Certified Network Defender (CND)

1. Which of the following terms may be defined as “a measure of possible inability to achieve a goal, objective, or target within a defined security, cost plan and technical limitations that adversely affects the organization’s operation and revenues?

A. Risk

B. Vulnerability

C. Threat

D. Incident Response

Answer(s): A

---

2. A distributed Denial of Service (DDoS) attack is a more common type of DoS Attack, where a single system is targeted by a large number of infected machines over the Internet. In a DDoS attack, attackers first infect multiple systems which are known as:

A. Trojans

B. Zombies

C. Spyware

D. Worms

Answer(s): B

---

3. The goal of incident response is to handle the incident in a way that minimizes damage and reduces recovery time and cost. Which of the following does NOT constitute a goal of incident response?

A. Dealing with human resources department and various employee conflict behaviors.

B. Using information gathered during incident handling to prepare for handling future incidents in a better way and to provide stronger protection for systems and data.

C. Helping personal to recover quickly and efficiently from security incidents, minimizing loss or theft and disruption of services.

D. Dealing properly with legal issues that may arise during incidents.

Answer(s): A

---

4. An organization faced an information security incident where a disgruntled employee passed sensitive access control information to a competitor. The organization's incident response manager, upon investigation, found that the incident must be handled within a few hours on the same day to maintain business continuity and market competitiveness. How would you categorize such information security incident?

A. High level incident

B. Middle level incident

C. Ultra-High level incident

D. Low level incident

Answer(s): A

---

5. Business continuity is defined as the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy. Identify the plan which is mandatory part of a business continuity plan?

A. Forensics Procedure Plan

B. Business Recovery Plan

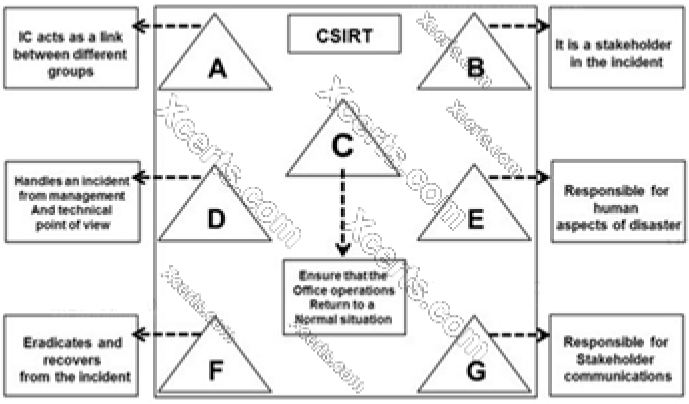
C. Sales and Marketing plan

D. New business strategy plan

Answer(s): B

---

6. The flow chart gives a view of different roles played by the different personnel of CSIRT. Identify the incident response personnel denoted by A, B, C, D, E, F and G.


IC acts as a link between different groups
A
CSIRT
B
It is a stakeholder in the incident
C
Handles an incident from management And technical point of view
D
E
Responsible for human aspects of disaster
Ensure that the Office operations Return to a Normal situation
Eradicates and recovers from the incident
F
G
Responsible for Stakeholder communications

A. A-Incident Analyst, B- Incident Coordinator, C- Public Relations, D-Administrator, E- Human Resource, F- Constituency, G-Incident Manager

B. A- Incident Coordinator, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, F- Constituency, G-Incident Manager

C. A- Incident Coordinator, B- Constituency, C-Administrator, D-Incident Manager, E- Human Resource, F- Incident Analyst, G-Public relations

D. A- Incident Manager, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, F- Constituency, G-Incident Coordinator

Answer(s): C

---

7. Which of the following is an appropriate flow of the incident recovery steps?

A. System Operation-System Restoration-System Validation-System Monitoring

B. System Validation-System Operation-System Restoration-System Monitoring

C. System Restoration-System Monitoring-System Validation-System Operations

D. System Restoration-System Validation-System Operations-System Monitoring

Answer(s): D

---

8. A computer Risk Policy is a set of ideas to be implemented to overcome the risk associated with computer security incidents. Identify the procedure that is NOT part of the computer risk policy?

