DUMPSBOSS.

Implementing and Operating Cisco Security Core Technologies (SCOR 350-701)

Cisco 350-701

Version Demo

Total Demo Questions: 20

Total Premium Questions: 687

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, New Update	355
Topic 2, Security Concepts	68
Topic 3, Network Security	82
Topic 4, Securing the Cloud	36
Topic 5, Content Security	46
Topic 6, Endpoint Protection and Detection	36
Topic 7, Secure Network Access, Visibility, and Enforcement	64
Total	687

QUESTION NO: 1

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.) The eDirectory client must be installed on each client workstation.

A. Create NTLM or Kerberos authentication realm and enable transparent user identification

B. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.

C. Create an LDAP authentication realm and disable transparent user identification.

D. Deploy a separate eDirectory server: the client IP address is recorded in this server

ANSWER: A B

Explanation:

 Transparently identify users with authentication realms – This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:

o Active Directory – Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory.

o LDAP – Create an LDAP authentication realm configured as an eDirectory, and enable transparent user identification. For more information, see Transparent User Identification with LDAP.

Details:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01001.html#:~:text=Transparently%20identify%20users%20with%20authentication,User%20Identification%20with%20LDAP.

QUESTION NO: 2

What is an advantage of the Cisco Umbrella roaming client?

A. the ability to see all traffic without requiring TLS decryption

B. visibility into IP-based threats by tunneling suspicious IP connections

C. the ability to dynamically categorize traffic to previously uncategorized sites

D. visibility into traffic that is destined to sites within the office environment

ANSWER: C

QUESTION NO: 3

What are two ways that Cisco Container Platform provides value to customers who utilize cloud service providers? (Choose two.)

A. Allows developers to create code once and deploy to multiple clouds

B. helps maintain source code for cloud deployments

C. manages Docker containers

D. manages Kubernetes clusters

E. Creates complex tasks for managing code

ANSWER: A E

QUESTION NO: 4

An administrator is adding a new Cisco ISE node to an existing deployment. What must be done to ensure that the addition of the node will be successful when inputting the FQDN?

A. Change the IP address of the new Cisco ISE node to the same network as the others.

B. Make the new Cisco ISE node a secondary PAN before registering it with the primary.

C. Open port 8905 on the firewall between the Cisco ISE nodes.

D. Add the DNS entry for the new Cisco ISE node into the DNS server.

ANSWER: A

QUESTION NO: 5

Which type of attack is MFA an effective deterrent for?

A. ping of death

B. phishing

C. teardrop

D. syn flood

ANSWER: B

QUESTION NO: 6

Which two actions does the Cisco Identity Services Engine posture module provide that ensures endpoint security? (Choose two.)

A. Assignments to endpoint groups are made dynamically, based on endpoint attributes.

B. Endpoint supplicant configuration is deployed.

C. A centralized management solution is deployed.

D. Patch management remediation is performed.

E. The latest antivirus updates are applied before access is allowed.

ANSWER: A D

QUESTION NO: 7

Which two mechanisms are used to control phishing attacks? (Choose two.)

A. Enable browser alerts for fraudulent websites.

B. Define security group memberships.

C. Revoke expired CRL of the websites.

D. Use antispyware software.

E. Implement email filtering techniques.

ANSWER: A E

QUESTION NO: 8

What is the term for having information about threats and threat actors that helps mitigate harmful events that would otherwise compromise networks or systems?

