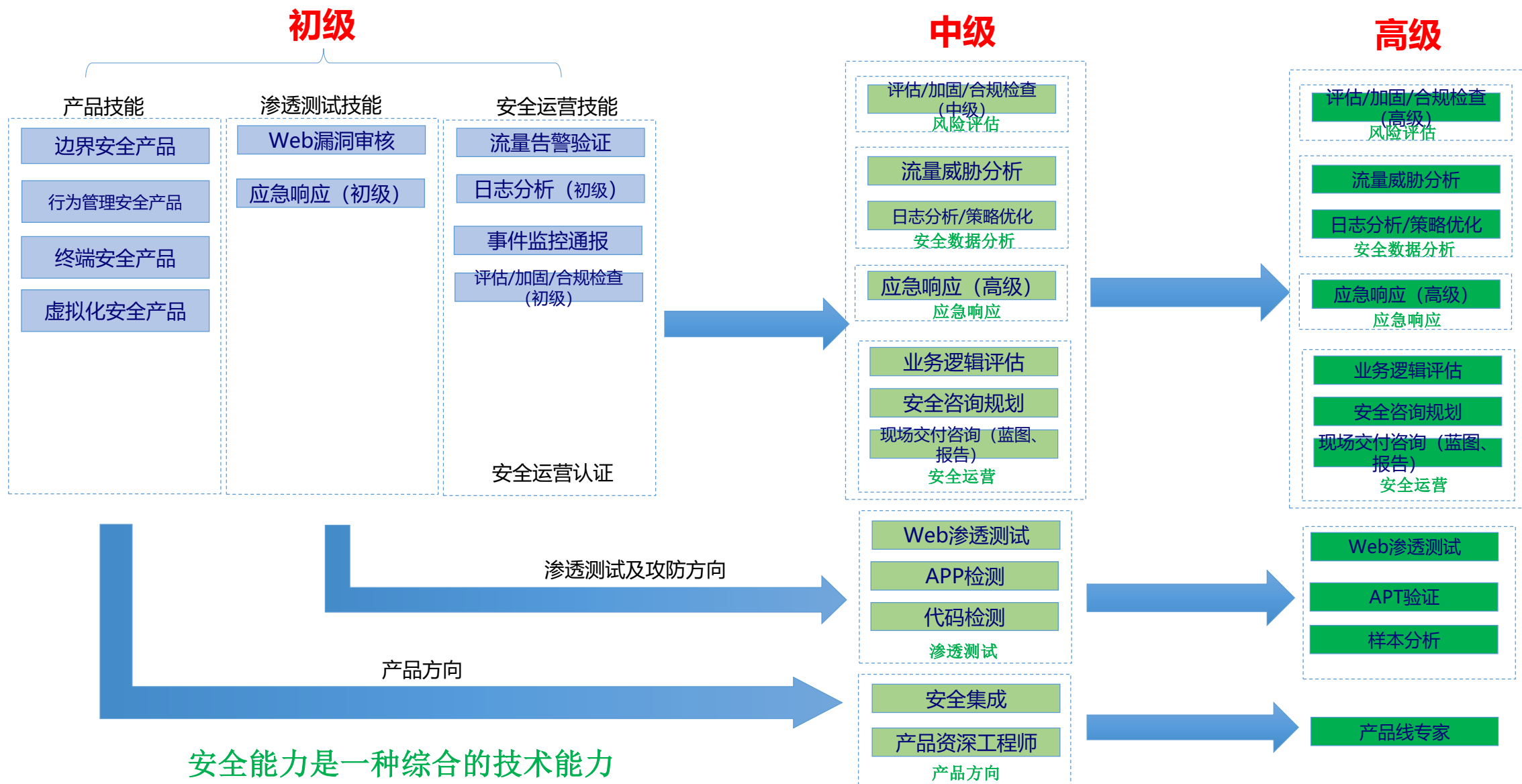
## 实验与实践脱节

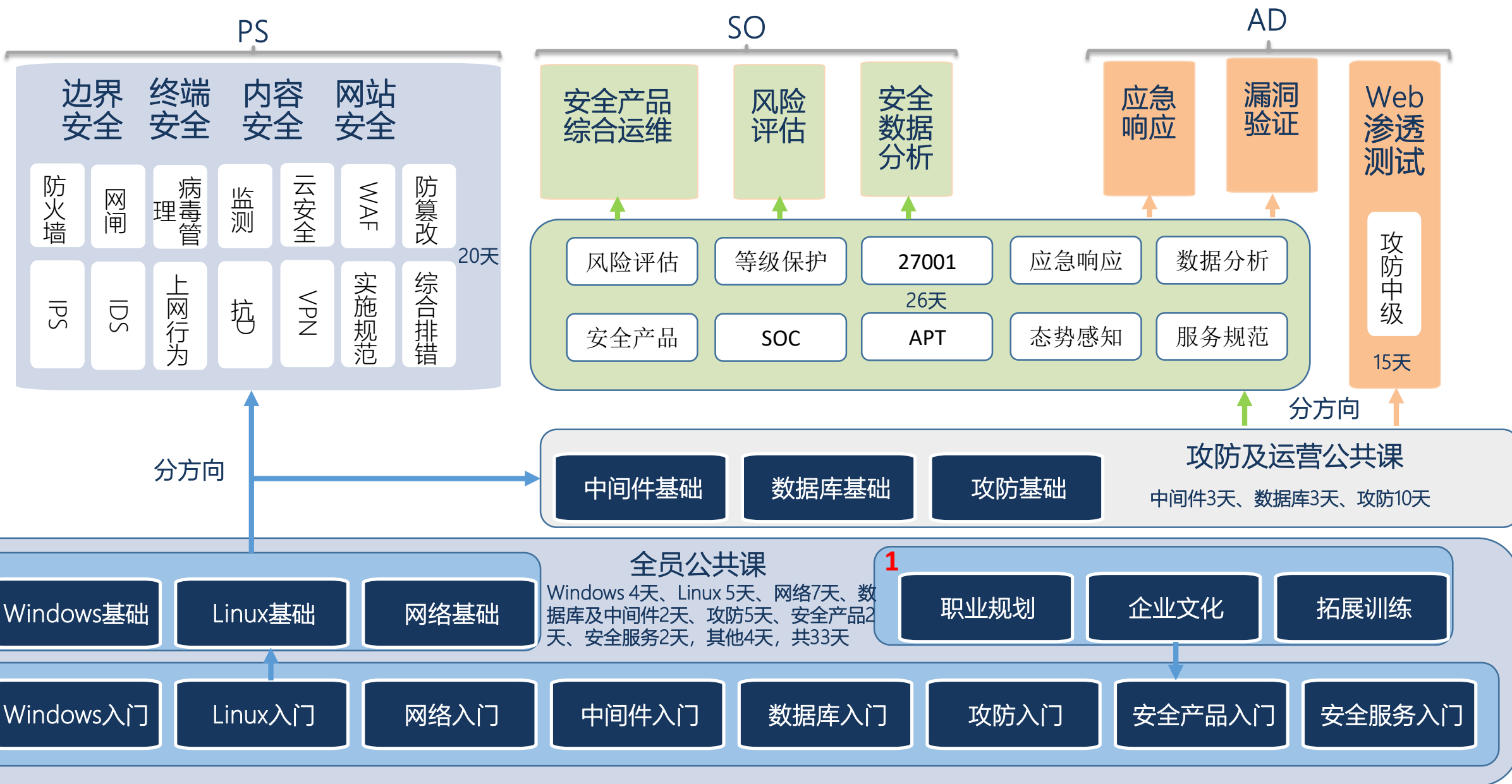
- 实验环境不适用
- 缺乏实验开发环境
- 实验效果难评估



## 实习就业与应用场景脱节

- 实习公司不匹配
- 实习场景脱节
- 就业岗位不匹配







企业办公网安全			网站群安全			数据中心安全			
企业办公网概述			网站群概述			数据中心概述			
企业办公网面临的安全问题			网站群面临的安全问题			数据中心面临的安全问题			
企业办公网安全解决方案和关键技术			网站群安全解决方案和关键技术			数据中心安全解决方案和关键技术			
部署域控补丁服务器	域、域树、域林	信任关系、活动目录	网站数据泄露事件	web安全概述	OWASP常见漏洞	安全域划分	安全域划分概述	网络安全体系设计	
	活动目录	补丁服务器		HTTP协议	XSS漏洞		安全域划分原则	VLSM技术	
	创建配置活动目录	账户管理		远程文件包含漏洞	本地文件包含漏洞		安全纵深防御	CIDR技术	
	域和补丁服务器	策略管理		文件处理漏洞	SQL注入漏洞		安全域规划	安全域划分与实现	
杀毒软件系统	终端安全概述	杀毒应用场景	网站（Windows）系统应急响应事件	网页木马介绍	windows系统介绍	边界访问控制	边界访问控制概述	边界访问控制技术	
	杀毒软件产品介绍	升级管理、防病毒管理		windows下应急工具	应急响应流程		安全功能应用	边界访问控制设备	
	服务端、客户端部署	漏洞管理和策略管理		文件分析	进程名称分析		设备部署	日志分析	
				系统信息调查	网站后门排查		访问控制策略	设备升级与管理	
部署准入控制系统	终端准入产品介绍	准入流程和技术手段	网站（Linux）系统应急响应事件	linux下应急工具	系统信息调查	主机安全防护	操作系统安全	操作系统攻击技术	
	终端应用场景	终端桌面管理		文件和进程分析	应急事件处置		漏洞扫描漏洞修复	恶意代码防护	
	控制中心、客户端部署	准入控制		后门排查	日志分析		安全配置核查	补丁升级	
路由交换	路由技术	交换技术	网站WAF安全防护	web系统安全概述	web应用防火墙	数据保护	数据防泄漏	数据加密	
	网络IP	访问控制		Web应用防护	HTTP校验和访问控制		数据容灾系统	数据抗抵赖性	
