- Filename: eccouncil-ceh31250-v11-1-16-1-incident-handling-and-response.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Incident Management

==========

Incident Management

Objectives:

- List and define the 9 steps of the IH&R process

- Preparation
    - Create Policy and Procedure
        - Generate documentation
    - Training
        - IH&R Team
        - End User Security Awareness
    - Assemble a toolkit
- Incident Recording and Assignment
    - Addresses how to properly report and record an incident
        - Identify what happened
        - Contact the right people
            - Using proper communication channels
        - Ticket submission
- Triage
    - Analyze, confirm, categorize, and prioritize Security Incidents
        - Attack type
        - Severity
        - Intended Target
        - Impact
        - Propagation Method
        - Vulnerabilities that were exploited
- Notification
    - Time to inform
        - Stakeholders
            - Management
            - 3rd Party Vendors
            - Clients
- Containment
    - Self-explanatory
        - Pull the plug
        - Network segmentation

        - Sandbox
        - Quarantine

- Evidence Gathering and Forensic Analysis
    - CSI TIME!
        - Explain the attack using evidence and logic
            - Get as much detail as possible

- Eradication
    - Remove the root cause of the incident
    - Secure the vulnerabilities that facilitated the attack

- Recovery
    - Bring affected resource(s) back online
        - This should cause no further disruption to the organization

- Post-Incident Activities
    - Incident Analysis / Final Review
        - Documentation
        - Impact Assessment
        - Policy creation/revision
        - Lessons Learned
        - Disclosure