ISACA CCOA Exam | CCOA Actual Test Answers - Help you Pass CCOA: ISACA Certified Cybersecurity Operations Analyst Exam

2025 Latest CramPDF CCOA PDF Dumps and CCOA Exam Engine Free Share: https://drive.google.com/open?id=1rl31tJdJX402Qt1TjVsPpHGDBQX3Z_C9

The page of our CCOA simulating materials provides demo which are sample questions. The purpose of providing demo is to let customers understand our part of the topic and what is the form of our CCOA study materials when it is opened? In our minds, these two things are that customers who care about the CCOA Exam may be concerned about most. We will give you our software which is a clickable website that you can visit the product page.

ISACA CCOA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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	• 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	• 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.

First-hand ISACA CCOA Actual Test Answers - Guaranteed ISACA Certified Cybersecurity Operations Analyst Questions Answers

CCOA study guide provides free trial services, so that you can gain some information about our study contents, topics and how to make full use of the software before purchasing. It's a good way for you to choose what kind of CCOA training prep is suitable and make the right choice to avoid unnecessary waste. Our purchase process is of the safety and stability if you have any trouble in the purchasing CCOA practice materials or trail process, you can contact us immediately.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q39-Q44):

NEW QUESTION # 39
Following a ransomware incident, the network teamprovided a PCAP file, titled ransom.pcap, located in theInvestigations folder on the Desktop.
What is the full User-Agent value associated with theransomware demand file download. Enter your responsein the field below.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To identify thefull User-Agent valueassociated with theransomware demand file downloadfrom the ransom.pcapfile, follow these detailed steps:
Step 1: Access the PCAP File
* Log into the Analyst Desktop.
* Navigate to theInvestigationsfolder located on the desktop.
* Locate the file:
ransom.pcap
Step 2: Open the PCAP File in Wireshark
* LaunchWireshark.
* Open the PCAP file:
mathematica
File > Open > Desktop > Investigations > ransom.pcap
* ClickOpento load the file.
Step 3: Filter HTTP Traffic
Since ransomware demands are often served astext files (e.g., README.txt)via HTTP/S, use the following filter:
http.request or http.response
* This filter will show bothHTTP GETandPOSTrequests.
Step 4: Locate the Ransomware Demand File Download
* Look for HTTPGETrequests that include common ransomware filenames such as:
* README.txt
* DECRYPT_INSTRUCTIONS.html
* HELP_DECRYPT.txt
* Right-click on the suspicious HTTP packet and select:
arduino

Follow > HTTP Stream
* Analyze theHTTP headersto find theUser-Agent.
Example HTTP Request:
GET /uploads/README.txt HTTP/1.1
Host: 10.10.44.200
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36 Step 5: Verify the User-Agent
* Check multiple streams to ensure consistency.
* Confirm that theUser-Agentbelongs to the same host(10.10.44.200)involved in the ransomware incident.
swift
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.
0.5414.75 Safari/537.36
Step 6: Document and Report
* Record the User-Agent for analysis:
* PCAP Filename:ransom.pcap
* User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36
* Related File:README.txt
Step 7: Next Steps
* Forensic Analysis:
* Look for more HTTP requests from the sameUser-Agent.
* Monitor Network Activity:
* Identify other systems with the same User-Agent pattern.
* Block Malicious Traffic:
* Update firewall rules to block any outbound connections to suspicious domains.

NEW QUESTION # 40
An organization has received complaints from a number of its customers that their data has been breached.
However, after an investigation, the organization cannot detect any indicators of compromise. The breach was MOST likely due to which type of attack?

- A. injection attack
- B. Zero-day attack
- C. Supply chain attack
- D. Man-in the-middle attack

Answer: C

Explanation:
Asupply chain attackoccurs when a threat actor compromises athird-party vendoror partner that an organization relies on. The attack is then propagated to the organization through trusted connections or software updates.
* Reason for Lack of Indicators of Compromise (IoCs):
* The attack often occursupstream(at a vendor), so the compromised organization may not detect any direct signs of breach.
* Trusted Components:Malicious code or backdoors may be embedded intrusted software updatesor services.
* Real-World Example:TheSolarWinds breach, where attackers compromised the software build pipeline, affecting numerous organizations without direct IoCs on their systems.
* Why Not the Other Options:
* B. Zero-day attack:Typically leaves some traces or unusual behavior.
* C. injection attack:Usually detectable through web application monitoring.
* D. Man-in-the-middle attack:Often leaves traces in network logs.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Advanced Threats and Attack Techniques:Discusses the impact of supply chain attacks.
* Chapter 9: Incident Response Planning:Covers the challenges of detecting supply chain compromises.

