[Full Version Try Lead2pass Latest Cisco 500-290 Dumps To Pass The Exam Successfully (1-10)

2017 February Cisco Official New Released 500-290 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Are you struggling for the 500-290 exam? Good news, Lead2pass Cisco technical experts have collected all the questions and answers which are updated to cover the knowledge points and enhance candidates' abilities. We offer the latest 500-290 PDF and VCE dumps with new version VCE player for free download, and the new 500-290 dump ensures your 500-290 exam 100% pass. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/500-290.html QUESTION 1 Which option transmits policy-based alerts such as SNMP and syslog? A. the Defense Center B. FireSIGHT C. the managed device D. the hostAnswer: C QUESTION 2 Which option is used to implement suppression in the Rule Management user interface? A. Rule Category B. Global C. Source D. Protocol Answer: C QUESTION 3 FireSIGHT recommendations appear in which layer of the Policy Layers page? A. Layer Summary B. User Layers C. Built-In Layers D. FireSIGHT recommendations do not show up as a layer. Answer: C QUESTION 4 In addition to the discovery of new hosts, FireSIGHT can also perform which function? A. block traffic B. determine which users are involved in monitored connections C. discover information about users D. route traffic Answer: B QUESTION 5 A user discovery agent can be installed on which platform? A. OpenLDAP B. Windows C. RADIUS D. Ubuntu Answer: B QUESTION 6 Other than navigating to the Network File Trajectory page for a file, which option is an alternative way of accessing the network trajectory of a file? A. from Context Explorer B. from the Analysis menu C. from the cloud D. from the Defense Center Answer: A QUESTION 7 Which option can you enter in the Search text box to look for the trajectory of a particular file? A. the MD5 hash value of the file B. the SHA-256 hash value of the file C. the URL of the file D. the SHA-512 hash value of the file Answer: B QUESTION 8 A context box opens when you click on an event icon in the Network File Trajectory map for a file. Which option is an element of the box? A. Scan B. Application Protocol C. Threat Name D. File Name Answer: B QUESTION 9 Which Cisco IPS signature parameter can be tuned to reduce the volume of the alerts that are written to the event store? A. alert action B. alert frequency C. alert fidelity rating D. alert severity E. alert firing mode F. alert logging Answer: B QUESTION 10 Which two operations would put an inline Cisco IPS sensor in detection mode? (Choose two.) A. subtract all aggressive actions using event action filters B. decrease the event count using event action filters C. increase the maximum inter-event interval using event action overrides D. remove the default event action override, which drops traffic with a risk rating of 90 to 100 E. enable anomaly detection in detection mode only Answer: AD We ensure our new version 500-290 PDF and VCE dumps are 100% valid for passing exam, because Lead2pass is the top IT certification study training materials vendor. Many candidates have passed exam with the help of Lead2pass's VCE or PDF dumps. Lead2pass will update the study materials timely to make them be consistent with the current exam. Download the free demo on Lead2pass, you can pass the exam easily. 500-290 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDbVYtOTNZU0FUYTQ 2017 Cisco 500-290 exam dumps (All 70 Q&As) from Lead2pass: http://www.lead2pass.com/500-290.html [100% Exam Pass Guaranteed]