[Nov-2018Download Braindump2go CS0-001 PDF and VCE for Free[Q203-213

2018/November Braindump2go CS0-001 Exam Dumps with PDF and VCE New Updated Today! Following are some new CS0-001 Real Exam Questions:1.|2018 Latest CS0-001 Exam Dumps (PDF & VCE) 252Q&As Download:https://www.braindump2go.com/cs0-001.html2.|2018 Latest CS0-001 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNclFka2Z1NWtOaG8?usp=sharingQUESTION 203A company has decided to process credit card transactions directly. Which of the following would meet the requirements for scanning this type of data?A. QuarterlyB. YearlyC. Bi-annuallyD. Monthly**Answer: A**QUESTION 204Which of the following countermeasures should the security administrator apply to MOST effectively mitigate Bootkit-level infections of the organization's workstation devices?A. Remove local administrator privileges.B. Configure a BIOS-level password on the device.C. Install a secondary virus protection application.D. Enforce a system state recovery after each device reboot.**Answer: A**QUESTION 205A new zero-day vulnerability was discovered within a basic screen capture app, which is used throughout the environment. Two days after discovering the vulnerability, the manufacturer of the software has not announced a remediation or if there will be a fix for this newly discovered vulnerability. The vulnerable application is not uniquely critical, but it is used occasionally by the management and executive management teams. The vulnerability allows remote code execution to gain privileged access to the system. Which of the following is the BEST course of actions to mitigate this threat?A. Work with the manufacturer to determine the time frame for the fix.B. Block the vulnerable application traffic at the firewall and disable the application services on each computer.C. Remove the application and replace it with a similar non-vulnerable application.D. Communicate with the end users that the application should not be used until the manufacturer has resolved the vulnerability.**Answer: D**QUESTION 206Which of the following tools should a cybersecurity analyst use to verify the integrity of a forensic image before and after an investigation?A. stringsB. sha1sumC. fileD. ddE. gzip**Answer: B**QUESTION 207A centralized tool for organizing security events and managing their response and resolution is known as:A. SIEMB. HIPSC. SyslogD. Wireshark**Answer: A**QUESTION 208 After a recent security breach, it was discovered that a developer had promoted code that had been written to the production environment as a hotfix to resolve a user navigation issue that was causing issues for several customers. The code had inadvertently granted administrative privileges to all users, allowing inappropriate access to sensitive data and reports. Which of the following could have prevented this code from being released into the production environment?A. Cross trainingB. Succession planningC. Automate reportingD. Separation of duties**Answer: D**QUESTION 209A security analyst is assisting with a computer crime investigation and has been asked to secure a PC and deliver it to the forensic lab. Which of the following items would be MOST helpful to secure the PC? (Choose three.)A. Tamper-proof sealsB. Faraday cageC. Chain of custody formD. Drive eraserE. Write blockersF. Network tapG. Multimeter**Answer: ABC**QUESTION 210A nuclear facility manager determined the need to monitor utilization of water within the facility. A startup company just announced a state-of-the-art solution to address the need for integrating the business and ICS network. The solution requires a very small agent to be installed on the ICS equipment. Which of the following is the MOST important security control for the manager to invest in to protect the facility?A. Run a penetration test on the installed agent.B. Require that the solution provider make the agent source code available for analysis.C. Require through guides for administrator and users.D. Install the agent for a week on a test system and monitor the activities.**Answer: D** QUESTION 211A company has implemented WPA2, a 20-character minimum for the WiFi passphrase, and a new WiFi passphrase every 30 days, and has disabled SSID broadcast on all wireless access points. Which of the following is the company trying to mitigate?A. Downgrade attacksB. Rainbow tablesC. SSL pinningD. Forced deauthentication**Answer: A**QUESTION 212A staff member reported that a laptop has degraded performance. The security analyst has investigated the issue and discovered that CPU utilization, memory utilization, and outbound network traffic are consuming the laptop resources. Which of the following is the BEST course of actions to resolve the problem?A. Identify and remove malicious processes.B. Disable scheduled tasks.C. Suspend virus scan.D. Increase laptop memory.E. Ensure the laptop OS is properly patched.**Answer: A**QUESTION 213A security analyst has discovered that an outbound SFTP process is occurring at the same time of day for the past several days. At the time this was discovered, large amounts of business critical data were delivered. The authentication for this process occurred using a service account with proper credentials. The security analyst investigated the destination IP for this transfer and discovered that this new process is not documented in the change management log. Which of the following would be the BEST course of action for the analyst to take?A. Investigate a potential incident.B. Verify user permissions.C. Run a vulnerability scan.D. Verify SLA with cloud provider.**Answer: A**!!!RECOMMEND!!!1.|2018 Latest CS0-001 Exam Dumps (PDF & VCE) 252Q&As Download:https://www.braindump2go.com/cs0-001.html2.|2018 Latest CS0-001 Study Guide Video: YouTube Video: YouTube.com/watch?v=m9hajso3rNc