



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.geekcert.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

What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

- A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
- C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

Correct Answer: B

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c4.html#wp6039879000>

QUESTION 2

Which solution provides end-to-end visibility of applications and insights about application performance?

- A. Cisco AppDynamics
- B. Cisco Tetration
- C. Cisco Secure Cloud Analytics
- D. Cisco Cloudlock

Correct Answer: A

QUESTION 3

What is the function of Cisco Cloudlock for data security?

- A. data loss prevention
- B. controls malicious cloud apps
- C. detects anomalies
- D. user and entity behavior analytics

Correct Answer: A

<https://umbrella.cisco.com/products/casb>

QUESTION 4

What do tools like Jenkins, Octopus Deploy, and Azure DevOps provide in terms of application and infrastructure



automation?

- A. continuous integration and continuous deployment
- B. cloud application security broker
- C. compile-time instrumentation
- D. container orchestration

Correct Answer: A

QUESTION 5

A company discovered an attack propagating through their network via a file. A custom file policy was created in order to track this in the future and ensure no other endpoints execute the infected file. In addition, it was discovered during testing that the scans are not detecting the file as an indicator of compromise. What must be done in order to ensure that the created is functioning as it should?

- A. Create an IP block list for the website from which the file was downloaded
- B. Block the application that the file was using to open
- C. Upload the hash for the file into the policy
- D. Send the file to Cisco Threat Grid for dynamic analysis

Correct Answer: C

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.html

[350-701 Practice Test](#)

[350-701 Study Guide](#)

[350-701 Exam Questions](#)