安全以人为本

中关村可信计算产业联盟人才专委会
国卫信安教育科技（北京）有限公司
钱晓斌

国卫信安
COVISION

网络空间安全实训开放平台

网络空间安全实训技能体系

网络空间安全技能测评服务

安全人才培养管道增值服务

帮助个人与组织快速提升岗位与业务所需的安全技能，构筑安全能力，降低人才成本与安全风险

全国大学生信息安全竞赛

- 国卫信安是历届教指委全国大学生信息安全竞赛的秘书单位与平台支撑单位。
- 竞赛平台积累22000多优秀信安大学生，以及众多业内安全专家。

Z-TCIA 中关村可信计算产业联盟

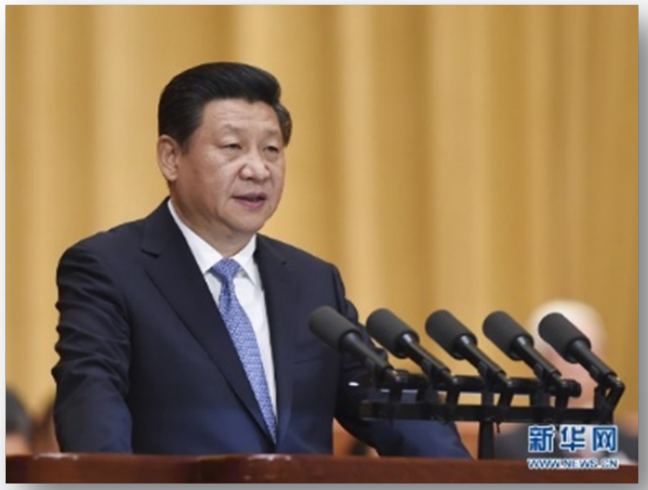
- 国卫信安是中关村可信计算产业联盟副理事长单位，是人才专业委员会主任单位。安全人才培训服务于联盟。
- 联盟成员单位具有广泛的代表性，150多家会员单位涉及到国内可信计算产业链的各个环节，覆盖了“产学研用”各界。

Agenda

1 网络空间安全人才问题

2 安全人才培养模式思考

安全人才的形势与政策



国务院学位委员会
教育部 文件

学位〔2015〕11号

国务院学位委员会 教育部
关于增设网络空间安全一级学科的通知

各省、自治区、直辖市学位委员会、教育厅（教委）、新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务

习主席讲话

没有网络安全，就没有国家安全。网络空间的竞争，归根结底是人才的竞争。建设网络强国，要有高素质的网路安全和信息化人才队伍。

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。

要建立适应网信特点的人才评价机制，以实际能力为衡量标准。

《网络安全法》

第十六条　国家支持企业和高等院校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全技术人才，促进网络安全技术人才交流。

第二十八条　除本法第十七条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：定期对从业人员进行网络安全教育、技术培训和技能考核。