A. trusted automated exchange

B. Indicators of Compromise

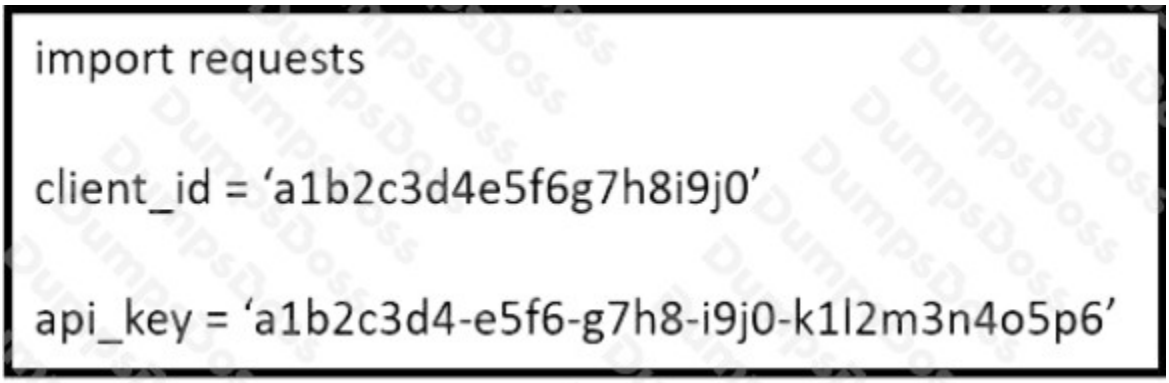
C. The Exploit Database

D. threat intelligence

ANSWER: D

QUESTION NO: 9

Refer to the exhibit.



What does the API key do while working with https://api.amp.cisco.com/v1/computers?

A. displays client ID

B. HTTP authorization

C. Imports requests

D. HTTP authentication

ANSWER: D

QUESTION NO: 10

An engineer needs to add protection for data in transit and have headers in the email message Which configuration is needed to accomplish this goal?

A. Provision the email appliance

B. Deploy an encryption appliance.

C. Map sender !P addresses to a host interface.

D. Enable flagged message handling

ANSWER: D

QUESTION NO: 11

Which two parameters are used for device compliance checks? (Choose two.)

A. endpoint protection software version

B. Windows registry values

C. DHCP snooping checks

D. DNS integrity checks

E. device operating system version

ANSWER: C E

QUESTION NO: 12

An organization deploys multiple Cisco FTD appliances and wants to manage them using one centralizedsolution. The organization does not have a local VM but does have existing Cisco ASAs that must migrate overto Cisco FTDs. Which solution meets the needs of the organization?

A. Cisco FMC

B. CSM

C. Cisco FDM

D. CDO

ANSWER: B

QUESTION NO: 13

A company has 5000 Windows users on its campus. Which two precautions should IT take to prevent WannaCry ransomware from spreading to all clients? (Choose two.)

A. Segment different departments to different IP blocks and enable Dynamic ARp inspection on all VLANs

B. Ensure that noncompliant endpoints are segmented off to contain any potential damage.

C. Ensure that a user cannot enter the network of another department.

D. Perform a posture check to allow only network access to (hose Windows devices that are already patched.

E. Put all company users in the trusted segment of NGFW and put all servers to the DMZ segment of the Cisco NGFW. ni

ANSWER: B D

QUESTION NO: 14

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

A. Create an LDAP authentication realm and disable transparent user identification.

B. Create NTLM or Kerberos authentication realm and enable transparent user identification.

C. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.

D. The eDirectory client must be installed on each client workstation.

E. Deploy a separate eDirectory server; the dent IP address is recorded in this server.

ANSWER: A C

QUESTION NO: 15

An engineer needs a cloud solution that will monitor traffic, create incidents based on events, and integrate withother cloud solutions via an API. Which solution should be used to accomplish this goal?

A. SIEM

B. CASB

C. Adaptive MFA

D. Cisco Cloudlock

ANSWER: D

Explanation:

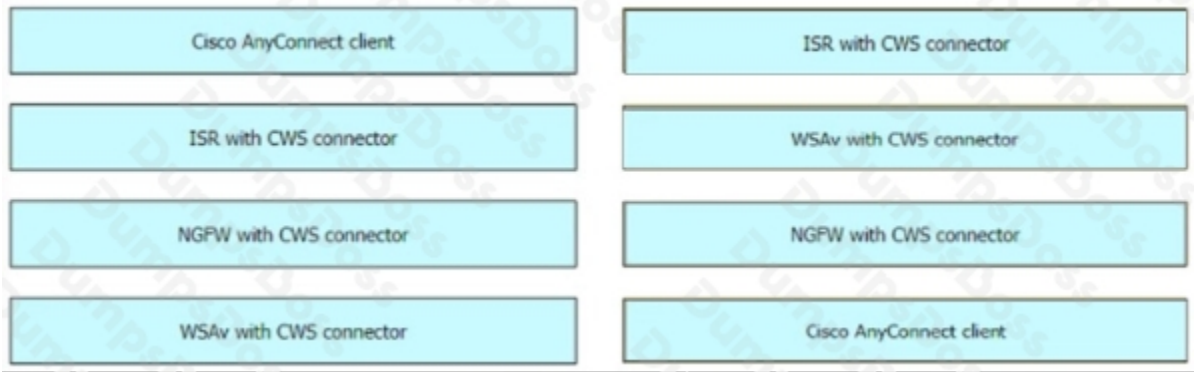
ExplanationExplanation+ Cisco Cloudlock continuously monitors cloud environments with a cloud Data Loss Prevention (DLP) engineto identify sensitive information stored in cloud environments in violation of policy.+ Cloudlock is API-based.+ Incidents are a key resource in the Cisco Cloudlock application. They are triggered by the Cloudlock policy engine when a policy detection criteria result in a match in an object (document, field, folder, post, or file).Reference: https://docs.umbrella.com/cloudlock-documentation/docs/endpointsNote:+ Security information and event management (SIEM) platforms collect log and event data from securitysystems, networks and computers, and turn it into actionable security insights.+ An incident is a record of the triggering of an alerting policy. Cloud Monitoring opens an incident when acondition of an alerting policy has been met.

QUESTION NO: 16 - (DRAG DROP)

Drag and drop the Cisco CWS redirection options from the left onto the capabilities on the right.

ANSWER:

Explanation:



Reference: https://www.westconcomstor.com/medias/CWS-data-sheet-c78-729637-1-.pdf?context=bWFzdGVyfHJvb3R8Mjg2MDA4fGFwcGxpY2F0aW9uL3BkZnxoY2QvaDhjLzg3OTcwOTc0OTI1MTAucGRmfDc1MzU2MjFhZmNiOTkwOWNjMDI5ZTFmZmRkYzQ3MzZiZGIyMjE1YzgwZWU1NTFhMTM2YjVhM2UxMjJlNGU5OGQ

QUESTION NO: 17

What is the Cisco API-based broker that helps reduce compromises, application risks, and data breaches in an environment that is not on-premise?

A. Cisco AppDynamics

B. Cisco Cloudlock

C. Cisco Umbrella

D. Cisco AMP

ANSWER: B

QUESTION NO: 18

Due to a traffic storm on the network, two interfaces were error-disabled, and both interfaces sent SNMP traps.Which two actions must be taken to ensure that interfaces are put back into service? (Choose two)

A. Have Cisco Prime Infrastructure issue an SNMP set command to re-enable the ports after the preconfigured interval.

B. Use EEM to have the ports return to service automatically in less than 300 seconds.

C. Enter the shutdown and no shutdown commands on the interfaces.

D. Enable the snmp-server enable traps command and wait 300 seconds

E. Ensure that interfaces are configured with the error-disable detection and recovery feature

ANSWER: C E

Explanation:

ExplanationExplanationYou can also bring up the port by using these commands:+ The “shutdown” interface configuration command followed by the “no shutdown” interface configurationcommand restarts the disabled port.+ The “errdisable recovery cause …” global configuration command enables the timer to automatically recover error-disabled state, and the “errdisable recovery interval interval” global configuration command specifies the time to recover error-disabled state.

QUESTION NO: 19

Refer to the exhibit.

```
ASA#  show  service-policy sfr

Global policy:
  Service-policy:  global_policy
    Class-map:  SFR
      SFR:  card status Up,  mode fail-open monitor-only
        Packet input 0, packet output [redacted]  drop 0,  reset-drop 0
```

What are two indications of the Cisco Firepower Services Module configuration?

(Choose two.)

