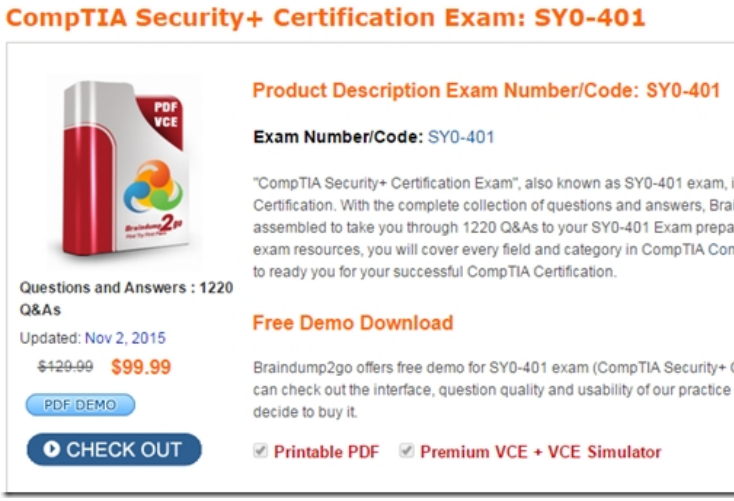
[OFFICIALBraindump2go SY0-401 PDF Instant Download (141-150)

COMPTIA NEWS: SY0-401 Exam Questions has been Updated Today! Get Latest SY0-401 VCE and SY0-401 PDF Instantly! Welcome to Download the Newest Braindump2go SY0-401 VCE&SY0-401 PDF Dumps:
http://www.braindump2go.com/sy0-401.html (1220 Q&As) 2015 CompTIA SY0-401 Certification Exam is coming! Getting a Laest SY0-401 Practice Test is very important for an Exam Candiate! Braindump2go New Updated SY0-401 Exam Questions Well Formatted in PDF and VCE versions, providing you convenience and excellence both at the same time! Free Questions and Answer are provided Following: Exam Code: SY0-401Exam Name: CompTIA Security+Certification Provider: CompTIACorresponding Certification: CompTIA Security+SY0-401 Dump,SY0-401 PDF,SY0-401 VCE,SY0-401 Braindump,SY0-401 Study Guide,SY0-401 Study Guide PDF,SY0-401 Objectives,SY0-401 Practice Test,SY0-401 Practice Exam,SY0-401 Performance Based Questions,SY0-401 Exam Questions,SY0-401 Exam Dumps,SY0-401 Exam PDF,SY0-401 Dumps Free,SY0-401 Dumps PDF

QUESTION 141Which of the following is the BEST approach to perform risk mitigation of user access control rights? A. Conduct surveys and rank the results.B. Perform routine user permission reviews.C. Implement periodic vulnerability scanning. D. Disable user accounts that have not been used within the last two weeks. Answer: BExplanation:Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on. User permissions may be the most basic aspect of security and is best coupled with a principle of least privilege. And related to permissions is the concept of the access control list (ACL). An ACL is literally a list of who can access what resource and at what level. Thus the best risk mitigation steps insofar as access control rights are concerned, is the regular/routine review of user permissions. QUESTION 142An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this? A. User rights reviewsB. Least privilege and job rotationC. Change managementD. Change Control Answer: AExplanation:A privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of an organization. This means that a user rights review will reveal whether user accounts have been assigned according to their `new' job descriptions , or if there are privilege creep culprits after transfers has occurred. QUESTION 143A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews? A. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.C. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources. Answer: AExplanation:Reviewing user permissions and group memberships form part of a privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation. QUESTION 144Various network outages have occurred recently due to unapproved changes to network and security devices. All changes were made using various system credentials. The security analyst has been tasked to update the security policy. Which of the following risk mitigation strategies would also need to be implemented to reduce the number of network outages due to unauthorized changes? A. User rights and permissions reviewB. Configuration managementC. Incident managementD.

Implement security controls on Layer 3 devices Answer: AExplanation:Reviewing user rights and permissions can be used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation and their job descriptions. Also reviewing user rights and permissions will afford the security analyst the opportunity to put the principle of least privilege in practice as well as update the security policy QUESTION 145Which of the following assets is MOST likely considered for DLP? A. Application server contentB. USB mass storage devicesC. Reverse proxyD. Print server Answer: BExplanation:Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. A USB presents the most likely device to be used to steal data because of its physical size. QUESTION 146The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud? A. HPM technologyB. Full disk encryptionC. DLP policyD. TPM technology Answer: CExplanation:Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. The Software as a Service (SaaS) applications are remotely run over the Web and as such requires DLP monitoring. QUESTION 147Which of the following is a Data Loss Prevention (DLP) strategy and is MOST useful for securing data in use? A. Email scanningB. Content discoveryC. Database fingerprintingD. Endpoint protection Answer: DExplanation:Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. DLP systems share commonality with network intrusion prevention systems. Endpoint protection provides security and management over both physical and virtual environments. QUESTION 148A customer service department has a business need to send high volumes of confidential information to customers electronically. All emails go through a DLP scanner. Which of the following is the BEST solution to meet the business needs and protect confidential information? A. Automatically encrypt impacted outgoing emailsB. Automatically encrypt impacted incoming emailsC. Monitor impacted outgoing emailsD. Prevent impacted outgoing emails Answer: AExplanation: Encryption is done to protect confidentiality and integrity of data. It also provides authentication, nonrepudiation and access control to the data. Since all emails go through a DLP scanner and it is outgoing main that requires protection then the best option is to put a system in place that will encrypt the outgoing emails automatically. QUESTION 149Which of the following is a best practice when a mistake is made during a forensics examination? A. The examiner should verify the tools before, during, and after an examination.B. The examiner should attempt to hide the mistake during cross-examination.C. The examiner should document the mistake and workaround the problem.D. The examiner should disclose the mistake and assess another area of the disc. Answer: CExplanation:Every step in an incident response should be documented, including every action taken by end users and the incident-response team. QUESTION 150An incident response team member needs to perform a forensics examination but does not have the required hardware. Which of the following will allow the team member to perform the examination with minimal impact to the potential evidence? A. Using a software file recovery discB. Mounting the drive in read-only modeC. Imaging based on order of volatilityD. Hashing the image after capture Answer: BExplanation:Mounting the drive in read-only mode will prevent any executable commands from being executed. This is turn will have the least impact on potential evidence using the drive in question. 100% SY0-401 Complete Success & Money Back Guarantee!By utilizing Braindump2go high quality CompTIA SY0-401 Exam Dumps Products, You can surely pass SY0-401 certification 100%! Braindump2go also offers 100% money back guarantee to individuals in case they fail to pass CompTIA SY0-401 in one attempt.



FREE DOWNLOAD: NEW UPDATED SY0-401 PDF Dumps & SY0-401 VCE Dumps from Braindump2go:
http://www.braindump2go.com/sy0-401.html (1220 Q&A)