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.pass4itsure.com/350-701.html

100% Passing Guarantee
100% Money Back Assurance

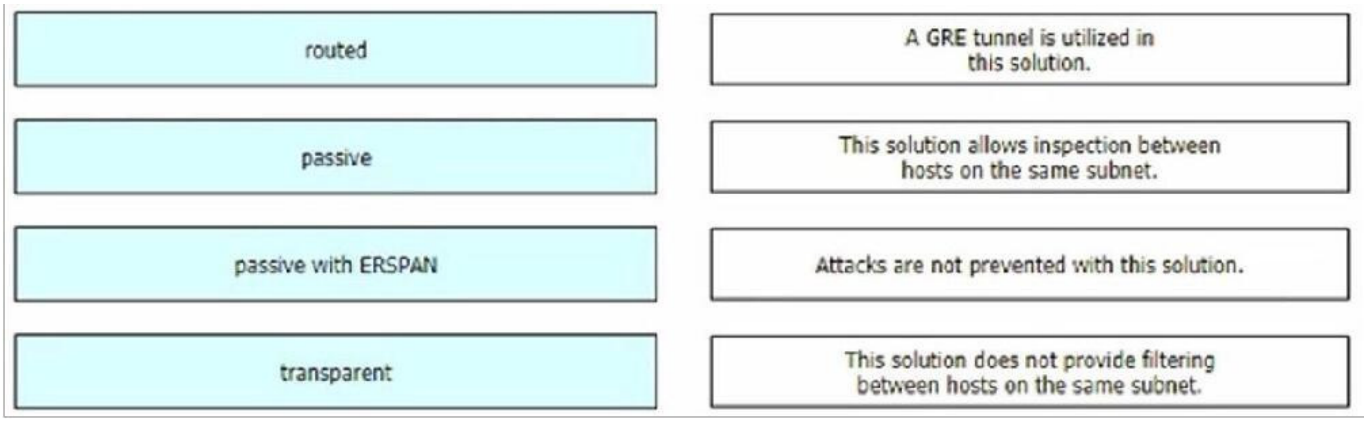
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

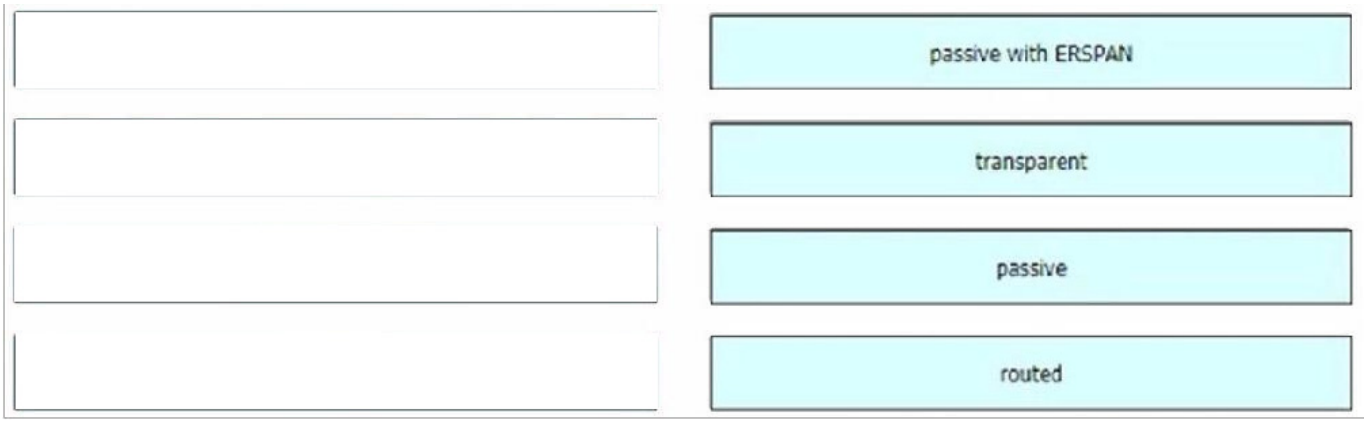
DRAG DROP

Drag and drop the deployment models from the left onto the corresponding explanations on the right.

Select and Place:



Correct Answer:



QUESTION 2

Which two capabilities does an MDM provide? (Choose two.)

A. delivery of network malware reports to an inbox in a schedule

B. unified management of mobile devices, Macs, and PCs from a centralized dashboard

C. enforcement of device security policies from a centralized dashboard

D. manual identification and classification of client devices

E. unified management of Android and Apple devices from a centralized dashboard

Correct Answer: CE

QUESTION 3

Which type of protection encrypts RSA keys when they are exported and imported?

