



MOMETRIX
SMARTER PREP. BETTER RESULTS.

01	A	B	C	D	E
02	A	B	C	D	E
03	A	B	C	D	E
04	A	B	C	D	E
05	A	B	C	D	E
06	A	B	C	D	E
07	A	B	C	D	E
08	A	B	C	D	E
09	A	B	C	D	E
10	A	B	C	D	E
11	A	B	C	D	E
12	A	B	C	D	E
13	A	B	C	D	E

14	A	B	C	D	E
15	A	B	C	D	E
16	A	B	C	D	E
17	A	B	C	D	E
18	A	B	C	D	E
19	A	B	C	D	E
20	A	B	C	D	E
21	A	B	C	D	E
22	A	B	C	D	E
23	A	B	C	D	E
24	A	B	C	D	E
25	A	B	C	D	E
26	A	B	C	D	E

27	A	B	C	D	E
28	A	B	C	D	E
29	A	B	C	D	E
30	A	B	C	D	E
31	A	B	C	D	E
32	A	B	C	D	E
33	A	B	C	D	E
34	A	B	C	D	E
35	A	B	C	D	E
36	A	B	C	D	E
37	A	B	C	D	E
38	A	B	C	D	E
39	A	B	C	D	E

PRACTICE QUESTIONS

Cisco

CCST—CYBERSECURITY— CISCO—CERTIFIED— SUPPORT—TECHN

CCST Cybersecurity (Cisco Certified Support Technician)

EDITION

Demo

QUESTIONS

9

FORMAT

Limited Edition PDF

WEB www.mometrix.net

SUPPORT support@mometrix.net

Before you begin

What this is

9 practice questions for Cisco **CCST-CYBERSECURITY-CISCO-CERTIFIED-SUPPORT-TECHN**, each with its answer key and an explanation. Answer a question before you read its key — the explanation is worth more once you have committed.

If something looks wrong

Send us three things and we will check it:

- the exam code, **CCST-CYBERSECURITY-CISCO-CERTIFIED-SUPPORT-TECHN**
- the question number
- the email address on your order

Write to **support@mometrix.net**. We reply within one business day.

QUESTION 1

SINGLE CHOICE

Which security principle is demonstrated when a user is granted only the minimum permissions necessary to perform their job functions?

- ☐ A Defense in depth
- ☒ B Least privilege
- ☐ C Separation of duties
- ☐ D Zero trust

ANSWER B

WHY Least privilege is the principle of granting users only the minimum access rights necessary to perform their job duties. Defense in depth uses multiple layers of security controls, separation of duties splits critical tasks among multiple people, and zero trust assumes no implicit trust and verifies every access request.

QUESTION 2

SINGLE CHOICE

At which layer of the OSI model does a network firewall typically operate to filter traffic based on IP addresses and port numbers?

- ☐ A Layer 2 (Data Link)
- ☐ B Layer 3 (Network)
- ☒ C Layer 4 (Transport)
- ☐ D Layer 7 (Application)

ANSWER C

WHY A traditional stateful firewall filters traffic based on IP addresses (Layer 3) and port numbers (Layer 4), and tracks the state of active connections. A packet filter is Layer 3 only, while an application-layer firewall operates at Layer 7 and can inspect payload content.

QUESTION 3

SINGLE CHOICE

Which type of malware is designed to replicate itself and spread to other computers without requiring user interaction?

- ☐ A Trojan horse
- ☒ B Worm
- ☐ C Spyware
- ☐ D Ransomware

ANSWER B

WHY A worm is self-replicating malware that spreads across networks automatically without user interaction. A Trojan horse disguises itself as legitimate software and requires a user to execute it, spyware secretly collects information, and ransomware encrypts files and demands payment.

QUESTION 4

MULTIPLE CHOICE

Which of the following are common sources of security log data that would typically be forwarded to a SIEM for correlation? (Choose two.)

- ☒ A Firewall logs
- ☒ B Operating system event logs
- ☐ C Spreadsheet documents
- ☐ D IDS/IPS alerts

ANSWER A - B

WHY Firewall logs and operating system event logs are standard sources of telemetry ingested by a SIEM for correlation and analysis. Spreadsheet documents are not a security telemetry source, and while IDS/IPS alerts are also a valid SIEM source, they are not among the selected answers here (the two best matches to the listed choices are firewall logs and OS event logs).

QUESTION 5

SINGLE CHOICE

Which cryptographic method uses a pair of mathematically related keys, one public and one private, to provide confidentiality and digital signatures?

- ☐ A Symmetric encryption
- ☐ B Hashing
- ☒ C Asymmetric encryption
- ☐ D Steganography

ANSWER C

WHY Asymmetric encryption uses a public/private key pair: the public key encrypts data or verifies signatures, and the private key decrypts data or creates signatures. Symmetric encryption uses a single shared secret key, hashing produces a one-way fixed-size digest, and steganography hides data within other files.

QUESTION 6

SINGLE CHOICE

Which authentication factor is classified as 'something you are'?

- ☐ A Smart card
- ☒ B Fingerprint
- ☐ C Password
- ☐ D PIN code

ANSWER B

WHY Authentication factors are categorized as 'something you know' (password, PIN), 'something you have' (smart card, token), and 'something you are' (biometric such as fingerprint, retina, or facial recognition).

QUESTION 7 MULTIPLE CHOICE

Which of the following are elements typically found in a formal organizational security policy? (Choose two.)

- ☒ **A** Scope and purpose of the policy
- ☐ **B** Employee salary information
- ☒ **C** Roles and responsibilities
- ☐ **D** Marketing campaign schedule

ANSWER A • C

WHY A formal security policy defines its scope/purpose and the roles and responsibilities of those who must comply with it. Employee salary information and marketing schedules are unrelated HR/business documents and are not part of a security policy.

QUESTION 8 SINGLE CHOICE

Which component of the CIA triad is primarily compromised when an attacker intercepts and reads confidential email messages in transit?

- ☒ **A** Confidentiality
- ☐ **B** Integrity
- ☐ **C** Availability
- ☐ **D** Authentication

ANSWER A

WHY Confidentiality is preserved by preventing unauthorized disclosure of information. When an attacker reads messages they should not be able to, confidentiality has been breached. Integrity is about preventing unauthorized modification, availability ensures systems remain accessible, and authentication verifies identity.

QUESTION 9

SINGLE CHOICE

Which well-known TCP port number is used by HTTPS for encrypted web traffic?

- ☐ A 21
- ☐ B 25
- ☐ C 80
- ☒ D 443

ANSWER D

WHY HTTPS uses TCP port 443. Port 21 is FTP, port 25 is SMTP, and port 80 is HTTP (unencrypted).

mometrix.net