[2017 New Exam Collection SY0-401 Dumps And SY0-401 New Questions (101-125)

2017 August CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!

We never believe in second chances and Lead2pass brings you the best SY0-401 Exam Questions which will make you pass in the first attempt. We guarantee all questions and answers in our SY0-401 Dumps are the latest released, we check all exam dumps questions from time to time according to CompTIA Official Center, in order to guarantee you can read the latest questions! Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 101Three of the primary security control types that can be implemented are. A. Supervisory, subordinate, and peer.B. Personal, procedural, and legal.C. Operational, technical, and management.D. Mandatory, discretionary, and permanent.Answer: CExplanation:The National Institute of Standards and Technology (NIST) places controls into various types. The control types fall into three categories: Management, Operational, and Technical. QUESTION 102 Which of the following technical controls is BEST used to define which applications a user can install and run on a company issued mobile device? A. AuthenticationB. BlacklistingC. WhitelistingD. Acceptable use policy Answer: CExplanation:White lists are closely related to ACLs and essentially, a white list is a list of items that are allowed. QUESTION 103To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation? A. ManagementB. AdministrativeC. TechnicalD. Operational Answer: CExplanation:controls such as preventing unauthorized access to PC's and applying screensavers that lock the PC after five minutes of inactivity is a technical control type, the same as Identification and Authentication, Access Control, Audit and Accountability as well as System and Communication Protection. QUESTION 104Which of the following is a management control? A. Logon bannersB. Written security policyC. SYN attack preventionD. Access Control List (ACL) Answer: B Explanation:Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category. QUESTION 105Which of the following can result in significant administrative overhead from incorrect reporting? A. Job rotationB. Acceptable usage policiesC. False positivesD. Mandatory vacations Answer: CExplanation:False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. This causes a significant administrative overhead because the reporting is what results in the false positives. QUESTION 106A vulnerability scan is reporting that patches are missing on a server. After a review, it is determined that the application requiring the patch does not exist on the operating system.Which of the following describes this cause? A. Application hardeningB. False positiveC. Baseline code reviewD. False negative Answer: BExplanation:False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. QUESTION 107Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results? A. True negativesB. True positivesC. False positivesD. False negatives Answer: CExplanation:False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. QUESTION 108Which of the following is an example of a false negative? A. The IDS does not identify a buffer overflow.B. Anti-virus identifies a benign application as malware.C. Anti-virus protection interferes with the normal operation of an application.D. A user account is locked out after the user mistypes the password too many times. Answer: AExplanation:With a false negative, you are not alerted to a situation when you should be alerted. QUESTION 109A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this? A. Command shell restrictionsB. Restricted interfaceC. Warning bannersD. Session output pipe to /dev/null Answer: CExplanation:Within Microsoft Windows, you have the ability to put signs (in the form of onscreen pop-up banners) that appear before the login telling similar information--authorized access only, violators will be prosecuted, and so forth. Such banners convey warnings or regulatory information to the user that they must "accept" in order to use the machine or network. You need to make staff aware that they may legally be prosecuted and a message is best given via a banner so that all staff using workstation will get notification. QUESTION 110Joe, a security analyst, asks each employee of an organization to sign a statement saying that they understand how their activities may be monitored. Which of the following BEST describes this statement? (Select TWO). A. Acceptable use policyB. Risk acceptance policyC. Privacy policyD. Email policyE. Security policy Answer: ACExplanation:Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment. Privacy policy is a legal document that outlines how data collected is secured. It should encompass information regarding the information the company collects, privacy choices you have

