DUMPSBOSS.COM

Implementing and Operating Cisco Security Core Technologies

Cisco 350-701

Version Demo

Total Demo Questions: 20

Total Premium Questions: 687

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

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

Which cloud model is a collaborative effort where infrastructure is shared and jointly accessed by several organizations from a specific group?

A. community

B. private

C. public

D. hybrid

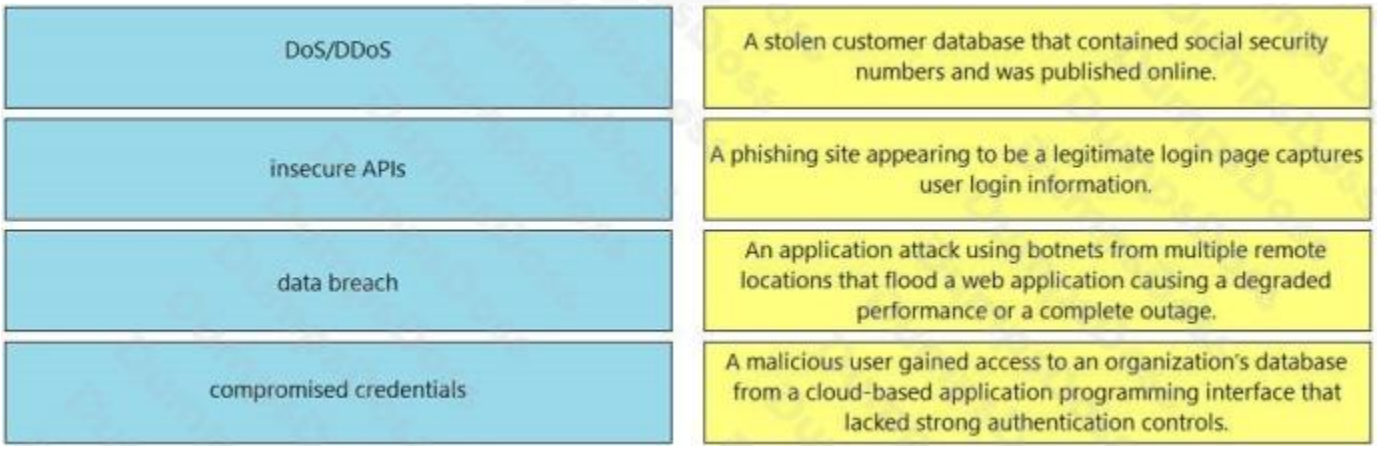
ANSWER: A

QUESTION NO: 2 - (DRAG DROP)

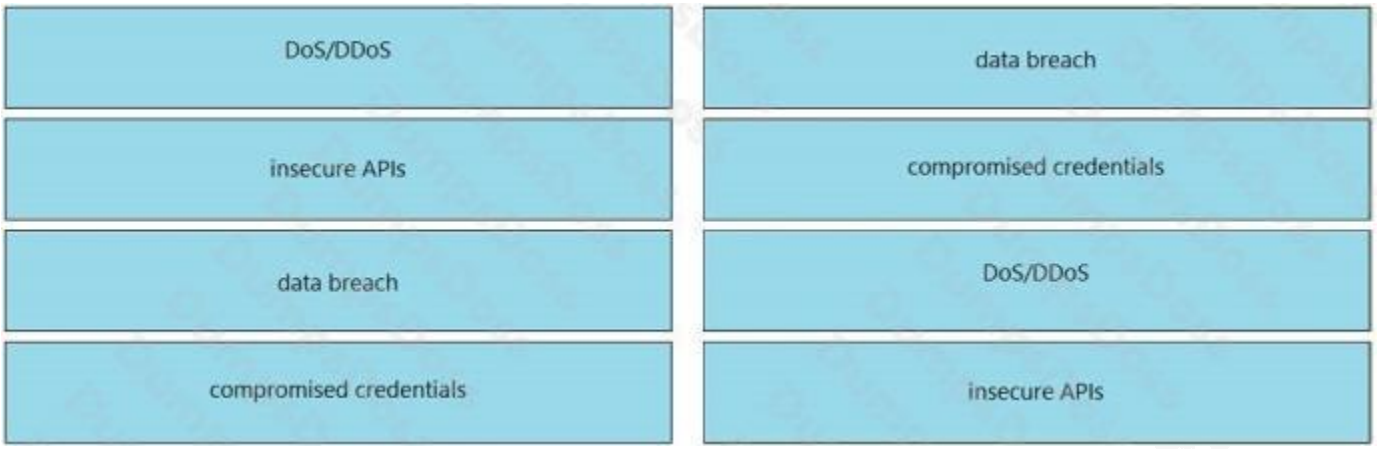
DRAG DROP

Drag and drop the threats from the left onto examples of that threat on the right.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 3

Which two key and block sizes are valid for AES? (Choose two.)

