中国奥委会官方赞助商

探索教育数字化转型背景下的

网络安全人才培养新模式

奇安信教育行业部 朱燕飞

2023-05-19

目录

1

网络安全产业人才需求调研报告

产业急需懂攻防、懂运营的实战型网络安全人才

数字化战略行动，网络安全是基础工程

- “新基建”将深远的影响产业变革，形成新的生产方式、产业形态、商业模式，同时也带来新的风险和挑战。
- 云、大数据、物联网、移动应用、5G、智能制造等新技术的应用也引入了更多风险，攻击面呈几何级数增长。

- 国家级APT攻击愈演愈烈
- 美国大选邮件门
- 乌克兰电网攻击
- 震网Stuxnet 攻击伊朗核电站
- 勒索软件攻击美国最大石油管道公司

- 勒索蠕虫影响多国的政府机构、医疗、公共服务等设施；
- 国内多次大规模数据泄漏；

- 勒索病毒使得台积电、车企等企业停工；
- 多国银行因SWIFT攻击遭受数亿美元损失；

国家安全

社会安全

经济-生产安全

近年网络威胁的变化：

- ✓ 勒索攻击
- ✓ 有组织的高级持续性威胁（APT）
- ✓ 软件供应链攻击
- ✓ 社会工程攻击
- ✓ ……

数字化时代网络安全内涵的转变：

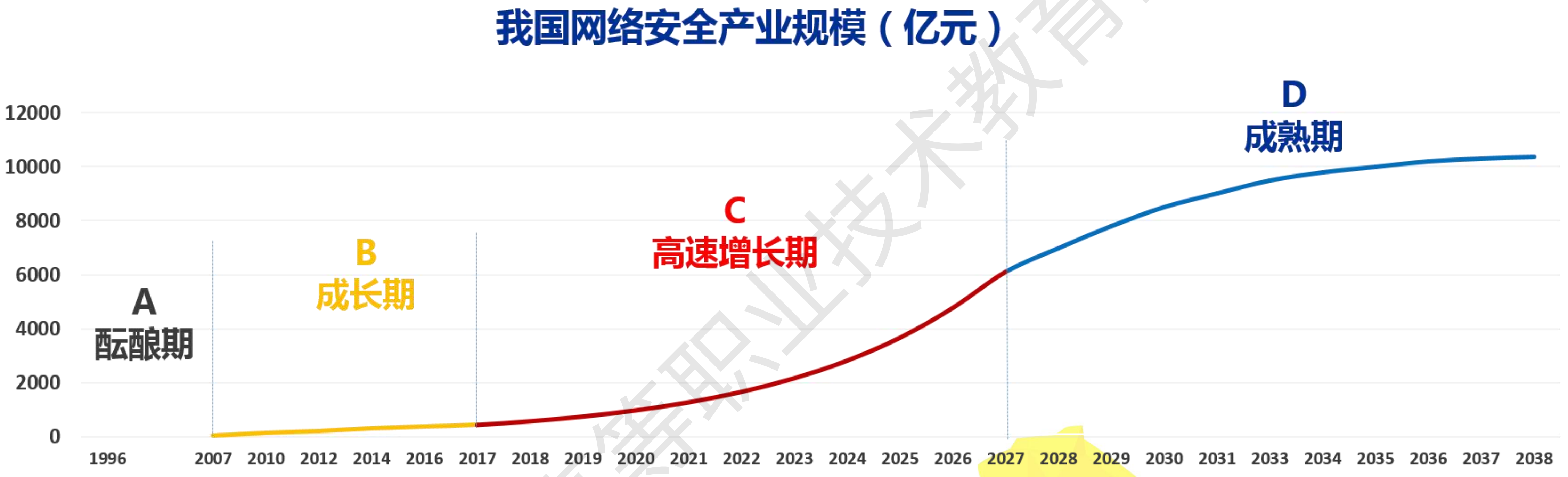
从 网络与信息安全 到 业务运营与生产安全；

安全焦点从 以网络为中心 到 以数据和业务为中心；

“非传统安全”对“传统安全”的影响；

2032年国内网络安全市场将达万亿级规模

中国奥委会官方赞助商



A：1996-2007年

网络安全从无到有

十年发展至56亿

B：2007-2017年

$(1+23\%)^{10}$ ×56亿=450亿

