[18/July/2019 Updated New PassLeader 470q CAS-003 Practice Test Guarantee 100 Percent Exam Pass

New Updated CAS-003 Exam Questions from PassLeader CAS-003 PDF dumps! Welcome to download the newest PassLeader CAS-003 VCE dumps: https://www.passleader.com/cas-003.html (470 Q&As) Keywords: CAS-003 exam dumps, CAS-003 exam questions, CAS-003 VCE dumps, CAS-003 PDF dumps, CAS-003 practice tests, CAS-003 study guide, CAS-003 braindumps, CompTIA Advanced Security Practitioner (CASP) Exam P.S. New CAS-003 dumps PDF: https://drive.google.com/open?id=1bfoVeMAPqLPPEtiIibD38-i-xMle-2O0 NEW QUESTION 444 After the departure of a developer under unpleasant circumstances, the company is concerned about the security of the software to which the developer has access. Which of the following is the BEST way to ensure security of the code following the incident? A.   Hire an external red tem to conduct black box testing. B.   Conduct a peer review and cross reference the SRTM. C.   Perform white-box testing on all impacted finished products. D.   Perform regression testing and search for suspicious code. Answer: A NEW QUESTION 445 A Chief Information Security Officer (CISO) is developing a new BIA for the organization. The CISO wants to gather requirements to determine the appropriate RTO and RPO for the organization's ERP. Which of the following should the CISO interview as MOST qualified to provide RTO/RPO metrics? A.   Data custodian B.   Data owner C.   Security analyst D.   Business unit director E.   Chief Executive Officer (CEO) Answer: D NEW QUESTION 446 A security engineer is employed by a hospital that was recently purchased by a corporation. Throughout the acquisition process, all data on the virtualized file servers must be shared by departments within both organizations. The security engineer considers data ownership to determine ____. A.   the amount of data to be moved B.   the frequency of data backups C.   which users will have access to which data D.   when the file server will be decommissioned Answer: C NEW QUESTION 447 An information security manager conducted a gap analysis, which revealed a 75% implementation of security controls for high-risk vulnerabilities, 90% for medium vulnerabilities, and 10% for low-risk vulnerabilities. To create a road map to close the identified gaps, the assurance team reviewed the likelihood of exploitation of each vulnerability and the business impact of each associated control. To determine which controls to implement, which of the following is the MOST important to consider? A.   KPI B.   KRI C.   GRC D.   BIA Answer: C NEW QUESTION 448 A development team is testing an in-house-developed application for bugs. During the test, the application crashes several times due to null pointer exceptions. Which of the following tools, if integrated into an IDE during coding, would identify these bugs routinely? A.   Issue tracker B.   Static code analyzer C.   Source code repository D.   Fuzzing utility Answer: D NEW QUESTION 449 A legacy web application, which is being used by a hospital, cannot be upgraded for 12 months. A new vulnerability is found in the legacy application, and the networking team is tasked with mitigation. Middleware for mitigation will cost $100,000 per year. Which of the following must be calculated to determine ROI? (Choose two.) A.   ALE B.   RTO C.   MTBF D.   ARO E.   RPO Answer: AD NEW QUESTION 450 A project manager is working with a software development group to collect and evaluate user stories related to the organization's internally designed CRM tool. After defining requirements, the project manager would like to validate the developer's interpretation and understanding of the user's request. Which of the following would BEST support this objective? A.   Peer review B.   Design review C.   Scrum D.   User acceptance testing E.   Unit testing Answer: C NEW QUESTION 451 A network printer needs Internet access to function. Corporate policy states all devices allowed on the network must be authenticated. Which of the following is the MOST secure method to allow the printer on the network without violating policy? A.   Request an exception to the corporate policy from the risk management committee. B.   Require anyone trying to use the printer to enter their username and password. C.   Have a help desk employee sign in to the printer every morning. D.   Issue a certificate to the printer and use certificate-based authentication. Answer: D NEW QUESTION 452 The Chief Information Security Officer (CISO) of an established security department, identifies a customer who has been using a fraudulent credit card. The CISO calls the local authorities, and when they arrive on- site, the authorities ask a security engineer to create a point-in-time copy of the running database in their presence. This is an example of ____. A.   creating a forensic image B.   deploying fraud monitoring C.   following a chain of custody

