北京深育技术服务有限公司
参与北京网络职业学院人才培养年度报告

（2022）

企业名称：北京深育技术服务有限公司

院校名称：北京网络职业学院

2021 年 11 月

目录

一、合作简介

（一）双方概况

北京深育技术服务有限公司成立于2017年，公司现有员工近100人,是一家集信息安全产品销售、信息安全服务、信息安全咨询为主要业务的信息安全服务公司。

北京深育技术服务有限公司成立以来与深信服科技有限公司深度合作，成为该公司的五星安全服务站和钻石级安全产品代理公司。主要为政府、学校、高校等单位提供全面的信息安全服务、产品安装部署、信息安全咨询的业务。客户覆盖北京主要的重点中小学和重点高等院校。

北京网络职业学院是北京市属独立设置的民办高等职业院校，其前身为中国信息大学。中国信息大学是由国家信息中心于1993年创办的全日制民办高校。2003年6月，为适应民办高等学校办学体制及政府机构职能转变的需要，学校进行了改制重组，举办者由国家信息中心变更为北京国信大教育发展有限公司，2003年9月，北京市民政局给学校颁发了《民办非企业单位登记证书》，2004年11月学校从昌平原校区整体搬迁至房山区窦店镇，由此，学校进入了新的发展阶段。经过十几年的探索和努力，为国家培养了一批信息化建设人才，也为后续发展打下了一定的基础。

为了适应新时期社会经济发展的要求，按照北京城市功能定位及为首都地方经济发展服务的理念，在国家大力推动高职教育发展的打好形势下，2015年10月，经北京市教委审批、北京市政府批准、报教育部备案，在中国信息大学原有教育资源的基础上成立了北京网络职业学院。

北京网络职业学院成立至今，历时五年，始终以培养生产一线用得上、留得住的高素质技术技能型人才为己任，走上了职业教育高速发展的快车道。

（二）合作背景

1.国内信息安全技术人才的需求现状

调查显示，从2006到2012年，网络信息安全行业的就业需求将以年均14%的速度递增。到2012年，网络安全行业的就业总人数将由目前的220万上升到310万，即以每年15万的需求量递增。无论是职业前景、受重视程度、提升空间还是薪酬基数、薪酬增长预期等，网络安全职业较IT其它职业都更为优越。调查结果再次说明了网络安全重要性的日益增强，"整个企业领域逐渐认识到网络安全的重要性"。

另外，从目前国内各企事业单位的IT技术人员需求来看，信息安全技术人才十分匮乏。随着计算机的广泛使用，病毒的种类也越来越多，危害越来越大。专业的信息安全技术人才还是国内IT人才架构中的一个空白。随着信息安全受到社会各界越来越多的关注，以及入侵事件和电脑病毒危害的频频发生，从企业内部网络的管理维护到反病毒软件的安装、调试、维护及使用，都需要具备一定安全技能的技术人员来担任。因此，信息安全技术人才必将成为国内IT技术人才需求的一个新热点。

2.国内信息安全技术人才的需求类型

纵观我国目前信息安全专业人才需求情况，包括了多个层次和多个方面的需求，大体可以分为以下四种类型：

（1）第一类是对理论研究人才的需求，这种需求通常来源于各类科研院所、高等院校、大型企业中的信息安全相关研究机构。这方面人才属于具有创新意识的研究型人才，要求具有良好的学术功底，具备扎实的学科理论基础知识，能系统深入地掌握密码学、安全协议、安全体系结构、信息对抗、网络安全等信息安全理论和方法。

（2）第二类是对技术开发人才的需求，这种需求通常来源于提供信息安全产品、信息安全服务的各种企事业单位。信息安全技术开发人才要求具备良好的信息安全基础知识具有较强的动手实践能力，熟练的产品设计开发能力，包括良好的规划设计以及软硬件实现能力。

（3）第三类是对管理服务人才的需求，这种需求目前是广大企事业单位和政府部门的主要需求。对很多企事业单位来说，虽然不经营信息安全产品和服务，但是其信息化管理，以及企业的核心技术知识产权保护，都需要建立专门的信息安全管理部门，需要专门的信息安全管理人才来保证企业的生存和正常运行。同时，随着我国政务信息化的迅速发展和普及，政府部门对信息安全管理人才也存在大量的需求。信息安全管理服务人才要求是一种复合型和应用型的人才，不仅需要具备一定信息安全技术能力，能够正确使用、配置、维护常规的信息安全设备，还必须具有一定的管理和法律知识，能正确规划、实施和维护信息系统的安全保障体系。

（4）第四类是对教育培训人才的需求，这种需求主要来源于高等院校和各种培训机构。目前，越来越多的高等院校申报开办信息安全专业，信息安全专业的本科、研究生教育需要一批德才兼备的专业教师。另外，我国信息安全非学历教育也已基本形成了以各种认证为核心，以各种职业技能培训为辅的信息安全人才培训体系，出现了各种各样的培训机构，这些培训机构也需要一些专门的培训教师。随着各行各业信息化的普及以及信息安全意识的增强，可以预期以上各个层面上的信息安全人才都将有很强的社会需求。尤其，随着我国国民经济和社会信息化的进一步发展，最符合社会大量需求的人才应该是从事信息安全管理和安全服务的复合型、应用型人才。

3.国内信息安全技术人才的培养现状

据有关权威部门提供的数据，目前我国共有信息化安全专业人才数千人，而获得中国信息安全产品测评认证中心注册证书的仅三百多人。人才培训与培养的滞后，使得我国信息安全产业在开发、管理、运用等方面人才匮之，从而制约了我国信息安全产业的进一步发展，也严重影响了我国这一行业的国际竞争力。另外，我国目前从事信息安全专业人才培养的大学也不多，而且他们开办相关专业的时间也不长，不过近两年发展较快。2001 年全国第一个信息安全本科专业在武汉大学创建，2002 年又有 18 所高等学校建立了信息安全本科专业，但信息安全专业应用服务型人才(专科层次)培养几乎还是空缺。随着信息化进程加快和计算机的广泛应用，信息安全问题日益突出，我国信息安全人才培养还远远不能满足需要。目前存在以下突出问题。

（1）高层专业技术人才缺乏

在信息安全体系结构的研究和技术应用方面，我国仍处于起步阶段，我国从事与信息安全有关的副研究员职称以上的人才约 2000 多人，且从事密码研究所占的比例较大。这与发达国家相比存在很大的差距，最突出的是核心芯片和系统内核不能自主开发，主要原因是我国缺乏具有自主创新能力的专业人才。国人的研究仍集中在修补现有系统的安全漏洞上。另外,我国从事网络信息安全