A. file

B. passphrase

C. NGE

D. nonexportable

Correct Answer: B

QUESTION 4

What are two rootkit types? (Choose two)

A. registry

B. virtual

C. bootloader

D. user mode

E. buffer mode

Correct Answer: CD

The term `rootkit\\' originally comes from the Unix world, where the word `root\\' is used to describe a user with thehighest possible level of access privileges, similar to an `Administrator\\' in Windows. The word `kit\\' refers to thesoftware that grants root-level access to the machine. Put the two together and you get `rootkit\\', a program thatgives someone ?with legitimate or malicious intentions ?privileged access to a computer.There are four main types of rootkits: Kernel rootkits, User mode rootkits, Bootloader rootkits, Memory rootkits

QUESTION 5

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

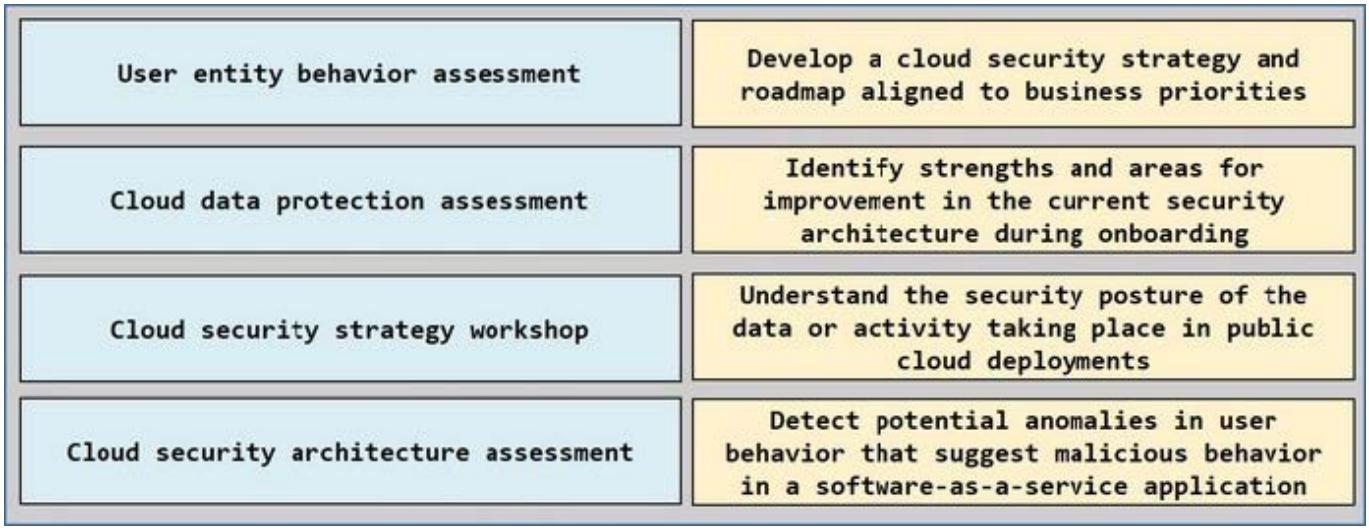
Correct Answer: A

QUESTION 6

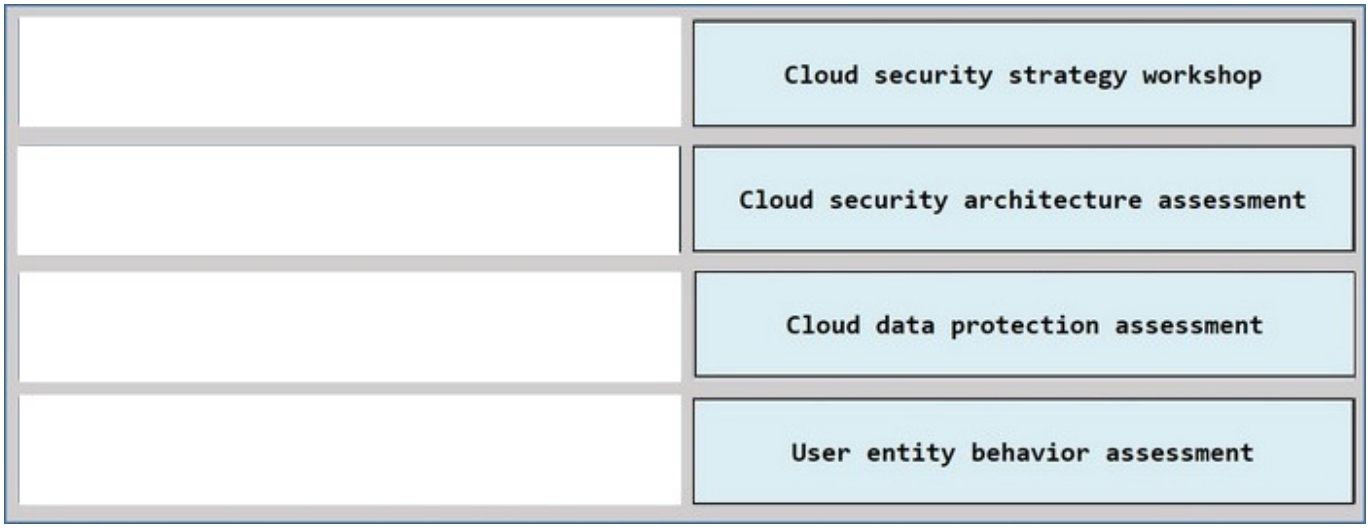
DRAG DROP

Drag and drop the cloud security assessment components from the left onto the definitions on the right.

Select and Place:



Correct Answer:



QUESTION 7

Refer to the exhibit.

```
SwitchA(config)#interface gigabitethernet1/0/1
SwitchA(config-if)#dot1x host-mode multi-host
SwitchA(config-if)#dot1x timeout quiet-period 3
SwitchA(config-if)#dot1x timeout tx-period 15
SwitchA(config-if)#authentication port-control
auto
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 12
```

An engineer configured wired 802.1x on the network and is unable to get a laptop to authenticate. Which port configuration is missing?

A. authentication open

B. dotlx reauthentication

C. cisp enable

D. dot1x pae authenticator

Correct Answer: D

QUESTION 8

A large organization wants to deploy a security appliance in the public cloud to form a site- to-site VPN and link the public cloud environment to the private cloud in the headquarters data center. Which Cisco security appliance meets these requirements?

A. Cisco Cloud Orchestrator

B. Cisco ASAV

C. Cisco WSAV

D. Cisco Stealthwatch Cloud

Correct Answer: B

QUESTION 9

Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

A. TLSv1.2

B. TLSv1.1

C. BJTLSv1

D. DTLSv1

Correct Answer: D

DTLS is used for delay sensitive applications (voice and video) as its UDP based while TLS is TCP based.Therefore DTLS offers strongest throughput performance. The throughput of DTLS at the time of AnyConnect connection can be expected to have processing performance close to VPN throughput.

QUESTION 10

An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable to WannaCry ransomware. Which two solutions mitigate the risk of this ransom ware infection? (Choose two)

A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.

B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.

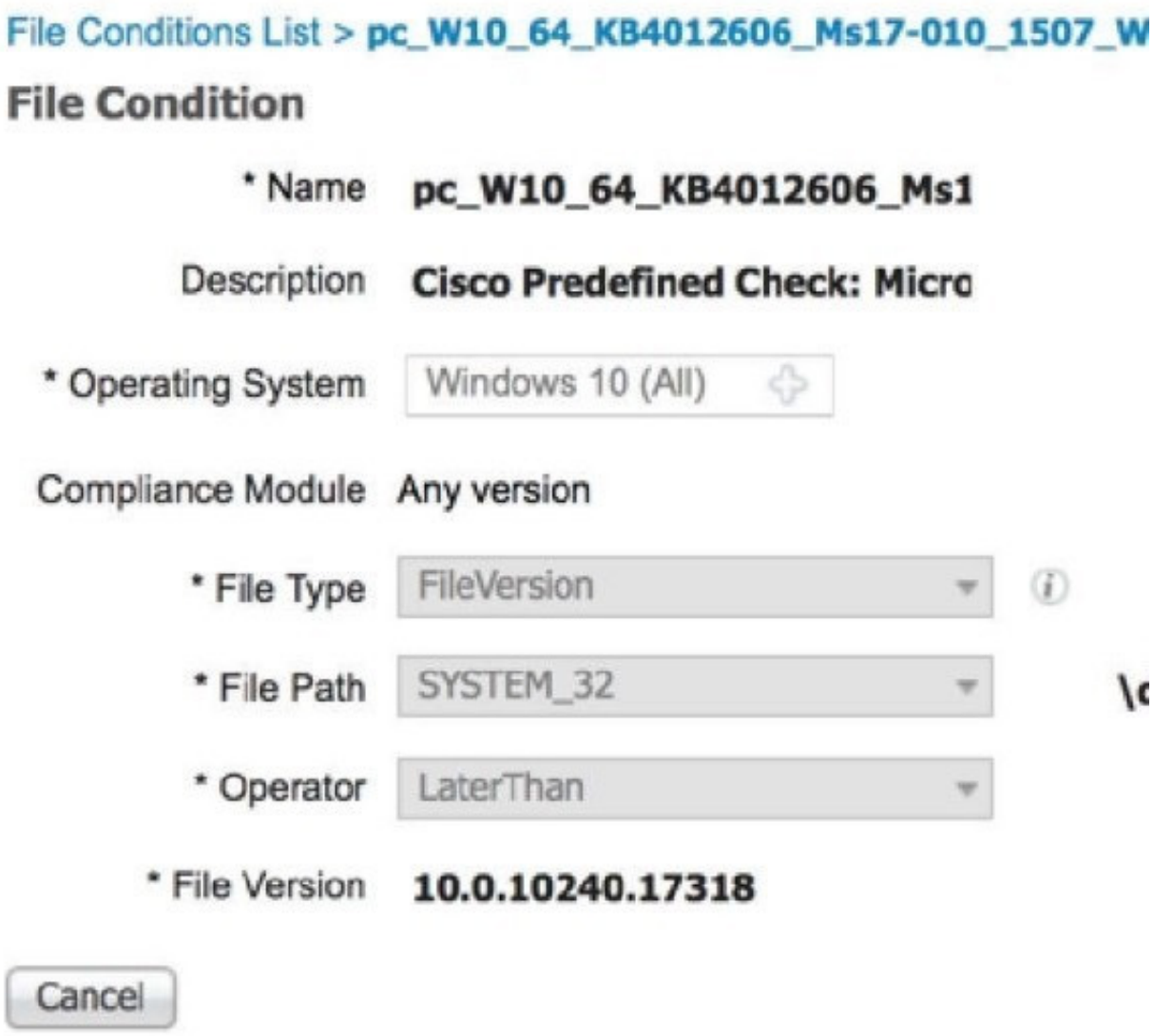
C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.

