[Full Version 500-265 New Questions For Passing The 500-265 Certification Exam (31-40)

 2017 February Cisco Official New Released 500-265 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Although the Cisco 500-265 dumps are very popular, Lead2pass offers a wide range of Cisco 500-265 exam dumps and will continue to release new study guide to meet the rapidly increasing demand of the IT industry.   Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/500-265.html QUESTION 31   Consider the process that begins with file retrospection, continues to interrogate the file and update its disposition over time, then records the pathway that the software and files take from device to device. This process is an example of which Cisco AMP feature? A.   file reputation   B.   attack chain weaving   C.   breach hunting   D.   file sandboxing   E.   machine learningAnswer: B   QUESTION 32   How does the Device Trajectory feature work? A.   It searches for potential threats based on identified activities.   B.   It tracks file behavior across the network to see which devices it enters and exits. C.   It analyzes the data from file and process retrospection to provide a new level of threat intelligence. D.   It isolates suspicious files and runs tests to determine their authenticity.   E.   It tracks file behavior on a device to pinpoint the root cause of a compromise. Answer: E   QUESTION 33   Which Cisco Secure Access solution should you recommend to a customer who is experiencing access complications due to too many policies and too many user groups? A.   Cisco AnyConnect   B.   Cisco TrustSec C.   Cisco ISE   D.   Cisco AMP for Endpoints   E.   Cisco site-to-site VPN   F.   Cisco SIO Answer: B   QUESTION 34   Which statement best describes Cisco ISE? A.   Cisco ISE consolidates user AAA, Security Group Access features, and ScanSafe functionality into one product.   B.   Cisco ISE consolidates user authentication with NAC components into one solution. C.   Cisco ISE provides AAA features, guest provisioning, and device profiling features in the base feature set; link encryption policies, host posture, and security group access require the advanced feature set.   D.   Cisco ISE combines the capabilities of Cisco Secure ACS and Cisco Virtual Security Gateway into one product. Answer: B QUESTION 35   Which two statements about the capabilities of the Cisco AnyConnect Secure Mobility Client for Windows are true? (Choose two.) A.   It supports always-on connectivity by automatically establishing a VPN connection as needed. If multiple VPN gateways exist, load sharing occurs in a Round-robin fashion.   B.   It supports session persistence after hibernation or standby.   C.   Trusted Network Detection allows the connection to be established without any user intervention (authentication), if the client is located inside the office.   D.   It is exclusively configured by central policies; no local configuration is possible.   E.   The order of policy enforcement is as follows: dynamic access policy, user attributes, tunnel group, group policy attributes. Answer: BC   QUESTION 36   Which statement about wireless intrusion prevention and rogue access point detection is true? A.   A local mode access point provides power to wireless clients.   B.   A monitor mode access point performs background scanning in order to detect rogue access points.   C.   A monitor mode access point is dedicated to scanning (listen-only).   D.   A monitor mode access point can distribute a white list of all known access points.   E.   Any access point that broadcasts the same RF group name or is part of the same mobility group is considered to be a rogue access point. Answer: C   QUESTION 37   Which Cisco technology solution can resolve a customer's inability to properly restrict and authorize access to protected resources, while still introducing new applications, devices, and business partnerships? A.   Cisco TrustSec   B.   Cisco Data Center Management Policy Implementation   C.   Cisco Data Center Virtualization and Cloud   D.   Cisco Cyber Threat Defense   E.   Cisco Application Centric Infrastructure   F.   Cisco Secure Data Center   G.   Cisco Security Intelligence Operations Answer: A   QUESTION 38   Which two advanced malware protection features are available on Cisco AMP for Content? (Choose two.) A.   URL filtering B.   retrospective security   C.   attack chain weaving   D.   breach hunting   E.   trajectory   F.   behavioral indications of compromise Answer: AB QUESTION 39   Which option best describes granular app control using application visibility and control? A.   blocking harmful sites based on content, such as pokerstars.com   B.   blocking World of Warcraft but allowing Google+   C.   blocking Facebook games but allowing Facebook posts D.   blocking Twitter to increase employee productivity Answer: C   QUESTION 40   The first phase of

email security analyzes "who-what-where-when-how" information and context-based policies during which component of threat detection? A.   antivirus defense   B.   advanced malware protection for email C.   outbreak filters   D.   data loss prevention   E.   encryption F.   antispam defense Answer: F   Lead2pass offers the latest Cisco 500-265 dumps and a good range of Cisco Certification 500-265 answers. Most of our Cisco 500-265 exam dumps are exclusively prepared by the best brains and highly skilled professionals from the IT domain to ensure 100% pass in your Cisco 500-265 Exam.   500-265 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDNHNoN0tSZkJEYWs 2017 Cisco 500-265 exam dumps (All 71 Q&As) from Lead2pass: http://www.lead2pass.com/500-265.html [100% Exam Pass Guaranteed]