A. Procedure to identify security funds to hedge risk

B. Procedure to monitor the efficiency of security controls

C. Procedure for the ongoing training of employees authorized to access the system

D. Provisions for continuing support if there is an interruption in the system or if the system crashes

Answer(s): C

---

9. Identify the network security incident where intended authorized users are prevented from using system, network, or applications by flooding the network with high volume of traffic that consumes all existing network resources.

A. URL Manipulation

B. XSS Attack

C. SQL Injection

D. Denial of Service Attack

Answer(s): D

10. Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following steps focus on limiting the scope and extent of an incident?

A. Eradication

B. Containment

C. Identification

D. Data collection

Answer(s): B

---

11. Identify the malicious program that is masked as a genuine harmless program and gives the attacker unrestricted access to the user’s information and system. These programs may unleash dangerous programs that may erase the unsuspecting user’s disk and send the victim’s credit card numbers and passwords to a stranger.

A. Cookie tracker

B. Worm

C. Trojan

D. Virus

Answer(s): C

---

12. Quantitative risk is the numerical determination of the probability of an adverse event and the extent of the losses due to the event. Quantitative risk is calculated as:

A. (Probability of Loss) X (Loss)

B. (Loss) / (Probability of Loss)

C. (Probability of Loss) / (Loss)

D. Significant Risks X Probability of Loss X Loss

Answer(s): A

---

13. An incident recovery plan is a statement of actions that should be taken before, during or after an incident. Identify which of the following is NOT an objective of the incident recovery plan?

A. Creating new business processes to maintain profitability after incident

B. Providing a standard for testing the recovery plan

C. Avoiding the legal liabilities arising due to incident

D. Providing assurance that systems are reliable

Answer(s): A

---

14. Risk is defined as the probability of the occurrence of an incident. Risk formulation generally begins with the likeliness of an event's occurrence, the harm it may cause and is usually denoted as Risk = ∑(events)X (Probability of occurrence)X?

A. Magnitude

B. Probability

C. Consequences

D. Significance

Answer(s): A

---

15. An audit trail policy collects all audit trails such as series of records of computer events, about an operating system, application or user activities. Which of the following statements is NOT true for an audit trail policy?

A. It helps calculating intangible losses to the organization due to incident

B. It helps tracking individual actions and allows users to be personally accountable for their actions

C. It helps in compliance to various regulatory laws, rules, and guidelines

D. It helps in reconstructing the events after a problem has occurred

Answer(s): A

---

16. Computer forensics is methodical series of techniques and procedures for gathering evidence from computing equipment, various storage devices and or digital media that can be presented in a course of law in a coherent and meaningful format. Which one of the following is an appropriate flow of steps in the computer forensics process?

A. Examination> Analysis > Preparation > Collection > Reporting

B. Preparation > Analysis > Collection > Examination > Reporting

C. Analysis > Preparation > Collection > Reporting > Examination

D. Preparation > Collection > Examination > Analysis > Reporting

Answer(s): D

---

17. Multiple component incidents consist of a combination of two or more attacks in a system. Which of the following is not a multiple component incident?

A. An insider intentionally deleting files from a workstation

B. An attacker redirecting user to a malicious website and infects his system with Trojan

C. An attacker infecting a machine to launch a DDoS attack

D. An attacker using email with malicious code to infect internal workstation

Answer(s): A

---

18. Computer Forensics is the branch of forensic science in which legal evidence is found in any computer or any digital media device. Of the following, who is responsible for examining the evidence acquired and separating the useful evidence?

A. Evidence Supervisor

B. Evidence Documenter

C. Evidence Manager

D. Evidence Examiner/ Investigator

Answer(s): D

---

19. The network perimeter should be configured in such a way that it denies all incoming and outgoing traffic/ services that are not required. Which service listed below, if blocked, can help in preventing Denial of Service attack?

A. SAM service

B. POP3 service

C. SMTP service

D. Echo service

Answer(s): D

---

20. A US Federal agency network was the target of a DoS attack that prevented and impaired the normal authorized functionality of the networks. According to agency's reporting timeframe guidelines, this incident should be reported within two (2) HOURS of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity. Which incident category of the US Federal Agency does this incident belong to?

A. CAT 5

B. CAT 1

C. CAT 2

D. CAT 6

Answer(s): C