NEW QUESTION # 41
Most of the operational responsibility remains with the customerin which of the following cloudservice models?

- A. Platform as a Service (PaaS)

- B. Software as a Service (SaaS)
- C. Data Platform as a Service (DPaaS)
- D. Infrastructure as a Service (IaaS)

Answer: D

Explanation:
In theIaaS (Infrastructure as a Service)model, the majority of operational responsibilities remain with the customer.
* Customer Responsibilities:OS management, application updates, security configuration, data protection, and network controls.
* Provider Responsibilities:Hardware maintenance, virtualization, and network infrastructure.
* Flexibility:Customers have significant control over the operating environment, making them responsible for most security measures.
Incorrect Options:
* A. Data Platform as a Service (DPaaS):Managed data services where the provider handles database infrastructure.
* B. Software as a Service (SaaS):Provider manages almost all operational aspects.
* C. Platform as a Service (PaaS):Provider manages the platform; customers focus on application management.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 3, Section "Cloud Service Models," Subsection "IaaS Responsibilities" - IaaS requires customers to manage most operational aspects, unlike PaaS or SaaS.

NEW QUESTION # 42
Which of the following Is the MOST effective way to ensure an organization's management of supply chain risk remains consistent?

- A. Regularly meeting with suppliers to informally discuss Issues
- B. Periodically counting the number of incident tickets associated with supplier services
- C. Regularly seeking feedback from the procurement team regarding supplier responsiveness
- D. Periodically confirming suppliers' contractual obligations are met

Answer: D

Explanation:
To maintain consistent management ofsupply chain risk, it is essential toperiodically confirm that suppliers meet their contractual obligations.
* Risk Assurance:Verifies that suppliers adhere to security standards and commitments.
* Compliance Monitoring:Ensures that the agreed-upon controls and service levels are maintained.
* Consistency:Regular checks prevent lapses in compliance and identify potential risks early.
* Supplier Audits:Include reviewing security controls, data protection measures, and compliance with regulations.
Incorrect Options:
* A. Seeking feedback from procurement:Useful but not directly related to risk management.
* C. Counting incident tickets:Measures service performance, not risk consistency.
* D. Informal meetings:Lacks formal assessment and verification of obligations.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Supply Chain Risk Management," Subsection "Monitoring and Compliance" - Periodic verification of contractual compliance ensures continuous risk management.

NEW QUESTION # 43
Robust background checks provide protection against:

- A. phishing.
- B. ransomware.
- C. distributed dental of service (DDoS) attacks.
- D. insider threats.

Answer: D

Explanation:
Robust background checks help mitigateinsider threatsby ensuring that individuals withaccess to sensitive data or critical systemsdo not have a history of risky or malicious behavior.
* Screening:Identifies red flags like past criminal activity or suspicious financial behavior.
* Trustworthiness Assessment:Ensures that employees handling sensitive information have a proven history of integrity.

* Insider Threat Mitigation:Helps reduce the risk of data theft, sabotage, or unauthorized access.
* Periodic Rechecks:Maintain ongoing security by regularly updating background checks.
Incorrect Options:
* A. DDoS attacks:Typically external; background checks do not mitigate these.
* C. Phishing:An external social engineering attack, unrelated to employee background.
* D. Ransomware:Generally spread via malicious emails or compromised systems, not insider actions.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 4, Section "Insider Threat Management," Subsection "Pre-Employment Screening" - Background checks are vital in identifying potential insider threats before hiring.

NEW QUESTION # 44
.....

CramPDF's ISACA CCOA Exam Training materials is no other sites in the world can match. Of course, this is not only the problem of quality, it goes without saying that our quality is certainly the best. More important is that CramPDF's exam training materials is applicable to all the IT exam. So the website of CramPDF can get the attention of a lot of candidates. They believe and rely on us. It is also embodied the strength of our CramPDF site. The strength of CramPDF is embodied in it. Our exam training materials could make you not help recommend to your friends after you buy it. Because it's really a great help to you.