This page was exported from - Offer Free Microsoft and Cisco Exam Dumps
Export date: Fri Nov 14 4:33:25 2025 / +0000 GMT

[2018-June-NewHigh Quality Braindump2go CAS-002 Dumps VCE and PDF 900Q Free Share[56-66

2018 June New CompTIA CAS-002 Exam Dumps with PDF and VCE Just Updated Today! Following are some new CAS-002 Real Exam Questions: 1.|2018 Latest CAS-002 Exam Dumps (PDF & VCE) 900Q&As Download:https://www.braindump2go.com/cas-002.html2.|2018 Latest CAS-002 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNQjRNekVOcFlaVm8?usp=sharingQUESTION 56A new malware spreads over UDP Port 8320 and several network hosts have been infected. A new security administrator has determined a possible cause, and the infected machines have been quarantined. Which of the following actions could a new security administrator take to further mitigate this issue?A. Limit source ports on the firewall to specific IP addresses.B. Add an explicit deny-all and log rule as the final entry of the firewall rulebase.C. Implement stateful UDP filtering on UDP ports above 1024.D. Configure the firewall to use IPv6 by default.**Answer: B**QUESTION 57At one time, security architecture best practices led to networks with a limited number (1-3) of network access points. This restriction allowed for the concentration of security resources and resulted in a well defined attack surface. The introduction of wireless networks, highly portable network devices, and cloud service providers has rendered the network boundary and attack surface increasingly porous. This evolution of the security architecture has led to which of the following?A. Increased security capabilities, the same amount of security risks and a higher TCO but a smaller corporate datacenter on average.B. Increased business capabilities and increased security risks with a lower TCO and smaller physical footprint on the corporate network.C. Increased business capabilities and increased security risks with a higher TCO and a larger physical footprint.D. Decreased business capabilities and increased security risks with a lower TCO and increased logical footprint due to virtualization.**Answer: C**QUESTION 58Company A is trying to implement controls to reduce costs and time spent on litigation.To accomplish this, Company A has established several goals:- Prevent data breaches from lost/stolen assets- Reduce time to fulfill e-discovery requests- Prevent PII from leaving the network- Lessen the network perimeter attack surface- Reduce internal fraudWhich of the following solutions accomplishes the MOST of these goals?A. Implement separation of duties; enable full encryption on USB devices and cell phones, allow cell phones to remotely connect to e-mail and network VPN, enforce a 90 day data retention policy.B. Eliminate VPN access from remote devices. Restrict junior administrators to read-only shell access on network devices. Install virus scanning and SPAM filtering. Harden all servers with trusted OS extensions.C. Create a change control process with stakeholder review board, implement separation of duties and mandatory vacation, create regular SAN snapshots, enable GPS tracking on all cell phones and laptops, and fully encrypt all email in transport.D. Implement outgoing mail sanitation and incoming SPAM filtering. Allow VPN for mobile devices; cross train managers in multiple disciplines, ensure all corporate USB drives are provided by Company A and de-duplicate all server storage.**Answer: A**QUESTION 59Company A is merging with Company B. Company B uses mostly hosted services from an outside vendor, while Company A uses mostly in-house products.The project manager of the merger states the merged systems should meet these goals:- Ability to customize systems per department- Quick implementation along with an immediate ROI- The internal IT team having administrative level control over all productsThe project manager states the in-house services are the best solution. Because of staff shortages, the senior security administrator argues that security will be best maintained by continuing to use outsourced services.Which of the following solutions BEST solves the disagreement?A. Raise the issue to the Chief Executive Officer (CEO) to escalate the decision to senior management with the recommendation to continue the outsourcing of all IT services.B. Calculate the time to deploy and support the in-sourced systems accounting for the staff shortage and compare the costs to the ROI costs minus outsourcing costs. Present the document numbers to management for a final decision.C. Perform a detailed cost benefit analysis of outsourcing vs. in-sourcing the IT systems and review the system documentation to assess the ROI of in-sourcing. Select COTS products to eliminate development time to meet the ROI goals.D. Arrange a meeting between the project manager and the senior security administrator to review the requirements and determine how critical all the requirements are.**Answer: B**QUESTION 60A corporation relies on a server running a trusted operating system to broker data transactions between different security zones on their network. Each zone is a separate domain and the only connection between the networks is via the trusted server.The three zones at the corporation are as followeD.Zone A connects to a network, which is also connected to the Internet through a router.Zone B to a closed research and development network. Zone C to an intermediary switch supporting a SAN, dedicated to long-term audit log and file storage, so the corporation meets compliance requirements.A firewall is deployed on the inside edge of the Internet connected router.Which of the following is the BEST location to place other security equipment?A. HIPS on all hosts in Zone A and B, and an antivirus and patch server in Zone C.B. A WAF on the switch in Zone C, an additional firewall in Zone A, and an antivirus server in Zone B.C. A NIPS on the switch in Zone C, an antivirus server in Zone A, and a patch server in Zone B.D. A NIDS on the switch in Zone C,

a WAF in Zone A, and a firewall in Zone B.**Answer: C**QUESTION 61A security architect is seeking to outsource company server resources to a commercial cloud service provider. The provider under consideration has a reputation for poorly controlling physical access to datacenters and has been the victim of multiple social engineering attacks. The service provider regularly assigns VMs from multiple clients to the same physical resources. When conducting the final risk assessment which of the following should the security architect take into consideration?A. The ability to implement user training programs for the purpose of educating internal staff about the dangers of social engineering.B. The cost of resources required to relocate services in the event of resource exhaustion on a particular VM.C. The likelihood a malicious user will obtain proprietary information by gaining local access to the hypervisor platform.D. Annual loss expectancy resulting from social engineering attacks against the cloud service provider affecting corporate network infrastructure.**Answer: C**QUESTION 62Virtual hosts with different security requirements should be:A. encrypted with a one-time password.B. stored on separate physical hosts.C. moved to the cloud.D. scanned for vulnerabilities regularly.**Answer: B**QUESTION 63The company is considering issuing non-standard tablet computers to executive management. Which of the following is the FIRST step the security manager should perform?A. Apply standard security policy settings to the devices.B. Set up an access control system to isolate the devices from the network.C. Integrate the tablets into standard remote access systems.D. Develop the use case for the devices and perform a risk analysis.**Answer: D**QUESTION 64An employee of a company files a complaint with a security administrator. While sniffing network traffic, the employee discovers that financially confidential emails were passing between two warehouse users. The two users deny sending confidential emails to each other. Which of the following security practices would allow for non-repudiation and prevent network sniffers from reading the confidential mail? (Select TWO).A. Transport encryptionB. Authentication hashingC. Digital signatureD. Legal mail holdE. TSIG code signing**Answer: AC**QUESTION 65Company XYZ is selling its manufacturing business consisting of one plant to a competitor, Company QRS. All of the people will become QRS employees, but will retain permissions to plant-specific information and resources for one month. To ease the transition, Company QRS also connected the plant and employees to the Company QRS network. Which of the following threats is the HIGHEST risk to Company XYZ?A. Malware originating from Company XYZ's networkB. Co-mingling of company networksC. Lack of an IPSec connection between the two networksD. Loss of proprietary plant information**Answer: B**QUESTION 66A programming team is deploying a new PHP module to be run on a Solaris 10 server with trusted extensions. The server is configured with three zones, a management zone, a customer zone, and a backend zone. The security model is constructed so that only programs in the management zone can communicate data between the zones. After installation of the new PHP module, which handles on-line customer payments, it is not functioning correctly. Which of the following is the MOST likely cause of this problem?A. The PHP module is written to transfer data from the customer zone to the management zone, and then from the management zone to the backend zone.B. The iptables configuration is not configured correctly to permit zone to zone communications between the customer and backend zones.C. The PHP module was installed in the management zone, but is trying to call a routine in the customer zone to transfer data directly to a MySQL database in the backend zone.D. The ipfilters configuration is configured to disallow loopback traffic between the physical NICs associated with each zone.**Answer: C**!!!RECOMMEND!!!1.|2018 Latest CAS-002 Exam Dumps (PDF & VCE) 900Q&As Download:https://www.braindump2go.com/cas-002.html2.|2018 Latest CAS-002 Study Guide Video: YouTube Video: YouTube.com/watch?v=k4FW5mVem0w