- Incident escalation: the process of identifying a potential security incident and transfer it to more experienced department or team member.
- Escalation policy: a set of actions that outlines who should be notified when an incident alert occurs and how that incident should be handled.
- **Incident classification Types:**
  - Malware infection: occurs when malicious software designed to disrupt a system infiltrates an organization's computers or network.
  - Unauthorized access: occurs when an individual gains digital or physical access to a system or application without permission.
  - Improper usage: occurs when an employee of an organization violates the organization's acceptable use policies.
- **Data roles and responsibilities:**
  - Data Owner:
    - Decides who can access, edit, use, or destroy their information.
  - Data controllers:
    - Determine the procedure and purpose for processing data.
    - Focuses on collecting the personal information of customers.
  - Data processors:
    - Report directly to the data controller and are responsible for processing the data on behalf of the data controller.
    - Tasked with installing security measures to help protect the data.
  - Data custodians:
    - Assign and remove access to software or hardware.
    - Responsible for implementing security controls for the data they are responsible for.
  - Data protection officers:
    - Responsible for monitoring the internal compliance of an organization's data protection procedures.