A. The module is operating in IDS mode.

B. Traffic is blocked if the module fails.

C. The module fails to receive redirected traffic.

D. The module is operating in IPS mode.

E. Traffic continues to flow if the module fails.

ANSWER: A E

Explanation:

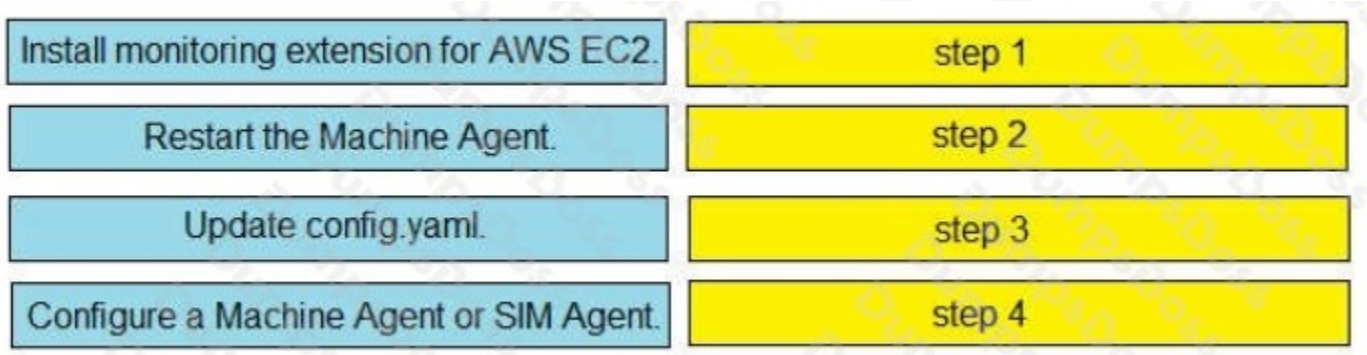
sfr {fail-open | fail-close [monitor-only]} <- There's a couple different options here. The first one is fail-open which means that if the Firepower software module is unavailable, the ASA will continue to forward traffic. fail-close means that if the Firepower module fails, the traffic will stop flowing. While this doesn't seem ideal, there might be a use case for it when securing highly regulated environments. The monitor-only switch can be used with both and basically puts the Firepower services into IDS-mode only. This might be useful for initial testing or setup.

QUESTION NO: 20 - (DRAG DROP)

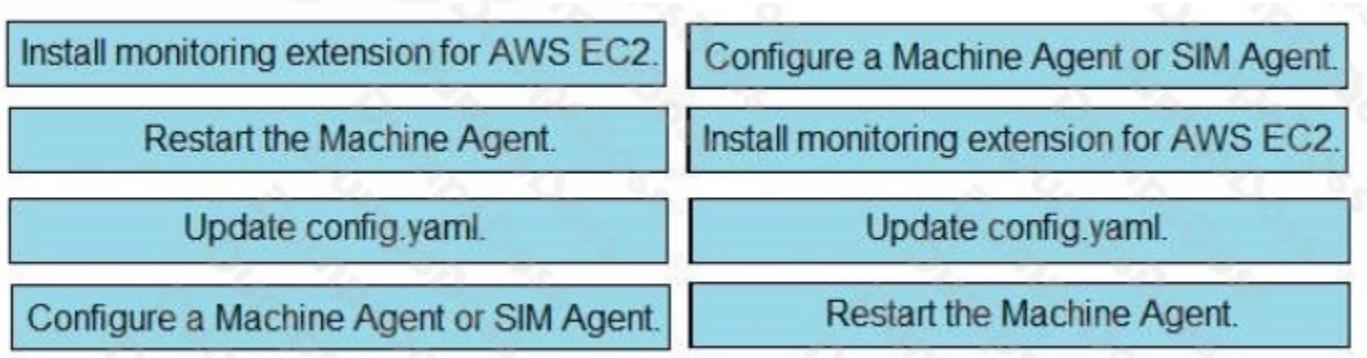
DRAG DROP

Drag and drop the steps from the left into the correct order on the right to enable Cisco AppDynamics to monitor an EC2 instance in AWS.

Select and Place:



ANSWER:



Explanation: