Question 13
Answer saved
Marked out of 1
Flag question

When a threat becomes a valid attack, it is classified as an information security incident if:

- a. It has a realistic chance of success
- b. It is directed against information assets
- c. All choices are true
- d. It threatens the confidentiality, integrity, or availability of information assets

Clear my choice

Question 14
Answer saved
Marked out of 1
Flag question

Process of identifying, assessing, and evaluating the levels of risk facing the organization

- a. Policy
- b. Planning
- c. Control
- d. Risk management

Clear my choice

Question 15
Answer saved
Marked out of 1
Flag question

IR planning team seeks to develop pre-defined responses that guide users through steps needed to prevent an incident

Select one:

- True
- False

Question 16

Answer saved

Marked out of 1

Flag question

Leadership generally addresses the direction and motivation of the human resource

Select one:

- (•) True
- ( ) False

Question 17

Answer saved

Marked out of 1

Flag question

The top-Down security implementation approach is always more successful than the bottom-up approach!

Select one:

- (•) True
- ( ) False

Question 18

Not yet answered

Marked out of 3

Remove flag

Individuals at the organization can be notified in the event of an actual incident either sequentially or hierarchically, what is the difference?

Sequentially means that every employee has to contact each and every other employee.
Hierarchically means that one chosen employee will contact another chosen employee that will do the same thing until everyone is notified

Question 19
Answer saved
Marked out of 1
Flag question

Those who document the damage must be trained to collect and preserve evidence, in case the incident is part of a crime or results in a civil action

Select one:
- (●) True
- ( ) False

Question 20
Answer saved
Marked out of 1
Flag question

document containing contact information of individuals to be notified in the event of actual incident either sequentially or hierarchically

- ( ) a. Alert message
- (●) b. Alert roster
- ( ) c. Alert notebook
- ( ) d. Contact list

Clear my choice

Question 21
Answer saved
Marked out of 1
Remove flag

The configurations of technology intended to support information security are classified under:

- ( ) a. software-specific security policies
- ( ) b. Systems-specific security policies
- (●) c. General or security program policy
- ( ) d. Issue-specific security policies

Question 22
Answer saved
Marked out of 1
Flag question

in SecSDLC Physical design phase: the technology needed to support the security blueprint is implemented, generate alternative solutions, and agree upon a final design

Select one:

- (●) True
- ( ) False

Question 23
Answer saved
Marked out of 1
Flag question

Which of the following attacks is more dangerous:

- ( ) a. DoS
- (●) b. DDoS
- ( ) c. Spam
- ( ) d. Hoaxes

Clear my choice

Question 24
Answer saved
Marked out of 1
Flag question

If you notified that your partner system has been attacked by PCs in your company, this incident indicator could be classified as:

- ( ) a. Possible incident indicator
- ( ) b. Probable incident indicator
- (●) c. Definite incident indicator
- ( ) d. All choices are true

Clear my choice

Question 25

Answer saved

Marked out of 1

Flag question

If the incident increase in scope or severity to the point that the IRP cannot adequately contain the incident, in this case, the incident could be classified as a:

- a. Risk
- b. Disaster
- c. attack
- d. Incident Escalation

Clear my choice

Question 26

Answer saved

Marked out of 1

Flag question

Security models provide frameworks for ensuring that all areas of security are addressed

Select one:

- True
- False

Question 1
Answer saved
Marked out of 1
Flag question

focuses on restoring operations at the main site after disasters occur

- a. BCP
- b. Risk management
- c. DRP
- d. IRP

Clear my choice

Question 2
Answer saved
Marked out of 1
Flag question

Expresses what the organization wants to become

- a. Mission statement
- b. Value statement
- c. Vision statement
- d. Strategic planning

Clear my choice

Question 3
Answer saved
Marked out of 1
Remove flag

The bottom-up approach can begin as a grass-roots effort in which CISO attempt to improve the security of their systems.

Select one:

- True
- False

Question 4
Answer saved
Marked out of 1
Flag question

Unusual consumption of Memory storage and CPU processing is classified as:

- a. Definite incident indicator
- b. Possible incident Indicator
- c. Probable incident Indicator
- d. All choices are true

Clear my choice

Question 5
Answer saved
Marked out of 1
Flag question

if we using SDLC, In which phase of the team members specifies the technology needed to support the project blueprint.

- a. Physical Design
- b. Logical Design
- c. Implementation
- d. analysis

Clear my choice

Question 6
Not yet answered
Marked out of 3
Remove flag

SETA program consists of three elements: Security education, security training, security awareness. what the difference between security education and security training?

Security Education :
is the process of improving theoretical in-depth knowledge of security systems, how they function, and the components of each system.

Security Training:
is the process of improving the set of skills needed for security personnel, by allowing them to put theoretical knowledge into practice.

Question 7
Answer saved
Marked out of 1
Flag question

The planing focuses on day-to-day operations of local resources

- a. Operational paining
- b. strategic planing
- c. Tactical planing
- d. Mission planing

Clear my choice

Question 8
Answer saved
Marked out of 1
Flag question

Strategic goals are translated into tasks with superior, measurable, achievable, reasonably high and time-bound objectives (SMART)

Select one:

- True
- False

Question 9
Answer saved
Marked out of 1
Flag question

If you notified you that your partner system has been attacked by PCs in your company, this incident indicator could be classified as:

- a. Possible incident Indicator
- b. All choices are true
- c. Probable incident Indicator
- d. Definite incident indicator

Clear my choice

Question 10
Answer saved
Marked out of 1
Remove flag

The use of a shared login user name and password breck up:

- a. availability
- b. Privacy
- c. Integrity
- d. accountability

Clear my choice

Question 11
Answer saved
Marked out of 1
Flag question

÷n which phase in the SecSDLC personnel issues are evaluated and specific training and education programs conducted

- a. Implementation phase
- b. investigation phase
- c. Physical design phase
- d. analysis phase

Clear my choice

Question 12
Answer saved
Marked out of 1
Flag question

CIO plays a more active role in the development of the planning details than does the CISO

Select one:

- True
- False