New CCOA Test Objectives | Standard CCOA Answers

What's more, part of that ActualCollection CCOA dumps now are free: https://drive.google.com/open?id=1dr5LcVI0IPtAB-JlF3LjdsZFFYBl4ToD

Our website has focused on the study of CCOA PDF braindumps for many years and created latest ISACA CCOA dumps pdf for all level of candiates. All questions and answers are tested and approved by our professionals who are specialized in the CCOA Pass Guide. To ensure your post-purchase peace of mind, we provide you with up to 12 months of free ISACA CCOA exam questions updates. Grab these offers today!

ISACA CCOA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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	• 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	• 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.

Buy ActualCollection ISACA CCOA Practice Questions and Save Money With Free Updates

Once you compare our CCOA study materials with the annual real exam questions, you will find that our CCOA exam questions are highly similar to the real exam questions. We have strong strengths to assist you to pass the exam. All in all, we hope that you are brave enough to challenge yourself. Our CCOA learning prep will live up to your expectations. It will be your great loss to miss our CCOA practice engine.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q11-Q16):

NEW QUESTION # 11
On the Analyst Desktop is a Malware Samples folderwith a file titled Malscript.viruz.txt.
What is the name of the service that the malware attempts to install?

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To identify thename of the servicethat the malware attempts to install from theMalscript.viruz.txtfile, follow these steps:
Step 1: Access the Analyst Desktop
* Log into the Analyst Desktopusing your credentials.
* Navigate to theMalware Samplesfolder located on the desktop.
* Locate the file:
Malscript.viruz.txt
Step 2: Examine the File Contents
* Open the file with a text editor:
* Windows:Right-click > Open with > Notepad.
* Linux:
cat ~/Desktop/Malware\ Samples/malscript.viruz.txt
* Review the content to identify any lines that relate to:
* Service creation
* Service names
* Installation commands
Common Keywords to Look For:
* New-Service
* sc create
* Install-Service
* Set-Service
* net start
Step 3: Identify the Service Creation Command
* Malware typically uses commands like:
powershell
New-Service -Name "MalService" -BinaryPathName "C:\Windows\malicious.exe" or cmd sc create MalService binPath=

"C:\Windows\System32\malicious.exe"
* Focus on lines where the malware tries toregister or create a service.
Step 4: Example Content from Malscript.viruz.txt
arduino
powershell.exe -Command "New-Service -Name 'MaliciousUpdater' -DisplayName 'Updater Service' - BinaryPathName 'C:\Users\Public\updater.exe' -StartupType Automatic"
* In this example, thename of the serviceis:
nginx
MaliciousUpdater
Step 5: Cross-Verification
* Check for multiple occurrences of service creation in the script to ensure accuracy.
* Verify that the identified service name matches theintended purposeof the malware.
pg
The name of the service that the malware attempts to install is: MaliciousUpdater Step 6: Immediate Action
* Check for the Service:
powershell
Get-Service -Name "MaliciousUpdater"
* Stop and Remove the Service:
powershell
Stop-Service -Name "MaliciousUpdater" -Force
sc delete "MaliciousUpdater"
* Remove Associated Executable:
powershell
Remove-Item "C:\Users\Public\updater.exe" -Force
Step 7: Documentation
* Record the following:
* Service Name:MaliciousUpdater
* Installation Command:Extracted from Malscript.viruz.txt
* File Path:C:\Users\Public\updater.exe
* Actions Taken:Stopped and deleted the service.

NEW QUESTION # 12
Which of the following Is a control message associated with the Internet Control Message Protocol (ICMP)?

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

Answer: B

Explanation:
TheInternet Control Message Protocol (ICMP)is used forerror reporting and diagnosticsin 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 inpingto test connectivity.
* Time Exceeded:Indicates that a packet'sTTL (Time to Live)has expired.
* Common Usage:Troubleshooting network issues (e.g.,pingandtraceroute).
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 # 13
Which of the following would BCST enable an organization to prioritize remediation activities when multiple vulnerabilities are

identified?

