Lab Assignment



Cybersecurity Professional Program

Digital Forensics &
Incident Response

# Incident Response Preparation

## DFIR-02-L3
## Incident Response Plan

## Lab Objective

Acquire significant experience working with incident response plans, and understand the importance of having a plan that outlines actions to be taken during an incident.

## Lab Mission

Practice how to create an incident response plan for an alert.

## Lab Duration

20-30 minutes

## Requirements

- Knowledge of incident response procedures.

## Resources

- Text editor

## Textbook References

- Chapter 2: Incident Response Preparation
    - Section 3: Security Operation Center
    - Section 4: Incident Response Plan

## Lab Task

Write an incident response plan that includes the first four phases:

- Preparation
- Identification
- Containment
- Eradication

Include at least three examples for each phase in the following scenarios:

1. An employee receives a malicious email with malware.
2. A hacker executes a defacement attack on a company's website, whereby the website's contents or appearance is changed.