

New Released Free Version of Cisco 500-275 Exam Study Materials in Lead2pass

With the complete collection of 500-275 Questions and Answers, Lead2pass has assembled to take you through Questions and Answers to your 500-275 Exam preparation. In the 500-275 exam resources, you will cover every field of 500-275 exam helping to ready you for your successful Cisco Certification.

QUESTION 1 Custom whitelists are used for which purpose? A. to specify which files to alert on B. to specify which files to delete C. to specify which files to ignore D. to specify which files to sandbox
Answer: C

QUESTION 2 How 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 3 Which 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 4 Advanced custom signatures are written using which type of syntax? A. Snort signatures B. Firewall signatures C. ClamAV signatures D. bash shell
Answer: C

QUESTION 5 What is a valid data source for DFC Windows connector policy configuration? A. SANS B. NIST C. Emerging Threats D. Custom and Sourcefire
Answer: D

QUESTION 6 The Update Window allows you to perform which action? A. identify which hosts need to be updated B. email the user to download a new client C. specify a timeframe when an upgrade can be started and stopped D. update your cloud instance
Answer: C

QUESTION 7 The FireAMP connector supports which proxy type? A. SOCKS6 B. HTTP_proxy C. SOCKS5_filename D. SOCKS7
Answer: B

QUESTION 8 What do policies enable you to do? A. specify a custom whitelist B. specify group membership C. specify hosts to include in reports D. specify which events to view
Answer: A

QUESTION 9 What is the default clean disposition cache setting? A. 3600 B. 604800 C. 10080 D. 1 hour
Answer: B

The Lead2pass Cisco 500-275 questions and answers in PDF&VCE that we have, is the most reliable guide for Cisco 500-275 certification exams from our test Engine. These easy to understand Cisco 500-275 questions and answers are available in PDF&VCE format to make it simpler to utilize, and guarantee Cisco 500-275 exam 100% success. <http://www.lead2pass.com/500-275.html>