上网行为管理	上网行为产品介绍	设备部署	网站篡改安全	web应用防火墙部署	策略有效性验证				
	用户管理	全局配置、上网管理		升级与管理	策略配置				
	流量管理	系统管理和监控		网页篡改的原理	常用的网页篡改方法				
				网页篡改方法技术	防篡改系统部署				
				策略配置日志分析	策略有效性验证				
				防篡改升级与管理	防篡改系统问题排查				

### 团队破冰

1, 职场生涯第一课

2, 拓展训练

1-2天

### IT基础理论课程

- 1, 网络基础课程
- 2, Linux基础课程
- 3, 数据库基础课程
- 4, 语言基础课程
- 5, 网络空间安全基础

3-7天

第8天  
第一次考核淘汰  
2/50淘汰

### IT基础实训课程1

- 1, 仿真实训环境介绍
- 2, 网络实训课程
- 3, linux实训课程
- 4, 数据库实训课程
- 5, 计算机语言实训课程
- 6, Office办公软件

9-18天

第19天  
第二次考核淘汰  
2/48淘汰

### IT基础实训课程2

- 1, 网络实训课程
- 2, linux实训课程
- 3, 数据库实训课程
- 4, 计算机语言实训课程

•第20-27天

第28-29天  
第三次考核淘汰  
2/46淘汰

### 基础攻防实践 第30-46天

- 1, 入侵类型和阶段
- 2, 信息搜集、漏洞扫描
- 3, 病毒蠕虫
- 4, 木马后门
- 5, 系统渗透
- 6, 缓冲区溢出
- 7, 密码加密破解
- 8, 网络嗅探
- 9, 决绝服务和社会工程
- 10, 会话劫持
- 11, 攻击WEB应用
- 12, SQL注入和XSS跨站
- 13, 日志分析和擦除
- 14, 综合渗透测试

第46-48天  
第四次考核淘汰  
2/46淘汰

### 安全产品实践 第49-62天

- 1, 防火墙技术和实践
- 2, 负载均衡产品技术和实践
- 3, IDS/IPS技术和实践
- 4, 扫描器产品技术和实践
- 5, WAF产品技术和实践
- 6, 上网行为管理产品技术和实践
- 7, 数据库审计产品技术和实践
- 8, 杀毒软件产品技术和实践
- 9, 终端管理网络准入产品技术和实践
- 10, SOC产品技术和实践
- 11, 产品销售和售前规范技能
- 12, 产品测试和售后规范技能

