This page was exported from - Free Download Lead2pass VCE And PDF Dumps
Export date: Thu Mar 28 16:05:36 2024 / +0000 GMT

# [2017 New Lead2pass CompTIA SY0-401 VCE And PDF Instant Download (126-150)

2017 August CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Lead2pass SY0-401 latest updated braindumps including all new added SY0-401 exam questions from exam center which guarantees you can 100% success SY0-401 exam in your first try! Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 126Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years.Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years.Which of the following should Sara do to address the risk? A. Accept the risk saving $10,000.B. Ignore the risk saving $5,000.C. Mitigate the risk saving $10,000.D. Transfer the risk saving $5,000.Answer: DExplanation:Risk transference involves sharing some of the risk burden with someone else, such as an insurance company. The cost of the security breach over a period of 5 years would amount to$30,000 and it is better to save $5,000. QUESTION 127Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE). A. ConfidentialityB. AvailabilityC. IntegrityD. AuthorizationE. AuthenticationF. Continuity Answer: ABCExplanation:Confidentiality, integrity, and availability are the three most important concepts in security. Thus they form the security triangle. QUESTION 128Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns? A. Hardware integrityB. Data confidentialityC. Availability of serversD. Integrity of data Answer: BExplanation:Data that is not kept separate or segregated will impact on that data's confidentiality maybe being compromised. Be aware of the fact that your data is only as safe as the data with which it is integrated. For example, assume that your client database is hosted on a server that another company is also using to test an application that they are creating. If their application obtains root- level access at some point (such as to change passwords) and crashes at that point, then the user running the application could be left with root permissions and conceivably be to access data on the server for which they are not authorized, such as your client database. Data segregation is crucial; keep your data on secure servers. QUESTION 129Acme Corp has selectively outsourced proprietary business processes to ABC Services. Due to some technical issues, ABC services wants to send some of Acme Corp's debug data to a third party vendor for problem resolution. Which of the following MUST be considered prior to sending data to a third party? A. The data should be encrypted prior to transportB. This would not constitute unauthorized data sharingC. This may violate data ownership and non-disclosure agreementsD. Acme Corp should send the data to ABC Services' vendor instead Answer: CExplanation:With sending your data to a third party is already a risk since the third party may have a different policy than yours. Data ownership and non-disclosure is already a risk that you will have to accept since the data will be sent for debugging /troubleshooting purposes which will result in definite disclosure of the data. QUESTION 130An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame.Which of the following strategies would the administrator MOST likely implement? A. Full backups on the weekend and incremental during the weekB. Full backups on the weekend and full backups every dayC. Incremental backups on the weekend and differential backups every dayD. Differential backups on the weekend and full backups every day Answer: AExplanation:A full backup is a complete, comprehensive backup of all fi les on a disk or server. The full backup is current only at the time it's performed. Once a full backup is made, you have a complete archive of the system at that point in time. A system shouldn't be in use while it undergoes a full backup because some fi les may not get backed up. Once the system goes back into operation, the backup is no longer current. A full backup can be a time-consuming process on a large system. An incremental backup is a partial backup that stores only the information that has been changed since the last full or the last incremental backup. If a full backup were performed on a Sunday night, an incremental backup done on Monday night would contain only the information that changed since Sunday night. Such a backup is typically considerably smaller than a full backup. Each incremental backup must be retained until a full backup can be performed. Incremental backups are usually the fastest backups to perform on most systems, and each incremental backup tape is relatively small. QUESTION 131A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed? A. The request needs to be sent to the incident management team.B. The request needs to be approved through the incident management process.C. The request needs to be approved through the change management process.D. The request needs to be sent to the change management team. Answer: CExplanation:Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. Thus the actual switch configuration should first be subject to the change management approval. QUESTION 132Developers currently have access to update production servers without