平均年复合增长率为23%

十年发展至450亿

C：2017-2027年

$(1+30\%)^{10}$ ×450亿=6210亿

高速增长期，以年复合增长率30%计

2027年市场将超6000亿

D：2027年-未来

$(1+10\%)^{5}$ ×6210亿=10000亿

市场成熟期，以年复合增长率10%计

2032年将达万亿级规模

网络空间的竞争，归根结底是人才竞争

中国奥委会官方赞助商

奇安信

培养网信人才，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院。

— 习近平

网络安全人才市场状况研究

奇安信

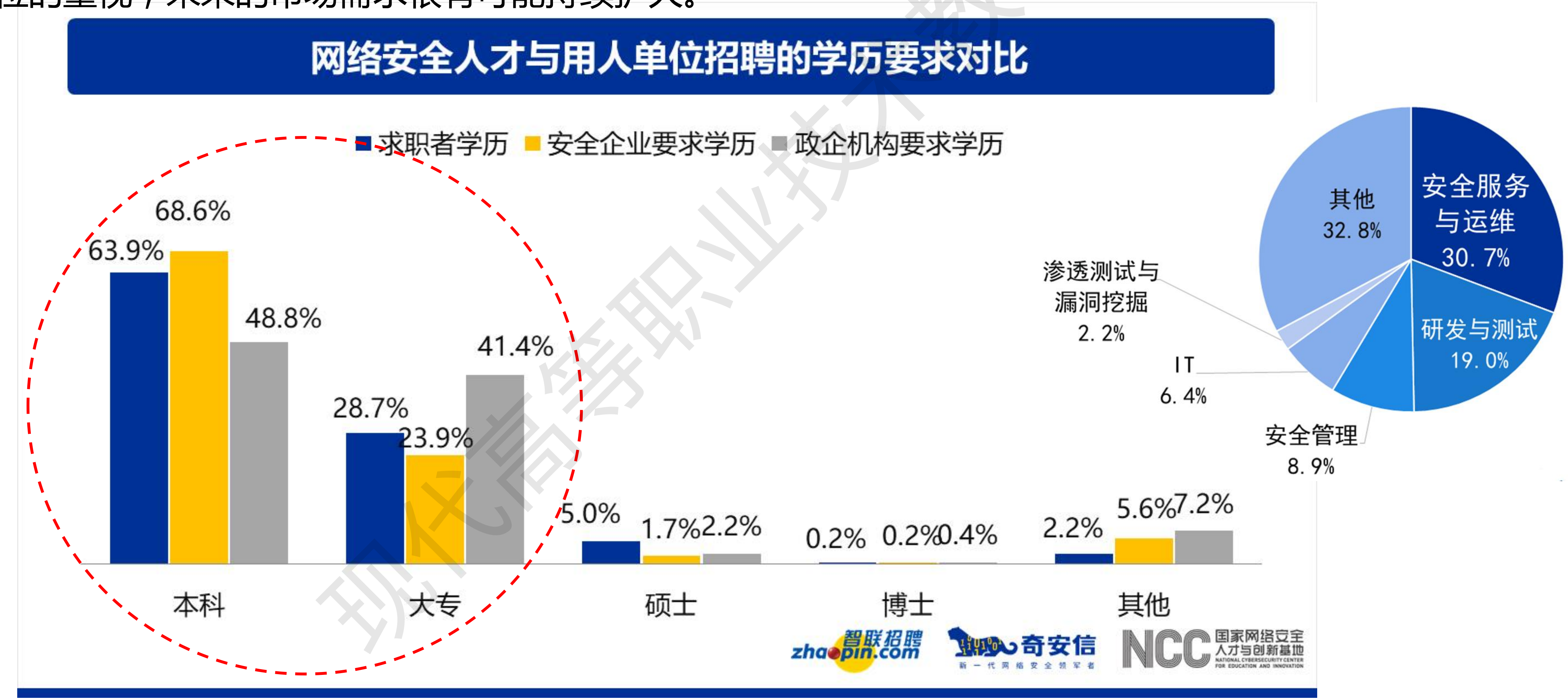
中国奥委会官方赞助商

自2017 年开始，智联招聘与奇安信行业安全研究中心展开联合研究，每年发布《网络安全人才市场状况研究报告》，对安全人才的招聘需求与求职简历进行分析。在需求变化、供需结构、用人单位特点以及人才自身特征等多个方面对网络安全人才市场现状展开了全面、深入的研究。

网络空间安全人才市场需求

奇安信 BEIJING 2022 北京2022年冬奥会官方赞助商 Official Sponsor of the Olympic Winter Games Beijing 2022

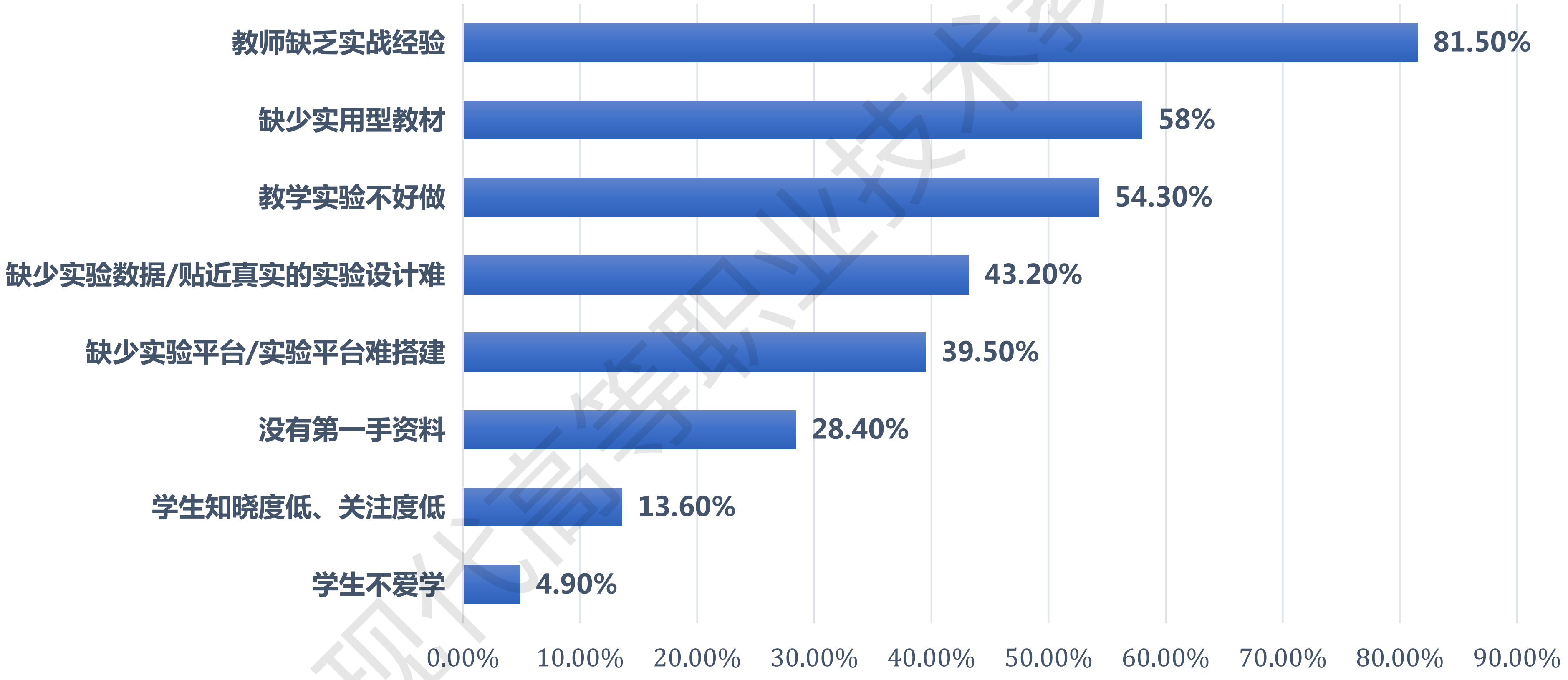
安全服务与运维类的岗位需求大幅增长，成为政企机构招聘最多的岗位类型，占比高达30.7%，首次超过研发测试岗位。随着，政企机构安全建设水平的提升，安全运营与服务越来越受到用人单位的重视，未来的市场需求很有可能持续扩大。