的系统集成商大多数都缺乏专业的安全支撑技术力量，这样一来，整个方案中充斥着各类产品的介绍，一套安全解决方案成为各种安全厂商产品的堆砌，这不仅造成用户投资的浪费，而且从根本上很难抵挡黑客的攻击和各种恶意代码威胁。

（2）信息安全管理和服务人员严重不足

任何一种安全产品所能提供的服务都是有限的，也是不全面的，要有效发挥操作系统、应用软件和安全产品的安全功能，必须进行全面的检测、合理的配置和适当的优化，才能使整个安全系统良好地运转起来。这需要一整套系统的安全过程来实现。而实现这些严密的安全措施需要信息安全专业人员参与，并发挥主要作用。另外，从事信息安全产品生产的企业也非常缺乏懂专业知识的销售服务人员。

（3）信息安全人才培养的梯队尚未形成

当前信息安全人才培养的高中低人才梯队尚未形成，中低层应用服务管理型专门人才的培养还没起步，按现代信息安全观点来说，“三分技术，七分管理”，而这类干具体实际工作的人恰恰是不容忽略的群体。保障信息安全，需要多样化、多层次的人才，因此，信息安全专业人才的培养目标应不尽相同，既要在研究生和本科教育阶段培养能从事整个网络信息安全系统规划、设计的高层次人才，也要在专科教育阶段培养具体进行网络安全系统某个环节建设的专业技能型人才，还需要在普教行业开展网络安全的认知，了解网络安全的重要性和合规性。

（三）合作规划

1.应用型人才培养目标

信息安全应用型人才培养计划全面落实“产、学、研、用”一体化的思想和模式，将建设及融合各个基础及专项的综合实验平台，迎合技术发展趋势，满足各层次实践教学、满足学校的实验教学、科研、技术培训和对外服务的需求。同时，由于本科教学和高职教学的区别，而各个院校在同一专业上又会追求各自的特色；尤其是信息安全在很多学校并没有作为一级学科，而是作为其他计算机学科门类的一个专业方向存在，所以深信服信息安全实训室规避大而全的做法，以培养厚基础、宽专业，动手能力强的应用型安全人才为目标。以深信服信息安全产品“下一代防火墙”、“VPN接入网关”、“上网行为管理”“应用交付”为核心架构，融合信息安全理论教学、实训、实战以及深信服真实的安全项目案例等各层次实践教学内容，搭建信息安全综合实训平台和专项实训平台，将理论学习、实践教学和工程实践融为一体，由难而易、循序渐进，逐步提升学生的学习技能和实践水平，提高“学”的质量和成效。最终让学生熟练掌握信息安全建设、规划、运维技能，提升就业竞争力。

所谓信息安全应用型服务人才，是指熟悉掌握常见的信息安全产品的技术，能够独立完成所有信息安全种类设备的安装、调试、维护等一般类技术服务工作，在这个基础上再选择信息安全技术某一个领域（比如漏洞扫描、入侵检测、行为管理、安全加密等）进行专业的培养，使之成为信息安全用人单位的业务骨干并能完成售前支持、工程项目管理、安全检测与防范、复杂安全故障排查等等复杂类业务工作，并且有良好的发展潜力，今后能成长为用人单位骨干的市场/技术专家。

信息安全应用型服务人才，为了能够胜任的工作任务，除了要有过硬的专业技术，还需要具有高度的职业素养和良好的综合素质，包括：充分的服务意识、较强的营销能力，善于学习、善于管理、善于创新等。

2.应用型人才培养规划

信息安全人才培养分为四个阶段：

第一阶段：实验环境搭建，通过安全硬件搭建安全实验环境，满足学校最基本的信息安全实验教学，促进信息安全知识的吸收与巩固。

第二阶段：师资培养，实验室搭建完成后学校具备了做安全攻防实验的必备条件，但还必需有能熟练掌握实验设备、具备授课技能的的师资。深信服为学校教师提供标准化的师资培养计划，通过对专业课程、授课技巧、实验室管理等内容的培训，使教师能轻松的开展安全攻防的实验教学。

第三阶段:资格认证，鼓励学生参与深信服卓越工程师认证考试，对于优秀的学生深信服优先推荐给当地合作伙伴实习、就业。

第四阶段：校企合作，共建深信服信息安全网络学院，对学生开展深信服职业资格认证服务，把厂商的认证课程引入到课题教学中，实现课程置换。共同开展学术与科研课题合作以及教学资源开发。

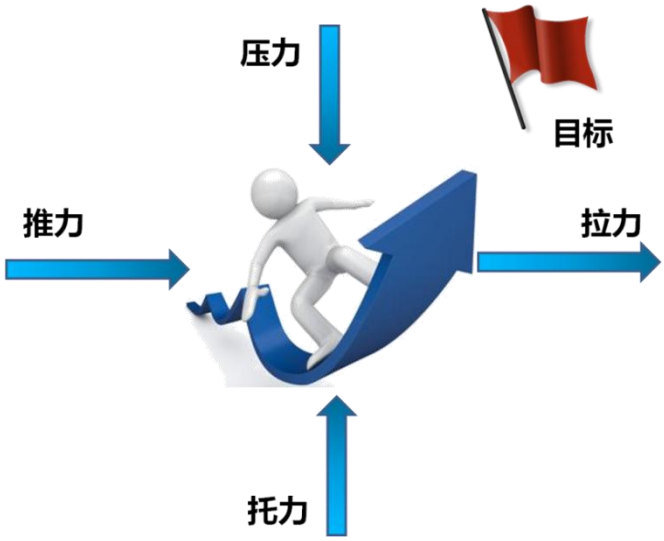
3.应用型人才岗位能力素质模型

信息安全专业培养的是能够作为信息安全技术企业合格员工并投入服务业务工作的应用型服务人才，其所需要具备的能力、素质见下面的职业能力与任务分析表：

工作岗位	工作职责	工作任务	工作任务描述	所需知识/技能	所需素质/意识
信息安全技术服务工程师	从事信息安全技术服务工作，保障客户IT业务系统高	技术支持服务	为客户IT系统设备提供信息安全设备的安装、巡检、	1、IT行业背景知识； 2、信息安全技术产品相关	1、主人翁意识与创业思维； 2、以结果为