网络空间安全一级学科

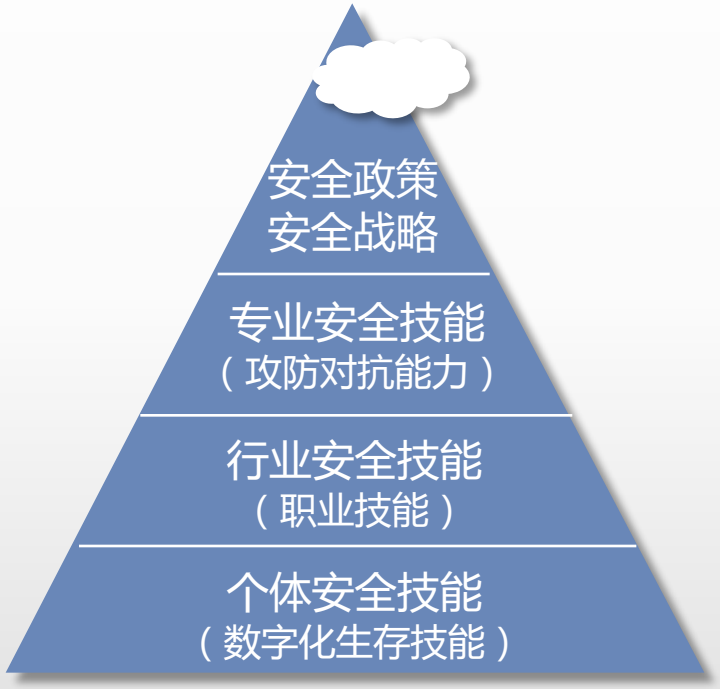
2015年6月，网络空间安全一级学科正式获批。

2015年10月，教育部下发增设网络空间安全一级学科的通知。

2015年11月，高等教育信息安全专业类教学指导委员会下发《信息安全专业实验实训课程指导规范》课题。

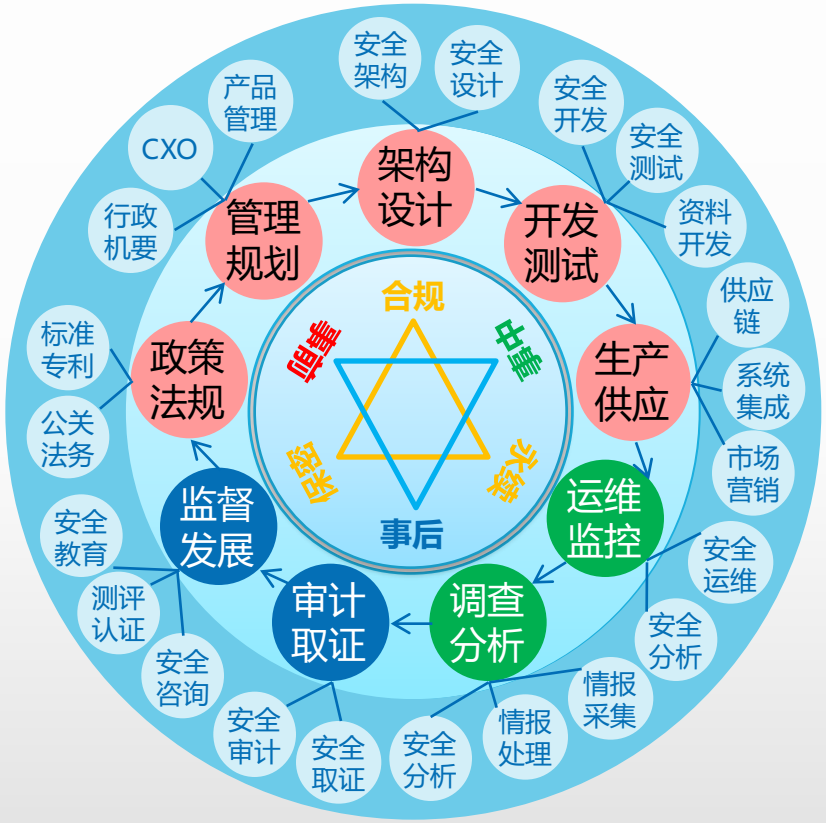
2016年4月，5年高校网络空间安全学院建设获得网信办互联网发展基金资助。

大安全、泛安全：安全人才层次结构

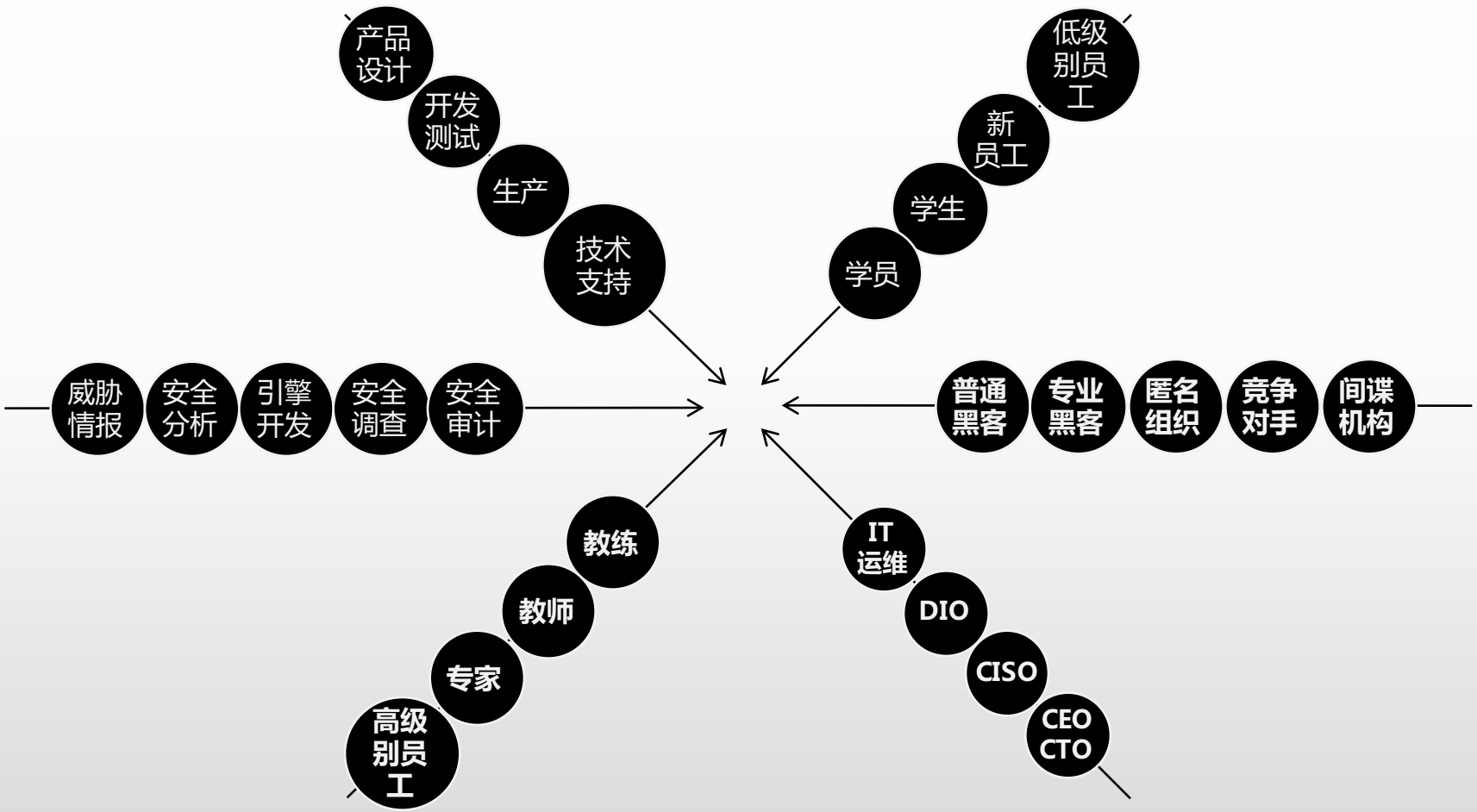


	需求分层	用户分层	群体量级
国家安全	安全战略 / 安全政策 安全思想 / 安全理论	党政军领导干部 高级研究机构	十万级
安全行业	安全分析 / 安全架构 安全开发 / 安全测试 安全运维 / 安全取证	恶意代码分析师 软件开发工程师 测试工程师、网管	百万级
普通行业	云安全 / 支付安全 / 电子商务安全 / 办公安全 / 供应链安全 / 工控安全 / 保密安全	互联网/金融/能源/交通/政府/高科技	千万级
个体生存	安全意识 安全思维 安全文化	网络公民	亿级

1. 云化移动化　　2. 行管加强　　3. 立法趋严　　4. 安全人才缺口巨大



网络空间安全岗位全景图


产品设计
开发测试
生产
技术支持
威胁情报
安全分析
引擎开发
安全调查
安全审计
教练
教师
专家
高级别员工
低级别员工
新员工
学生
学员
普通黑客
专业黑客
匿名组织
竞争对手
间谍机构
IT运维
DIO
CISO
CEO
CTO

