کارگاه آموزشی

جرم‌یابی و پاسخ‌گویی به حوادث امنیتی در شبکه‌های رایانه‌ای

مهندس سبحان علی‌آبادی

آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

چکیده: هدف از این کارگاه آموزشی ایجاد آمادگی و آشنایی مخاطبین با راه‌کارها و ابزارهای مناسب در برخورد با حملات، تهدیدات و جرائم سایبری در شبکه‌ها و سیستم‌های رایانه‌ای می‌باشد. با توجه به رشد فزاینده‌ی تهدیدات امنیتی در شبکه‌ها و زیرساخت‌های ارتباطی و لزوم آمادگی و کسب دانش و تخصص‌های مرتبط در پاسخ‌گویی و رسیدگی‌های فنی، ضمن بیان ضرورت‌ها و مفاهیم مرتبط، دانش و فناوری‌های مورد نیاز جهت تشکیل تیم‌های فنی در رسیدگی و پاسخ‌گویی به حوادث امنیتی شرح داده می‌شود.

سرفصل کارگاه:

- ضرورت پاسخ‌گویی به حوادث و رخدادهای امنیتی و ماموریت‌های مراکز آپا
- جرم‌یابی دیجیتالی و حوزه‌های مرتبط
- تشریح جرم‌یابی شبکه‌های رایانه‌ای
- مقایسه‌ی جرم‌یابی سنتی و جرم‌یابی نوین
- انواع روش‌های پاسخ‌گویی به حوادث امنیتی
- ایجاد آمادگی فنی در مهیاکردن شبکه و زیرساخت در زمان پاسخ‌گویی
  - پروتکل‌های پایش
  - مرکز عملیات شبکه (NOC)
  - مدیریت اطلاعات و رخدادهای امنیتی (SIEM)
  - مرکز عملیات امنیت (SOC)
- راه‌کارها و ابزارها
- چالش‌ها و موانع

مدت زمان کارگاه: ۴ ساعت