《2020网络安全人才市场状况研究报告》

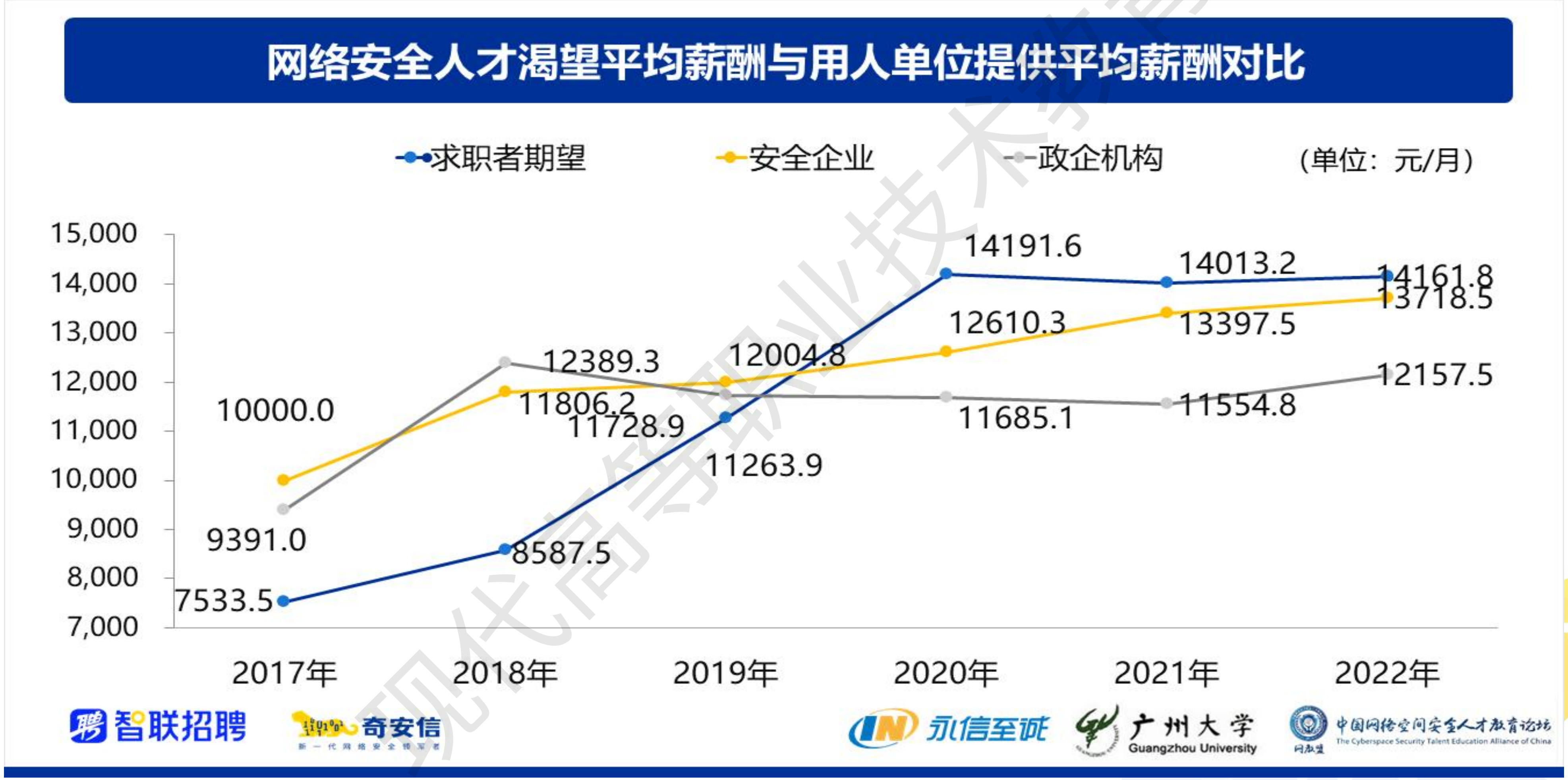
65所高校学科建设负责人的调研报告

老师视角：实战型网络安全人才“难”培养的因素排行



数据来源：《2018年网络安全人才市场状况研究报告》

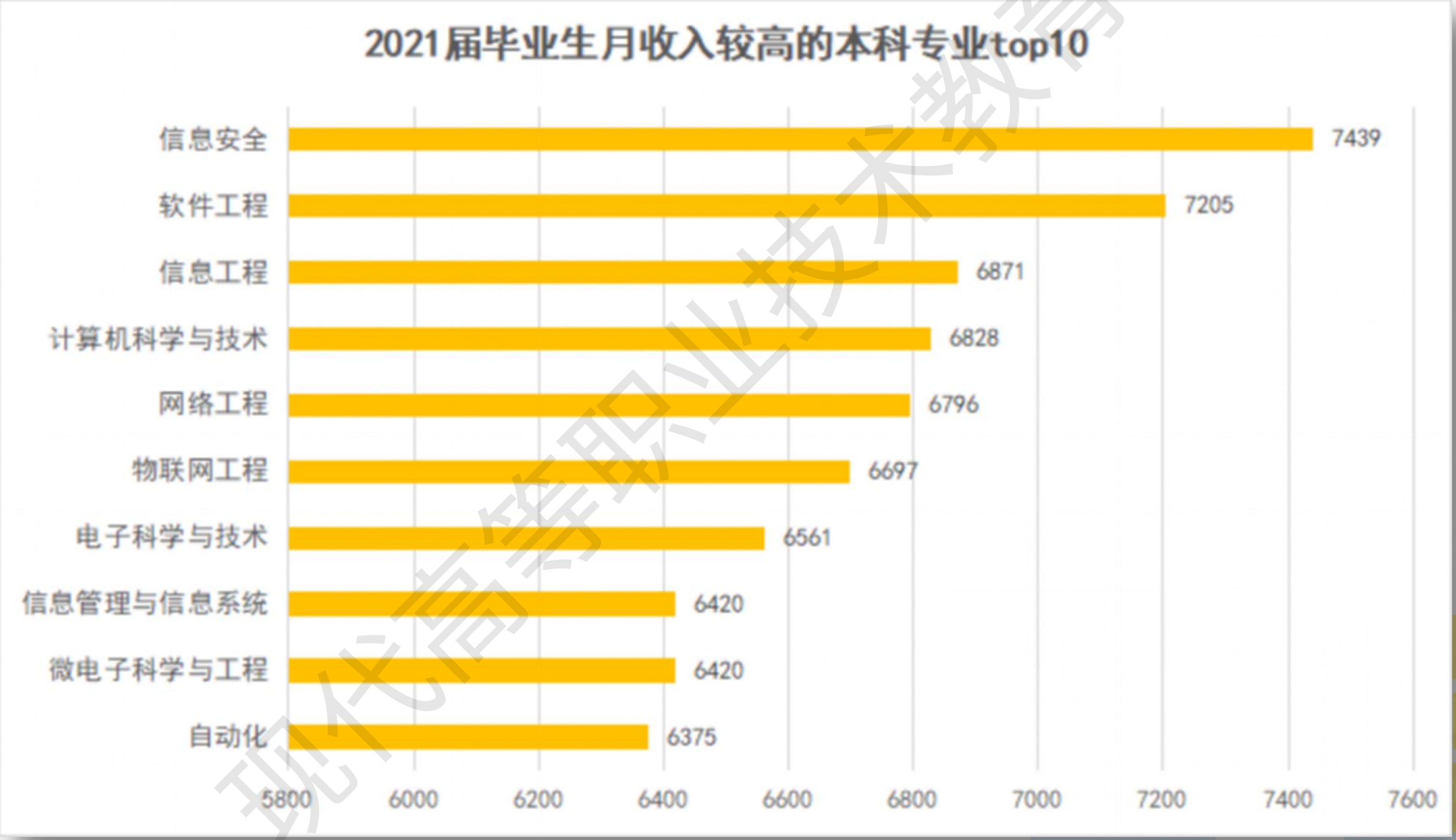
我国网络安全产业人才需求情况



《2022网络安全人才市场状况调研报告》

大学毕业生月收入最高的10个专业

中国奥委会官方赞助商



《2022年中国大学生就业报告》

2 网络安全人才培养理念及方案

深度产教融合的实战化人才培养闭环

网络安全工程师能力全景图

奇安信
中国奥委会官方赞助商

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

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

产教融合人才培养的目的：把人送到产业和岗位上去

奇安信

中国奥委会官方赞助商

主要培养方向

（>95%能力覆盖）：

✓ 安全运维工程师
✓ Web安全工程师
✓ 安全服务工程师

次要培养方向