- A. Vulnerability exception process
- B. Risk assessment
- C. executive reporting process
- D. Business Impact analysis (BIA)

Answer: B

Explanation:
Arisk assessmentenables organizations toprioritize remediation activitieswhen multiple vulnerabilities are identified because:
* Contextual Risk Evaluation:Assesses the potential impact and likelihood of each vulnerability.
* Prioritization:Helps determine which vulnerabilities pose the highest risk to critical assets.
* Resource Allocation:Ensures that remediation efforts focus on the most significant threats.
* Data-Driven Decisions:Uses quantitative or qualitative metrics to support prioritization.
Other options analysis:
* A. Business Impact Analysis (BIA):Focuses on the impact of business disruptions, not directly on vulnerabilities.
* B. Vulnerability exception process:Manages known risks but does not prioritize them.
* C. Executive reporting process:Summarizes security posture but does not prioritize remediation.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Risk Assessment Techniques:Emphasizes the importance of risk analysis in vulnerability management.
* Chapter 7: Prioritizing Vulnerability Remediation:Guides how to rank threats based on risk.

NEW QUESTION # 14
Which of the following BEST enables an organization to identify potential security threats by monitoring and analyzing network traffic for unusual activity?

- A. Web application firewall (WAP)
- B. Endpoint security
- C. Data loss prevention (DLP)
- D. Security operation center (SOC)

Answer: D

Explanation:
ASecurity Operation Center (SOC)is tasked with monitoring and analyzing network traffic to detect anomalies and potential security threats.
* Role:SOCs collect and analyze data from firewalls, intrusion detection systems (IDS), and other network monitoring tools.
* Function:Analysts in the SOC identify unusual activity patterns that may indicate intrusions or malware.
* Proactive Threat Detection:Uses log analysis and behavioral analytics to catch threats early.
Incorrect Options:
* A. Web application firewall (WAF):Protects against web-based attacks but does not analyze network traffic in general.
* B. Endpoint security:Focuses on individual devices, not network-wide monitoring.
* D. Data loss prevention (DLP):Monitors data exfiltration rather than overall network activity.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 8, Section "Security Monitoring and Threat Detection," Subsection "Role of the SOC" - SOCs are integral to identifying potential security threats through network traffic analysis.

NEW QUESTION # 15
Which of the following utilities is MOST suitable for administrative tasks and automation?

- A. System service dispatcher (SSO)
- B. Integrated development environment (IDE)
- C. Command line Interface (CLI)
- D. Access control list (ACL)

Answer: C

Explanation:

TheCommand Line Interface (CLI)ismost suitable for administrative tasks and automationbecause:
* Scriptable and Automatable:CLI commands can be combined in scripts for automating repetitive tasks.
* Direct System Access:Administrators can directly interact with the system to configure, manage, and troubleshoot.
* Efficient Resource Usage:Consumes fewer system resources compared to graphical interfaces.
* Customizability:Advanced users can chain commands and create complex workflows using shell scripting.
Other options analysis:
* B. Integrated Development Environment (IDE):Primarily used for software development, not system administration.
* C. System service dispatcher (SSO):Not relevant for administrative tasks.
* D. Access control list (ACL):Manages permissions, not administrative automation.
CCOA Official Review Manual, 1st Edition References:
* Chapter 9: System Administration Best Practices:Highlights the role of CLI in administrative and automation tasks.
* Chapter 7: Automation in Security Operations:Explains the efficiency of CLI-based automation.

NEW QUESTION # 16
.....

If you suffer from procrastination and cannot make full use of your sporadic time during your learning process, it is an ideal way to choose our CCOA training dumps. We can guarantee that you are able not only to enjoy the pleasure of study but also obtain your CCOA Certification successfully, which can be seen as killing two birds with one stone. And you will be surprised to find our superiorities of our CCOA exam questions than the other vendors'.