	效、持续、稳定、安全的发展，避免遭受网络攻击、泄密等一系列网络安全挑战，提升客户核心竞争力		升级、割接、系统评估和优化等服务，对突发故障进行应急响应和处理；	知识、产品操作使用方法； 3、公司业务流程规范； 4、项目管理基础知识和技能； 5、商务基础知识和技能； 6、财务基础知识； 7、办公技能；	导向的高目标性； 3、以客户为中心的服务意识； 4、自我管理和抗压能力； 5、个人发展意愿与学习能力； 6、团队合作能力； 7、创新意识； 8、营销意识；
		工程项目实施	负责信息安全工程的前期勘测、规划、准备，工程项目中各类设备器材设施的施工，参与工程项目组的协调管理。		
		基础售前支持	配合商务人员开展客户拜访、技术方案沟通、产品试用测试、商务投标等工作；在日常技术工作中主动挖掘客户 IT 业务需求，促成需求落地；		
		技术培训	整理准备技术培训资料，对 IT 系统用户、渠道合作伙伴、公司同事进行产品、技术、方案的培训和辅导。		

4.应用型人才培养理论模型



信息安全技术人才培养理论模型

根据自身积累的信息安全技术行业经验，在人才培养方面形成了自己独特的视角和观点，信息安全技术人才培养理论模型，对人才培养需要考虑的各个要素说明如下：

作用力	要素	要素描述
目标	目标	方向明确，通过努力可以分阶段实现的合理目标；
拉力	个人发展意愿	个人需要有成功、成就、自我发展的意愿；
	激励措施	公平的激励机制，对积极、正向的行为和阶段性的成就给予物质、精神上的激励；
推力	合作团队	可以信赖和互相交流、支持的合作团队；
	导师	经验丰富的导师，可以进行经验分享和指导支持；
	组织氛围	良性的组织氛围和文化；
压力	竞争环境	活跃的竞争氛围，激励各人全力以赴、互相比拼；
	时间期限	在规定的时间必须完成目标，否则就是失败；
	处罚措施	公平的处罚机制，对未达标的结果和消极的行为给予处罚和批评；
托力	发展空间	个人从事的事业是有创造性

		的，对个人和组织都有价值；
	锻炼机会	个人有实践锻炼的机会和平台，能够获取经验甚至通过试错得到教训；
	方法经验	经过前人总结提炼的实用方法和宝贵经验，让个人发展时少走弯路；
	工具资源	必须的学习、工作工具，可以利用的人力、物力资源；

二、合作事项

（一）信息安全实验室建设方案与教学计划

社会或企事业单位用人的标准是需要具有动手能力的网络安全规划、建设与运维方面的技术人才，这和学校的人才培养模式、培养目标等方面与存在着差距。现在很多学校更多的是注重理论的教学。比如，很多政府机关、电信及金融行业更需要的是具有动手能力的网络安全技术人才。对于学校来说，学生动手能力的培养，在很大程度上取决于学校的安全实验环境和学生的实践经验。而且还有很多学校只注重攻击、渗透知识的学习与演练，而对社会或企事业单位实际所需的安全防护建设知识与技能却不重视。因此掌握主流的网络安全规划、建设与运维技能的技术人员才是企事业单位眼前最急需的。

信息安全学科是由数学、计算机科学与技术和通信工程等学科交叉而成的一门综合性学科，主要研究领域涉及现代密码学、计算机系统安全、计算机与通信网络安全、信息系统安全、电子商务、电子政务系统安全、信息隐藏与伪装等，这些课程的设置无疑对学校的信息安全实训室提出了更高的要求。

信息安全实训室应一方面对信息安全及其相关领域的前沿技术和热点应用进行深入研究，另一方面，应建设良好的信息安全工程实践环境，培养信息安全应用型人才。信息安全领域工程应用性很强，因此，对于信息安全技术领域而言，实验是教学实践的主要形式，要注重实验环境的真实性，设计综合的实验，以培养学生的整体安全意识。

1.实训室设计原则

（1）系统性。信息安全是一个系统概念，也是一个整体概念。单一的安全措施并不能保障整个信息系统或者网络环境的安全。整个系统的安全是由不同的安全技术、安全措施有机地耦合来达成的。安全人员需要对网络环境有一个系统的认识，技术要全面。因此要培养学生的系统能力和整体安全观。

（2）真实性。信息安全保障的是有价值的资源，它们或是关系国家安全机密，或是企业商业情报，或是个人隐私等。不同于常规信息技术运用，信息安全的实施者必须清楚他们权限的特殊性和所担负的责任。如果综合实验系统能够提供接近于真实网络环境的实验环境，那么将有助于培养

