

Exam CCOA Study Solutions & CCOA Preparation Store

CCOA EXAM UPDATED QUESTIONS AND ANSWERS

How do you convert a caller into a patient? - CORRECT ANSWER Communicate your expertise, Ask questions, Establish a personal rapport

The uveal tract consists of the iris, ciliary body, and _____? - CORRECT ANSWER Choroid

What skill(s) do(es) an optometric assistant require? - CORRECT ANSWER Communication, Interpersonal, Time Management

What is ultimately NOT a goal when booking patient appointments? - CORRECT ANSWER The needs of the OA

When scheduling an appointment, an example of a positive question is: - CORRECT ANSWER "What type of health insurance coverage do you have?"

What is a legal responsibility of an OA? - CORRECT ANSWER Keep patient information confidential

What is a typical recall for an adult over 65 years of age? - CORRECT ANSWER Once a year

What is the abbreviation for "with correction"? - CORRECT ANSWER cc

What is the term for double vision? - CORRECT ANSWER Diplopia

Which structure produces aqueous humor? - CORRECT ANSWER Ciliary Body

What is the abbreviation for "as needed"? - CORRECT ANSWER prn

Which of the following is an example of a pleasant phrase? - CORRECT ANSWER "Thank you for your feedback."

2026 Latest PDFDumps CCOA PDF Dumps and CCOA Exam Engine Free Share: https://drive.google.com/open?id=1xBNFR33_V5PJpEe9jsl_2rvE9uep5sW4

The ISACA CCOA is available in three easy-to-use forms. The first one is ISACA CCOA dumps PDF format. It is printable and portable. You can print ISACA Certified Cybersecurity Operations Analyst (CCOA) questions PDF or access them via your smartphones, tablets, and laptops. The PDF format can be used anywhere and is essential for students who like to learn on the go.

ISACA CCOA Exam Syllabus Topics:

Topic	Details
Topic 1	<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 2	<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 3	<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.
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"> 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.

>> Exam CCOA Study Solutions <<

ISACA CCOA Preparation Store, Valid CCOA Study Notes

If you are finding a study material to prepare your exam, our material will end your search. Our CCOA exam torrent has a high quality that you can't expect. I think our ISACA Certified Cybersecurity Operations Analyst prep torrent will help you save much time, and you will have more free time to do what you like to do. I can guarantee that you will have no regrets about using our CCOA Test Braindumps When the time for action arrives, stop thinking and go in, try our CCOA exam torrent, you will find our products will be a very good choice for you to pass your exam and get you certificate in a short time.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q55-Q60):

NEW QUESTION # 55

Which of the following roles is responsible for approving exceptions to and deviations from the incident management team charter on an ongoing basis?

- A. Incident response manager
- B. Cybersecurity analyst
- C. Chief information security officer (CISO)
- D. Security steering group

Answer: C

Explanation:

The CISO is typically responsible for approving exceptions and deviations from the incident management team charter because:

* Strategic Decision-Making: As the senior security executive, the CISO has the authority to approve deviations based on risk assessments and business priorities.

* Policy Oversight: The CISO ensures that any exceptions align with organizational security policies.

* Incident Management Governance: As part of risk management, the CISO is involved in high-level decisions impacting incident response.

Other options analysis:

* A. Security steering group: Advises on strategy but does not typically approve operational deviations.

* B. Cybersecurity analyst: Executes tasks rather than making executive decisions.

* D. Incident response manager: Manages day-to-day operations but usually does not approve policy deviations.

CCOA Official Review Manual, 1st Edition References:

- * Chapter 2: Security Governance:Defines the role of the CISO in managing incident-related exceptions.
- * Chapter 8: Incident Management Policies:Discusses decision-making authority within incident response.

NEW QUESTION # 56

Which of the following Is a control message associated with the Internet Control Message Protocol (ICMP)?

- A. 404 is not found.
- B. Transport Layer Security (TLS) protocol version Is unsupported.
- C. Webserver Is available.
- D. Destination is unreachable.

Answer: D

Explanation:

The Internet Control Message Protocol (ICMP) is used for error reporting and diagnostics in IP networks.

* Control Messages: ICMP messages inform the sender about network issues, such as:

* Destination Unreachable: Indicates that the packet could not reach the intended destination.

* Echo Request/Reply: Used in ping to test connectivity.

* Time Exceeded: Indicates that a packet's TTL (Time to Live) has expired.

* Common Usage: Troubleshooting network issues (e.g., ping and traceroute).

Other options analysis:

* A. TLS protocol version unsupported: Related to SSL/TLS, not ICMP.

* C. 404 not found: An HTTP status code, unrelated to ICMP.