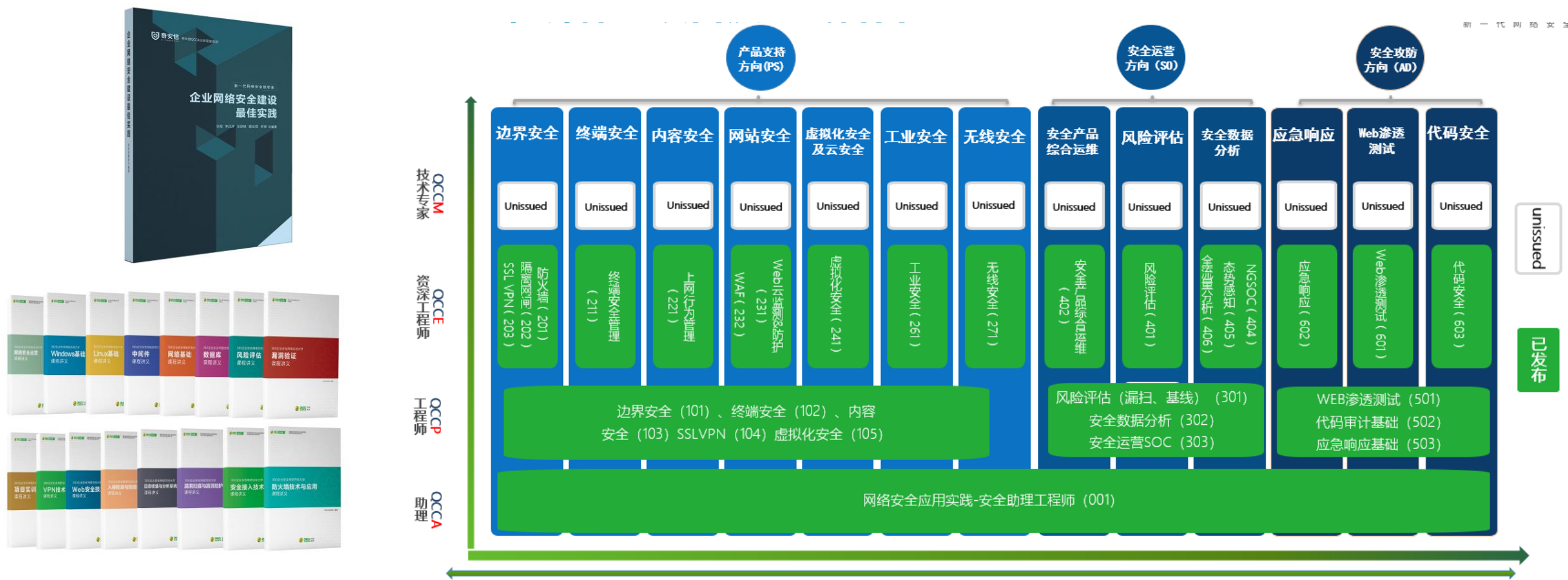
第63-66天  
第五次考核淘汰  
2/42淘汰

### 安全服务和运维实践 第67-77天

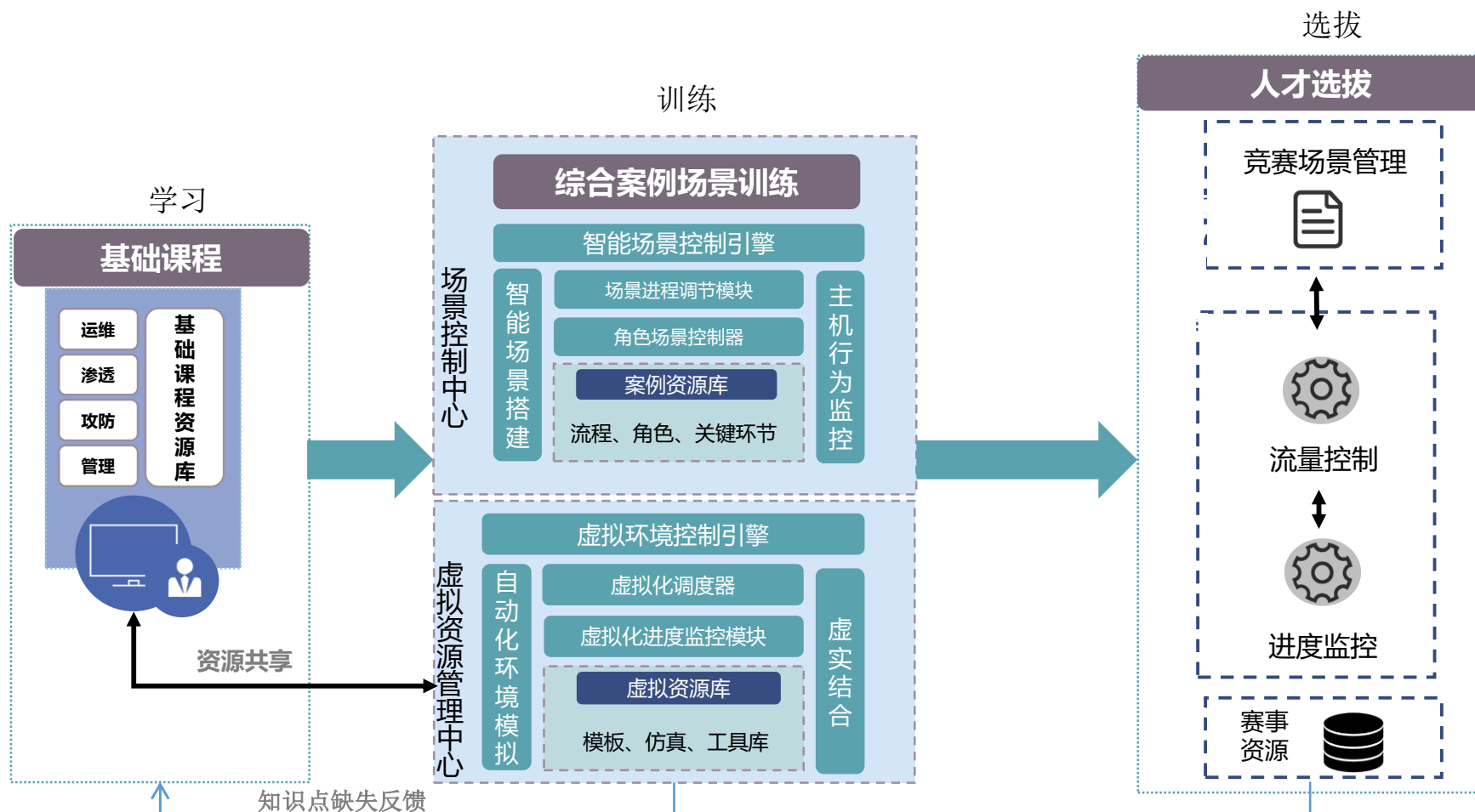
- 1, 网络安全域和访问控制策略
- 2, 安全体系和架构
- 3, 信息安全风险评估
- 4, 安全加固和风险处置
- 5, 等级保护合规要求
- 6, 安全运维工作实践
- 7, 安全态势感知平台参观实践
- 8, 安全应急体系和应急处置