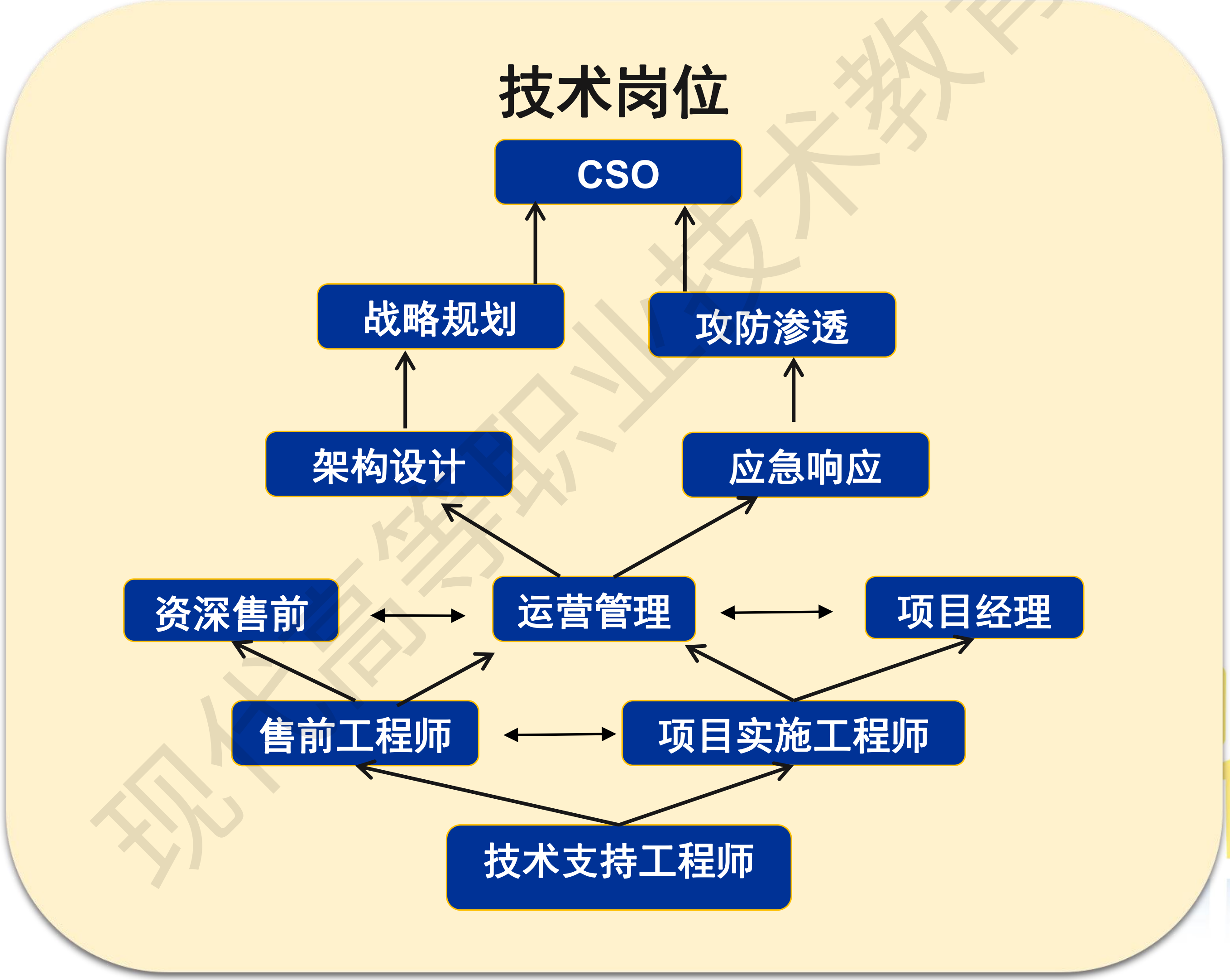
（>60%能力覆盖）

✓ 售后工程师
✓ 售前工程师
✓ 安全产品销售等

其他培养方案

（>20%能力覆盖）

✓ 产品规划岗位
✓ 产品研发岗位
✓ 安全测试岗位



✓ 信息安全咨询顾问
✓ 首席安全专家
✓ 安全审计工程师
✓ 首席安全官
✓ 安全讲师

✓ 代码安全
✓ 云安全
✓ 物联网安全
✓ 工控安全

由”互联网+”到”安全+”

✓ 安全+互联网
✓ 安全+人工智能
✓ 安全+大数据
✓ 安全+AI
✓ 安全+电子取证
✓ 安全+……

网络安全人员能力成长的四大阶段

奇安信
中国奥委会官方赞助商

人培方案
课程体系
专业教材
实验实训
岗位知识
产业场景
实战演练

渗透测试
安全编程
交付运维
风险评估
等保测评
商密评估
关基测评

技术评价
综合评价
QCC认证
CISP-PTE
CISP-IRE
其他认证

工程实践		产业实践
交付运维	信息通报	**产品管家**（展现安全建设成果）
数据分析	安全监测	**安全评估**（基础安全服务
安全咨询	安全运营	**安全监察**（威胁响应与回溯）
事件处置	应急响应	**国家级网络攻防实战演习**