学生的安全意识、法律意识。同时，一个接近于现实网络环境的安全实验系统对于加强学生的实践能力有着无可比拟的作用。

（3）安全性。信息安全实验环境也要保障自身的安全。因为实验环境所包含的信息资源、研究的内容本身就是有价值的，需要得到保护。

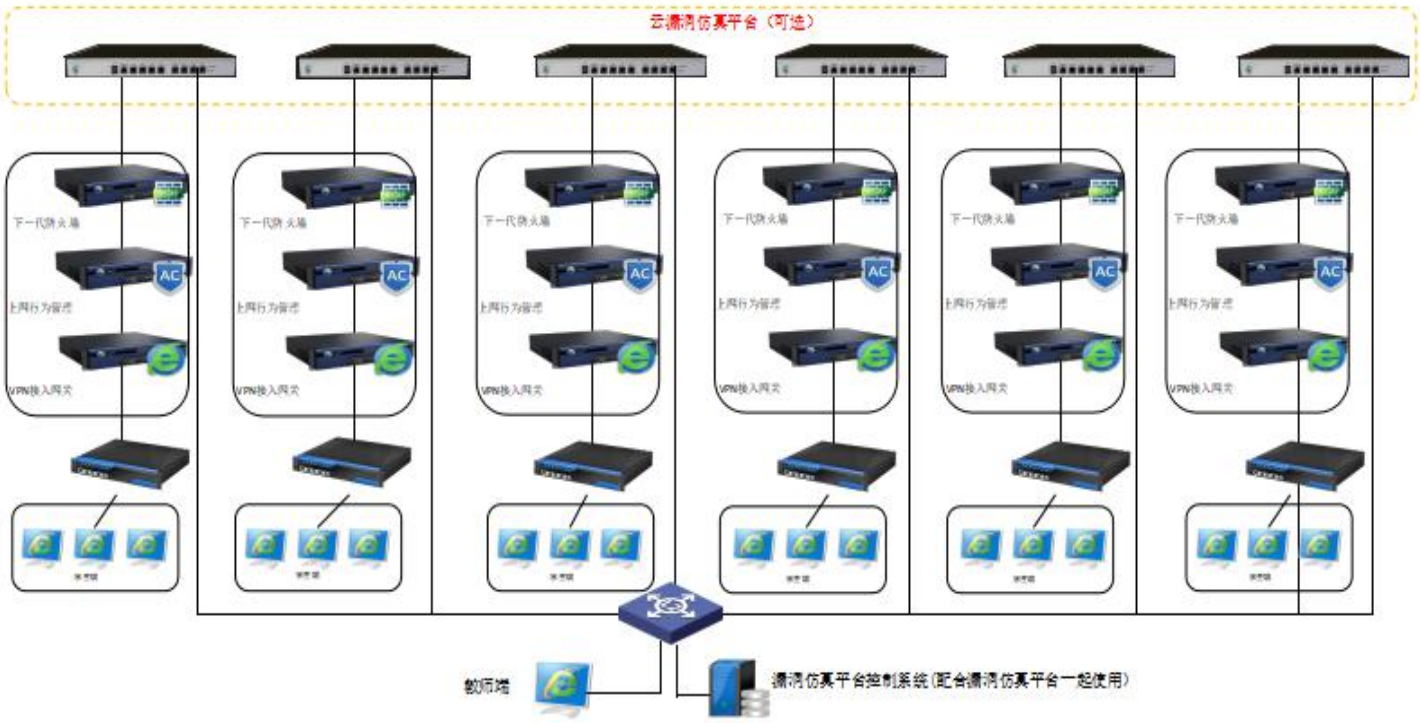
（4）工程性。信息安全是一门工程学科，直接面向工程应用，因此非常强调工程性。

（5）前瞻性。信息安全理论和技术的更新很快，这要求实验环境能够支持现有理论技术的教学与实践，还要能够支持有价值的前瞻性研究。

（6）开放性。信息安全实验环境应该是一个开放的体系，可以根据需要加入新的实验内容，以满足教学实践的需求。

由上分析，可以认为信息安全实训室的建设必须依托一个基于现实网络模型建立的信息安全综合实验系统。该系统由一定软硬件设施构成，能够模拟和仿真现实网络系统中的综合实验环境；在这个环境中，学生可以通过交互手段进行实验规划、实施、分析和报告，也可以进行安全理论技术拓展研究。

图：实验组网拓扑图



2.实验组件建议配置

为了有效开展教学，提供专业性的信息安全实验与实训教学，深信服信息安全实验包含信息安全实验（必选）、和安全攻防实验（可选、拔高）两大类。每组实验台的设备分成不同的实验包，包括：信息安全包、安全攻防包，通过提供主流信息安全建设、安全攻防对抗等方面实验案例，为学生提供更贴近实际环境的实验学习环境。学校可以根据实际需要来有针对性地选择实验台的组合。

3.信息安全实验室建议配置

N 为实验组数，每组支持 3-5 人实验。

模块	建议数量	实验设备
信息安全包	1*N	下一代防火墙
		上网行为管理与审计
		VPN 接入网关
安全攻防包	1*N	IEC-516S-SY（最大 5 人同时使用）

4.主要实验组件介绍

（1）下一代防火墙

深信服下一代防火墙品牌：下一代防火墙的领跑者，是国内下一代防火墙标准核心制定者。强势入围 Gartner 魔力象限，中国最先获得 NSSLabs“web 攻击防护”最高评价“推荐”。

深信服下一代防火墙概述：提供 L2-L7 层全访问安全防护，能有效抵御 DDOS 攻击、具备 IPS、WAF 功能，能进行僵尸网络监测、病毒防护、网页防篡改、安全可视化、安全监测等。

深信服下一代防火墙市场：2011 年 7 月，深信服率先推出国内第一台下一代防火墙，截止至 2015 年末，下一代防火墙在全国的用户累计超过 20000 家，用户覆盖各行各业，其中包括 120 多家部委省厅级单位、100 多家运营商和金融单位、120 多家知名教育单位、250 多家大型企业和国资委下属央企集团，用户数量遥遥领先。

5.上网行为管理与审计

深信服上网行为管理品牌：深信服是上网行为管理产品品类的创始者，在 2005 年开创了上网行为管理的市场，并在市场、技术、用户等方面一直保持市场第一的位置。首家推出有线无线网络统一上网行为管理解决方案。中国唯一入围国际 GartnerSWG 魔力象限的上网行为管理产品，并且连续 5 年成功入围，率先通过国家信息安全产品 EAL3 最高等级认证。

深信服上网行为管理概述：专业的行为管理、应用控制、流量管控、信息管控、非法热点管控、行为分析、无线网络管理等功能,有效防止人员进行与工作无关的网络行为、提高带宽资源利用率、规避泄密和法规风险、保障内网数据安全、可视化管理以及全面管控无线 AP,真正做到有线无线统一上网行为管理。

深信服上网行为管理市场：连续 9 年上网行为管理市场占有率第一，服务于全国 18000 多家各行业用户，服务于 80%进入世界 500 强的中国企业，覆盖最高人民检察院、外交部、公安部等 60 多个政府细分行业;，服务于全国 18 个省的运营商用户，覆盖全国 32 个省级电子政务外网，地市区县覆盖率达 70%以上，金融行业中客户数达到 430 家,包括中农建工交五大行、招商、兴业、民生等 12 家股份制银行，服务于世界互联网大会、奥运会、世博会、亚运会、青奥会等大型活动。

6.VPN 接入网关

深信服 VPN 接入网关品牌：国家 SSL/IPSECVPN 技术标准核心制定者，2005 年推出全球第一款 IPSEC/SSL 二合一 VPN，国内唯一一家入选 GartnerSSLVPN 魔力象限厂商，率先在 SSLVPN 领域开发了远程应用发布技术

深信服 VPN 接入网关概述：用于端到端的安全防护，通过业内领先加密技术，多种认证方式、主从绑定等特色功能，保证用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全；通过多线路智能选路、单边加速等多项专利技术，从链路、传输、数据、引用，层层优化，访问速度可提升 80%，给每个接入用户不同以往的畅快体验。

