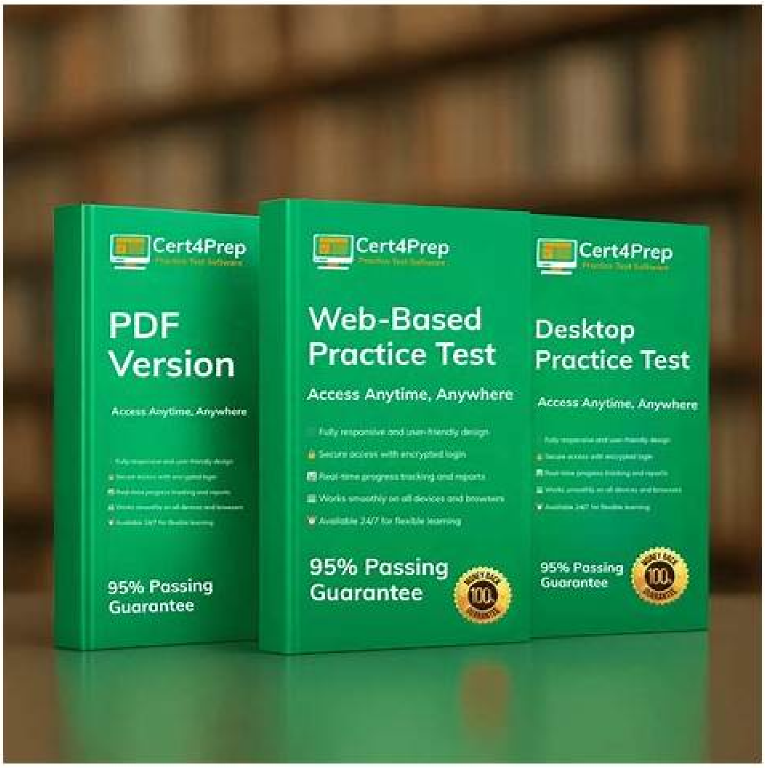
100% ISACA CCOA Correct Answers | CCOA Reliable Dumps Questions



BONUS!!! Download part of TestkingPDF CCOA dumps for free: https://drive.google.com/open?id=1lJU4csPbsoDHPVtnsa3ksX3YgEGcrMZd

The quality of TestkingPDF product is very good and also have the fastest update rate. If you purchase the training materials we provide, you can pass ISACA Certification CCOA Exam successfully.

In today's competitive ISACA industry, only the brightest and most qualified candidates are hired for high-paying positions. Obtaining CCOA certification is a wonderful approach to be successful because it can draw in prospects and convince companies that you are the finest in your field. Pass the ISACA Certified Cybersecurity Operations Analyst to establish your expertise in your field and receive certification. However, passing the ISACA Certified Cybersecurity Operations Analyst CCOA Exam is challenging.

>> 100% ISACA CCOA Correct Answers <<

CCOA Reliable Dumps Questions - CCOA Real Sheets

One of the main unique qualities of TestkingPDF ISACA Certified Cybersecurity Operations Analyst Exam Questions is its ease of use. Our practice exam simulators are user and beginner friendly. You can use ISACA Certified Cybersecurity Operations Analyst (CCOA) PDF dumps and Web-based software without installation. ISACA CCOA PDF Questions work on all the devices like smartphones, Macs, tablets, Windows, etc. We know that it is hard to stay and study for the ISACA Certified Cybersecurity Operations Analyst (CCOA) exam dumps in one place for a long time.

ISACA CCOA Exam Syllabus Topics:

Topic	Details

Topic 1	• 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 2	• 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	• 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 4	• 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 5	• 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.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q114-Q119):

NEW QUESTION # 114

The user of the Accounting workstation reported thattheir calculator repeatedly opens without their input.
The following credentials are used for thisquestion.
Username:Accounting
Password:1x-4cc0unt1NG-x1
Using the provided credentials, SSH to the Accountingworkstation and generate a SHA256 checksum of the filethat triggered RuleName Suspicious PowerShell usingeither certutil or Get-FileHash of the file causing theissue. Copy the hash and paste it below.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To generate theSHA256 checksumof the file that triggeredRuleName: Suspicious PowerShellon the Accounting workstation, follow these detailed steps:
Step 1: Establish an SSH Connection
* Open a terminal on your system.
* Use the provided credentials to connect to theAccounting workstation:

```
ssh Accounting@<Accounting_PC_IP>
```

* Replace <Accounting_PC_IP> with the actual IP address of the workstation.
* Enter the password when prompted:
1x-4cc0unt1NG-x1
Step 2: Locate the Malicious File
* Navigate to the typical directory where suspicious scripts are stored:

```
cd C:\Users\Accounting\AppData\Roaming
```

* List the contents to identify the suspicious file:

```
dir
```

* Look for a file related toPowerShell(e.g., calc.ps1), as the issue involved thecalculator opening repeatedly.