科研合作

学历教育 **专项训练** **知识逻辑** **能力验证**

方案重构 **知识合成** **安全评价** **实践同构**

从人才培养到服务产业到创新创业的深度产教融合

教学实训

实验室建设　师资培训
专业建设　技能认证
竞技竞赛　科研合作

产教融合
职业转化

就业培养

职业解析　知识架构
专业教材　安全设备
安全技术　试题测试
技能训练　综合实训
实战演练　实习就业

产业赋能
能力转化

产业服务

数据分析　安全检测
实战演习　应急处置
信息通报　专项重保
咨询规划　等级保护
安全运维　考试培训

成果转化
创新转化

科研创新

产品创新　科研报告
技术创新　理论创新
工具开发　漏洞挖掘
技术测试　业务创新

旧

校企合作

学校　企业

设备、教材、案例

校企合作

- 学校主体，企业参与
- 调整人才培养方案

新

产教融合

学校——进入产业，在真正的产业环境中培养人

企业——参与教学运营，将业务带进学校

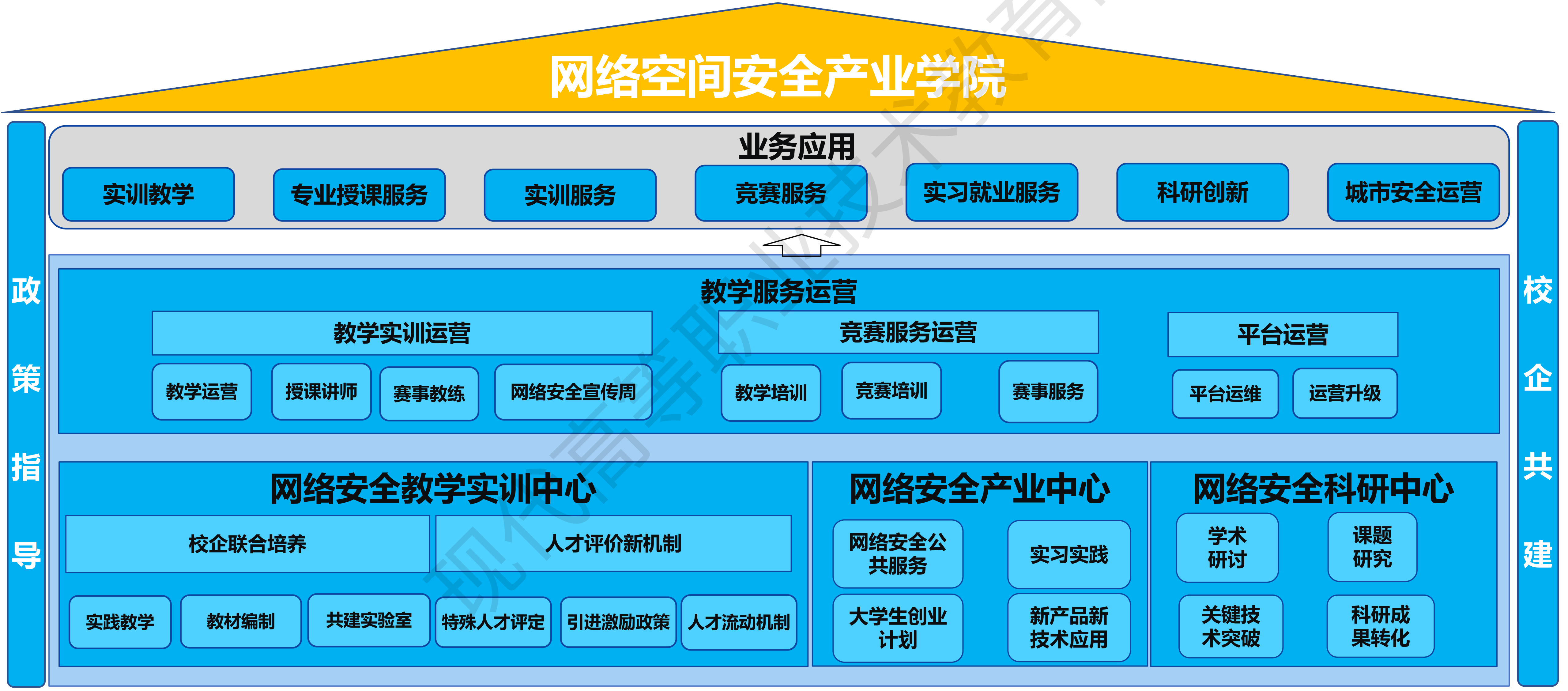
产教融合

- 企业、学校双主体
- 同构产业实践体系

学校要融入产业，学生在校期间就要能够服务产业。学生进产业、老师进产业、学校进产业。

网络空间安全产业学院框架设计

奇安信
中国奥委会官方赞助商



第一阶段、网络空间安全学院—专业教学能力建设

主要完成人才培养方案、实训教学环境、教学资源库建设，师资体系建设，实验平台建设，认证体系建设。

专业化人才培训
完备化课程体系
学科建设
网络安全人才培养

卓越仿真资源库体系
仿真资源库
靶场资源环境

虚实结合测试
安全设备仿真实验环境课程
信息安全科研测试
安全产品测试研究分析

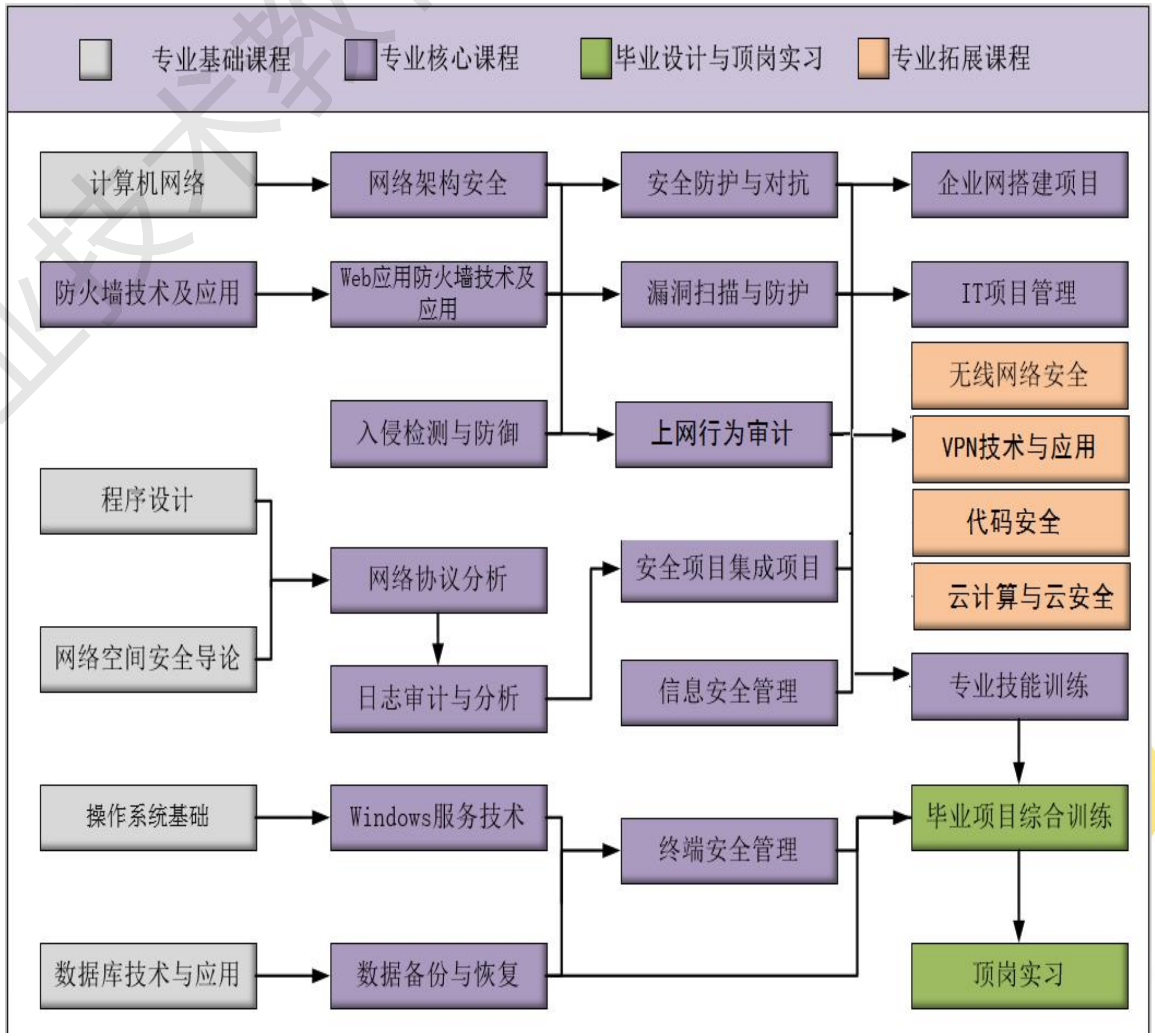
CTF赛事
攻防混战赛事
行业信息安全技能比武
VIP赛事定制及自助赛事举办

基于岗位任务的课程体系设计开发

工作任务 → **技能要求** → **专业课程** → **项目实训**

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	岗位典型任务	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，以满足网络系统安全稳定运行的需要。	设备安装上线	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. 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*
		安全策略部署	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	
		安全运维管理	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	
		应急响应	1. 事前预防准备 2. 事中安全检测和事件定位 3. 事后快速恢复 4. 总结和提高安全水平	
