

When a cyberattack hits, your SOC team is your first and last line of defense. It is imperative that they are ready.

Training Outline

Incident Response - Principal Tactics

CybergymIEC's comprehensive Incident Response - Principal Tactics training will not only test your SOC team's theoretical knowledge and practical skills, it will also give them the opportunity to work 'under fire' – together, as a team – to mitigate a cyberattack.

Your experts will be required to manage and lead a complete incident response process, from the moment our 'hackers' infiltrate 'your systems', until they have foiled the attack. Through a combination of theoretical content, case studies, practical tools, and realistic hands-on training in our cyberwarfare arena, participants will gain in-depth knowledge of incident response concepts and tools that will enable them to manage, investigate and analyze real-life cyber incidents.

Over the course of the training, your team will practice corporate security policies and compliance with standards and regulations, while learning to develop and optimize policies and procedures. They will also evaluate the extent of the damage, assign responsibilities, and detect and mitigate real-life complex APTs, all in a realistic setting that replicates your actual work environment.



Participants

- IT Professionals
- Incident Response Team Members



Prerequisites

- Understanding of basic information security concepts and tools
- Familiarity with networking principles, architecture, and protocols
- Knowledge of computer and operating system architectures and internals



Training Outcomes

- A new perspective – from the hackers' point of view
- The necessary expertise, methodology and skill set required to be an effective first responder
- Practical experience in working as a team to overcome a cyberattack



Duration

- 24 hours (3 x 8-hour days)

#IncidentResponseTeam #Investigating #Analyzing #CyberPolicies #Compliance #CoreSkills #FirstResponder