A. 64-bit block size, 112-bit key length

B. 64-bit block size, 168-bit key length

C. 128-bit block size, 192-bit key length

D. 128-bit block size, 256-bit key length

E. 192-bit block size, 256-bit key length

ANSWER: C D

Explanation:

Reference: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

QUESTION NO: 4

What are two Trojan malware attacks? (Choose two)

A. Frontdoor

B. Rootkit

C. Smurf

D. Backdoor

E. Sync

ANSWER: B D

QUESTION NO: 5

Which feature requires a network discovery policy on the Cisco Firepower NGIPS?

A. security intelligence

B. impact flags

C. health monitoring

D. URL filtering

ANSWER: A

QUESTION NO: 6

Which term describes when the Cisco Firepower downloads threat intelligence updates from Cisco Talos?

A. consumption

B. sharing

C. analysis

D. authoring

ANSWER: A

Explanation:

ExplanationExplanation… we will showcase Cisco Threat Intelligence Director (CTID) an exciting feature on Cisco's FirepowerManagement Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads/downloads of STIX and simple blacklists. Reference: https://blogs.cisco.com/developer/automate-threat-intelligence-using-cisco-threat-intelligencedirector

QUESTION NO: 7

Which two aspects of the cloud PaaS model are managed by the customer but not the provider? (Choose two.)

A. middleware

B. applications

C. virtualization

D. operating systems

E. data

ANSWER: B E

QUESTION NO: 8

While using Cisco Firepower's Security Intelligence policies, which two criteria is blocking based upon? (Choose two.)

A. IP addresses

B. URLs

C. port numbers

D. protocol IDs

E. MAC addresses

ANSWER: A B

QUESTION NO: 9

What are two recommended approaches to stop DNS tunneling for data exfiltration and command and control call backs? (Choose two.)

A. Use intrusion prevention system.

B. Block all TXT DNS records.

C. Enforce security over port 53.

D. Use next generation firewalls.

E. Use Cisco Umbrella.

ANSWER: C E

QUESTION NO: 10

A network engineer entered the snmp-server user asmith myv7 auth sha cisco priv aes 256

cisc0xxxxxxxxx command and needs to send SNMP information to a host at 10.255.255.1. Which

command achieves this goal?

A. snmp-server host inside 10.255.255.1 version 3 myv7

B. snmp-server host inside 10.255.255.1 snmpv3 myv7

C. snmp-server host inside 10.255.255.1 version 3 asmith

D. snmp-server host inside 10.255.255.1 snmpv3 asmith

ANSWER: C

QUESTION NO: 11

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: 12

Which system performs compliance checks and remote wiping?

A. MDM

B. ISE

C. AMP

D. OTP

ANSWER: A

QUESTION NO: 13

What are two functions of IKEv1 but not IKEv2? (Choose two)

