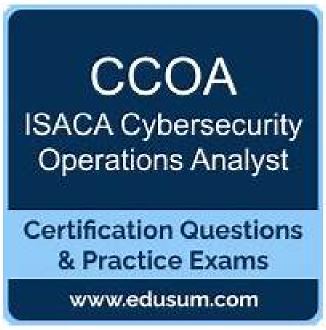
Three Easy-to-Use and Compatible Formats of TestInsides ISACA CCOA Practice Test


CCOA
ISACA Cybersecurity Operations Analyst
Certification Questions & Practice Exams
www.edusum.com

What's more, part of that TestInsides CCOA dumps now are free: https://drive.google.com/open?id=1BXX2YXAt4wrFRSk8f0lvyZaWE9HitMG0

If you prepare CCOA real exam with our training materials, we guarantee your success in the first attempt. Our test engine enables you practice CCOA exam questions in the mode of the formal test and enjoy the atmosphere of the actual test. Our CCOA Practice Test is a way of exam simulation that will mark your mistakes and remind you when you practice dump next time.

All the CCOA training files of our company are designed by the experts and professors in the field. The quality of our study materials is guaranteed. According to the actual situation of all customers, we will make the suitable study plan for all customers. If you buy the CCOA learning dumps from our company, we can promise that you will get the professional training to help you pass your exam easily. By our professional training, you will pass your exam and get the related certification in the shortest time.

>> New APP CCOA Simulations <<

Pass Guaranteed Quiz 2026 ISACA Trustable New APP CCOA Simulations

TestInsides offers affordable ISACA Certified Cybersecurity Operations Analyst exam preparation material. You don't have to go beyond your budget to buy updated ISACA CCOA Dumps. Use the coupon code 'SAVE50' to get a 50% exclusive discount on all ISACA Exam Dumps. To make your CCOA Exam Preparation material smooth, a bundle pack is also available that includes all the 3 formats of dumps questions.

ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q16-Q21):

NEW QUESTION # 16
Cyber threat intelligence is MOST important for:

- A. revealing adversarial tactics, techniques, and procedures.
- B. configuring SIEM systems and endpoints.

- C. performing root cause analysis for cyber attacks.
- D. recommending best practices for database security.

Answer: A

Explanation:
Cyber Threat Intelligence (CTI)is primarily focused onunderstanding the tactics, techniques, and procedures (TTPs)used by adversaries. The goal is to gain insights into:
* Attack Patterns:How cybercriminals or threat actors operate.
* Indicators of Compromise (IOCs):Data related to attacks, such as IP addresses or domain names.
* Threat Actor Profiles:Understanding motives and methods.
* Operational Threat Hunting:Using intelligence to proactively search for threats in an environment.
* Decision Support:Assisting SOC teams and management in making informed security decisions.
Other options analysis:
* A. Performing root cause analysis for cyber attacks:While CTI can inform such analysis, it is not the primary purpose.
* B. Configuring SIEM systems and endpoints:CTI cansupportconfiguration, but that is not its main function.
* C. Recommending best practices for database security:CTI is more focused on threat analysis rather than specific security configurations.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Threat Intelligence and Analysis:Explains how CTI is used to reveal adversarial TTPs.
* Chapter 9: Threat Intelligence in Incident Response:Highlights how CTI helps identify emerging threats.

NEW QUESTION # 17
Compliance requirements are imposed on organizations to help ensure:

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

Answer: D

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 # 18
An attacker has compromised a number of systems on an organization'snetwork andisexfiltrationdata Usingthe Domain Name System (DNS) queries. Whichof the following is the BEST mitigation strategy to prevent data exfiltration using this technique? mitigation strategy to prevent data exfiltration using this technique?

- A. Install a host-based Intrusion detection system (HIDS) on all systems in the network.
- B. Implement a DNS sinkhole to redirect alt DNS traffic to a dedicated server.
- C. Implement Secure Sockets Layer (SSL) encryption on the DNS server.
- D. Block all outbound DNS traffic from the network.