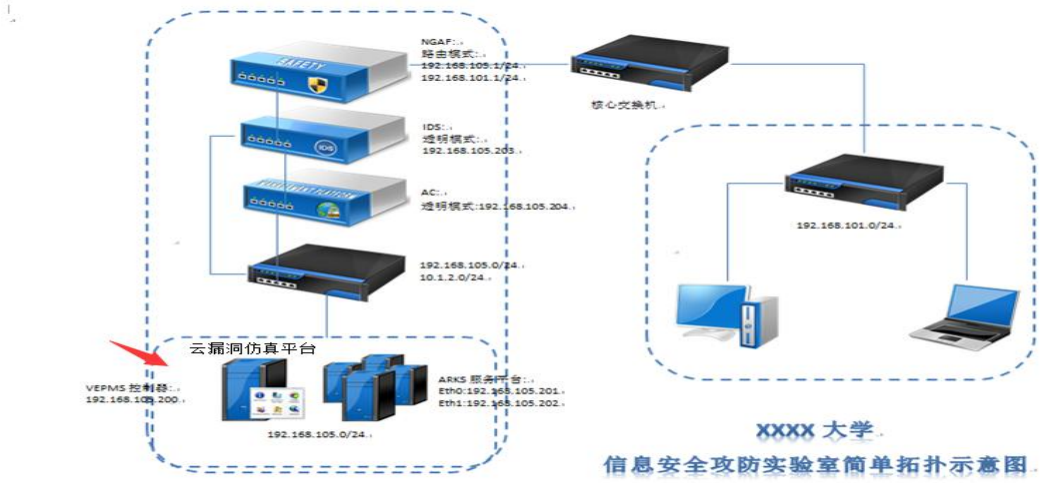
深信服 VPN 接入网关市场：连续五年市场占有率第一，市场份额超过 40%，用户数量超过 15000 家，囊括政府、金融、运营商、能源、教育、企业等各行业用户。拥有业内最多的高端客户，包括国务院国资委、海关总署、环保部、公安部、最高检、最高法、中国移动、中国联通、中国人民银行、银监会、伊利集团、海尔集团、三一重工、中广核等。中国 500 强企业中，有 70%的企业选择了深信服 SSLVPN 产品。

7.攻防平台

（1）漏洞仿真平台 IEC-516S-SY

深信服漏洞仿真实验平台是深信服研发的实验室安全、应用环境实验平台，主要面向信息安全实验室中行业应用环境生成、信息安全实验环境、课件设计等功能。

漏洞仿真平台能够支持复杂多样的实验环境以满足网络攻防、信息安全实验对基础实验环境的需求；内置多种网络攻防实验，能够与下一代防火墙等行业安全设备联动进行实验，以模拟真实行业网络环境；能够快速搭建实验环境、实验结束后可以快速高效的恢复实验环境，提高教学效率，简化信息安全实验室管理工作；支持环境生成器、应用生成器、实验设计器功能，用户可以根据教学需求快速搭建教学环境并生成相应实验课件，将用户的网络工程实验、信息安全实验与行业应用环境结合起来；可靠的带外管理及图像传输，保障使用过程中的网络攻击、信息安全等实验不会对实验管理造成影响；后续可以扩展支持信息安全实验包、行业应用环境包等丰富的实验课件。



图：攻防模拟实验拓扑

（2）平台具有如下特性：

•支持复杂多样的实验环境

•支持搭建真实行业特色应用实验环境

•多种网络攻防实验并支持更多实验包扩展

•高效的实验设计、课件生成功能

•高性能实验平台

•简便、可靠的管理方式

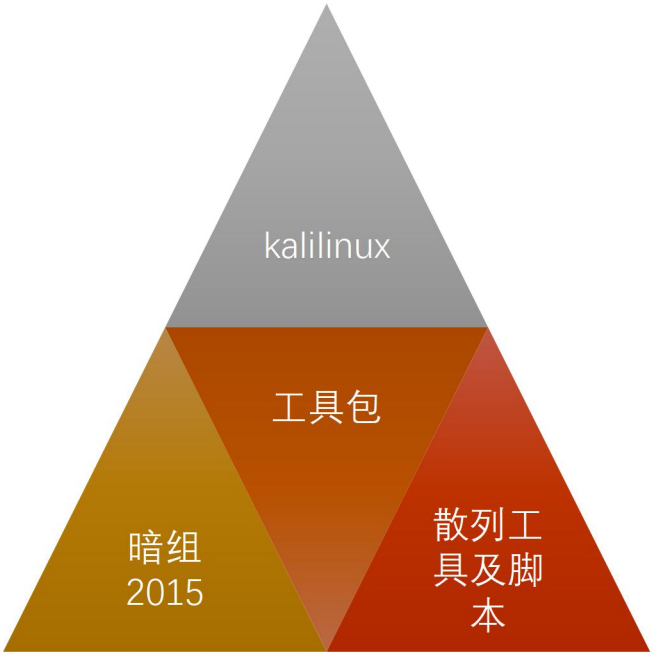
•完善的远程实验支持

•内容丰富的信息安全实验包

•方便的虚拟机使用方式

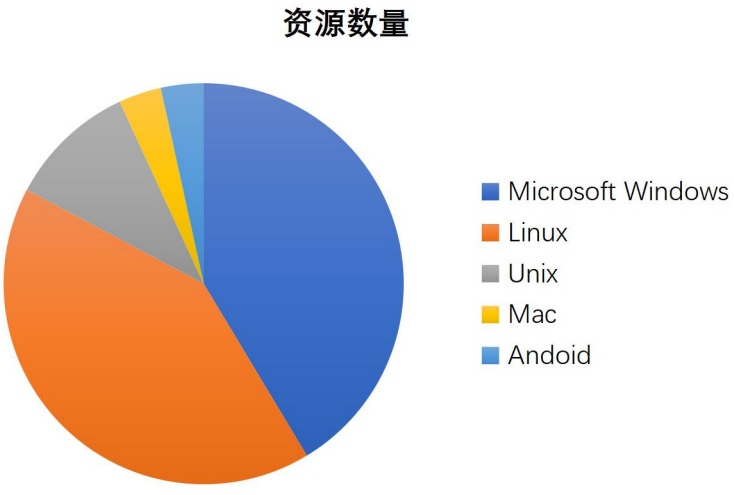
（3）渗透工具包

渗透工具包是以渗透测试工具为核心内置于服务器上的综合性管理系统，通过非任务执行模式来进行工具的应用，当获取到敏感数据和信息时，可以利用系统内部其他工具来智能的进行更深层次渗透测试，使得整个渗透测试工作都能依靠系统来进行，适用于初学者使用。其主要分为 kalilinux，暗组 2015 工具集合包及一些散列的工具及脚本，共计 1000 多个工具。



