

工业和信息化部 电子工业标准化研究院培训中心

电标培〔2024〕024号

关于举办《网络安全体系架构师规划与部署实践沙盘演练课》

培训班的通知

各有关单位：

随着云计算、大数据、物联网、移动互联等新技术不断迭代，黑客攻击从脱库已经演变为实时盗取数据阶段，网络安全运营者如何开展体系设计？如何从技术上实现层层防护，设关布阵，如何能够实现安全态势监控、入侵流量拦截、分析入侵程度、快速应急响应，这些都已经成为企事业网络安全技术专家和骨干必须掌握的关键技能。本课程定位于培养“网络安全体系架构师”，从单位一线需求出发，结合现网建设程度，按照国家法律法规要求，以沙盘演练方式开展架构师级的能力训练，为企业储备一批政治和技术都过硬的技术管理人才。

本课程管理篇让学员站在管理高层视角分析如何从战略到架构设计，研讨如何把握好网络安全风险？如何做好顶层规划？如何做好信息化战略规划和架构设计过程中的“排雷”工作？通过授课专家解读法律法规标准，结合等保 2.0 和关基保护要求，通过案例场景形象生动讲述体系架构设计的重要性，沙盘中演练分析企业网安差距，熟悉如何制定企业发展的方针和策略，

如何让各项安全工作全面落地。

本课程技术篇以 HW 为基线，研讨如何真正防住黑客，根据常见攻防技术、典型案例、典型问题等设计而成，通过典型案例分析提高人员的安全防范意识和技能。在网络安全攻防技术方面，通过“红黑演义攻防演练云平台”，使学员进行防守技能实操练习，通过“知己知彼”的战术，提高单位网络安全人员的防守技能。

工业和信息化部电子工业标准化研究院培训中心定于 2024 年 3 月 26 日-30 日在苏州举办《网络安全体系架构师规划与部署实践沙盘演练课》培训班。具体安排如下：

一、培训内容

日 期		课程名称	课程内容简介
第一天	上午	网络安全相关法规与企业现状之间有哪些合法合规差距？	1) 企事业单位网络安全管理当前学员困惑抛出 ■ 管理高层已认识到网络安全很重要，但如何真正落实下去？心里没抓手 ■ HW 被打穿而同时又要忙于应对国家监管合规，该如何建立应急体系？ ■ 安全管理喊口号刷脸时代远去，机制如何建立才能管住部门、管住个人？ ■ 设备软件堆如山却不知防御水平高低，如何开展保障能力评价好放心？ ■ 如果网络事件不能绝对避免，如何尽职尽责从而免责或减责？

		网络安全工作重点核心如何建立	2) 国内外网络安全形势与安全惨痛案例分析 ■ 网络安全法处罚案例分析 ■ 网络入侵损失案例分析 ■ 商业秘密泄密案例分析 3) 中办《党委（党组）网络安全工作责任制》 4) 《网络安全法》解读与等级保护政策深度剖析； 5) 《数据安全法解读》与《个人信息保护法解读》解读与合规差距分析 6) 网络安全工作高管领导的抓手如何建立？ 7) 工作核心建立：网络安全责任制与量化考核
	下午	国家强制性合规政策要求如何开展合规建设演练	1) 等级保护制度深度解读 ■ 等级保护相关定义和发展历程 ■ 等级保护工作流程和重要环节 ■ 等级保护 2.0 基本要求及要点讲解 ■ 等级保护各级别所需要的软硬件概述 2) 网络安全等级保护体系建设指引 ■ 等级保护建设整改中安全管理体系建设 ■ 等级保护建设整改中安全技术体系实现 3) 国内外网络安全标准与行业规范如何落地 ■ 《网络安全审查办法》 ■ 网络安全建设规划相关国内外标准介绍 ■ 等保 2.0、ISO27001 对比解读 ■ 《关键信息基础设施网络安全保护要求》解读 4) 网安管理架构设计分组沙盘演练 ■ 小组划分 ■ 角色扮演 ■ 沙盘演练

第二天	上午	如何让运维工作始终处于安全状态？	1) 国内网络安全运维现状分析 ■ 国内外安全建设现状对比与问题分析 ■ 网络安全运维中踩“红线”案例场景分析 ■ 网络安全运维所面临的问题总结 ■ 周期性的安全评估与考核机制 ■ 重保与护网攻防演习如何做的更好？
		企业应急管理如何合规？如何避免“天天处于救火状态”	1) 应急管理体系建立 ■ 大中型企业惨痛案例分析 ■ “国家网络安全事件应急预案”合规要求 ■ 建立应急管理体系的概念与目的 ■ 如何建立应急管理体系 2) 业务安全分析与业务流程梳理演练 ■ 安全关键路径分析与风险点识别
		审计、法务和人力资源部门应该如何开展网络与信息安全工作？	2) 审计部门网络安全审计实践演练 ■ 网络安全法律标准合规审计 ■ 网络与信息安全审计如何开展 3) 法务部网络安全法律应用演练 ■ 网络安全法差距分析与合规护航开展 ■ 数据安全与个人信息保护宣贯与落地 ■ 信息化建设类合同网络与信息安全审核 4) 人力资源网络安全合规演练 ■ 自有员工岗位网络安全职责界定 ■ 员工招聘、绩效与离职时如何管理 ■ 外包人员人力风险识别与控制措施 ■ 网络安全骨干与梯队人才培养机制