安全人才：安全系统的最短木板

安全人才供需矛盾亟待解决

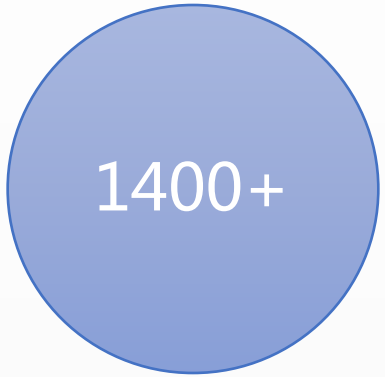
- **量少**：
  - 总量少，具备实际操作能力的人少，高端安全人才数量更少
- **分布不均**：
  - 地域上集中分布在北京、上海、杭州、武汉、成都、西安等大城市
  - 行业上向BTA3等互联网企业流动趋势明显
- **结构失衡**：
  - 渗透攻击者多，安全防御者少
  - 工具使用者多，工具研发者少
  - 漏洞利用者多，漏洞挖掘者少
  - 利益驱动者多，理念驱动者少
- **机制落后**：
  - 缺乏成熟的专业培养机制，以岗位摸索与社区学习为主
  - 缺乏有效的岗位分类定义，以用人单位自行设置为主
  - 缺少有效的技能鉴定机制，以江湖口碑为主

关键安全岗位设置问题

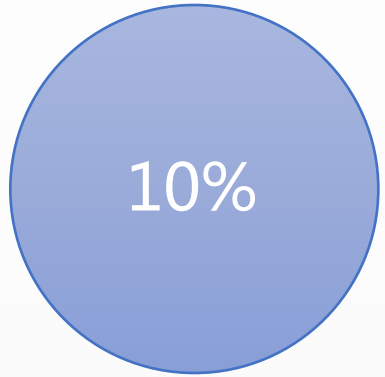
建筑行业：五大员	医疗行业	安全行业？
预算员 施工员 质检员 材料员 安全员	几乎所有工种 都需要持证上岗	网信办通过 相关工作文件 CISO？ 安全保密人员？ 风险评估人员？ 审计取证人员？

人才问题后果严重

某省党政机关
涉密网数量



某省党政机关
非涉密网数量



某省保密工作技术人员
胜任率

问题：

1. 无人、缺人、缺专家，一线缺“保安”无“保安” ，网络运维安全保障靠“墙外人”
2. “重建设、轻运管”现象比较普遍
3. 缺少规范化、科学化、制度化的网络安全管理

