

2015 Latest Updated SY0-401 VCE Free Download from Braindump2go (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) SY0-401 Exam Dumps Free Shared By Braindump2go For Instant Download Now! Download Latest SY0-401 Exam Questions and pass SY0-401 one time easily! Do you want to be a winner? Exam Code: SY0-401 Exam Name: CompTIA Security+ Certification Provider: CompTIA Corresponding 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

CompTIA Security+ Certification



Product Description

Exam Number/Code: SY0-401

"CompTIA Security+ Certification. With the complete set of exam resources, you will be ready for your success."

Questions and Answers : 1220 Q&As

Updated: Nov 2, 2015

~~\$129.99~~ **\$99.99**

[PDF DEMO](#)

[CHECK OUT](#)

Printable PDF **PDF**

Free Demo Download

Braindump2go offers free demo. You can check out the interface and decide to buy it.

QUESTION 131 A 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: C Explanation: 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 132 Developers 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 management B. Clean desk policy C. Routine audits D. Change management Answer: D Explanation: 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 133 Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems? A. Incident management B. Server clustering C. Change management D. Forensic analysis Answer: C 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 `performing updates to business critical systems. QUESTION 134 The 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 hardening B. Application firewall review C. Application change management D. Application patch management Answer: C Explanation: 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 135 Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages? A. Risk transference B. Change management C. Configuration management D. 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 136 A 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 Policy B. Change

Control PolicyC. Incident Management PolicyD. Regression Testing PolicyE. Escalation PolicyF. Application Audit Policy

Answer: B
Explanation: A backout (regression testing) is a reversion from a change that had negative consequences. It could be, for example, that everything was working fine 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, hotfixes, 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 137 A 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 forward B. Contact the help desk and/or incident response team to determine next steps C. Provide the requestor with the email information since it will be released soon anyway D. Reply back to the requestor to gain their contact information and call them

Answer: B
Explanation: 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 incident
- Procedures to gather and secure evidence
- List 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 incident

Since 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 138 Which of the following is BEST carried out immediately after a security breach is discovered? A. Risk transference B. Access control revalidation C. Change management D. Incident management

Answer: D
Explanation: Incident management is the steps followed when security incident occurs.

QUESTION 139 A 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 management B. Chain of custody management C. Change management D. Incident management


Answer: D
Explanation: 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 140 Requiring technicians to report spyware infections is a step in which of the following? A. Routine audits B. Change management C. Incident management D. Clean desk policy

Answer: C
Explanation: 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).

100% Full Money Back Guarantee Promised By Braindump2go to All SY0-401 Exam Candidates: Braindump2go is confident that our NEW UPDATED SY0-401 Exam Questions and Answers are changed with CompTIA Official Exam Center, If you cannot PASS SY0-401 Exam, nevermind, we will return your full money back! Visit Braindump2go exam dumps collection website now and download SY0-401 Exam Dumps Instantly Today!

CompTIA Security+ Certification Exam: SY0-401



Product Description Exam Number/Code: SY0-401

Exam Number/Code: SY0-401

"CompTIA Security+ Certification Exam", also known as SY0-401 exam, is a CompTIA Certification. With the complete collection of questions and answers, Braindump2go has assembled to take you through 1220 Q&As to your SY0-401 Exam preparation. In the SY0-401 exam resources, you will cover every field and category in CompTIA Security+ helping to ready you for your successful CompTIA Certification.

Questions and Answers : 1220 Q&As

Updated: Nov 2, 2015

~~\$429.99~~ **\$99.99**

[PDF DEMO](#)

[CHECK OUT](#)

Printable PDF **Premium VCE + VCE Simulator**

Free Demo Download

Braindump2go offers free demo for SY0-401 exam (CompTIA Security+ Certification Exam). You can check out the interface, question quality and usability of our practice exams before you decide to buy it.

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