PassQueen
a.k.a dumpsqueen.com

Cisco Certified Support Technician (CCST) Cybersecurity

Cisco 100-160

Version Demo

Total Demo Questions: 7

Total Premium Questions: 75

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Security Principles	7
Topic 2, Basic Network Security Concepts	30
Topic 3, Endpoint Security Concepts	11
Topic 4, Vulnerability Assessment and Risk Management	9
Topic 5, Incident Handling	17
Topic 6, Mix Questions	1
Total	75

QUESTION NO: 1 - (SIMULATION)

You need to manage security risks at your company. In which order should you complete the actions?

Move all the actions to the answer area and place them in the correct order.



ANSWER: See the explanation for the answer

Explanation:

Place the risk-management actions in this order:

This sequence first identifies possible threats and vulnerabilities, then ranks them by likelihood and business impact. The organization then applies the selected treatment or response and continuously monitors whether that response is effective.

QUESTION NO: 2

Your supervisor suspects that someone is attempting to gain access to a Windows computer by guessing user account IDs and passwords. The supervisor asks you to use the Windows Event Viewer security logs to verify the attempts.

Which two audit policy events provide information to determine whether someone is using invalid credentials to attempt to log in to the computer?*(Choose 2.)*

Note: You will receive partial credit for each correct selection.

A. Object access failure

B. Account logon failure

C. Account lockout success

D. Account logoff success

ANSWER: B C

Explanation:

Account logon failure is correct because it records an unsuccessful authentication attempt. In the Security log, failed authentication activity provides key evidence for investigating suspected password guessing: analysts can correlate the affected account name, source workstation or network address, logon context, status or substatus details, and timestamps. A high volume of failures, particularly from a common source or against many accounts in a brief interval, is a strong indicator that invalid credentials are being repeatedly tried.

Account lockout success is also correct because it records that Windows locked an account after the configured lockout threshold was met. This event corroborates repeated failed authentication attempts and identifies the account that was locked. Used with the failed account-logon records, it helps an analyst establish both the repeated invalid-credential activity and its security-control outcome. Reviewing these records in time order is useful for scoping the incident, identifying targeted accounts, and determining whether the pattern originated locally or remotely.

Microsoft documents failed logon auditing and the details available in Security event 4625 at Windows Security Event 4625. It documents account-lockout activity in Windows Security Event 4740.

QUESTION NO: 3 - (SIMULATION)

Move each worm mitigation step from the list on the left to the correct description on the right.

Note: You will receive partial credit for each correct answer.

ANSWER: See the explanation for the answer

Explanation:

Match the worm mitigation steps as follows:

Containment — Limit the worm's spread by segmenting the network and restricting traffic from infected areas.
Inoculation — Apply patches or updates to uninfected systems so they cannot be compromised.
Quarantine — Remove or block infected systems from the network to prevent further infection.
Treatment — Clean infected systems to remove the worm and patch the vulnerabilities that enabled it.

Containment controls traffic between areas, whereas quarantine isolates the specific infected hosts.

QUESTION NO: 4

During an incident response, the security team needs to isolate a compromised server from the rest of the network but still allow forensic analysis. Which action should they take?

A. Power off the server immediately.

B. Disconnect the server from the network and connect it to an isolated forensic network.

C. Delete suspicious files from the server.

D. Reset all user passwords on the server.

ANSWER: B

Explanation:

Disconnect the server from the network and connect it to an isolated forensic network. This is an appropriate containment action because it immediately prevents the compromised host from communicating with external command-and-control infrastructure, attacking other systems, or continuing to exfiltrate data. At the same time, retaining the server in a controlled forensic environment preserves the system, its storage, volatile state where feasible, logs, and other artifacts needed to determine the scope, timeline, initial access vector, and impact of the incident.

