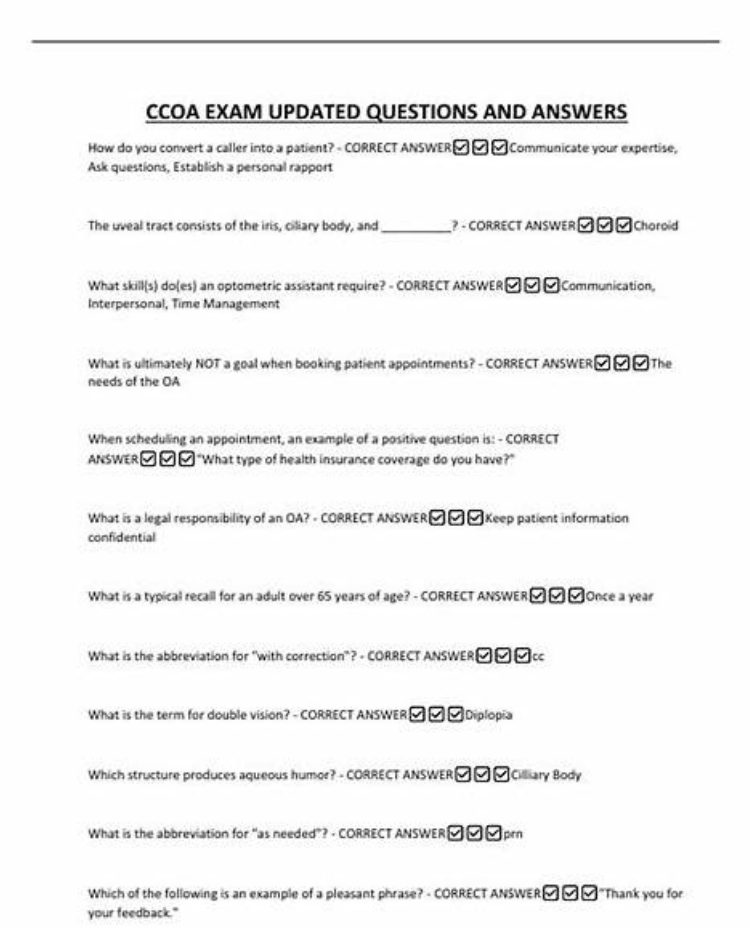
Updated CCOA CBT - CCOA New Practice Questions



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☑☑☑Cilliary 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."

What's more, part of that BraindumpsIT CCOA dumps now are free: https://drive.google.com/open?id=1vj_vzGYoqjnNMQos-Zw8fOGlaQ_szoqF

You can attempt the CCOA test multiple times to relieve exam stress and boosts confidence. Besides Windows, BraindumpsIT ISACA CCOA web-based practice exam works on iOS, Android, Linux, and Mac. You can take ISACA Certified Cybersecurity Operations Analyst (CCOA) practice exams (desktop and web-based) of BraindumpsIT multiple times to improve your critical thinking and understand the CCOA test inside out. BraindumpsIT has been creating the most reliable ISACA Dumps for many years. And we have helped thousands of ISACA aspirants in earning the CCOA certification.

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	• 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	• 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	• 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.

Know How To Resolve The Anxiety ISACA CCOA Exam Fever After The Preparation

Do you still worry about that you can't find an ideal job and earn low wage? Do you still complaint that your working abilities can't be recognized and you have not been promoted for a long time? You can try to obtain the CCOA certification and if you pass the exam you will have a high possibility to find a good job with a high income. If you buy our CCOA questions torrent you will pass the exam easily and successfully. Our CCOA Study Materials are compiled by experts and approved by professionals with experiences for many years. We provide 3 versions for the client to choose and free update. Different version boosts different advantage and please read the introduction of each version carefully before your purchase.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q100-Q105):

NEW QUESTION # 100
In which phase of the Cyber Kill Chain" would a red team run a network and port scan with Nmap?

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

Answer: C

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 # 101
Compliance requirements are imposed on organizations to help ensure:

- A. minimum capabilities for protecting public interests are in place.
- B. systemvulnerabilities are mitigated in a timely manner.
- C. rapidly changing threats to systems are addressed.
- D. security teams understand which capabilities are most important for protecting organization.