Web 安全工程师	对企事业网站、信息系统进行安全评估测试及安全加固；通过安全措施的实施，防护各种针对以网站、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	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. 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 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. 网站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*
		等级保护	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	
		Web 安全加固	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	
		应急响应	1. 事前预防准备 2. 事中安全检测和事件定位	



课程体系及实训环境建设

奇安信
中国奥委会官方赞助商

人才培养方案 课程体系教材

2个培养方案及课程体系

网络安全专业(本科)培养方案

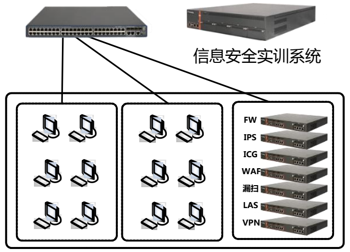
网络安全专业(高职)培养方案

21门网络安全课程

11门 安全基础课程	5门 安全专业课程	3门 特色安全课程	2门 综合实验课程

教学大纲、讲义、授课PPT、试题库、实验课程

虚实结合实验 场景案例教学



信息安全实训系统

信息安全竞技系统

- 防火墙技术及应用
- 漏洞检测与防护
- 入侵检测与VPN
- Web安全检测与防御
- 日志采集与分析

- 云计算与云安全实验室
- 源代码安全实验室
- 移动(无线)安全实验室

师资力量培训 安全能力传递

师资培训
- 安全能力培训
- 企业挂职锻炼
- 教育部协同育人项目

学生短训
- 攻防竞赛赛前培训
- 暑期短训班-攻防培训

实习就业
- 毕业实习
- 岗前培训
- 入职奇安信

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

学历教育系列教材

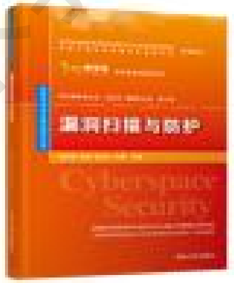
奇安信
中国奥委会官方赞助商

教材包含《课程大纲》、《课程讲义》、《课程讲义（PPT）》、《实验指导书》、《试题库》五部分。既有理论知识和技术的介绍，也融合了客户典型的应用案例，同时引入了最新产品理念和产品特色，形成一套独具特色的立体化教学资源。目前与清华大学出版社签约4套教材，入选网络空间安全教育系列教材。

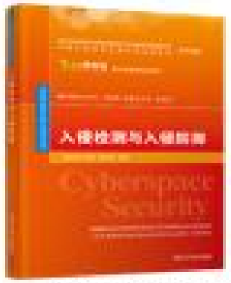
《防火墙技术与应用》★
课程学时：64学时（其中理论学时为16学时，实验学时为48学时）

