

























































- Guidelines for Incident Containment
- Forensic Investigation
  - Network Forensics Investigation
  - People Involved in Forensics Investigation
  - Typical Forensics Investigation Methodology
- Eradication and Recovery
  - Countermeasures
  - Systems Recovery
- Post-incident Activities
  - Incident Documentation
  - Incident Damage and Cost Assessment
  - Review and Update the Response Policies
- Training and Awareness