

SY0-701유효한덤프자료 - SY0-701인증덤프샘플다운



참고: ExamPassdump에서 Google Drive로 공유하는 무료, 최신 SY0-701 시험 문제집이 있습니다:
<https://drive.google.com/open?id=1rPq7eYtyYXbapmNkvjsyDSPYMSYxNrgN>

ExamPassdump의 CompTIA SY0-701덤프로 CompTIA SY0-701시험준비를 하면 시험패스는 간단한 일이라는걸 알게 될것입니다. CompTIA SY0-701덤프는 최근CompTIA SY0-701시험의 기출문제모음으로 되어있기에 적응율이 높습니다.시험에서 떨어지면 덤프비용 전액 환불해드리기에 우려없이 덤프를 주문하셔도 됩니다.

ExamPassdump의 CompTIA SY0-701덤프는 IT업계에 오랜 시간동안 종사한 전문가들의 끊임없는 노력과 지금까지의 노하우로 만들어낸CompTIA SY0-701시험대비 알맞춤 자료입니다. ExamPassdump의 CompTIA SY0-701덤프만 공부하시면 여러분은 충분히 안전하게 CompTIA SY0-701시험을 패스하실 수 있습니다. ExamPassdump CompTIA SY0-701덤프의 도움으로 여러분은 IT업계에서 또 한층 업그레이드 될것입니다

>> SY0-701유효한 덤프자료 <<

SY0-701유효한 덤프자료 100%시험패스 가능한 덤프

ExamPassdump는 CompTIA SY0-701인증시험을 아주 쉽게 패스할 수 있도록 도와드리는 사이트입니다. ExamPassdump의 엘리트한 전문가가 끈임 없는 노력으로 최고의CompTIA SY0-701자료를 만들었습니다. 이 자료로 여러분은 100%CompTIA의SY0-701인증시험을 패스할 수 있으며, ExamPassdump를 선택함으로 성공을 선택한 것입니다. ExamPassdump가 제공하는 시험가이드로 효과적인 학습으로 많은 분들이 모두 인증시험을 패스하였습니다. 이건 모두 ExamPassdump 인증시험덤프로 공부하였기 때문입니다. 그 중CompTIA SY0-701인증시험을 패스한 분들도 모두 ExamPassdump인증시험덤프를 사용하였기 때문입니다.

최신 CompTIA Security+ SY0-701 무료샘플문제 (Q121-Q126):

질문 # 121

Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

- A. Manual audit
- B. Attestation

- C. Compliance checklist
- **D. Automation**

정답: D

설명:

Explanation

Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs.

Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise¹².

The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:

Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis³.

Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis⁴.

Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022; Automation and Scripting - CompTIA Security+ SY0-701 - 5.1, video by Professor Messer³; CompTIA Security+ SY0-701 Certification Study Guide, page 974; CompTIA Security+ SY0-701 Certification Study Guide, page 98. :

CompTIA Security+ SY0-701 Certification Study Guide, page 99.

질문 # 122

A company is in the process of cutting jobs to manage costs. The Chief Information Security Officer is concerned about the increased risk of an insider threat. Which of the following would most likely help the security awareness team address this potential threat?

- A. Raise awareness for business leaders on social engineering techniques.
- B. Configure DLP to monitor staff who will be terminated.
- C. Immediately disable the accounts of staff who are likely to be terminated.
- **D. Train supervisors to identify and manage disgruntled employees.**

정답: D

설명:

When layoffs occur, disgruntled employees pose a significant insider threat risk. Training supervisors to identify signs of disgruntlement and manage employees empathetically helps reduce insider threat risks by addressing issues before they escalate. Supervisors act as the first line of defense in recognizing behavioral changes and intervening.

Immediately disabling accounts (A) may cause operational issues if done prematurely; monitoring with DLP (C) is reactive and less proactive than awareness; raising awareness about social engineering (D) targets external threats more than insider risks.

This approach is part of insider threat awareness and workforce management in Security Program Management#6:Chapter 16 CompTIA Security+ Study Guide#.

질문 # 123

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

- A. To discover which systems have been affected
- B. To eradicate any trace of malware on the network
- **C. To prevent future incidents of the same nature**
- D. To gather IoCs for the investigation

정답: C

설명:

Root cause analysis is a process of identifying and resolving the underlying factors that led to an incident. By conducting root cause analysis as part of incident response, security professionals can learn from the incident and implement corrective actions to prevent future incidents of the same nature. For example, if the root cause of a data breach was a weak password policy, the security team can enforce a stronger password policy and educate users on the importance of password security. Root cause analysis can also help to improve security processes, policies, and procedures, and to enhance security awareness and culture within the organization. Root cause analysis is not meant to gather IoCs (indicators of compromise) for the investigation, as this is a task performed during the identification and analysis phases of incident response. Root cause analysis is also not meant to discover which systems have been affected or to eradicate any trace of malware on the network, as these are tasks performed during the containment and eradication phases of incident response. References = CompTIA Security+ SY0-701 Certification Study Guide, page 424-425; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.1 - Incident Response, 9:55 - 11:18.

질문 # 124

A company is implementing a policy to allow employees to use their personal equipment for work. However, the company wants to ensure that only company-approved applications can be installed. Which of the following addresses this concern?

- A. DLP
- B. FIM
- C. Containerization
- **D. MDM**

정답: D

질문 # 125

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile.

Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

- **A. Password complexity**
- **B. Federation**
- C. Default password changes
- D. Open authentication
- E. Password manager
- F. Identity proofing

정답: A,B

설명:

Explanation

Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them.

Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-313 1

질문 # 126

.....

여러분이 다른 사이트에서도 CompTIA 인증 SY0-701 시험 관련 덤프 자료를 보셨을 것입니다 하지만 우리

참고: ExamPassdump에서 Google Drive로 공유하는 무료 2025 CompTIA SY0-701 시험 문제집이 있습니다:
<https://drive.google.com/open?id=1rPq7eYtYXbapmNkvjsyDSPYMSYxNrgN>