



# 212-82<sup>Q&As</sup>

Certified Cybersecurity Technician(C|CT)

## Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/212-82.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**

Stella purchased a smartwatch online using her debit card. After making payment for the product through the payment gateway, she received a transaction text message with a deducted and available balance from her bank.

Identify the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario.

- A. Non-repudiation
- B. Integrity
- C. Availability
- D. Confidentiality

Correct Answer: C

Explanation: Availability is the information security element that ensures that Stella's transaction status is immediately reflected in her bank account in this scenario. Information security is the practice of protecting information and information systems from unauthorized access, use, disclosure, modification, or destruction. Information security can be based on three fundamental principles: confidentiality, integrity, and availability. Confidentiality is the principle that ensures that information is accessible only to authorized parties and not disclosed to unauthorized parties. Integrity is the principle that ensures that information is accurate, complete, and consistent and not altered or corrupted by unauthorized parties. Availability is the principle that ensures that information and information systems are accessible and usable by authorized parties when needed. In the scenario, Stella purchased a smartwatch online using her debit card. After making payment for the product through the payment gateway, she received a transaction text message with a deducted and available balance from her bank. This means that her transaction status was immediately reflected in her bank account, which indicates that availability was ensured by her bank's information system.

---

**QUESTION 2**

Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat-hunting process using existing data collected from DNS and proxy logs.

Identify the type of threat-hunting method employed by Mark in the above scenario.

- A. Entity-driven hunting
- B. TTP-driven hunting
- C. Data-driven hunting
- D. Hybrid hunting

Correct Answer: C

Explanation: A data-driven hunting method is a type of threat hunting method that employs existing data collected from various sources, such as DNS and proxy logs, to generate and test hypotheses about potential threats. This method relies on data analysis and machine learning techniques to identify patterns and anomalies that indicate malicious activity. A data-driven hunting method can help discover unknown or emerging threats that may evade traditional detection methods. An entity-driven hunting method is a type of threat hunting method that focuses on specific entities,



such as users, devices, or domains, that are suspected or known to be involved in malicious activity. A TTP-driven hunting method is a type of threat hunting method that leverages threat intelligence and knowledge of adversary tactics, techniques, and procedures (TTPs) to formulate and test hypotheses about potential threats. A hybrid hunting method is a type of threat hunting method that combines different approaches, such as data-driven, entity-driven, and TTP-driven methods, to achieve more comprehensive and effective results.

---

### QUESTION 3

Zion belongs to a category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. He was instructed by the management to check the functionality of equipment related

to physical security.

Identify the designation of Zion.

- A. Supervisor
- B. Chief information security officer
- C. Guard
- D. Safety officer

Correct Answer: C

Explanation: The correct answer is C, as it identifies the designation of Zion. A guard is a person who is responsible for implementing and managing the physical security equipment installed around the facility. A guard typically performs tasks such as: Checking the functionality of equipment related to physical security Monitoring the surveillance cameras and alarms Controlling the access to restricted areas Responding to emergencies or incidents In the above scenario, Zion belongs to this category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. Option A is incorrect, as it does not identify the designation of Zion. A supervisor is a person who is responsible for overseeing and directing the work of other employees. A supervisor typically performs tasks such as: Assigning tasks and responsibilities to employees Evaluating the performance and productivity of employees Providing feedback and guidance to employees Resolving conflicts or issues among employees In the above scenario, Zion does not belong to this category of employees who are responsible for overseeing and directing the work of other employees. Option B is incorrect, as it does not identify the designation of Zion. A chief information security officer (CISO) is a person who is responsible for establishing and maintaining the security vision, strategy, and program for an organization. A CISO typically performs tasks such as: Developing and implementing security policies and standards Managing security risks and compliance Leading security teams and projects Communicating with senior management and stakeholders In the above scenario, Zion does not belong to this category of employees who are responsible for establishing and maintaining the security vision, strategy, and program for an organization. Option D is incorrect, as it does not identify the designation of Zion. A safety officer is a person who is responsible for ensuring that health and safety regulations are followed in an organization. A safety officer typically performs tasks such as: Conducting safety inspections and audits Identifying and eliminating hazards and risks Providing safety training and awareness Reporting and investigating accidents or incidents In the above scenario, Zion does not belong to this category of employees who are responsible for ensuring that health and safety regulations are followed in an organization. References: Section 7.1

---

### QUESTION 4

Cairo, an incident responder, was handling an incident observed in an organizational network. After performing all IHandR steps, Cairo initiated post-incident activities. He determined all types of losses caused by the incident by



identifying And evaluating all affected devices, networks, applications, and software. Identify the post-incident activity performed by Cairo in this scenario.

- A. Incident impact assessment
- B. Close the investigation
- C. Review and revise policies
- D. Incident disclosure

Correct Answer: A

Explanation: Incident impact assessment is the post-incident activity performed by Cairo in this scenario. Incident impact assessment is a post-incident activity that involves determining all types of losses caused by the incident by identifying and evaluating all affected devices, networks, applications, and software. Incident impact assessment can include measuring financial losses, reputational damages, operational disruptions, legal liabilities, or regulatory penalties<sup>1</sup>.

References: Incident Impact Assessment

---

## QUESTION 5

Ruben, a crime investigator, wants to retrieve all the deleted files and folders in the suspected media without affecting the original files. For this purpose, he uses a method that involves the creation of a cloned copy of the entire media and prevents the contamination of the original media.

Identify the method utilized by Ruben in the above scenario.

- A. Sparse acquisition
- B. Bit-stream imaging
- C. Drive decryption
- D. Logical acquisition

Correct Answer: B

Explanation: Bit-stream imaging is the method utilized by Ruben in the above scenario. Bit-stream imaging is a method that involves creating a cloned copy of the entire media and prevents the contamination of the original media. Bit-stream imaging copies all the data on the media, including deleted files and folders, hidden partitions, slack space, etc., at a bit level. Bit-stream imaging preserves the integrity and authenticity of the digital evidence and allows further analysis without affecting the original media. Sparse acquisition is a method that involves creating a partial copy of the media by skipping empty sectors or blocks. Drive decryption is a method that involves decrypting an encrypted drive or partition using a password or a key. Logical acquisition is a method that involves creating a copy of the logical files and folders on the media using file system commands.

[212-82 PDF Dumps](#)

[212-82 VCE Dumps](#)

[212-82 Braindumps](#)