[May-2018-NewHigh Quality Braindump2go CAS-003 Dumps VCE 270Q Free Share[89-99

2018 May New CompTIA CAS-003 Exam Dumps with PDF and VCE Just Updated Today! Following are some new CAS-003 Real Exam Questions:1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 270Q Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Exam Questions & Answers Download:https://drive.google.com/drive/folders/11eVcvdRTGUBlESzBX9a6YlPUYiZ4xoHE?usp=sharing QUESTION 89A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?A. Encryption of each individual partitionB. Encryption of the SSD at the file levelC. FDE of each logical volume on the SSDD. FDE of the entire SSD as a single diskAnswer: AExplanation:In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading. Therefore, the solution is to encrypt each individual partition separately.QUESTION 90A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of-concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?A. Assess the reliability of the information source, likelihood of exploitability, and impact to hosted data. Attempt to exploit via the proof-of-concept code. Consider remediation options.B. Hire an independent security consulting agency to perform a penetration test of the web servers. Advise management of any `high' or `critical' penetration test findings and put forward recommendations for mitigation.C. Review vulnerability write-ups posted on the Internet. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software. D. Notify all customers about the threat to their hosted data. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch.Answer: AExplanation:The first thing you should do is verify the reliability of the claims. From there you can assess the likelihood of the vulnerability affecting your systems. If it is determined that your systems are likely to be affected by the exploit, you need to determine what impact an attack will have on your hosted data. Now that you know what the impact will be, you can test the exploit by using the proof-of-concept code. That should help you determine your options for dealing with the threat (remediation).QUESTION 91A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobsB. Interview employees and managers to discover the industry hot topics and trendsC. Attend meetings with staff, internal training, and become certified in software managementD. Attend conferences, webinars, and training to remain current with the industry and job requirementsAnswer: DExplanation:Conferences represent an important method of exchanging information between researchers who are usually experts in their respective fields. Together with webinars and training to remain current on the subject the manager will be able to gain valuable insight into the cyber defense industry and be able to recruit personnel.QUESTION 92The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?A. AvoidB. AcceptC. MitigateD. TransferAnswer: CExplanation:Mitigation means that a control is used to reduce the risk. In this case, the control is training.QUESTION 93During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40 percent of the desktops do not meet requirements. Which of the following is the MOST likely cause of the noncompliance?A. The devices are being modified and settings are being overridden in production.B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.C. The desktop applications were configured with the default username and password.D. 40 percent of the devices use full disk encryption.Answer: AExplanation:The question states that all hosts are hardened at the OS level before deployment. So we know the desktops are fully patched when the users receive them. Six months later, the desktops do not meet the compliance standards. The most likely explanation for this is that the users have changed the settings of the desktops during the six months that they've had them.QUESTION 94ABC Company must

achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).A. Establish a list of users that must work with each regulationB. Establish a list of devices that must meet each regulationC. Centralize management of all devices on the networkD. Compartmentalize the networkE. Establish a company frameworkF. Apply technical controls to meet compliance with the regulationAnswer: BDFExplanation: Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.There are six main requirements for PCI compliance. The vendor must:Build and maintain a secure networkProtect cardholder dataMaintain a vulnerability management programImplement strong access control measuresRegularly monitor and test networksMaintain an information security policyTo achieve PCI and SOX compliance you should:Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.Apply technical controls to meet compliance with the regulation. Secure the data as required.QUESTION 95The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.D. Behavior based IPS with a communication link to a cloud based vulnerability and threat feed.Answer: DExplanation:Good preventive security practices are a must. These include installing and keeping firewall policies carefully matched to business and application needs, keeping antivirus software updated, blocking potentially harmful file attachments and keeping all systems patched against known vulnerabilities. Vulnerability scans are a good means of measuring the effectiveness of preventive procedures. Real-time protection: Deploy inline intrusion- prevention systems (IPS) that offer comprehensive protection. When considering an IPS, seek the following capabilities: network-level protection, application integrity checking, application protocol Request for Comment (RFC) validation, content validation and forensics capability. In this case it would be behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed.QUESTION 96A company provides on-demand cloud computing resources for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two- factor authentication for customer access to the administrative website. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data from customer A was found on a hidden directory within the VM of company B. Company B is not in the same industry as company A and the two are not competitors. Which of the following has MOST likely occurred?A. Both VMs were left unsecured and an attacker was able to exploit network vulnerabilities to access each and move the data.B. A stolen two factor token was used to move data from one virtual guest to another host on the same network segment.C. A hypervisor server was left un-patched and an attacker was able to use a resource exhaustion attack to gain unauthorized access.D. An employee with administrative access to the virtual guests was able to dump the guest memory onto a mapped disk.Answer: AExplanation:In this question, two virtual machines have been accessed by an attacker. The question is asking what is MOST likely to have occurred.It is common for operating systems to not be fully patched. Of the options given, the most likely occurrence is that the two VMs were not fully patched allowing an attacker to access each of them. The attacker could then copy data from one VM and hide it in a hidden folder on the other VM.QUESTION 97An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?A. Ensure the SaaS provider supports dual factor authentication.B. Ensure the SaaS provider supports encrypted password transmission and storage.C. Ensure the SaaS provider supports secure hash file exchange.D. Ensure the SaaS provider supports role-based access control.E. Ensure the SaaS provider supports directory services federation.Answer: EExplanation:A SaaS application that has a federation server within the customer's network that interfaces with the customer's own enterprise user-directory service can provide single sign-on authentication. This federation server has a trust relationship with a corresponding federation server located within the SaaS provider's network. Single sign-on will mitigate the risk of managing separate user credentials.QUESTION 98A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?A. Client side input validationB. Stored procedureC. Encrypting credit card detailsD. Regular expression matchingAnswer: DExplanation:Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected

input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code.QUESTION 99A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame for whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?A. During the Identification PhaseB. During the Lessons Learned phaseC. During the Containment PhaseD. During the Preparation PhaseAnswer: BExplanation:The Lessons Learned phase is the final step in the Incident Response process, when everyone involved reviews what happened and why.
!!!RECOMMEND!!!1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 270Q Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Exam Questions & Answers Download: YouTube Video: YouTube.com/watch?v=wiypGN6OqiA