

Help You in ISACA CCOA Exam Preparation [2026]



BONUS!!! Download part of TestInsides CCOA dumps for free: <https://drive.google.com/open?id=1BXX2YXA44wrFRSk8f0IvyZaWE9HitMG0>

Being anxious for the CCOA exam ahead of you? Have a look of our CCOA training engine please. Presiding over the line of our practice materials over ten years, our experts are proficient as elites who made our CCOA learning questions, and it is their job to officiate the routines of offering help for you. All points are predominantly related with the exam ahead of you. You will find the exam is a piece of cake with the help of our CCOA Study Materials.

The content of our CCOA exam questions emphasizes the focus and seizes the key to use refined CCOA questions and answers to let the learners master the most important information by using the least amount of them. And we provide varied functions to help the learners learn our CCOA Study Materials and prepare for the exam. The CCOA self-learning and self-evaluation functions help the learners the learners find their weak links and improve them promptly .

>> Valid Dumps CCOA Files <<

CCOA Updated CBT - CCOA Download

Before you take the CCOA exam, you only need to spend 20 to 30 hours to practice, so you can schedule time to balance learning and other things. Of course, you care more about your passing rate. If you choose our CCOA exam guide, under the guidance of our CCOA exam torrent, we have the confidence to guarantee a passing rate of over 99%. Our CCOA Quiz prep is compiled by experts based on the latest changes in the teaching syllabus and theories and practices. So our CCOA quiz prep is quality-assured, focused, and has a high hit rate.

ISACA CCOA Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">Technology Essentials: This section of the exam measures skills of a Cybersecurity Specialist and covers the foundational technologies and principles that form the backbone of cybersecurity. It includes topics like hardware and software configurations, network protocols, cloud infrastructure, and essential tools. The focus is on understanding the technical landscape and how these elements interconnect to ensure secure operations.
Topic 2	<ul style="list-style-type: none">Incident Detection and Response: This section of the exam measures the skills of a Cybersecurity Analyst and focuses on detecting security incidents and responding appropriately. It includes understanding security monitoring tools, analyzing logs, and identifying indicators of compromise. The section emphasizes how to react to security breaches quickly and efficiently to minimize damage and restore operations.

Topic 3	<ul style="list-style-type: none"> Adversarial Tactics, Techniques, and Procedures: This section of the exam measures the skills of a Cybersecurity Analyst and covers the tactics, techniques, and procedures used by adversaries to compromise systems. It includes identifying methods of attack, such as phishing, malware, and social engineering, and understanding how these techniques can be detected and thwarted.
Topic 4	<ul style="list-style-type: none"> Securing Assets: This section of the exam measures skills of a Cybersecurity Specialist and covers the methods and strategies used to secure organizational assets. It includes topics like endpoint security, data protection, encryption techniques, and securing network infrastructure. The goal is to ensure that sensitive information and resources are properly protected from external and internal threats.
Topic 5	<ul style="list-style-type: none"> Cybersecurity Principles and Risk: This section of the exam measures the skills of a Cybersecurity Specialist and covers core cybersecurity principles and risk management strategies. It includes assessing vulnerabilities, threat analysis, and understanding regulatory compliance frameworks. The section emphasizes evaluating risks and applying appropriate measures to mitigate potential threats to organizational assets.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q86-Q91):

NEW QUESTION # 86

Which types of network devices are MOST vulnerable due to age and complexity?

- A. Mainframe technology
- B. Operational technology
- C. Ethernet
- D. Wireless

Answer: B

Explanation:

Operational Technology (OT) systems are particularly vulnerable due to their age, complexity, and long upgrade cycles.

- * Legacy Systems: Often outdated, running on old hardware and software with limited update capabilities.
- * Complexity: Integrates various control systems like SCADA, PLCs, and DCS, making consistent security challenging.
- * Lack of Patching: Industrial environments often avoid updates due to fear of system disruptions.
- * Protocols: Many OT devices use insecure communication protocols that lack modern encryption.

Incorrect Options:

- * A. Ethernet: A network protocol, not a system prone to aging or complexity issues.
- * B. Mainframe technology: While old, these systems are typically better maintained and secured.
- * D. Wireless: While vulnerable, it's not primarily due to age or inherent complexity.

Exact Extract from CCOA Official Review Manual, 1st Edition:

Refer to Chapter 7, Section "Securing Legacy Systems," Subsection "Challenges in OT Security" - OT environments often face security challenges due to outdated and complex infrastructure.

NEW QUESTION # 87

Which of the following is the PRIMARY purpose of load balancers in cloud networking?

- A. Load testing applications
- B. Monitoring network traffic
- C. Optimizing database queries
- D. Distributing traffic between multiple servers

Answer: D

Explanation:

The primary purpose of load balancers in cloud networking is to distribute incoming network traffic across multiple servers, thereby:

- * Ensuring Availability: By balancing traffic, load balancers prevent server overload and ensure high availability.
- * Performance Optimization: Evenly distributing traffic reduces response time and improves user experience.

- * Fault Tolerance: If one server fails, the load balancer redirects traffic to healthy servers, maintaining service continuity.
- * Scalability: Automatically adjusts to traffic changes by adding or removing servers as needed.
- * Use Cases: Commonly used for web applications, databases, and microservices in cloud environments.

Other options analysis:

- * B. Optimizing database queries: Managed at the database level, not by load balancers.
- * C. Monitoring network traffic: Load balancers do not primarily monitor but distribute traffic.
- * D. Load testing applications: Load balancers do not perform testing; they manage live traffic.