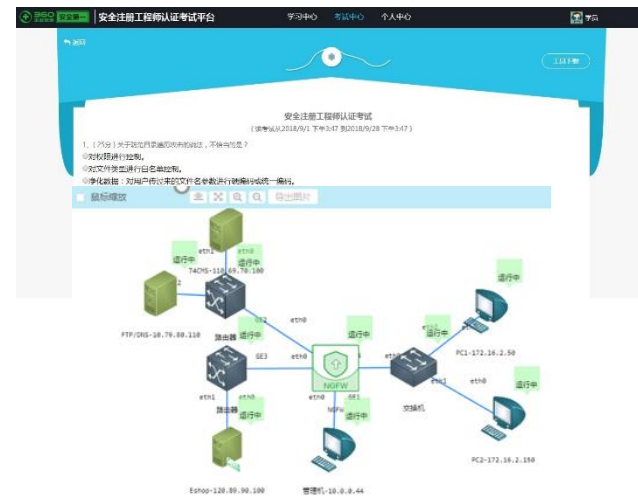
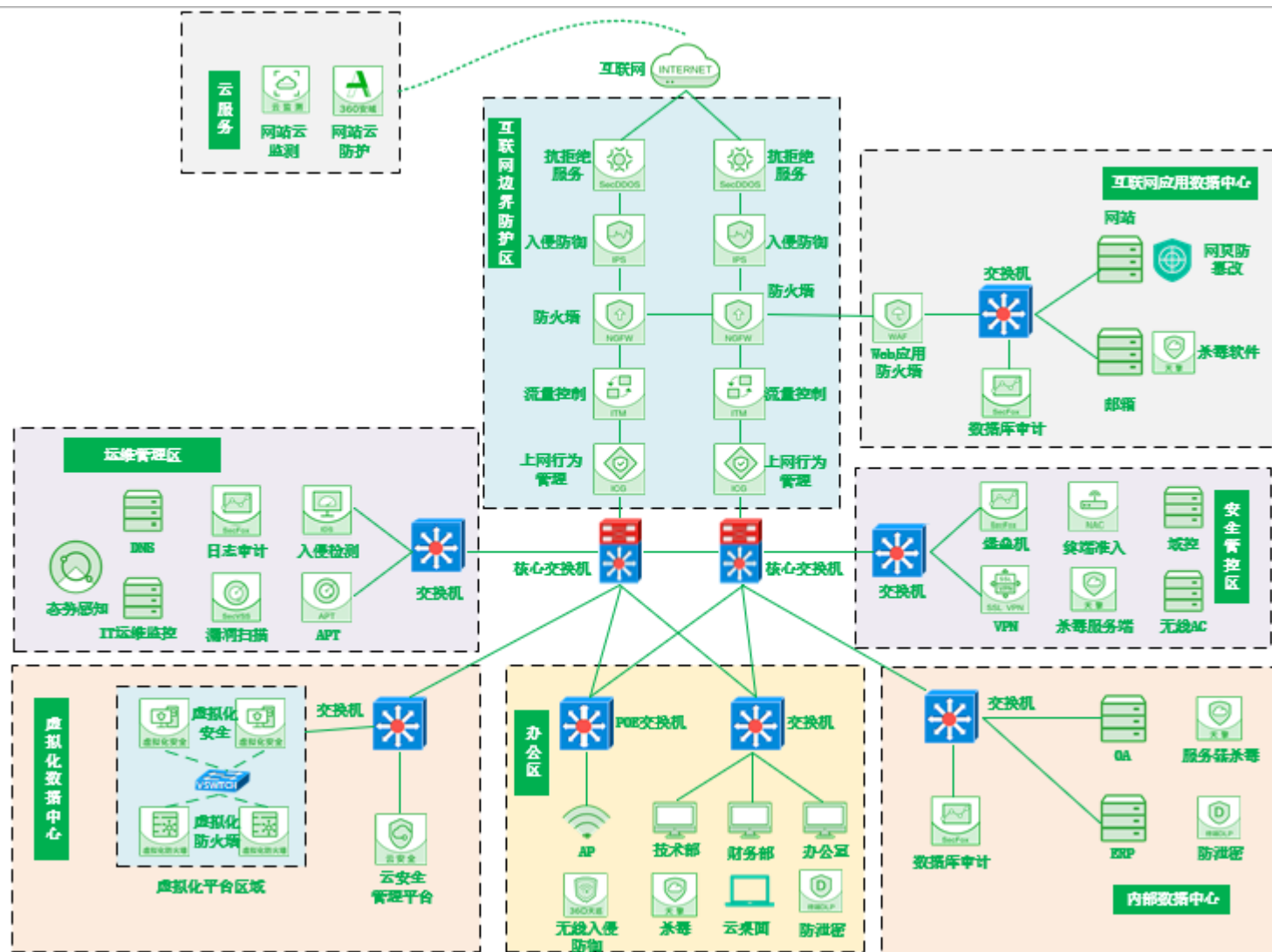
认证特点：以安全理念、安全方案、安全产品为主，分为3个方向3个等级，用于培养、选拔、鉴别安全工程师的技术水平和能力

认证配套：16套培训教材、安全实训教学产品、安全认证考试产品、特定安全仿真场景



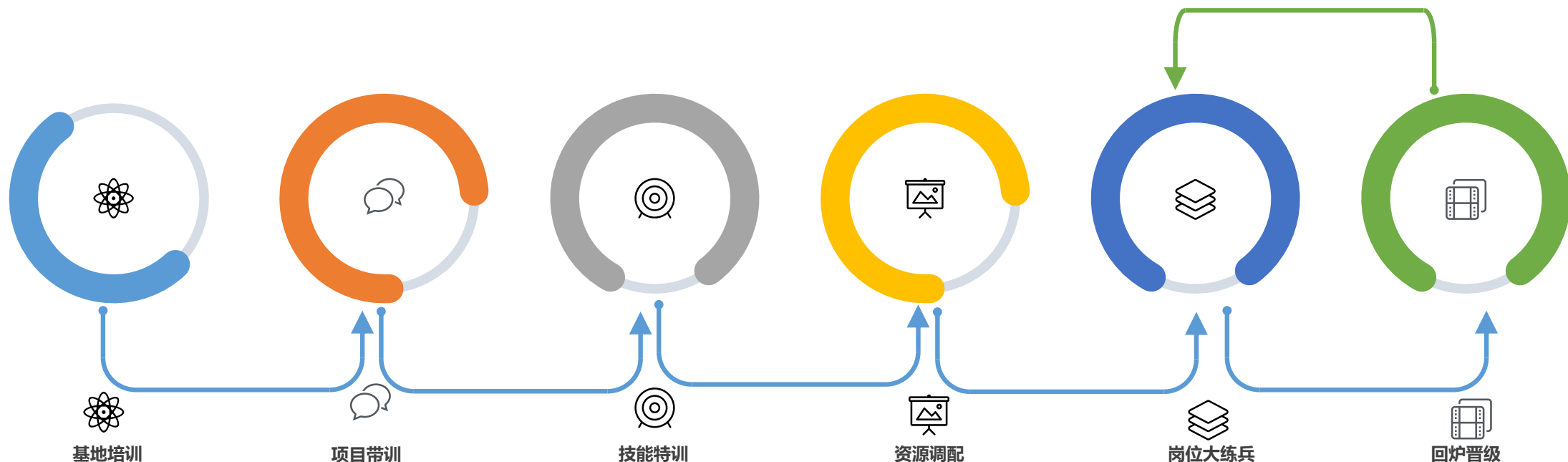






- 基于绝大多数政企业单位IT系统架构
  - 办公网仿真场景
  - 网站群仿真场景
  - 数据中心仿真场景
- 动态背景流量和安全事件脚本
  - 实训教学为主，理论教学为辅
  - 侧重于体验式教学模式

