CCOA Top Exam Dumps, CCOA Valid Test Braindumps

BTW, DOWNLOAD part of ITdumpsfree CCOA dumps from Cloud Storage: https://drive.google.com/open?id=1j97p6Hg2xOtkC9pAIar3FrHwE6sldzvG

We are dedicated to helping you pass the next certificate exam fast. CCOA Exam Braindumps contains questions and answers, and they will be enough for you to deal with your exam. CCOA exam dumps have most of knowledge pointes of the exam. In the process of practicing, you can also improve your ability. Furthermore, we provide you with free demo for you to have a try before purchasing, so that you can have a better understanding of what you are going to buying. If you indeed have questions, just contact our online service stuff.

ISACA CCOA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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	• 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 3	• 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	• 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 5	• 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.

ISACA CCOA Online Practice Test Engine Recommendation

Nowadays passing the test CCOA certification is extremely significant for you and can bring a lot of benefits to you. Passing the test CCOA certification does not only prove that you are competent in some area but also can help you enter in the big company and double your wage. Buying our CCOA Study Materials can help you pass the test easily and successfully. We provide the study materials which are easy to be mastered, professional expert team and first-rate service to make you get an easy and efficient learning and preparation for the CCOA test.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q27-Q32):

NEW QUESTION # 27
Which of the following is MOST important for maintaining an effective risk management program?

- A. Automated reporting
- B. Approved budget
- C. Ongoing review
- D. Monitoring regulations

Answer: C

NEW QUESTION # 28
Which of the following should occur FIRST during the vulnerability identification phase?

- A. Run vulnerability scans of all in-scope assets.
- B. Assess the risks associated with the vulnerabilities Identified.
- C. Inform relevant stakeholders that vulnerability scanning will be taking place.
- D. Determine the categories of vulnerabilities possible for the type of asset being tested.

Answer: C

Explanation:
During thevulnerability identification phase, thefirst stepis toinform relevant stakeholdersabout the upcoming scanning activities:
* Minimizing Disruptions:Prevents stakeholders from mistaking scanning activities for an attack.
* Change Management:Ensures that scanning aligns with operational schedules to minimize downtime.
* Stakeholder Awareness:Helps IT and security teams prepare for the scanning process and manage alerts.
* Authorization:Confirms that all involved parties are aware and have approved the scanning.
Incorrect Options:
* B. Run vulnerability scans:Should only be done after proper notification.
* C. Determine vulnerability categories:Done as part of planning, not the initial step.
* D. Assess risks of identified vulnerabilities:Occurs after the scan results are obtained.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 6, Section "Vulnerability Management," Subsection "Preparation and Communication" - Informing stakeholders

ensures transparency and coordination.

NEW QUESTION # 29
The user of the Accounting workstation reported thattheir calculator repeatedly opens without their input.
Perform a query of startup items for the agent.nameaccounting-pc in the SIEM for the last 24 hours.
Identifythe file name that triggered RuleName SuspiciousPowerShell. Enter your response below. Your responsemust include the file extension.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To identify thefile namethat triggered theRuleName: Suspicious PowerShellon theaccounting-pc workstation, follow these detailed steps:
Step 1: Access the SIEM System
* Open your web browser and navigate to theSIEM dashboard.
* Log in with youradministrator credentials.
Step 2: Set Up the Query
* Go to theSearchorQuerysection of the SIEM.
* Set theTime Rangeto thelast 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
* Theprocess_namein the output showspowershell.exeexecuting a suspicious script.
* Thefile pathindicates 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 theaccounting-pcworkstation.
* Check the contents of calc.ps1 for any malicious PowerShell code.
* Hash Verification:
* Generate theSHA256 hashof the file and compare it with known malware signatures.
calc.ps1
Step 7: Immediate Response
* Isolate the Workstation:Disconnectaccounting-pcfrom 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:
* CheckStartup itemsandScheduled Tasksfor 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 # 30
Which of the following can be used to identity malicious activity through a take user identity?

- A. Honeypot
- B. Multi-factor authentication (MFA)
- C. Honey account
- D. Indicator of compromise (IoC)

Answer: C

Explanation:
Ahoney accountis adecoy user accountset up to detectmalicious activity, such as:
* Deception Techniques:The account appears legitimate to attackers, enticing them to use it.
* Monitoring Usage:Any interaction with the honey account triggers an alert, indicating potential compromise.
* Detection of Credential Theft:If attackers attempt to use the honey account, it signals possible credential leakage.
* Purpose:Specifically designed toidentify malicious activitythrough themisuse of seemingly valid accounts.
Other options analysis:
* A. Honeypot:A decoy system or network, not specifically an account.
* C. Indicator of compromise (IoC):Represents evidence of an attack, not a decoy mechanism.
* D. Multi-factor authentication (MFA):Increases authentication security, but does not detect malicious use directly.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Threat Detection and Deception:Discusses the use of honey accounts for detecting unauthorized access.
* Chapter 8: Advanced Threat Intelligence:Highlights honey accounts as a proactive detection technique.

NEW QUESTION # 31
What is the GREATEST security concern associated with virtual (nation technology?

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

Answer: D

Explanation:
The greatest security concern associated withvirtualization technologyis theinsufficient 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 # 32
.....

If you feel difficult in choosing which version of our CCOA reliable exam guide, if you want to be simple, PDF version may be suitable for you. PDF version is a normal file. Many candidates are used to printing out and then writing & reading of CCOA reliable exam guide on paper. Yes, it is silent and clear. Also if you have some unclearly questions, you can ask or talk with others easily. Others may just think that it is normally practice material. Also you can print out many copies of ISACA CCOA Reliable Exam Guide and share with others.

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, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, Disposable vapes

P.S. Free & New CCOA dumps are available on Google Drive shared by ITdumpsfree: https://drive.google.com/open?id=1j97p6Hg2xOtkC9pAIar3FrHwE6sldzvG