[30/Nov/2018 Updated PassLeader CS0-001 PDF Dumps And VCE Dumps For Free Download

New Updated CS0-001 Exam Questions from PassLeader CS0-001 PDF dumps! Welcome to download the newest PassLeader CS0-001 VCE dumps: https://www.passleader.com/cs0-001.html (252 Q&As) Keywords: CS0-001 exam dumps, CS0-001 exam questions, CS0-001 VCE dumps, CS0-001 PDF dumps, CS0-001 practice tests, CS0-001 study guide, CS0-001 braindumps, CompTIA Cybersecurity Analyst (CSA+) Exam P.S. New CS0-001 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpaXd6TXJ4T3ItSDQ NEW QUESTION 200 A security analyst begins to notice the CPU utilization from a sinkhole has begun to spike. Which of the following describes what may be occurring? A.   Someone has logged on to the sinkhole and is using the device. B.   The sinkhole has begun blocking suspect or malicious traffic. C.   The sinkhole has begun rerouting unauthorized traffic. D.   Something is controlling the sinkhole and causing CPU spikes due to malicious utilization. Answer: C NEW QUESTION 201 Alerts have been received from the SIEM, indicating infections on multiple computers. Base on threat characteristics, these files were quarantined by the host-based antivirus program. At the same time, additional alerts in the SIEM show multiple blocked URLs from the address of the infected computers; the URLs were classified as uncategorized. The domain location of the IP address of the URLs that were blocked is checked, and it is registered to an ISP in Russia. Which of the following steps should be taken NEXT? A.   Remove those computers from the network and replace the hard drives. Send the infected hard drives out for investigation. B.   Run a full antivirus scan on all computers and use Splunk to search for any suspicious activity that happened just before the alerts were received in the SIEM. C.   Run a vulnerability scan and patch discovered vulnerabilities on the next pathing cycle. Have the users restart their computers. Create a use case in the SIEM to monitor failed logins on the infected computers. D.   Install a computer with the same settings as the infected computers in the DMZ to use as a honeypot. Permit the URLs classified as uncategorized to and from that host. Answer: B NEW QUESTION 202 Which of the following has the GREATEST impact to the data retention policies of an organization? A.   The CIA classification matrix assigned to each piece of data. B.   The level of sensitivity of the data established by the data owner. C.   The regulatory requirements concerning the data set. D.   The technical constraints of the technology used to store the data. Answer: D NEW QUESTION 203 A company has decided to process credit card transactions directly. Which of the following would meet the requirements for scanning this type of data? A.   Quarterly B.   Yearly C.   Bi-annually D.   Monthly Answer: A NEW QUESTION 204 Which of the following counter measures 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 NEW QUESTION 205 A 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 NEW QUESTION 206 Which of the following tools should a cybersecurity analyst use to verify the integrity of a forensic image before and after an investigation? A.   strings B.   sha1sum C.   file D.   dd E.   gzip Answer: B NEW QUESTION 207 A centralized tool for organizing security events and managing their response and resolution is known as what? A.   SIEM B.   HIPS C.   Syslog D.   Wireshark Answer: A NEW 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 training B.   Succession planning C.   Automate reporting D.   Separation of duties Answer: D NEW QUESTION 209 A 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 seals B.   Faraday cage C.   Chain of custody form D.   Drive eraser E.   Write blockers F.   Network tap G.   Multimeter Answer: ABC NEW QUESTION 210 A 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 NEW QUESTION 211 A 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 attacks B.   Rainbow tables C.   SSL pinning D.   Forced deauthentication Answer: A NEW QUESTION 212 A 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 NEW QUESTION 213 A 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 NEW QUESTION 214 During an investigation, a computer is being seized. Which of the following is the FIRST step the analyst should take? A.   Power off the computer and remove it from the network. B.   Unplug the network cable and take screenshots of the desktop. C.   Perform a physical hard disk image. D.   Initiate chain-of-custody documentation. Answer: A NEW QUESTION 215 An organization has recently experienced a data breach. A forensic analysis confirmed the attacker found a legacy web server that had not been used in over a year and was not regularly patched. After a discussion with the security team, management decided to initiate a program of network reconnaissance and penetration testing. They want to start the process by scanning the network for active hosts and open ports. Which of the following tools is BEST suited for this job? A.   Ping B.   Nmap C.   Netstat D.   ifconfig E.   Wireshark F.   L0phtCrack Answer: B NEW QUESTION 216 A medical organization recently started accepting payments over the phone. The manager is concerned about the impact of the storage of different types of data. Which of the following types of data incurs the highest regulatory constraints? A.   PHI B.   PCI C.   PII D.   IP Answer: B NEW QUESTION 217 An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive? A.   Reports indicate that findings are informational. B.   Any items labeled `low' are considered informational only. C.    The scan result version is different from the automated asset inventory. D.    `HTTPS' entries indicate the web page is encrypted securely. Answer: B NEW QUESTION 218 An insurance company employs quick-response team drivers that carry corporate-issued mobile devices with the insurance company's app installed on them. Devices are configuration-hardened by an MDM and kept up to date. The employees use the app to collect insurance claim information and process payments. Recently, a number of customers have filed complaints of credit card fraud against the insurance company, which

occurred shortly after their payments were processed via the mobile app. The cyber-incident response team has been asked to investigate. Which of the following is MOST likely the cause? A.   The MDM server is misconfigured. B.   The app does not employ TLS. C.   USB tethering is enabled. D.   3G and less secure cellular technologies are not restricted. Answer: B NEW QUESTION 219 A cybersecurity consultant found common vulnerabilities across the following services used by multiple servers at an organization: VPN, SSH, and HTTPS. Which of the following is the MOST likely reason for the discovered vulnerabilities? A.   Leaked PKI private key B.   Vulnerable version of OpenSSL C.   Common initialization vector D.   Weak level of encryption entropy E.   Vulnerable implementation of PEAP Answer: D NEW QUESTION 220 A recent audit included a vulnerability scan that found critical patches released 60 days prior were not applied to servers in the environment. The infrastructure team was able to isolate the issue and determined it was due to a service being disabled on the server running the automated patch management application. Which of the following would be the MOST efficient way to avoid similar audit findings in the future? A.   Implement a manual patch management application package to regain greater control over the process. B.   Create a patch management policy that requires all servers to be patched within 30 days of patch release. C.   Implement service monitoring to validate that tools are functioning properly. D.   Set services on the patch management server to automatically run on start-up. Answer: D NEW QUESTION 221 ..... Download the newest PassLeader CS0-001 dumps from passleader.com now! 100% Pass Guarantee! CS0-001 PDF dumps & CS0-001 VCE dumps: https://www.passleader.com/cs0-001.html (252 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New CS0-001 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpaXd6TXJ4T3ItSDQ