Bestselling On-The-Job CAS-005 Reference Exam Questions

BTW, DOWNLOAD part of TrainingDump CAS-005 dumps from Cloud Storage: https://drive.google.com/open?id=19iOpEOMVZiRLq4wspxOxDBJt_zLF9XEd

Nowadays in this information-based world the definition of the talents mean that the personnel boost both the knowledge in CAS-005 area and the practical abilities now. So if you want to be the talent the society actually needs you must apply your knowledge into the practical working and passing the test CAS-005 Certification can make you become the talent the society needs. If you buy our CAS-005 study materials you will pass the exam successfully and realize your goal to be the talent.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering.
Topic 2	• Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security.
Topic 3	• Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems.
Topic 4	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.

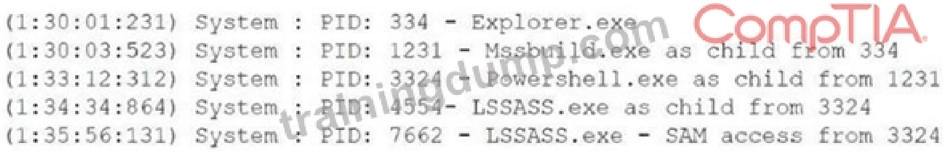
>> New CAS-005 Test Pattern <<

Pass Guaranteed Quiz 2025 Updated CompTIA CAS-005: New CompTIA SecurityX Certification Exam Test Pattern

As a market leader, our company is able to attract quality staffs, it actively seeks out those who are energetic, persistent, and professional to various CAS-005 certificate and good communicator. And we strongly believe that the key of our company's success is its people, skills, knowledge and experience. Over 50% of the account executives and directors have been with the Group for more than ten years. The successful selection, development and CAS-005 training of personnel are critical to our company's ability to provide a high pass rate of CAS-005 exam questions for you to pass the CAS-005 exam.

CompTIA SecurityX Certification Exam Sample Questions (Q212-Q217):

NEW QUESTION # 212
A security engineer is reviewing the SIEM logs after a server crashed. The following list of events represents the timeline of actions collected from the SIEM:



```
(1:30:01:231) System : PID: 334 - Explorer.exe
(1:30:03:523) System : PID: 1231 - Mssbuild.exe as child from 334
(1:33:12:312) System : PID: 3324 - Powershell.exe as child from 1231
(1:34:34:864) System : PID: 4554- LSSASS.exe as child from 3324
(1:35:56:131) System : PID: 7662 - LSSASS.exe - SAM access from 3324
```

Which of the following TTPs is most likely associated with this SIEM log?

- A. Credential dumping
- B. LOLBins use
- C. Data exfiltration
- D. Lateral movement

Answer: A

NEW QUESTION # 213
A company recentlyexperienced aransomware attack. Although the company performssystems and data backupon a schedule that aligns with itsRPO (Recovery Point Objective) requirements, thebackup administratorcould not recovercritical systems and datafrom its offline backups to meet the RPO. Eventually, the systems and data were restored with information that wassix months outside of RPO requirements.
Which of the following actions should the company take to reduce the risk of a similar attack?

- A. Implement a business continuity process that includes reverting manual business processes.
- B. Perform regular disaster recovery testing of IT and non-IT systems and processes.
- C. Encrypt and label the backup tapes with the appropriate retention schedule before they are sent to the off-site location.
- D. Carry out a tabletop exercise to update and verify the RACI matrix with IT and critical business functions.

Answer: B

Explanation:
Comprehensive and Detailed Explanation:
* Understanding the Ransomware Issue:
* The key issue here is thatbackups were not recoverable within the required RPO timeframe.
* This means the organizationdid not properly testitsbackup and disaster recovery (DR) processes.
* To prevent this from happening again, regular disaster recovery testing is essential.
* Why Option C is Correct:
* Disaster recovery testing ensures that backups are functionaland can meetbusiness continuity needs.
* Frequent DR testingallows organizations to identify and fixgaps in recovery strategies.
* Regular testing ensuresthat recoverymeets the RPO & RTO (Recovery Time Objective) requirements.
* Why Other Options Are Incorrect:
* A (Encrypt & label backup tapes):While encryption is important, it does not address thefailure to meet RPO requirements.
* B (Reverting to manual business processes):While amanual continuity planis good for resilience, it doesnot resolve the backup and recovery failure.
* D (Tabletop exercise & RACI matrix):Atabletop exerciseis a planning activity, butit does not involve actual recovery testing.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide:Disaster Recovery & Business Continuity Planning NIST SP 800-34:Contingency Planning Guide for Information Systems ISO 22301:Business Continuity Management Standards

NEW QUESTION # 214
A company recently experienced an incident in which an advanced threat actor was able to shim malicious code against the hardware static of a domain controller The forensic team cryptographically validated that com the underlying firmware of the box and

the operating system had not been compromised. However, the attacker was able to exfiltrate information from the server using a steganographic technique within LOAP.
Which of the following is me best way to reduce the risk oi reoccurrence?

- A. Enforcing allow lists for authorized network pons and protocols
- B. Measuring and attesting to the entire boot chum
- C. Using code signing to verify the source of OS updates
- D. Rolling the cryptographic keys used for hardware security modules

Answer: A

Explanation:
The scenario describes a sophisticated attack where the threat actor used steganography within LDAP to exfiltrate data. Given that the hardware and OS firmware were validated and found uncompromised, the attack vector likely exploited a network communication channel. To mitigate such risks, enforcing allow lists for authorized network ports and protocols is the most effective strategy.
Here's why this option is optimal:
Port and Protocol Restrictions: By creating an allow list, the organization can restrict communications to only those ports and protocols that are necessary for legitimate business operations. This reduces the attack surface by preventing unauthorized or unusual traffic.
Network Segmentation: Enforcing such rules helps in segmenting the network and ensuring that only approved communications occur, which is critical in preventing data exfiltration methods like steganography.
Preventing Unauthorized Access: Allow lists ensure that only predefined, trusted connections are allowed, blocking potential paths that attackers could use to infiltrate or exfiltrate data.
Other options, while beneficial in different contexts, are not directly addressing the network communication threat:
B: Measuring and attesting to the entire boot chain: While this improves system integrity, it doesn't directly mitigate the risk of data exfiltration through network channels.
C: Rolling the cryptographic keys used for hardware security modules: This is useful for securing data and communications but doesn't directly address the specific method of exfiltration described.
D: Using code signing to verify the source of OS updates: Ensures updates are from legitimate sources, but it doesn't mitigate the risk of network-based data exfiltration.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy" CIS Controls Version 8, Control 9: Limitation and Control of Network Ports, Protocols, and Services

NEW QUESTION # 215
Company A and Company D ate merging Company A's compliance reports indicate branch protections are not in place A security analyst needs to ensure that potential threats to the software development life cycle are addressed. Which of the following should me analyst cons<der when completing this basic?

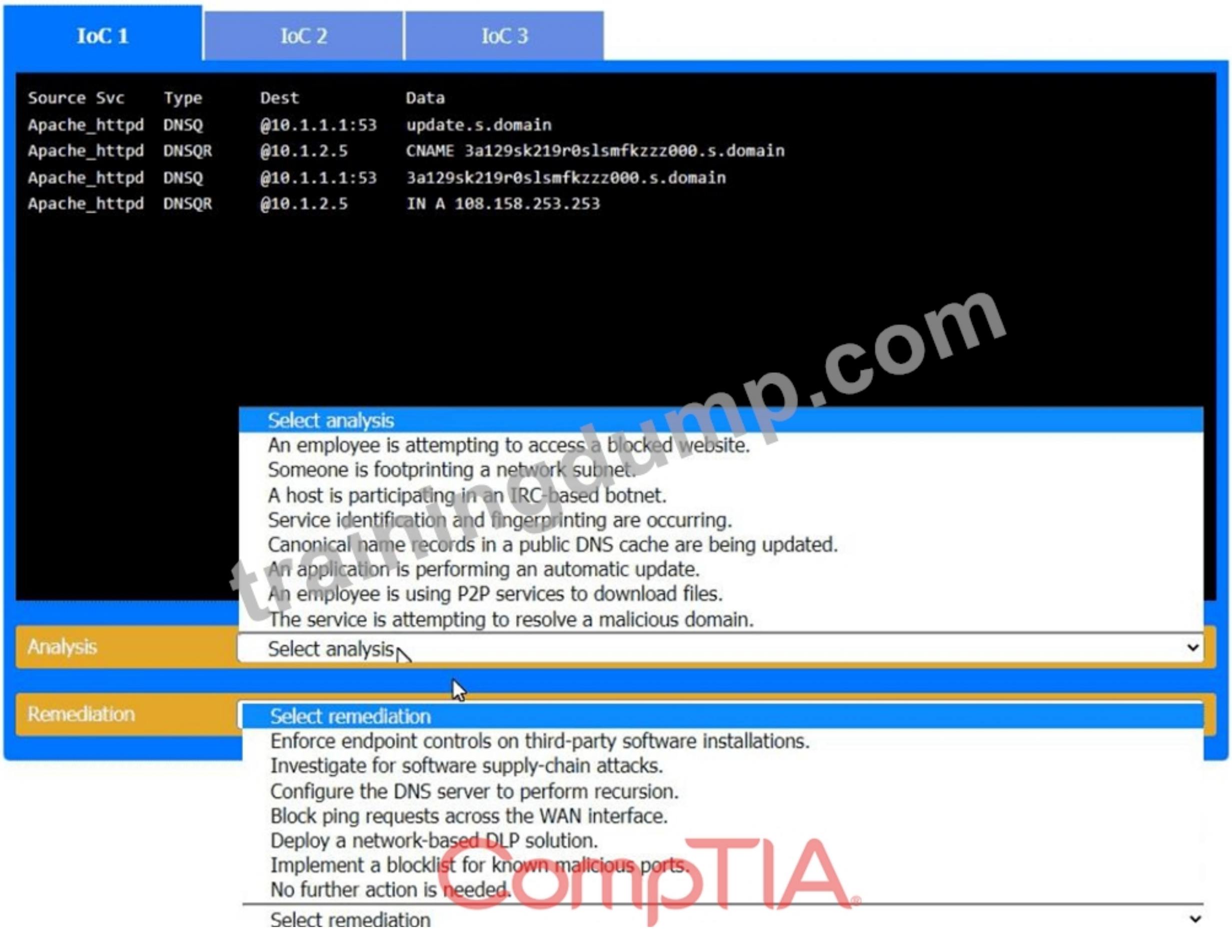
- A. If role-based training is deployed
- B. If DAST code is being stored to a single code repository
- C. If developers are unable to promote to production
- D. If DAST scans are routinely scheduled

Answer: D

Explanation:
Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process.
Why Routine DAST Scans?
Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.
Compliance: Routine scans ensure that the development process complies with security standards and regulations.
Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.
Integration into SDLC: Ensures security is embedded within the development process, promoting a security- first approach.
Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:

A: If developers are unable to promote to production: This is more of an operational issue than a security assessment.
B: If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.
D: If role-based training is deployed: While important, training alone does not ensure continuous security assessment.

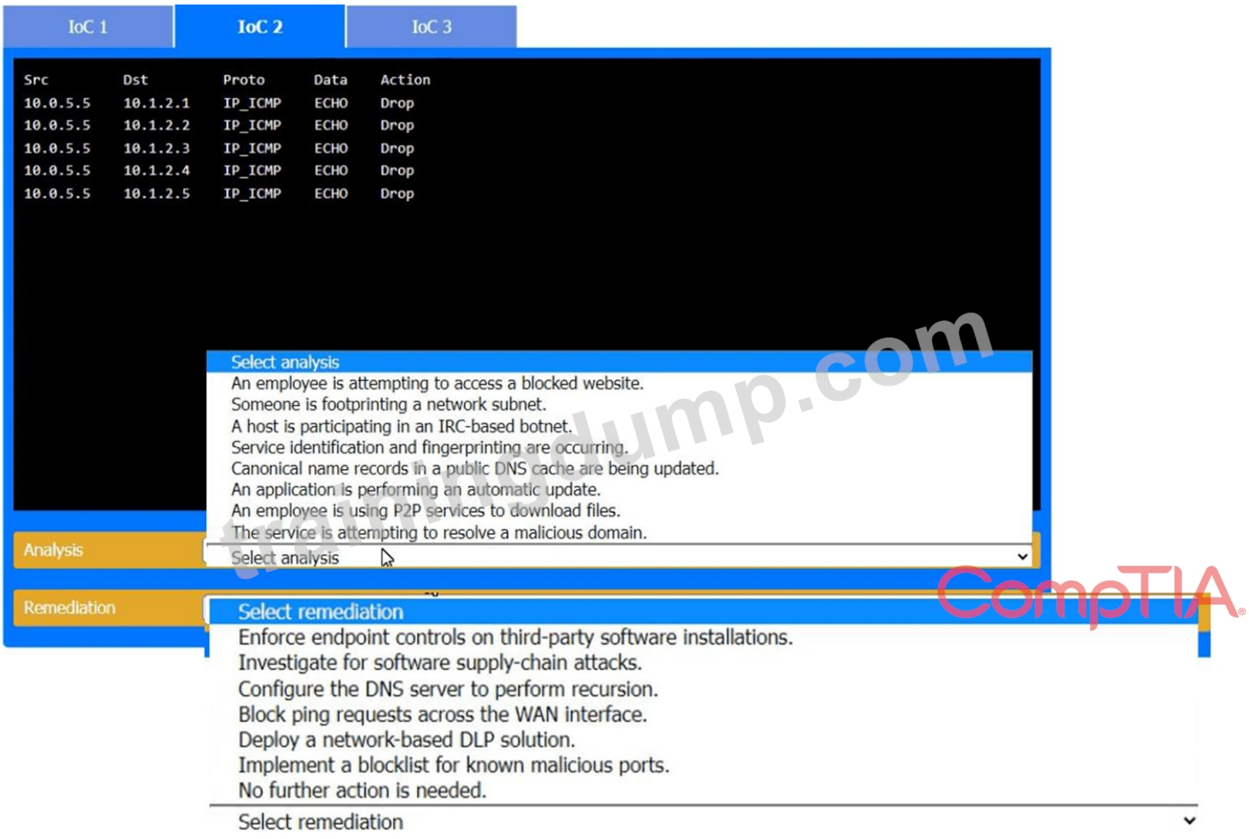
NEW QUESTION # 216
SIMULATION
[Security Architecture]
During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.
INSTRUCTIONS
Review each of the events and select the appropriate analysis and remediation options for each IoC.



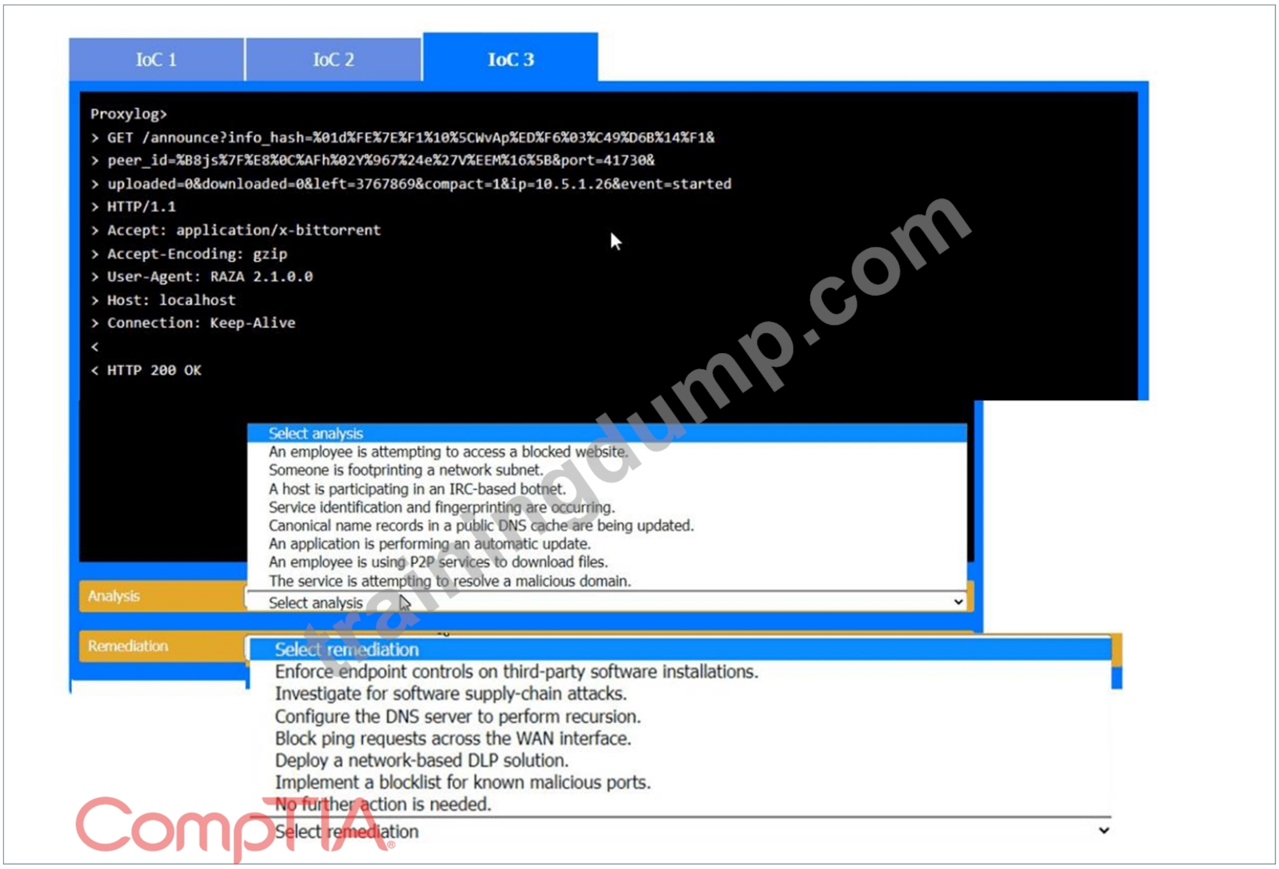
```
Source Svc    Type     Dest          Data
Apache_httpd  DNSQ     @10.1.1.1:53  update.s.domain
Apache_httpd  DNSQR    @10.1.2.5     CNAME 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd  DNSQ     @10.1.1.1:53  3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd  DNSQR    @10.1.2.5     IN A 108.158.253.253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

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


IoC 1
IoC 2
IoC 3
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.
Analysis
Select analysis
Remediation
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
```


IoC 1
IoC 2
IoC 3
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.
Analysis
Select analysis
Remediation
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
```

Answer:

Explanation:
See the 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 HTTP200 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 # 217

......

- Answers CAS-005 Real Questions □ CAS-005 Valid Dumps Ppt □ Actual CAS-005 Test □ Open website { www.prep4sures.top } and search for “ CAS-005 ” for free download □CAS-005 Valid Test Sample
- Updated CAS-005 CBT □ CAS-005 Latest Study Materials ☢ Test CAS-005 Free □ Open ▹ www.pdfvce.com ◃ enter ✔ CAS-005 □✔□ and obtain a free download ☣New CAS-005 Exam Questions
- CompTIA CAS-005 Questions - Shortcut To Success 2025 □ Search for ➽ CAS-005 □ and download it for free on ☀ www.passtestking.com □☀□ website □New CAS-005 Test Duration
- CompTIA CAS-005 Exam Questions - Proven Way Of Quick Preparation □ The page for free download of ➥ CAS-005 □ on □ www.pdfvce.com □ will open immediately □CAS-005 Test Discount Voucher
- CAS-005 New Braindumps Book □ Answers CAS-005 Real Questions □ New CAS-005 Dumps Free □ Search on “ www.vceengine.com ” for ☀ CAS-005 □☀□ to obtain exam materials for free download □Test CAS-005 Free
- 100% Pass Quiz 2025 CompTIA CAS-005: CompTIA SecurityX Certification Exam – Reliable New Test Pattern □ Search for ➡ CAS-005 □□□ and download it for free immediately on ➡ www.pdfvce.com □□□ □CAS-005 Valid Test Sample
- New New CAS-005 Test Pattern 100% Pass | High-quality Test CAS-005 Voucher: CompTIA SecurityX Certification Exam □ Search for ➠ CAS-005 □ and download it for free on 「 www.pdfdumps.com 」 website □Reliable CAS-005 Dumps Book
- CAS-005 Valid Dumps Ppt □ CAS-005 Test Discount Voucher □ Reliable CAS-005 Dumps Book □ Open ➠ www.pdfvce.com □ and search for 「 CAS-005 」 to download exam materials for free □CAS-005 Latest Exam Practice
- CompTIA CAS-005 Exam Questions - Proven Way Of Quick Preparation □ Open ☀ www.exams4collection.com □☀□ enter “ CAS-005 ” and obtain a free download □□CAS-005 Valid Test Sample
- Actual CAS-005 Test □ New CAS-005 Test Duration □ New CAS-005 Exam Questions □ Search for （ CAS-005 ） on 「 www.pdfvce.com 」 immediately to obtain a free download □CAS-005 Latest Study Materials
- CAS-005 Valid Test Syllabus □ New CAS-005 Dumps Free □ CAS-005 Valid Dumps Ppt □ □ www.pass4test.com □ is best website to obtain 「 CAS-005 」 for free download □Updated CAS-005 CBT
- goldmanpennentertainment.com, korodhsoaqoon.com, 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, study.stcs.edu.np, www.fuxinwang.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that TrainingDump CAS-005 dumps now are free: https://drive.google.com/open?id=19iOpEOMVZiRLq4wspxOxDBJt_zLF9XEd