

350-701^{Q&As}

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/350-701.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

An organization has two systems in their DMZ that have an unencrypted link between them for communication.

The organization does not have a defined password policy and uses several default accounts on the systems.

The application used on those systems also have not gone through stringent code reviews.

Which vulnerability would help an attacker brute force their way into the systems?

- A. weak passwords
- B. lack of input validation
- C. missing encryption
- D. lack of file permission

Correct Answer: A

Reference: <https://tools.ietf.org/html/rfc3954>

QUESTION 2

A Cisco AMP for Endpoints administrator configures a custom detection policy to add specific MD5 signatures. The configuration is created in the simple detection policy section, but it does not work. What is the reason for this failure?

- A. The administrator must upload the file instead of the hash for Cisco AMP to use.
- B. The MD5 hash uploaded to the simple detection policy is in the incorrect format.
- C. The APK must be uploaded for the application that the detection is intended.
- D. Detections for MD5 signatures must be configured in the advanced custom detection policies.

Correct Answer: D

QUESTION 3

An organization is trying to improve their Defense in Depth by blocking malicious destinations prior to a connection being established. The solution must be able to block certain applications from being used within the network. Which product should be used to accomplish this goal?

- A. Cisco Firepower
- B. Cisco Umbrella
- C. ISE
- D. AMP

Correct Answer: B

Explanation Cisco Umbrella protects users from accessing malicious domains by proactively analyzing and blocking unsafe destinations before a connection is ever made. Thus it can protect from phishing attacks by blocking suspicious domains when users click on the given links that an attacker sent.

QUESTION 4

In which two ways does Easy Connect help control network access when used with Cisco TrustSec? (Choose two)

- A. It allows multiple security products to share information and work together to enhance security posture in the network.
- B. It creates a dashboard in Cisco ISE that provides full visibility of all connected endpoints.
- C. It allows for the assignment of Security Group Tags and does not require 802.1x to be configured on the switch or the endpoint.
- D. It integrates with third-party products to provide better visibility throughout the network.
- E. It allows for managed endpoints that authenticate to AD to be mapped to Security Groups (PassiveID).

Correct Answer: CE

Reference: <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/trustsec-witheasy-connect-configuration-guide.pdf>

QUESTION 5

An organization wants to improve its cybersecurity processes and to add intelligence to its data The organization wants to utilize the most current intelligence data for URL filtering, reputations, and vulnerability information that can be integrated with the Cisco FTD and Cisco WSA What must be done to accomplish these objectives?

- A. Create a Cisco pxGrid connection to NIST to import this information into the security products for policy use
- B. Create an automated download of the Internet Storm Center intelligence feed into the Cisco FTD and Cisco WSA databases to tie to the dynamic access control policies.
- C. Download the threat intelligence feed from the IETF and import it into the Cisco FTD and Cisco WSA databases
- D. Configure the integrations with Talos Intelligence to take advantage of the threat intelligence that it provides.

Correct Answer: D

[Latest 350-701 Dumps](#)

[350-701 Practice Test](#)

[350-701 Study Guide](#)