# 项目实训、带训、特训、回炉提升的流程



- 达到教学大纲要求水平;
  - 输出基地培训课程大纲;
  - 基地课件质量标准评定;
  - 讲师资源协同和素质评估;
  - 考核标准参加评定;
  - 考务基本要求;
  - 技能培养 (前置课程)。
- 完成知识到技能转变;
  - 对接认证和基地确定带训资格;
  - 带训人员分配干系事件;
  - 带训质量控制 (日报、周报、期中、期末、指导手册、管理办法);
  - 确定入职资格交付给招聘组。
- 完成学生到职场人的转变;
  - 资源准备 (课程、人员、物料、后勤);
  - 教学过程质量控制和调整;
  - 课程质量控制和结果反馈;
  - 培训复盘和改进计划。
- 需求管理包括头部模式、行业需求、普通需求、撤换场需求 (到期和中期);
  - 供给管理包括人员数据维护和人员各种相关权限开通;
  - 资源池人员管理包括日报、周报、考勤管理;
  - 倚天系统流程梳理
- 使DE能够达到合格安全运维水平;
  - 软技能设计包括软技能分类、内容设计、培训方式;
  - 软技能培训包括每日一练、案例分享;
  - 硬技能
- 对达到既定目标的DE进行综合能力检验和训练使他们能达到新里程碑;
  - 课程设计、课程安排、课件制做;
  - 回炉人员筛选, 达到晋级资格人员
  - 替换流程制定, 确保人员可参加
  - 确定人员达到既定目标检验。