图：攻防课件资源池

攻防实验课件资源是存放在云漏洞仿真平台里的环境模板，包含密码学、PKI、缓冲区溢出与漏洞分析、恶意代码分析、软件水印、安全编程、windows 取证和司法鉴定、数据保密安全、隐写软件安全及使用、信息隐藏、安全风险评估、数据库攻击技术及安全、网络欺骗技术、网络攻防分析、安全防护、web 应用安全、KaliLinux&BT5、社会工程学、入侵检测、容灾备份、网络扫描与嗅探等二十五个大类，在每个分类中均提供数量可观的安全实验课件资源。从 Windows95 到 Windows8，从 FreeBSD 到 MacOS，平台能支持目前市面上所存在的大部分基于 X86 结构的操作系统（包括 x86andoid 系统），扩充了课件资源的丰富程度。



图：漏洞平台综合实验管理系统

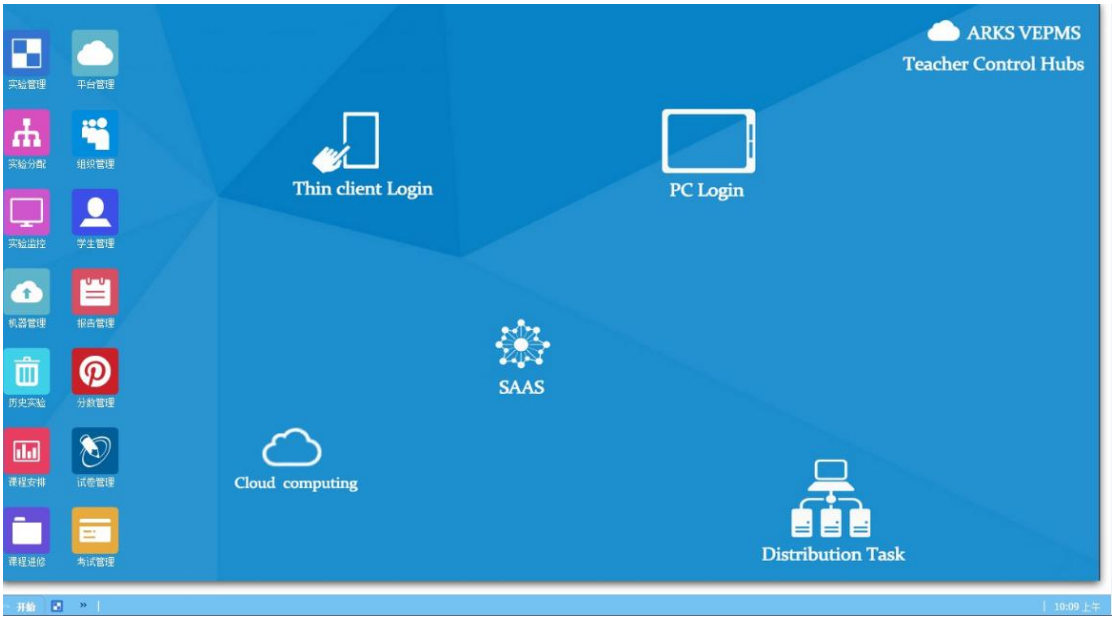
综合实验室管理平台作为整个云漏洞仿真平台的核心，对云漏洞仿真平台的所有资源进行统一调度，让整个安全实验室环境成为一个整体。综合实验室管理平台对教师和学生提供不同的功能接口。

8. 学生接口

学生登陆综合实验室管理平台选择相应的课程，综合实验室管理平台即可自动生成一个独立的符合课程要求的实验环境以供学生进行实验，并对整个实验情况以及结果进行详细的跟踪和记录；

9. 教师接口

通过教师接口，教师们可以根据课程的进度，对实验进行授权，开启或关闭相关的实验环境。可以根据课程的不同需要自定义不同的网络结构，综合实验室管理平台会根据定义好的网络结构自动组成网络环境共实验使用。同时教师可以用过查看学生的操作过程记录和结果对实验情况进行评分。

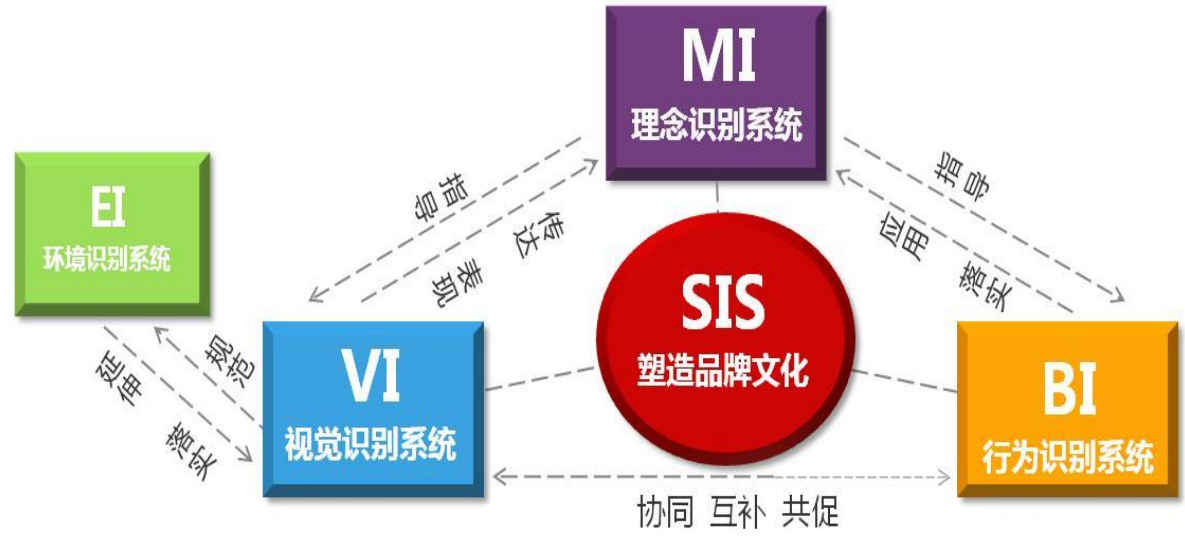


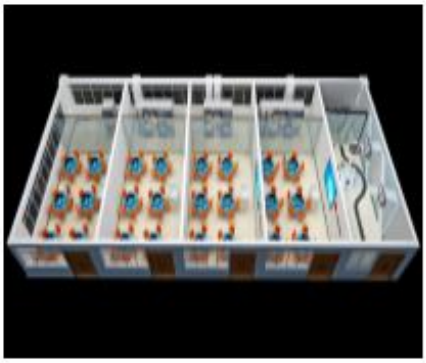
10. 实训室 VI 设计

院校传统的实训室只是满足基本教学需求，从实训室设计和布置上没有考虑本专业的特殊性，也没有针对教学进行专门的优化，环境千人一面，不能提高学生的兴趣，新一代深信服信息安全实

