附件 2

安全运营工程师培训内容

章节	课程名称	培训内容	课时
初级课程（40 课时）			
1	课程介绍及概述	介绍课程体系、培训体系、教学内容	1
2	安全运营概述	主要介绍安全运营的基本概念和方法，重点介绍安全运营的目标、模型、内容、团队和流程等方面	2
3	弱点检测	常见 Web 漏洞详解	3
		常见网络安全漏洞详解	2
		弱点扫描器介绍与实践	2
		常见漏洞验证实践	2
4	安全运维	防火墙设备介绍与管理	3
		Web 应用防火墙介绍与管理	2
		堡垒机设备介绍与管理	2
		审计类设备介绍与管理	2
5	安全监测	全流量分析设备介绍与实践	3
		EDR 终端安全系统介绍与实践	3
		态势感知系统介绍与实践	3
6	应急响应	安全事件响应概述	2
		终端检测与排查（Windows）	3
		终端检测与排查（Linux）	3
7	课程测试	对所学内容进行测试	2
中级课程（40 课时）			
1	课程介绍及概述	介绍课程体系、培训体系、教学内容	1
2	安全运营概述	主要介绍安全运营的基本概念和方法，重点介绍安全运营的目标、模型、内容、团队和流程等方面	2
3	安全运营组件介绍	主要介绍安全运营所需的各类组件和设备，重点介绍终端类防护设备、边界类防护设备、流量检测类设备、安全信息和事件管理(SIEM)、态势感知类设备、安全编排与自动化响应类设备（SOAR）等的功能、特点和应用场景	2
4	风险识别	风险识别概述	1
		资产运营及管理	1
		脆弱性管理	2
5	安全防御	纵深防御体系	1
		安全加固	1

章节	课程名称	培训内容	课时
		威胁情报运营	1
		欺骗防御	1
		红队评估	2
6	安全检测	网络监控和分析	8
		威胁检测与分析	4
7	事件响应	安全事件响应概述	1
		终端检测与排查（Windows）	1
		终端检测与排查（Linux）	1
		钓鱼邮件的预防与处置	1
		远控木马通用排查技术	1
		勒索病毒网络安全应急响应	1
		数据库攻击应急响应	1
		溯源反制技术	1
8	运营管理	安全运营制度及流程	1
		安全运营指标	1
		持续改进、分析和自动化	1
9	课程测试	对所学内容进行测试	2
高级课程（40 课时）			
1	课程介绍及概述	介绍课程体系、培训体系、教学内容	1
2	安全运营概述	主要介绍安全运营的基本概念和方法，重点介绍安全运营的目标、模型、内容、团队和流程等方面	2
3	SOC 设计与规划	主要介绍构建安全运营中心所需的关键要素，包括 SOC 的架构、人员、流程、技术、工具、服务和指标等	2
4	安全防御	入侵和攻击模拟	3
		安全运营防御模型	2
5	威胁检测与分析	入侵分析	8
		时间线分析	4
6	事件响应	高级应急响应	4
		恶意样本分析	8
7	指标、自动化和持续改进	指标、自动化和持续改进是安全运营的核心要素，它们可以帮助安全运营团队有效地衡量和提升安全能力，降低安全风险，提高安全效率，满足业务需求	4
8	课程测试	对所学内容进行测试	2