Module 15– Objectives and Key Instruction Points

Objectives:
Response is guaranteed to happen in a CDC. The probability of attack is one. Teams must have some sense of what to do prior to the attack. Response is stressful, and not being prepared makes it more so. Moreover, winning is an objective that motivates the responders in part. In reality the defender is never a winner in an attack that is sufficiently successful to merit a response. The question is how well did the defenders minimize losses and costs. Students need a greater understanding of response in order to plan.
The guiding question is "What concepts and skills do students need to be successful defending an IT environment within the CDC?"

Video Segment 1 –

1. Introduction to response
2. Resilience
3. Block
4. Evaluate, Contain, Eradicate, Recover (addressing vulnerability(s))
5. Impact management
6. Response planning

Activities

Name	Objectives	Content ideas
Activity1	Develop a hypothetical response strategy to a worm inside the environment	It may be necessary to establish a fictional IT environment to provide some technical context to the scenario and provide a control set to which they can refer in their response strategy.
Activity 2	Practice response to a hypothetical incident case	Provide students a small collection of VMs that have undergone an attack. Set the context for the IT environment provided and provide initial indicators. Response teams should be no larger than a typical CDC team. Provide either CDC based or industrial criteria for the responders to incorporate as constraints and priorities.

Activity design

Handouts
Title:

Revision: 20131113

Objectives:
Length: X pages
Notes: