

SY0-701 Boot Camp, Brain SY0-701 Exam



2025 Latest ActualPDF SY0-701 PDF Dumps and SY0-701 Exam Engine Free Share: https://drive.google.com/open?id=1g-WrI039iPtWmOkbgn3_NYpICA8WlFph

Someone always asks: Why do we need so many certifications? One thing has to admit, more and more certifications you own, it may bring you more opportunities to obtain better job, earn more salary. This is the reason that we need to recognize the importance of getting the test SY0-701 certifications. More qualified certification for our future employment has the effect to be reckoned with, only to have enough qualification certifications to prove their ability, can we win over rivals in the social competition. Therefore, the SY0-701 Guide Torrent can help users pass the qualifying examinations that they are required to participate in faster and more efficiently.

After you have used our SY0-701 learning prep, you will make a more informed judgment. We strongly believe that our SY0-701 practice quiz will conquer you. After that, you can choose the version you like. We also provide you with three trial versions of our SY0-701 Exam Questions. You can choose one or more versions according to your situation, and everything depends on your own preferences. And you will definitely love our SY0-701 training materials.

>> SY0-701 Boot Camp <<

Pass Guaranteed SY0-701 - The Best CompTIA Security+ Certification Exam Boot Camp

High efficiency service has won reputation for us among multitude of customers, so choosing our SY0-701 real study dumps we guarantee that you won't be regret of your decision. Helping our candidates to pass the SY0-701 exam and achieve their dream has always been our common ideal. We believe that your satisfactory on our SY0-701 Exam Questions is the drive force for our company. Meanwhile, we adopt a reasonable price for you, ensures people whoever is rich or poor would have the equal access to buy our useful SY0-701 real study dumps.

CompTIA Security+ Certification Exam Sample Questions (Q464-Q469):

NEW QUESTION # 464

Which of the following architectures is most suitable to provide redundancy for critical business processes?

- A. Multitenant
- **B. Cloud-native**
- C. Network-enabled
- D. Server-side

Answer: B

NEW QUESTION # 465

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure.

Which of the following data classifications should be used to secure patient data?

- A. Sensitive
- B. Critical
- C. Public
- D. Private

Answer: A

Explanation:

Explanation

Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical.

Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.

Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised.

Examples of private data include employee records, financial reports, and internal policies.

Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.

Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.

Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards.

Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

NEW QUESTION # 466

A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

- A. An in-depth penetration test of all suppliers and vendors
- B. A legally enforceable corporate acquisition policy
- C. A thorough analysis of the supply chain
- D. A right to audit clause in vendor contracts and SOWs

Answer: C

Explanation:

Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM). It can pose serious risks to network quality, performance, safety, and reliability¹². Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it³. To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain, which is the network of entities involved in the production, distribution, and delivery of the hardware. By analyzing the supply chain, the company can verify the origin, authenticity, and integrity of the hardware, and identify any potential sources of counterfeit or tampered products. A thorough analysis of the supply chain can include the following steps:

Establishing a trusted relationship with the OEM and authorized resellers
Requesting documentation and certification of the hardware from the OEM or authorized resellers
Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components
Testing the hardware for functionality, performance, and security
Implementing a tracking system to monitor the hardware throughout its lifecycle
Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agencies

Reference = 1: Identify Counterfeit and Pirated Products - Cisco, 2: What Is Hardware Security? Definition, Threats, and Best Practices, 3: Beware of Counterfeit Network Equipment - TechNewsWorld, : Counterfeit Hardware: The Threat and How to Avoid It

NEW QUESTION # 467

A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

- A. A keylogger is installed on [smith's workstation
- B. Ransomware has been deployed in the domain.
- C. The user jsmith's account has been locked out.
- **D. An attacker is attempting to brute force ismith's account.**

Answer: D

Explanation:

Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tool or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes - SY0-601 CompTIA Security+ : 1.1

NEW QUESTION # 468

During a recent log review, an analyst discovers evidence of successful injection attacks. Which of the following will best address this issue?

- A. Authentication
- B. Static code analysis
- **C. Input validation**
- D. Secure cookies

Answer: C

Explanation:

Input validation is the primary defense against injection attacks, such as SQL injection or command injection. It ensures that user-supplied data is properly sanitized before processing, preventing attackers from injecting malicious code.

Authentication (A) helps verify user identity but does not prevent injection attacks.

Secure cookies (B) improve session security but do not address injection vulnerabilities.

Static code analysis (C) helps identify vulnerabilities in source code but does not actively prevent attacks in real-time.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain.

NEW QUESTION # 469

.....

You can use SY0-701 guide materials through a variety of electronic devices. At home, you can use the computer and outside you can also use the phone. Now that more people are using mobile phones to learn our SY0-701 study guide, you can also choose the one you like. We have three versions of our SY0-701 Exam Braindumps: the PDF, the Software and the APP online. And you can free download the demo s to check it out.

Brain SY0-701 Exam: https://www.actualpdf.com/SY0-701_exam-dumps.html

The objective of SY0-701 is to assist candidates in preparing for the CompTIA Security+ Certification Exam (SY0-701) certification test by equipping them with the actual CompTIA SY0-701 questions PDF and SY0-701 practice exams to attempt the prepare for your SY0-701 exam successfully, CompTIA SY0-701 Boot Camp We have a good command to the examination questions, so you can trust us, In addition, this SY0-701 prep material comes with up to 365 days of free CompTIA Dumps updates and a free demo.

The objective of SY0-701 is to assist candidates in preparing for the CompTIA Security+ Certification Exam (SY0-701) certification test by equipping them with the actual CompTIA SY0-701 questions PDF and SY0-701 practice exams to attempt the prepare for your SY0-701 exam successfully.

2025 Latest ActualPDF SY0-701 PDF Dumps and SY0-701 Exam Engine Free Share: https://drive.google.com/open?id=1g-WrI039iPtWmOkbgm3_NYpICA8WlFph