导致：

运维不到位，监管不得力，失管弃管，城门洞开，隐患若现

人才问题后果严重

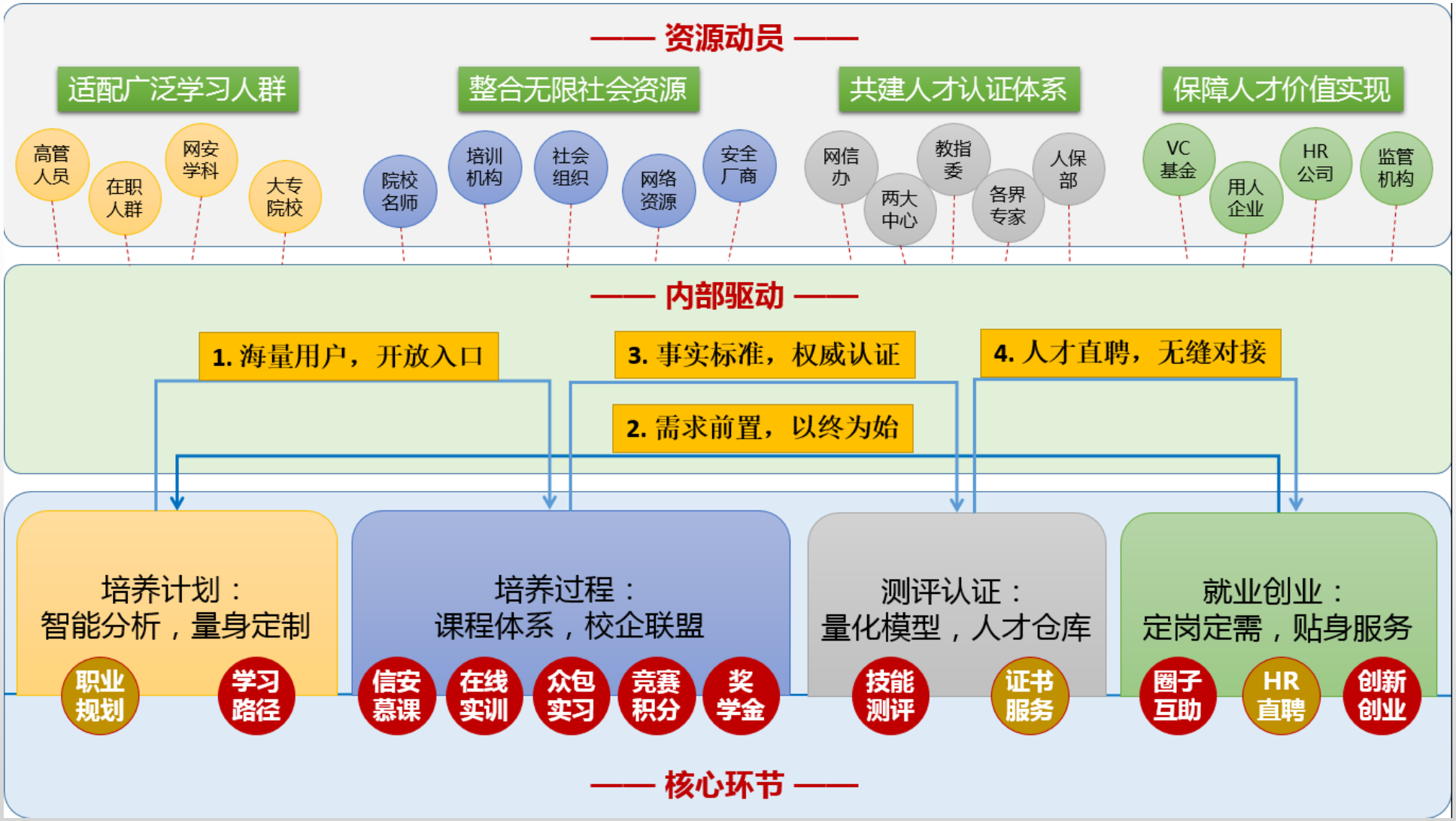
安全系统	弱点	风险
FW	大量攻击都是通过合法的访问控制策略进出，mail与web是两大入口	对APT攻击无能为力
IPS	- 特征库只能覆盖当前已知漏洞或弱点列表的子集，大量黑市0day漏洞无法覆盖 - 180种以上逃避检测手法，从URL变形到大量的编码相关变形，全面覆盖的成本非常高 - 安全产品在某些特殊场景下，会启用bypass策略，特定时间窗内会透传流量	给APT攻击留出非常多的机会。针对bypass，只要攻击持续发生，就有机会渗入
主机AV	- 功能使用不当； - 特征库更新不及时； - 检测最新3天的病毒样本检测率在30-40%	未知病毒无法检测，容易被绕过
主机IPS	并不比IPS与主机AV高明	未知攻击无法检测，容易被绕过
审计系统	依赖于安全系统的输出，自身无增强功能；对于伪装进程检测能力弱	容易被欺骗
DLP	功能很不完善，各家产品有自己侧重点，不是完整的数据防窃取	作用有很大局限性
软件	连通性；复杂性；扩展性	研发过程的安全亟待加强
人	- 安全意识差，惯性、惰性 - 工作过程中追求方便不断降低安全标准、破坏安全状态、破坏攻防平衡 - 利益驱动；	防不胜防

Agenda

1 网络空间安全人才问题

2 安全人才培养模式思考

共建安全人才培养生态


—— 资源动员 ——
适配广泛学习人群
整合无限社会资源
共建人才认证体系
保障人才价值实现
高管人员
在职人群
网安学科
大专院校
院校名师
培训机构
社会组织
网络资源
安全厂商
网信办
两大中心
教指委
各界专家
人保部
VC基金
用人企业
HR公司
监管机构
—— 内部驱动 ——
1. 海量用户，开放入口
3. 事实标准，权威认证
4. 人才直聘，无缝对接
2. 需求前置，以终为始
培养计划：
智能分析，量身定制
职业规划
学习路径
培养过程：
课程体系，校企联盟
信安慕课
在线实训
众包实习
竞赛积分
奖学金
测评认证：
量化模型，人才仓库
技能测评
证书服务
就业创业：
定岗定需，贴身服务
圈子互助
HR直聘
创新创业
—— 核心环节 ——

开放创新的安全教育平台与工具链

知识系统	教学系统	考试系统	认证系统	HR系统	创业平台
内容生产 知识树管理 课件商店 点评与推荐	课程管理 课堂测试 大数据工具 众包任务	认证考试 安全竞赛	认证机构管理 证书管理 证书查询 续证服务	档案管理 职业评估 HR服务	创业投资 开放项目