Effective incident handling balances rapid containment with evidence preservation. The isolated environment should have tightly controlled access, no route to production resources or the internet unless specifically required and monitored, and documented evidence-handling procedures. Investigators can then acquire forensic images, collect logs and memory when appropriate, calculate hashes, and analyze the host without exposing the organization to further harm. Cisco incident-response guidance identifies containment as a phase used to limit the incident's spread while enabling the response team to investigate and recover safely. See Cisco's Incident Response overview and the NIST Computer Security Incident Handling Guide for containment and evidence-preservation practices.

QUESTION NO: 5

How do threat actors launch ransomware attacks on organizations?

A. They implant malware to collect data from the corporation's financial system.

B. They deface an organization's public-facing website.

C. They lock data and deny access to the data until they receive money.

D. They secretly spy on employees and collect employees' personal information.

ANSWER: C

Explanation:

They lock data and deny access to the data until they receive money. Ransomware is malware designed to disrupt an organization's availability of data or systems, most commonly by encrypting files so that users and administrators cannot read them. The threat actor then demands a ransom, often in cryptocurrency, in exchange for a purported decryption key or restoration of access. Modern ransomware operations may also steal data before encryption and threaten to publish it, but the core ransomware behavior remains denying access to data or systems while demanding payment. Organizations can reduce ransomware risk through tested offline backups, timely patching, multifactor authentication, least-privilege access, endpoint protection, and user awareness training to recognize phishing attempts. Cisco's CCST Cybersecurity training identifies ransomware as malware that prevents access to data and demands payment, matching the behavior described here. The U.S. Cybersecurity and Infrastructure Security Agency similarly explains that ransomware encrypts files or otherwise blocks access to systems and data until a ransom is demanded. See Cisco: What Is Ransomware? and CISA: Ransomware Guide.

QUESTION NO: 6

A company is retiring several laptops that stored confidential customer records. The storage devices will be reused within the company.

Which two actions help ensure that confidential data cannot be recovered by the next users? *(Choose 2.)*

A. Use an approved data-sanitization method on the storage device

B. Delete the user files and empty the recycle bin

C. Verify that the sanitization process completed successfully

D. Perform a quick format of the storage device

E. Reassign the laptop after removing the user account

ANSWER: A C

Explanation:

Using an approved data-sanitization method and verifying that the sanitization completed successfully are appropriate actions before storage media are reused. Sanitization removes or renders data inaccessible so that a subsequent user cannot recover confidential records from the device.

Deleting files or performing a quick format usually removes file-system references rather than securely removing the underlying data. Reassigning the device without sanitization leaves the prior information exposed. Encryption is an important protection while data is stored, but simply enabling encryption does not remove existing data unless the organization performs an approved cryptographic erase or other sanitization process.

QUESTION NO: 7

You need to design your company's password policy to adhere to the National Institute of Standards and Technology (NIST) guidelines for user password security.

What is the minimum password length that you should require to be consistent with the NIST guidelines?

A. 4 characters

B. 8 characters

C. 16 characters

D. No minimum length

ANSWER: B

Explanation:

8 characters is the minimum length presented in Cisco's CCST Cybersecurity authentication-best-practices material for user-created passwords under the NIST guidance commonly taught from SP 800-63B. This baseline reflects NIST's recognition that password length is a primary contributor to resistance against guessing and password-cracking attacks. A policy should permit users to create substantially longer passwords or passphrases, because additional length generally provides much greater security while remaining easier to remember than artificially complex short passwords.

NIST's detailed digital-identity guidance distinguishes between authentication contexts: an eight-character minimum applies when the password is used as part of multifactor authentication, while a longer minimum is specified for single-factor password authentication. In the CCST question's intended baseline framing, **8 characters** is therefore the expected minimum. A well-designed enterprise policy should also allow long passwords, support password managers, compare proposed passwords against blocklists of common or compromised values, and avoid arbitrary composition requirements that do not meaningfully improve password strength.

See NIST's SP 800-63B Digital Identity Guidelines and Cisco Networking Academy's CCST Cybersecurity course overview.