[May 2018 Lead2pass 500-265 Exam Questions Guarantee 500-265 Certification Exam 100% Success 118q

Lead2pass Free 500-265 Exam Questions Download 100% Pass 500-265 Exam: https://www.lead2pass.com/500-265.html QUESTION 31Consider 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 reputationB. attack chain weavingC. breach huntingD. file sandboxingE. machine learningAnswer: B QUESTION 32How 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 33Which 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 AnyConnectB. Cisco TrustSecC. Cisco ISED. Cisco AMP for EndpointsE. Cisco site-to-site VPNF. Cisco SIO Answer: B QUESTION 34Which 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 35Which 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 36Which 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 37Which 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 TrustSecB. Cisco Data Center Management Policy ImplementationC. Cisco Data Center Virtualization and CloudD. Cisco Cyber Threat DefenseE. Cisco Application Centric InfrastructureF. Cisco Secure Data CenterG. Cisco Security Intelligence Operations Answer: A QUESTION 38Which two advanced malware protection features are available on Cisco AMP for Content? (Choose two.) A. URL filteringB. retrospective securityC. attack chain weavingD. breach huntingE. trajectoryF. behavioral indications of compromise Answer: AB QUESTION 39Which option best describes granular app control using application visibility and control? A. blocking harmful sites based on content, such as pokerstars.comB. blocking World of Warcraft but allowing Google+C. blocking Facebook games but allowing Facebook postsD. blocking Twitter to increase employee productivity Answer: C QUESTION 40The first phase of email security analyzes "who-what-where-when-how" information and context-based policies during which component of threat detection? A. antivirus defenseB. advanced malware protection for emailC. outbreak filtersD. data loss preventionE. encryptionF. antispam defense Answer: F **500-265 dumps full version (PDF&VCE):** https://www.lead2pass.com/500-265.html **Large amount of free 500-265 exam questions on Google Drive:** https://drive.google.com/open?id=0B3Syig5i8gpDMFRoaVJfYURMNmM