D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.

E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Correct Answer: AC

A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. We can configure ISE to check for the Windows patch at Work Centers > Posture > Posture Elements > Conditions > File.In this example, we are going to use the predefined file check to ensure that our Windows 10 clients have the critical security patch installed to prevent the Wanna Cry malware.



QUESTION 11

An administrator configures a new destination list in Cisco Umbrella so that the organization can block specific domains for its devices. What should be done to ensure that all subdomains of domain.com are blocked?

A. Configure the *.com address in the block list.

B. Configure the *.domain.com address in the block list

C. Configure the *.domain.com address in the block list

D. Configure the domain.com address in the block list

Correct Answer: C

QUESTION 12

What is a functional difference between Cisco AMP for Endpoints and Cisco Umbrella Roaming Client?

A. The Umbrella Roaming client stops and tracks malicious activity on hosts, and AMP for Endpoints tracks only URL-based threats.

B. The Umbrella Roaming Client authenticates users and provides segmentation, and AMP for Endpoints allows only for VPN connectivity

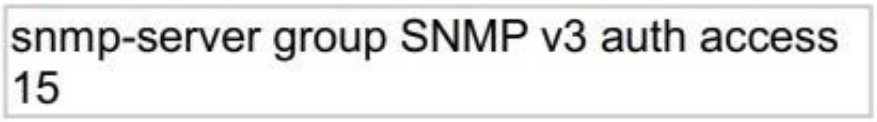
C. AMP for Endpoints authenticates users and provides segmentation, and the Umbrella Roaming Client allows only for VPN connectivity.

D. AMP for Endpoints stops and tracks malicious activity on hosts, and the Umbrella Roaming Client tracks only URL-based threats.

Correct Answer: B

QUESTION 13

Refer to the exhibit.



What does the number 15 represent in this configuration?

A. privilege level for an authorized user to this router

B. access list that identifies the SNMP devices that can access the router

C. interval in seconds between SNMPv3 authentication attempts

D. number of possible failed attempts until the SNMPv3 user is locked out

Correct Answer: B

The syntax of this command is shown below: snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list] The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don\\'t come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

QUESTION 14

Which attack is commonly associated with C and C++ programming languages?

A. cross-site scripting

B. water holing

C. DDoS

D. buffer overflow

Correct Answer: D

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations. Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it\\'s alloted memory space. This happens quite frequently in the case of arrays.

QUESTION 15

For a given policy in Cisco Umbrella, how should a customer block website based on a custom list?

A. by specifying blocked domains in me policy settings

B. by specifying the websites in a custom blocked category

C. by adding the websites to a blocked type destination list

D. by adding the website IP addresses to the Cisco Umbrella blocklist

Correct Answer: C