训室的设计，是让信息安全专业群学生了解信息安全发展的背景、发展现状以及发展趋势，从根本上了解信息安全产业，充分展现文化识别。另一方面也充分融入了深信服的企业文化，深刻体现了校企合作，工学一体的办学思想。

深信服可提供信息安全实训室 VI 设计服务：包括实验室外墙设计、内墙设计、桌椅设计、实验室布置图、施工图、实验室装饰海报设计。





（二）实训课程体系设计

深信服信息安全实训室课程主要以信息安全产品应用教学为主，并提供用于学生拔高能力的的攻防课程。

信息安全应用教学课程资源包包含：下一代防火墙技术与应用、VPN 接入网关技术与应用、上网行为管理与安全审计技术与应用、应用交付技术与应用等商用主流安全技术在信息安全的整体建设、规划、运维方面的具体应用课程。资源包含实训教材、实验指导书、电子教案、PPT、视频课件，为学生的学习、老师的授课提供一整套配套工具，方便教与学的顺利开展。

信息安全应用课程共计 128 学时，10 学分。

1.《下一代防火墙技术与应用》建议 32 学时 3 学分

（1）课程目标

●掌握网络安全系统基础知识

●了解网络安全威胁和发展趋势

●掌握防火墙的基本概念和技术演进

●掌握深信服下一代防火墙的重要功能和模式

（2）课程内容：

●防火墙概论

●防火墙技术

●基本网络配置及常见网络环境部署

●VPN 互联技术

●服务器防护技术

●网页防篡改技术

●流量管理技术

●高可用技术

●风险发现与防护技术

●常见攻击测试技术

●产品部署排错

2.《构建安全 VPN 网络》建议 32 学时 3 学分

（1）课程目标：

●掌握密码学理论知识

●掌握 VPN 的体系结构和各 VPN 的选用

●掌握 3G/4GVPN、WIFIVPN、IPsecVPN、SSLVPN 的原理

●掌握 MIG 一体化网关的管理和配置

●掌握深信服 SSLVPN 接入平台的管理和配置

（2）课程内容：

●密码学的基本概念

●对称和非对称密码

●密钥交换技术

●数字签名

●公共密钥基础设施

●VPN 的体系结构

●3G/4GVPN 的工作原理和配置

●WIFIVPN 的工作原理和配置

●IPsecVPN 的工作原理和配置

●SSL 协议的工作原理

●深信服 MIGVPN 的主要功能和实现原理

●深信服 SSL/IPsec 二合一 VPN 的组网与配置

3.《安全审计与上网行为管理》建议 64 学时 4 学分

（1）课程目标

●了解网络病毒的特点和防御手段

●熟悉内网安全与审计技术的实现和典型应用

●掌握 SSL 内容识别、上网时长控制，流量配额适用场景及配置方法

●掌握虚拟线路及流控子通道适用场景及配置方法

●掌握网关杀毒测试方法

●掌握链路负载适用场景及配置方法

●掌握事件告警配置

●掌握深信服 AC 的部署于配置

（2）课程内容

●内网安全控制及审计技术的概念

●深信服 AC 的安装、配置及管理

●短信认证及微信认证

●单点登录的应用场景

●深信服 AC 无线管理

●深信服 AC 系统管理

●深信服 AC 流量管理

●网络病毒的起源、历史和发展

●常见的计算机病毒

●计算机病毒症状与传播途径

●深信服 AC 安全防护体系

●内网安全控制及审计技术的典型应用

拔高用的攻防课程主要包含：密码学、PKI、缓冲区溢出与漏洞分析、恶意代码分析、软件水印、安全编程、windows 取证和司法鉴定、数据保密安全、隐写软件安全及使用、信息隐藏、安全风险评估、数据库攻击技术及安全、网络欺骗技术、网络攻防分析、安全防护、web 应用安全、KaliLinux&BT5、社会工程学、入侵检测、容灾备份、网络扫描与嗅探等方面。主要涉及课程信息安全数学基础、信息安全概论、系统安全、网络安全等基础课程。

最后，通过深信服的信息安全真实行业案例让学生充分理解信息安全的应用环境及场景，使学生在真实的网络环境中完成技术实践，具备行业安全人才必备的思考方式和技术能力。

（三）细致周到的师资培训

深信服为每所学校提供 1-2 个名的信息安全师资培训服务，包含 32 课时的专业技能和项目案例培训、4 课时的授课技巧培训、4 课时的实验室管理培训。

深信服根据学校老师时间，灵活提供月、季度、寒暑假期间的师资培训，学校老师可根据邀请函选择参与集中培训、或者灵活选择各省会城市单独培训。

深信服可提供院校专业教师到当地渠道处随工项目实习的机会，积极采取校企合作、企业培训、顶岗实习等多种方式方法，提升教师的理论水平、教学水平和实践能力。

为了能够使教师快速掌握实验内容，深信服还准备了与实验内容配套的在线实验课程，教师可以随时登陆学习，快速提升自己的实验能力，这样可以解决教师由于工作繁忙，无法参加集中的教