* D. Webserver is available: A general statement, not an ICMP message.

CCOA Official Review Manual, 1st Edition References:

* Chapter 4: Network Protocols and ICMP: Discusses ICMP control messages.

* Chapter 7: Network Troubleshooting Techniques: Explains ICMP's role in diagnostics.

NEW QUESTION # 57

The user of the Accounting workstation reported that their calculator repeatedly opens without their input.

Perform a query of startup items for the agent.name:accounting_pc in the SIEM for the last 24 hours.

Identify the file name that triggered RuleName: SuspiciousPowerShell. Enter your response below. Your response must include the file extension.

Answer:

Explanation:

See the solution in Explanation.

Explanation:

To identify the file name that triggered the RuleName: Suspicious PowerShell on the accounting_pc workstation, follow these detailed steps:

Step 1: Access the SIEM System

* Open your web browser and navigate to the SIEM dashboard.

* Log in with your administrator credentials.

Step 2: Set Up the Query

* Go to the Search or Query section of the SIEM.

* Set the Time Range to the last 24 hours.

Query Parameters:

* Agent Name:accounting_pc

* Rule Name: Suspicious PowerShell

* Event Type: Startup items or Process creation

Step 3: Construct the SIEM Query

Here's an example of how to construct the query:

Example Query (Splunk):

index=windows_logs

| search agent.name="accounting_pc" RuleName="Suspicious PowerShell"

| where _time > now() - 24h

| table _time, agent.name, process_name, file_path, RuleName

Example Query (Elastic SIEM):

```
{  
  "query": {  
    "bool": {  
      "must": [  
        { "match": { "agent.name": "accounting-pc" }},  
        { "match": { "RuleName": "Suspicious PowerShell" }},  
        { "range": { "@timestamp": { "gte": "now-24h" } } }  
      ]  
    }  
  }  
}
```

Step 4: Analyze the Query Results

* The query should return a table or list containing:

- * Time of Execution
- * Agent Name:accounting-pc
- * Process Name
- * File Path
- * Rule Name

Example Output:

```
_time  
agent.name  
process_name  
file_path  
RuleName  
2024-04-07T10:45:23  
accounting-pc  
powershell.exe  
C:\Users\Accounting\AppData\Roaming\calc.ps1  
Suspicious PowerShell
```

Step 5: Identify the Suspicious File

* The process_name in the output shows powershell.exe executing a suspicious script.

* The file path indicates the script responsible:

```
makefile  
C:\Users\Accounting\AppData\Roaming\calc.ps1
```

* The suspicious script file is:

calc.ps1

Step 6: Confirm the Malicious Nature

* Manual Inspection:

* Navigate to the specified file path on the accounting-pc workstation.

* Check the contents of calc.ps1 for any malicious PowerShell code.

* Hash Verification:

* Generate the SHA256 hash of the file and compare it with known malware signatures.

calc.ps1

Step 7: Immediate Response

* Isolate the Workstation: Disconnect accounting-pc from the network.

* Terminate the Malicious Process:

* Stop the powershell.exe process running calc.ps1.

* Use Task Manager or a script:

powershell

```
Stop-Process -Name "powershell" -Force
```

* Remove the Malicious Script:

powershell

```
Remove-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Force
```

* Scan for Persistence Mechanisms:

* Check Startup items and Scheduled Tasks for any references to calc.ps1.

Step 8: Documentation

* Record the following:

* Date and Time: When the incident was detected.

* Affected Host: accounting-pc

* Malicious File: calc.ps1

* Actions Taken: File removal and process termination.

NEW QUESTION # 58

An organization's financial data was compromised and posted online. The forensics review confirms proper access rights and encryption of the database at the host site. A lack of which of the following controls MOST likely caused the exposure?

- A. Multi-factor authentication (MFA)
- B. Encryption of data in transit
- C. Continual backups
- D. Properly configured firewall

Answer: A

Explanation:

The compromise occurred despite encryption and proper access rights, indicating that the attacker likely gained access through compromised credentials. MFA would mitigate this by:

- * Adding a Layer of Security: Even if credentials are stolen, the attacker would also need the second factor (e.g., OTP).
- * Account Compromise Prevention: Prevents unauthorized access even if username and password are known.
- * Insufficient Authentication: The absence of MFA often leaves systems vulnerable to credential-based attacks.

Other options analysis:

- * A. Continual backups: Addresses data loss, not unauthorized access.
- * C. Encryption in transit: Encryption was already implemented.
- * D. Configured firewall: Helps with network security, not authentication.

