Overview of Threat Assessment

- Threat Assessment: the process of examining, filtering, transforming, and modeling acquired threat data to extract threat intelligence.
- Target threats and Assets: Organizational resources attacked by threat actors to gain complete control of the organization or to steal information to launch further attacks against the organization.
- Threat Intelligence: the collection and analysis of information about threats and adversaries. Includes the drawing of patterns that inform knowledgeable decisions related to cyberattack preparedness, prevention, and response.
- Threat Contextualization: the process of assessing threats and their impacts in various conditions. Obtained by detecting and analyzing current vulnerabilities in IT resources such as networks and information systems.
- Threat Correlation: helps organizations monitor, detect, and escalate evolving threats to organizational systems and networks. The main objective of threat correlation is to reduce false-positive alert rates and detect and escalate stealthy, complex attacks.
- Threat Correlation Techniques:
    - Relating Multiple Incident Types and Sources across Multiple Nodes: The correlation mechanism must have the capability of processing data irrespective of its origin.
    - Incident Sequence: Past security incidents faced by an organization might influence security-related decisions taken presently.
    - Incident Persistence: A prolonged and targeted incident on a network can indicate an attack.
    - Incident-directed Data Collection: in many situations, it is necessary to interact with other systems in the network in order to complete the correlation process.

Created by: Abdelrahim Alsadiq

- Threat Attribution: the process of identifying and attributing the actors behind an attack as well as their goals, motives, and sponsors.
  - Group: Attribution based on the common group or association of multiple malicious actors and their attack methodologies
  - Campaign: Attribution based on the malware or the campaign strategy of specific malware.
  - Intrusion-set: Attribution the attacker based on the intrusion patterns.
  - True: Identification of a specific person, society, or country sponsoring a well-planned and executed intrusion into or attack on its target.
  - Nation-state: Attribution of attacks sponsored by any nation against another nation.