

212-89^{Q&As}

EC-Council Certified Incident Handler

Pass EC-COUNCIL 212-89 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.certbus.com/212-89.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Keyloggers do NOT:

- A. Run in the background
- B. Alter system files
- C. Secretly records URLs visited in browser, keystrokes, chat conversations, ...etc
- D. Send log file to attacker's email or upload it to an ftp server

Correct Answer: B

QUESTION 2

The policy that defines which set of events needs to be logged in order to capture and review the important data in a timely manner is known as:

- A. Audit trail policy
- B. Logging policy
- C. Documentation policy
- D. Evidence Collection policy

Correct Answer: B

QUESTION 3

Incident prioritization must be based on:

- A. Potential impact
- B. Current damage
- C. Criticality of affected systems
- D. All the above

Correct Answer: D

QUESTION 4

Incidents such as DDoS that should be handled immediately may be considered as:

- A. Level One incident

- B. Level Two incident
- C. Level Three incident
- D. Level Four incident

Correct Answer: C

QUESTION 5

The correct sequence of Incident Response and Handling is:

- A. Incident Identification, recording, initial response, communication and containment
- B. Incident Identification, initial response, communication, recording and containment
- C. Incident Identification, communication, recording, initial response and containment
- D. Incident Identification, recording, initial response, containment and communication

Correct Answer: A

QUESTION 6

Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?

- A. To restore the original site, tests systems to prevent the incident and terminates operations
- B. To define the notification procedures, damage assessments and offers the plan activation
- C. To provide the introduction and detailed concept of the contingency plan
- D. To provide a sequence of recovery activities with the help of recovery procedures

Correct Answer: A

QUESTION 7

Insiders understand corporate business functions. What is the correct sequence of activities performed by Insiders to damage company assets:

- A. Gain privileged access, install malware then activate
- B. Install malware, gain privileged access, then activate
- C. Gain privileged access, activate and install malware
- D. Activate malware, gain privileged access then install malware

Correct Answer: A

QUESTION 8

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

Correct Answer: A

QUESTION 9

Which of the following is NOT one of the common techniques used to detect Insider threats:

- A. Spotting an increase in their performance
- B. Observing employee tardiness and unexplained absenteeism
- C. Observing employee sick leaves
- D. Spotting conflicts with supervisors and coworkers

Correct Answer: A

QUESTION 10

A risk mitigation strategy determines the circumstances under which an action has to be taken to minimize and overcome risks. Identify the risk mitigation strategy that focuses on minimizing the probability of risk and losses by searching for vulnerabilities in the system and appropriate controls:

- A. Risk Assumption
- B. Research and acknowledgment
- C. Risk limitation
- D. Risk absorption

Correct Answer: B

QUESTION 11

The most common type(s) of intellectual property is(are):

- A. Copyrights and Trademarks
- B. Patents
- C. Industrial design rights and Trade secrets
- D. All the above

Correct Answer: D

QUESTION 12

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

Correct Answer: C

QUESTION 13

An incident is analyzed for its nature, intensity and its effects on the network and systems. Which stage of the incident response and handling process involves auditing the system and network log files?

- A. Incident recording
- B. Reporting
- C. Containment
- D. Identification

Correct Answer: D

QUESTION 14

An information security incident is

- A. Any real or suspected adverse event in relation to the security of computer systems or networks
- B. Any event that disrupts normal today's business functions

- C. Any event that breaches the availability of information assets
- D. All of the above

Correct Answer: D

QUESTION 15

The main feature offered by PGP Desktop Email is:

- A. Email service during incidents
- B. End-to-end email communications
- C. End-to-end secure email service
- D. None of the above

Correct Answer: C

[Latest 212-89 Dumps](#)

[212-89 VCE Dumps](#)

[212-89 Braindumps](#)