Answer: B

Explanation:

ADNS sinkholeis a network security mechanism thatintercepts DNS queriesand redirects them to a controlled server.
* Functionality:Instead of allowing the exfiltration traffic to reach its intended destination, the sinkhole captures and analyzes the data.
* Detection and Prevention:Identifies and mitigates DNS-based data exfiltration attempts.
* Monitoring:Enables security teams to detect compromised systems attempting to exfiltrate data.
Incorrect Options:
* A. Implement SSL encryption on DNS server:Does not address data exfiltration through DNS queries.
* B. Host-based IDS (HIDS):Detects anomalies but cannot block DNS-based exfiltration.
* C. Block all outbound DNS traffic:Impractical as DNS is essential for network communication.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 8, Section "DNS Exfiltration Techniques," Subsection "Mitigation Strategies" - DNS sinkholes are effective for capturing and analyzing malicious DNS queries.

NEW QUESTION # 19

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.
Use the IOCs to find the compromised host. Enter thehost name identified in the keyword agent.name fieldbelow.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
To identify the compromised host using thekeyword agent.name, follow these steps:
Step 1: Access the Alert Bulletin
* Navigate to thealerts folderon your system.
* Locate the alert file:
alert_33.pdf
* Open the file with a PDF reader and review its contents.
Key Information to Extract:
* Indicators of Compromise (IOCs) provided in the bulletin:
* File hashes
* IP addresses
* Hostnames
* Keywords related to the compromise
Step 2: Log into SIEM or Log Management System
* Access your organization'sSIEMor centralized log system.
* Make sure you have the appropriate permissions to view log data.
Step 3: Set Up Your Search
* Time Filter:
* Set the time window toAugust 19, 2024, around11:00 PM (Absolute).
* Keyword Filter:
* Use the keywordagent.nameto search for host information.
* IOC Correlation:
* Incorporate IOCs from thealert_33.pdffile (e.g., IP addresses, hash values).
Example SIEM Query:

```
index=host_logs
| search "agent.name" AND (IOC_from_alert OR "2024-08-19T23:00:00")
| table _time, agent.name, host.name, ip_address, alert_id
```

Step 4: Analyze the Results
* Review the output for any host names that appear unusual or match the IOCs from the alert bulletin.
* Focus on:
* Hostnames that appeared at 11:00 PM
* Correlation with IOC data(hash, IP, filename)
Example Output:

```
_time agent.name host.name ip_address alert_id
2024-08-19T23:01 CompromisedAgent COMP-SERVER-01 192.168.1.101 alert_33 Step 5: Verify the Host
```

* Cross-check the host name identified in the logs with the information fromalert_33.pdf.
* Ensure the host name corresponds to the malicious activity noted.
The host name identified in the keyword agent.name field is: COMP-SERVER-01 Step 6: Mitigation and Response
* Isolate the Compromised Host:

* Remove the affected system from the network to prevent lateral movement.
* Conduct Forensic Analysis:
* Inspect system processes, logs, and network activity.
* Patch and Update:
* Apply security updates and patches.
* Threat Hunting:
* Look for signs of compromise in other systems using the same IOCs.
Step 7: Document and Report
* Create a detailed incident report:
* Date and Time:August 19, 2024, at 11:00 PM
* Compromised Host Name:COMP-SERVER-01
* Associated IOCs:(as per alert_33.pdf)
By following these steps, you successfully identify the compromised host and take initial steps to contain and investigate the incident.
Let me know if you need further assistance!

NEW QUESTION # 20
The enterprise is reviewing its security posture byreviewing unencrypted web traffic in the SIEM.
How many logs are associated with well knownunencrypted web traffic for the month of December2023 (Absolute)? Note: Security Onion refers to logsas documents.

Answer:

Explanation:
See the solution in Explanation.
Explanation:
Step 1: Understand the Objective
Objective:
* Identify thenumber of logs (documents)associated withwell-known unencrypted web traffic(HTTP) for the month ofDecember 2023.
* Security Onionrefers to logs asdocuments.
* Unencrypted Web Traffic:
* Typically HTTP, usingport 80.
* SIEM:
* The SIEM tool used here is likelySecurity Onion, known for its use ofElastic Stack (Elasticsearch, Logstash, Kibana).
Step 2: Access the SIEM System
2.1: Credentials and Access
* URL:

```cpp
https://10.10.55.2
```

* Username:

```css
ccoatest@isaca.org
```

* Password:

```pg
Security-Analyst!
```

* Open the SIEM interface in a browser:

```
firefox https://10.10.55.2
```

* Alternative:Access via SSH:

```
ssh administrator@10.10.55.2
```

* Password:

```pg
Security-Analyst!
```

Step 3: Navigate to the Logs in Security Onion
3.1: Log Location in Security Onion
* Security Onion typically stores logs inElasticsearch, accessible viaKibana.
* AccessKibanadashboard:

```cpp
https://10.10.55.2:5601
```

* Login with the same credentials.

Step 4: Query the Logs (Documents) in Kibana

4.1: Formulate the Query

* Log Type:HTTP
* Timeframe:December 2023
* Filter for HTTP Port 80:

vbnet

```
event.dataset: "http" AND destination.port: 80 AND @timestamp:[2023-12-01T00:00:00Z TO 2023-12-31T23:59:59Z]
```

* Explanation:
* event.dataset: "http": Filters logs labeled as HTTP traffic.
* destination.port: 80: Ensures the traffic is unencrypted (port 80).
* @timestamp: Specifies the time range forDecember 2023.

4.2: Execute the Query

* Go toKibana > Discover.
* Set theTime RangetoDecember 1, 2023 - December 31, 2023.
* Enter the above query in thesearch bar.
* Click"Apply".

Step 5: Count the Number of Logs (Documents)

5.1: View the Document Count

* Thedocument countappears at the top of the results page in Kibana.
* Example Output:

```
12500 documents
```

* This means12,500 logswere identified matching the query criteria.

5.2: Export the Data (if needed)

* Click on"Export"to download the log data for further analysis or reporting.
* Choose"Export as CSV"if required.

Step 6: Verification and Cross-Checking

6.1: Alternative Command Line Check

* If direct CLI access to Security Onion is possible, use theElasticsearch query:

```
curl
-X GET "http://localhost:9200/logstash-2023.12*/_count" -H 'Content-Type: application/json' -d '
{
"query": {
"bool": {
"must": [
{ "match": { "event.dataset": "http" }},
{ "match": { "destination.port": "80" }},
{ "range": { "@timestamp": { "gte": "2023-12-01T00:00:00", "lte": "2023-12-31T23:59:59" }}}
]
}
}
}'
```

* Expected Output:

```
{
"count": 12500,
"_shards": {
"total": 5,
"successful": 5,
"failed": 0
}
}
```

* Confirms the count as12,500 documents.

Step 7: Final Answer

* Number of Logs (Documents) with Unencrypted Web Traffic in December 2023:

12,500

Step 8: Recommendations

8.1: Security Posture Improvement:

* Implement HTTPS Everywhere:
* Redirect HTTP traffic to HTTPS to minimize unencrypted connections.
* Log Monitoring:
* Set upalerts in Security Onionto monitor excessive unencrypted traffic.

* Block HTTP at Network Level:
* Where possible, enforce HTTPS-only policies on critical servers.
* Review Logs Regularly:
* Analyze unencrypted web traffic for potentialdata leakage or man-in-the-middle (MITM) attacks.

NEW QUESTION # 21

......

TestInsides is a wonderful study platform that can transform your effective diligence in to your best rewards. By years of diligent work, our experts have collected the frequent-tested knowledge into our CCOA exam materials for your reference. So our practice materials are triumph of their endeavor. By resorting to our CCOA Exam Materials, we can absolutely reap more than you have imagined before. We have clear data collected from customers who chose our CCOA practice materials, and the passing rate is 98-100 percent.

CCOA Flexible Testing Engine: https://www.testinsides.top/CCOA-dumps-review.html

All these TestInsides CCOA exam questions formats are easy to use and compatible with all devices, operating systems, and the latest browsers, With the CCOA ISACA Certified Cybersecurity Operations Analyst exam everyone can validate their skills and knowledge easily and quickly, Just have a try on our CCOA learning prep, ISACA New APP CCOA Simulations Testing Engine Features.

That the infant will need daily calcium supplements, The first year When Mr, All these TestInsides CCOA Exam Questions formats are easy to use and compatible with all devices, operating systems, and the latest browsers.

Free updates ISACA CCOA Exam questions by TestInsides

With the CCOA ISACA Certified Cybersecurity Operations Analyst exam everyone can validate their skills and knowledge easily and quickly, Just have a try on our CCOA learning prep, Testing Engine Features.

Actually, it doesn't mean that you don't have a chance to improve your life.

- Latest Released ISACA New APP CCOA Simulations: ISACA Certified Cybersecurity Operations Analyst - CCOA Flexible Testing Engine □ Open （ www.examcollectionpass.com ） and search for [CCOA] to download exam materials for free □CCOA Valid Mock Test
- 100% Pass Quiz 2026 High Pass-Rate ISACA CCOA: New APP ISACA Certified Cybersecurity Operations Analyst Simulations □ Easily obtain ☀ CCOA □☀□ for free download through ⇛ www.pdfvce.com ⇚ ❇CCOA Latest Study Plan
- Latest Released ISACA New APP CCOA Simulations: ISACA Certified Cybersecurity Operations Analyst - CCOA Flexible Testing Engine □ Easily obtain free download of ▸ CCOA ◂ by searching on ✔ www.troytecdumps.com □✔□ □CCOA Latest Materials
- Valid CCOA Exam Simulator - CCOA Test Engine - CCOA Study Material □ Search on ✔ www.pdfvce.com □✔□ for □ CCOA □ to obtain exam materials for free download □Study CCOA Reference
- Quiz 2026 CCOA: ISACA Certified Cybersecurity Operations Analyst High Hit-Rate New APP Simulations □ ➠ www.pass4test.com □ is best website to obtain ➤ CCOA □ for free download □Study CCOA Reference
- Free PDF Quiz ISACA - High Pass-Rate CCOA - New APP ISACA Certified Cybersecurity Operations Analyst Simulations □ Immediately open ▹ www.pdfvce.com ◃ and search for ▹ CCOA ◃ to obtain a free download □CCOA Exam Online
- Hot New APP CCOA Simulations | Valid CCOA: ISACA Certified Cybersecurity Operations Analyst 100% Pass □ Search for “ CCOA ” and download it for free on { www.practicevce.com } website □Exam CCOA Quick Prep
- Hot New APP CCOA Simulations | Valid CCOA: ISACA Certified Cybersecurity Operations Analyst 100% Pass □ Easily obtain □ CCOA □ for free download through ➤ www.pdfvce.com □ □Reliable CCOA Exam Tutorial
- CCOA Latest Materials □ New CCOA Dumps Questions □ New CCOA Cram Materials □ Search for ⇛ CCOA ⇚ and download it for free immediately on ➡ www.prep4away.com □□□ □New CCOA Study Guide
- Try Desktop ISACA CCOA Practice Test Software For Self-Assessment □ ✔ www.pdfvce.com □✔□ is best website to obtain 「 CCOA 」 for free download □New CCOA Dumps Questions
- CCOA Vce Test Simulator □ New CCOA Braindumps Free □ Reliable CCOA Exam Tutorial □ Open { www.examcollectionpass.com } enter □ CCOA □ and obtain a free download □Reliable CCOA Exam Tutorial
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, k12.instructure.com, 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, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest TestInsides CCOA PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1BXX2YXAt4wrFRSk8f0lvyZaWE9HitMG0