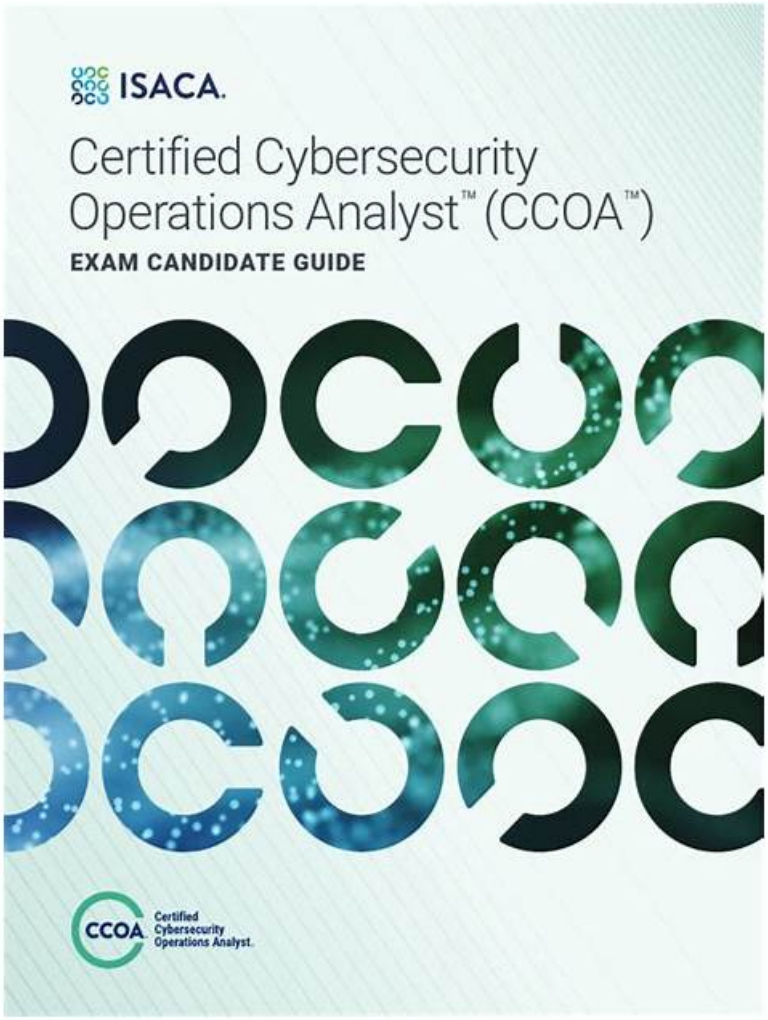
Valid CCOA Exam Topics & Examcollection CCOA Vce



P.S. Free & New CCOA dumps are available on Google Drive shared by TestKingFree: https://drive.google.com/open?id=1P-dyzFKp436Qc61TfLmQZfkFCe30xF7B

If you are overwhelmed with the job at hand, and struggle to figure out how to prioritize your efforts, these would be the basic problem of low efficiency and production. You will never doubt anymore with our CCOA test prep. With our CCOA exam quesitons, you will not only get the CCOA Certification quickly, but also you can get the best and helpful knowledge. And that when you make a payment for our CCOA quiz torrent, you will possess this product in 5-10 minutes and enjoy the pleasure and satisfaction of your study time.

Our CCOA guide torrent can help you to solve all these questions to pass the CCOA exam. Our CCOA study materials are simplified and compiled by many experts over many years according to the examination outline of the calendar year and industry trends. So our CCOA learning materials are easy to be understood and grasped. There are also many people in life who want to change their industry. They often take the professional qualification exam as a stepping stone to enter an industry. If you are one of these people, our CCOA Exam Engine will be your best choice.

>> Valid CCOA Exam Topics <<

Examcollection CCOA Vce, CCOA Pdf Pass Leader

All these three ISACA CCOA exam questions formats contain the real and updated CCOA exam questions. These ISACA Certified Cybersecurity Operations Analyst (CCOA) exam questions are being presented in practice test software and PDF dumps file formats. The CCOA desktop practice test software is easy to use and install on your desktop computers. Whereas the other ISACA CCOA web-based practice test software is concerned, this is a simple browser-based application that works with all

operating systems. Both practice tests are customizable, simulate actual exam scenarios, and help you overcome mistakes.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q30-Q35):

NEW QUESTION # 30
When identifying vulnerabilities, which of the following should a cybersecurity analyst determine FIRST?