《Web应用防火墙技术与应用》★
课程学时：48学时（其中理论学时为16学时，实验学时为32学时）

《日志审计与分析》★
课程学时：48学时（其中理论学时为16学时，实验学时为32学时）



《漏洞扫描与漏洞防护》★
课程学时：48学时（其中理论学时为16学时，实验学时为32学时）

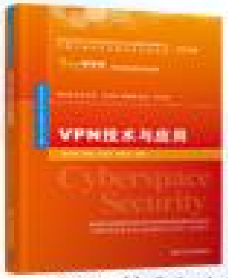


《入侵检测与入侵防御》
课程学时：48学时（其中理论学时为16学时，实验学时为32学时）

《网络安全运营》
课程学时：80学时（其中理论学时为20学时，实验学时为60学时）

《云计算与云安全》
课程学时：48学时（其中理论学时为16学时，实验学时为32学时）

《代码安全》
课程学时：48学时（其中理论学时为16学时，实验学时为32学时）



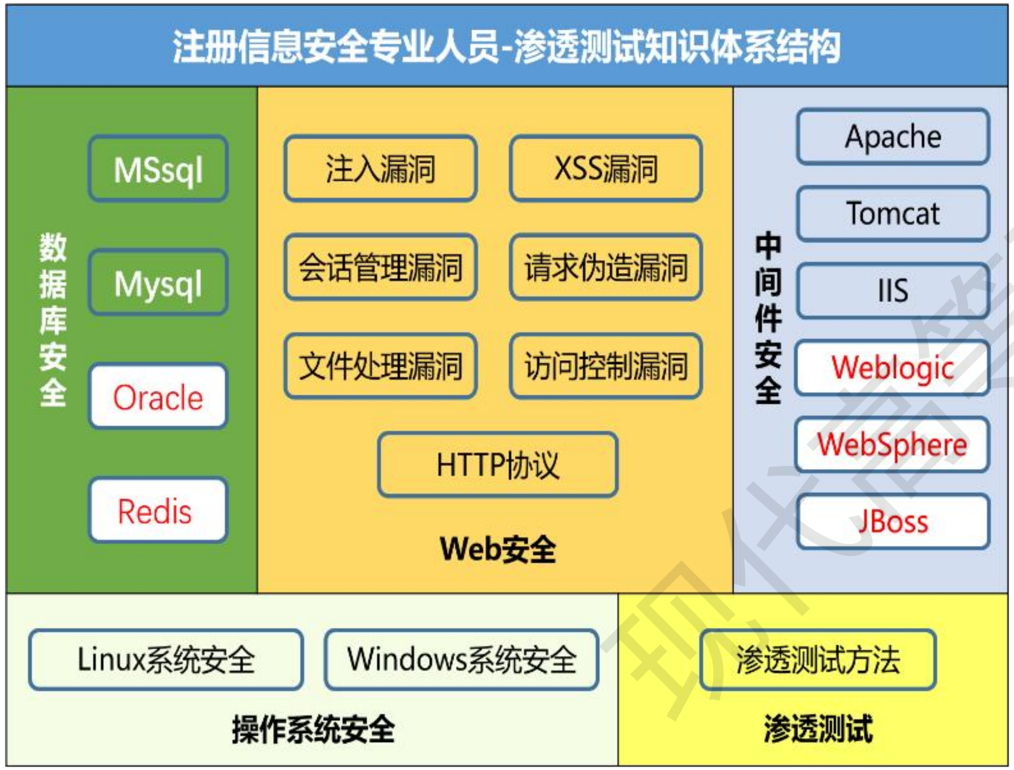
《VPN技术与应用》
课程学时：48学时（其中理论学时为16学时，实验学时为32学时）

《无线网络安全》
课程学时：48学时（其中理论学时为16学时，实验学时为32学时）

奇安信
中国奥委会官方赞助商

双师型师资培训体系建设

提供全方位的师资培训服务
1，安全产品类培训
2，安全攻防类培训
3，安全管理/工程/服务类培训
4，安全认证类培训



日期	时间	课程名称	知识点分解
第一天	上午 9:00—12:00	网络安全专业体系建设	1. 网络安全技术发展趋势 2. 网络安全人才与技能需求
	下午 13:30—17:30		1. 传统信息安全专业建设 2. 新形势下网络空间安全专业课程体系建设
第二天	上午 9:00—12:00	Web 应用安全课程建设	1. Web 应用架构剖析 2. Web 应用安全隐患分析
	下午 13:30—17:30		1. Web 应用安全分析实践 2. Web 应用技术趋势与安全技术演进
第三天	全天 9:00—17:30	拓展活动	
第四天	上午 9:00—12:00	二进制安全技术课程建设	1. 二进制安全方向技术研究 2. 二进制安全技能要求
	下午 13:30—17:30		1. 二进制安全相关技能与课程建设 2. 移动应用安全技术概览
第五天	上午 9:00—12:00	安全技能竞赛人才培养	1. 安全技能竞赛技术方向与技能要求 2. 安全竞赛人才培养指南
	下午 13:30—17:30		1. 竞赛技能培训与赛题体验 2. 培训总结回顾，交流探讨

产业创新服务中心：工程实践

奇安信

中国奥委会官方赞助商

组织合作高校学生参与第十四届全运会保障

通过有针对性的系列企业工程实训及实操训练，使得学生能够为企业的交付、安服等项目提供合格的人力支撑，解决企业在重保、HW等项目大量突击用人的需求。

组织合作高校学生参与北京冬奥会保障

中国科学院大学、北京理工大学、北京邮电大学、北京工业大学、北京电子科技学院、江苏大学等国内高校并在各大网络安全竞赛中崭露头角的优秀学生均在其中。

成立网络安全认证培训中心

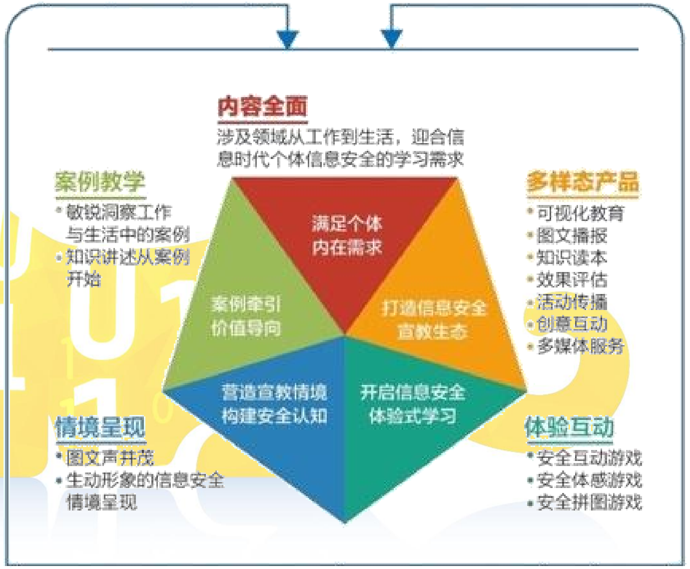
奇安信认证
工程师体系
QCC系列

行业认证培训
行业人才培养
CISP系列

网络安全观
意识教育

业界唯一覆盖网络安全各技术领域的安全工程师技术能力评估体系

国家级攻防领域认证，国内首个渗透测试类认证体系CISP/CISP-PTE/ECSP



第二阶段、社会服务能力建设---举办行业演练和大赛

奇安信

中国奥委会官方赞助商

行业应急攻防演练：真实全面地展示攻击方流量实时状态，展示攻方与被攻击目标的IP地址及名称，通过光线流动效果及数字标识形成攻击流量信息的直观展示，支持全国多城市视图切换，支持多种攻击类型标识。

网络安全攻防大赛：是以网络安全人才培养为核心，构建了专业化赛事支撑平台，具有FCTF火种CTF在线竞赛平台、攻防混战竞赛平台，可进行多种竞赛演练模式于一体的考核、实战演练平台。

