

- Filename: eccouncil-ceh31250-v11-1-15-1-incident-management.md
- Show Name: CEHV11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Incident Management

---

## Incident Management

### Objectives:

- Define Incident Management
  - Elaborate on what Incident Management is designed to accomplish
- 
- What is a Security Incident?
    - An event where security and data CIA is threatened
      - Phishing attacks
      - Ransomware
      - DDoS
      - Injection attacks
  - So what do we mean by the term Incident Management?
    - Process by which we...
      - Identify
      - Analyze
      - Prioritize
      - Resolve
    - This is all in an effort to...
      - Restore normal business operations
        - ASAP
  - Are there any other benefits with Incident Management?
    - Increase service quality and availability
    - Increase effectiveness and efficiency
    - Mitigate negative impact of Security Incidents
    - Improved user/customer experience
  - Are there any other elements of Incident Management that we need to be aware of?
    - The importance of End-User Awareness training as a part of IM
    - Relevant Departments and their involvement in IM
      - HR when sanction or termination is required
      - Legal
      - IT Security staff
      - 3rd Parties that may be affected by an incident

...