CCOA Official Review Manual, 1st Edition References:

- * Chapter 7: Access Management and Authentication: Discusses the critical role of MFA in preventing unauthorized access.
- * Chapter 9: Identity and Access Control: Highlights how MFA reduces the risk of data exposure.

NEW QUESTION # 59

Management has requested an additional layer of remote access control to protect a critical database that is hosted online. Which of the following would BEST provide this protection?

- A. Implementation of group rights
- B. Incremental backups conducted continuously
- C. A proxy server with a virtual private network (VPN)
- D. Encryption of data at rest

Answer: C

Explanation:

To add an extra layer of remote access control to a critical online database, using a proxy server combined with a VPN is the most effective method.

- * Proxy Server: Acts as an intermediary, filtering and logging traffic.
- * VPN: Ensures secure, encrypted connections from remote users.
- * Layered Security: Integrating both mechanisms protects the database by restricting direct public access and encrypting data in transit.
- * Benefit: Even if credentials are compromised, attackers would still need VPN access.

Incorrect Options:

- * A. Incremental backups: This relates to data recovery, not access control.
- * C. Implementation of group rights: This is part of internal access control but does not add a remote protection layer.
- * D. Encryption of data at rest: Protects stored data but does not enhance remote access security.

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

Refer to Chapter 4, Section "Remote Access Security," Subsection "Securing Remote Access with VPNs and Proxies" - VPNs combined with proxies are recommended for robust remote access control.

NEW QUESTION # 60

.....

You may find that on our website, we have free renewal policy for customers who have bought our CCOA practice quiz. You can enjoy one year free updated service. This policy greatly increase the pass percentage of the candidates if they can't pass in one time or in the limited date. And they can enjoy 50% off if they buy them again one year later. All in all, our service is completely considerate. Come to experience our CCOA Training Materials.

CCOA Preparation Store: <https://www.pdfdumps.com/CCOA-valid-exam.html>

- User-Friendly ISACA CCOA Exam Questions in PDF Format □ Search for ➤ CCOA □ on (www.easy4engine.com) immediately to obtain a free download □ Online CCOA Training Materials
- Prep CCOA Guide □ CCOA Testking Exam Questions * Valid CCOA Exam Pdf □ Copy URL 「 www.pdfvce.com 」 open and search for ▷ CCOA ▲ to download for free □ CCOA Actual Braindumps
- User-Friendly ISACA CCOA Exam Questions in PDF Format □ Enter 「 www.dumpsquestion.com 」 and search for ➡ CCOA □ to download for free □ Prep CCOA Guide
- Exam CCOA Study Solutions Unparalleled Questions Pool Only at Pdfvce □ Copy URL * www.pdfvce.com □ * □ open and search for ▷ CCOA ▲ to download for free □ Reliable CCOA Study Materials
- CCOA Sample Questions □ CCOA Valid Test Review □ Valid CCOA Exam Pdf □ Easily obtain free download of [CCOA] by searching on □ www.troytecdumps.com □ □ Latest Braindumps CCOA Book
- 100% Pass Quiz 2026 ISACA CCOA: Professional Exam ISACA Certified Cybersecurity Operations Analyst Study Solutions □ Search for 《 CCOA 》 on ✓ www.pdfvce.com □ ✓ □ immediately to obtain a free download □ Valid CCOA Test Labs
- Hot ISACA Exam CCOA Study Solutions Carefully Researched by ISACA Experienced Trainers □ Enter * www.troytecdumps.com □ * □ and search for “ CCOA ” to download for free □ Exam CCOA Topics
- Free CCOA Sample □ Valid CCOA Test Sample □ CCOA Valid Exam Dumps □ The page for free download of ⇒ CCOA ⇄ on ➤ www.pdfvce.com □ will open immediately □ Free CCOA Sample
- Pass Leader CCOA Dumps □ CCOA Reliable Test Questions □ Exam CCOA Topics □ Go to website ➡ www.pdfdumps.com □ □ □ open and search for { CCOA } to download for free □ Pass Leader CCOA Dumps
- Get Access To ISACA CCOA Questions Using Three Different Formats □ Open { www.pdfvce.com } and search for ➡ CCOA □ □ □ to download exam materials for free □ CCOA Sample Questions
- Online CCOA Training Materials □ New CCOA Test Book □ New CCOA Test Book □ Easily obtain free download of { CCOA } by searching on { www.vceengine.com } □ CCOA Reliable Test Questions
- academy.makeskilled.com, www.competize.com, bbs.t-firefly.com, disqus.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.bandlab.com, www.yuliancaishang.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New CCOA dumps are available on Google Drive shared by PDFDumps: https://drive.google.com/open?id=1xBNFR33_V5Pjpe9jsl_2rvE9uep5sW4