# 实习到上岗的流程

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE



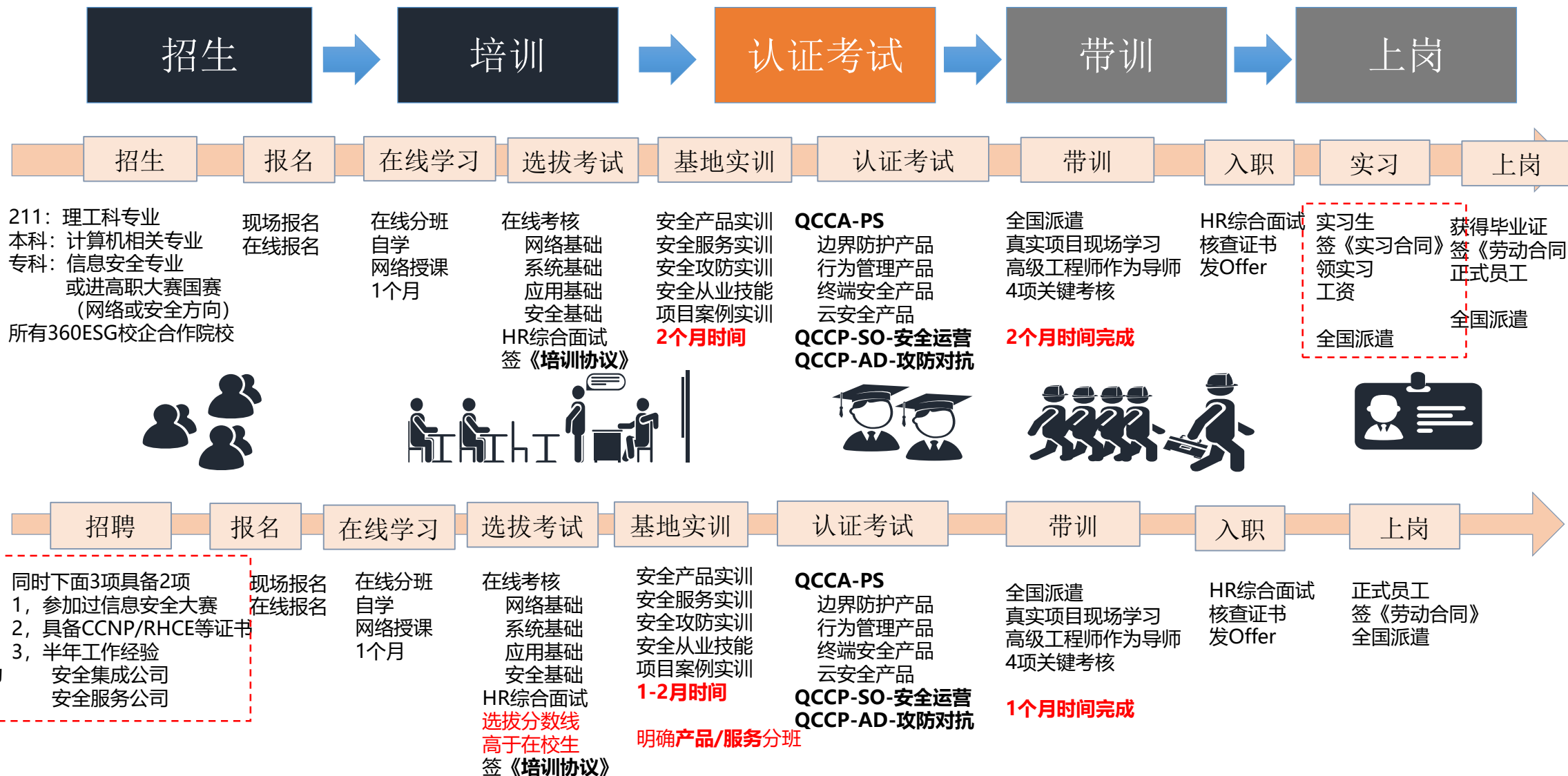
在校生

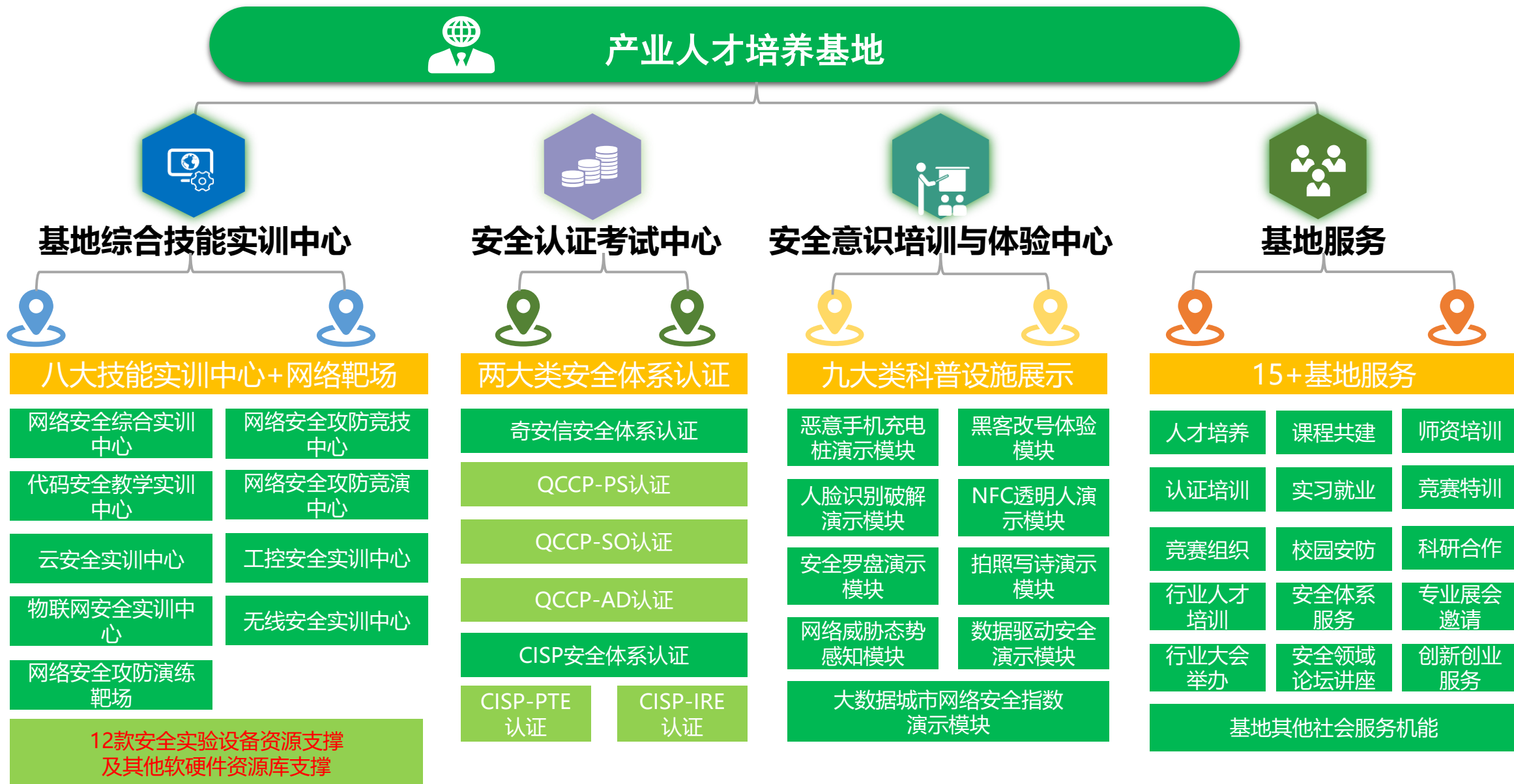
下一年度6月毕业



毕业生

已经毕业  
28岁以下  
半年以上工作经验  
有安全岗位基础能力







# 实战运营人才培养基地一年半累计培养2000人



2000人/30000人





## 目录

实战安全运营人才需求

安全人才实训基地建设和培养方式

校企合作支撑网络空间安全专业建设

# 安全运营人才教育需经历的四大阶段

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE



校企合作/人才培养

岗位能力  
知识体系  
课程设计  
专业教材  
技能训练  
实战演练  
实习就业

学历教育

整体视野

安全运维

渗透测试

安全编程

风险评估

等保测评

专项训练

知识逻辑

QCCE

QCCP

QCCA

认证体系

专业化服务

数据分析

安全检测

实战演习

事件处置

信息通报

专项重保

安全运维

考试培训

安全运营

产品管家 (展现安全建设成果)

安全监察 (威胁响应与回溯)

安全评估 (基础安全服务)

实习实训体验

未来发展



安全运营/专业服务

# 从岗位职责到学历教育课程体系

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

工作任务

技能要求

专业课程

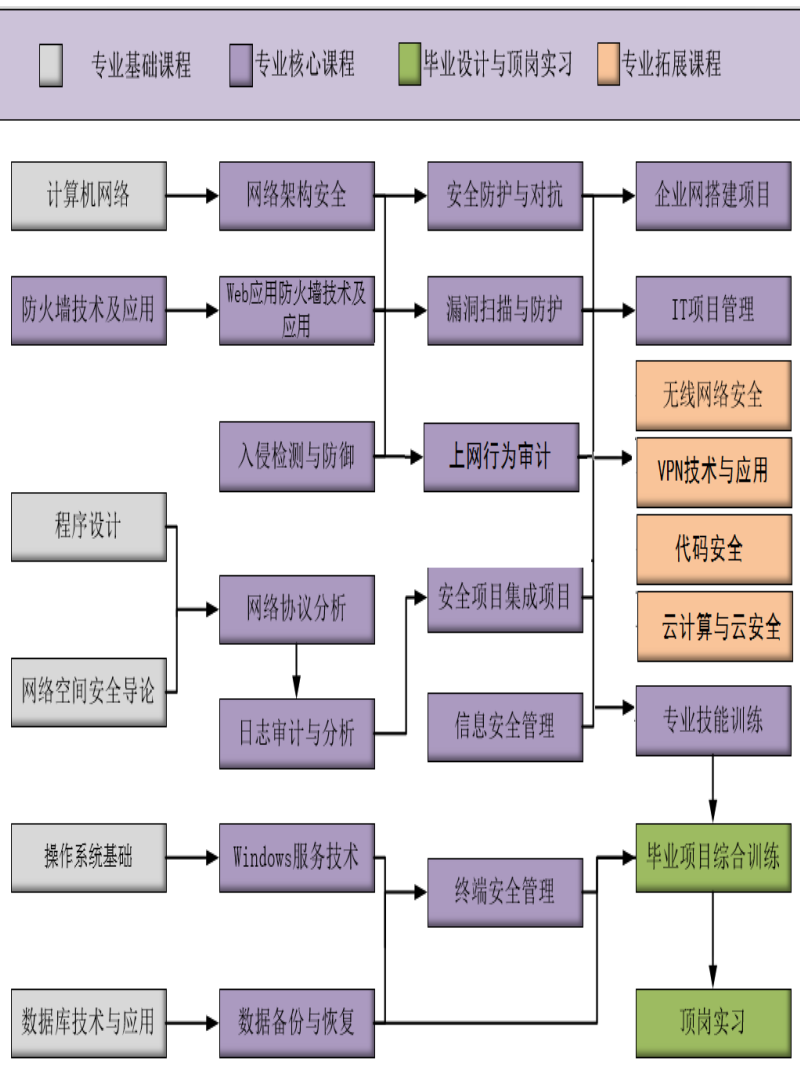
课程演进

表 1: 安全岗位与技能要求 (带\*为专项技能要求)

