



Eccouncil 312-76 Mock Exam

Shared by Goff on 17-06-2026

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)



Question 1

Question Type: MultipleChoice

Peter works as a Technical Representative in a CSIRT for SecureEnet Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

Options:

- A- Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps
- B- Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system
- C- Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces
- D- Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces

Answer:

D

Question 2

Question Type: MultipleChoice

Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial-of-service attacks, or unauthorized changes to system hardware, software, or data?

Options:

- A- Cyber Incident Response Plan
- B- Crisis Communication Plan
- C- Occupant Emergency Plan
- D- Disaster Recovery Plan

Answer:

A

Question 3

Question Type: MultipleChoice

You work as an Incident handling manager for Orangesect Inc. You detect a virus attack incident in the network of your company. You develop a signature based on the characteristics of the detected virus. Which of the following phases in the Incident handling process will utilize the signature to resolve this incident?

P2P
exams

Options:

- A- Eradication
- B- Identification
- C- Containment
- D- Recovery

Answer:

A

Question 4

Question Type: MultipleChoice

Which option best is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

P2P
exams

Options:

- A- Snooping
- B- Patent
- C- Utility model
- D- Copyright

Answer:

B

Question 5

Question Type: MultipleChoice

Which of the following individuals incorporates risk assessment in training programs for the organization's personnel?

Options:

- A- Chief information officer
- B- Information system security officer
- C- Functional manager
- D- Security awareness trainer

Answer:

D

Question 6

Question Type: MultipleChoice

Which option best roles is responsible for the review and risk analysis of all the contracts on regular basis?

Options:

- A- The IT Service Continuity Manager
- B- The Configuration Manager
- C- The Supplier Manager
- D- The Service Catalogue Manager

Answer:

C

Question 7

Question Type: MultipleChoice

In which of the following prototyping, a version of the system is built to check the requirements and is then discarded?

Options:

- A- Evolutionary prototyping
- B- Incremental prototyping
- C- Project prototyping
- D- Throw-away prototyping



Answer:

D

Question 8

Question Type: MultipleChoice

You work as a senior project manager in SoftTech Inc. You are working on a software project using configuration management. Through configuration management, you are decomposing the verification system into identifiable, understandable, manageable, traceable units that are known as Configuration Items (CIs). According to you, which of the following processes is known as the decomposition process of a verification system into Configuration Items?

Options:

- A- Configuration auditing
- B- Configuration identification
- C- Configuration status accounting
- D- Configuration control



Answer:

B

Question 9

Question Type: MultipleChoice

Which of the following types of control gives an instance of the audit log?

Options:

- A- Preventive
- B- Detection
- C- Containment
- D- Recovery



Answer:

B

Question 10

Question Type: MultipleChoice

Which of the following BCP teams is the first responder and deals with the immediate effects of the disaster?

Options:

- A- Emergency management team
- B- Damage assessment team
- C- Off-site storage team
- D- Emergency action team



Answer:

D

To Get Premium Files for 312-76 Visit

<https://www.p2pexams.com/products/312-76>

For More Free Questions Visit

<https://www.p2pexams.com/eccouncil/pdf/312-76>

20%
DISCOUNT

P2P
exams