网络安全应急响应管理

一、课程描述：

本课程从管理及规范角度讲解了网络安全应急响应预案的构建以及应急的技术规范。内容包括：网络安全应急响应概述、网络安全应急响应实践、网络安全应急响应技术与平台、网络安全应急响应案例分析等。为学员提供理论指南、实践指导和趋势指引。

二、课程大纲：

第 1 讲 网络安全应急响应综述
- ◇ 什么是应急响应
- ◇ 什么是网络安全应急响应
- ◇ 网络安全应急响应的形势与挑战
- ◇ 网络安全应急响应的探索与实践
- ◇ 网络安全应急响应的发展与趋势

第 2 讲 网络安全应急响应的法律法规、政策与相关机构
- ◇ 我国网络安全应急响应的法律法规、政策与相关机构
- ◇ 国外网络安全应急响应的法律法规、政策与相关机构

第 3 讲 网络安全应急响应的标准与模型
- ◇ 网络安全应急响应的国家标准
- ◇ 网络安全应急响应的常用模型
- ◇ 网络安全应急响应的常用方法-PDCERF（6 阶段）

第 4 讲 建立网络安全应急响应体系
- ◇ 网络安全应急响应处置的事件类型
- ◇ 网络安全应急响应事件的损失划分
- ◇ 网络安全应急响应事件的等级划分
- ◇ 建立网络安全应急响应的组织体系
- ◇ 网络安全应急响应体系的能力建设

第 5 讲 网络安全应急响应与实战演练
- ◇ 网络安全演练的必要性与目的
- ◇ 网络安全演练的发展和形式
- ◇ 网络安全实战演练攻击手法
- ◇ 网络安全实战演练的管控要点
- ◇ 红、蓝、紫三方的真实对抗演练

第 6 讲 网络安全应急响应的具体实施
- ◇ 检测阶段
- ◇ 抑制阶段
- ◇ 根除阶段
- ◇ 恢复阶段

第 7 讲 网络安全应急响应事件的总结
- ◇ 总结阶段
- ◇ 应急响应文档的分类
- ◇ 应急响应文档示例

第 8 讲 重要活动的网络安全应急保障

- 重保风险和对象
- 重保方案设计

第 9 讲 网络安全应急响应中的关键技术

- 灾备技术
- 威胁情报技术
- 态势感知技术
- 流量威胁检测技术
- 恶意代码分析技术
- 网络检测响应技术
- 终端检测响应技术
- 电子数据取证技术

第 10 讲 网络安全应急响应中的平台和工具

- 新一代安全运营中心
- 网络安全应急响应工具箱
- 网络安全应急响应中的常用工具

第 11 讲 网络安全漏洞响应平台

- 漏洞概述
- 国内外知名的漏洞平台
- 第三方漏洞响应平台

第 12 讲 大中型企业的网络安全应急响应典型案例

- 部分行业网络安全应急响应案例总结
- 勒索软件攻击典型案例
- 网站遭遇攻击典型案例
- 服务器遭遇攻击典型案例
- 遭遇 APT 攻击典型案例
- 忽视网络安全建设易遭遇的问题
- 安全意识不足易遭遇的问题
- 第三方企业系统造成的安全问题
- 海外竞争中遇到的安全问题