云资源管理与内容运营平台

云桌面、虚拟网络、实验拓朴、虚拟设备、接入认证、课件商店等

实训室/基地	实训平台	实训APP	技能测评系统
多媒体 体验/演练 案例/研讨 本地/远程	实训/竞赛 独立/集群	轻量版本 碎片化学习	专业技能 非专业素质

开放创新的安全教育平台与工具链

维度	优势
规范	1. 网信办《网络安全岗位分类规范与能力标准研究》 2. 教指委《网络空间安全专业实验实训课程规范》
内容	普及：安全运维、安全意识，面向大众 门槛：保密、军工、工控，面向特殊行业 运营：实时更新、课件商店
技术	云计算水平扩展能力，既提供专用硬件，也支持通用服务器集群部署 虚实结合的虚拟化能力，支持FW、UTM、NGFW、IPS、 WAF、上网行为管理、扫描器、交接机、路由器虚拟化，**方便学员独占使用** 大数据教学分析能力 构建大型复杂场景能力，支持大型僵尸网络、DDoS、云计算、工控、大数据场景
体验	高性能 基于业务流程与角色代入

加强校企对接，形成安全能力考核标准

能力分项 \ 能力级别		初级	一级	二级	三级	四级	五级	六级
必备素质	《安全意识》	SL1	SL2	SL2	SL3	SL3	SL4	SL4
	《黑客思维》	SL1	SL2	SL2	SL3	SL3	SL4	SL5
	《系统思维》	/	SL1	SL2	SL3	SL3	SL4	SL5
必备知识	《互联网与应用系统知识》	SL1	SL2	SL2	SL3	SL3	SL4	SL5
	《网络与信息安全法规知识》	SL1	SL2	SL2	SL3	SL3	SL4	SL5
	《安全运维方法学》	SL1	SL2	SL2	SL3	SL3	SL4	SL5
操作能力	《Web安全运维》	SL1	SL2	SL2	SL3	SL3	SL4	SL5
	《DB安全运维》	SL1	SL2	SL2	SL3	SL3	SL4	SL5
	《OS安全运维》	SL1	SL2	SL2	SL3	SL3	SL4	SL5
	《网络设备安全运维》	/	SL1	SL2	SL3	SL3	SL4	SL5
	《数据中心安全运维》	/	SL1	SL2	SL3	SL3	SL4	SL5
	《工控系统安全运维》	/	/	SL1	SL2	SL3	SL4	SL5
	《物联网系统安全运维》	/	/	SL1	SL2	SL3	SL4	SL5
	《安全分析》							
	《安全调查与数字取证》							
工程能力	《安全运维流程管理》	/	SL1	SL2	SL3	SL3	SL4	SL5
	《安全架构设计》	SL1	SL2	SL3	SL4	SL5	SL5	SL5
	《安全运维自动化与工具开发》	/	SL1	SL2	SL3	SL4	SL4	SL5
	《安全运维架构设计》	/	/	SL1	SL2	SL3	SL4	SL5
研究能力	《大数据安全运维》	/	/	/	/	SL1	SL2	SL3
	《安全运维标准与专利》	/	/	/	/	SL1	SL2	SL3

能力等级	能力阶位	熟练程度	影响范围
SL1	10% 20% 30% 40% 50% 60% 70% 80% 90% 100%	指导下工作：在他人指导下开展工作，仅仅有一般的、概念性的知识。 - 基本的知识和能力 - 初步接触或学习现有流程、技术和方法 - 在他人指导下开展工作	个人
SL2	10% 20% 30% 40% 50% 60% 70% 80% 90% 100%	独立工作：独立安排好进试度和要求，解决常见问题。 - 良好的知识和能力 - 应用现有的流程、技术和方法 - 解决常见问题 - 能够理解所做改进 - 独立安排好进度和要求	小组级
SL3	10% 20% 30% 40% 50% 60% 70% 80% 90% 100%	指导他人工作：重复的、成功的经验和案例，能够改进积极地做出贡献 - 触类旁通的知识和能力 - 定义并解决那些需要仔细分析的复杂问题 - 能够为改进积极地做出贡献 - 指导他人工作，能够影响进度和要求	部门级
SL4	10% 20% 30% 40% 50% 60% 70% 80% 90% 100%	被视作专家：深入彻底的知识，能够提供指导或指引方向 - 深入透彻的知识及能力 - 优化或扩展现有的流程、技术和方法 - 研究并解决那些需要综合分析的复杂问题 - 能够提供指导或指引方向，驱动改进	产品线或公司级
SL5	10% 20% 30% 40% 50% 60% 70% 80% 90% 100%	被视为权威：被其他人当作磋商者和领袖；非凡的知识和正确的评判能力；能领导、教练其他人成功运作 - 非凡的知识及能力 - 在需要的时候对流程、技术和方法进行创新 - 擅长解决纷繁复杂的问题和挑战 - 作为权威，能够意识到并能发起变革或改进 - 能领导、教练其他人成功运作	公司或行业级