	下午	业务部门、数据管理部门、软件开发测试部门网络与信息安全如何管理？	1) 业务部门网络与信息安全工作演练 ■ 业务部门网络安全责任界定与界面划分 ■ 业务系统中的网络安全风险识别与应对 ■ 业务系统中数据异常规则设计与监测 ■ 业务系统中数据分级分类与访问权限
			2) 数据管理部门数据安全工作演练 ■ 国内数据安全现状分析 ■ 数据与个人信息安全如何保护？ ■ 数据安全防护体系建设路线
			3) 软件开发测试部门软件安全工作演练 ■ 软件安全漏洞现状与成因 ■ 软件人员与业务人员中间壁垒如何打破 ■ 软件安全工作需要生命周期管理 ■ 如何做好变更和配置管理避免大灾难
第三天	上午	网络安全架构规划设计演练	1) 如何从业务角度分析网络安全风险？ 2) 网络安全体系化建设与规划思路 3) 如何进行网络安全架构设计？ 4) 如何建立网络安全体系并持续优化？ ■ 防火墙防御配置与渗透分析 ■ 堡垒机防御配置与渗透分析 ■ WAF 防御配置与渗透分析
		系统与应用架构规划设计演练	1) 典型黑客入侵思路路线分析：重点 APT 攻击 2) 网络层攻击溯源实战演练：实操+场景推演 3) 主机层攻击溯源实战演练：实操+场景推演

	下午	HW 蓝队建设与 排兵布阵迎战	1) 红队入侵路线 2) HW 前期自查演练 ■ HW 工作要点 ■ 资产梳理实战指导 ■ 漏洞如何加固好 ■ 网络安全防护网如何建立 3) HW 中如何应急处置 4) 如何实现事件闭环管理
		HW 红蓝队攻防 对抗演练	1) 网站挂马过程重现实践演练 2) 内网渗透重现实践演练 3) 网站挂马入侵侦察分析实践演练 4) 网站挂马入侵应急响应实践演练

二、培训方式、时间、地点

本次培训采用面授的方式开展，过程中穿插案例分析、剧本杀式场景推演、实践落地沙盘演练。

2024 年 3 月 26 日-3 月 30 日(26 日全天报到)

地点：苏州，具体地点详见《报到通知》

会务组将于开班前一周将《报到通知》发给各参培学员，详细报到地点、乘车路线、食宿及日程安排等事宜。

三、参加对象

培训对象为网络安全技术人员、系统管理员、网络管理员、应用管理员和数据管理员等企事业单位骨干人员，涉及到企事业一线网络与数据安

全管理、规划设计、部署实施、优化改进相关工作。

四、证书颁发

考试合格者，由工业和信息化部电子工业标准化研究院统一颁发《网络安全体系架构师》培训证书。

五、学习费用

培训费：5800 元/人（含师资、教材资料费、证书费、辅导费等；含三天午餐；晚餐及住宿统一安排，费用自理）。

六、报名须知

此次培训工作将由启强赐恒科技（北京）有限公司具体承办，请参加培训的学员认真填写报名表，以电话、传真及邮件的方式反馈至我单位。

电 话：010-53397598 010-64102658

联系人：田 悦 张筱悠

联系邮箱：2021411678@qq.com

七、汇款账号

单位名称：启强赐恒科技（北京）有限公司

开 户 行：中国农业银行股份有限公司北京房山城关支行

汇款帐号：1110 0101 0400 23694

汇款附言： 网络安全体系培训费（姓名、单位）

附件 1：报名表

附件 2：个人信息备案表

工业和信息化部电子工业标准化研究院

培训中心

2024 年 1 月 11 日

附件 1

《网络安全体系架构师规划与部署实践沙盘演练课》

报 名 表

姓名	性 别	部 门	职 务	手机	邮箱
培训形式	面 授				
发票类型	☒ 增值税普通发票		☐ 增值税专用发票		
开票项目	技术服务费 （备注说明：网络安全体系培训费）				
增值税发票开票信息（以提供信息为准，确保无误）					
单位名称			纳税人识别号		
地 址			电 话		
开户行			账 号		
汇款账号	户 名： 启强赐恒科技（北京）有限公司 开 户行： 中国农业银行股份有限公司北京房山城关支行 账 号： 1110 0101 0400 23694				
地点北京；是否住宿： ☒ 是 ☐ 否 预定房间数量（ ）			单 位 印 章 日期： 2024 年 月 日		
注：各参培人员请在报名 3 日内将相关费用通过银行等方式付款，会务组确认到款后，统一开具发票。					
联 系 人：田 悦 18511991911 （同微信） 联系电话：010-53397598 传真：010-53397598 邮 箱：2021411678@qq.com					

附件 2

《网络安全体系架构师》个人信息备案表

姓 名		性 别		正面免冠彩色照片 (2 寸)	
政治面貌		最高学历			
证件名称					
证件号码					
工作单位					
通信地址			邮 编		
联系电话			办公电话		
传 真			电子邮件		
最高学历	时 间	毕业学校		学 历	专 业
网络与信息 安全行业工 作经历	起止日期	工作单位	职务	主要工作任务	