Step 3: Verify the Malicious File

* To ensure it is the problematic file, check for recent modifications:

powershell

```
Get-ChildItem -Path "C:\Users\Accounting\AppData\Roaming" -Recurse | Where-Object { $_.LastWriteTime
-ge (Get-Date).AddDays(-1) }
```

* This will list files modified within the last 24 hours.
* Check file properties:

powershell

```
Get-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" | Format-List *
```

* Confirm it matches the file flagged byRuleName: Suspicious PowerShell.

Step 4: Generate the SHA256 Checksum

Method 1: Using PowerShell (Recommended)

* Run the following command to generate the hash:

powershell

```
Get-FileHash "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Algorithm SHA256
```

* Output Example:

mathematica

```
Algorithm Hash Path
--------- ---- ----
SHA256 d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d C:
\Users\Accounting\AppData\Roaming\calc.ps1
```

Method 2: Using certutil (Alternative)

* Run the following command:

cmd

```
certutil -hashfile "C:\Users\Accounting\AppData\Roaming\calc.ps1" SHA256
```

* Example Output:

```
SHA256 hash of calc.ps1:
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
CertUtil: -hashfile command completed successfully.
```

Step 5: Copy and Paste the Hash

* Copy theSHA256 hashfrom the output and paste it as required.

Final Answer:

nginx

```
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
```

Step 6: Immediate Actions

* Terminate the Malicious Process:

powershell

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

* Delete the Malicious File:

powershell

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

* Disable Startup Entry:
* Check for any persistent scripts:

powershell

```
Get-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"
```

* Remove any entries related to calc.ps1.

Step 7: Document the Incident

* Record the following:
* Filename:calc.ps1
* File Path:C:\Users\Accounting\AppData\Roaming\
* SHA256 Hash:d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
* Date of Detection:(Today's date)

NEW QUESTION # 115

Which of the following has been established when a business continuity manager explains that a critical system can be unavailable up to 4 hours before operation is significantly impaired?

- A. Service level agreement (SLA)
- B. Recovery time objective (RTO)

- C. Recovery point objective (RPO)
- D. Maximum tolerable downtime (MID)

Answer: B

Explanation:
TheRecovery Time Objective (RTO)is themaximum acceptable timethat a system can be down before significantly impacting business operations.
* Context:If thecritical system can be unavailable for up to 4 hours, the RTO is4 hours.
* Objective:To define how quickly systems must be restored after a disruption tominimize operational impact.
* Disaster Recovery Planning:RTO helps design recovery strategies and prioritize resources.
Other options analysis:
* A. Maximum tolerable downtime (MTD):Represents the absolute maximum time without operation, not the target recovery time.
* B. Service level agreement (SLA):Defines service expectations but not recovery timelines.
* C. Recovery point objective (RPO):Defines data loss tolerance, not downtime tolerance.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Business Continuity and Disaster Recovery:Explains RTO and its role in recovery planning.
* Chapter 7: Recovery Strategy Planning:Highlights RTO as a key metric.

NEW QUESTION # 116
A change advisory board Is meeting to review a remediation plan for a critical vulnerability, with a cybersecurity analyst in attendance. When asked about measures to address post-implementation issues, which o! the following would be the analyst's BEST response?

- A. Details for rolling back applied changes should be included In the remediation plan.
- B. The severity of the vulnerability determines whether a rollback plan is required.
- C. The remediation should be canceled if post-implementation issues are anticipated.
- D. The presence of additional onsite staff during the implementation removes the need for a rollback plan.

Answer: A

Explanation:
When discussing a remediation plan for acritical vulnerability, it is essential to include arollback plan because:
* Post-Implementation Issues:Changes can cause unexpected issues or system instability.
* Risk Mitigation:A rollback plan ensures quick restoration to the previous state if problems arise.
* Best Practice:Always plan for potential failures when applying significant security changes.
* Change Management:Ensures continuity by maintaining a safe fallback option.
Other options analysis:
* A. Canceling remediation:This is not a proactive or practical approach.
* C. Severity-based rollback:Rollback plans should be standard regardless of severity.
* D. Additional staff presence:Does not eliminate the need for a rollback strategy.
CCOA Official Review Manual, 1st Edition References:
* Chapter 9: Change Management in Security Operations:Emphasizes rollback planning during critical changes.
* Chapter 8: Vulnerability Management:Discusses post-remediation risk considerations.

