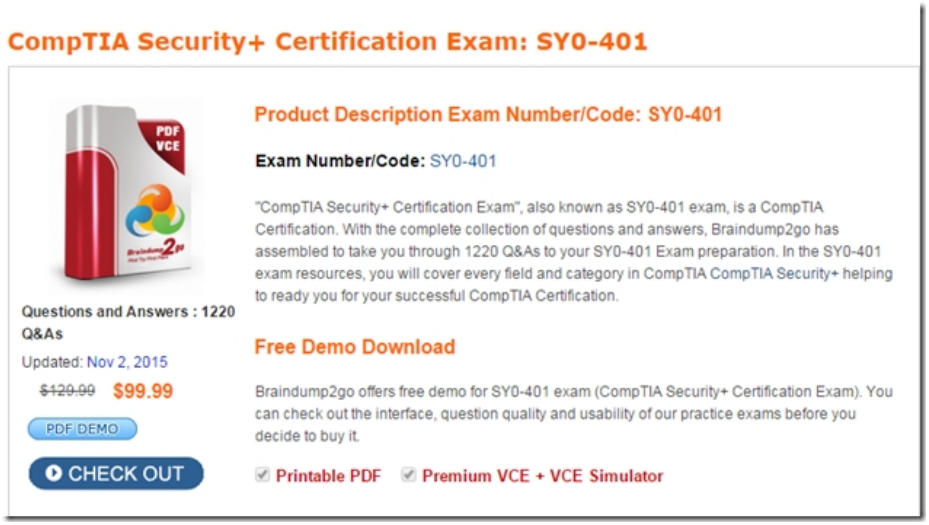
2015 SY0-401 Dumps VCE Latest Updated By Braindump2go Today (131-140)

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) New Braindump2go SY0-401 Exam Questions Updated Today! Want to know New Questions in 2015 SY0-401 Exam? Download Free Braindump2go SY0-401 Exam Preparation Materials Now! 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 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: B Explanation: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 PolicyD. 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: D Explanation: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 managementD. 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). Braindump2go Promise All SY0-401 Questions and Answers are the Latest Updated,we aim to provide latest and guaranteed questions for all certifications.You just need to be braved in trying then we will help you arrange all left things! 100% Pass All Exams you want Or Full Money Back! Do yo want to have a try on passing SY0-401?



FREE DOWNLOAD: NEW UPDATED SY0-401 PDF Dumps & SY0-401 VCE Dumps from Braindump2go:

http://www.braindump2go.com/sy0-401.html (1220 Q&A)