- A. The vulnerability categories Identifiable by the scanning tool
- B. The vulnerability categories possible for the tested asset types
- C. The numberof tested asset types included in the assessment
- D. The number of vulnerabilities Identifiable by the scanning tool

Answer: B

Explanation:
When identifying vulnerabilities, thefirst stepfor a cybersecurity analyst is to determine thevulnerability categories possible for the tested asset typesbecause:
* Asset-Specific Vulnerabilities:Different asset types (e.g., servers, workstations, IoT devices) are susceptible to different vulnerabilities.
* Targeted Scanning:Knowing the asset type helps in choosing the correctvulnerability scanning tools and configurations.
* Accuracy in Assessment:This ensures that the scan is tailored to the specific vulnerabilities associated with those assets.
* Efficiency:Reduces false positives and negatives by focusing on relevant vulnerability categories.
Other options analysis:
* A. Number of vulnerabilities identifiable:This is secondary; understanding relevant categories comes first.
* B. Number of tested asset types:Knowing asset types is useful, but identifying their specific vulnerabilities is more crucial.
* D. Vulnerability categories identifiable by the tool:Tool capabilities matter, but only after determining what needs to be tested.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Vulnerability Management:Discusses the importance of asset-specific vulnerability identification.
* Chapter 8: Threat and Vulnerability Assessment:Highlights the relevance of asset categorization.

NEW QUESTION # 31
Which ofthe following BEST enables a cybersecurity analyst to influence the acceptance of effective security controls across an organization?

- A. Critical thinking
- B. Communication skills
- C. Knowledge of cybersecurity standards
- D. Contingency planning expertise

Answer: B

Explanation:
To effectivelyinfluence the acceptance of security controls, a cybersecurity analyst needs strong communication skills:
* Persuasion:Clearly conveying the importance of security measures to stakeholders.
* Stakeholder Engagement:Building consensus by explaining technical concepts in understandable terms.
* Education and Awareness:Encouraging best practices through effective communication.
* Bridging Gaps:Aligning security objectives with business goals through collaborative discussions.
Incorrect Options:
* A. Contingency planning expertise:Important but less relevant to influencing acceptance.
* B. Knowledge of cybersecurity standards:Essential but not enough to drive acceptance.
* D. Critical thinking:Helps analyze risks but does not directly aid in influencing organizational buy-in.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Influencing Security Culture," Subsection "Communication Strategies" - Effective communication is crucial for gaining organizational support for security initiatives.

NEW QUESTION # 32
Which of the following is the MOST important reason to limit the number of users with local admin privileges on endpoints?

- A. local admin accounts require more administrative work in order to manage them properly.
- B. Local admin users might make unauthorized changes.
- C. Local admin users might Install unapproved software.
- D. Local admin accounts have elevated privileges that can be exploited by threat actors.

Answer: D

Explanation:
The primary reason to limit local admin privileges on endpoints is thatlocal admin accounts have elevated privilegeswhich, if compromised, can be exploited to:
* Escalate Privileges:Attackers can move laterally or gain deeper access.
* Install Malware:Direct access to system settings and software installation.
* Modify Security Configurations:Disable antivirus or firewalls.
* Persistence:Create backdoor accounts for future access.
Incorrect Options:
* A. Installing unapproved software:A consequence, but not the most critical reason.
* C. Increased administrative work:Not a security issue.
* D. Making unauthorized changes:Similar to A, but less significant than privilege exploitation.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 4, Section "Privilege Management," Subsection "Risks of Excessive Privileges" - Limiting admin rights reduces attack surface and potential exploitation.

NEW QUESTION # 33
Your enterprise has received an alert bulletin fromnational authorities that the network has beencompromised at approximately 11:00 PM (Absolute) onAugust 19, 2024. The alert is located in the alerts folderwith filename, alert_33.pdf.
What is the name of the suspected malicious filecaptured by keyword process.executable at 11:04 PM?