A. NAT-T is supported in IKEv1 but rot in IKEv2.

B. With IKEv1, when using aggressive mode, the initiator and responder identities are passed cleartext

C. With IKEv1, mode negotiates faster than main mode

D. IKEv1 uses EAP authentication

E. IKEv1 conversations are initiated by the IKE_SA_INIT message

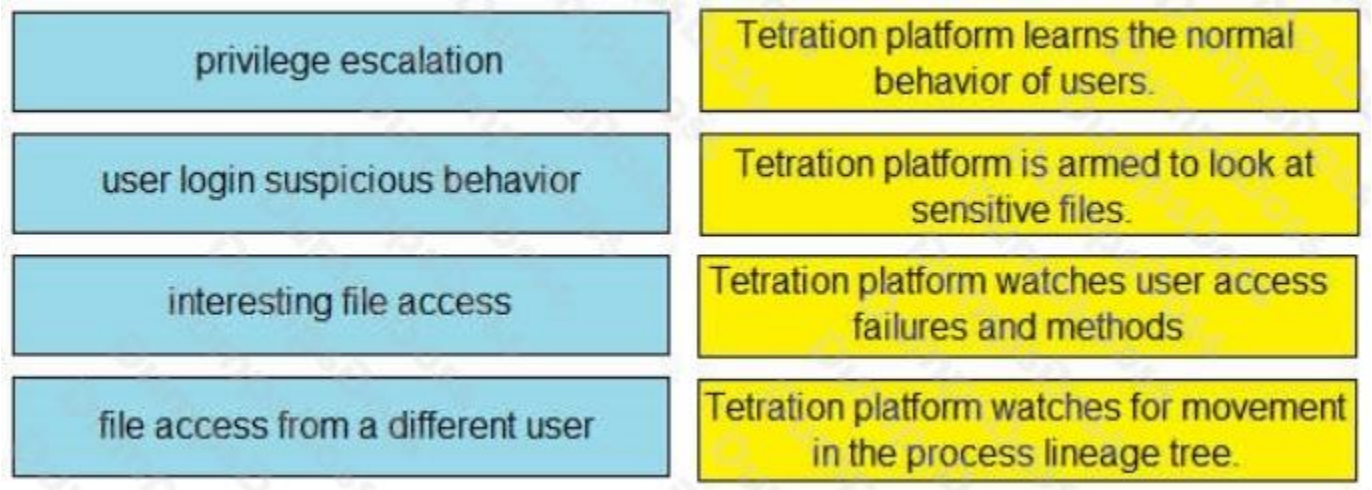
ANSWER: C E

QUESTION NO: 14 - (DRAG DROP)

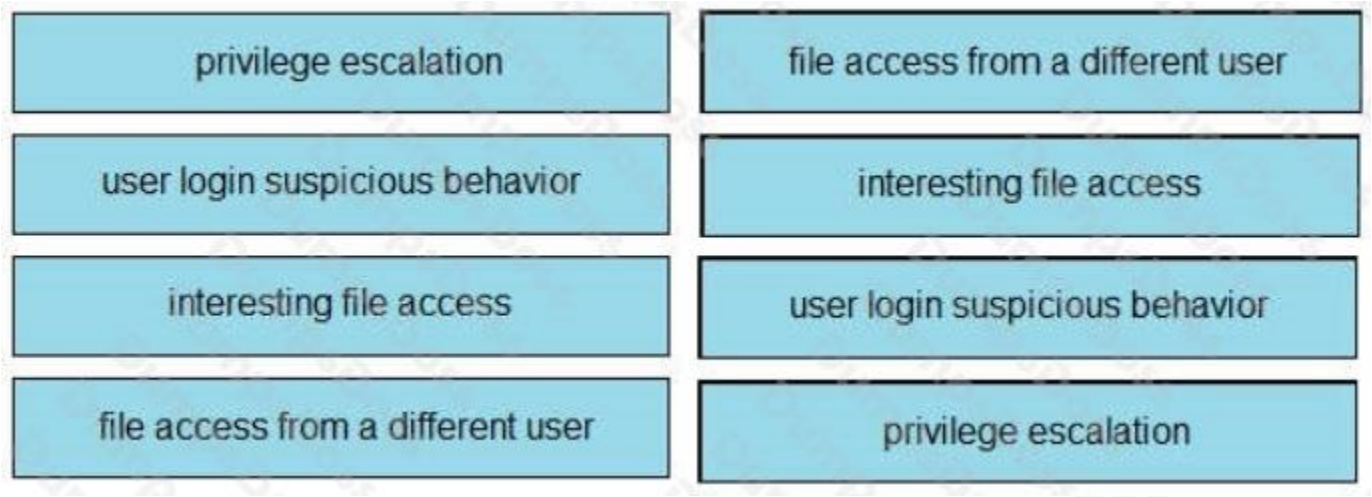
DRAG DROP

Drag and drop the suspicious patterns for the Cisco Tetration platform from the left onto the correct definitions on the right.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 15

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

ANSWER: C

QUESTION NO: 16

What are two benefits of using an MDM solution? (Choose two.)

A. grants administrators a way to remotely wipe a lost or stolen device

B. provides simple and streamlined login experience for multiple applications and users

C. native integration that helps secure applications across multiple cloud platforms or on-premises environments

D. encrypts data that is stored on endpoints

E. allows for centralized management of endpoint device applications and configurations

ANSWER: A E

QUESTION NO: 17

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

ANSWER: A

Explanation:

Reference:
https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/administration/guide/b_AnyConnect_Administrator_Guide_4-6/configure-posture.html

QUESTION NO: 18

Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings

B. content categories

C. security settings

D. destination lists

ANSWER: D

QUESTION NO: 19

Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)

A. phishing

B. brute force

C. man-in-the-middle

D. DDOS

E. tear drop

ANSWER: B C

QUESTION NO: 20

What is the purpose of the Cisco Endpoint IoC feature?

A. It provides stealth threat prevention.

B. It is a signature-based engine.

C. It is an incident response tool

D. It provides precompromise detection.

ANSWER: C

Explanation:

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Secure_Managed_Endpoint.pdf