CCOA Official Review Manual, 1st Edition References:

- * Chapter 4: Network Traffic Management: Discusses the role of load balancers in cloud environments.
- * Chapter 7: High Availability and Load Balancing: Explains how load balancers enhance system resilience.

NEW QUESTION # 88

On the Analyst Desktop is a Malware Samples folder with a file titled Malscript.virus.txt.

What is the name of the service that the malware attempts to install?

Answer:

Explanation:

See the solution in Explanation.

Explanation:

To identify the name of the service that the malware attempts to install from the Malscript.virus.txt file, follow these steps:

Step 1: Access the Analyst Desktop

- * Log into the Analyst Desktop using your credentials.
- * Navigate to the Malware Samples folder located on the desktop.
- * Locate the file:

Malscript.virus.txt

Step 2: Examine the File Contents

- * Open the file with a text editor:
- * Windows: Right-click > Open with > Notepad.
- * Linux:

```
cat ~/Desktop/Malware/Samples/malscript.virus.txt
```

- * Review the content to identify any lines that relate to:

- * Service creation
- * Service names
- * Installation commands

Common Keywords to Look For:

- * New-Service
- * sc create
- * Install-Service
- * Set-Service
- * net start

Step 3: Identify the Service Creation Command

- * Malware typically uses commands like:

powershell

```
New-Service -Name "MalService" -BinaryPathName "C:\Windows\malicious.exe" or cmd sc create MalService binPath="C:\Windows\System32\malicious.exe"
```

- * Focus on lines where the malware tries to register or create a service.

Step 4: Example Content from Malscript.virus.txt

arduino

```
powershell.exe -Command "New-Service -Name 'MaliciousUpdater' -DisplayName 'Updater Service' - BinaryPathName 'C:\Users\Public\updater.exe' -StartupType Automatic"
```

- * In this example, the name of the service is:

nginx

MaliciousUpdater

Step 5: Cross-Verification

- * Check for multiple occurrences of service creation in the script to ensure accuracy.
- * Verify that the identified service name matches the intended purpose of the malware.

pg

The name of the service that the malware attempts to install is: MaliciousUpdater

Step 6: Immediate Action

- * Check for the Service:

```
powershell
Get-Service -Name "MaliciousUpdater"
* Stop and Remove the Service:
powershell
Stop-Service -Name "MaliciousUpdater" -Force
sc delete "MaliciousUpdater"
* Remove Associated Executable:
powershell
Remove-Item "C:\Users\Public\updater.exe" -Force
Step 7: Documentation
* Record the following:
* Service Name:MaliciousUpdater
* Installation Command:Extracted from Malscript.virus.txt
* File Path:C:\Users\Public\updater.exe
* Actions Taken:Stopped and deleted the service.
```

NEW QUESTION # 89

What is the GREATEST security concern associated with virtual (nation technology)?

- A. Insufficient isolation between virtual machines (VMs)
- B. Shared network access
- C. Inadequate resource allocation
- D. Missing patch management for the technology

Answer: A

Explanation:

The greatest security concern associated with virtualization technology is the insufficient isolation between VMs.

- * VM Escape: An attacker can break out of a compromised VM to access the host or other VMs on the same hypervisor.
- * Shared Resources: Hypervisors manage multiple VMs on the same hardware, making it critical to maintain strong isolation.
- * Hypervisor Vulnerabilities: A flaw in the hypervisor can compromise all hosted VMs.
- * Side-Channel Attacks: Attackers can exploit shared CPU cache to leak information between VMs.

Incorrect Options:

- * A. Inadequate resource allocation: A performance issue, not a primary security risk.
- * C. Shared network access: Can be managed with proper network segmentation and VLANs.
- * D. Missing patch management: While important, it is not unique to virtualization.

Exact Extract from CCOA Official Review Manual, 1st Edition:

Refer to Chapter 6, Section "Virtualization Security," Subsection "Risks and Threats" - Insufficient VM isolation is a critical concern in virtual environments.

NEW QUESTION # 90

Which of the following BEST describes JSON web tokens?

- A. They can be used to store user information and session data.
- B. They are signed using a public key and verified using a private key.
- C. They can only be used to authenticate users in web applications.
- D. They are only used with symmetric encryption.

Answer: A

Explanation:

JSON Web Tokens (JWTs) are used to transmit data between parties securely, often for authentication and session management.

- * Data Storage: JWTs can contain user information and session details within the payload section.
- * Stateless Authentication: Since the token itself holds the user data, servers do not need to store sessions.
- * Signed, Not Encrypted: JWTs are typically signed using private keys to ensure integrity but may or may not be encrypted.
- * Common Usage: API authentication, single sign-on (SSO), and user sessions in web applications.

Other options analysis:

- * B. Only for authentication: JWTs can also carry claims for authorization or session data.
- * C. Signed using public key: Usually, JWTs are signed with a private key and verified using a public key.

CCOA Official Review Manual, 1st Edition References:

* Chapter 9: API Security: Discusses the use of JWTs for secure API communication.

• • • • •

CCOA Updated CBT: <https://www.testinsides.top/CCOA-dumps-review.html>

- P.S. Free 2026 ISACA CCOA dumps are available on Google Drive shared by TestInsides: <https://drive.google.com/open?id=1BXX2YXA4t4wrFRSk8f0byZaWE9HitMG0>