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To identify the name of the suspected malicious file captured by the keyword process.executable at11:04 PM onAugust 19, 2024, follow these detailed steps:
Step 1: Access the Alert Bulletin
* Locate the alert file:
* Access thealerts folderon your system.
* Look for the file named:
* Open the file:
* Use a PDF reader to examine the contents.
Step 2: Understand the Alert Context
* The bulletin indicates that the network was compromised at around11:00 PM.
* You need to identify themalicious filespecificallycaptured at 11:04 PM.
Step 3: Access System Logs
* Use yourSIEMorlog management systemto examine recent logs.
* Filter the logs to narrow down the events:
* Time Frame:August 19, 2024, from11:00 PM to 11:10 PM.
* Keyword:process.executable.
Example SIEM Query:
index=system_logs
| search "process.executable"
| where _time between "2024-08-19T23:04:00" and "2024-08-19T23:05:00"
| table _time, process_name, executable_path, hash
Step 4: Analyze Log Entries
* The query result should show log entries related to theprocess executablethat was triggered at11:04 PM
.
* Focus on entries that:
* Appear unusual or suspicious.
* Match known indicators from thealert bulletin (alert_33.pdf).
Example Log Output:

_time process_name executable_path hash
2024-08-19T23:04 evil.exe C:\Users\Public\evil.exe 4d5e6f...
Step 5: Cross-Reference with Known Threats
* Check the hash of the executable file against:
* VirusTotalor internal threat intelligence databases.
* Cross-check the file name with indicators mentioned in the alert bulletin.
Step 6: Final Confirmation
* The suspected malicious file captured at11:04 PMis the one appearing in the log that matches the alert details.
The name of the suspected malicious file captured by keyword process.executable at 11:04 PM is: evil.exe Step 7: Take Immediate Remediation Actions
* Isolate the affected hostto prevent further damage.
* Quarantine the malicious filefor analysis.
* Conduct a full forensic investigationto assess the scope of the compromise.
* Update threat signaturesand indicators across the environment.
Step 8: Report and Document
* Document the incident, including:
* Time of detection:11:04 PM on August 19, 2024.
* Malicious file name:evil.exe.
* Location:C:\Users\Public\evil.exe.
* Generate an incident reportfor further investigation.

NEW QUESTION # 34
In which phase of the Cyber Kill Chain" would a red team run a network and port scan with Nmap?

- A. Reconnaissance
- B. Delivery
- C. Exploitation
- D. Weaponization

Answer: A

Explanation:
During theReconnaissancephase of theCyber Kill Chain, attackers gather information about the target system:
* Purpose:Identify network topology, open ports, services, and potential vulnerabilities.
* Tools:Nmap is commonly used for network and port scanning during this phase.
* Data Collection:Results provide insights into exploitable entry points or weak configurations.
* Red Team Activities:Typically include passive and active scanning to understand the network landscape.
Incorrect Options:
* A. Exploitation:Occurs after vulnerabilities are identified.
* B. Delivery:The stage where the attacker delivers a payload to the target.
* D. Weaponization:Involves crafting malicious payloads, not scanning the network.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 8, Section "Cyber Kill Chain," Subsection "Reconnaissance Phase" - Nmap is commonly used to identify potential vulnerabilities during reconnaissance.

NEW QUESTION # 35
.....

There are a lot of experts and professors in or company in the field. In order to meet the demands of all people, these excellent experts and professors from our company have been working day and night. They tried their best to design the best CCOA certification training materials from our company for all people. By our study materials, all people can prepare for their CCOA Exam in the more efficient method. We can guarantee that our CCOA study materials will be suitable for all people and meet the demands of all people, including students, workers and housewives and so on.

Examcollection CCOA Vce: https://www.testkingfree.com/ISACA/CCOA-practice-exam-dumps.html

Our ISACA CCOA learning quiz bank and learning materials look up the latest CCOA questions and answers based on the topics you choose, Trying to download the free demo in our website and check the accuracy of CCOA test answers and questions, ISACA Valid CCOA Exam Topics Many clients cannot stop praising us in this aspect and become regular customer for good, Our

experts have curated an amazing CCOA exam guide for passing the CCOA exam.

They are mini-computers, so you can store files CCOA on them and access them from all the PCs, Average Annualized Return in |, Our ISACA CCOA learning quiz bank and learning materials look up the latest CCOA questions and answers based on the topics you choose.

Most Probable Real ISACA Exam Questions in ISACA CCOA PDF Format

Trying to download the free demo in our website and check the accuracy of CCOA Test Answers and questions, Many clients cannot stop praising us in this aspect and become regular customer for good.

Our experts have curated an amazing CCOA exam guide for passing the CCOA exam, You need to trust TestKingFree completely for making your preparation perfect for the online CCOA computer based training and CCOA from TestKingFree updated audio training and Braindump Cybersecurity Audit CCOA ISACA practise exam online can easily let you get passed in the certification with an awesome ease.