Section Introduction, Preparation

This section of the Incident Response domain will teach you how organizations should prepare for and prevent incidents from occurring. This includes forming an incident response team, plans, policies and procedures to support the overall incident response process, and develop or deploy security controls that can work to prevent incidents before they occur.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Demonstrate an understanding of how incident response teams can be composed, the skills that are needed, and the departments that are typically involved.
- Demonstrate an understanding of host defenses, including anti-virus, endpoint detection and response (EDR), and group policy objects (GPOs) in Windows domains.
- Demonstrate an understanding of network defenses, including intrusion detection and prevention systems (IDPS), network access control (NAC), and firewalls.
- Demonstrate the ability to deploy Snort, the open-source IDPS, and create simple custom rules.
- Demonstrate an understanding of email defenses, including spam filters, marking external emails, and attachment filtering.
- Demonstrate an understanding of physical defenses, including deterrents, monitor, and access controls.
- Demonstrate the ability to suggest appropriate physical security controls for a fictional facility.
- Demonstrate an understanding of human defenses, including awareness training, positive reinforcement, and incentives.