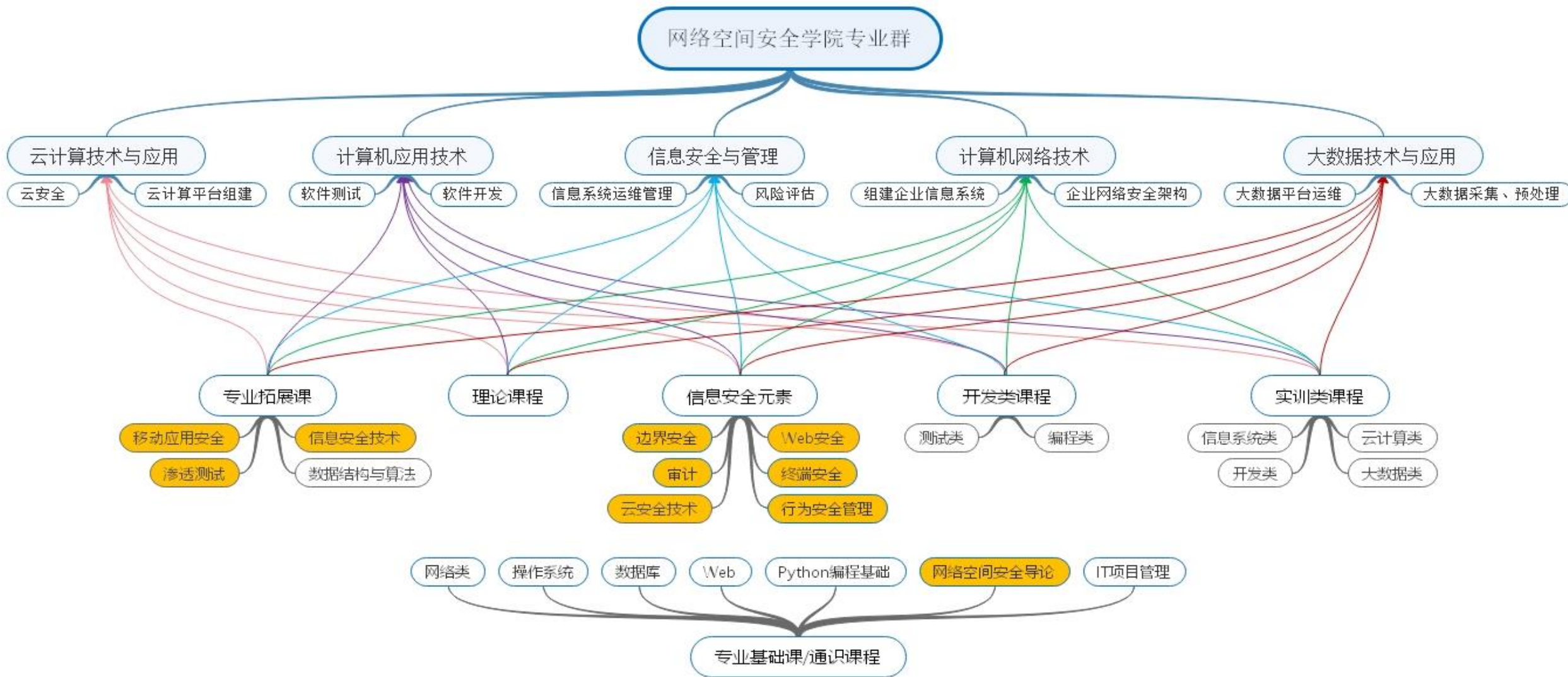
岗位名称	岗位描述	岗位要求	工作过程	网络安全技能要求
网络安全运维工程师	主要参与企事业单位网络的部署、软硬件设备的安装、配置、升级、运行维护与管理, 服务器及安全系统等运行监控与管理, 统计整理运维数据并撰写安全运维技术文档, 以满足网络安全系统安全稳定运行的需要。	设备安装上线 安全策略部署 安全运维管理	1. 安装前设备检验。 2. 遵照网络结构设计布线。 3. 设备安装上电、联网。 4. 基本配置。 1. 安全需求分析。 2. 安全策略制定。 3. 安全策略实施。 4. 安全策略投入使用。 1. 执行安全巡检。 2. 排查可疑事件。 3. 撰写安全巡检报告。 4. 处理安全事件。 5. 提交巡检报告。	1. 网络空间安全法律意识 2. 网络安全意识 3. 计算机编程基础 4. 网络安全技术应用能力 5. 网络连接与传输协议应用能力 6. 操作系统安装与应用能力 7. 病毒与木马分析与防范基础能力 8. 防火墙、漏洞扫描、日志收集、入侵检测、VPN 等安全设备的部署和维护能力 9. 操作系统安全配置能力* 10. C++ 编程能力* 11. 数据库基础能力* 12. 网络安全运维综合实践能力*
Web 安全工程师	对企事业单位网站、信息系统进行安全评估测试及安全加固; 通过安全策略的实施, 防护各种针对网站、数据库为主的应用系统的攻击, 并在攻击发生时进行及时和必要的响应, 将损失降到最低。	风险评估 等级保护 Web 安全加固 应急响应	1. Web 系统资产识别。 2. Web 系统脆弱性识别。 3. 已有安全措施确认。 4. 风险分析。 5. 撰写风险评估报告。 1. 安全定级和备案。 2. 安全规划设计。 3. 安全整改实施。 4. 安全运行管理。 1. 分析渗透测试报告。 2. 编写 web 安全漏洞加固方案。 3. 执行 web 安全加固。 4. 漏洞复测。 1. 事前预防准备。 2. 事中安全检测和事件定位。	1. 网络空间安全法律意识 2. 网络安全意识 3. 计算机编程基础 4. 网络安全技术应用能力 5. 网络连接与传输协议应用能力 6. 操作系统安装与应用能力 7. 病毒与木马分析与防范基础能力 8. 防火墙、漏洞扫描、日志收集、入侵检测、VPN 等安全设备的部署和维护能力 9. 网站建设能力* 10. 网络安全运维与加固能力* 11. 网络协议分析能力* 12. 信息安全等级保护实施的能力* 13. 网络攻防综合实战能力*