going through an approval process. Which of the following strategies would BEST mitigate this risk? A. Incident managementB. Clean desk policyC. Routine auditsD. Change management Answer: DExplanation:Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. This structured approach involves policies that should be in place and technological controls that should be enforced. QUESTION 133Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems? A. Incident managementB. Server clusteringC. Change managementD. Forensic analysis Answer: CExplanation:Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case `performing updates to business critical systems. QUESTION 134The network administrator is responsible for promoting code to applications on a DMZ web server. Which of the following processes is being followed to ensure application integrity? A. Application hardeningB. Application firewall reviewC. Application change managementD. Application patch management Answer: CExplanation: Change management is the structured approach that is followed to secure a company's assets. Promoting code to application on a SMZ web server would be change management. QUESTION 135Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages? A. Risk transferenceB. Change managementC. Configuration managementD. Access control revalidation Answer: BExplanation:Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case `scheduled system patching'. QUESTION 136A security engineer is given new application extensions each month that need to be secured prior to implementation. They do not want the new extensions to invalidate or interfere with existing application security. Additionally, the engineer wants to ensure that the new requirements are approved by the appropriate personnel. Which of the following should be in place to meet these two goals? (Select TWO). A. Patch Audit PolicyB. Change Control PolicyC. Incident Management Policy D. Regression Testing PolicyE. Escalation PolicyF. Application Audit Policy Answer: BDExplanation:A backout (regression testing) is a reversion from a change that had negative consequences. It could be, for example, that everything was working fi ne until you installed a service pack on a production machine, and then services that were normally available were no longer accessible. The backout, in this instance, would revert the system to the state that it was in before the service pack was applied. Backout plans can include uninstalling service packs, hotfi xes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the backout. A change control policy refers to the structured approach that is followed to secure a company's assets in the event of changes occurring. QUESTION 137A user has received an email from an external source which asks for details on the company's new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT? A. Contact their manager and request guidance on how to best move forwardB. Contact the help desk and/or incident response team to determine next stepsC. Provide the requestor with the email information since it will be released soon anywayD. Reply back to the requestor to gain their contact information and call them Answer: BExplanation:This is an incident that has to be responded to by the person who discovered it- in this case the user. An incident is any attempt to violate a security policy, a successful penetration, a compromise of a system, or any unauthorized access to information. It's important that an incident response policy establish at least the following items:Outside agencies that should be contacted or notified in case of an incident Resources used to deal with an incidentProcedures to gather and secure evidenceList of information that should be collected about an incident Outside experts who can be used to address issues if needed Policies and guidelines regarding how to handle an incidentSince the spec sheet has been marked Internal Proprietary Information the user should refer the incident to the incident response team.Incorrect Answers:A: The manager may or may not be part of the incident response team.C: The information has been marked Internal Proprietary Information and providing the information to the requestor would be in violation to the company. D: You should have the incident response team handle the situation rather than addressing the issue yourself. QUESTION 138Which of the following is BEST carried out immediately after a security breach is discovered? A. Risk transferenceB. Access control revalidationC. Change managementD. Incident management Answer: DExplanation:Incident management is the steps followed when security incident occurs. QUESTION 139A security analyst informs the Chief Executive Officer (CEO) that a security breach has just occurred. This results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the CEO asks for further information. Which of the following strategies should be implemented to ensure the Risk Manager and CIO are not caught unaware in the future? A. Procedure and policy managementB. Chain of custody managementC. Change management D. Incident management Answer: DExplanation:incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets). The events that could occur include security breaches. QUESTION 140Requiring technicians to report spyware infections is a step in which of the following? A. Routine auditsB. Change managementC. Incident managementD. Clean desk policy Answer: CExplanation:Incident management refers

to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets). 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. Lead2pass regular updates of CompTIA SY0-401 dumps, with accurate answers, keeps the members one step ahead in the real SY0-401 exam. The experts with more than 10 years experience in Certification Field work with us. SY0-401 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzFZWExUbFM0YU0 2017 CompTIA **SY0-401** exam dumps (All 1868 Q&As) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]