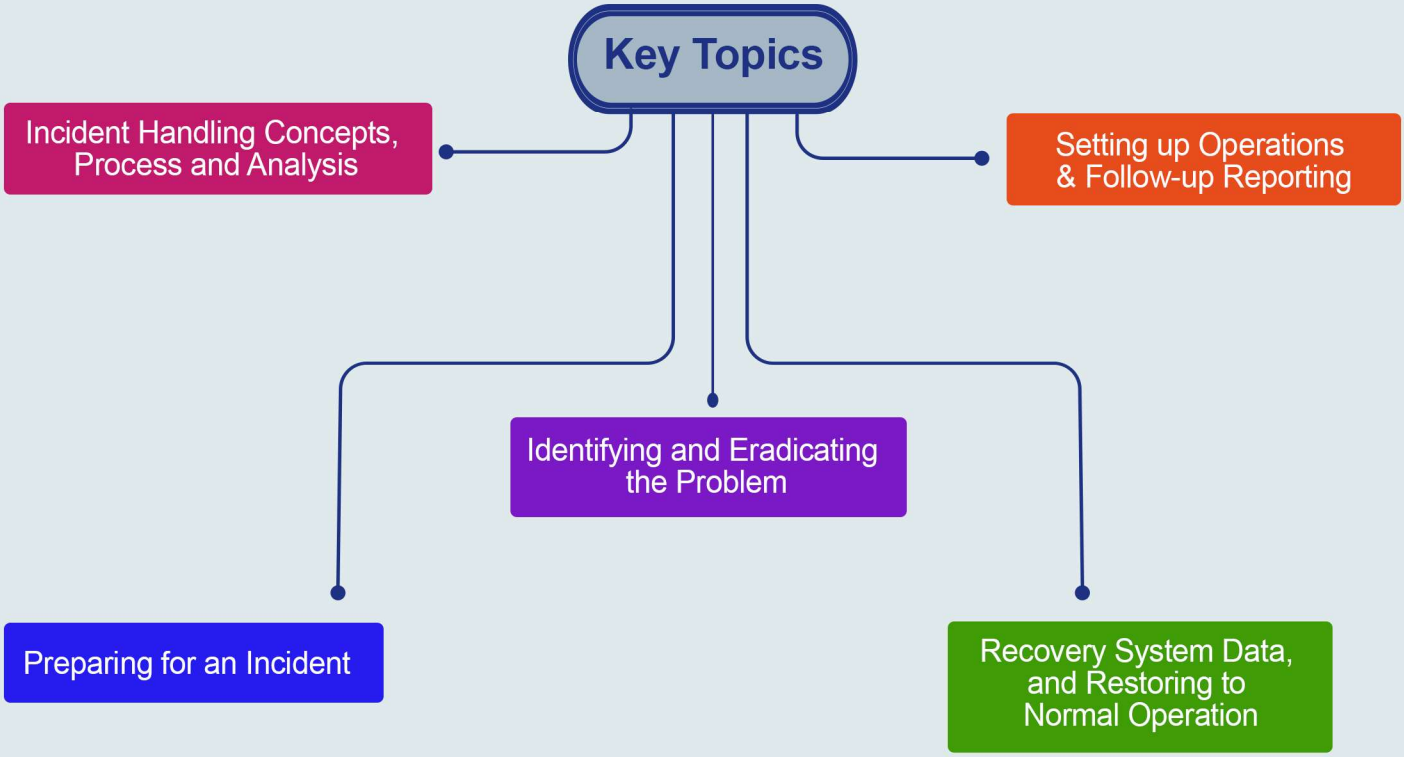
Terminus System

About the Course

Organizations must have a plan in place, and must know the steps they will take to deal with incidents when they occur. This course examines what information security incident management is, how responses are prepared, and concepts and technologies that are used when dealing with incidents. This course also looks at the principles, importance of, and outcomes of incident management and how the information security manager, with the approval of senior management, prepares the people and the resources to deal with incidents when they occur. Finally, this course explains the steps for conducting a business impact analysis as technique used in effective incident management.

Learning Objectives

Key Topics



Pre Requisites

- Information Security Concepts and Principles Course

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Information Security Incident Management eBook

Who Should Attend

- CISOs
- Incident Responders

Syllabus

Incident Management

- Definitions and Concepts
- Events and Incidents
- Classification of Events
- Incident Support Method

Preparation

- Policies
- Management Support
- Incident Handling Team Setup
- Emergency Communication Plan
- Easy Reporting Facilities
- Training Team Members
- Contacts List
- Guidelines for Collaboration between Different Organization's Units
- Communication with System Administrators and Network Administrators
- Communication and Sharing Information with Regulatory Agencies and other CIRTs

Identification

- Determine the Person to be responsible for the incident
- Determining the Incident
- Maintain a Provable Custody Chain
- Coordinate with Network Officials
- Informing the Relevant Authorities

Syllabus

Containment

- Determining Dimensions and Goals
- Send Warning Banners
- Deploy a Team on Site to Survey the Situation
- Keep a Low Profile
- Avoid Potentially Compromised Code if Possible
- Backup the System
- Determine the Risks of Continuing Operations
- Consult System Owners
- Change Passwords

Eradication

- Determining the Cause and Effects of the Incident
- Improving the Defense System
- Vulnerability Analysis
- Eliminate the Cause of the Incident
- Locate the Latest Clean Backup

Recovery

- System Restore
- System Validation
- Restore Operations
- System Monitoring

Follow-up

- Preparation of Reports

Hands-on Training

- Lab 1: Preparing to deal with incidents
- Lab 2: Incident identification
- Lab 3: Incident Control
- Lab 4: Incident Recovery
- Lab 5: Incident Reporting