[NEW-500-275-DumpsInstant Download Braindump2go 500-275 VCE Exam Dump 60q[1-10

2016/12 New Cisco 500-275: Securing Cisco Networks with Sourcefire FireAMP Endpoints Exam Questions Updated Today!Free Instant Download 500-275 Exam Dumps (PDF & VCE) 60Q&As from Braindump2go.com Today! 100% Real Exam Questions! 100% Exam Pass Guaranteed! 1.|2016/12 New 500-275 Exam Dumps (PDF & VCE) 60Q&As Download: **http://www.braindump2go.com/500-275.html** 2.|2016/12 New 500-275 Exam Questions & Answers: https://1drv.ms/f/s!AvI7wzKf6QBjgTORnNkRWih6Psy- QUESTION 1Custom whitelists are used for which purpose? A. to specify which files to alert onB. to specify which files to deleteC. to specify which files to ignoreD. to specify which files to sandbox Answer: C QUESTION 2How does application blocking enhance security? A. It identifies and logs usage.B. It tracks application abuse.C. It deletes identified applications.D. It blocks vulnerable applications from running, until they are patched. Answer: D QUESTION 3Which set of actions would you take to create a simple custom detection? A. Add a SHA-256 value; upload a file to calculate a SHA-256 value; upload a text file that contains SHA-256 values.B. Upload a packet capture; use a Snort rule; use a ClamAV rule.C. Manually input the PE header data, the MD-5 hash, and a list of MD-5 hashes.D. Input the file and file name. Answer: A QUESTION 4Advanced custom signatures are written using which type of syntax? A. Snort signatures B. Firewall signaturesC. ClamAV signaturesD. bash shell Answer: C QUESTION 5Which statement represents a best practice for deploying on Windows servers? A. You should treat Windows servers like any other host in the deployment.B. You should obtain the Microsoft TechNet article that describes the proper exclusions for Windows servers.C. You should never configure exclusions for Windows servers.D. You should deploy FireAMP connectors only alongside existing antivirus software on Windows servers. Answer: B QUESTION 6File information is sent to the Sourcefire Collective Security Intelligence Cloud using which format? A. MD5B. SHA-1C. filenamesD. SHA-256 Answer: D QUESTION 7When discussing the FireAMP product, which term does the acronym DFC represent? A. It means Detected Forensic Cause.B. It means Duplicate File Contents.C. It means Device Flow Correlation.D. It is not an acronym that is associated with the FireAMP product. Answer: C QUESTION 8 What do policies enable you to do? A. specify a custom whitelistB. specify group membershipC. specify hosts to include in reportsD. specify which events to view Answer: A QUESTION 9What is the default clean disposition cache setting? A. 3600B. 604800C. 10080D. 1 hour Answer: B QUESTION 10How many days' worth of data do the widgets on the dashboard page display? A. the previous 5 days of dataB. the previous 6 days of dataC. the previous 7 days of dataD. the number of days you set in the dashboard configuration Answer: C !!!RECOMMEND!!! 1.Braindump2go|2016/12 New 500-275 Exam Dumps (PDF & VCE) 60Q&As Download:http://www.braindump2go.com/500-275.html 2.Braindump2go|2016/12 New 500-275 Study Guide: YouTube Video: YouTube.com/watch?v=evptKD9ZEYU