NEW QUESTION # 117
Which layer ofthe TCP/IP stack promotes the reliable transmission of data?

- A. Application
- B. Transport
- C. Internet
- D. Link

Answer: B

Explanation:
TheTransport layerof theTCP/IP stackis responsible for thereliable transmission of databetween hosts.
* Protocols:IncludesTCP (Transmission Control Protocol)andUDP (User Datagram Protocol).
* Reliable Data Delivery:TCP ensures data integrity and order through sequencing, error checking, and acknowledgment.

* Flow Control and Congestion Handling:Uses mechanisms likewindowingto manage data flow efficiently.
* Connection-Oriented Communication:Establishes a session between sender and receiver for reliable data transfer.
Other options analysis:
* A. Link:Deals with physical connectivity and media access.
* B. Internet:Handles logical addressing and routing.
* C. Application:Facilitates user interactions and application-specific protocols (like HTTP, FTP).
CCOA Official Review Manual, 1st Edition References:
* Chapter 4: Network Protocols and Layers:Details the role of the Transport layer in reliable data transmission.
* Chapter 6: TCP/IP Protocol Suite:Explains the functions of each layer.

NEW QUESTION # 118

An organization was breached via a web application attack to a database in which user inputs were not validated. This can BEST be described as which type of attack?

- A. Infection
- B. Broken access control
- C. X-Path
- D. Buffer overflow

Answer: B

Explanation:
The described scenario indicates aInjection (i)attack, where the attacker exploitsinsufficient input validation in a web application to manipulate queries. This type of attack falls under the category ofBroken Access Controlbecause:
* Improper Input Handling:The application fails to properly sanitize or validate user inputs, allowing malicious commands to execute.
* Direct Database Manipulation:Attackers can bypass normal authentication or gain elevated access by injecting code.
* OWASP Top Ten 2021:ListsBroken Access Controlas a critical risk, often leading to data breaches when input validation is weak.
Other options analysis:
* B. Infection:Typically involves malware, which is not relevant here.
* C. Buffer overflow:Involves memory management errors, not manipulation.
* D. X-Path:Involves XML query manipulation, not databases.
CCOA Official Review Manual, 1st Edition References:
* Chapter 4: Web Application Security:Discusses Injection as a common form of broken access control.
* Chapter 9: Secure Coding and Development:Stresses the importance of input validation to prevent i.

NEW QUESTION # 119

......

CCOAcertification exam questions have very high quality services in addition to their high quality and efficiency. If you use CCOAtest prep, you will have a very enjoyable experience while improving your ability. We have always advocated customer first. If you use our CCOA Learning Materials to achieve your goals, we will be honored. And our CCOA pdf files give you more efficient learning efficiency and allows you to achieve the best results in a limited time. Our CCOA pdf files are the best exam tool that you have to choose.

download it for free on ▷ www.practicevce.com ◁ website □CCOA Associate Level Exam

- CCOA Valid Exam Camp □ CCOA Exam Blueprint □ Reliable CCOA Exam Answers □ Search for { CCOA } on " www.pdfvce.com " immediately to obtain a free download □CCOA Associate Level Exam
- CCOA Prep Torrent - ISACA Certified Cybersecurity Operations Analyst Exam Torrent -amp; CCOA Test Braindumps □ □ Open website □ www.examcollectionpass.com □ and search for [CCOA] for free download □CCOA Prepaway Dumps
- ISACA Best Available 100% CCOA Correct Answers – Pass CCOA First Attempt □ Search for ➠ CCOA □ on □ www.pdfvce.com □ immediately to obtain a free download ☎CCOA Valid Dumps Free
- CCOA Exam Dumps Provider □ CCOA Valid Exam Camp □ Reliable CCOA Exam Answers □ Easily obtain free download of ➤ CCOA □ by searching on ▶ www.prepawayete.com ◀ □CCOA Valid Test Pdf
- Reliable CCOA Exam Sample □ CCOA Exam Blueprint □ CCOA Reliable Test Guide □ Easily obtain ▷ CCOA ◁ for free download through ☀ www.pdfvce.com □☀□ □CCOA Exam Actual Questions
- 100% CCOA Correct Answers - Free PDF ISACA Realistic ISACA Certified Cybersecurity Operations Analyst Reliable Dumps Questions □ Open ✔ www.verifieddumps.com □✔□ enter ▶ CCOA ◀ and obtain a free download □CCOA Exam Dumps Provider
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, ncon.edu.sa, myportal.utt.edu.tt, drmsobhy.net, www.speaksmart.site, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

What's more, part of that TestkingPDF CCOA dumps now are free: https://drive.google.com/open?id=1lJU4csPbsoDHPVtnsa3ksX3YgEGcrMZd