CCSSP网络空间安全技能测评体系

主任单位

国家信息安全工程技术研究中心

暨上海信息安全工程技术研究中心，成立于2001年10月是受国家科技部领导，由国家密码管理局、国家保密局、公安部、安全部、工业和信息化部、上海市科委共同指导的专事信息安全工程技术研究与系统集成、安全人才培养的研究机构。

秘书长单位

国卫信安教育科技（北京）有限公司

级别	专业方向						
	安全意识	安全保密	安全管理	安全运维	安全测试	安全开发	安全专项
大师级 CCSSP-4	面向在职人员，大师级课程+专业方向课程						
专家级 CCSSP-3	面向在职人员，专家级课程+专业方向课程						
专业级 CCSSP-2	面向在职人员，专业级课程+专业方向课程						
预备级 CCSSP-1	面向在校学生，院校提高课程+安全普及课程						

说明：

1、CCSSP是面向网络与信息相关人员，尤其是与信息安全工作密切相关的专业技术人员和管理人员的技能水平认证，目前其涉及7个专业方向、4个认证级别。

2、CCSSP认证体系的各级课程均包含理论课程、实验课程，课程授课形式为线上+线下交互。

CCSSP网络空间安全技能测评体系（ex. 安全运维工程师）

科目	模块
计算机与网络基础	计算机硬件基础
	计算机网络基础
	计算机与网络故障诊断
	互联网基础设施-PKI与CA
	互联网基础设施-国际组织
网络与信息安全基础	安全三要素
	安全模型
	威胁建模
	安全体系结构
	安全标准与安全合规
	应用密码学
	网络与应用协议分析
	软件逆向分析工程
安全运维基础	安全运维的概念
	安全运维的目标
	安全运维的内容
	安全运维的技术架构
	安全运维的工具
	安全应急响应
	安全运维的安全性

科目	模块
网络安全运维	安全组网
	防火墙/下一代防火墙
	漏洞扫描器
	VPN
	SSL VPN
	堡垒主机
	IDS/IPS/NGIPS
	蜜罐/蜜网
	沙箱
系统安全运维	系统安全配置
	系统加固
	计算机病毒
	高级恶意软件
	终端审计与取证
应用安全运维	Web服务器安全
	数据库服务器安全
	邮件服务器安全

科目	模块	核心内容
网络与信息安全基础	安全漏洞与脆弱性	硬件安全隐患
		软件安全隐患
		网络协议安全
		安全管理漏洞
高级安全运维技术	SIEM	日志泛化
		关联分析
		事件归并
	SOC	资产管理
		风险评估
		事件响应
	安全调查	攻击链
		痕迹采集
		事件分析
	自动化运维	SHELL
		PYTHON
		JAVASCRIPT
		PERL
	大数据安全分析	大数据存储
		大数据处理
		弹性搜索
		机器学习
		异常建模
		威胁建模
	应急响应	终端隔离
		应用隔离
		网络隔离
		系统恢复

CCSSP网络空间安全技能测评中心

网络空间安全人才技能测评

认证证书

王治超 技能测评成绩合格，并通过相关资格审查，符合我中心《网络空间安全人才技能测评规范》要求，准予注册，特颁此证。

注册等级：预备级

证 书 号：CCSSA201511300034

发证日期：2015年12月

有 效 期：3年

国家信息安全工程技术研究中心
网络空间安全人才技能测评中心

原晓岩

谢 谢
钱晓斌
WeChat: AlanQianChina