Incident Handling and Response Best Practices

- OWASP's best practices:
  - Audit and Due Diligence: Performing an audit will help to know how well prepared the organization is for incident response.
  - Create a Response Team: Preventing and managing attacks or incidents that can occur without prior notice is best done by experts who belong to an incident response team.
  - Create a documented Incident response: An organization should have a well-documented incident response plan to guide the incident response team during an incident.
  - Identify All Triggers and Indicators: It is important to clearly define what can trigger an incident in the organization.
  - Investigate the Problem: A thorough investigation will require input from the incident response team and might also require input from external resources.
  - Triage and Mitigation: As the team identifies potential exposure, they should plan and execute effective mitigation accordingly.
  - Recovery: restoring whatever services or materials might have been affected during an incident.
  - Documentation and Reporting: Reporting and documentation are critical actions that must continuously occur, before, during, and after incident response.
  - Process Review: continuously monitor an incident and the performance of the team or incident handler.
  - Practice: Organizations should not wait for incidents to occur; rather, incident handling teams should always be prepared.

Created by: Abdelrahim Alsadiq

- ENISA's Best Practices:
  - Workflow: organize periodic workshops to develop and review common incident handling workflow
  - Incident Handling Process: Organizations should start with a simple model and then, as the team becomes more experienced, develop the procedure further.
  - Legal Officer: It is good practice to train one or a few team members in the most important legal issues or procedures related to incident activities.
  - Incident Report: Use network monitoring systems to actively look for incidents in organizational networks.
  - Incident Verification: The CERT should answer with some explanation of what scanning or probing is, why incident handlers do not handle it, and what to do to avoid successful attacks on the network of the incident reporter.
  - Final Classification: Classify incidents according to what is reported by incident reporters and according to what is recognized by incident handlers at the very beginning of the incident handling process.
  - Policies: Alongside creating and using policies, a quality review process should be in place for them, with feedback incorporated into existing policies and policy revisions conducted accordingly.
  - Entry and Exit Procedures: As CERT personnel are hard to get, organizations should make sure that new people are brought up to speed quickly and have enough challenge and variety in their jobs to ensure that organizations can retain them. Organizations should also ensure that when CERT personnel leave, proper actions are taken.
  - Eradication and Recovery: If there are doubts whether a problem is eradicated and service is recovered, it is good practice to check and verify to the degree possible and/or get positive confirmation from each party that in their opinion everything is operating normally again

- GOG18 and Forensic Readiness Planning (SPF):
  - Principle 1: Organizations must develop and implement a forensic readiness policy to comply with SPF MR 9.
  - Principle 2: A Forensic Readiness Policy should be owned at a director level within the organization.
  - Principle 3: Organizations should have a recognized and consistent point of contact for establishing and maintaining relationships during planning and exercises.
  - Principle 4: Organizations should have a recognized and consistent point of contact for establishing and maintaining relationships during planning and exercises.
  - Principle 5: Organizations should have a recognized and consistent point of contact for establishing and maintaining relationships during planning and exercises.
  - Principle 6: Organizations should closely integrate Forensic Readiness plans with incident management.
  - Principle 7: Investigations should seek to produce the best standard of digital forensic evidence.
  - Principle 8: Any internal or external digital forensic capability employed by an organization should apply formal quality assurance processes.
  - Principle 9: Organizations should maintain high quality and effective records management systems.
  - Principle 10: Organizations should provide appropriate records retrieval processes to ensure that they can efficiently and securely respond to any requirement/request to disclose information.
  - Principle 11: Organizations should adopt a collaborative approach to encourage internal acceptance of methods used to support investigations and incident handling.
  - Principle 12: Organizations should normalize a management review process that improves plans in accordance with experience.