师培训的问题，也可以使教师在参加教师培训后，能够随时随地巩固所学知识，更好地指导学生实验。

深信服会根据技术的发展开发新的实验文档，在云端实时更新。学校老师可授权访问深信服教学资源库，根据老师要求开放所需视频课件、电子教材、教案访问、下载权限。

深信服师资培训还提供以下服务：

1.参加厂商提供的师资培训和认证，获得深信服认证信息安全讲师资格证书

2.与全国其它学校老师共享交流教学经验

3.获得厂商后续服务，获得最新教学资料

4.合作开发教材

5.参与评选优秀教师

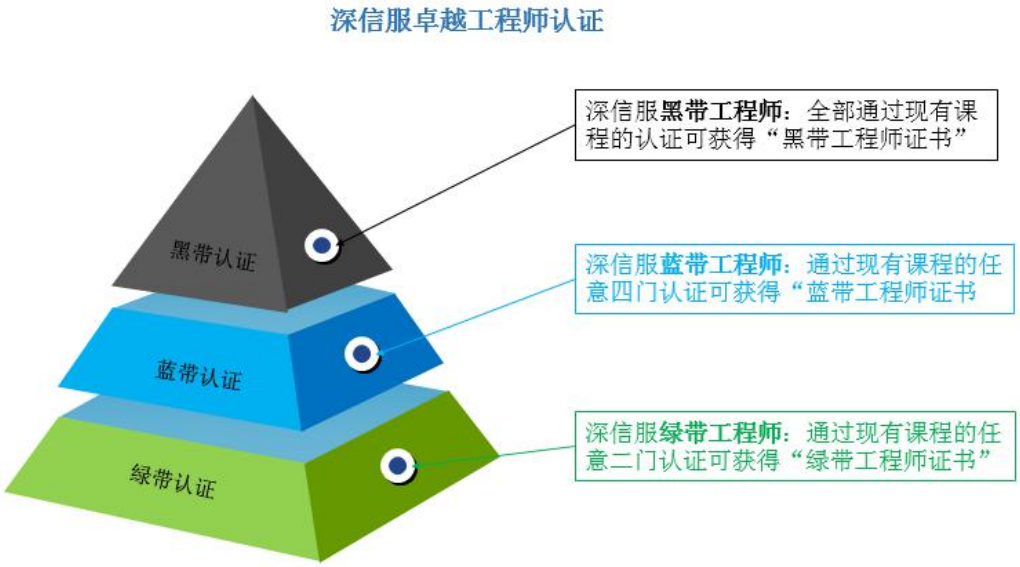
（四）完善的资格认证体系

深信服鼓励学习信息安全课程的在校学生积极参与深信服卓越工程师资格认证考试，深信服为参加信息安全实训的的在校学生提供以下服务：

1.免费参加结业考试，学员学习完课程，由学校组织结业考试，考核通过后由深信服公司颁发《深信服网络学院结业证》。

2.参加专业的考试服务商 ATAC 权威认证考试并通过后，可获得“深信服卓越工程师”认证证书。

3.有机会获得深信服公司每年向优秀学员颁发的荣誉证书和奖励。



（五）多层次校企合作

1.共建“深信服网络安全学院”

深信服网络安全学院是深信服科技推出的校企合作模式之一，院校可以通过申请网络安全学院，来对学生开展深信服职业资格认证服务，把厂商的认证课程引入到课题教学中，实现课程置换。

2.推荐实习就业：

通过深信服信息安全实训学习，且通过认证考试的获取认证证书的优秀学员，深信服优先荐到深信服当地核心渠道实习就业，并由深信服组织核心渠道进行校园专场招聘，通过建设线上人力资源平台、数据库，提供四方接口，为认证学生、核心渠道、企业客户等安全、虚拟化人才供需方提供双向选择平台；

三、信息安全专业共建的重要意义

（一）学生方面

1. 高质量就业保障

参加校企合作信息安全专业共建的学生，凡学习表现合格的，就获得进入公司广泛的合作伙伴的工作机会，获得广阔的发展空间。

2. 综合竞争力提升

深信服“信息安全”共建专业为学生开设的职业素质、专业技能培养科目，在信息安全行业一般只针对各大知名网络厂商已经入职的新员工开设。这些将让学员在学习知识的同时提升职业化素养，增强综合能力，并获得宝贵的业务实践经验，这些不但能增强学生在就业时的竞争力，更能让学生走上良性发展的职业化道路，获得终生受益。

3.良好经济效益

深信服“信息安全”共建专业学生，在企业实践期间，可以按照企业标准获得实习工资、出差补贴，在收获工作经验和技能的同时还可以获得收益，为父母解愁。

学生顺利毕业进入企业，将得到稳定的工资，另外，深信服“信息安全”共建专业根据培养规划考取信息安全相关技术认证后，一方面可以拿到证书提升自己的竞争力，另一方面在加入企业后更可以获得加薪激励，相当于将认证考试的费用逐步回收，这个政策是业内一般企业所没有的。

（二）学校方面

1.提高学生就业率和就业质量

深信服“信息安全”共建专业学生只要合格，具有良好的就业保障，获得高质量就业，另外更推荐到公司广泛合作的信息技术厂商、运营商、渠道合作伙伴就业，实现学生就业率和质量的双增长。

2.帮助提升学校办学水平

通过共建专业，学校方面一方面获得可以推广应用的优秀培训教学教材，另一方面再与企业合作和交流中，可以吸收信息行业人才培养的实践经验，让学校的相关教师通过业务实践的锻炼实践经验和能力，运用到办学之中。这些都对提升学校办学水平有良好的促进作用。

3.树立学校品牌

信息安全精品专业的建设，体现了学校响应国家加快发展现代职业教育的战略规划要求，并大力拓展办学创新的精神，有利于树立学校品牌和在职业教育领域的地位，这种品牌的提升是学校的一项无形资产，对学校的各方面建设和发展都有深远意义。

4.带来良好经济和社会效益

通过深信服“信息安全”共建专业，不但帮助学校提升在校学生的就业率，而深信服“信息安全”共建专业教学的高水平，所培养学生的高质量就业、以及先进的实训都会在当地产生良好的社会效应，这一方面可以使得学校招生的生源数量、质量得以提升，另一方面还可以帮助学校更有效得参与当地社会的信息化建设，开展信息化应用、实验、开发、认证、培训等的增值服务，成为区域信息化建设的龙头。这样学校也能得够获得良好的经济效益。

（三）企业方面

1.获得持续稳定的高素质人才

通过深信服“信息安全”共建专业，企业可以在各地信息技术专业院校持续不断地培养一批认同企业文化，熟悉企业技术，具有优良的信息安全技术服务能力和意识的高素质人才，对于企业的发展有决定性的支撑作用。

综上所述，深信服“信息安全”共建专业项目，对于学生、学校、企业都能带来良好的收益，实现三方共赢。