350-701$^{\text{Q\&As}}$

Implementing and Operating Cisco Security Core Technologies (SCOR)

QUESTION 1

What is a description of microsegmentation?

A. Environments deploy a container orchestration platform, such as Kubernetes, to manage the application delivery.

B. Environments apply a zero-trust model and specify how applications on different servers or containers can communicate.

C. Environments deploy centrally managed host-based firewall rules on each server or container.

D. Environments implement private VLAN segmentation to group servers with similar applications.

Correct Answer: B

QUESTION 2

Which Cisco ASA deployment model is used to filter traffic between hosts in the same IP subnet using higher-level protocols without readdressing the network?

A. routed mode

B. transparent mode

C. single context mode

D. multiple context mode

Correct Answer: B

QUESTION 3

A hacker initiated a social engineering attack and stole username and passwords of some users within a company. Which product should be used as a solution to this problem?

A. Cisco NGFW

B. Cisco AnyConnect

C. Cisco AMP for Endpoints

D. Cisco Duo

Correct Answer: D

QUESTION 4

What is the primary benefit of deploying an ESA in hybrid mode?

A. You can fine-tune its settings to provide the optimum balance between security and performance for your environment

B. It provides the lowest total cost of ownership by reducing the need for physical appliances

C. It provides maximum protection and control of outbound messages

D. It provides email security while supporting the transition to the cloud

Correct Answer: D

Cisco Hybrid Email Security is a unique service offering that facilitates the deployment of your email securityinfrastructure both on premises and in the cloud. You can change the number of on-premises versus cloudusers at any time throughout the term of your contract, assuming the total number of users does not change.This allows for deployment flexibility as your organization\\'s needs change.

QUESTION 5

Which Cisco product is open, scalable, and built on IETF standards to allow multiple security products from Cisco and other vendors to share data and interoperate with each other?

A. Advanced Malware Protection

B. Platform Exchange Grid

C. Multifactor Platform Integration

D. Firepower Threat Defense

Correct Answer: B

With Cisco pxGrid (Platform Exchange Grid), your multiple security products can now share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster.

QUESTION 6

An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10. What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

A. Cisco Identity Services Engine and AnyConnect Posture module

B. Cisco Stealthwatch and Cisco Identity Services Engine integration

C. Cisco ASA firewall with Dynamic Access Policies configured

D. Cisco Identity Services Engine with PxGrid services enabled

Correct Answer: A

QUESTION 7

What is the function of SDN southbound API protocols?

A. to allow for the dynamic configuration of control plane applications

B. to enable the controller to make changes

C. to enable the controller to use REST

D. to allow for the static configuration of control plane applications

Correct Answer: B

Reference: https://www.ciscopress.com/articles/article.asp?p=3004581andseqNum=2 Note: Southbound APIs helps us communicate with data plane (not control plane) applications

QUESTION 8

Which two capabilities does TAXII support? (Choose two)

A. Exchange

B. Pull messaging

C. Binding

D. Correlation

E. Mitigating

Correct Answer: AB

https://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.html

"There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery." "Discovery does, however, allow for the automated exchange of information..."

QUESTION 9

Which two components do southbound APIs use to communicate with downstream devices? (Choose two.)

A. services running over the network

B. OpenFlow

C. external application APIs

D. applications running over the network

E. OpFlex

Correct Answer: BE

QUESTION 10

Which two risks is a company vulnerable to if it does not have a well-established patching solution for endpoints? (Choose two)

A. exploits

B. ARP spoofing

C. denial-of-service attacks

D. malware

E. eavesdropping

Correct Answer: AD

Malware means "malicious software", is any software intentionally designed to cause damage to a computer, server, client, or computer network. The most popular types of malware includes viruses, ransomware and spyware. Virus Possibly

the most common type of malware, viruses attach their malicious code to clean code and wait to be run.

Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again.Spyware is spying software that can secretly record everything you enter, upload,

download, and store on your computers or mobile devices. Spyware always tries to keep itself hidden.An exploit is a code that takes advantage of a software vulnerability or security flaw.Exploits and malware are two risks for endpoints that

are not up to date. ARP spoofing and eavesdropping are attacks against the network while denial-of-service attack is based on the flooding of IP packets.

QUESTION 11

Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

A. Group Policy

B. Access Control Policy

C. Device Management Policy

D. Platform Service Policy

Correct Answer: D

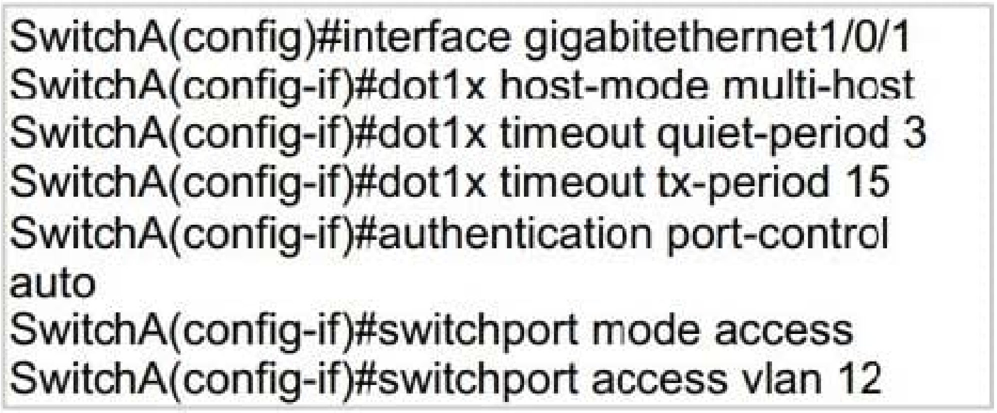
Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc- configguide-v62/platform_settings_policies_for_managed_devices.html

Therefore the answer should be "Platform Settings Policy", not "Platform Service Policy" but it is the bestanswer here so we have to choose it.

QUESTION 12

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 13

Which Cisco network security device supports contextual awareness?

A. ISE

B. Cisco IOS

C. Cisco ASA

D. Firepower

Correct Answer: A

QUESTION 14

A network engineer has been tasked with adding a new medical device to the network. Cisco ISE is being used as the NAC server, and the new device does not have a supplicant available. What must be done in order to securely connect this device to the network?

A. Use MAB with profiling

B. Use MAB with posture assessment.

C. Use 802.1X with posture assessment.

D. Use 802.1X with profiling.

Correct Answer: A

Reference: https://community.cisco.com/t5/security-documents/ise-profiling-design- guide/ta-p/3739456

QUESTION 15

An engineer is configuring their router to send NetfFow data to Stealthwatch which has an IP address of 1.1.1.1 using the flow record Stealthwatch406143794 command. Which additional command is required to complete the flow record?

A. transport udp 2055

B. match ipv4 ttl

C. cache timeout active 60

D. destination 1.1.1.1

Correct Answer: B

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/config-trouble-netflow-stealth.pdf