Overview of Incident Management

- Incident Management: a set of pre-defined processes to identify, analyze, prioritize, and resolve incidents.
- Incident Management includes:
  - Vulnerability Analysis
  - Artifact Analysis
  - Security Awareness Training
  - Intrusion Detection
  - Technology Monitoring
- Incident Handling and Response: a process of taking organized and careful steps when reacting to a security incident or cyberattack.
- Incident Handling and Response steps:
  - Preparation:
    - Audit of resources and assets to determine the purpose of security and defining the rules, policies, and procedures that drive the IH&R process.
    - Building and training an incident response team, defining incident readiness procedures, and gathering required tools as well as training employees to secure their systems and accounts.
  - Incident Recording and Assignment:
    - Initial reporting and recording of the incident take place.
    - The identification of an incident, defining incident communication plans for employees.
    - communication methods involving informing IT support personnel or raising an appropriate ticket.

Created by: Abdelrahim Alsadiq

- Incident Triage:
  - identified security incidents are analyzed, validated, categorized, and prioritized.
- Notification:
  - The IH&R team informs various stakeholders, including management, third-party vendors, and clients, about the identified incident.
- Containment:
  - involves stopping the spread of infection to other organizational assets and preventing additional damage.
- Evidence Gathering and Forensic Analysis:
  - The IH&R team accumulates all possible evidence related to the incident and submits it to the forensic department for investigation.
- Eradication:
  - The IH&R team removes or eliminates the root cause of the incident and closes all the attack vectors to prevent similar incidents in future.
- Recovery:
  - The IH&R team restores the affected systems, services, resources, and data through recovery.
- Post-Incident Activities:
  - the security incident requires additional review and analysis before closing the process. Conducting the final review is an important step in the IH&R process which includes:
    - Incident documentation
    - Incident impact assessment
    - Reviewing and revising policies
    - Closing the investigation
    - Incident disclosure