- Playbook is a manual that provides details about any operational action.
- Incident and vulnerability response playbooks are commonly used by entry-level cybersecurity professionals. They are developed based on the goals outlined in an organization's business continuity plan
- **Common steps included in incident and vulnerability playbooks include:**
  - Preparation: Before incidents occur, mitigate potential impacts on the organization by documenting, establishing staffing plans, and educating users.
  - Detection & Analysis: Detect and analyze events by implementing defined processes and appropriate technology.
  - Containment: Prevent further damage and reduce immediate impact of incidents.
  - Eradication and recovery: Completely remove artifacts of the incident so that an organization can return to normal operations.
  - Post-incident activity: Document the incident, inform organizational leadership, and apply lessons learned.
  - Coordination: Report incidents and share information throughout the response process, based on established standards.