第二阶段、社会服务能力建设---科普基地

奇安信
中国奥委会官方赞助商

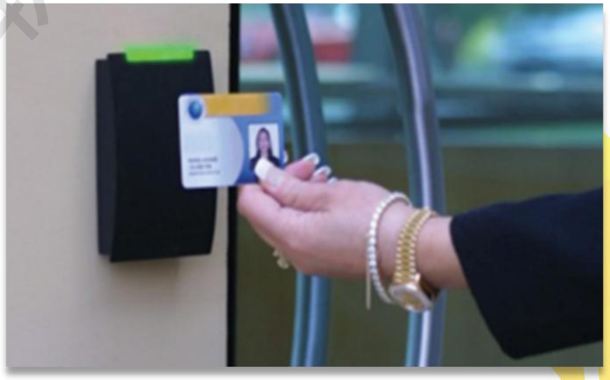
中国网络安全态势感知演示系统

数据驱动安全理念展示

工业互联网安全展示

NFC网络透明人

黑客改号体验



门禁卡克隆

智能门锁破解

第三阶段、科研能力建设---双创、实习和推荐就业

通过孵化创业创新项目，**带动科研落地**，孵化辐射产业

在基地内设置 **“双创空间”**，为大众创业，万众创新提供合适的孵化空间

各地产业网络安全运营基地

安庆网络安全运营基地

宿州网络安全运营基地

宜宾网络安全运营基地

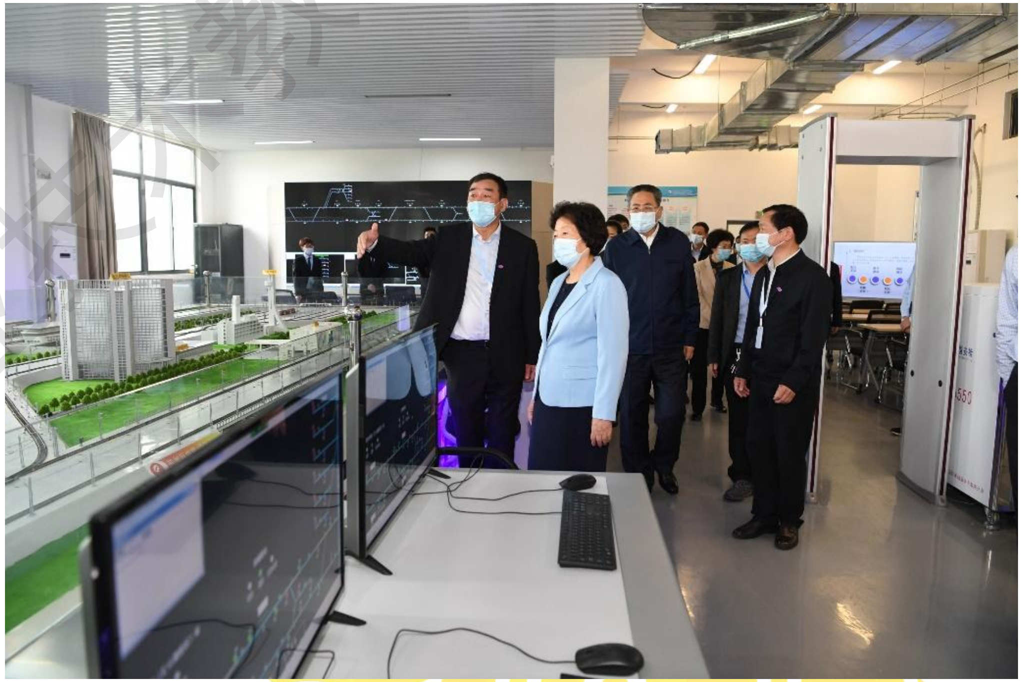
长沙网络安全运营基地

中国奥委会官方赞助商

3 深化产教融合·校企合作案例

整合资源、重点建设、错位发展、换道超车

合肥职业技术学院-国家领导人考察基地



2022年4月23日，中央政治局委员、国务院副总理孙春兰考察了奇安信与合肥职业技术学院共同发展的产教融合实训基地，考察过程中，对合肥职业技术学院紧扣“三业一体”的“双元育人” 培养思路，给予了充分肯定。

福建信息职业技术学院网络安全产业学院

奇安信
中国奥委会官方赞助商

背景：

福建信息职业技术学院与奇安信集团开展校企合作，建设特色高水平产业学院，构建“G+2+E”生态体系，其中“G（Government）”指政府，包括教育厅、网信办、人社厅、科技厅、工信厅等；“2”指合作双方——高水平学校+行业龙头企业，“E（Ecosystem）”指生态系统。

内容：

整个方案建设目标包括：

- 建设一个多主体（G+2+E）共建的网络安全产业学院创新人才培养模式
- 建设一个产业急需的信息安全与管理专业（职业本科&中高本衔接人才培养
- 方案）
- 建设一套体现网络安全产业和技术最新发展的新课程（物联网安全等）
- 建设一个集教学，实训、技术创新、社会服务等于一体的产教融合实训基地
- 建设一个工程实践能力强的高水平双师型队伍
- 建设一个企业级的网络安全协同创新平台
- 建设一个直接面向当地产业的双创服务中心
- 形成一套可推广的网络安全产业学院建设改革成果

广东技术师范大学-广东省教学成果一等奖

奇安信

中国奥委会官方赞助商

广东技术师范大学与奇安信科技集团股份有限公司
建立 网络与信息安全领域 硕士专业学位
研究生培养实践基地合作协议

甲方：广东技术师范大学
法定代表人：戴青云
联系电话：020-38256628
通讯地址：广州市天河区中山大道 293 号广东技术师范大学
乙方：奇安信科技集团股份有限公司
法定代表人：齐向东
联系电话：010-56509199
通讯地址：北京市西城区新街口外大街 28 号 102 号楼 3 层 332 号

为了充分发挥甲乙双方资源优势，切实提高专业学位研究生培养质量，按照“优势互补、资源共享、互利共赢、协同创新”的原则，甲乙双方经过友好协商，就建立硕士专业学位研究生培养实践基地及相关事项，达成如下协议：

第一条 甲方在乙方设立（网络与信息安全领域）硕士专业学位研究生培养实践基地，甲乙双方开展（与研究生培养工作相关的技术交流讲座、项目实践、毕业设计与论文指导、毕业

广东技术师范大学
专业学位研究生实践基地建设
申 报 书

学院名称：网络空间安全学院
专业学位类型：电子信息
基地名称：广东技术师范大学网络与信息安全领域硕士专业学位研究生实践基地
单位性质：民营企业

研究生院
2022 年 04 月

编号：

广东省联合培养研究生示范基地
申 请 书

申报高校：广东技术师范大学 （盖章）
校方负责人：廖丽平
学科领域：工科
培养层次：☐博士生 ☑硕士生
合作单位：奇安信科技集团股份有限公司 （盖章）
合作方负责人：李双嘉

广东省教育厅 制表

2019年9月奇安信与广师大达成战略合作，共同打造产教融合示范基地，其合作内容包括：共建学科专业、共建课程体系、打造“双师型”教师队伍、打造“国家”一流本科专业、共同开展科学研究、共建“科研应用技术服务中心”、共建“人力资源培训服务中心”。

2021年，网络空间安全学院与奇安信联合申报的“四元协同，四位一体”：信息类专业卓越人才培养模式探索与实践，获**广东省教学成果奖（高等教育类）一等奖。**

奇安信

中国奥委会官方赞助商

在数字化转型下
期待和各位行业专家
探索网络安全人才培养的“中国模式”