# [OFFICIALBraindump2go SY0-401 VCE Instant Download (101-110)

**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) We never believe in second chances and Braindump2go brings you the best SY0-401 Exam Preparation Materials 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! 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 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 102Which 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: BExplanation: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 106 A 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 policy E.   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. Braindump2go is one of the Leading SY0-401 Exam Preparation Material Providers Around the World! We Offer 100% Money Back Guarantee on All Products! Feel Free In Downloading Our New Released SY0-401 Real Exam Questions!

**CompTIA Security+ C**

Prod

Exam

"Comp
Certifi
assem
exam
to reac

Questions and Answers : 1220
Q&As
Updated: Nov 2, 2015
$129.99 $99.99
PDF DEMO
CHECK OUT

Free

Braind
can ch
decide

Pri

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