D.   analyzing the order of volatility Answer: C NEW QUESTION 453 A technician is configuring security options on the mobile device manager for users who often utilize public Internet connections while travelling. After ensuring that full disk encryption is enabled, which of the following security measures should the technician take? (Choose two.) A.   Require all mobile device backups to be encrypted. B.   Ensure all mobile devices back up using USB OTG. C.   Issue a remote wipe of corporate and personal partitions. D.   Restrict devices from making long-distance calls during business hours. E.   Implement an always-on VPN. Answer: CE NEW QUESTION 454 A systems administrator receives an advisory email that a recently discovered exploit is being used in another country and the financial institutions have ceased operations while they find a way to respond to the attack. Which of the following BEST describes where the administrator should look to find information on the attack to determine if a response must be prepared for the systems? (Choose two.) A.   Bug bounty websites B.   Hacker forums C.   Antivirus vendor websites D.   Trade industry association websites E.   CVE database F.   Company's legal department Answer: EF NEW QUESTION 455 A security assessor is working with an organization to review the policies and procedures associated with managing the organization's virtual infrastructure. During a review of the virtual environment, the assessor determines the organization is using servers to provide more than one primary function, which violates a regulatory requirement. The assessor reviews hardening guides and determines policy allows for this configuration. It would be MOST appropriate for the assessor to advise the organization to ____. A.   segment dual-purpose systems on a hardened network segment with no external access B.   assess the risks associated with accepting non-compliance with regulatory requirements C.   update system implementation procedures to comply with regulations D.   review regulatory requirements and implement new policies on any newly provisioned servers Answer: A NEW QUESTION 456 While conducting a BIA for a proposed acquisition, the IT integration team found that both companies outsource CRM services to competing and incompatible third-party cloud services. The decision has been made to bring the CRM service in-house, and the IT team has chosen a future solution. With which of the following should the Chief Information Security Officer (CISO) be MOST concerned? (Choose two.) A.   Data remnants B.   Sovereignty C.   Compatible services D.   Storage encryption E.   Data migration F.   Chain of custody Answer: CE NEW QUESTION 457 The Chief Information Security Officer (CISO) suspects that a database administrator has been tampering with financial data to the administrator's advantage. Which of the following would allow a third-party consultant to conduct an on-site review of the administrator's activity? A.   Separation of duties B.   Job rotation C.   Continuous monitoring D.   Mandatory vacation Answer: A NEW QUESTION 458 Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed? A.   Lessons learned review B.   Root cause analysis C.   Incident audit D.   Corrective action exercise Answer: A NEW QUESTION 459 Following a recent network intrusion, a company wants to determine the current security awareness of all of its employees. Which of the following is the BEST way to test awareness? A.   Conduct a series of security training events with comprehensive tests at the end. B.   Hire an external company to provide an independent audit of the network security posture. C.   Review the social media of all employees to see how much proprietary information is shared. D.   Send an email from a corporate account, requesting users to log onto a website with their enterprise account. Answer: B NEW QUESTION 460 A company's security policy states any remote connections must be validated using two forms of network- based authentication. It also states local administrative accounts should not be used for any remote access. PKI currently is not configured within the network. RSA tokens have been provided to all employees, as well as a mobile application that can be used for 2FA authentication. A new NGFW has been installed within the network to provide security for external connections, and the company has decided to use it for VPN connections as well. Which of the following should be configured? (Choose two.) A.   Certificate-based authentication B.   TACACS+ C.   802.1X D.   RADIUS E.   LDAP F.   Local user database Answer: DE NEW QUESTION 461 The finance department has started to use a new payment system that requires strict PII security restrictions on various network devices. The company decides to enforce the restrictions and configure all devices appropriately. Which of the following risk response strategies is being used? A.   Avoid B.   Mitigate C.   Transfer D.   Accept Answer: D NEW

QUESTION 462 A security administrator is updating a company's SCADA authentication system with a new application. To ensure interoperability between the legacy system and the new application, which of the following stakeholders should be involved in the configuration process before deployment? (Choose two.) A.   Network engineer B.   Service desk personnel C.   Human resources administrator D.   Incident response coordinator E.   Facilities manager F.   Compliance manager Answer: DF NEW QUESTION 463 A company has decided to replace all the T-1 uplinks at each regional office and move away from using the existing MPLS network. All regional sites will use high-speed connections and VPNs to connect back to the main campus. Which of the following devices would MOST likely be added at each location? A.   SIEM B.   IDS/IPS C.   Proxy server D.   Firewall E.   Router Answer: D NEW QUESTION 464 First responders, who are part of a core incident response team, have been working to contain an outbreak of ransomware that also led to data loss in a rush to isolate the three hosts that were calling out to the NAS to encrypt whole directories, the hosts were shut down immediately without investigation and then isolated. Which of the following were missed? (Choose two.) A.   CPU, process state tables, and main memory dumps. B.   Essential information needed to perform data restoration to a known clean state. C.   Temporary file system and swap space. D.   Indicators of compromise to determine ransomware encryption. E.   Chain of custody information needed for investigation. Answer: DE NEW QUESTION 465 A regional business is expecting a severe winter storm next week. The IT staff has been reviewing corporate policies on how to handle various situations and found some are missing or incomplete. After reporting this gap in documentation to the information security manager, a document is immediately drafted to move various personnel to other locations to avoid downtime in operations. This is an example of ____. A.   a disaster recovery plan B.   an incident response plan C.   a business continuity plan D.   a risk avoidance plan Answer: A NEW QUESTION 466 ..... Download the newest PassLeader CAS-003 dumps from passleader.com now! 100% Pass Guarantee! CAS-003 PDF dumps & CAS-003 VCE dumps: https://www.passleader.com/cas-003.html (470 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New CAS-003 dumps PDF: https://drive.google.com/open?id=1bfoVeMAPqLPPEtiIibD38-i-xMle-2O0