Understanding Incident Response

Automation and Orchestration

- Incident response automation: the process of superseding the manual IR actions with automatic IR actions using machines and tools.
- The automation of IR process assists in:
    - Investigating incidents, as in the process of incident identification, by providing data from different sources such as past incidents, threat intelligence, and SIEM
    - Providing a functionality with which responders can give instructions and change the configuration of various security controls.
    - Reducing the time required for analyzing and responding to incidents (the main requirement for an incident response is speed).
    - Attending to the alerts generated by critical incidents (as opposed to checking every alert and prioritizing them in order to respond to the most critical ones).
- Incident Response Orchestration: refers to the process of combining human, processes, and technologies to gain better results.
- Difference between IR Automation and IR Orchestration:
    - IR automation converts the manual process into an automated process based on the preset instruction from the responders.
    - IR orchestration involves combining automation with machine and human intelligence to build an environment that learns and evolves with changing situations.

Created by: Abdelrahim Alsadiq