Answer: A

Explanation:
Compliance requirements are imposed on organizations to ensure that they meetminimum standards for protecting public interests.
* Regulatory Mandates:Many compliance frameworks (like GDPR or HIPAA) mandate minimum data protection and privacy measures.
* Public Safety and Trust:Ensuring that organizations follow industry standards to maintain data integrity and confidentiality.
* Baseline Security Posture:Establishes a minimum set of controls to protect sensitive information and critical systems.
Incorrect Options:
* A. System vulnerabilities are mitigated:Compliance does not directly ensure vulnerability management.
* B. Security teams understand critical capabilities:This is a secondary benefit but not the primary purpose.
* C. Rapidly changing threats are addressed:Compliance often lags behind new threats; it's more about maintaining baseline security.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Compliance and Legal Considerations," Subsection "Purpose of Compliance" - Compliance frameworks aim to ensure that organizations implement minimum protective measures for public safety and data protection.

NEW QUESTION # 102
An employee has been terminated for policy violations.Security logs from win-webserver01 have been collectedand located in the Investigations folder on theDesktop as win-webserver01_logs.zip.
Create a new case in Security Onion from the win-webserver01_logs.zip file. The case title is WindowsWebserver Logs - CCOA New Case and TLP must beset to Green. No additional fields are required.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To create a new case inSecurity Onionusing the logs from the win-webserver01_logs.zip file, follow these detailed steps:
Step 1: Access Security Onion
* Open a web browser and go to yourSecurity Onionweb interface.
URL: https://<security-onion-ip>/
* Log in using yourSecurity Onioncredentials.
Step 2: Prepare the Log File
* Navigate to theDesktopand open theInvestigationsfolder.
* Locate the file:
win-webserver01_logs.zip
* Unzip the file to inspect its contents:
unzip ~/Desktop/Investigations/win-webserver01_logs.zip -d ~/Desktop/Investigations/win-webserver01_logs
* Ensure that the extracted files, including System-logs.evtx, are accessible.
Step 3: Open the Hunt Interface in Security Onion
* On the Security Onion dashboard, go to"Hunt"(or"Cases"depending on the version).
* Click on"Cases"to manage incident cases.
Step 4: Create a New Case
* Click on"New Case"to start a fresh investigation.
Case Details:
* Title:
Windows Webserver Logs - CCOA New Case
* TLP (Traffic Light Protocol):

* Set toGreen(indicating that the information can be shared freely).
Example Configuration:
Field
Value
Title
Windows Webserver Logs - CCOA New Case
TLP
Green
Summary
(Leave blank if not required)
* Click"Save"to create the case.
Step 5: Upload the Log Files
* After creating the case, go to the"Files"section of the new case.
* Click on"Upload"and select the unzipped log file:
~/Desktop/Investigations/win-webserver01_logs/System-logs.evtx
* Once uploaded, the file will be associated with the case.
Step 6: Verify the Case Creation
* Go back to theCasesdashboard.
* Locate and verify that the case"Windows Webserver Logs - CCOA New Case"exists withTLP:
Green.
* Check that thelog filehas been successfully uploaded.
Step 7: Document and Report
* Document the case details:
* Case Title:Windows Webserver Logs - CCOA New Case
* TLP:Green
* Log File:System-logs.evtx
* Include anyinitial observationsfrom the log analysis.
Example Answer:
A new case titled "Windows Webserver Logs - CCOA New Case" with TLP set to Green has been successfully created in Security Onion. The log file System-logs.evtx has been uploaded and linked to the case.
Step 8: Next Steps for Investigation
* Analyze the log file:Start hunting for suspicious activities.
* Create analysis tasks:Assign team members to investigate specific log entries.
* Correlate with other data:Cross-reference with threat intelligence sources.

NEW QUESTION # 103
Which of the following is MOST important for maintaining an effective risk management program?

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

Answer: C

NEW QUESTION # 104
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 # 105
......

before making a choice, you can download a trial version of CCOA preparation materials. After you use it, you will have a more complete understanding of this CCOA exam questions. In this way, you can use our CCOA study materials in a way that suits your needs and professional opinions. We hope you will have a great experience with CCOA Preparation materials. At the same time, we also hope that you can realize your dreams with our help. We will be honored.