based on your account, potential information sharing of your data with other parties, security measures in place, and enforcement. Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware. QUESTION 111Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems? A. Acceptable Use PolicyB. Privacy PolicyC. Security PolicyD. Human Resource Policy Answer: AExplanation:Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware. QUESTION 112Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT? A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.B. Tell the application development manager to code the application to adhere to the company's password policy.C. Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.D. Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded. Answer: BExplanation:Since the application is violating the security policy it should be coded differently to comply with the password policy. QUESTION 113A major security risk with co-mingling of hosts with different security requirements is: A. Security policy violations.B. Zombie attacks.C. Password compromises.D. Privilege creep. Answer: AExplanation:The entire network is only as strong as the weakest host. Thus with the co-mingling of hosts with different security requirements would be risking security policy violations. QUESTION 114Which of the following provides the BEST explanation regarding why an organization needs to implement IT security policies? A. To ensure that false positives are identifiedB. To ensure that staff conform to the policyC. To reduce the organizational riskD. To require acceptable usage of IT systems Answer: CExplanation:Once risks has been identified and assessed then there are five possible actions that should be taken. These are: Risk avoidance, Risk transference, Risk mitigation, Risk deterrence and Risk acceptance. Anytime you engage in steps to reduce risk, you are busy with risk mitigation and implementing IT security policy is a risk mitigation strategy. QUESTION 115Which of the allow Pete, a security analyst, to trigger a security alert reduce the risk of employees working in collusion to embezzle funds from their company? A. Privacy PolicyB. Least PrivilegeC. Acceptable UseD. Mandatory Vacations Answer: DExplanation:A mandatory vacation policy requires all users to take time away from work to refresh. But not only does mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels as well as an opportunity to discover fraud. QUESTION 116Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together? A. Least privilege accessB. Separation of dutiesC. Mandatory access controlD. Mandatory vacations Answer: DExplanation:A mandatory vacation policy requires all users to take time away from work to refresh. Mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels. Mandatory vacations also provide an opportunity to discover fraud. In this case mandatory vacations can prevent the two members from colluding to steal the information that they have access to. QUESTION 117One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following? A. Mandatory accessB. Rule-based access controlC. Least privilegeD. Job rotation Answer: CExplanation:A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more. QUESTION 118A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate this issue so that only security administrators can make changes to the firewall? A. Mandatory vacationsB. Job rotationC. Least privilegeD. Time of day restrictions Answer: CExplanation:A least privilege policy is to give users only the permissions that they need to do their work and no more. That is only allowing security administrators to be able to make changes to the firewall by practicing the least privilege principle. QUESTION 119Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles? A. User rights reviewsB. Incident management C. Risk based controlsD. Annual loss expectancy Answer: AExplanation:A least privilege policy should be used when assigning permissions. Give users only the permissions and rights that they need to do their work and no more. QUESTION 120An IT security manager is asked to provide the total risk to the business. Which of the following calculations would he security manager choose to determine total risk? A. (Threats X vulnerability X asset value) x controls gapB. (Threats X vulnerability X profit) x asset value

C. Threats X vulnerability X control gapD. Threats X vulnerability X asset value Answer: DExplanation:Threats X vulnerability X asset value is equal to asset value (AV) times exposure factor (EF). This is used to calculate a risk. QUESTION 121A company is preparing to decommission an offline, non-networked root certificate server. Before sending the server's drives to be destroyed by a contracted company, the Chief Security Officer (CSO) wants to be certain that the data will not be accessed. Which of the following, if implemented, would BEST reassure the CSO? (Select TWO). A. Disk hashing proceduresB. Full disk encryptionC. Data retention policiesD. Disk wiping proceduresE. Removable media encryption Answer: BDExplanation:B: Full disk encryption is when the entire volume is encrypted; the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption.D: Disk wiping is the process of overwriting data on the repeatedly, or using a magnet to alter the magnetic structure of the disks. This renders the data unreadable. QUESTION 122Identifying residual risk is MOST important to which of the following concepts? A. Risk deterrenceB. Risk acceptanceC. Risk mitigationD. Risk avoidance Answer: BExplanation:Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition. To truly qualify as acceptance, it cannot be a risk where the administrator or manager is unaware of its existence; it has to be an identified risk for which those involved understand the potential cost or damage and agree to accept it. Residual risk is always present and will remain a risk thus it should be accepted (risk acceptance) QUESTION 123A software company has completed a security assessment. The assessment states that the company should implement fencing and lighting around the property. Additionally, the assessment states that production releases of their software should be digitally signed. Given the recommendations, the company was deficient in which of the following core security areas? (Select TWO). A. Fault toleranceB. EncryptionC. AvailabilityD. IntegrityE. SafetyF. Confidentiality Answer: DEExplanation:Aspects such as fencing, proper lighting, locks, CCTV, Escape plans Drills, escape routes and testing controls form part of safety controls.Integrity refers to aspects such as hashing, digital signatures, certificates and non-repudiation - all of which has to do with data integrity. QUESTION 124Which of the following defines a business goal for system restoration and acceptable data loss? A. MTTRB. MTBFC. RPOD. Warm site Answer: CExplanation:The recovery point objective (RPO) defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). This is an essential business goal insofar as system restoration and acceptable data loss is concerned. QUESTION 125Drag and Drop QuestionA Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type.Instructions: Controls can be used multiple times and not all placeholders needs to be filled. When you have completed the simulation, Please select Done to submit. Answer: Explanation:http://www.mentor-app.com/ Lead2pass new released SY0-401 PDF are now for free download, download it right now and pass your exam 100%. 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]