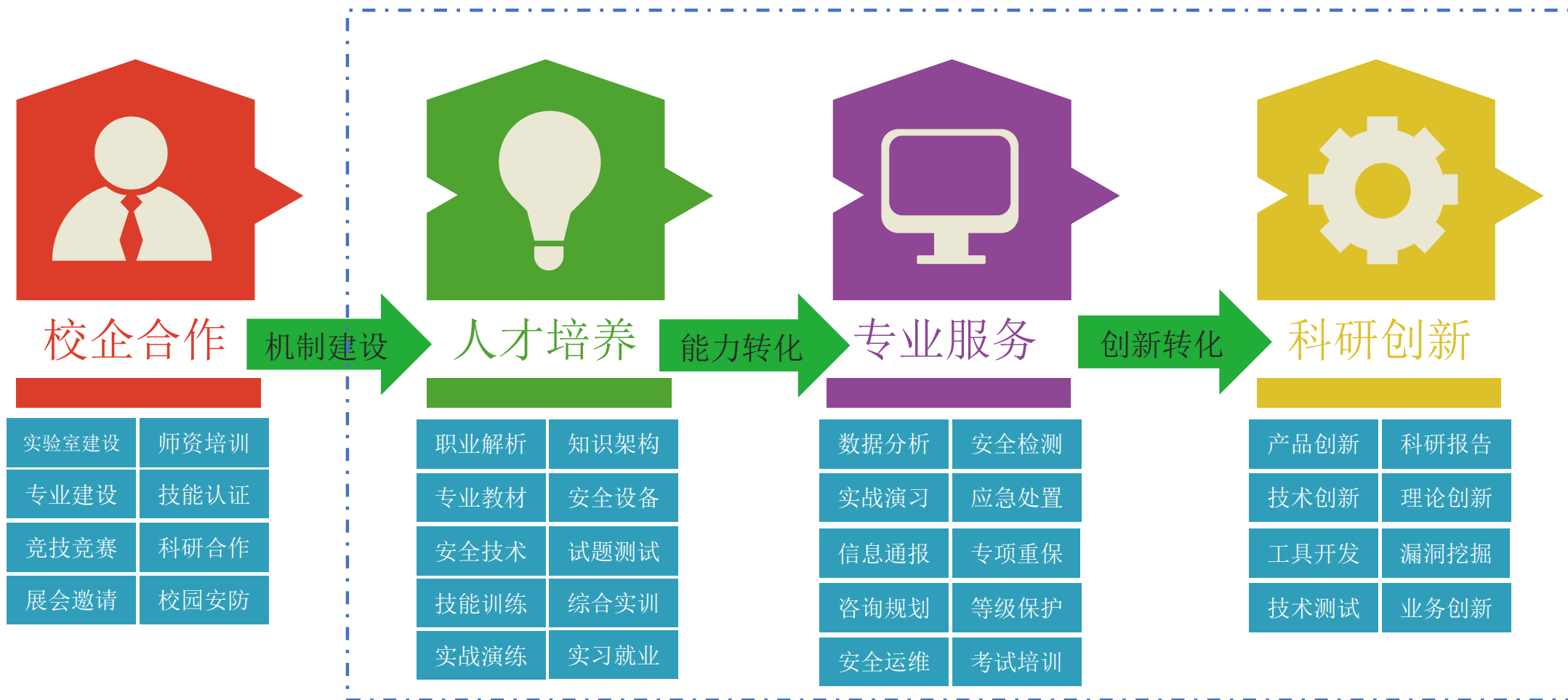
表 2: 网络安全技能与对应课程

类别	技术能力项	技术能力具体要求	对应课程
专业基础能力	网络空间安全法律意识	熟悉网络安全法律法规, 具备网络安全与反欺诈意识, 熟悉网络安全的法律规定和刑事责任; 遵纪守法, 洁身自律	网络空间安全导论
	网络安全意识	了解网络安全常识; 熟悉个人、企业员工的常见网络安全问题和危害; 掌握个人和企业员工的常见网络安全问题防护方法。	网络空间安全导论, 信息安全管理
	计算机编程基础	熟练掌握计算机编程逻辑, 具备独立程序编写能力	计算机导论与程序设计
	C++ 编程能力	熟练掌握 C++ 编程语言, 熟练面向对象编程思维, 能够灵活应用, 完成实际程序需求	C++ 高级语言程序设计, 算法分析与设计, 数据结构
	Python 编程能力	熟练掌握 Python 编程语言, 熟练三方库 (如网络编程等), 能够灵活应用, 并完成实际程序需求	Python 编程, 算法分析与设计, 数据结构
	数据库查询、管理、维护的能力	熟悉常用数据库原理, 掌握常用数据库搭建、基本操作与维护, 熟悉 SQL Server、MySQL、Oracle 数据库及其应用	数据库技术及应用, 数据结构
	网络安全技术应用基础能力	熟悉网络安全技术的应用场景, 体验技术方法、常用工具及岗位操作过程, 学习和掌握从事网络安全工作所必备的基础知识	网络空间安全导论, 网络安全
	网站建设应用能力	熟悉 PHP、JSP、ASP、HTML 等常见开发语言基础, 熟悉常见网站架构, 掌握网站开发和搭建能力	Web 开发技术基础
	网络连接与传输协议应用能力	计算机网络通信的基本原理、网络体系结构、组建局域网技术、Internet 及其应用、计算机网络安全和常用网络操作系统。	计算机网络
	操作系统安装与应用能力	熟悉 windows 和 Linux 操作系统原理, 掌握基础服务搭建, 基本操作和使用命令	操作系统









通过**校企合作**的方式，加强网络安全专业建设及**人才培养机制**，结合奇安信集团的技术实力和场景的实践经验，设计课程体系，采用理论和实践相结合的教学方式，培养学生专业知识和实践能力，使学生毕业后具备一定的安全咨询、技术支持、安全运维等场景下的专业**安全服务及运营**能力和科研思维。

## 基础阶段:

- 操作系统基础
- 网络基础
- 数据库基础
- 编程基础



30天 (线上)

1

## 网安入行

- 行业认知/就业环境/职业规划
- 网安法律法规和标准解读



1-3天 (线下)

2

## 网安核心课

- 信息安全技术和管理体系
- 信息安全渗透测试攻防技术
- 网络安全新技术
- 网安教学工具应用



4天-8天 (线下)

3

## 专业核心课

- 信安专业核心课  
防火墙/漏洞扫描  
上网行为管理/终端安全/WAF
- 云计算专业核心课
- 大数据专业核心课



15-20天 (线下)

4

## 企业安全项目实践

- 办公网安全实践
- 网站群安全实践
- 数据中心安全实践



5天-10天 (线下)





## 人才培养

- 应用型人才培养方案
- 拔尖人才的培养环境



## 课程体系建设

- 课程体系推荐与设计



## 师资培训

- 针对学校教师的培训



## 实验室建设

- 产品和技术支持
- 提供实验室运营建议



## 实习就业

- 针对教师的项目锻炼机会
- 针对学生的实习就业推荐



## 竞赛支撑

- 协助学校举办或参与安全竞赛



## 能力认证

- 对于发布后的CISP和企业认证, 导入到学校的培训体系中



## 科研合作

- 对于有科研实力的院校进行研发合作或项目合作申请




## 专业展会邀请

- 每年ISC专业安全会议的优先邀请和参与



## 校园安全防护

- 校方优先选择奇安信作为校园网络安全防护建设方

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE