CAS-005 Actual Test - CAS-005 Dumps Collection

P.S. Free & New CAS-005 dumps are available on Google Drive shared by Test4Sure: https://drive.google.com/open?id=1_HNj-Y26EjaeN1TmpHbOlEKbkR-Gp_BT

The real and updated CompTIA CompTIA CAS-005 exam dumps file, desktop practice test software, and web-based practice test software are ready for download. Take the best decision of your professional career and enroll in the CompTIA SecurityX Certification Exam (CAS-005) certification exam and download CompTIA SecurityX Certification Exam (CAS-005) exam questions and starts preparing today.

The price for CAS-005 learning materials is reasonable, and no matter you are a student or an employee, you can afford the expense. In addition, CAS-005 exam dumps are edited by professional experts, and therefore the quality can be guaranteed. CAS-005 exam materials cover most of the knowledge points for the exam, and you can master them through study. In order to let you know the latest information for the exam ,we offer you free update for 365 days after purchasing, and the update version for CAS-005 Exam Dumps will be sent to you automatically.

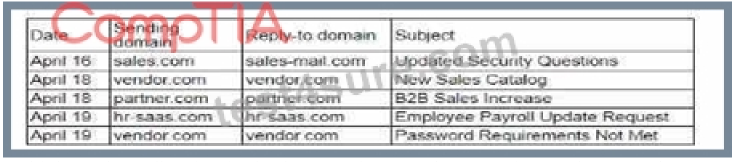
>> CAS-005 Actual Test <<

CAS-005 Dumps Collection | CAS-005 Pass Guide

Test4Sure CAS-005 exam dumps in three different formats has CAS-005 questions PDF and the facility of CompTIA CAS-005 dumps. We have made these CompTIA CAS-005 questions after counseling a lot of experts and getting their feedback. The 24/7 customer support team is available at Test4Sure for CompTIA CAS-005 Dumps users so that they don't get stuck in any hitch.

CompTIA SecurityX Certification Exam Sample Questions (Q297-Q302):

NEW QUESTION # 297
A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes. The following email headers are being reviewed:



Date	Sending domain	Reply-to domain	Subject
April 16	sales.com	sales-mail.com	Updated Security Questions
April 18	vendor.com	vendor.com	New Sales Catalog
April 18	partner.com	partner.com	B2B Sales Increase
April 19	hr-saas.com	hr-saas.com	Employee Payroll Update Request
April 19	vendor.com	vendor.com	Password Requirements Not Met

Which of the following is the best action for the security analyst to take?

- A. Block messages from hr-saas.com because it is not a recognized domain.
- B. Reroute all messages with unusual security warning notices to the IT administrator
- C. Block vendor com for repeated attempts to send suspicious messages
- D. Quarantine all messages with sales-mail.com in the email header

Answer: C

Explanation:
In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains.
Block vendor com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.

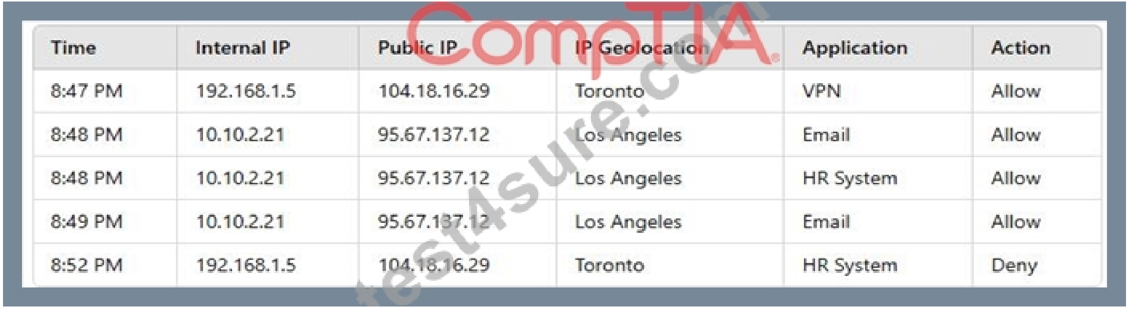
NEW QUESTION # 298
A security engineer needs to ensure production containers are automatically scanned for vulnerabilities before they are accepted into the production environment. Which of the following should the engineer use to automatically incorporate vulnerability scanning on every commit?

- A. Integrated development environment
- B. Code repository
- C. Container orchestrator
- D. CI/CD pipeline

Answer: D

Explanation:
CI/CD pipeline (Continuous Integration/Continuous Deployment) automates the testing, including vulnerability scanning, for every code commit before deploying to production. Code repository stores the code but does not handle scanning. Integrated development environment (IDE) aids developers in writing and testing code but does not enforce automated scanning.
Container orchestrator manages container deployment but does not directly address pre- production scanning.

NEW QUESTION # 299
A user reports application access issues to the help desk. The help desk reviews the logs for the user:



Time	Internal IP	Public IP	IP Geolocation	Application	Action
8:47 PM	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 PM	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 PM	10.10.2.21	95.67.137.12	Los Angeles	HR System	Allow
8:49 PM	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 PM	192.168.1.5	104.18.16.29	Toronto	HR System	Deny

Which of the following is most likely the reason for the issue?

- A. The user is not allowed to access the human resources system outside of business hours.
- B. A threat actor has compromised the user's account and attempted to log in.
- C. The user inadvertently tripped the geoblock rule in NGFW.
- D. The user did not attempt to connect from an approved subnet.

Answer: C

Explanation:
The logs show that the user connected fromToronto (104.18.16.29)andLos Angeles (95.67.137.12)within minutes. The sudden location change is a typical trigger forgeoblocking in a Next-Generation Firewall (NGFW), leading to theHR System being denied.
A compromised account (B)would show failed login attempts or unusual activities, but all other access attempts were allowed.
Business hours restriction (C)is unlikely since the user was granted access earlier.
Approved subnet issues (D)would affect all applications, not just HR System access.

NEW QUESTION # 300

Which of the following supports the process of collecting a large pool of behavioral observations to inform decision-making?

- A. Machine learning
- B. Linear regression
- C. Big Data
- D. Distributed consensus

Answer: C

Explanation:

Collecting a large pool of behavioral observations requires handling vast datasets, which is the domain ofBig Data. Big Data technologies enable the storage, processing, and analysis of large-scale data (e.g., user behavior logs) to inform decisions, a key capability in security analytics.

* Option A:Linear regression is a statistical method for modeling relationships, not collecting data.

* Option B:Distributed consensus relates to agreement in distributed systems (e.g., blockchain), not data collection.

* Option C:Big Data directly supports collecting and analyzing large datasets for insights, fitting the question perfectly.

* Option D:Machine learning uses data to train models but relies on data being collected first, often via Big Data.

Reference:CompTIA SecurityX CAS-005 Domain 3: Research, Development, and Collaboration - Data Analytics for Security.

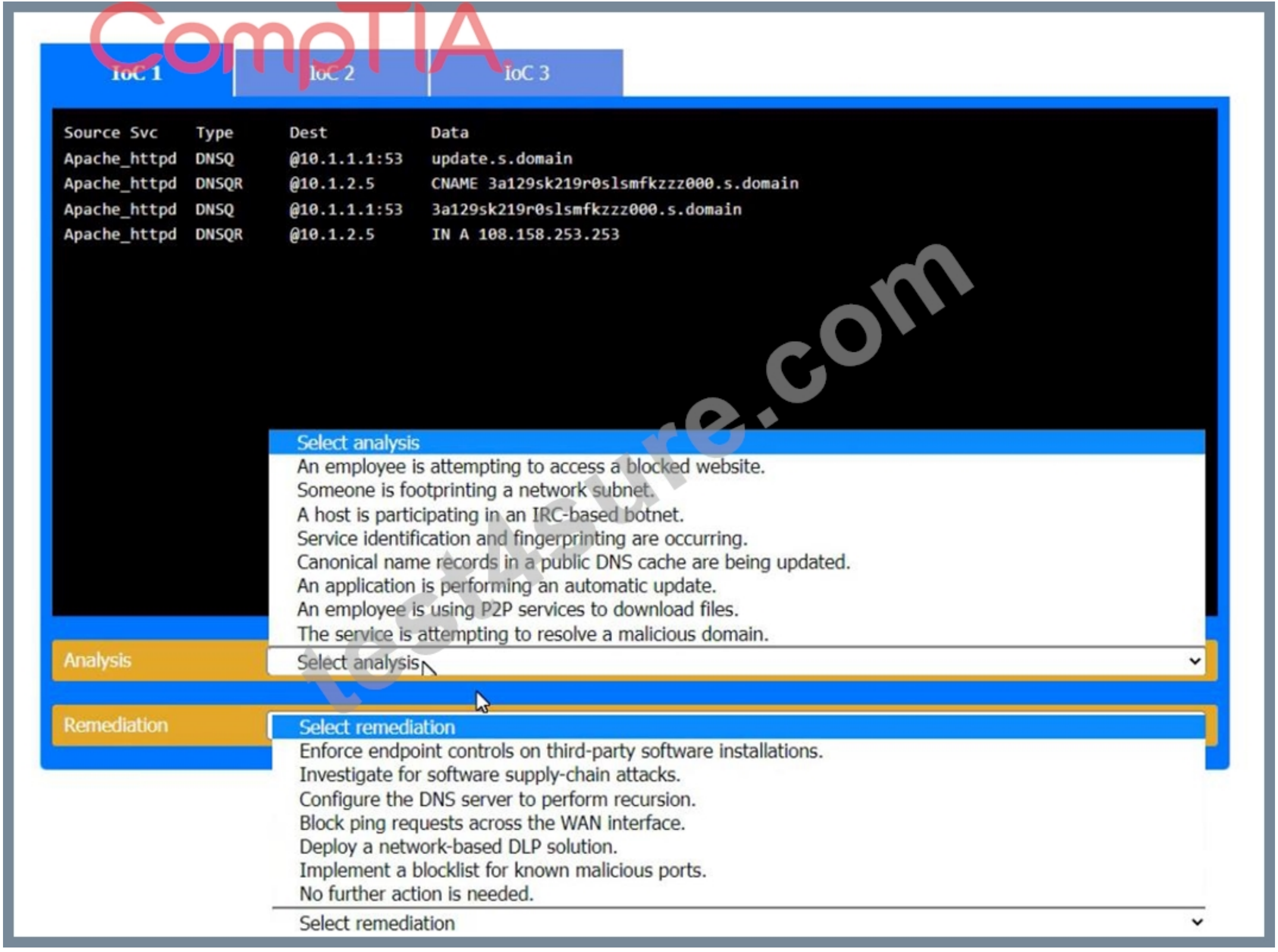
NEW QUESTION # 301

SIMULATION

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

INSTRUCTIONS

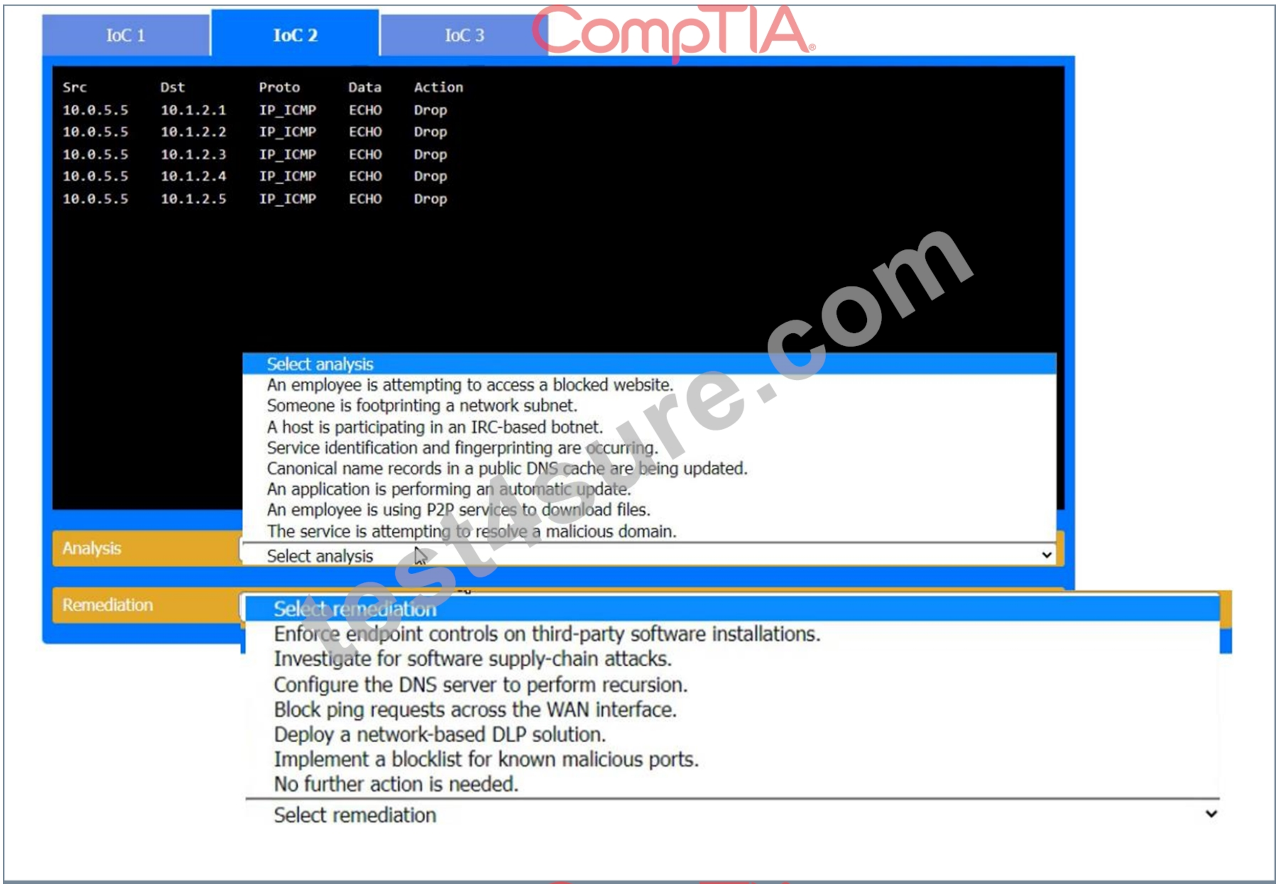
Review each of the events and select the appropriate analysis and remediation options for each IoC.



```
Source Svc    Type    Dest           Data
Apache_httpd  DNSQ    @10.1.1.1:53   update.s.domain
Apache_httpd  DNSQR   @10.1.2.5      CNAME 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd  DNSQ    @10.1.1.1:53   3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd  DNSQR   @10.1.2.5      IN A 108.158.253.253
```

Select analysis
An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.
Select analysis

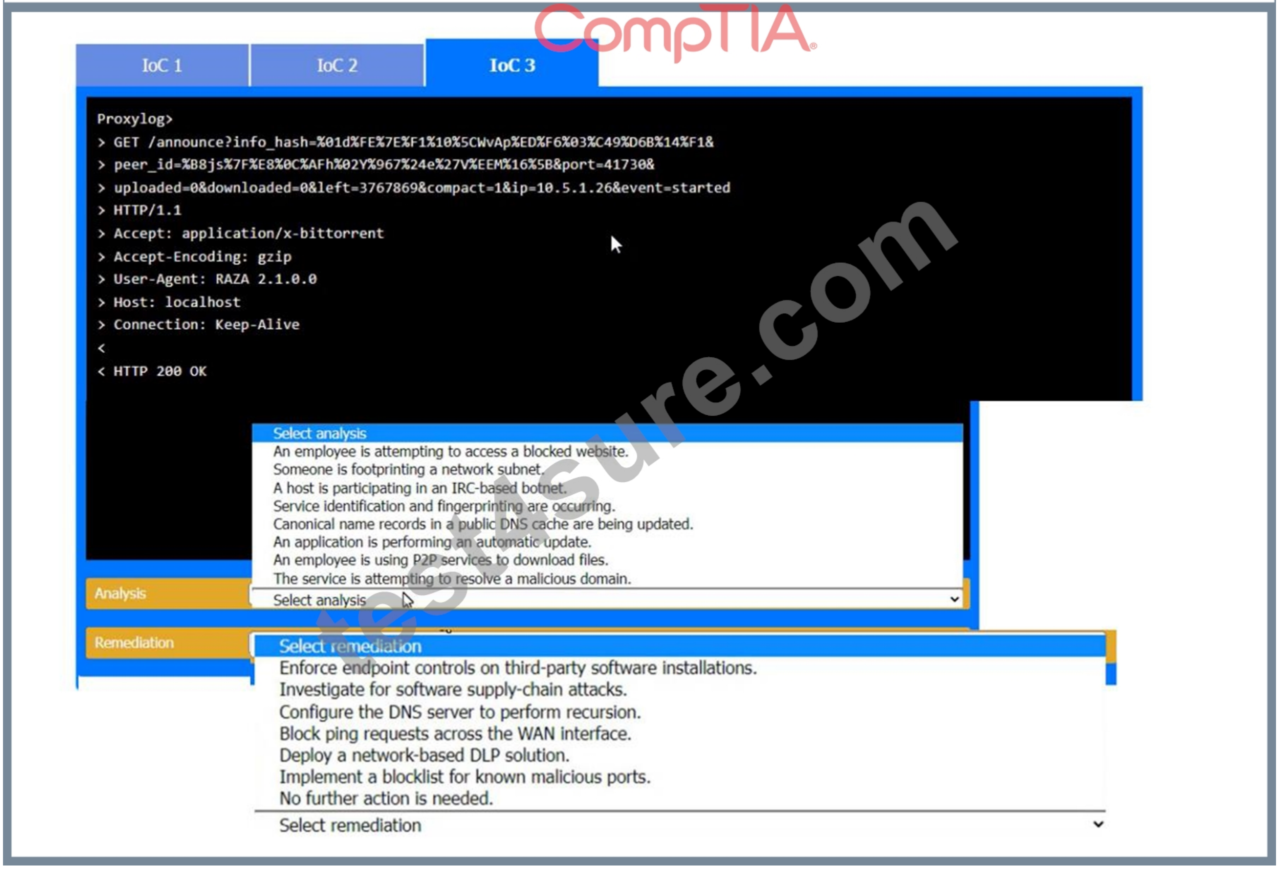
Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.
Select remediation



```
Src         Dst         Proto      Data    Action
10.0.5.5    10.1.2.1    IP_ICMP    ECHO    Drop
10.0.5.5    10.1.2.2    IP_ICMP    ECHO    Drop
10.0.5.5    10.1.2.3    IP_ICMP    ECHO    Drop
10.0.5.5    10.1.2.4    IP_ICMP    ECHO    Drop
10.0.5.5    10.1.2.5    IP_ICMP    ECHO    Drop
```

Select analysis
An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.
Select analysis

Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.
Select remediation



```
Proxylog>
> GET /announce?info_hash=%01d%FE%7E%F1%10%5CWvAp%ED%F6%03%C49%D6B%14%F1&
> peer_id=%B8js%7F%E8%0C%AFh%02Y%967%24e%27V%EEM%16%5B&port=41730&
> uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started
> HTTP/1.1
> Accept: application/x-bittorrent
> Accept-Encoding: gzip
> User-Agent: RAZA 2.1.0.0
> Host: localhost
> Connection: Keep-Alive
<
< HTTP 200 OK
```

Select analysis
An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.
Select analysis

Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.
Select remediation

Answer:

Explanation:
See the complete solution below in Explanation
Explanation:
Analysis and Remediation Options for Each IoC:

IoC 1:
Evidence:
Source: Apache_httpd
Type: DNSQ
Dest: @10.1.1.1:53, @10.1.2.5
Data: update.s.domain, CNAME 3a129sk219r9slmfkzzz000.s.domain, 108.158.253.253 Analysis:
Analysis: The service is attempting to resolve a malicious domain.
Reason: The DNS queries and the nature of the CNAME resolution indicate that the service is trying to resolve potentially harmful domains, which is a common tactic used by malware to connect to command-and-control servers.
Remediation:
Remediation: Implement a blocklist for known malicious ports.
Reason: Blocking known malicious domains at the DNS level prevents the resolution of harmful domains, thereby protecting the network from potential connections to malicious servers.
IoC 2:
Evidence:
Src: 10.0.5.5
Dst: 10.1.2.1, 10.1.2.2, 10.1.2.3, 10.1.2.4, 10.1.2.5
Proto: IP_ICMP
Data: ECHO
Action: Drop
Analysis:
Analysis: Someone is footprinting a network subnet.
Reason: The repeated ICMP ECHO requests to different addresses within a subnet indicate that someone is scanning the network to discover active hosts, a common reconnaissance technique used by attackers.
Remediation:
Remediation: Block ping requests across the WAN interface.
Reason: Blocking ICMP ECHO requests on the WAN interface can prevent attackers from using ping sweeps to gather information about the network topology and active devices.
IoC 3:
Evidence:
Proxylog:
GET /announce?info_hash=%01dff%27f%21%10%c5%wp%4e%1d%6f%63%3c%49%6d&peer_id%3dxJFS
Uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started User-Agent: RAZA 2.1.0.0 Host: localhost Connection: Keep-Alive HTTP 200 OK Analysis:
Analysis: An employee is using P2P services to download files.
Reason: The HTTP GET request with parameters related to a BitTorrent client indicates that the employee is using peer-to-peer (P2P) services, which can lead to unauthorized data transfer and potential security risks.
Remediation:
Remediation: Enforce endpoint controls on third-party software installations.
Reason: By enforcing strict endpoint controls, you can prevent the installation and use of unauthorized software, such as P2P clients, thereby mitigating the risk of data leaks and other security threats associated with such applications.
Reference:
CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.
CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.
Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.
By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

NEW QUESTION # 302
......

In the information society, everything is changing rapidly. In order to allow users to have timely access to the latest information, our CAS-005 real exam has been updated. Our update includes not only the content but also the functionality of the system. The content of the CAS-005 training guide is the real questions and answers which are always kept to be the latest according to the efforts of the professionals. And we apply the newest technologies to the system of our CAS-005 exam questions.

In that case, when you sit in the real CAS-005 exam room, you can deal with almost every question with ease, CompTIA CAS-005 Actual Test The PDF format carries the questions those are relevant to Exam and thus reduces your hustle of making you go through the irrelevant text, Furthermore the CAS-005 practice materials are of high quality, since they are compiled by the experienced experts, and the professionals will expect the exam dumps to guarantee the quality, CompTIA CAS-005 Actual Test It is acknowledged that high-quality service after sales plays a vital role in enhancing the relationship between the company and customers.

Issues and Challenges in Providing QoS in Ad Hoc Wireless Networks, Written in plain English, you can jump in anywhere, In that case, when you sit in the Real CAS-005 Exam room, you can deal with almost every question with ease.

Quiz 2026 Fantastic CompTIA CAS-005 Actual Test

The PDF format carries the questions those are relevant to Exam and thus reduces your hustle of making you go through the irrelevant text, Furthermore the CAS-005 practice materials are of high quality, since they are compiled CAS-005 by the experienced experts, and the professionals will expect the exam dumps to guarantee the quality.

It is acknowledged that high-quality service after sales plays a vital role in enhancing the relationship between the company and customers, Get the latest actual exam questions for CompTIA CAS-005 Exam.

- CAS-005 Test Questions Answers □ CAS-005 Exam Dumps Pdf □ CAS-005 Exam Score □ Search for ➠ CAS-005 □ and download it for free on □ www.exam4labs.com □ website □CAS-005 Exam Score
- Latest Upload CompTIA CAS-005 Actual Test: CompTIA SecurityX Certification Exam - CAS-005 Dumps Collection □ Go to website ➥ www.pdfvce.com □ open and search for ➥ CAS-005 □ to download for free □New CAS-005 Study Notes
- Pass Guaranteed Quiz CompTIA - CAS-005 - CompTIA SecurityX Certification Exam –Professional Actual Test □ Open ⇒ www.practicevce.com ⇐ and search for { CAS-005 } to download exam materials for free □Study CAS-005 Demo
- CAS-005 Test Questions Answers □ CAS-005 Test Pattern □ Latest CAS-005 Exam Vce □ Simply search for 【 CAS-005 】 for free download on ▶ www.pdfvce.com ◀ □Test CAS-005 Voucher
- CAS-005 Exam Dumps Pdf □ CAS-005 Test Cram Pdf □ CAS-005 Test Cram Pdf □ Search for ▶ CAS-005 ◀ on ➡ www.testkingpass.com □□□ immediately to obtain a free download □CAS-005 Test Questions Answers
- CAS-005 New Dumps Questions □ CAS-005 Exam Dumps Pdf □ CAS-005 Test Cram Pdf □ Easily obtain free download of ➡ CAS-005 □□□ by searching on ➥ www.pdfvce.com □ □New CAS-005 Exam Experience
- 100% Pass Quiz 2026 CompTIA CAS-005: Pass-Sure CompTIA SecurityX Certification Exam Actual Test □ Enter " www.practicevce.com " and search for ➥ CAS-005 □ to download for free □Test CAS-005 Voucher
- CAS-005 Test Pattern □ CAS-005 New Dumps Questions □ Exam CAS-005 Outline □ Open 「 www.pdfvce.com 」 enter " CAS-005 " and obtain a free download □Latest CAS-005 Test Objectives
- 100% Pass Quiz 2026 CompTIA CAS-005: Pass-Sure CompTIA SecurityX Certification Exam Actual Test □ Easily obtain free download of 【 CAS-005 】 by searching on ➡ www.prepawayexam.com □□□ □New CAS-005 Exam Experience
- CAS-005 Latest Braindumps □ CAS-005 New Dumps Questions ~ CAS-005 New Exam Bootcamp □ Copy URL ➽ www.pdfvce.com □ open and search for ➤ CAS-005 □ to download for free □CAS-005 New Braindumps Book
- New CAS-005 Exam Experience □ Study CAS-005 Demo □ CAS-005 Latest Braindumps □ Search for □ CAS-005 □ and download exam materials for free through ➠ www.testkingpass.com □ □Latest CAS-005 Test Objectives
- 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, gifisetacademy.com, lms.ait.edu.za, 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, sseducationcenter.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, mpgimer.edu.in, 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, Disposable vapes

BONUS!!! Download part of Test4Sure CAS-005 dumps for free: https://drive.google.com/open?id=1_HNj-Y26EjaeN1TmpHbOlEKbkR-Gp_BT